Tivoli® OMEGAMON XE for Mainframe Networks

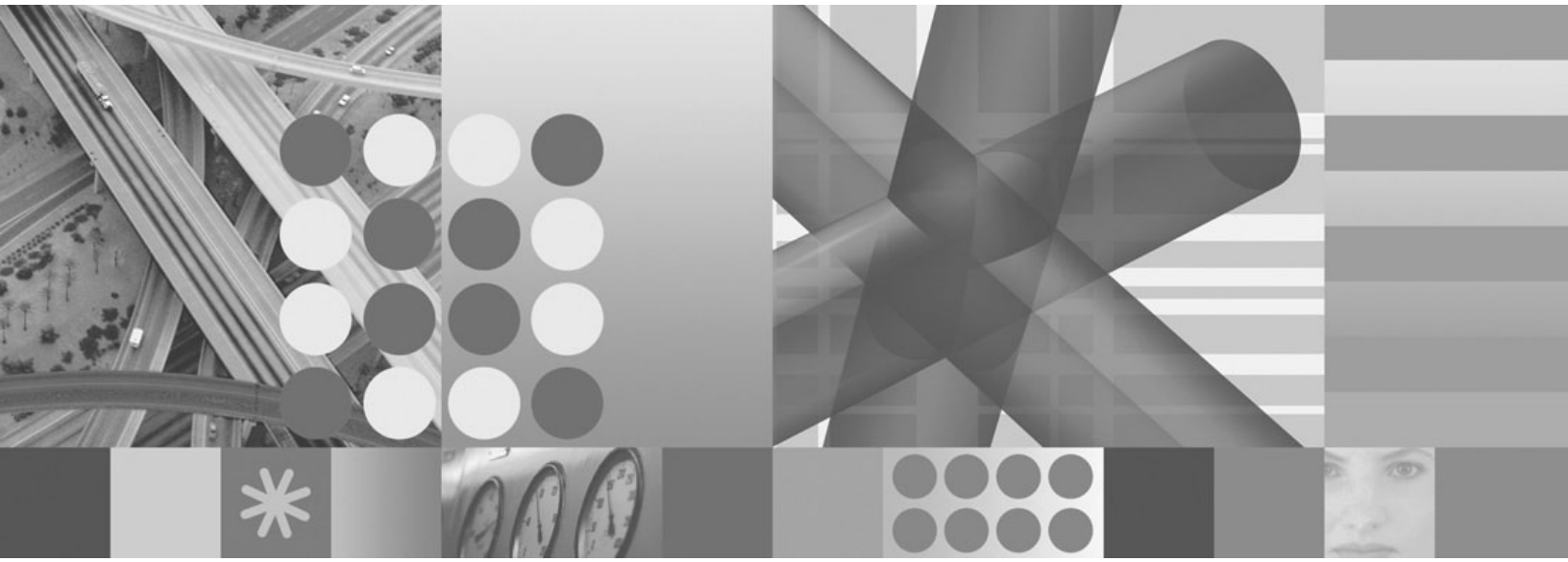
Version 4.1.0

Fix Pack 001 Readme and Documentation Addendum

GI11-8116-00

Tivoli® OMEGAMON XE for Mainframe Networks

Version 4.1.0



Fix Pack 001 Readme and Documentation Addendum

GI11-8116-00

Note

Before using this information and the product it supports, read the information in Appendix C, “Notices,” on page 169.

This edition applies to version 4, release 1, modification 0 of IBM Tivoli OMEGAMON XE for Mainframe Networks (program number 5698-A35) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

Chapter 1. What this book describes

This book describes the various enhancements in the IBM® Tivoli® OMEGAMON® XE for Mainframe Networks version 4 release 1 Fix Pack 001. Most of the updates in Fix Pack 001 were made to support the z/OS® Communication Server network management interface (NMI) enhancements in z/OS versions 1.8 and 1.9 that enable IP Security (IPSec) monitoring.

Table 1. Fix pack contents

Description	Information
New planning considerations	Chapter 2, “New planning information,” on page 7
New configuration information	Chapter 3, “New configuration required for IPSec,” on page 19
New filters, attribute tables, and linking	Chapter 4, “New filters, attribute tables, and linking,” on page 25
New attribute groups	Chapter 5, “New and changed attribute groups,” on page 27
New workspaces	Chapter 6, “New and updated workspaces,” on page 63
New situations	Chapter 7, “New IPSec situations,” on page 141
New commands	Chapter 8, “New and changed KN3FCCMD commands,” on page 147
New messages	Chapter 9, “New and changed messages and problem determination,” on page 153

New function since version 4.1 availability

By applying this OMEGAMON XE for Mainframe Networks fix pack, you have support for the following features:

- Support for z/OS version 1.9, including toleration for Address Space (ASID) reuse. Support was delivered in a previous APAR.

  The z/OS ASID Reuse function enables an address space to be created with a reusable ASID. If you use the End to End Response Time Monitor (ETE™), you can now specify REUSASID=YES on the ETE startup procedures.
- Monitoring IP filters and IPSec tunnels on z/OS version 1.8 or higher.
- New workspaces and attribute groups to enable monitoring of the IP security (IPSec) enhancement available in z/OS version 1.8. IPSec is an emerging Internet security standard developed by the IETF (Internet Engineering Task Force). It defines security extensions to the Internet Protocol (IP) that allows any two IP machines (such as hosts, routers, or gateways) to communicate securely over the Internet by authenticating and encrypting the traffic between them. By securing data at the IP layer, IPSec also provides transparent security to higher-layer protocols and applications. These new workspaces enable you to:
  - Monitor the effect of IP filters defined for the TCP/IP stacks of a z/OS system on traffic traversing the stacks.
  - Monitor the performance of IPSec tunnels for which a z/OS system TCP/IP stack is an endpoint.
  - Monitor the performance of Internet Key Exchange (IKE) tunnels for which the IKE daemon on a z/OS system is an endpoint.
  - Perform problem determination for problems related to filters and IPSec security associations.

Table 2. New IPSec workspaces

Workspace name	New or changed displayed attributes
IPSec Status	"IPSec Status Attributes (KN3ISS)" on page 51
IP Filters Statistics	"IPSec Status Attributes (KN3ISS)" on page 51
Current IP Filters	"Current IP Filters Attributes (KN3IFC)" on page 27
Current IP Filters by Destination Address	"Current IP Filters Attributes (KN3IFC)" on page 27
Current IP Filters by Filter Rule Definition Name	"Current IP Filters Attributes (KN3IFC)" on page 27
Current IP Filters in Scan Order	"Current IP Filters Attributes (KN3IFC)" on page 27
Dynamic IP Tunnels Statistics	"IPSec Status Attributes (KN3ISS)" on page 51
Dynamic IP Tunnels	"Dynamic IP Tunnels Attributes (KN3ITD)" on page 36
Dynamic IP Tunnels by Destination Address	"Dynamic IP Tunnels Attributes (KN3ITD)" on page 36
Dynamic IP Tunnel by Filter Rule Definition Name	"Dynamic IP Tunnels Attributes (KN3ITD)" on page 36
Dynamic IP Tunnel by Tunnel ID	"Dynamic IP Tunnels Attributes (KN3ITD)" on page 36
Dynamic IP Tunnels with Byte Rate < 2048	"Dynamic IP Tunnels Attributes (KN3ITD)" on page 36
Manual IP Tunnels	"Manual IP Tunnels attributes (KN3ITM)" on page 57
Manual IP Tunnels by Tunnel ID	"Manual IP Tunnels attributes (KN3ITM)" on page 57
IKE Tunnels Statistics	"IPSec Status Attributes (KN3ISS)" on page 51
IKE Tunnels	"Internet Key Exchange (IKE) Tunnels Attributes (KN3ITI)" on page 45
IKE Tunnels with Byte Rate < 2048	"Internet Key Exchange (IKE) Tunnels Attributes (KN3ITI)" on page 45
IKE Tunnels by Security Endpoint	"Internet Key Exchange (IKE) Tunnels Attributes (KN3ITI)" on page 45
IKE Tunnels by Tunnel ID	"Internet Key Exchange (IKE) Tunnels Attributes (KN3ITI)" on page 45
IKE Tunnels with Byte Rate < 1024	"Internet Key Exchange (IKE) Tunnels Attributes (KN3ITI)" on page 45

- Additional and changed attributes. Table 3 includes a list of existing workspaces that contain new or changed attributes.

Table 3. Enhancements to existing workspaces

Workspace name	New or changed displayed attributes
Connections, Applications Connections, and TCP Connections	Three additional attributes were added: • Local IP address (new in this fix pack) • Application Name and Port (new in this fix pack) • DVIPA (new in this fix pack)
Interfaces and Interfaces History	This attribute was changed. • Physical Address The existing attribute was deprecated.

Table 3. Enhancements to existing workspaces (continued)

Workspace name	New or changed displayed attributes
Gateways and Devices (TCP/IP Gateways summary table)	The following attributes were changed to accommodate IPv6 addresses: • First Hop • Network Address • Subnet Mask • Subnet Value The existing attributes are deprecated. New attributes with the same name but a longer length have been added to accommodate the longer IPv6 addresses. The Packet Size attribute is no longer displayed.

- Support for two new formula functions that measure a rate of change. These formula functions are CHANGE and PCTCHANGE and are available in the Situation Editor. For additional information on these formula functions, see the Situation Editor help.
- New predefined situations for IPSec. The list of new situations is as follows:
  - N3T_IPSec_Dyn_Act_Fail
  - N3T_IPSec_Dyn_Act_Fail_IKE_Tnl
  - N3T_IPSec_Dyn_Act_Fail_IKE_TnR
  - N3T_IPSec_IKE_Act_Fail
  - N3T_IPSec_Key_Msgs_Auth_Fail
  - N3T_IPSec_Key_Msgs_Invalid
  - N3T_IPSec_Key_Msgs_Replayed
  - N3T_IPSec_Key_Msgs_Rtrnsmttd
  - N3T_IPSec_Pkts_Denied_DENY
  - N3T_IPSec_Pkts_Denied_Mismatch
  - N3T_IPSec_QUICKMODE_Invalid
  - N3T_IPSec_QUICKMODE_Replayed
  - N3T_IPSec_QUICKMODE_Rtrnsmttd
- Additional dynamic linking from selected Tivoli OMEGAMON XE for Mainframe Networks workspaces to IBM Tivoli NetView® for z/OS workspaces.

Changes to the navigation tree

With IPSec enabled, new entries are added to the navigation tree, and the default workspace for the TCP/IP branch is changed, as shown in Figure 1 on page 4.

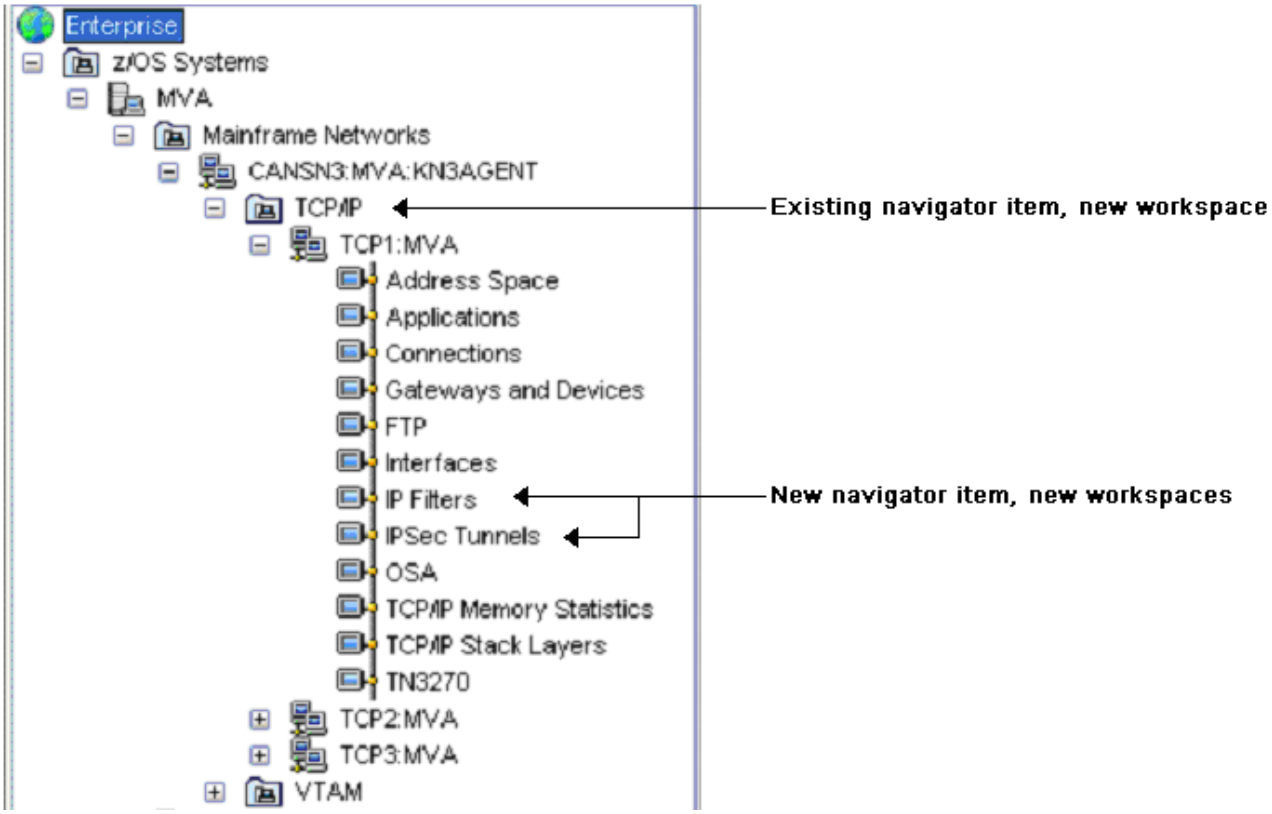


Figure 1. Updates to the navigation tree because of IPSec support

The TCP/IP branch of the Navigator provides access to the following IPSec workspaces for each TCP/IP stack being monitored:

- TCP/IP node adds a workspace named IPSec Status.
- IP Filters, which includes the following;
  - IP Filters Statistics (Default)
  - Current IP Filters
- IPSec Tunnels, which includes the following:
  - Dynamic IP Tunnels Statistics (Default)
  - Dynamic IP Tunnels
  - Dynamic IP Tunnels With Byte Rate < 2048
  - Manual IP Tunnels
  - IKE Tunnels Statistics
  - IKE Tunnels
  - IKE Tunnels With Byte Rate < 1024

Limited help available for globalized environments

This fix pack is not globalized. When you install this PTF, the new workspaces and attributes found in the fix pack are displayed in the user interface in English. The English navigator are merged with your nationalized navigation tree. You can expect these behaviors:

- New workspaces and their associated attributes: English-only
- Hover help for new workspaces: available but English-only

- Full-text (PF1) help for new workspaces and their associated attributes: not available. Use the information in this book.
- New attributes added to existing Connections, Applications Connections, and Gateways workspaces: attributes are displayed in English-only and no hover help is available.

Chapter 2. New planning information

This section provides the following updated planning information:

- Worksheets to identify configuration information
- Information to help you determine what kinds of data to collect
- Worksheets for determining space allocations in the persistent data store

Updated planning worksheets

This section provides updates to the planning worksheets found in Chapter 5 of the version 4.1.0 *IBM Tivoli OMEGAMON XE for Mainframe Networks: Planning Guide*.

Use this table to identify the configuration settings you will provide for each RTE.

RTE Name		
VIO Name		
Collection Interval	**TCP/IP**	
	SNA	
TCP/IP Data File		
SNMP Configuration File		

Provide the TCP/IP procedure name and specify the types of data that will be collected for each TCP/IP address space.

TCP/IP Proc Name	**TCP/IP Connections**	**IPSec**	**Routing Table**		**TN3270**		**FTP**	
			Collect? Y/N	Frequency	Collect? Y/N	Display Interval	Collect? Y/N	Display Interval

In the Configuration Tool, you will be asked for a global setting for each of the above types of data, as well as for CSM and EE/HPR data. Specify the global setting for each of the following.

	TCP/IP Connections	**IPSec**	**Routing Table**		**TN3270**		**FTP**		**CSM**	**EE/HPR**	
			Collect? Y/N	Fre-quency	Collect? Y/N	Display Interval	Collect? Y/N	Display Interval		Collect? Y/N	allhpr?
Global Setting											

Updates to "Determining which types of real-time data to collect" in the planning guide

The *IBM Tivoli OMEGAMON XE for Mainframe Networks: Planning Guide* includes the following section in "Chapter 6: Performance and Storage Consideration." The information in *italics* in this section has been added either to accommodate the addition of IPSec or to correct known problems. The section follows.

By default, the IBM Tivoli OMEGAMON XE for Mainframe Networks monitoring agent is configured to monitor all resources (TCP/IP address spaces, TN3270 server sessions, High Performance Routing connections, Enterprise Extender connections, FTP sessions and transfers, OSA adapters, TCP/IP connections, interfaces, gateways, Communication Storage Manager, VTAM® buffer pools, and VTAM environment). The monitoring agent always collects a required minimum amount of real-time data. You may choose to disable one or more of the following optional types of data:

- TCP/IP Connection and Application Performance statistics collection
- Routing Table statistics collection
- TN3270 server statistics collection
- FTP data collection
- Enterprise Extender and High Performance Routing statistics collection
- Communications Storage Manager (CSM) buffer reporting
- Buffer Pool and VTAM Environment data collection

You may choose to enable the following optional types of data (by default, data collection for these types of data is disabled):

- *IPSec security collection*

The following tables show the storage costs for monitoring the required and optional types of resources. These tables are provided to inform you of the relative size of attribute tables and the frequency in which data is collected. You might use this information to determine what to monitor: which types of resources, which systems and at what collection interval.

The data shown in Table 4 on page 10 is collected once every collection interval and stored in memory (in a dataspace). The memory will be reused each collection interval. When a user navigates to a workspace, a query will result in the monitoring agent retrieving the appropriate data from a dataspace. Use this table to calculate the memory usage by multiplying the row size by the number of resources. Total the memory usage column to obtain the total memory used to hold data collected in an interval for a TCP/IP address space. Perform these calculations for each TCP/IP address space you are monitoring.

Table 4. Data collected once every collection interval

LPAR Name				
TCP/IP Address Space				
Name Type of Data	**Real-Time Data Attribute Table**	**Row Size in Bytes**	**Frequency Per Interval**	**Memory Usage**
TCP/IP and VTAM (required collection)	TCPIP Address Space	*560*	1 row per TCPIP address space	
	TCPIP Devices	422	1 row per Device	
	Interfaces	468	1 row per interface	
	OSA Express Channels	412	1 row per OSA channel	
	OSA Express LPARs	104	16 rows per OSA Channel per LPAR per local channel subsystem	
	OSA Express Ports	752	1 row per OSA channel per port	
	TCPIP Memory Statistics	392	1 row per TCP/IP address space	
	TCPIP Stack Layer	552	1 row per TCP/IP address space	
TCP/IP Connection and Application Performance statistics collection	TCPIP Applications	568	1 row per TCP/IP application	
	TCPIP Connections	*600*	1 row per TCPIP connection	
	TCPIP Details	*396*	1 row per TCP connection	
	TCP Listener	204	1 row per TCP listener	
	UDP Connections	304	1 row per UDP endpoint	
Routing Table Statistics Collection	TCPIP Gateways	*584*	1 row per TCP/IP gateway	
IPSec Security Collection	*IPSec Status*	*376*	*1 row per TCP/IP address space*	
	Current IP Filters	*812*	*1 row per IP filter*	
	Dynamic IP Tunnels	*376*	*1 row per dynamic IP tunnel*	
	IKE Tunnels	*660*	*1 row per IKE tunnel*	
	Manual IP Tunnels	*364*	*1 row per manual IP tunnel*	

The data shown in Table 5 is collected once every collection interval and stored in memory. This data is collected for each LPAR you monitor. The memory will be reused each collection interval. Use this table to calculate the memory usage by multiplying the row size by the number of resources. Total the memory usage column to obtain the total memory used to hold data collected in an interval for these resources.

Table 5. Data collected for each monitored LPAR

LPAR Name				
Type of Data	**Real-Time Data Attribute Table**	**Row Size in Bytes**	**Frequency Per Interval**	**Memory Usage**
TCP/IP and VTAM (required collection)	VTAM Summary Statistics	72	1 row	
Enterprise Extender (EE) and High Performance Routing (HPR) statistics collection	EE Connections	216	1 row per EE connection	
	EE Connections Details	212	5 rows per EE connection	
	HPR RTP Connections	536	1 row per HPR RTP connection	
Communications Storage Manager (CSM) buffer reporting	CSM Storage	112	1 row	

Table 5. Data collected for each monitored LPAR (continued)

LPAR Name				
Type of Data	**Real-Time Data Attribute Table**	**Row Size in Bytes**	**Frequency Per Interval**	**Memory Usage**
Buffer Pool and VTAM Environment data collection	VTAM Address Space	244	1 row	
	VTAM I/O	72	*1 row for each of 6 resources*	
	VTAM Buffer Pools	*154*	*1 row for each of 14 resources*	
	VTAM Buffer Pool Extents	96	1 row per buffer pool extent	
	VTAM Buffer Usage by Address Space	72	*1 row per address space using IO00 or CRPL buffers*	
	VTAM Buffer Usage by Application	*74*	1 row per application per address space using IO00 buffers	
	VTAM Buffer Usage by Category	68	*1 row for each of 12 resources*	

The FTP data shown in Table 6 is collected when a new session or transfer is opened or when an existing session or transfer is closed. This data is collected when z/OS Communications Server notifies the monitoring agent when data is available and therefore does not adhere to a collection interval. As explained above, new records are appended to the previously collected data until the table in the dataspace is full, at which time the table wraps. Therefore, over time 256 MB per TCP/IP address space will be used to hold FTP data.

This data is collected for each TCP/IP stack where FTP is running.

Table 6. FTP data collected

LPAR Name				
TCP/IP Address Space Name				
Type of Data	**Real-Time Data Attribute Table**	**Row Size in Bytes**	**Frequency**	**Maximum Rows Stored**
FTP Data Collection	FTP Sessions	348	2 rows per FTP session	25,000
	TCPIP FTP	2420	2 rows per FTP transfer	100,000

The TN3270 session workspaces display information about open, closed and active TN3270 sessions for a TCP/IP address space. Data for open and closed sessions is provided when z/OS Communications Server notifies the monitoring agent that data is available and therefore is not driven by a collection interval. On an LPAR running z/OS 1.8 or higher, data for active sessions is collected once per collection interval.

Memory used to store data for one session will be reused for the same session each collection interval and for the data collected when the session is closed. Approximately 24 hours after a session is closed, the memory used to hold that session's data will be made available for a new session.

Use Table 7 on page 12 to calculate the memory usage by multiplying the row size by the number of resources. Total the memory usage column to obtain the total memory used to hold TN3270 data collected for a TCP/IP address space. Perform these calculations for each TCP/IP address space you are monitoring.

Note: The TN3270 Response Time Buckets table is not collected or stored as a separate table. Instead, it is a different view into the TN3270 Server Sess Avail table. When a query is issued to retrieve

TN3270 Response Time Buckets data, the appropriate TN3270 Response Time Buckets rows (one row for each of the five response time buckets) are created from the corresponding row in the TN3270 Server Sess Avail table.

Table 7. TN3270 data collected

LPAR Name				
TCP/IP Address Space Name				
Type of Data	**Real-Time Data Attribute Table**	**Row Size in Bytes**	**Frequency**	**Maximum Rows Stored**
TN3270 Server Statistics Collection	TN3270 Server Sess Avail	400	1 row per TN3270 server session that is active or was closed in the last 24 hours	
	TN3270 Response Time Buckets	204	0 rows	0

Use the Configuration Tool or the z/OS `MODIFY` command to enable or disable data collection for specific types of data. Refer to the KN3FCCMD commands appendix in the *IBM Tivoli OMEGAMON XE for Mainframe Networks: Configuration Guide* book.

Note: OMEGAMON II for Mainframe Networks is capable of collecting TCP/IP performance data. However, this option is disabled by default. IBM Tivoli OMEGAMON XE for Mainframe Networks provides more extensive coverage of TCP/IP and its resources and provides a more efficient monitoring solution. Be aware that enabling both OMEGAMON II for Mainframe Networks and IBM Tivoli OMEGAMON XE for Mainframe Networks to monitor TCP/IP generates unnecessary processing overhead. It is highly recommended to use IBM Tivoli OMEGAMON XE for Mainframe Networks to monitor TCP/IP resources in your enterprise.

Updated historical data tables in Appendix E of the configuration guide

Changes made in this fix pack require new information for the IPSec Status attribute table and updated information for three existing TCP/IP attribute tables.

Updates to the "Historical data tables" section

The *IBM Tivoli OMEGAMON XE for Mainframe Networks: Configuration Guide* includes the following section in "Appendix E: Disk space requirements for historical data tables." The information in *italics* in this section has been added either to accommodate the addition of IPSec or to correct known problems. In the original document, this information is included in Table 40. The section follows.

Table 8 lists the IBM Tivoli OMEGAMON XE for Mainframe Networks attribute tables available for historical collection. This table displays the storage used when monitoring one resource for 24 hours.

Table 8. Historical data tables

Attribute Table	**Filename**	**Default**	**Estimated Storage Required for One Data Set (in KB)**	**Estimated Storage Required for One Data Set (3390 Cylinders; No. of Cylinders = KB/717)**
TCPIP Address Space	KN3TAS	Yes	56	0.0781
TCPIP Devices	KN3TDV	Yes	43	0.0600
Interfaces	KN3TIF	Yes	47	0.0654
IPSec Status	KN3ISS	Yes	*38*	*0.0530*

Table 8. Historical data tables (continued)

Attribute Table	Filename	Default	Estimated Storage Required for One Data Set (in KB)	Estimated Storage Required for One Data Set (3390 Cylinders; No. of Cylinders = KB/717)
OSA Express Channels	KN3TCH	Yes	42	0.0586
OSA Express LPARs	KN3TLP	Yes	198	0.2762
OSA Express Ports	KN3TPO	Yes	74	0.1032
TCPIP Memory Statistics	KN3TPV	Yes	40	0.0558
TCPIP Stack Layer	KN3TSL	Yes	55	0.0767
TCPIP Applications	KN3TAP	Yes	56	0.0781
TCPIP Connections	KN3TCN	Yes	*59*	*0.0823*
TCPIP Details	KN3TCP	Yes	*40*	*0.0558*
TCP Listener	KN3TCL	Yes	22	0.0307
UDP Connections	KN3UDP	Yes	32	0.0446
TCPIP Gateways	KN3TGA	Yes	*55*	*0.0767*
IPSec Status	*KN3ISS*	*No*	*38*	*0.0530*
VTAM Summary Statistics	KN3SNA	Yes	10	0.0139
EE Connections	KN3EEC	Yes	23	0.0321
EE Connections Details	KN3EED	Yes	113	0.1576
HPR RTP Connections	KN3HPR	Yes	53	0.0739
CSM Storage	KN3CSM	Yes	14	0.0195
VTAM Address Space	KN3VAS	Yes	12	0.0167
VTAM I/O	KN3VIO	Yes	*57*	*0.0795*
VTAM Buffer Pools	KN3BPD	Yes	*276*	*0.3849*
VTAM Buffer Pool Extents	KN3BPE	Yes	*12*	*0.0117*
VTAM Buffer Usage by Address Space	KN3BPS	Yes	*10*	*0.0098*
VTAM Buffer Pool by Application	KN3BPA	Yes	*10*	*0.0098*
VTAM Buffer Pool Usage by Category	KN3BPG	Yes	*108*	*0.1055*
FTP Sessions	KN3FSE	Yes	0.74	0.0010
TCPIP FTP (FTP transfers)	KN3FTP	Yes	4.78	0.0067
TN3270 Server Sess Avail	KN3TNA	Yes	14	0.0195
Total			*1575 KB*	*2.2 cylinders*

Updates to historical data storage tables for new and changed attribute tables

This section provides the information you will need to determine space allocations for storing historical data in the persistent data store for the new and changed attribute tables for each monitoring agent. Therefore, the disk space requirements in the tables in this section are for short-term history, which is stored on z/OS in the OMEGAMON XE persistent data store. For more information about these tables and methods for determining store requirements, refer to "Appendix E: Disk space requirements for historical data tables" in the *IBM Tivoli OMEGAMON XE for Mainframe Networks: Configuration Guide*.

TCP/IP historical data storage

Attribute group record sizes:

This data is collected once every collection interval for each TCP/IP stack. If you have an LPAR with multiple TCP/IP stacks, combine the storage required for each stack you will monitor.

Table 9. Data collected once every collection interval

Type of Data	Real-Time Data Attribute Group	Row Size in Bytes	Frequency Per Interval	Subtotal Storage Required (KB)
TCP/IP and VTAM (required collection)	IPSec Status (new)	404	1 row per TCP/IP address space	38
TCP/IP Connection and Application Performance statistics collection	Interfaces (updated)	500	1 row per interface	47
	TCPIP Connections (updated)	628	1 row per TCPIP connection	59
	TCPIP Details (updated)	424	1 row per TCP connection	40
Routing Table Statistics Collection	TCPIP Gateways (updated)	584	1 row per TCP/IP gateway	55

IPSec Status(KN3ISS) worksheet (new):

Table 10. IPSec Status (KN3ISS) worksheet

Interval	Record Size	Formula	TCP/IP Address Space Resources	TCP/IP Stack	Expected Storage Required for 24 Hours
15 minutes	404	4 x 24 x 404x 1 x 1 / 1024	1	1	38 KB

Table 24: Interfaces (KN3TIF) worksheet (updated):

Table 11. Interfaces (KN3TIF) worksheet

Interval	Record Size	Formula	TCP/IP Connections	TCP/IP Stack	Expected Storage Required for 24 Hours
15 minutes	484	4 x 24 x 500 x 1 x 1 x 1 / 1024	1	1	47 KB

Table 31: TCPIP Connections (KN3TCN) worksheet (updated):

Table 12. TCPIP Connections (KN3TCN) worksheet

Interval	Record Size	Formula	TCP/IP Connections	TCP/IP Stack	Expected Storage Required for 24 Hours
15 minutes	628	4 x 24 x 628 x 1 x 1 x 1 / 1024	1	1	59 KB

Table 12. TCPIP Connections (KN3TCN) worksheet (continued)

Interval	Record Size	Formula	TCP/IP Connections	TCP/IP Stack	Expected Storage Required for 24 Hours

Table 32: TCPIP Details (KN3TCP) worksheet (updated):

Table 13. TCPIP Details (KN3TCP) worksheet

Interval	Record Size	Formula	TCP Connections	TCP/IP Stack	Expected Storage Required for 24 Hours
15 minutes	424	4 x 24 x 424 x 1 x 1 x 1 / 1024	1	1	40 KB

Table 35: TCPIP Gateways (KN3TGA) worksheet (updated):

Table 14. TCPIP Gateways (KN3TGA) worksheet

Interval	Record Size	Formula	Gateways	TCP/IP Stack	Expected Storage Required for 24 Hours
15 minutes	584	4 x 24 x 584 x 1 x 1 x 1 / 1024	1	1	55 KB

VTAM historical data storage

Attribute group record sizes: The following data is collected once every collection interval. This data is collected for each LPAR you will monitor.

Table 15. Data collected once every collection interval

Type of Data	Real-Time Data Attribute Group	Row Size in Bytes	Frequency Per Interval	Subtotal Storage Required
TCP/IP and VTAM (minimum collection)	VTAM Summary Statistics	100	1 row	10
Enterprise Extender (EE) and High Performance Routing (HPR) statistics collection	EE Connections	244	1 row per EE connection	23
	EE Connections Details	240	5 rows per EE connection	113
	HPR RTP Connections	564	1 row per HPR RTP connection	53
Communications Storage Manager (CSM) buffer reporting	CSM Storage	140	1 row	13

Table 15. Data collected once every collection interval (continued)

Type of Data	Real-Time Data Attribute Group	Row Size in Bytes	Frequency Per Interval	Subtotal Storage Required
Buffer Pool and VTAM environment collection	VTAM Address Space	272	1 row	26
	VTAM I/O	100	1 row for each of 6 resources	57
	VTAM Buffer Pools	210	1 row for each of 14 resources	276
	VTAM Buffer Pool Extents	124	1 row per buffer pool extent	12
	VTAM Buffer Pool Usage by Address Space	100	1 row per address space using IO00 or CRPL buffers	10
	VTAM Buffer Pool Usage by Application	102	1 row per application using IO00 buffers	10
	VTAM Buffer Pool Usage by Category	96	1 row for each of 12 resources	108

Table 43: VTAM I/O (KN3VIO) worksheet (updated):

Table 16. VTAM I/O (KN3VIO) worksheet

Interval	Record Size	Formula	Number of Resources	Expected Storage Required for 24 Hours
15 minutes	100	4 x 24 x 100 x 6 x 1 / 1024	6	57KB

Table 44: VTAM Buffer Pools (KN3BPD) worksheet (updated):

Table 17. VTAM Buffer Pools (KN3BPD) worksheet

Interval	Record Size	Formula	Number of Resources	Expected Storage Required for 24 Hours
15 minutes	210	4 x 24 x 210x 14 x 1 / 1024	14	276 KB

Table 45: VTAM Buffer Pool Extents (KN3BPE) worksheet (updated):

Table 18. VTAM Buffer Pool Extents (KN3BPE) worksheet

Interval	Record Size	Formula	Number of Resources	Expected Storage Required for 24 Hours
15 minutes	124	4 x 24 x 124 x 1 x 1 / 1024	1	12 KB

Table 46: VTAM Buffer Pool Usage by Address Space (KN3BPS) worksheet (updated):

Table 19. VTAM Buffer Pool Usage by Address Space (KN3BPS) worksheet

Interval	Record Size	Formula	Number of Resources	Expected Storage Required for 24 Hours
15 minutes	100	4 x 24 x 100 x 1 x 1 / 1024	1	10 KB

Table 47: VTAM Buffer Pool Usage by Application (KN3BPA) worksheet (updated):

Table 20. VTAM Buffer Pool Usage by Application (KN3BPA) worksheet

Interval	Record Size	Formula	Number of Resources	Expected Storage Required for 24 Hours
15 minutes	102	4 x 24 x 102 x 1 x 1 / 1024	1	10 KB

Table 48: VTAM Buffer Pool Usage by Category (KN3BPG) worksheet (updated):

Table 21. VTAM Buffer Pool Usage by Category (KN3BPG) worksheet

Interval	Record Size	Formula	Number of Resources	Expected Storage Required for 24 Hours
15 minutes	96	4 x 24 x 96 x 12 x 1 / 1024	12	108 KB

Chapter 3. New configuration required for IPSec

When you are ready to monitor IP filters and IPSec tunnels, you will need to prepare your z/OS system and modify your RTE configuration. The following sections describe how to prepare your z/OS systems and how to run the Configuration Tool to configure each RTE to collect data for IP filters and IPSec tunnels.

New steps to prepare your z/OS environment

Chapter 2 of the *IBM Tivoli OMEGAMON XE for Mainframe Networks: Configuration Guide* describes how to prepare your z/OS environment. In addition to the steps provided in Chapter 2, prepare your z/OS environment by performing the following on each z/OS system where you will monitor IP filters and IPSec tunnels:

- "Enabling IPSec monitoring"
- "Verifying IKE daemon and Policy Agent daemon are started"

Enabling IPSec monitoring

The NMI for IP filters and IPSec tunnels is available for monitoring agents without updating the TCP/IP profile. The IKE daemon and Policy Agent daemon must be started for IP filters and IPSec tunnels to be monitored.

Verifying IKE daemon and Policy Agent daemon are started

Confirm that the IKE daemon and Policy Agent daemon have started:

```
D A,L
```

If the daemons have not started, start them. Refer to the *z/OS Communications Server IP Configuration Guide* (SC31-8775) for more information about the IKE daemon and Policy Agent daemon.

Changes to Configuration Tool panels

Chapter 8 of the *IBM Tivoli OMEGAMON XE for Mainframe Networks: Configuration Guide* describes how to configure a monitoring agent. To direct the monitoring agent to collect IP filters and IPSec tunnels data, you will need to change the value for the **IPSec Security Collection** question that has been added to the configuration panels and then run both the N3#5xxxx job to create the TCP/IP monitored systems member (kn3tcpmo) and the N3#3xxxx job to create the runtime members for the OMEGAMON XE for Mainframe Networks agent. Details about performing these steps follow.

1. Navigate in the Configuration Tool panels to the panel titled SPECIFY COMPONENT CONFIGURATION (PAGE 2), found in Chapter 8 of the Configuration Guide under **Step 2 Specify configuration parameters** in Figure 32 on page 64 of the existing configuration guide. The panel is replaced by Figure 2 on page 20.

```
------------------- SPECIFY COMPONENT CONFIGURATION (Page 2)---------------
Command ===>

 Specify the following global information:

    TCP/IP Connection and Application Performance Statistics Collection:
          ==> Y   (Y,N)

    IP Filters and IPSec Tunnels Statistics Collection: ==> N   (Y,N)

    Routing Table Statistics Collection: ==> Y   (Y,N)
    Routing Table Collection Frequency:  ==> 10  (1-99)      (Optional)

    TN3270 Server Statistics Collection: ==> Y   (Y,N)
    TN3270 Data Display Interval:        ==> 2   (1-24 hours)(Optional)

    FTP Data Collection:                 ==> Y   (Y,N)
    FTP Data Display Interval:           ==> 2   (1-24 hours)(Optional)

    SNMP Configuration file (USER.SNMP(SNMPCONF)):
          ==> USER.SNMP(SNMPCONF)

 Enter=Next  F1=Help  F3=Back
```

Figure 2. Specify component configuration (page 2) panel

The new IPSec Security Collection configuration parameter is defined as shown below.

IP Filters and IPSec Tunnels Statistics Collection
Determines whether or not to collect IPSec security data. **Y** indicates IPSec Security data will be collected. **N** indicates IPSec Security data will not be collected (the default).

Specify **Y** to collect IPSec Security data. Verify that all displayed values are correct and press **Enter** to continue.

2. Continue navigating in the Configuration Tool to the panel titled **SPECIFY TCP/IP MONITORED SYSTEMS INFORMATION**, which is Figure 35 on page 68 of the existing configuration guide.
3. On the SPECIFY TCP/IP MONITORED SYSTEMS INFORMATION panel, type **A** for a row and press **Enter** to navigate to the panel titled **ADD TCP/IP MONITORED SYSTEMS INFO**. This panel can be found in Figure 38 on page 71 of the existing configuration guide. The panel is replaced by Figure 3.

```
-------------- ADD TCP/IP MONITORED SYSTEMS INFO / RTE: HUBN3IRA ------------
COMMAND ===>

 Complete the items on this panel:

   Sys                  ==>

   TCP/IP address space ==>

   TCP/IP profile dataset name:  ==>
     Member name        ==>                                      (Optional)

   TCP/IP Connection Collection Override            ==>     (Y,N)  (Optional)

   IP Filters and IPSec Tunnels Collection Override ==>     (Y,N)  (Optional)

   Routing Table Collection Override                ==>     (Y,N)  (Optional)
   Routing Table Collection Frequency               ==>     (1-99) (Optional)



 Enter=Next  F1=Help  F3=Back
```

Figure 3. Add TCP/IP monitored systems information panel

The new IPSec Security Collection configuration parameter is defined as shown below.

IP Filters and IPSec Tunnels Collection Override

Determines whether or not to collect IP Security and tunnel data for this address space. **Y** indicates IP Security data will be collected. **N** indicates IP Security data will not be collected. Leaving the field blank indicates that IP Security Data collection will use the default. See Notes® below for additional restrictions.

Specify **Y** to collect IPSec Security data. Verify that all displayed values are correct and press **Enter** to continue.

Note: This new configuration parameter has also been added to the following similar configuration panels:

- View TCP/IP Monitoring Systems Info
- Update TCP/IP Monitoring Systems Info

4. When you have finished adding configuration information for the monitored TCP/IP address spaces, you will be returned to the SPECIFY TCP/IP MONITORED SYSTEMS INFORMATION panel. Press **F3** to view the N3#5xxxx JCL job that is generated to created the TCP/IP monitored systems member, *&rhilev.&midlev.*RKANPARU(KN3TCPMO). Review and submit the JCL. You might want to change the jobname to match the member name so that you can easily identify this job (N3#5xxxx) later on. Verify that the job completes successfully.
5. Press **F3** to exit the job. Press **F3** a second time to exit the SPECIFY TCP/IP MONITORED SYSTEM INFORMATION panel.
6. Type **4** and press **Enter** to display the **Create Runtime Members** panel for job N3#3xxxx. Review and submit the JCL. Verify that the job completes successfully.
7. Perform the steps described in section “New steps to "Loading the runtime libraries and completing the configuration".”

New steps to "Loading the runtime libraries and completing the configuration"

Chapter 9 of the *IBM Tivoli OMEGAMON XE for Mainframe Networks: Configuration Guide* describes the steps required to load the runtime libraries and complete the configuration. Perform the following for each RTE in your environment:

- Load the runtime libraries for each RTE (follow the instructions in Chapter 9, section “Loading the runtime libraries”). KN3ATR, KN3CAT, KN3PDICT, and load modules were updated. The LOAD job will copy these members to the appropriate libraries. If your RTE shares the SMP/E target libraries, you can run the following jobs instead of the LOAD job:
  - To copy KN3ATR and KN3CAT, follow the instructions in “Step 1: Register with local TEMS” in Chapter 9.
  - To copy KN3PDICT, follow the instructions for option “3 Create runtime members” under “Step 5: Configure Persistent datastore (in Agent)” in Chapter 9.
- Edit and run the KN3LINK job, if appropriate for your environment. Read the information in “Operating system considerations,” locating in Chapter 9 in section “Completing the Configuration.”
- Define monitoring agent access to the NMI for each z/OS system where you will monitor IP filters and IPSec tunnels.

Defining monitoring agent access to the NMI

Note

This is an update to an existing section that is currently part of Chapter 9 in the configuration guide. Updates are in *italics*.

If your site has the security groups defined for z/OS Communications Server Network Management Interface (NMI), then the OMEGAMON XE for Mainframe Networks monitoring agent must be authorized to access this interface. *One or more of the following security groups may be defined in the SERVAUTH class:*

- *EZB.NETMGMT.systemname.tcpipprocname.**
- *EZB.NETMGMT.systemname.tcpipprocname.SYSTCPCN*
- *EZB.NETMGMT.systemname.tcpipprocname.SYSTCPSM*
- *EZB.NETMGMT.systemname.tcpipprocname.IPSEC.DISPLAY*
- *IST.NETMGMT.systemname.SNAMGMT*

If the resources are not defined, then the user ID that the monitoring agent procedure runs under needs to be a superuser, which is a user that has been permitted to the BPX.SUPERUSER resource in the FACILITY class.

The Configuration Tool placed a sample JCL job in the *&rhilev.&midlev*.RKANSAMU library called KN3UAUTH that will create a new KN3USER user and grant access to *all of the z/OS Communications Server Network Manager Interface APIs by granting the monitoring agent access to the IST.NETMGMT.systemname.SNAMGMT and EZB.NETMGMT.systemname.tcpipprocname.* resources.*

This job is run outside of the Configuration Tool. Make the following changes to this job before you run it:

- Change **omvsgrp** to a valid OMVS group in RACF® and **password** to a valid password for your enterprise.
- Change **systemname** to the system name where the monitoring agent will run.
- Change **agentproc** to the started procedure name for the IBM Tivoli OMEGAMON XE for Mainframe Networks monitoring agent. The default is **CANSN3**.
- Change **tcpipprocname** to your TCP/IP startup procedure name for the TCP/IP stack that you want to monitor. Repeat this pair of lines (RDEFINE and PERMIT) for every TCP/IP address space you want to monitor.

  Notes:

  1. The RDEFINE and PERMIT statements for IST.NETMGMT* do not need to be repeated if you have more than one TCP/IP address space you are monitoring.
  2. If you start your TCP/IP address space using the `S procedure` syntax, use procedure for *tcpipprocname*. If you start your TCP/IP address space using the `S procedure.identifier` syntax, use identifier for *tcpipprocname*.

For information about values in this job that you need to edit, refer to comments in the JCL job.

Your security administrator must run this job from a user ID that has RACF SPECIAL and UID(0) authority or code USERID and PASSWORD on the jobcard for an ID that has RACF SPECIAL and UID(0) authority. KN3USER is the default user ID. If you choose to use a different ID, change all occurrences of KN3USER in the job. Make these changes and review this job before you provide it to your security department. It should run with a zero return code.

The KN3UAUTH job will be created every time you go through the configuration process. Copy this job into another data set and customize it for your environment and leave *&rhilev.&midlev.*RKANSAMU as a backup copy. This job should not be run more than once for this started task.

Potential changes to the batch parameter deck

If you manually edit the batch parameter deck and choose to override any of the global parameters for a TCP/IP address space, you must also ensure that the KN3_TCPX_OGBL parameter is set to **Y** for each address space that you modify. This designation is found in the batch job near the section that includes the following parameters:

```
KN3_TCPX_ROW
KN3_TCPX_SYS_NAME         0023
KN3_TCPX_ADDR_SPACE       TCPCS5
KN3_TCPX_PROF_DATASET     CS390.BASE.TCPPARMS
KN3_TCPX_OGBL             Y
KN3_TCPX_OTCPC
KN3_TCPX_OIPSEC           Y
KN3_TCPX_ORTC
KN3_TCPX_ORTF
KN3_TCPX_OFTPC
KN3_TCPX_FTP_INT_SPEC
KN3_TCPX_OTNC
KN3_TCPX_TNC_INT_SPEC
KN3_TCPX_PROF_MEMBER      TCPCS5S
```

Chapter 4. New filters, attribute tables, and linking

The filters provided with the IPSec workspaces in Tivoli OMEGAMON XE for Mainframe Networks are shown in Table 22.

Table 22. Filters provided with Tivoli OMEGAMON XE for Mainframe Networks

Attribute table	Table prefix	Workspace	Source filters	Other filters
IPSec Status	KN3ISS	IPSec Status	None	None
	KN3ISS	IP Filter Statistics	None	None
	KN3ISS	Dynamic IP Tunnel Statistics	None	None
	KN3ISS	IKE Tunnel Statistics	None	None
Current IP Filters	KN3IFC	Current IP Filters	None	PAGE = “0000”
Dynamic IP Tunnels	KN3ITD	Dynamic IP Tunnels	None	Byte Rate >= 2048
	KN3ITD	Dynamic IP Tunnels with Byte Rate < 2048	None	Byte Rate < 2048
Manual IP Tunnels	KN3ITM	Manual IP Tunnels	None	None
IKE Tunnels	KN3ITI	IKE Tunnels	None	Byte Rate >= 1024
	KN3ITI	IKE Tunnels with Byte Rate < 1024	None	Byte Rate < 1024

Mapping IPSec workspaces to attribute tables

Tivoli OMEGAMON XE for Mainframe Networks provides workspaces that are accessed from the Navigator. Each of these IPSec workspaces display tables that can be altered or replaced, to meet your needs. Table 23 shows which attribute tables display in which workspaces as well as the table prefix. These are the source tables for the Tivoli Data Warehouse.

Table 23. Mapping Navigator workspaces to attribute tables

Workspace	Attribute table	Table prefix
IPSec Status	IPSec Status	KN3ISS
IP Filter Statistics	IPSec Status	KN3ISS
Dynamic IP Tunnel Statistics	IPSec Status	KN3ISS
Current IP Filters	Current IP Filters	KN3IFC
Dynamic IP Tunnels	Dynamic IP Tunnels	KN3ITD
IKE Tunnels	IKE Tunnels	KN3ITI
IKE Tunnels Statistics	IPSec Status	KN3ISS
Manual IP Tunnels	Manual IP Tunnels	KN3ITM

Tivoli OMEGAMON XE for Mainframe Networks also provides workspaces that are accessed by linking from other workspaces. Each of these IPSec workspaces also displays tables that can be altered or replaced, to meet your needs. Table 24 shows which attribute tables display in which linked workspaces as well as the table prefix for each.

Table 24. Mapping linked workspaces to attribute tables

Workspace	Attribute table	Table prefix
Current IP Filters by Destination Address	Current IP Filters	KN3IFC

Table 24. Mapping linked workspaces to attribute tables (continued)

Workspace	Attribute table	Table prefix
Current IP Filters by Rule Name	Current IP Filters	KN3IFC
Current IP Filters in Scan Order	Current IP Filters	KN3IFC
Dynamic IP Tunnels by Destination Address	Dynamic IP Tunnels	KN3ITD
Dynamic IP Tunnels by Filter Name	Dynamic IP Tunnels	KN3ITD
Dynamic IP Tunnels by Tunnel ID	Dynamic IP Tunnels	KN3ITD
Dynamic IP Tunnels with Byte Rate < 2048	Dynamic IP Tunnels	KN3ITD
IKE Tunnels by Security Endpoint	IKE Tunnels	KN3ITI
IKE Tunnels by Tunnel ID	IKE Tunnels	KN3ITI
IKE Tunnels with Byte Rate < 1024	IKE Tunnels	KN3ITI
Manual IP Tunnels by Tunnel ID	Manual IP Tunnels	KN3ITM

Additional dynamic linking to cross-product workspaces

Release 4.1.0 first exploited dynamic workspace links, a feature that allows you to easily navigate between workspaces that are provided by multiple products. This feature aids problem determination and improves integration across the monitoring products, allowing you to quickly determine the root cause of a problem. Predefined cross-product links provided by the OMEGAMON XE products allow you to obtain additional information about systems, subsystems, resources, or network components that are being monitored by other monitoring agents. Refer to the *IBM Tivoli OMEGAMON XE for Mainframe Networks: User's Guide* for more information about dynamic workspace links. Refer to the workspace descriptions in Chapter 6, "New and updated workspaces," on page 63 for information about the predefined links provided with each new or updated workspace. Table 25 summarizes the links available when this product shipped:

Table 25. Links from IBM Tivoli OMEGAMON XE for Mainframe Networks to other agents and applications

IBM Tivoli OMEGAMON XE for Mainframe Networks workspace	Target application or monitoring agent	Name of workspace in target application or monitoring agent	Attributes used to locate target workspace	Attributes used to filter data in target workspace
Applications Connections **Note:** This link is available only if the new DVIPA attribute in this workspace has the value of **Yes**.	IBM Tivoli NetView for z/OS	IBM Tivoli NetView for z/OS DVIPA Definition and Status Workspace	• Sysplex name • SMFID	Local IP Address
Connections **Note:** This link is available only if the new DVIPA attribute in this workspace has the value of **Yes**.	IBM Tivoli NetView for z/OS	IBM Tivoli NetView for z/OS DVIPA Definition and Status Workspace	• Sysplex name • SMFID	Local IP Address
TCP Connections **Note:** This link is available only if the new DVIPA attribute in this workspace has the value of **Yes**.	IBM Tivoli NetView for z/OS	IBM Tivoli NetView for z/OS DVIPA Definition and Status Workspace	• Sysplex name • SMFID	Local IP Address
TCP/IP Summary Workspace	IBM Tivoli NetView for z/OS	IBM Tivoli NetView for z/OS DVIPA Definition and Status Workspace	• Sysplex name • SMFID	Host IP Address

Chapter 5. New and changed attribute groups

For this fix pack, five new attribute groups were added and three attribute groups were updated.

The following new attribute groups or tables were added to the OMEGAMON XE for Mainframe Networks product to support IPSec. These attributes are used in the table views in the various product-defined workspaces that support IPSec.

- "Current IP Filters Attributes (KN3IFC)"
- "Dynamic IP Tunnels Attributes (KN3ITD)" on page 36
- "Internet Key Exchange (IKE) Tunnels Attributes (KN3ITI)" on page 45
- "IPSec Status Attributes (KN3ISS)" on page 51
- "Manual IP Tunnels attributes (KN3ITM)" on page 57

These attributes groups were updated:

- "Interfaces Attributes (KN3TIF)" on page 61
- "Connections Attributes (KN3TCN)" on page 61
- "TCP/IP Details Attributes (KN3TCP)" on page 62
- "TCPIP Gateways Attributes (KN3TGA)" on page 62

For more information about the workspaces associated with these attribute groups, see Chapter 6, "New and updated workspaces," on page 63.

Current IP Filters Attributes (KN3IFC)

Use the Current IP Filters attributes to display IP filter information for the filters currently in use by the TCP/IP stack.

This data is available for monitoring agents running under z/OS version 1.8 or higher.

Action The action to be applied to the packet when filter's condition is met. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = PERMIT
- 2 = DENY
- 3 = IPSEC

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)

- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Create Time The time when the filter was created, based on how the filter was created.

- For a statically defined filter originating from the Policy Agent configuration, this field represents the time that the filter was first defined to the current instance of the Policy Agent. Filters of this type have the value of **1** meaning Policy for the Filter Set attribute.
- For a filter originating from the TCP/IP profile, this field represents the time that the profile filter configuration was last replaced. Filters of this type have the value of **0** meaning Default for the Filter Set attribute.
- For dynamically defined filters, this field is blank. Dynamically defined filters have a value of **DYNAMIC**, **NATTDYN**, or **NRF**.

This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Destination Address Destination IP address or addresses affected by the current filter. This address may be in IPv4 or IPv6 format. Filters apply to either IPv4 addresses or IPv6 addresses, but not both. If the filter applies to all destination IP addresses, the field will be displayed as blank; a value of “0” padded to the right with blanks will be stored in the table. If the filter is for a range of destination IP addresses, this is the lower address in the range. This value is represented as a 45-character string.

Note: For comparison, leading zeros are added for unspecified digits in IPv4 and IPv6 addresses when they are stored.

Destination Address Granularity Indicates the origin of the destination address used for on-demand activations of tunnels associated with a dynamic anchor filter. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>: This is not a dynamic anchor filter.
- 1 = FILTER: Destination address for the tunnel is from the filter definition.
- 2 = PACKET: Destination address for the tunnel is from the packet requiring the tunnel activation.

Destination Port Granularity Indicates the origin of the destination port used for on-demand activations of tunnels associated with a dynamic anchor filter. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>: This is not a dynamic anchor filter
- 1 = FILTER: The destination address for the tunnel is from the filter definition.
- 2 = PACKET: The destination address for the tunnel is from the packet requiring the tunnel activation.

A value of FILTER indicates the destination port comes from the filter definition. A value of PACKET indicates the destination port comes from the packet. This field is significant if the filter type indicates this is a dynamic anchor filter. If the filter is not a dynamic anchor filter, a value of zero (0) is stored and blanks are displayed in the field.

Direction Indicates the direction of the IP traffic. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = INBOUND
- 2 = OUTBOUND

Filter Rule Definition Name The name specified for an IP filter rule definition. This column is stored as a 48-character string.

Filter Set Identifies which filter set is currently in use by the TCP/IP stack. One of two filter sets may be in use at any time.

- The default filter set, which is made up of filters defined in the TCP/IP profile.
- The policy filter set, which is made up of filters defined in the Policy Agent configuration files.

This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Default
- 1 = Policy

Filter Use Indicator The value in this column is used to identify the filters that are matching the most packets. Values 1 to 4 are used to identify the 5 filters with the most matches, the most denies by DENY and the most denies by mismatch. Value 5 is used to identify filters 6 to 100 with the most matches. A query can return the 5 filters with the most matches by using a where clause like:

```
(Filter Use Indicator = 1) OR (Filter Use Indicator = 3)
```

A query can return the 100 filters with the most matches by adding another OR clause to the previous condition:

```
(Filter Use Indicator = 5)
```

This value is stored as a one character string and is displayed as a string. Valid values are:

- 1 = MostMatched: The filter is one of the 5 most-matched filters.
- 2 = MostDENY: The filter is one of the 5 filters with a DENY action that has the most matched packets. This also means that the filter has denied the most packets due to DENY.
- 3 = MostMatchedAndMostDeny: The filter is both one of the five most matched filters and one of the five filters that has denied the most packets by DENY.
- 4 = MostMismatched: The filter is one of the 5 filters that has the most matched packets.

- 5 = MostMatchedAndMosMismatched: The filter is both one of the five most matched filters and one of the five most mismatched filters.
- 6 = MostMatched6to100: The filter is one of the 6 to 100 filters that has the most matches.

This field is not displayed.

Group Name The name of the filter group that the filter rule is associated with. This field is stored as blanks if the filter rule is not associated with a filter group. The format is an alphanumeric string of up to 48 characters.

ICMP Code The Internet Control Message Protocol (ICMP) code that qualifies the ICMP Type Code attribute. This field is stored as blanks if the filter applies to all ICMP codes. This field is defined as an integer of up to 2 characters. 0 is a defined ICMP code. The value in this field is not meaningful unless a non-blank value appears in the ICMP Type Code field.

ICMP Type Code The Internet Control Message Protocol (ICMP) code that identifies the ICMP traffic to be filtered. This field is stored as blanks if the filter applies to all ICMP types. This field is defined as an integer of up to 2 characters. 0 is a defined ICMP Type Code.

IP Address Version The version of the IP addresses being used for the traffic descriptor and the security endpoints. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = IPv4: The traffic descriptor and the security endpoints are using IPv4 addresses.
- 1 = IPv6: The traffic descriptor and the security endpoints are using IPv6 addresses.

Last Page The value in this column saves the page number of the last page of filters. It is used in queries to determine whether or not more pages of filters are available to retrieve. This value is stored as a 4-character string, with 0000 representing the first page.

Local Start Action Name The name specified for an IpLocalStartAction statement that is referenced by this filter. The IpLocalStartAction statement specifies how to determine the local IP, remote IP, local port, remote port, and protocol specification for the local activation of a dynamic virtual private network (VPN). This field is stored as blanks if no local start action name is associated with this filter. This field is stored as a 48-character string.

Log Indicator Indicates which packets to log. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = NONE: Do not log any packets.
- 1 = PERMIT: Log packets permitted by the filter.
- 2 = DENY: Log packets denied by the filter.
- 3 = ALL: Log all packets that match this filter.

Lower Destination Address The lower address in a range of IP addresses being filtered. If the filter is for a range of destination IP addresses, this is the lower address in the range. Otherwise, this field is stored as blanks. The format is a string of up to 45 characters.

Note: For comparison, leading zeros are added for unspecified digits in IPv4 and IPv6 addresses when they are stored.

Lower Destination Port If the filter is for a range of destination IP port addresses, this is the low value for the range. This field is stored as blanks if the filter is not for a range of IP port addresses and applies to all ports. This value is represented as a 5-character string.

Lower Source Port If the filter is for a range of IP ports, this is the low value for the range. This field is stored as blanks if the filter is not for a range of IP port addresses and applies to all ports. This value is represented as a 5-character string.

NAPT Indicator Indicates whether a network address port translation (NAPT) has been detected in front of the IPSec peer. This field is significant for filters with a type of dynamic. If the filter is not dynamic, this field is stored as blanks. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

NAT Indicator Indicates whether network address translation (NAT) has been detected in front of the IPSEC peer. This field is significant for filters with a type of dynamic. If the filter is not dynamic, this field is stored as blanks. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

NAT Traversal Gateway Indicates that the peer is acting as an IPSec gateway and the tunnel uses UDP encapsulation. This field is significant for dynamic filters. If the filter is not dynamic, this field is stored as blanks. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

NATT Client ID If the peer is behind a NAT and a gateway and the peer supplied a client ID, indicates the NAT traversal gateway (NATT) client ID. This field contains an IPv4 dotted decimal address if the NATT Client ID Type is IPv4_ADDR. This field contains an IPv4 dotted decimal address if the NATT Client ID Type is IPv4_ADDR_RANGE. The address in the field is the lower address for the range. This field will have an MD5 hash of the client ID if the NATT Client ID Type is OTHER. If the NATT Client ID Type is 0, this field is stored as blanks. The format is a string of up to 32 characters.

NATT Client ID Type If the peer is behind a NAT and a gateway and the peer supplied a client ID, indicates what type of client ID was supplied. Otherwise, this field is stored as blanks. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = NONE
- 1 = IPv4_ADDR
- 2 = IPv4_ADDR_RANGE
- 3 = IPv4_ADDR_RANGE
- 4 = OTHER

NATT Peer UDP Port If this is a dynamic filter for UDP-encapsulated NAT Traversal (NATT) traffic, this is the UDP port for the IKE peer. Otherwise, this field is stored as blanks. This field is represented as a character string of up to 5 characters.

NRF Original Port If this is a NAT Traversal Resolution Filter (NRF), this field contains the original remote port for the TCP or UDP traffic. Otherwise this field is stored as blanks. This field is represented as a character string of up to 5 characters.

On Demand Indicator Indicates whether or not on-demand activations are allowed for the traffic described for this filter. On demand activations are activations of tunnels initiated automatically when traffic requiring the use of the tunnel is sent. This field is meaningful if the filter type is one of the following:

- Dynamic anchor filter
- Dynamic filter
- Network Address Translation (NAT) Traversal anchor filter
- NAT Traversal dynamic filter

This value is stored as an integer and displayed as a string. The field contains a zero (0) when the filter type is not one of these. Valid values are:

- 0 = <blank>
- 1 = NOT_PERMITTED
- 2 = PERMITTED

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters. This field is not displayed.

OSPF Type Identifies Open Shortest Path First (OSPF) protocol traffic to be filtered. This field is stored as blanks if the filter applies to all OSPF traffic. The format is an integer.

Packets Denied by Mismatch The number of packets denied due to a mismatch with this filter's action during the most recent collection interval. The format is an integer.

Packets Matched The total number of packets that matched this filter's condition and action during the most recent collection interval. The format is an integer.

Page The value in this column is used to group the filters into logical pages. Each page contains 500 filters. Links are implemented so that you can request all the filters on a particular page. This value is stored as a 4-character string, with 0000 representing the first page.

Percent Total Packets Denied by Mismatch The percentage of total packets denied due to an action mismatch by this filter compared to the total packets denied due to an action mismatch by all filters on the TCP/IP stack since the stack was started. The format is a number between 0 and 100 inclusive.

Percent Total Packets Matched The percentage of total packets matched by this filter compared to the total packets matched by all filters on the TCP/IP stack since the stack was started. The format is a number between 0 and 100 inclusive.

Protocol Granularity Indicates the origin of the protocol used for on-demand activations of tunnels associated with a dynamic anchor filter. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>: This is not a dynamic anchor filter
- 1 = FILTER: The protocol for the tunnel is from the filter definition.
- 2 = PACKET: The protocol for the tunnel is from the packet requiring the tunnel activation.

Protocol Number IP protocol number to match in the IPv4 or IPv6 header of packets. If the filter applies to all IP protocols, this field is stored as blanks. This value is expressed as a string of up to 3 characters. 0 is a valid IP protocol number.

Rule ID This column concatenates the Filter Rule Definition Name, Rule Tag and Tunnel ID into a single string that can be used to uniquely identify filter rules. The Rule ID is used to identify rules on graph views so that the values displayed on the graphs can be correlated with the rows in the table view. The three components of the Rule ID are separated by a colon (:) character. If the rule is not associated with a Tunnel ID, that component of the ID is omitted. This column is represented as a character string of 106 characters. This field is not displayed.

Rule Tag The filter rule definition name extension. The extension is assigned by the stack to identify related rules derived from the same definition. The column is stored as an 8-character string. This field is not displayed.

Scope The type of traffic that this filter applies to. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = LOCAL
- 2 = ROUTED

- 3 = SCOPEALL.

Security Class The IP filter security class. This filter is applied to all packets traversing the IP interfaces, and these interfaces are associated with security classes. This value is expressed as an integer between 0 and 255 inclusive. A value of zero (0) means that all security classes are filtered. If a non-zero value is specified for the security class, then the filter applies to data traversing all interfaces associated with the specified security class.

Sequence Number The value in this column is used to ensure that filters are displayed in the order that the Network Management Interface (NMI) returns them. This value is represented as an integer.

Source Address Source IP address or addresses that the filter applies to. Filters apply to either IPv4 addresses or IPv6 address, but not both. If the filter applies to all source IP addresses, the field is displayed as blank; a value of "0" padded to the right with blanks is stored in the table for this case. If the filter is for a range of source IP addresses, this field displays the lower address in the range. This value is represented as a 45-character string.

Note: For comparison, leading zeros are added for unspecified digits in IPv4 and IPv6 addresses when they are stored.

Source Address Granularity Indicates the origin of the source address used for on-demand activations of tunnels associated with a dynamic anchor filter. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>: This is not a dynamic anchor filter.
- 1 = FILTER: The source address for the tunnel is from filter definition.
- 2 = PACKET: The source address for the tunnel is from the packet requiring the tunnel activation.

Source Port Granularity Indicates the origin of the source port used for on-demand activations of tunnels associated with a dynamic anchor filter. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>: This is not a dynamic anchor filter
- 1 = FILTER: The source port for tunnel is from the filter definition.
- 2 = PACKET: The source port for tunnel is from the packet requiring the tunnel activation

State Current filter state. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = ACTIVE
- 1 = INACTIVE

SWSA Shadow Indicator Indicates whether or not the filter originated from a distributing stack (SHADOW) or the local stack (NOT_SHADOW). This value is only meaningful for dynamic filters. If the filter type is not dynamic, the value is set to 0 and a blank is displayed. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = NOT_SHADOW
- 2 = SHADOW

A value of SHADOW indicates that the filter originated from a distributing stack. This indicator is significant if filter type is dynamic. If the filter type is not dynamic, a value of zero (0) is stored and blanks are displayed in the field.

Sysplex Name The name of the sysplex that the monitored system is part of. This field is not displayed.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters. This field is not displayed.

TCP Connect Indicates what types of TCP connect attempts are to be filtered. TCP connect attempts (SYN packets) in the direction opposite that specified in this field do not match this filter. This field is meaningful for generic or anchor filters only. It is zero (0) when the filter is not one of these types. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = NONE
- 1 = INBOUND
- 2 = OUTBOUND

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters. This field is not displayed.

Total Packets Denied by Mismatch The total number of packets denied due to a mismatch with this filter's action since the start of the TCP/IP stack. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Packets Denied by Action Mismatch (in G) column to calculate the cumulative number of packets denied by action mismatch. The format is an integer.

Total Packets Denied by Mismatch (in G) The total number of packets denied due to a mismatch with this filter's action since the start of the TCP/IP stack, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Packets Denied By Action Mismatch column to calculate the cumulative number of packets denied by action mismatch. The format is an integer.

Total Packets Matched The total number of packets that matched this filter's condition and action since the start of the TCP/IP stack. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Packets Matched (in G) column to calculate the cumulative number of packets matched. The format is an integer.

Total Packets Matched (in G) The total number of packets that matched this filter's condition and action since the start of the TCP/IP stack, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Packets Matched column to calculate the cumulative number of packets matched. The format is an integer.

Tunnel ID Identifier for the associated tunnel. The tunnel ID is generated by the stack. It is not unique. Several related tunnels may have the same tunnel ID. The related tunnels are different instances of the same security association. Usually the related instances exist due to the expiration and refresh of tunnels.This field will be blank if filter is not associated with a tunnel. The ID is a character string of up to 48 characters.

Type Indicates the filter type. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = GENERIC
- 2 = MANUAL
- 3 = DYNANCHOR
- 4 = DYNAMIC
- 5 = NATTANCHOR
- 6 = NATTDYN
- 7 = NRF

Update Time The time when the filter was updated, based on how the filter was created.

- For a statically defined filter originating from the Policy Agent configuration, this field represents the time that the filter's attributes were last updated in the current instance of the Policy Agent. Filters of this type have the value of **1** meaning Policy for the Filter Set attribute.

- For a filter originating from the TCP/IP profile, this field represents the time that the profile filter configuration was last replaced. Filters of this type have the value of **0** meaning Default for the Filter Set attribute.
- For dynamically defined filters, this field is blank. Dynamically defined filters have a filter type of **DYNAMIC**, **NATTDYN**, or **NRF**.

This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Upper Destination Address If the filter is for a range of destination IP addresses, this is the high value for the range. This field will be displayed as blank if destination is not a range of addresses or the filter is for all destination addresses; a value of “0” padded to the right with blanks is stored in the table. This value is represented as a 45-character string.

Note: For comparison, leading zeros are added for unspecified digits in IPv4 and IPv6 addresses when they are stored.

Upper Destination Port If the filter is for a range of destination IP port addresses, this is the high value for the range. This field is stored as blanks if the filter is not for a range of IP port addresses and applies to all ports. This value is represented as a 5-character string.

Upper NATT Client ID If the peer is behind a NAT and a gateway and the peer supplied a client ID, indicates the upper address range of the NAT traversal gateway (NATT) client ID. This field contains an IPv4 dotted decimal address if the NATT Client ID Type is IPv4_ADDR_RANGE. If the NATT Client ID Type is 0, 1, or 4, this field is stored as blanks. This field is a character string of up to 15 characters.

Upper Source Address If the filter is for a range of source IP addresses, this is the high value for the range. This field will be displayed as blank if the source address is not a range or the filter applies to all source IP addresses; a value of “0” padded to the right with blanks will be stored in the table for this case. The format is a string of up to 45 characters.

Note: For comparison, leading zeros are added for unspecified digits in IPv4 and IPv6 addresses when they are stored.

Upper Source Port If the filter is for a range of source IP port addresses, this is the high value for the range. This field is stored as blanks if filter is not for a range of IP port addresses and applies to all ports. This value is represented as a 5-character string.

VPN Action Name The name specified on a virtual private network (VPN) action definition statement. The VPN action describes how to protect the traffic that flows on the tunnel. It specifies attributes of the tunnel, such as what type of encryption to use. The name is a character string of up to 48 characters.

Dynamic IP Tunnels Attributes (KN3ITD)

Use the Dynamic IP Tunnels attributes to display the availability and performance statistics for dynamic IP tunnels known to the Internet Key Exchange (IKE) daemon and the TCP/IP stack.

This data is available for monitoring agents running under z/OS version 1.8 or higher.

Activation Method Indicates how the tunnel was activated. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = USER: User activation from the command line.
- 2 = REMOTE: Remote activation from the IPSec peer.
- 3 = ONDEMAND: On-demand activation caused by IP traffic.
- 5 = TAKEOVER: Sysplex-Wide Security Associations (SWSA) activation as a result of a Dynamic Virtual IP Addressing (DVIPA) takeover.
- 6 = AUTOACT: Auto-activation.

Authentication Algorithm Identifies the authentication algorithm used for this tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 38 = MD5
- 39 = SHA1

Authentication Protocol Identifies the authentication protocol to be used by the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 51 = AH
- 50 = ESP

Bytes The number of inbound and outbound bytes for this tunnel during the most recent time interval. The format is an integer.

Byte Rate The number of inbound or outbound bytes, per minute, for this tunnel during the most recent time interval. The format is an integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute

- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Current Life Size The number of bytes of data that have traversed the tunnel since the tunnel was activated. This value is zero (0) if no life size was negotiated for the tunnel. The format is an integer.

Dest NAT-OA Payload The destination network address translation original address (NAT-OA) payload. NAT-OA payloads are exchanged only for certain UDP-encapsulated tunnels. During NAT traversal negotiations, the Internet Key Exchange (IKE) peer sends the known destination IPv4 address. If NAT traversal negotiation does not occur, or if peer does not send a source NAT-OA payload, this column is blank. This column is stored as a 15-character string. This field is not displayed.

Destination Address Destination IP address for data protected by the tunnel. This value may be an IPv4 or IPv6 address. If the traffic protected by the tunnel may have any destination IP address, this field is stored as blanks. If the traffic protected by the tunnel is a range of destination IP addresses, the value displayed is the lower address in the range. This value is represented as a 45-character string.

Note: For comparison, leading zeros are added for unspecified digits in IPv4 and IPv6 addresses when they are stored.

Destination Port Destination port for traffic protected by the tunnel. If the tunnel protects data for all destination ports, this value is 0. This field is represented by a 5-character string.

Diffie-Hellman Group Diffie-Hellman group used to generate keying material for the tunnel. Each group identifies the number of bits to be used in a prime number that is used to generate keying material. This column is blank if PFS (perfect forward security) was not negotiated for the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 99 = <blank>
- 0 = NONE
- 1 = GROUP1
- 2 = GROUP2
- 5 = GROUP5
- 14 = GROUP14

Encapsulation Mode Encapsulation mode to be used by the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = TUNNEL
- 2 = TRANSPORT

Encryption Algorithm Tunnel encryption algorithm. This field is undefined if the tunnel state is PENDING or INCOMPLETE. A value of 99 is assigned to the field in this case and blanks are displayed. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = NONE
- 3 = 3DES
- 11 = NULL
- 12 = AES
- 18 = DES
- 99 = <blank>

Extended State Indicates progress of tunnel negotiation. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = INIT: No key exchange messages have been initiated.
- 1 = KEP: Key exchange messages have been initiated.
- 2 = DONE: All key exchange messages have been completed, and the tunnel is usable for traffic.
- 3 = PENDING_NOTIFY: Key exchange messages have been completed, waiting to receive connection notification.
- 4 = PENDING_START: Waiting for the activation of an Internet Key Exchange (IKE) tunnel.

Filter Rule Definition Name The name specified for the filter rule definition that this tunnel is associated with. This column is stored as a 48-character string.

Inbound Authentication SPI Tunnel inbound authentication security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This field is an unsigned 4-byte integer and is displayed in hexadecimal. This field is undefined and displayed as blanks if the state of the tunnel is PENDING or INCOMPLETE. This field is not displayed.

Inbound Bytes The number of inbound bytes for this tunnel during the most recent time interval. The format is an integer.

Inbound Encryption SPI Tunnel inbound encryption security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This is an unsigned 4-byte integer and is displayed in hexadecimal. This field is undefined and displayed as blanks if the state of the tunnel is PENDING or INCOMPLETE. This field is not displayed.

Inbound Packets The number of inbound packets for this tunnel during the most recent time interval. The format is an integer.

Initiation Indicator Indicates if the local security endpoint may initiate dynamic tunnel negotiations with the remote security endpoint. Either security endpoint may initiate refreshes regardless of the value of this indicator. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

IP Address Version The version of the IP addresses being used for the traffic descriptor and the security endpoints. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = IPv4: The traffic descriptor and the security endpoints are using IPv4 addresses.
- 1 = IPv6: The traffic descriptor and the security endpoints are using IPv6 addresses.

This field is not displayed.

Life Expiration Time The time at which the tunnel will expire. This column is blank if no life time was negotiated. This time is displayed in the following format:

mm/dd/yy hh:mm:ss

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Life Refresh Time The time at which the tunnel is refreshed. This column is blank if no life time was negotiated. This time is displayed in the following format:

mm/dd/yy hh:mm:ss

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Life Size The number of bytes of data that may traverse the tunnel over the life of the tunnel. This value is zero (0) if no life size was negotiated for the tunnel. The format is an integer.

Local Client ID The Internet Security Associations Key Management Protocol (ISAKMP) identity of local client. A string containing an identifier as described by Local Client ID Type. Some of the ID strings can get

as long as 2048 characters. The ID is always truncated at 100 characters. If no IDs are exchanged, this fields contains blanks. The format is a string of up to 100 characters. This field is not displayed.

Local Client ID Type Internet Security Associations Key Management Protocol (ISAKMP) identity type for the local client ID as defined in RFC 2407. If client IDs were not exchanged during negotiation, this column is blank. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = IPv4_ADDR
- 2 = FQDN
- 3 = USER_FQDN
- 4 = IPv4_ADDR_SUBNET
- 5 = IPv6_ADDR
- 6 = IPv6_ADDR_SUBNET
- 7 = IPv4_ADDR_RANGE
- 8 = IPv6_ADDR_RANGE
- 9 = DER_ASN1_DN
- 10 = DER_ASN1_GN
- 11 = KEY_ID

This field is not displayed.

Local Dynamic VPN Rule Name The name specified on a z/OS Communications Server Policy Agent LocalDynVpnRule configuration statement. The statement describes traffic that is to be protected by a tunnel that is activated on demand using the ipsec command or when the Internet Key Exchange (IKE) daemon or the TCP/IP stack is started or both. This field is stored as blanks if the tunnel is not associated with a local rule. The name is a character string of up to 48 characters.

Local NAT Indicator Indicates if a NAT has been detected in front of the local security endpoint. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Local Security Endpoint The IP address of the local security endpoint responsible for negotiating the tunnel. The format is a character string of up to 45 characters.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters. This field is not displayed.

Outbound Authentication SPI Tunnel outbound authentication security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This is an unsigned 4-byte integer and is displayed in hexadecimal. This field is undefined and displayed as blanks if the state of the tunnel is PENDING or INCOMPLETE. This field is not displayed.

Outbound Bytes The number of outbound bytes for this tunnel during the most recent time interval. The format is an integer.

Outbound Encryption SPI Tunnel outbound encryption security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This is an unsigned 4-byte integer and is displayed in hexadecimal. This field is undefined and displayed as blanks if the state of the tunnel is PENDING or INCOMPLETE. This field is not displayed.

Outbound Packets The number of outbound packets for this tunnel during the most recent time interval. The format is an integer.

Packet Rate The number of inbound or outbound packets, per minute, for this tunnel during the most recent time interval. The format is an integer.

Packets The number of inbound and outbound packets for this tunnel during the most recent time interval. The format is an integer.

Parent IKE Tunnel ID Tunnel ID for this tunnel's parent IKE (Phase 1) tunnel. The Internet Key Exchange (IKE) tunnel is used to negotiate the IP tunnel. This field is represented as a 48-character string.

Pending New Indicator Pending new activation indicator. If set, this field indicates that dynamic IP tunnel is in the pending state and it represents a new activation rather than a refresh. If it is not set, the tunnel is either not in pending state or is not a new activation. For z/OS Communications Server Version 1.7, the value will always be 0. This value is stored as an integer and displayed as a string. Valid values are

- 0 = <blank>
- 1 = Yes

Protocol The IP protocol number for the data to be carried in the tunnel. A value of zero (0) indicates that tunnel protects data for any protocol. The format is an integer representing an Internet Engineering Task Force (IETF)-defined protocol number.

Refresh Life Size The number of bytes that may traverse the tunnel before a refresh is needed. This value is zero (0) if no life size was negotiated. The format is an integer.

Remote Client ID Internet Security Associations Key Management Protocol (ISAKMP) identity of remote client. A string containing an identifier as described by Remote Client ID Type. Some of the ID strings can get as long as 2048 characters. The ID is always truncated at 100 characters. If no IDs are exchanged, this field contains blanks. The format is a string of up to 100 characters. This field is not displayed.

Remote Client ID Type Internet Security Associations Key Management Protocol (ISAKMP) identity type for the remote client ID as defined in RFC 2407. If the client IDs were not exchanged during negotiation, this column is blank. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = IPv4_ADDR
- 2 = FQDN
- 3 = USER_FQDN
- 4 = IPv4_ADDR_SUBNET
- 5 = IPv6_ADDR
- 6 = IPv6_ADDR_SUBNET
- 7 = IPv4_ADDR_RANGE
- 8 = IPv6_ADDR_RANGE
- 9 = DER_ASN1_DN
- 10 = DER_ASN1_GN
- 11 = KEY_ID

This field is not displayed.

Remote IKE UDP Port The IKE UDP port of the remote security endpoint. This column is blank when UDP encapsulation is not being used by the tunnel. This column is stored as a 5-character string.

Remote NAPT Indicator Indicates if a network address port translation (NAPT) has been detected in front of the remote security endpoint. It is possible that an NAPT may exist but is detected only as a NAT. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>

- 1 = Yes

Remote NAT Indicator Indicates if a NAT has been detected in front of the remote security endpoint. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Remote NAT Traversal Gateway Indicator Indicates if the remote security endpoint is acting as a NAT traversal gateway. If the remote security endpoint is acting as a NAT traversal gateway, the tunnel uses UDP encapsulation and the remote security endpoint is acting as an IPSec gateway. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Remote Security Endpoint The IP address of the remote security endpoint responsible for negotiating the tunnel. The format is a character string of up to 45 characters.

Remote zOS Indicator Indicates if the remote peer is a z/OS system. This can be detected only if NAT traversal is enabled. Even if NAT traversal is enabled, it is possible for the remote peer to be a z/OS system and this indicator not to be set. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Source Address Source IP address for data protected by this tunnel. This address may be an IPv4 or IPv6 address. If the traffic protected by the tunnel may have any source IP address, the address is blank. If the traffic protected by the tunnel is a range of source IP addresses, the value displayed is the lower address in the range. This value is represented as a 45-character string.

Note: For comparison, leading zeros are added for unspecified digits in IPv4 and IPv6 addresses when they are stored.

Source NAT-OA Payload The source network address translation original address (NAT-OA) payload. NAT-OA payloads are exchanged only for certain UDP-encapsulated tunnels. During NAT traversal negotiations, the Internet Key Exchange (IKE) peer sends the source IPv4 address that it is aware of. If NAT traversal negotiation did not occur, or if peer did not send a source NAT-OA payload, this column is blank. This column is stored as a 15-character string. This field is not displayed.

Source Port Source port for traffic protected by tunnel. If the tunnel protects data for all source ports, this value is 0. This field is represented by a 5-character string.

State Current state of tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 2 = PENDING: Waiting for negotiation to start.
- 3 = INCOMPLETE: Negotiation in progress.
- 4 = ACTIVE: Tunnel is active and ready for use.
- 5 = EXPIRED: Expired and cannot be used.

SWSA Shadow Indicator Sysplex-Wide Security Associations shadow indicator. If this value is set, the tunnel is a SWSA shadow tunnel. This value is stored as an integer and displayed as a string.

- 0 = <blank>
- 1 = Yes

Sysplex Name The name of the sysplex that the monitored system is part of. This field is not displayed.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters. This field is not displayed.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters. This field is not displayed.

Total Bytes The total number of inbound and outbound bytes for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Bytes (in G) column to calculate the total bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Bytes (in G) The total number of inbound and outbound bytes for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Bytes column to calculate the total bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Inbound Bytes The total number of inbound bytes for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Inbound Bytes (in G) column to calculate the total inbound bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Inbound Bytes (in G) The total number of inbound bytes for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Inbound Bytes column to calculate the total inbound bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Inbound Packets The total number of inbound packets for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Inbound Packets (in G) column to calculate the total inbound packets for the tunnel. For SWSA tunnels, the value is for packets that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Inbound Packets (in G) The total number of inbound packets for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Inbound Packets column to calculate the total inbound packets for the tunnel. For SWSA tunnels, the value is for packets that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Outbound Bytes The total number of outbound bytes for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Outbound Bytes (in G) column to calculate the total outbound bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Outbound Bytes (in G) The total number of outbound bytes for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Outbound Bytes column to calculate the total outbound bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Outbound Packets The total number of outbound packets for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total

Outbound Packets (in G) column to calculate the total outbound packets for the tunnel. For SWSA tunnels, the value is for packets that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Outbound Packets (in G) The total number of outbound packets for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Outbound Packets column to calculate the total outbound packets for the tunnel. For SWSA tunnels, the value is for packets that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Packets The total number of inbound and outbound packets for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Packets (in G) column to calculate the total packets for the tunnel. For SWSA tunnels, the value is for packets that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Packets (in G) The total number of inbound and outbound packets for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Packets column to calculate the total packets for the tunnel. For SWSA tunnels, the value is for packets that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Tunnel ID Tunnel identifier. This identifier is generated by TCP/IP and is not unique. Multiple related tunnels may have the same tunnel ID. The format is an alphanumeric string of up to 48 characters.

Upper Destination Address If the traffic protected by the tunnel is a range of destination IP addresses, this is the upper address in the range. This value may be an IPv4 or IPv6 address. If the traffic protected by the tunnel is not a range of addresses or all addresses, this field is stored as blanks. This field is represented as a 45-character string.

Note: For comparison, leading zeros are added for unspecified digits in IPv4 and IPv6 addresses when they are stored.

Upper Source Address If the traffic protected by the tunnel is a range of source IP addresses, this is the upper address in the range. This may be an IPv4 or IPv6 address. If the traffic protected by the tunnel is not a range of addresses or is all addresses, this field is stored as blanks. This field is represented as a 45-character string.

Note: For comparison, leading zeros are added for unspecified digits in IPv4 and IPv6 addresses when they are stored.

VPN Action Name The name specified on a virtual private network (VPN) action definition statement. The VPN action describes how to protect the traffic that flows through the tunnel. It specifies attributes of the tunnel, such as what type of encryption to use. The format of the name is a character string of up to 48 characters.

VPN Life Expiration Time The time at which the tunnel should no longer be refreshed. This column is blank if no life time was negotiated for the VPN (security attributes implemented by the tunnel). This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour

- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Internet Key Exchange (IKE) Tunnels Attributes (KN3ITI)

Use the IKE tunnels attribute to display availability and performance statistics for IKE tunnels known to the IKE daemon for a specific stack. IKE tunnels are used by a security endpoint (IKE daemon) to negotiate dynamic IP tunnels.

This data is available for monitoring agents running under z/OS version 1.8 or higher.

Active Dynamic Tunnels Current count of active dynamic tunnels associated with this Internet Key Exchange (IKE) tunnel. The format is an integer.

Authentication Algorithm The authentication algorithm used for this tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 38 = MD5
- 39 = SHA1

Byte Rate The number of bytes protected, per minute, for this tunnel during the most recent time interval. The format is an integer.

Bytes The number of bytes protected by this tunnel during the most recent time interval. The format is an integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:
`mm/dd/yy hh:mm:ss`

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month

- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Diffie-Hellman Group Diffie-Hellman group used to generate keying material for the tunnel. Each group identifies the number of bits to be used in a prime number that is used to generate keying material. This column is blank if PFS (perfect forward security) was not negotiated for the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = NONE
- 1 = GROUP1
- 2 = GROUP2
- 5 = GROUP5
- 14 = GROUP14

Encryption Algorithm Encryption algorithm used by the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 3 = 3DES
- 12 = AES
- 18 = DES

Exchange Mode Exchange mode used by a tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 2 = MAIN
- 4 = AGGRESSIVE

Extended State Indicates the progress of the tunnel negotiation. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = INIT: No key exchange messages have been initiated.
- 1 = WAIT_SA: The first key exchange message has been sent and the endpoint is waiting for a response.
- 2 = IN_KE: A key exchange response has been sent.
- 3 = WAIT_KE: A key exchange message has been sent and the endpoint is waiting on a response.
- 4 = DONE: All key exchange messages have been completed and the tunnel is ready for data traffiic.
- 5 = EXPIRED: Tunnel has exceeded its life time or life size and is not available for data traffic.

In Progress Dynamic Tunnels Current count of in-progress dynamic tunnels associated with this Internet Key Exchange (IKE) tunnel. The format is an integer.

Initiation Indicator Indicates if the local security endpoint may initiate Internet Key Exchange (IKE) tunnel negotiations with the remote security endpoint. Either security endpoint may initiate refreshes regardless of the value of this indicator. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Initiator Cookie A string of hexadecimal digits that, when combined with the Responder Cookie, uniquely identifies the SA for the tunnel. This value is stored as a 16-character string. This field is not displayed.

IP Address Version The version of the IP addresses being used for the security endpoints.This value is stored as an integer and displayed as a string. Valid values are:

- 0 = IPv4: The traffic descriptor and the security endpoints are using IPv4 addresses.
- 1 = IPv6: The traffic descriptor and the security endpoints are using IPv6 addresses.

This value is not displayed.

Key Exchange Action Name The name specified on a z/OS Communications Server Policy Agent KeyExchangeAction configuration statement. This name identifies the action being used to activate this Internet Key Exchange (IKE) tunnel. Key exchange actions describe how key exchanges between security endpoints should be protected. This field is stored as a 48-character string.

Key Exchange Rule Name The name specified on a z/OS Communications Server Policy Agent KeyExchangeRule configuration statement. This name identifies the rule being used to activate this Internet Key Exchange (IKE) tunnel. Key exchange rules identify the security endpoints for an IKE tunnel and the policy to be used for the tunnel by referencing a key exchange action. This field is stored as a 48-character string.

Life Expiration Time The time at which the tunnel will expire. This column is blank if no life time was negotiated. This time is displayed in the following format:

`mm/dd/yy hh:mm:ss`

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Life Refresh Time The time at which the tunnel is refreshed. This column is blank if no life time was negotiated. This time is displayed in the following format:

`mm/dd/yy hh:mm:ss`

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute

- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Life Size The number of bytes of data that may traverse the tunnel over the life of the tunnel. This value is 0 if no life size was negotiated for the tunnel. The format is an integer.

Life Time The amount of time, in seconds, that the tunnel is to remain active. The format is an integer.

Local NAT Indicator Indicates if network address translation (NAT) has been detected in front of the local security endpoint. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Local Security Endpoint The IP address of the local security endpoint (IKE) responsible for negotiating the tunnel. The format is a character string of up to 45 characters.

Local Security Endpoint ID Internet Security Associations Key Management Protocol (ISAKMP) identity of local security endpoint. This field is a string containing an identifier, as described by local security endpoint ID type. Some ID strings can be as long as 2048 characters. The ID is always truncated at 100 characters. If no IDs are exchanged, this field is stored as blanks. This field is not displayed.

Local Security Endpoint ID Type Internet Security Associations Key Management Protocol (ISAKMP) identity type for the local security endpoint as defined in RFC 2407. If client IDs were not exchanged during negotiation, this column is blank. ISAKMP peers exchange and verify each other's identities as part of the Internet Key Exchange (IKE) tunnel (Phase 1) negotiation. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = IPv4_ADDR
- 2 = FQDN
- 3 = USER_FQDN
- 4 = IPv4_ADDR_SUBNET
- 5 = IPv6_ADDR
- 6 = IPv6_ADDR_SUBNET
- 7 = IPv4_ADDR_RANGE
- 8 = IPv6_ADDR_RANGE
- 9 = DER_ASN1_DN
- 10 = DER_ASN1_GN
- 11 = KEY_ID

This field is not displayed.

NAT Traversal Indicator Indicates if the network address translation (NAT) traversal function is enabled for the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

NAT Traversal Support Level Indicates the type of network address translation (NAT) traversal support being used. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = NONE: No NAT traversal support. Support is either not configured or not negotiated.
- 1 = RFCD2: RFC 3947 draft 2 support.
- 3 = RFCD3: RFC 3947 draft 3 support.
- 4 = RFC: RFC 3947 support with non-z/OS peer.
- 5 = ZOS: RFC 3947 support with z/OS peer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters. This field is not displayed.

Peer Authentication Method Peer authentication method. This value is stored as an integer and displayed as a string. Valid values are:

- 3 = PRESHAREDKEY
- 2 = RSASIGNATURE

Percent Failed Activations The percent of dynamic tunnel activations that have failed for this Internet Key Exchange (IKE) tunnel. The format is a number between 0 and 100 inclusive.

Percent In Progress Dynamic Tunnels The percentage of dynamic tunnels in progress compared to active dynamic tunnels. The format is a number between 0 and 100 inclusive.

Remote IKE UDP Port Remote UDP port used for Internet Key Exchange (IKE) negotiations. This column is stored as a 5-character string.

Remote NAT Indicator Indicates if a NAT has been detected in front of the remote security endpoint. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Remote NAPT Indicator Indicates if a network address port translation (NAPT) has been detected in front of the remote security endpoint. It is possible that a NAPT may exist but is detected only as a NAT. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Remote Security Endpoint The IP address of the remote security endpoint (IKE) responsible for negotiating the tunnel. The format is a character string of up to 45 characters.

Remote Security Endpoint ID Internet Security Associations Key Management Protocol (ISAKMP) identity of remote security endpoint. This field is a string containing an identifier, as described by remote security endpoint ID type. Some ID strings can be as long as 2048 characters. The ID is always truncated at 100 characters. If no IDs are exchanged, this field is stored as blanks. This field is not displayed.

Remote Security Endpoint ID Type Internet Security Associations Key Management Protocol (ISAKMP) identity type for the remote security endpoint as defined in RFC 2407. If client IDs were not exchanged

during negotiation, this column is blank. ISAKMP peers exchange and verify each other's identities as part of the Internet Key Exchange (IKE) tunnel (Phase 1) negotiation. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = IPv4_ADDR
- 2 = FQDN
- 3 = USER_FQDN
- 4 = IPv4_ADDR_SUBNET
- 5 = IPv6_ADDR
- 6 = IPv6_ADDR_SUBNET
- 7 = IPv4_ADDR_RANGE
- 8 = IPv6_ADDR_RANGE
- 9 = DER_ASN1_DN
- 10 = DER_ASN1_GN
- 11 = KEY_ID

This field is not displayed.

Responder Cookie A string of hexadecimal digits that, when combined with the Initiator Cookie, uniquely identifies the SA for the tunnel. This value is stored as a 16-character string. This field is not displayed.

Role Role of the local security endpoint in the activation of the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = INITIATOR
- 2 = RESPONDER

State Current state of the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 3 = INCOMPLETE: Tunnel negotiation is in progress.
- 4 = ACTIVE: Tunnel is active and ready for use.
- 5 = EXPIRED: Tunnel has expired and cannot be used.

Sysplex Name The name of the sysplex that the monitored system is part of. This field is not displayed.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters. This field is not displayed.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters. This field is not displayed.

Total Bytes The cumulative number of bytes protected by this tunnel since the tunnel was activated. The value in this column can be added to the product of 1,073,741,823 and the value in the Total Bytes (in G) column to calculate the total bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Bytes (in G) The cumulative number of bytes protected by this tunnel since the tunnel was activated, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,823 and added to the value in the Total Bytes column to calculate the total bytes for the tunnel. The format is an integer.

Total Failed Local Activations Cumulative count of failed locally initiated dynamic tunnel activations for this Internet Key Exchange (IKE) tunnel. The format is an integer.

Total Failed Remote Activations Cumulative count of failed remotely initiated dynamic tunnel activations for this Internet Key Exchange (IKE) tunnel. The format is an integer.

Total Successful Local Activations Cumulative count of successful locally initiated dynamic tunnel activations for this Internet Key Exchange (IKE) tunnel. The format is an integer.

Total Successful Remote Activations Cumulative count of successful remotely initiated dynamic tunnel activations for this Internet Key Exchange (IKE) tunnel. The format is an integer.

Tunnel ID Tunnel identifier. This identifier is generated by the Internet Key Exchange (IKE) daemon and is not unique. Multiple related tunnels may have the same tunnel ID. This value is a character string of up to 48 characters.

IPSec Status Attributes (KN3ISS)

Use the IPSec Status attributes to display IP stack security configuration information and IP stack security statistics.

This data is available for monitoring agents running under z/OS version 1.8 or higher.

Active Dynamic SWSA Shadow Tunnels The current number of active dynamic Sysplex-Wide Security Associations shadow tunnels known to the TCP/IP stack. The format is an integer.

Active Dynamic Tunnels The current number of active dynamic tunnels known to the TCP/IP stack. This number does not include Sysplex-Wide Security Associations (SWSA) shadow tunnels or manual tunnels. The format is an integer.

Active IKE Tunnels The number of Internet Key Exchange (IKE) tunnels that are currently active. The format is an integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:
`mm/dd/yy hh:mm:ss`

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Dynamic Tunnels in Progress The number of dynamic tunnels in progress. The state of the tunnel is either PENDING or IN NEGOTIATION. The format is an integer where:

- 0 means PENDING
- 1 means IN NEGOTIATION

Expired Dynamic Tunnels The number of dynamic tunnels that are currently expired. This value includes shadow and non-shadow tunnels. The format is an integer.

Expired IKE Tunnels The number of Internet Key Exchange (IKE) tunnels that are currently expired. The format is an integer.

Filter Logging Indicates whether or not filter logging is enabled for the TCP/IP stack. Filter logging was enabled by coding the LOGENABLE parameter of the IPSEC statement in the TCP/IP profile. For more information about the IPSEC statement, refer to the most recent edition of the z/OS Communication Server *IP Configuration Guide* or *IP Configuration Reference*. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Disabled
- 1 = Enabled

Filter Set In Use Identifies which filter set is currently in use by the TCP/IP stack. One of two filter sets may be in use at any time:

- The default filter set, which is made up of filters defined in the TCP/IP profile.
- The policy filter set, which is made up of filters defined in Policy Agent configuration files.

This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Default
- 1 = Policy

IKE Bytes Protected The number of bytes protected by Internet Key Exchange (IKE) tunnels in the last interval. The format is an integer.

IKE Inbound Bytes Protected The number of inbound bytes protected by IKE tunnels in the last interval. The format is an integer.

IKE Inbound Protected Byte Rate The number of inbound bytes flowing through Internet Key Exchange (IKE) tunnels every minute. The format is an integer.

IKE Outbound Bytes Protected The number of outbound bytes protected by Internet Key Exchange (IKE) tunnels in the last interval. The format is an integer.

IKE Outbound Protected Byte Rate The number of outbound bytes flowing through Internet Key Exchange (IKE) tunnels every minute. The format is an integer.

IKE Protected Byte Rate The number of bytes flowing through Internet Key Exchange (IKE) tunnels every minute. The format is an integer.

IKE Total Bytes Protected The cumulative number of inbound and outbound bytes of Internet Key Exchange (IKE) traffic protected by IKE tunnels since the IKE daemon was started. The value in this column can be added to the product of 1,073,741,824 and the value in the IKE Total Bytes Protected (in G) column to calculate the cumulative total bytes of IKE traffic protected by IKE tunnels. The format is an integer.

IKE Total Bytes Protected (in G) The cumulative number of inbound and outbound bytes of Internet Key Exchange (IKE) traffic protected by IKE tunnels since the IKE daemon was started, divided by

1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the IKE Total Bytes Protected column to calculate the cumulative total bytes of IKE traffic protected by IKE tunnels. The format is an integer.

IKE Total Inbound Bytes Protected The cumulative number of inbound bytes of IKE traffic protected by IKE tunnels since the IKE daemon was started. The value in this column can be added to the product of 1,073,741,824 and the value in the IKE Inbound Bytes Protected (in G) column to calculate the cumulative number of IKE Inbound Bytes Protected. The format is an integer.

IKE Total Inbound Bytes Protected (in G) The cumulative number of inbound bytes of IKE traffic protected by dynamic tunnels since the start of the IKE daemon, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the IKE Inbound Bytes Protected column to calculate the cumulative number of IKE inbound bytes protected. The format is an integer.

IKE Total Invalid Key Messages Cumulative number of invalid key exchange (phase 1) messages received since the Internet Key Exchange (IKE) daemon was started. This does not include message authentication failures. The format is an integer.

IKE Total Key Message Authentication Failures The cumulative number of key exchange (phase 1) message authentication failures since the Internet Key Exchange (IKE) daemon was started. The format is an integer.

IKE Total Outbound Bytes Protected The cumulative number of outbound bytes of IKE traffic protected by IKE tunnels since the IKE daemon was started. The value in this column can be added to the product of 1,073,741,824 and the value in the IKE Outbound Bytes Protected (in G) column to calculate the cumulative number of IKE Outbound Bytes Protected. The format is an integer.

IKE Total Outbound Bytes Protected (in G) The cumulative number of outbound bytes of IKE traffic protected by dynamic tunnels since the start of the IKE daemon, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the IKE Outbound Bytes Protected column to calculate the cumulative number of IKE outbound bytes protected. The format is an integer.

IKE Total Replayed Key Messages The cumulative number of replayed key exchange (phase 1) messages received since the Internet Key Exchange (IKE) daemon was started. The format is an integer.

IKE Total Retransmitted Key Messages The cumulative number of retransmitted key exchange (phase 1) messages that were sent since the Internet Key Exchange (IKE) daemon was started. The format is an integer.

IKE Tunnels in Progress The number of Internet Key Exchange (IKE) tunnels currently in progress. The format is an integer where:

- 0 means PENDING
- 1 means IN NEGOTIATION

IP Bytes Protected The number of bytes of IP traffic protected by dynamic IP tunnels in the last interval. The format is an integer.

IP Inbound Bytes Protected The number of inbound bytes protected by IP tunnels in the last interval. The format is an integer.

IP Inbound Protected Byte Rate The number of inbound bytes flowing through IP tunnels every minute. The format is an integer.

IP Outbound Bytes Protected The number of outbound bytes protected by IP tunnels in the last interval. The format is an integer.

IP Outbound Protected Byte Rate The number of outbound bytes flowing through IP tunnels every minute. The format is an integer.

IP Protected Byte Rate The number of bytes of IP traffic flowing through dynamic IP tunnels every minute. The format is an integer.

IP Security Indicates whether or not IP security functions are enabled for IPv4 interfaces. IP security was enabled by coding IPCONFIG IPSECURITY in the TCP/IP profile. For more information about the IPSEC statement, refer to the most recent edition of the z/OS Communication Server *IP Configuration Guide* or *IP Configuration Reference*. This value is stored as an integer and displayed as a string. Valid values are:

- 0=Disabled
- 1=Enabled

IP Total Bytes Protected The cumulative number of inbound and outbound bytes of IP traffic protected by dynamic tunnels since the TCP/IP stack was started. The value in this column can be added to the product of 1,073,741,824 and the value in the IP Total Bytes Protected (in G) column to calculate the cumulative total bytes of IP traffic protected by dynamic tunnels. The format is an integer.

IP Total Bytes Protected (in G) The cumulative number of inbound and outbound bytes of IP traffic protected by dynamic tunnels since the TCP/IP stack was started, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the IP Total Bytes Protected column to calculate the cumulative total bytes of IP traffic protected by dynamic tunnels. The format is an integer.

IP Total Inbound Bytes Protected The cumulative number of inbound bytes of IP traffic protected by dynamic tunnels since the start of the TCP/IP stack. The value in this column can be added to the product of 1,073,741,823 and the value in the IP Inbound Bytes Protected (in G) column to calculate the cumulative number of IP Inbound Bytes Protected. The format is an integer.

IP Total Inbound Bytes Protected (in G) The cumulative number of inbound bytes of IP traffic protected by dynamic tunnels since the start of the TCP/IP stack, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,823 and added to the value in the IP Inbound Bytes Protected column to calculate the cumulative number of IP inbound bytes protected. The format is an integer.

IP Total Outbound Bytes Protected The cumulative number of outbound bytes of IP traffic protected by dynamic tunnels since the start of the TCP/IP stack. The value in this column can be added to the product of 1,073,741,823 and the value in the IP Outbound Bytes Protected (in G) column to calculate the cumulative number of IP Outbound Bytes Protected. The format is an integer.

IP Total Outbound Bytes Protected (in G) The cumulative number of outbound bytes of IP traffic protected by dynamic tunnels since the start of the TCP/IP stack, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,823 and added to the value in the IP Outbound Bytes Protected column to calculate the cumulative number of IP outbound bytes protected. The format is an integer.

IPv6 Security Indicates whether or not IP security functions are enabled for IPv6 interfaces. IPv6 security was enabled by coding IPCONFIG IPSECURITY and IPCONFIG6 IPSECURITY in the TCP/IP profile. For more information about the IPSEC statement, refer to the most recent edition of the z/OS Communication Server *IP Configuration Guide* or *IP Configuration Reference*. This value is stored as an integer and displayed as a string. Valid values are:

- 0=Disabled
- 1=Enabled

NAT Keep Alive Interval The NAT keep-alive interval, in seconds. The interval is used to regulate the sending of NAT keep-alive messages for a NAT traversal tunnel when a NAT is detected in front of the local host. The format is an integer expressed in seconds.

Number of Configured Filters The number of configured IP Filters for this stack. The format is an integer.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters. This field is not displayed.

Packets Denied by DENY The number of packets denied by a DENY action on any filter during the most recent collection interval. The format is an integer.

Packets Denied by Mismatch The number of packets denied by a mismatched action on any filter during the most recent interval. The format is an integer.

Packets Filtered The number of packets filtered by the filter rule set during the most recent collection interval. The format is an integer.

Packets Matched The number of packets that matched the condition and action for any filter during the most recent interval. The format is an integer.

Packets Permitted The number of packets permitted by any filter during the most recent interval. The format is an integer.

Percent Packets Denied by DENY The percentage of packets denied by a DENY action on any filter during the most recent interval. The format is a number between 0 and 100 inclusive.

Percent Packets Denied by Mismatch The percentage of packets denied by a mismatched action on any filter during the most recent interval. The format is a number between 0 and 100 inclusive.

Percent Packets Permitted The percentage of packets permitted by any filter during the most recent interval. The format is a number between 0 and 100 inclusive.

Percent Total Packets Denied by DENY The percentage of total packets denied by a DENY action on any filter since the TCP/IP stack was started. The format is a number between 0 and 100 inclusive.

Percent Total Packets Denied by Mismatch The percentage of total packets denied due to a mismatch with any filter action since the stack was started. The format is a number between 0 and 100 inclusive.

Percent Total Packets Permitted The percentage of total packets that were permitted by any filter since the TCP/IP stack was started. The format is a number between 0 and 100 inclusive.

Pre-Decapsulation Filtering Indicates whether or not pre-decapsulation filtering is enabled. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Disabled
- 1 = Enabled

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters. This field is not displayed.

Sysplex Name The name of the sysplex that the monitored system is part of. This field is not displayed.

Sysplex-Wide Security Associations (SWSA) Indicates whether or not sysplex-wide security associations (SWSA) are enabled. SWSA was enabled by coding the DVIPSEC parameter on the IPSEC statement in the TCP/IP profile. For more information about the IPSEC statement, refer to the most recent

edition of the z/OS Communication Server *IP Configuration Guide* or *IP Configuration Reference*. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Disabled
- 1 = Enabled

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Total Active Dynamic Tunnels The total number of currently active dynamic tunnels. This includes active dynamic System-Wide Security Association (SWSA) shadow tunnels and dynamic IP tunnels. The format is an integer.

Total Failed Dynamic Tunnel Activations The cumulative number of failed dynamic tunnel activations since the TCP/IP stack was started. The format is an integer.

Total Failed IKE Tunnel Activations The cumulative number of failed Internet Key Exchange (IKE) tunnel activations that were initiated locally or remotely since the IKE daemon was started. The format is an integer.

Total Failed Local IKE Tunnel Activations The cumulative number of failed Internet Key Exchange (IKE) tunnel activations that were initiated locally since the IKE daemon was started. The format is an integer.

Total Failed Remote IKE Tunnel Activations The cumulative number of failed remote Internet Key Exchange (IKE) tunnel activations since the IKE daemon was started. The format is an integer.

Total Invalid QUICKMODE Messages The cumulative number of invalid QUICKMODE (phase 2) messages received since the Internet Key Exchange (IKE) daemon was started. The format is an integer.

Total Packets Denied by DENY The total number of packets denied by a DENY action on any filter since the TCP/IP stack was started. If the value in the Total Packets Denied By DENY (in G) column is not 0, then the value in this column can be added to the product of 1,073,741,824 and the value in the Total Packets Denied by DENY (in G) column to calculate the packets denied by DENY for any filter. The format is an integer.

Total Packets Denied by DENY (in G) The total number of packets denied by a DENY action on any filter since the TCP/IP stack was started, divided by 1,073,741,824. If the value in this column is not 0, then it can be multiplied by 1,073,741,824 and added to the value in the Total Packets Denied by DENY column to calculate the packets denied by DENY for any filter. The format is an integer.

Total Packets Denied by Mismatch The total number of packets denied due to a mismatch with any filter action since the TCP/IP stack was started. If the value in the Total Packets Denied By Action Mismatch (in G) column is not 0, then the value in this column can be added to the product of 1,073,741,824 and the value in the Packets Denied by Action Mismatch (in G) column to calculate the packets permitted. The format is an integer.

Total Packets Denied by Mismatch (in G) The total number of packets denied due to a mismatch with any filter action since the TCP/IP stack was started, divided by 1,073,741,824. If the value in this column is not 0, then it can be multiplied by 1,073,741,824 and added to the value in the Total Packets Denied by Action Mismatch column to calculate the packets denied by an action mismatch. The format is an integer.

Total Packets Filtered The total number of packets processed by the filter rule set since the TCP/IP stack was started. If the value in the Total Packets Filtered (in G) column is not 0, then the value in this column can be added to the product of 1,073,741,824 and the value in the Total Packets Filtered (in G) column to calculate the total packets processed. The format is an integer.

Total Packets Filtered (in G) The total number of packets processed by the filter rule set since the TCP/IP stack was started, divided by 1,073,741,824. If the value in this column is not 0, then it can be multiplied by 1,073,741,824 and added to the value in the Total Packets Filtered column to calculate the total packets processed. The format is an integer.

Total Packets Matched The total number of packets that matched both the condition and action for any filter since the TCP/IP stack was started. If the value in the Total Packets Matched (in G) column is not 0, then the value in this column can be added to the product of 1,073,741,824 and the value in Total Packets Matched (in G) column to calculate the total packets matched. The format is an integer.

Total Packets Matched (in G) The total number of packets that matched both the condition and action for any filter since the TCP/IP stack was started, divided by 1,073,741,824. If the value in this column is not 0, then it can be multiplied by 1,073,741,824 and added to the value in the Total Packets Matched column to calculate the total packets matched. The format is an integer.

Total Packets Permitted The total number of packets that were permitted by any filter since the TCP/IP stack was started. If the value in the Total Packets Permitted (in G) column is not 0, then the value in this column can be added to the product of 1,073,741,824 and the value in Total Packets Permitted (in G) column to calculate the packets permitted. The format is an integer.

Total Packets Permitted (in G) The total number of packets that were permitted by any filter since the TCP/IP stack was started, divided by 1,073,741,824. If the value in this column is not 0, then it can be multiplied by 1,073,741,824 and added to the value in the Total Packets Permitted column to calculate the packets permitted. The format is an integer.

Total Replayed QUICKMODE Messages The cumulative number of replayed QUICKMODE (phase 2) messages received since the Internet Key Exchange (IKE) daemon was started. The format is an integer.

Total Retransmitted QUICKMODE Messages The cumulative number of retransmitted QUICKMODE (phase 2) messages sent since the Internet Key Exchange (IKE) daemon was started. The format is an integer.

Total Successful Dynamic Tunnel Activations The cumulative number of successful dynamic tunnel activations since the TCP/IP stack was started. The format is an integer.

Total Successful IKE Tunnel Activations The cumulative number of successful Internet Key Exchange (IKE) tunnel activations that were initiated locally or remotely since the IKE daemon was started. The format is an integer.

Total Successful Local IKE Tunnel Activations The cumulative number of successful locally initiated Internet Key Exchange (IKE) tunnel activations since the IKE daemon was started. The format is an integer.

Total Successful Remote IKE Tunnel Activations The cumulative number of successful Internet Key Exchange (IKE) tunnel activations that were initiated locally or remotely since the IKE daemon was started. The format is an integer.

Manual IP Tunnels attributes (KN3ITM)

Use the Manual IP Tunnels attributes to display information about manually defined IP tunnels known to the TCP/IP stack.

This data is available for monitoring agents running under z/OS version 1.8 or higher.

Authentication Algorithm Identifies the authentication algorithm used for this tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 38 = MD5
- 39 = SHA1

Authentication Protocol Identifies the authentication protocol to be used by the tunnel. This value is stored as an integer and displayed as a string. Valid values are:
- 0 = <blank>
- 51 = AH
- 50 = ESP

Byte Rate The number of inbound or outbound bytes, per minute, for this tunnel during the most recent collection interval. The format is an integer.

Bytes The number of inbound and outbound bytes for this tunnel during the most recent collection interval. The format is an integer.

Collection Time The time and date of the data sampling. This time is displayed in the following format:
`mm/dd/yy hh:mm:ss`

Where:
- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:
- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Encapsulation Mode Tunnel encapsulation mode to be used by the tunnel. This value is stored as an integer and displayed as a string. Valid values are:
- 0 = <blank>
- 1 = TUNNEL
- 2 = TRANSPORT

Encryption Algorithm Encryption algorithm to be used by the tunnel. This value is stored as an integer and displayed as a string. Valid values are:
- 0 = NONE
- 3 = 3DES
- 11 = NULL

- 12 = AES
- 18 = DES
- 99 = <blank>

Inbound Authentication SPI Tunnel inbound authentication security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This is an unsigned 4-byte integer and displayed in hexadecimal. This value is not displayed.

Inbound Bytes The number of inbound bytes for this tunnel during the most recent collection interval. The format is an integer.

Inbound Encryption SPI Tunnel inbound encryption security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This is an unsigned 4-byte integer and displayed in hexadecimal. This value is not displayed.

Inbound Packets The number of inbound packets for this tunnel during the most recent collection interval. The format is an integer.

IP Address Version The version of the IP addresses being used for the security endpoints. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = IPv4: The traffic descriptor and the security endpoints are using IPv4 addresses.
- 1 = IPv6: The traffic descriptor and the security endpoints are using IPv6 addresses.

This value is not displayed.

Local Security Endpoint The IP address of the local security endpoint responsible for negotiating the tunnel. The format is an alphanumeric string of up to 45 characters.

Origin Node The unique identifier for the TCP/IP stack being displayed. The format is an alphanumeric string no longer than 32 characters. This field is not displayed.

Outbound Authentication SPI Tunnel outbound authentication security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This field is an unsigned 4-byte integer and displayed in hexadecimal. This value is not displayed.

Outbound Bytes The number of outbound bytes for this tunnel during the most recent collection interval. The format is an integer.

Outbound Encryption SPI Tunnel outbound encryption security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This field is an unsigned 4-byte integer and displayed in hexadecimal. This value is not displayed.

Outbound Packets The number of outbound packets for this tunnel during the most recent time interval. The format is an integer.

Packet Rate The number of inbound or outbound packets, per minute, for this tunnel during the most recent collection interval. The format is an integer.

Packets The number of inbound and outbound packets for this tunnel during the most recent collection interval. The format is an integer.

Remote Security Endpoint The IP address of the remote security endpoint responsible for negotiating the tunnel. The format is an alphanumeric string of up to 45 characters.

State Current tunnel state. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = INACTIVE
- 4 = ACTIVE

Sysplex Name The name of the sysplex that the monitored system is part of. This field is not displayed. This field is not displayed.

System ID The SMF system ID. The format is an alphanumeric string no longer than 4 characters. This field is not displayed.

TCPIP STC Name The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters. This field is not displayed.

Total Bytes The total number of inbound and outbound bytes for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Bytes (in G) column to calculate the total bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Bytes (in G) The total number of inbound and outbound bytes for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Bytes column to calculate the total bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer. The format is an integer.

Total Inbound Bytes The total number of inbound bytes for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Inbound Bytes (in G) column to calculate the total inbound bytes for the tunnel. The format is an integer.

Total Inbound Bytes (in G) The total number of inbound bytes for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Inbound Bytes column to calculate the total inbound bytes for the tunnel. The format is an integer.

Total Inbound Packets The total number of inbound packets for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Inbound Packets (in G) column to calculate the total inbound packets for the tunnel. The format is an integer.

Total Inbound Packets (in G) The total number of inbound packets for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Inbound Packets column to calculate the total inbound packets for the tunnel. The format is an integer.

Total Outbound Bytes The total number of outbound bytes for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Outbound Bytes (in G) column to calculate the total outbound bytes for the tunnel. The format is an integer.

Total Outbound Bytes (in G) The total number of outbound bytes for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Outbound Bytes column to calculate the total outbound bytes for the tunnel. The format is an integer.

Total Outbound Packets The total number of outbound packets for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Outbound Packets (in G) column to calculate the total outbound packets for the tunnel. The format is an integer.

Total Outbound Packets (in G) The total number of outbound packets for this tunnel since the tunnel was established, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,823 and added to the value in the Total Outbound Packets column to calculate the total outbound packets for the tunnel. The format is an integer.

Total Packets The total number of inbound and outbound packets for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Packets (in G) column to calculate the total packets for the tunnel. The format is an integer.

Total Packets (in G) The total number of inbound and outbound packets for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Packets column to calculate the total packets for the tunnel. The format is an integer.

Tunnel ID Tunnel identifier. This identifier is generated by TCP/IP and is not unique. Multiple related tunnels may have the same tunnel ID. The format is an alphanumeric string of up to 48 characters.

VPN Action Name The virtual private network (VPN) Action Name is the name associated with the definition of a security association. The security association describes the attributes of the tunnel. An example is the encryption algorithm to be used. The name is a character string of up to 48 characters.

Updated attribute groups

The following attributes groups were updated in this fix pack.

Interfaces Attributes (KN3TIF)

In APAR OA21641, a user discovered that the Physical Address attribute in the Interfaces and Interfaces History workspaces was not returning the intended data. In Fix Pack 1, this problem has been corrected. The old Physical Address attribute definition has been deprecated, and a new definition has been added.

Old Value:

Physical Address
(deprecated) The address of the interface at the protocol sub-layer. The format is a string up to four characters in length.

New Value:

Physical Address
The address of the interface at the protocol sub-layer or blank. The format is a string up to 12 characters in length. This field will be blank when the interface is not active or is not one of the following types:

- ATM
- HYPERchannel
- LCS Ethernet
- MPCIPA OSA Express QDIO

Connections Attributes (KN3TCN)

The Connections attributes were updated as shown below.

Application Name and Port The Application Name and Local Port are combined in this attribute, separated by a colon. The format is a string up to 15 characters in length.

DVIPA Identifies when the Local IP Address is a Dynamic Virtual IP Addressing (DVIPA) address. This value is stored as an integer and displayed as a string. The following are valid values:

- 0 = [blank] - Not available.
- 1 = Yes
- 2 = No

Note: This information is available only on z/OS version 1.9 or higher.

Local IP Address The local IP address for this connection. For UDP endpoints, a value of 0.0.0.0 (or ::) in this field indicates that the UDP endpoint is accepting datagrams from any local IP address. For TCP listeners, this IP address is 0.0.0.0 (or ::) when the application is accepting connections to any local IP address. The format is a string up to 45 characters in length.

TCP/IP Details Attributes (KN3TCP)

The TCPIP Details attributes were updated as shown below.

Application Name and Port The Application Name and Local Port are combined in this attribute, separated by a colon. The format is a string up to 15 characters in length.

DVIPA Identifies when the Local IP Address is a Dynamic Virtual IP Addressing (DVIPA) address. This value is stored as an integer and displayed as a string. The following are valid values:

- 0 = [blank] - Not available.
- 1 = Yes
- 2 = No

Note: This information is available only on z/OS version 1.9 or higher.

Local IP Address The local IP address for this connection. The format is a string up to 45 characters in length.

TCPIP Gateways Attributes (KN3TGA)

The TCPIP Gateways attributes were updated as shown below.

First Hop The first router in the path to the remote network. The format is an alphanumeric string no longer than 45 characters. This special value may be displayed as follows:

<direct> – First Hop is a host IP address.

Network Address The network address of this gateway. The format is an alphanumeric string no longer than 45 characters. Special values may be displayed as follows:

- *Defaultnet* – The Network Address is a host IP address.
- *Default* – The Network Address is 0.

Link-local IPv6 addresses are displayed in the following format:

FE80::<interface ID>%<interface name>

Subnet Mask The 32-bit (for IPv4 addresses) or 128-bit (for IPv6 addresses) mask for the subnetwork address in the IP address host portion. The format is an alphanumeric string no longer than 45 characters.

The following special values are displayed:

- <none> - Subnet Mask contains zeros
- HOST – Subnet Mask is a host IP address

Subnet Value The subnet identifier. A subnet composes a group of nodes within the same network ID. The format is an alphanumeric string no longer than 45 characters.

Chapter 6. New and updated workspaces

The following workspaces have been added or updated in this fix pack:

Table 26. New and updated workspaces in this fix pack

Workspace Name	Attribute Group	New or Updated?
"IPSec Status workspace" on page 64, as a new type of workspace that applies to all TCP/IP stacks	KN3ISS	New
"IP Filters Statistics workspace" on page 70	KN3ISS	New
"Current IP Filters workspace" on page 74	KN3IFC	New
"Current IP Filters by Destination Address workspace" on page 85	KN3IFC	New
"Current IP Filters by Filter Rule Definition Name workspace" on page 87	KN3IFC	New
"Current IP Filters in Scan Order workspace" on page 89	KN3IFC	New
"Dynamic IP Tunnels Statistics workspace" on page 91	KN3ISS	New
"Dynamic IP Tunnels workspace" on page 95	KN3ITD	New
"Dynamic IP Tunnels by Destination Address workspace" on page 106	KN3ITD	New
"Dynamic IP Tunnels by Filter Rule Definition Name workspace" on page 108	KN3ITD	New
"Dynamic IP Tunnels by Tunnel ID workspace" on page 110	KN3ITD	New
"Dynamic IP Tunnels with Byte Rate < 2048 workspace" on page 112	KN3ITD	New
"Manual IP Tunnels workspace" on page 131	KN3ITM	New
"Manual IP Tunnels by Tunnel ID workspace" on page 135	KN3ITM	New
"IKE Tunnels Statistics workspace" on page 114	KN3ISS	New
"IKE Tunnels workspace" on page 117	KN3ITI	New
"IKE Tunnels by Security Endpoint Workspace" on page 125	KN3ITI	New
"IKE Tunnels by Tunnel ID Workspace" on page 127	KN3ITI	New
"IKE Tunnels with Byte Rate < 1024 Workspace" on page 129	KN3ITI	New
Applications Connections Workspace	KN3TCN	Updated
Connections Workspace	KN3TCN	Updated
"Updates to the Interfaces and Interfaces History workspaces" on page 138	KN3TIF	Updated
TCP Connections Workspace	KN3TCP	Updated
"TCP/IP Gateways attributes" on page 138	KN3TGA	Updated

New TCP/IP Navigator item workspace

This fix pack introduces a workspace that displays a row of data for each TCP/IP stack, the **"IPSec Status workspace" on page 64**. This workspace displays statistics for IKE and dynamic IP tunnels and for IP filters for all monitored stacks on a z/OS system.

The **"IPSec Status workspace" on page 64** is displayed when you select the **TCP/IP** navigator item.

IPSec Status workspace

The IPSec Status workspace displays IP security configuration and IP security performance statistics for all active TCP/IP stacks on a z/OS image. There is one row of data for each active stack on the monitored system. This workspace provides a high level view of IP security information that may be used to quickly assess the status of IKE and dynamic IP tunnels and the effect of filter rules on IP traffic. There is one row of data for each active stack on the monitored system.

The IPSec Status workspace is displayed when you select the **TCP/IP** navigator item.

Links to Other Workspaces:

Right-click the Link icon in the IPSec Status table to display a list of other workspaces. Left-click the Link icon to select the default link and navigate to its target workspace.

- **Dynamic IP Tunnels Statistics** (default): Displays cumulative availability and performance statistics for the dynamic IP tunnels known to a TCP/IP stack.
- **IKE Tunnels Statistics**: Displays cumulative availability and performance statistics for all of the IKE tunnels known by the IKE daemon for a TCP/IP stack.
- **IP Filters Statistics**: Displays cumulative statistics for the IP filters in use by a TCP/IP stack.

Data Source:

z/OS Communication Server Network Management Interface.

Default Filter:

None.

Figure 4 on page 65 shows the IPSec Status workspace.

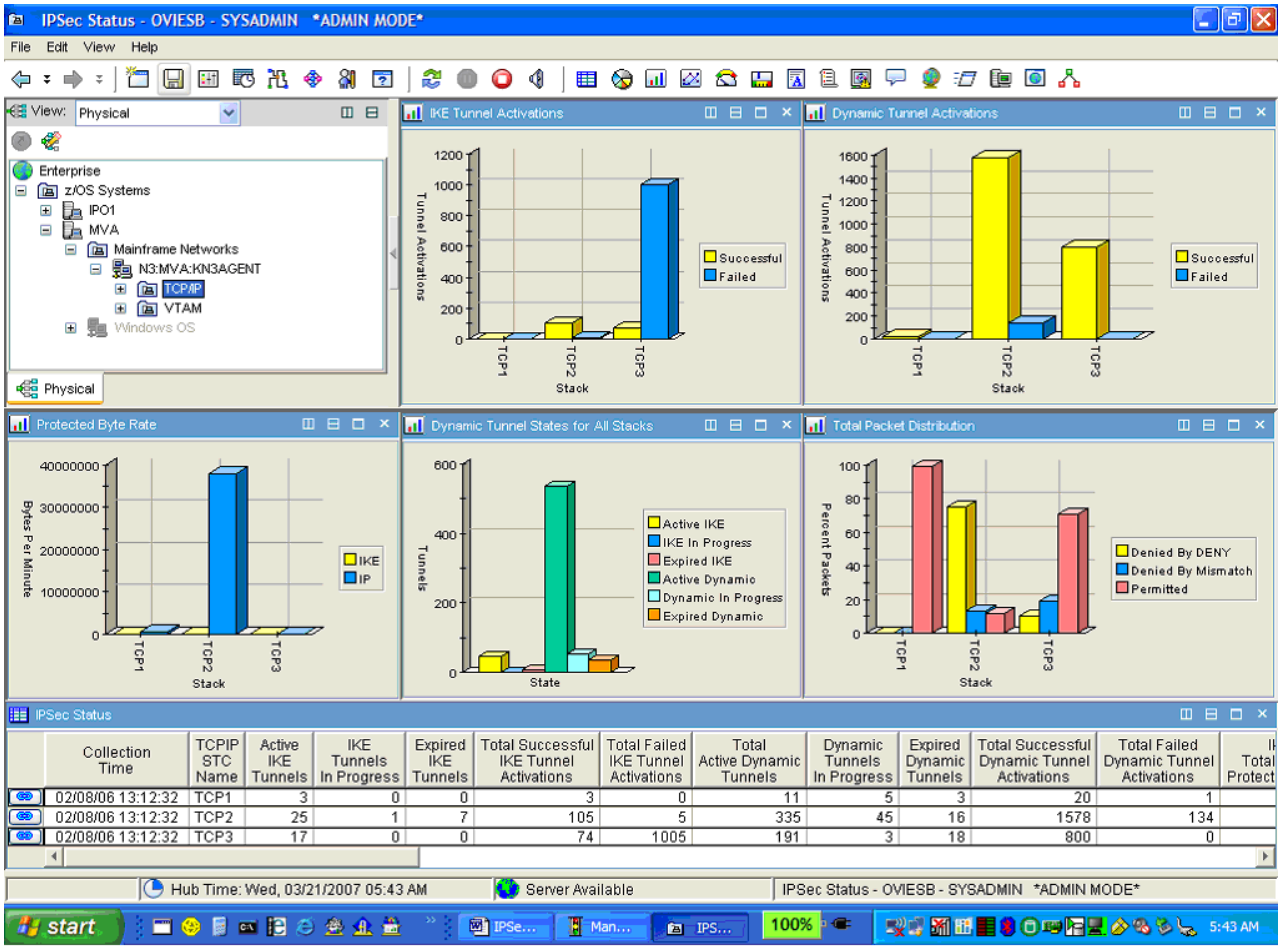


Figure 4. The Tivoli OMEGAMON XE for Mainframe Networks IPSec Status workspace

The IPSec Status workspace displays the following views:

IKE Tunnel Activations

Provides a snapshot of the cumulative number of successful and failed IKE tunnel activations for each TCP/IP stack. This bar chart shows the number of tunnel activations by TCPIP STC name with two bars for each stack as follows:

- Yellow represents successful IKE tunnel activations.
- Blue represents failed IKE tunnel activations.

Dynamic Tunnel Activations

Provides a snapshot of the cumulative number of successful and failed dynamic tunnel activations for each TCP/IP stack. This bar chart shows the number of tunnel activations by TCPIP STC name with two bars for each stack as follows:

- Yellow represents successful dynamic tunnel activations.
- Blue represents failed dynamic tunnel activations.

Protected Byte Rate

Shows the number of bytes per minute being protected by IKE and dynamic IP tunnels for each TCP/IP stack. The bar chart shows the number of bytes per minute by TCP/IP stack name with two bars for each stack as follows:

- Yellow represents IKE tunnels.
- Blue represents IP tunnels.

Dynamic Tunnel States for All Stacks

Provides a snapshot of the cumulative number of tunnels currently in different states across all the known TCP/IP stacks. The bar chart shows the number of tunnels in each of the states as follows:

- Yellow represents current number of active IKE tunnels.
- Blue represents the current number of active dynamic tunnels (including active dynamic SWSA shadow tunnels).
- Pink represents the current number of IKE tunnels in progress (either pending or in negotiation).
- Green represents the current number of dynamic tunnels in progress.
- Turquoise represents the current number of expired IKE tunnels.
- Orange represents the current number of expired dynamic tunnels.

Total Packet Distribution

Shows how packets are being distributed between permit and deny actions by the filters for each of the TCP/IP stacks. The bar charts shows the percentage of packets being permitted or denied (either by deny or mismatch action) by TCP/IP stack name.

- Yellow represents actions denied by deny.
- Blue represents actions denied by mismatch.
- Pink represents permitted actions.

IPSec Status summary table

Displays IP security performance and configuration information for all active TCP/IP stacks for a given z/OS image. Each row represents one of the active stacks running in the z/OS image.

IPSec Status attributes

The following attributes are displayed in the IPSec Status summary table:

Collection Time

The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

TCPIP STC Name

The name of the TCP/IP job. The format is an alphanumeric string no longer than 8 characters.

Active IKE Tunnels
The number of IKE tunnels that are currently active. The format is an integer.

IKE Tunnels in Progress
The number of IKE tunnels that are currently progressing through activation. The state of the tunnel is either pending or in negotiation. The format is an integer where:

- 0 means pending
- 1 means in negotiation

Expired IKE Tunnels
The number of IKE tunnels that are currently expired. The format is an integer.

Total Successful IKE Tunnel Activations
The cumulative number of successful locally initiated Internet Key Exchange (IKE) tunnel activations since the IKE daemon was started. The format is an integer

Total Failed IKE Tunnel Activations
The cumulative number of failed dynamic tunnel activations since the TCP/IP stack was started. The format is an integer.

Total Active Dynamic Tunnels
The total number of currently active dynamic tunnels. This includes active dynamic System-Wide Security Association (SWSA) shadow tunnels and dynamic IP tunnels. The format is an integer.

Dynamic Tunnels In Progress
The number of dynamic tunnels in progress. The state of the tunnel is either PENDING or IN NEGOTIATION. The format is an integer where:

- 0 means PENDING
- 1 means IN NEGOTIATION

Expired Dynamic Tunnels
The number dynamic tunnels that are currently expired. This value includes shadow and non-shadow tunnels. The format is an integer.

Total Successful Dynamic Tunnel Activations
The cumulative number of successful dynamic tunnel activations since the TCP/IP stack was started. The format is an integer.

Total Failed Dynamic Tunnel Activations
The cumulative of failed dynamic tunnel activations since the TCP/IP stack was started. The format is an integer

IKE Total Bytes Protected (in G)
The cumulative number of inbound and outbound bytes of Internet Key Exchange (IKE) traffic protected by IKE tunnels since the IKE daemon was started, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the IKE Total Bytes Protected column to calculate the cumulative total bytes of IKE traffic protected by IKE tunnels. The format is an integer.

IKE Total Bytes Protected
The cumulative number of inbound and outbound bytes of Internet Key Exchange (IKE) traffic protected by IKE tunnels since the IKE daemon was started. The value in this column can be added to the product of 1,073,741,824 and the value in the IKE Total Bytes Protected (in G) column to calculate the cumulative total bytes of IKE traffic protected by IKE tunnels. The format is an integer.

IKE Bytes Protected
The number of bytes protected by Internet Key Exchange (IKE) tunnels in the last interval. The format is an integer.

IKE Protected Byte Rate
The number of bytes flowing through Internet Key Exchange (IKE) tunnels every minute. The format is an integer.

IP Total Bytes Protected (in G)
The cumulative number of inbound and outbound bytes of IP traffic protected by dynamic tunnels since the TCP/IP stack was started, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the IP Total Bytes Protected column to calculate the cumulative total bytes of IP traffic protected by dynamic tunnels. The format is an integer.

IP Total Bytes Protected
The cumulative number of inbound and outbound bytes of IP traffic protected by dynamic tunnels since the TCP/IP stack was started. The value in this column can be added to the product of 1,073,741,824 and the value in the IP Total Bytes Protected (in G) column to calculate the cumulative total bytes of IP traffic protected by dynamic tunnels. The format is an integer.

IP Bytes Protected
The number of bytes of IP traffic protected by dynamic IP tunnels in the last interval. The format is an integer.

IP Protected Byte Rate
The number of bytes of IP traffic flowing through dynamic IP tunnels every minute. The format is an integer

Total Packets Denied by DENY (in G)
The total number of packets denied by a DENY action on any filter since the TCP/IP stack was started, divided by 1,073,741,824. If the value in this column is not 0, then it can be multiplied by 1,073,741,824 and added to the value in the Total Packets Denied by DENY column to calculate the packets denied by DENY for any filter. The format is an integer.

Total Packets Denied by DENY
The total number of packets denied by a DENY action on any filter since the TCP/IP stack was started. If the value in the Total Packets Denied By DENY (in G) column is not 0, then the value in this column can be added to the product of 1,073,741,824 and the value in the Total Packets Denied by DENY (in G) column to calculate the packets denied by DENY for any filter. The format is an integer.

Percent Total Packets Denied by DENY
The percentage of total packets denied by a DENY action on any filter. The format is a number between 0 and 100 inclusive. The format is an integer.

Total Packets Denied by Mismatch (in G)
The total number of packets denied due to a mismatch with any filter action, divided by 1,073,741,824. If the value in this column is not 0, then it can be multiplied by 1,073,741,823 and added to the value in the Total Packets Denied by Action Mismatch column to calculate the packets denied by an action mismatch. The format is an integer.

Total Packets Denied by Mismatch
The total number of packets denied due to a mismatch with any filter action. If the value in the Total Packets Denied By Action Mismatch (in G) column is not 0, then the value in this column can be added to the product of 1,073,741,823 and the value in the Packets Denied by Action Mismatch (in G) column to calculate the packets permitted. The format is an integer.

Percent Total Packets Denied by Mismatch
The percentage of total packets denied by a DENY action on any filter since the TCP/IP stack was started. The format is a number between 0 and 100 inclusive.

Total Packets Permitted (in G)
The total number of packets that were permitted by any filter, divided by 1,073,741,824. If the

value in this column is not 0, then it can be multiplied by 1,073,741,824 and added to the value in the Total Packets Permitted column to calculate the packets permitted. The format is an integer.

Total Packets Permitted
The total number of packets that were permitted by any filter since the TCP/IP stack was started. If the value in the Total Packets Permitted (in G) column is not 0, then the value in this column can be added to the product of 1,073,741,824 and the value in Total Packets Permitted (in G) column to calculate the packets permitted. The format is an integer.

Percent Total Packets Permitted
The percentage of total packets that were permitted by any filter. The format is a number between 0 and 100 inclusive.

Total Packets Matched (in G)
The total number of packets that matched both the condition and action for any filter since the TCP/IP stack was started, divided by 1,073,741,824. If the value in this column is not 0, then it can be multiplied by 1,073,741,824 and added to the value in the Total Packets Matched column to calculate the total packets matched. The format is an integer.

Total Packets Matched
The total number of packets that matched both the condition and action for any filter since the TCP/IP stack was started. If the value in the Total Packets Matched (in G) column is not 0, then the value in this column can be added to the product of 1,073,741,824 and the value in Total Packets Matched (in G) column to calculate the total packets matched. The format is an integer.

Total Packets Filtered (in G)
The total number of packets processed by the filter rule set since the TCP/IP stack was started, divided by 1,073,741,824. If the value in this column is not 0, then it can be multiplied by 1,073,741,824 and added to the value in the Total Packets Filtered column to calculate the total packets processed. The format is an integer.

Total Packets Filtered
The total number of packets processed by the filter rule set since the TCP/IP stack was started. If the value in the Total Packets Filtered (in G) column is not 0, then the value in this column can be added to the product of 1,073,741,824 and the value in the Total Packets Filtered (in G) column to calculate the total packets processed. The format is an integer.

IP Security
Indicates whether or not IP security functions are enabled for IPv4 interfaces. IP security was enabled by coding IPCONFIG IPSECURITY in the TCP/IP profile. For more information about the IPSEC statement, refer to the most recent edition of the z/OS Communication Server *IP Configuration Guide* or *IP Configuration Reference*. This value is stored as an integer and displayed as a string. Valid values are:

- 0=Disabled
- 1=Enabled

IPv6 Security
Indicates whether or not IP security functions are enabled for IPv6 interfaces. IPv6 security is enabled by coding IPCONFIG IPSECURITY and IPCONFIG6 IPSECURITY in the TCP/IP profile. For more information about the IPSEC statement, refer to the most recent edition of the z/OS Communication Server *IP Configuration Guide* or *IP Configuration Reference*. This value is stored as an integer and displayed as a string. Valid values are:

- 0=Disabled
- 1=Enabled

Sysplex-Wide Security Associations (SWSA)
Indicates whether or not sysplex-wide security associations (SWSA) are enabled. SWSA was enabled by coding the DVIPSEC parameter on the IPSEC statement in the TCP/IP profile. For more information about the IPSEC statement, refer to the most recent edition of the z/OS

Communication Server *IP Configuration Guide* or *IP Configuration Reference*. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Disabled
- 1 = Enabled

Filter Logging

Indicates whether or not filter logging is enabled for the TCP/IP stack. Filter logging was enabled by coding the LOGENABLE parameter of the IPSEC statement in the TCP/IP profile. For more information about the IPSEC statement, refer to the most recent edition of the z/OS Communication Server *IP Configuration Guide* or *IP Configuration Reference*. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Disabled
- 1 = Enabled

Pre-Decapsulation Filtering

Indicates whether or not pre-decapsulation filtering is enabled. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Disabled
- 1 = Enabled

Filter Set In Use

Identifies which filter set is currently in use by the TCP/IP stack. One of two filter sets may be in use at any time:

- The default filter set that is made up of filters defined in the TCP/IP profile.
- The policy filter set that is made up of filters defined in Policy Agent configuration files.

This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Default
- 1 = Policy

Number of Configured Filter

The number of configured IP Filters for this stack. The format is an integer.

NAT Keep Alive Interval

The NAT keep-alive interval, in seconds. The interval is used to regulate the sending of NAT keep-alive messages for a NAT traversal tunnel when a NAT is detected in front of the local host. The format is an integer expressed in seconds.

New TCP/IP Workspaces

IP Filters Statistics workspace

The IP Filters Statistics workspace displays cumulative statistics for the IP filters in use by a TCP/IP stack.

To display the IP Filters Statistics workspace, click the **IP Filters** Navigator item.

Additional Workspaces:

Right-click the TCP/IP Navigator item to display the following additional workspaces:

- **IP Filters Statistics** (Default): Displays cumulative statistics for the IP filters in use by a TCP/IP stack.
- **Current IP Filters**: Displays the currently active IP filters in use by a monitored TCP/IP stack on a z/OS system image.

Links To Other Workspaces:

Right-click the Link icon in the **IP Filters Statistics** summary table to display the following additional workspaces. Left-click the Link icon to select the default link and navigate to its target workspace.

- **Current IP Filters**: Displays the currently active IP filters in use by a monitored TCP/IP stack on a z/OS system image.

Data Source:

z/OS Communication Server Network Management Interface

Default Filter:

None.

Figure 5 shows the IP Filters Statistics workspace.

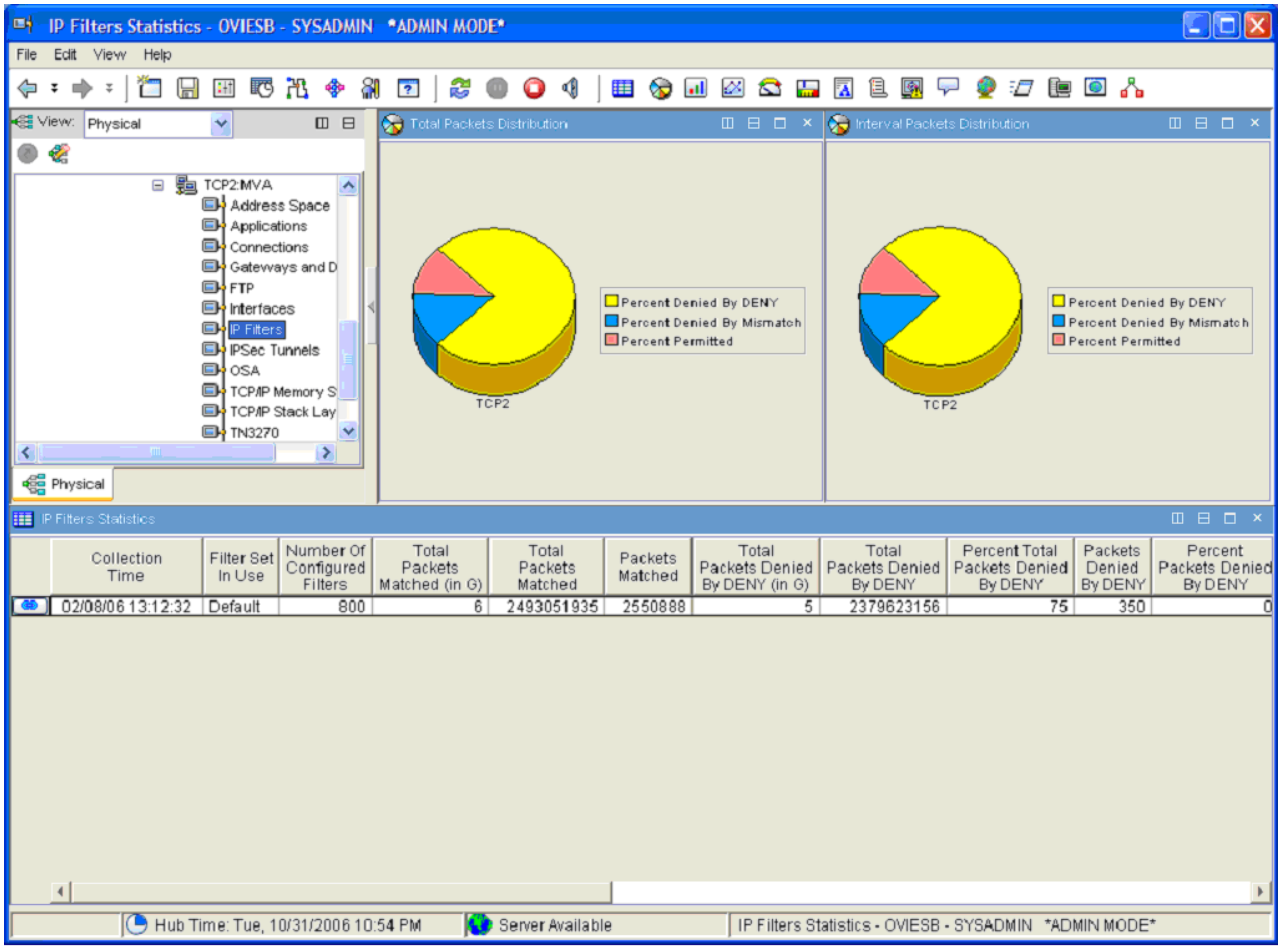


Figure 5. The Tivoli OMEGAMON XE for Mainframe Networks IP Filters Statistics workspace

The IP Filters Statistics workspace displays the following views:

Total Packets Distribution

Shows how all the packets filtered by the stack are distributed between deny and permit actions. This pie chart includes the following data:

- Yellow represents the percentage of packets denied by a DENY action.
- Blue represents the percentage of packets denied by a MISMATCH action.
- Pink represents the percentage of packets permitted.

Interval Packets Distribution

Shows how the packets filtered during the most recent interval are distributed between deny and permit actions. This pie chart includes the following data:

- Yellow represents the percentage of packets during the most recent interval denied by a DENY action.
- Blue represents the percentage of packets during the most recent interval denied by a MISMATCH action.
- Pink represents the percentage of packets permitted during the most recent interval.

IP Filters Statistics summary table
Provides cumulative statistics aggregated across all the filter rules known to the TCP/IP stack.

IP Filter Statistics attributes

The following attributes are displayed in the IP Filters Statistics summary table:

Collection Time
The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Filter Set In Use
Identifies which filter set is currently in use by the TCP/IP stack. One of two filter sets may be in use at any time:

- The default filter set, which is made up of filters defined in the TCP/IP profile.
- The policy filter set, which is made up of filters defined in Policy Agent configuration files.

This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Default
- 1 = Policy

Number of Configured Filters
The number of configured IP Filters for this stack. The format is an integer.

Total Packets Matched (in G)
The total number of packets that matched both the condition and action for any filter since the TCP/IP stack was started, divided by 1,073,741,824. If the value in this column is not 0, then it can be multiplied by 1,073,741,824 and added to the value in the Total Packets Matched column to calculate the total packets matched. The format is an integer.

Total Packets Matched
The total number of packets that matched both the condition and action for any filter since the TCP/IP stack was started. If the value in the Total Packets Matched (in G) column is not 0, then the value in this column can be added to the product of 1,073,741,824 and the value in Total Packets Matched (in G) column to calculate the total packets matched. The format is an integer.

Packets Matched
The number of packets that matched the condition and action for any filter during the most recent interval. The format is an integer.

Total Packets Denied By DENY (in G)
The total number of packets denied by a DENY action on any filter since the TCP/IP stack was started, divided by 1,073,741,824. If the value in this column is not 0, then it can be multiplied by 1,073,741,824 and added to the value in the Total Packets Denied by DENY column to calculate the packets denied by DENY for any filter. The format is an integer.

Total Packets Denied by DENY
The total number of packets denied by a DENY action on any filter since the TCP/IP stack was started. If the value in the Total Packets Denied By DENY (in G) column is not 0, then the value in this column can be added to the product of 1,073,741,824 and the value in the Total Packets Denied by DENY (in G) column to calculate the packets denied by DENY for any filter. The format is an integer.

Percent Total Packets Denied By DENY
The percentage of total packets denied by a DENY action on any filter. The format is a number between 0 and 100 inclusive.

Packets Denied By DENY
The number of packets denied by a DENY action on any filter during the most recent collection interval. The format is an integer.

Percent Packets Denied By DENY
The percentage of packets denied by a DENY action on any filter during the most recent interval. The format is a number between 0 and 100 inclusive.

Total Packets Denied By Mismatch (in G)
The total number of packets denied due to a mismatch with any filter action since the TCP/IP stack was started, divided by 1,073,741,824. If the value in this column is not 0, then it can be multiplied by 1,073,741,824 and added to the value in the Total Packets Denied by Action Mismatch column to calculate the packets denied by an action mismatch. The format is an integer.

Total Packets Denied By Mismatch
The total number of packets denied due to a mismatch with any filter action since the TCP/IP stack was started. If the value in the Total Packets Denied By Action Mismatch (in G) column is not 0, then the value in this column can be added to the product of 1,073,741,824 and the value in the Packets Denied by Action Mismatch (in G) column to calculate the packets permitted. The format is an integer.

Percent Total Packets Denied By Mismatch
The percentage of total packets denied due to a mismatch with any filter action. The format is a number between 0 and 100 inclusive.

Packets Denied By Mismatch
The number of packets denied by a mismatched action on any filter during the most recent interval. The format is an integer.

Percent Packets Denied By Mismatch
The percentage of total packets denied due to a mismatch with any filter action. The format is a number between 0 and 100 inclusive.

Total Packets Permitted (in G)
The total number of packets that were permitted by any filter, divided by 1,073,741,824. If the

value in this column is not 0, then it can be multiplied by 1,073,741,824 and added to the value in the Total Packets Permitted column to calculate the packets permitted. The format is an integer.

Total Packets Permitted
The total number of packets that were permitted by any filter since the TCP/IP stack was started. If the value in the Total Packets Permitted (in G) column is not 0, then the value in this column can be added to the product of 1,073,741,824 and the value in Total Packets Permitted (in G) column to calculate the packets permitted. The format is an integer.

Percent Total Packets Permitted
The percentage of total packets that were permitted by any filter since the TCP/IP stack was started. The format is a number between 0 and 100 inclusive.

Packets Permitted
The number of packets permitted by any filter during the most recent interval. The format is an integer.

Percent Packets Permitted
The percentage of packets permitted by any filter during the most recent interval. The format is a number between 0 and 100 inclusive.

Total Packets Filtered (in G)
The total number of packets processed by the filter rule set since the TCP/IP stack was started, divided by 1,073,741,824. If the value in this column is not 0, then it can be multiplied by 1,073,741,824 and added to the value in the Total Packets Filtered column to calculate the total packets processed. The format is an integer.

Total Packets Filtered
The total number of packets processed by the filter rule set since the TCP/IP stack was started. If the value in the Total Packets Filtered (in G) column is not 0, then the value in this column can be added to the product of 1,073,741,824 and the value in the Total Packets Filtered (in G) column to calculate the total packets processed. The format is an integer.

Packets Filtered
The number of packets filtered by the filter rule set during the most recent collection interval. The format is an integer.

Current IP Filters workspace

The Current IP Filters Workspace displays the currently active IP filters for a TCP/IP stack.

To display the Current IP Filters workspace, right-click the **IP Filters** navigator item for a specific TCP/IP stack, select **Workspaces** and select the **Current IP Filters** workspace.

Links to Other Workspaces:
Right-click the Link icon in the Current IP Filters in Scan Order table to display a list of links to other workspaces. Left-click the Link icon to select the default link and navigate to the link's target workspace.

- **Dynamic IP Tunnels By Filter Rule Definition Name (Default)**. This link navigates to the Dynamic IP Tunnels workspace and shows tunnels that have a filter rule definition name that matches the name of the selected filter.
- **Dynamic IP Tunnels By Tunnel ID**: This is a conditional link and is only displayed in the list of available links if the filter type is DYNAMIC (4) or NATTDYN (6) or NRF (7). This link navigates to the Dynamic IP Tunnels workspace and shows tunnels that have a tunnel ID that matches the tunnel ID associated with the selected filter.
- **Manual IP Tunnels by Tunnel ID**: This is a conditional link and is only displayed in the list of available links if the filter type is MANUAL (2). This link navigates to the Manual IP Tunnels workspace and shows tunnels that have a tunnel ID that matches the tunnel ID associated with the selected filter.

- **Current IP Filters In Scan Order By Previous Page:** This is a conditional link and will only be displayed in the list of available links if the page number for the selected link is greater than 0. This link navigates to the Current® IP Filters In Scan Order workspace and shows the IP filters that have a page number that is 1 less than the page number for the selected filter.
- **Current IP Filters In Scan Order By Next Page:** This is a conditional link and will only be displayed in the list of available links if the page number for the selected link is less than the value in the Last Page column of the selected row. This link navigates to the Current IP Filters In Scan Order workspace and shows the IP filters that have a page number that is 1 more than the page number for the selected filter.
- **Current IP Filters by Destination Address**: This link causes a dialog box to be displayed that prompts you for a destination IP address that is compared to the currently active filters for a TCP/IP stack. This field is filled in by default with the value from the **Destination Address** column for the selected filter, but you can change this value to be any IPv4 or IPv6 address. If the Destination Address column is blank, the field will display IP address that matches all addresses. With this address as input, this link navigates to the Current IP Filters By Destination Address Workspace showing the IP filters that match the destination IP address that you provided.

Data Source:

z/OS Communication Server Network Management Interface

Default Filter:

There can be tens of thousands of IP Filters. The query filter implemented for this workspace retrieves up to 500 IP Filters at a time.

The Tivoli Enterprise Portal displays 100 rows of IPSec Filters at a time. Use the Tivoli Enterprise Portal scrolling controls or change the page number at the top right of the table view to see the remaining IP Filters from the current set of up to 500 IP Filters.

If more than 500 IP Filters exist, a link named **Current IP Filters In Scan Order By Next Page** will be provided in the right-click menu of the link icons for each row in the Current IP Filters in Scan Order table view. Use this link to display each successive group of 500 IP Filters. When no more IP Filters are available for display, the link will not appear in the right click menu. If you have already used the **Current IP Filters In Scan Order By Next Page** link to display additional IP Filters, another link named **Current IP Filters In Scan Order By Previous Page** can be used to return to the previous set of 500 IP Filters.

Figure 6 on page 76 shows the Current IP Filters workspace.

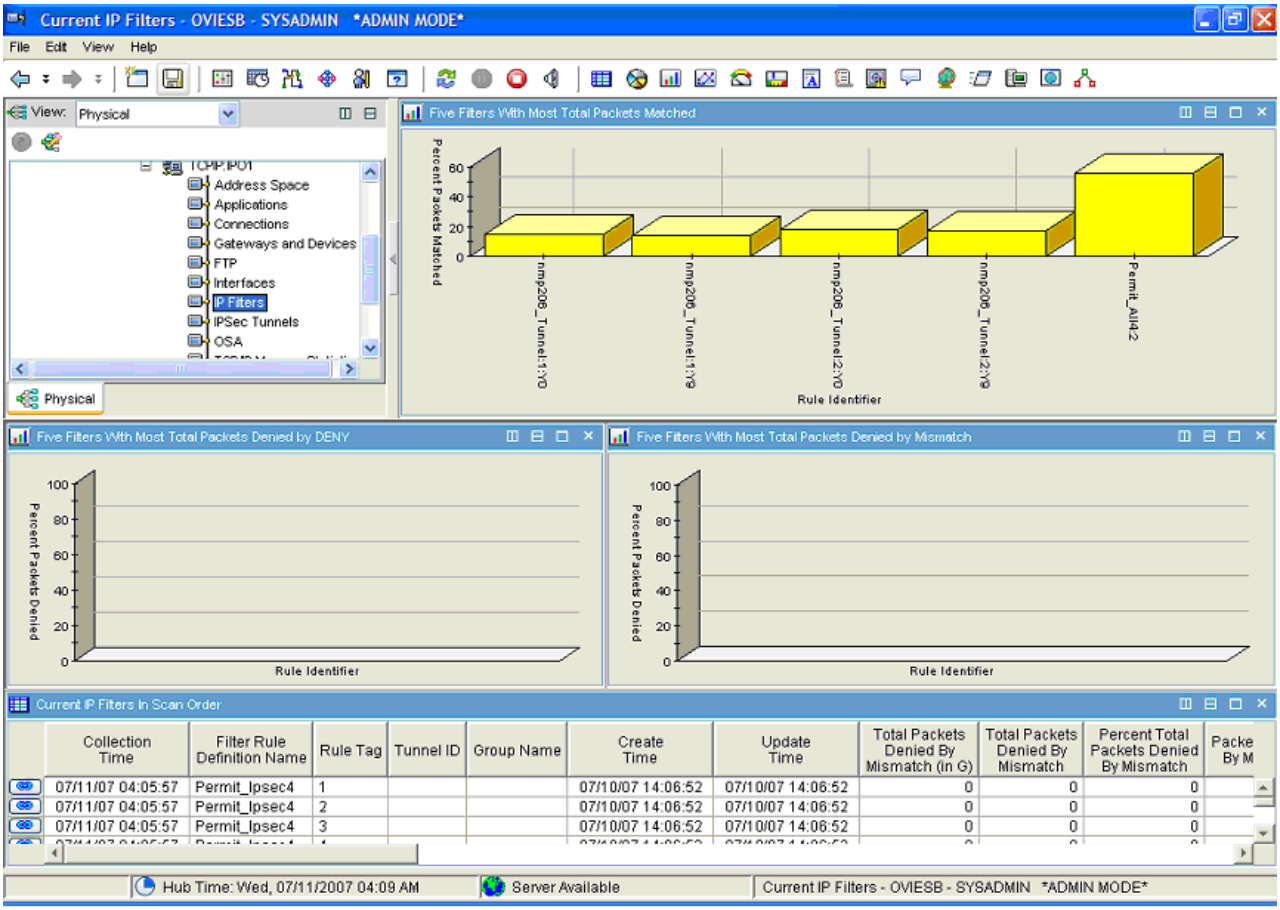


Figure 6. The Tivoli OMEGAMON XE for Mainframe Networks Current IP Filters workspace

The Current IP Filters workspace displays the following views:

Five Filters With Most Total Packets Matched
Displays the five filters that have the highest number of total packets that matched the filter's condition and action in the Current IP Filters table.

Five Filters With Most Total Packets Denied By DENY
Displays the five filters that have the highest number of total packets that matched the filter's condition and for which the action was DENY.

Five Filters With Most Total Packets Denied By Mismatch
Displays the five filters that have the highest number of total packets that matched the filter's condition but did not match the filter's action (for example, if a packet was sent "in the clear" but the action was coded as IPSec). This view can provide an indication of a configuration problem such as packets flowing in the clear when they should be encrypted.

Current IP Filters in Scan Order summary table
This summary table provides performance and configuration data about the currently active IP filters.

Each row in the table represents a single IP filter. The filters are displayed in the order that they would be scanned by the TCP/IP stack when it compares them to packets. The first 500 filters are displayed. Additional filters may be displayed by using the **Current IP Filters In Scan Order By Next Page** link defined for each row.

The rows in the Current IP Filters table have a page column and a last page column associated with them. The page column is initialized by the agent so that rows may be retrieved 500 row at a

time. The last “page” may have fewer than 500 rows. When you navigate to this workspace, the default filter displays the first page of rows or the first 500 filters. The filters are ordered in the table view in the order that the TCP/IP stack scans them to compare them to packets.

Current IP Filters attributes: The following attributes are displayed in the Current IP Filters in Scan Order summary table:

Collection Time

The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Filter Set

Identifies which filter set is currently in use by the TCP/IP stack. One of two filter sets may be in use at any time.

- The default filter set, which is made up of filters defined in the TCP/IP profile.
- The policy filter set, which is made up of filters defined in the Policy Agent configuration files.

This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Default
- 1 = Policy

Filter Rule Definition Name

The name specified for an IP filter rule definition. This column is stored as a 48-character string.

Rule Tag

The filter rule definition name extension. The extension is assigned by the stack to identify related rules derived from the same definition. The column is stored as an 8-character string. This field is not displayed.

Tunnel ID

Identifier for the associated tunnel. The tunnel ID is generated by the TCP/IP stack. This ID is not unique; several related tunnels may have the same tunnel ID. The related tunnels are different instances of the same security association. Usually the related instances exist due to the expiration and refresh of tunnels. This field is blank if the filter is not associated with a tunnel. The ID is a character string of up to 48 characters.

Group Name

The name of the filter group that the filter rule is associated with. This field is blank if the filter rule is not associated with a filter group. The format is an alphanumeric string of up to 48 characters.

Create Time

The time when the filter was created, based on how the filter was created.

- For a statically defined filter originating from the Policy Agent configuration, this field represents the time that the filter was first defined to the current instance of the Policy Agent. Filters of this type have the value of **1** meaning Policy for the Filter Set attribute.
- For a filter originating from the TCP/IP profile, this field represents the time that the profile filter configuration was last replaced. Filters of this type have the value of **0** meaning Default for the Filter Set attribute.
- For dynamically defined filters, this field is blank. Dynamically defined filters have a value of **DYNAMIC**, **NATTDYN**, or **NRF**.

This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Update Time

The time when the filter was updated, based on how the filter was created.

- For a statically defined filter originating from the Policy Agent configuration, this field represents the time that the filter's attributes were last updated in the current instance of the Policy Agent. Filters of this type have the value of **1** meaning Policy for the Filter Set attribute.
- For a filter originating from the TCP/IP profile, this field represents the time that the profile filter configuration was last replaced. Filters of this type have the value of **0** meaning Default for the Filter Set attribute.
- For dynamically defined filters, this field is blank. Dynamically defined filters have a filter type of **DYNAMIC**, **NATTDYN**, or **NRF**.

This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Total Packets Denied By Mismatch (in G)
The total number of packets denied due to a mismatch with this filter's action since the start of the TCP/IP stack, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Packets Denied By Action Mismatch column to calculate the cumulative number of packets denied by action mismatch. The format is an integer.

Total Packets Denied By Mismatch
The total number of packets denied due to a mismatch with this filter's action since the start of the TCP/IP stack. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Packets Denied by Action Mismatch (in G) column to calculate the cumulative number of packets denied by action mismatch. The format is an integer.

Percent Total Packets Denied By Mismatch
The percentage of total packets denied due to an action mismatch by this filter compared to the total packets denied due to an action mismatch by all filters on the TCP/IP stack since the stack was started. The format is a number between 0 and 100 inclusive.

Packets Denied By Mismatch
The number of packets denied due to a mismatch with this filter's action during the most recent collection interval. The format is an integer.

Total Packets Matched (in G)
The total number of packets denied due to a mismatch with this filter's action since the start of the TCP/IP stack, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Packets Denied By Action Mismatch column to calculate the cumulative number of packets denied by action mismatch. The format is an integer.

Total Packets Matched
The total number of packets that matched this filter's condition and action since the start of the TCP/IP stack. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Packets Matched (in G) column to calculate the cumulative number of packets matched. The format is an integer.

Percent Total Packets Matched
The percentage of total packets matched by this filter compared to the total packets matched by all filters on the stack. The format is a number between 0 and 100 inclusive.

Packets Matched
The total number of packets that matched this filter's condition and action during the most recent collection interval. The format is an integer.

Filter Set
Identifies which filter set is currently in use by the TCP/IP stack. One of two filter sets may be in use at any time.

- The default filter set, which is made up of filters defined in the TCP/IP profile.
- The policy filter set, which is made up of filters defined in the Policy Agent configuration files.

This value is stored as an integer and displayed as a string. Valid values are:

- 0 = Default
- 1 = Policy

Local Start Action Name
The name specified for an `IpLocalStartAction` statement that is referenced by this filter. The `IpLocalStartAction` statement specifies how to determine the local IP, remote IP, local port, remote port, and protocol specification for the local activation of a dynamic virtual private network (VPN). This field is blank if no local start action name is associated with this filter. This field is stored as a 48-character string.

VPN Action Name
The name specified on a virtual private network (VPN) action definition statement. The VPN action describes how to protect the traffic that flows on the tunnel. It specifies attributes of the tunnel, such as what type of encryption to use. The name is a character string of up to 48 characters.

Type Indicates the filter type. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = GENERIC
- 2 = MANUAL
- 3 = DYNANCHOR
- 4 = DYNAMIC
- 5 = NATTANCHOR
- 6 = NATTDYN
- 7 = NRF

State Current filter state. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = ACTIVE
- 1 = INACTIVE

Action
The action to be applied to the packet when filter's condition is met. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = PERMIT
- 2 = DENY
- 3 = IPSEC

Scope The type of traffic that this filter applies to. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = LOCAL
- 2 = ROUTED
- 3 = SCOPEALL.

Direction
Indicates the direction of the IP traffic. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = INBOUND
- 2 = OUTBOUND

Security Class
The IP filter security class. This filter is applied to all packets traversing the IP interfaces, and these interfaces are associated with security classes. This value is expressed as an integer between 0 and 255 inclusive. A value of zero (0) means that all security classes are filtered. If a non-zero value is specified for the security class, then the filter applies to data traversing all interfaces associated with the specified security class.

Protocol Number
IP protocol number to match in the IPv4 or IPv6 header of packets. If the filter applies to all IP protocols, this field is stored as blanks. This value is expressed as a string of up to 3 characters. 0 is a valid IP protocol number.

ICMP Type Code
The Internet Control Message Protocol (ICMP) code that identifies the ICMP traffic to be filtered. This field is blanks if the filter applies to all ICMP types. This field is defined as an integer of up to 2 characters. 0 is a defined ICMP Type Code.

ICMP Code
The Internet Control Message Protocol (ICMP) code that qualifies the ICMP Type Code attribute. This field is blank if the filter applies to all ICMP codes. This field is defined as an integer of up to 2 characters. 0 is a defined ICMP code. The value in this field is not meaningful unless a non-blank value appears in the ICMP Type Code field.

OSPF Type
Identifies Open Shortest Path First (OSPF) protocol traffic to be filtered. This field is blank if the filter applies to all OSPF traffic. The format is an integer.

On Demand Indicator
Indicates whether or not on-demand activations are allowed for the traffic described for this filter. On demand activations are activations of tunnels initiated automatically when traffic requiring the use of the tunnel is sent. This field is meaningful if the filter type is one of the following:

- Dynamic anchor filter
- Dynamic filter
- Network Address Translation (NAT) Traversal anchor filter
- NAT Traversal dynamic filter

This value is stored as an integer and displayed as a string. The field contains a zero (0) when the filter type is not one of these. Valid values are:

- 0 = <blank>
- 1 = NOT_PERMITTED
- 2 = PERMITTED

TCP Connect
Indicates what types of TCP connect attempts are to be filtered. TCP connect attempts (SYN packets) in the direction opposite that specified in this field do not match this filter. This field is meaningful for generic or anchor filters only. It is zero (0) when the filter is not one of these types. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = NONE
- 1 = INBOUND
- 2 = OUTBOUND

SWSA Shadow Indicator
Indicates whether or not the filter originated from a distributing stack (SHADOW) or the local stack

(NOT_SHADOW). This value is only meaningful for dynamic filters. If the filter type is not dynamic, the value is set to 0 and a blank is displayed. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = NOT_SHADOW
- 2 = SHADOW

A value of SHADOW indicates that the filter originated from a distributing stack. This indicator is significant if filter type is dynamic. If the filter type is not dynamic, a value of zero (0) is stored and blanks are displayed in the field.

Source Address

Source IP address or addresses that the filter applies to. Filters apply to either IPv4 addresses or IPv6 address, but not both. If the filter applies to all source IP addresses, the field is displayed as blank; a value of “0” padded to the right with blanks is stored in the table for this case. If the filter is for a range of source IP addresses, this field displays the lower address in the range. This value is represented as a 45-character string.

Note: For comparison, leading zeros are added for unspecified digits in IPv4 and IPv6 addresses when they are stored.

Upper Source Address

If the filter is for a range of source IP addresses, this is the high value for the range. This field will be displayed as blank if the source address is not a range or the filter applies to all source IP addresses; a value of “0” padded to the right with blanks will be stored in the table for this case. The format is a string of up to 45 characters.

Note: For comparison, leading zeros are added for unspecified digits in IPv4 and IPv6 addresses when they are stored.

Lower Source Port

If the filter is for a range of IP ports, this is the low value for the range. This field is blank if the filter is not for a range of IP port addresses and applies to all ports. This value is represented as a 5-character string.

Upper Source Port

If the filter is for a range of source IP port addresses, this is the high value for the range. This field is blank if filter is not for a range of IP port addresses and applies to all ports. This value is represented as a 5-character string.

Destination Address

Destination IP address or addresses affected by the current filter. This address may be in IPv4 or IPv6 format. Filters apply to either IPv4 addresses or IPv6 addresses, but not both. If the filter applies to all destination IP addresses, the field will be displayed as blank; a value of “0” padded to the right with blanks will be stored in the table. If the filter is for a range of destination IP addresses, this is the lower address in the range. This value is represented as a 45-character string.

Note: For comparison, leading zeros are added for unspecified digits in IPv4 and IPv6 addresses when they are stored.

Upper Destination Address

If filter is for a range of destination IP addresses, this is the high value for the range. This field will be displayed as blank if destination is not a range of addresses or the filter is for all destination addresses; a value of “0” padded to the right with blanks is stored in the table.This is represented as a 45 character string.

Note: For comparison, leading zeros are added for unspecified digits in IPv4 and IPv6 addresses when they are stored.

Lower Destination Port
If the filter is for a range of destination IP port addresses, this is the low value for the range. This field is blank if the filter is not for a range of IP port addresses and applies to all ports. This value is represented as a 5-character string.

Upper Destination Port
If the filter is for a range of destination IP port addresses, this is the high value for the range. This field is blank if the filter is not for a range of IP port addresses and applies to all ports. This value is represented as a 5-character string.

NATT Client ID Type
If the peer is behind a NAT and a gateway and the peer supplied a client ID, indicates what type of client ID was supplied. Otherwise, this field is stored as blanks. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = NONE
- 1 = IPv4_ADDR
- 2 = IPv4_ADDR_RANGE
- 3 = IPv4_ADDR_RANGE
- 4 = OTHER

NATT Client ID
If the peer is behind a NAT and a gateway and the peer supplied a client ID, indicates the NAT traversal gateway (NATT) client ID. This field contains an IPv4 dotted decimal address if the NATT Client ID Type is IPv4_ADDR. This field contains an IPv4 dotted decimal address if the NATT Client ID Type is IPv4_ADDR_RANGE. The address in the field is the lower address for the range. This field have an MD5 hash of the client ID if the NATT Client ID Type is OTHER. If the NATT Client ID Type is 0, this field is stored as blanks. The format is a string of up to 32 characters.

Upper NATT Client ID
If the peer is behind a NAT and a gateway and the peer supplied a client ID, indicates the upper address range of the NAT traversal gateway (NATT) client ID. This field contains an IPv4 dotted decimal address if the NATT Client ID Type is IPv4_ADDR_RANGE. If the NATT Client ID Type is 0, 1, or 4, this field is stored as blanks. This field is a character string of up to 15 characters.

NATT Peer UDP Port
If this is a dynamic filter for UDP-encapsulated NAT Traversal (NATT) traffic, this is the UDP port for the IKE peer. Otherwise, this field is stored as blanks. This field is represented as a character string of up to 5 characters.

NRF Original Port
If this is a NAT Traversal Resolution Filter (NRF), this field contains the original remote port for the TCP or UDP traffic. Otherwise this field is stored as blanks. This field is represented as a character string of up to 5 characters.

NAT Indicator
Indicates whether network address translation (NAT) has been detected in front of the IPSEC peer. This field is significant for filters with a type of dynamic. If the filter is not dynamic, this field is stored as blanks. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

NAPT Indicator
NAPT Indicator Indicates whether a network address port translation (NAPT) has been detected in front of the IPSec peer. This field is significant for filters with a type of dynamic. If the filter is not dynamic, this field is stored as blanks. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

NAT Traversal Gateway

Indicates that the peer is acting as an IPSec gateway and the tunnel uses UDP encapsulation. This field is significant for dynamic filters. If the filter is not dynamic, this field is stored as blanks. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Log Indicator

Indicates which packets to log. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = NONE: Do not log any packets.
- 1 = PERMIT: Log packets permitted by the filter.
- 2 = DENY: Log packets denied by the filter.
- 3 = ALL: Log all packets that match this filter.

Source Address Granularity

Indicates the origin of the source address used for on-demand activations of tunnels associated with a dynamic anchor filter. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>: This is not a dynamic anchor filter.
- 1 = FILTER: The source address for the tunnel is from filter definition.
- 2 = PACKET: The source address for the tunnel is from the packet requiring the tunnel activation.

Destination Address Granularity

Indicates the origin of the destination address used for on-demand activations of tunnels associated with a dynamic anchor filter. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>: This is not a dynamic anchor filter.
- 1 = FILTER: Destination address for the tunnel is from the filter definition.
- 2 = PACKET: Destination address for the tunnel is from the packet requiring the tunnel activation.

Protocol Granularity

Indicates the origin of the protocol used for on-demand activations of tunnels associated with a dynamic anchor filter. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>: This is not a dynamic anchor filter
- 1 = FILTER: The protocol for the tunnel is from the filter definition.
- 2 = PACKET: The protocol for the tunnel is from the packet requiring the tunnel activation.

Source Port Granularity

Indicates the origin of the source port used for on-demand activations of tunnels associated with a dynamic anchor filter. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>: This is not a dynamic anchor filter
- 1 = FILTER: The source port for tunnel is from the filter definition.
- 2 = PACKET: The source port for tunnel is from the packet requiring the tunnel activation

Destination Port Granularity

Indicates the origin of the destination port used for on-demand activations of tunnels associated with a dynamic anchor filter. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>: This is not a dynamic anchor filter

- 1 = FILTER: The destination address for the tunnel is from the filter definition.
- 2 = PACKET: The destination address for the tunnel is from the packet requiring the tunnel activation.

A value of FILTER indicates the destination port comes from the filter definition. A value of PACKET indicates the destination port comes from the packet. This field is significant if the filter type indicates this is a dynamic anchor filter. If the filter is not a dynamic anchor filter, a value of zero (0) is stored and blanks are displayed in the field.

IP Address Version

The version of the IP addresses being used for the traffic descriptor and the security endpoints. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = IPv4: The traffic descriptor and the security endpoints are using IPv4 addresses.
- 1 = IPv6: The traffic descriptor and the security endpoints are using IPv6 addresses.

Current IP Filters by Destination Address workspace

The Current IP Filters By Destination Address workspace displays all the IP filters that match a destination IP address you specify.

One of the ways to display the Current IP Filters by Destination Address workspace is to do the following:

1. Right-click the **IP Filters** navigator item for a specific TCP/IP stack.
2. Select **Workspaces**, and select the **Current IP Filters** workspace.
3. Click the Link icon in the **Current IP Filters** summary table and select **Current IP Filters by Destination Address**.
4. Provide a destination IP address for one of the filters in the current stack in the resulting dialog box. This field is filled in by default with the value from the **Destination Address** column for the selected filter, but you can change this value to be any IPv4 or IPv6 address. If the Destination Address column is blank, the field will display IP address that matches all addresses. With this address as input, this link navigates to the Current IP Filters By Destination Address Workspace showing the IP filters that match the destination IP address that you provided.

Links to Other Workspaces:

Right-click the Link icon in the Current IP Filters by Destination Address table to display a list of links to other workspaces. Left-click the Link icon to select the default link and navigate to the link's target workspace.

- **Dynamic IP Tunnels By Filter Rule Definition Name** (default). This link navigates to the Dynamic IP Tunnels workspace and shows tunnels that have a filter rule definition name that matches the name of the selected filter.
- **Dynamic IP Tunnels By Tunnel ID**: This is a conditional link and is only displayed in the list of available links if the filter type is DYNAMIC (4), NATTDYN (6), or NRF (7). This link navigates to the Dynamic IP Tunnels workspace and shows tunnels that have a tunnel ID that matches the tunnel ID associated with the selected filter.
- **Manual IP Tunnels by Tunnel ID**: This is a conditional link and is only displayed in the list of available links if the filter type is MANUAL (2). This link navigates to the Manual IP Tunnels workspace and shows tunnels that have a tunnel ID that matches the tunnel ID associated with the selected filter.
- **Current IP Filters In Scan Order By Same Page:** This is a conditional link and will only be displayed in the list of available links if the page number for the selected link is greater than 0. This link navigates to the Current IP Filters In Scan Order workspace and shows the IP filters that have a page number that is 1 less than the page number for the selected filter.

Data Source:

z/OS Communication Server Network Management Interface

Default Filter:

The table in this workspace is filtering using the destination IP address you provided.

Figure 7 shows the Current IP Filters by Destination Address workspace.

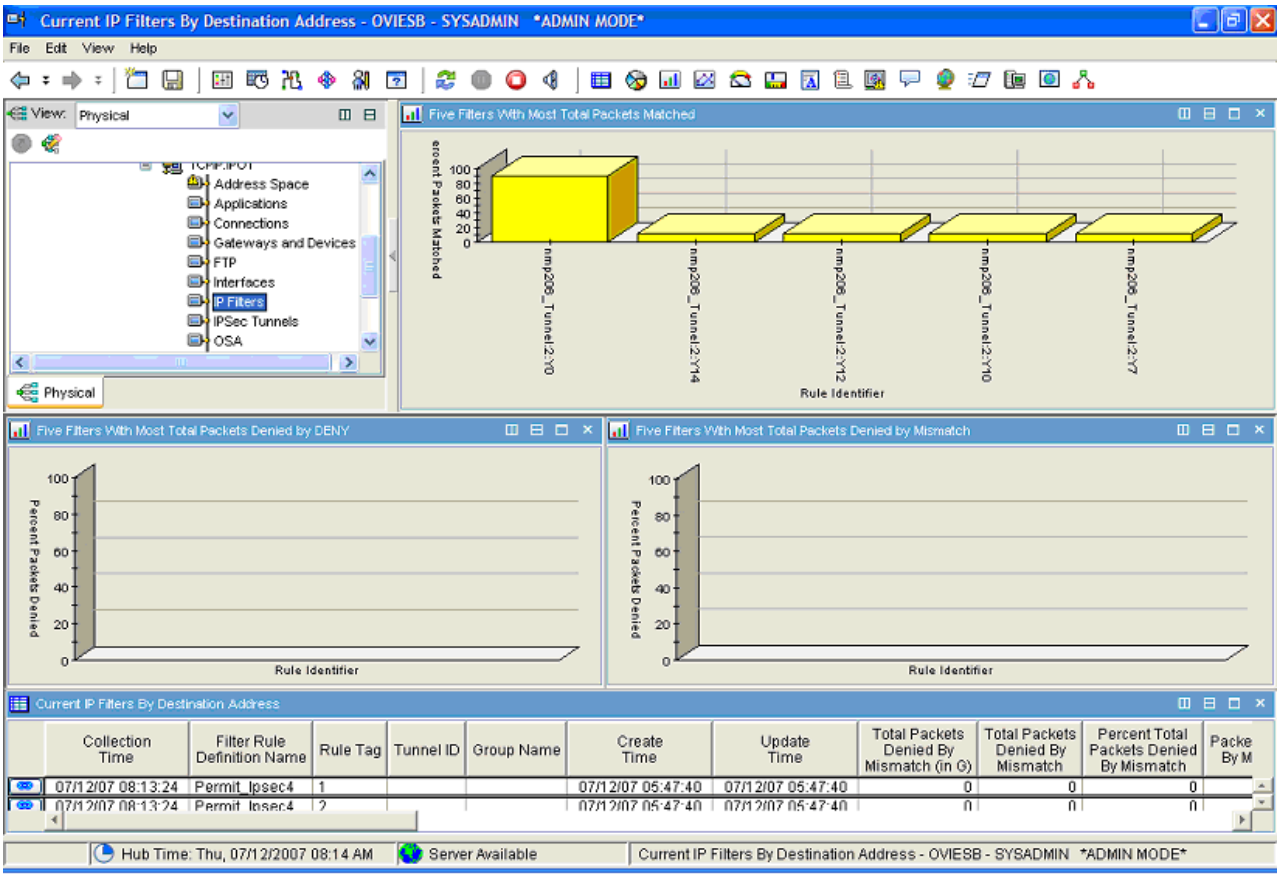


Figure 7. The Tivoli OMEGAMON XE for Mainframe Networks Current IP Filters by Destination Address workspace

The Current IP Filters by Destination Address workspace displays the following views:

Five Filters With Most Total Packets Matched
Displays the five filters that have the highest number of total packets that matched the filter's condition and action in the Current IP Filters table.

Five Filters With Most Total Packets Denied By DENY
Displays the five filters that have the highest number of total packets that matched the filter's condition and for which the action was DENY.

Five Filters With Most Total Packets Denied By Mismatch
Displays the five filters that have the highest number of total packets that matched the filter's condition but did not match the filter's action (for example, if a packet was sent "in the clear" but the action was coded as IPSec). This view can provide an indication of a configuration problem such as packets flowing in the clear when they should be encrypted.

Current IP Filters by Destination Address summary table
This summary table provides performance and configuration data about currently active IP filters. Each row in the table represents a single IP filter. The first 500 filters are displayed. Additional filters may be displayed by following one of the links.

Current IP Filters by Destination Address attributes: For a complete list of the attributes available in the Current IP Filters by Destination Address summary table, and a brief description of each, see the "Current IP Filters attributes" on page 77.

Current IP Filters by Filter Rule Definition Name workspace

The Current IP Filters By Filter Rule Definition Name workspace displays the IP filters whose filter rule definition name matches the name passed in the link.

One of the ways to display the Current IP Filters by Filter Rule Definition Name workspace is to do the following:

1. Right-click the **IPSec Tunnels** navigator items for a specific TCP/IP stack.
2. Select **Workspaces** and select the **Dynamic IP Tunnels** workspace.
3. From the **Dynamic IP Tunnels With Byte Rate = 0** summary table or the **Dynamic IP Tunnels With Byte Rate >= 2048** summary table, right-click a Link icon and select **Current IP Filters By Filter Rule Definition Name**. Rows of data are displayed that match the rule name.

Links to Other Workspaces:

Right-click the Link icon in the Current IP Filters by Filter Rule Definition Name table to display a list of links to other workspaces. Left-click the Link icon to select the default link and navigate to the link's target workspace.

- **Dynamic IP Tunnels by Tunnel ID** (default): This is a conditional link and is only displayed in the list of available links if the filter type is DYNAMIC (4), NATTDYN (6), or NRF (7). This link navigates to the Dynamic IP Tunnels workspace and shows tunnels that have a tunnel ID that matches the tunnel ID associated with the selected filter.
- **Current IP Filters in Scan Order By Same Page Workspace**: This link navigates to the Current IP Filters in Scan Order workspace and shows the IP filters that have a page number that is the same as the page for the selected filter. If the active filters have changed significantly between collection intervals (for example, if the filter set in use was switched or a large number of filters became inactive), this link might display a workspace with no filters
- **Current IP Filters by Destination Address**: This link causes a dialog box to be displayed that prompts you for a destination IP address that is compared to the currently active filters for a TCP/IP stack. This field is filled in by default with the value from the **Destination Address** column for the selected filter, but you can change this value to be any IPv4 or IPv6 address. If the Destination Address column is blank, the field will display IP address that matches all addresses. With this address as input, this link navigates to the Current IP Filters by Destination Address showing the IP filters that match the destination IP address that you provided.

Data Source:

z/OS Communication Server Network Management Interface

Default Filter:

The table in this workspace is filtering based on the Filter Rule Definition Name attribute.

Figure 6 on page 76 shows the Current IP Filters by Filter Rule Definition Name workspace.

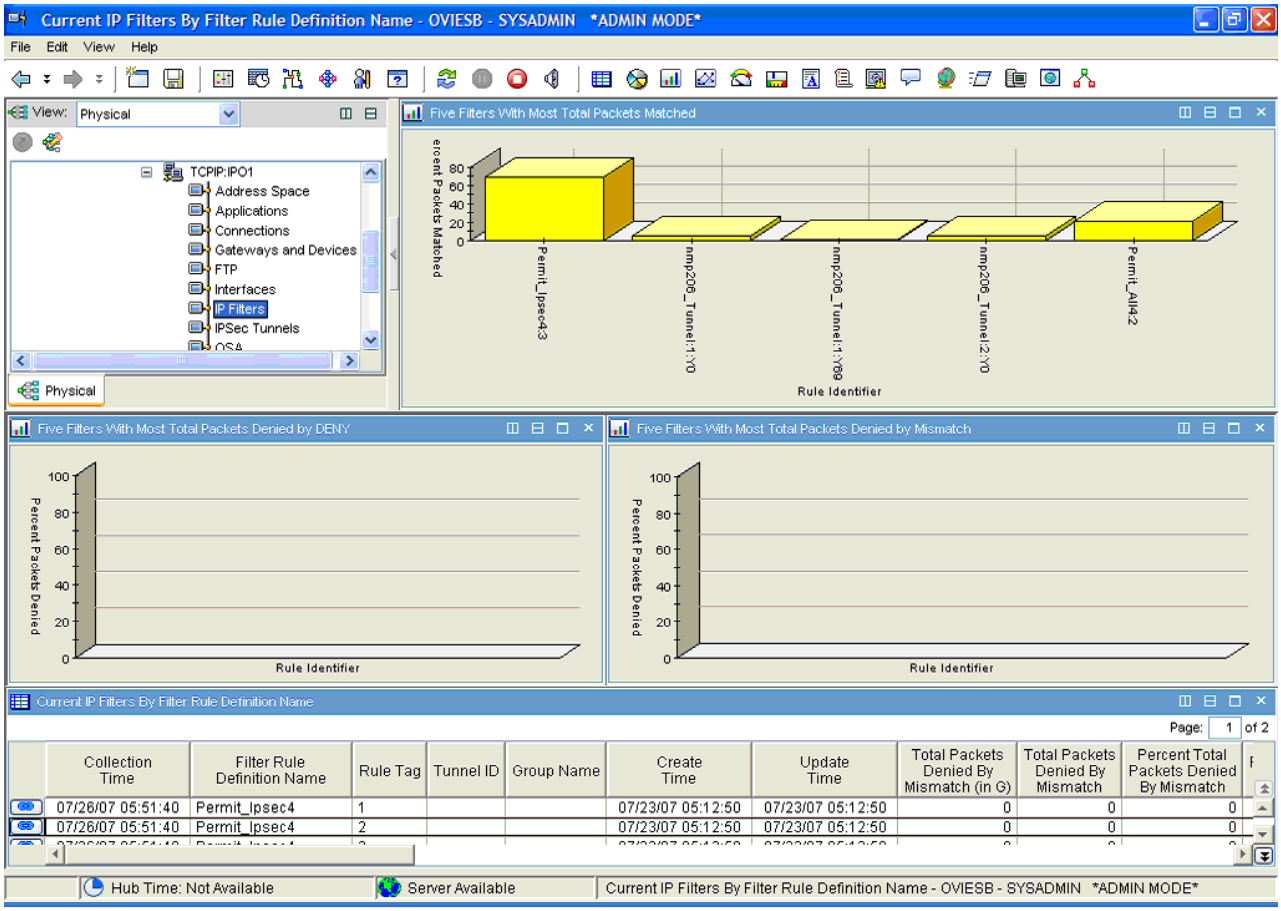


Figure 8. The Tivoli OMEGAMON XE for Mainframe Networks Current IP Filters by Filter Rule Definition Name workspace

The Current IP Filters by Filter Rule Definition Name workspace displays the following views:

Five Filters With Most Total Packets Matched
Displays the five filters that have the highest number of total packets that matched the filter's condition and action in the Current IP Filters table.

Five Filters With Most Total Packets Denied By DENY
Displays the five filters that have the highest number of total packets that matched the filter's condition and for which the action was DENY.

Five Filters With Most Total Packets Denied By Mismatch
Displays the five filters that have the highest number of total packets that matched the filter's condition but did not match the filter's action (for example, if a packet was sent "in the clear" but the action was coded as IPSec). This view can provide an indication of a configuration problem such as packets flowing in the clear when they should be encrypted.

Current IP Filters by Filter Rule Definition Name summary table
Provides performance and configuration data about currently active IP filters specified by the filter rule definition name. Each row in the table represents a single IP filter. The filters are displayed in the order that they would be scanned by the TCP/IP stack when it compares them to packets.

Current IP Filters by Filter Rule Definition Name attributes: For a complete list of the attributes available in the Current IP Filters by Filter Rule Definition Name summary table, and a brief description of each, see the "Current IP Filters attributes" on page 77.

Current IP Filters in Scan Order workspace

The Current IP Filters in Scan Order workspace is used to display IP filters beyond the first 500 IP Filters shown in the Current IP Filters Workspace. The filters are displayed in the order that the stack would scan them to match them to packets.

One of the ways to display the Current IP Filters in Scan Order workspace is to do the following:

1. Right-click the **IP Filters** navigator item for a specific TCP/IP stack.
2. Select **Workspaces** and select the **Current IP Filters** workspace.
3. Click the Link icon in the **Current IP Filters** summary table and select the **Current IP Filters in Scan Order by Next Page** link. Rows of data are displayed that match the scan order.

Links to Other Workspaces:

Right-click the Link icon in the Current IP Filters in Scan Order table to display a list of links to other workspaces. Left-click the Link icon to select the default link and navigate to the link's target workspace.

- **Dynamic IP Tunnels By Filter Rule Definition Name (Default)**. This link navigates to the Dynamic IP Tunnels workspace and shows tunnels that have a Filter Rule Definition Name that matches the name of the selected filter.
- **Dynamic IP Tunnels By Tunnel ID**: This is a conditional link and is only displayed in the list of available links if the filter type is DYNAMIC (4), NATTDYN (6), or NRF (7). This link navigates to the Dynamic IP Tunnels workspace and shows tunnels that have a tunnel ID that matches the tunnel ID associated with the selected filter.
- **Manual IP Tunnels by Tunnel ID**: This is a conditional link and is only displayed in the list of available links if the filter type is MANUAL (2). This link navigates to the Manual IP Tunnels workspace and shows tunnels that have a tunnel ID that matches the tunnel ID associated with the selected filter.
- **Current IP Filters In Scan Order By Previous Page:** This is a conditional link and will only be displayed in the list of available links if the page number for the selected link is greater than 0. This link navigates to the Current IP Filters In Scan Order workspace and shows the IP filters that have a page number that is 1 less than the page number for the selected filter. If the active filters have changed significantly between collection intervals (for example, if the filter set in use was switched or a large number of filters became inactive), this link will display a workspace with no filters.
- **Current IP Filters In Scan Order By Next Page:** This is a conditional link and will only be displayed in the list of available links if the page number for the selected link is greater than 0. This link navigates to the Current IP Filters In Scan Order workspace and shows the IP filters that have a page number that is 1 less than the page number for the selected filter. If the active filters have changed significantly between collection intervals (for example, if the filter set in use was switched or a large number of filters became inactive), this link will display a workspace with no filters.
- **Current IP Filters by Destination Address**: This link causes a dialog box to be displayed that prompts you for a destination IP address that is compared to the currently active filters for a TCP/IP stack. This field is filled in by default with the value from the **Destination Address** column for the selected filter, but you can change this value to be any IPv4 or IPv6 address. If the Destination Address column is blank, the field will display IP address that matches all addresses. With this address as input, this link navigates to the Current IP Filters by Destination Address showing the IP filters that match the destination IP address that you provided.

Data Source:

z/OS Communication Server Network Management Interface

Default Filter:

There can be tens of thousands of IP Filters. The query filter implemented for this workspace retrieves up to 500 IP Filters at a time.

The Tivoli Enterprise Portal displays 100 rows of IPSec Filters at a time. Use the Tivoli Enterprise Portal scrolling controls or change the page number at the top right of the table view to see the remaining IP Filters from the current set of up to 500 IP Filters.

If more IP Filters exist beyond the set of 500 currently displayed, a link named **Current IP Filters In Scan Order By Next Page** will be provided in the right-click menu of the link icons for each row in the Current IP Filters in Scan Order table view. Use this link to display each successive group of 500 IP Filters. When no more IP Filters are available for display, the link will not appear in the right click menu. If you have already used the **Current IP Filters In Scan Order By Next Page** link to display additional IP Filters, another link named **Current IP Filters In Scan Order By Previous Page** can be used to return to the previous set of 500 IP Filters.

Figure 6 on page 76 shows the Current IP Filters in Scan Order workspace.

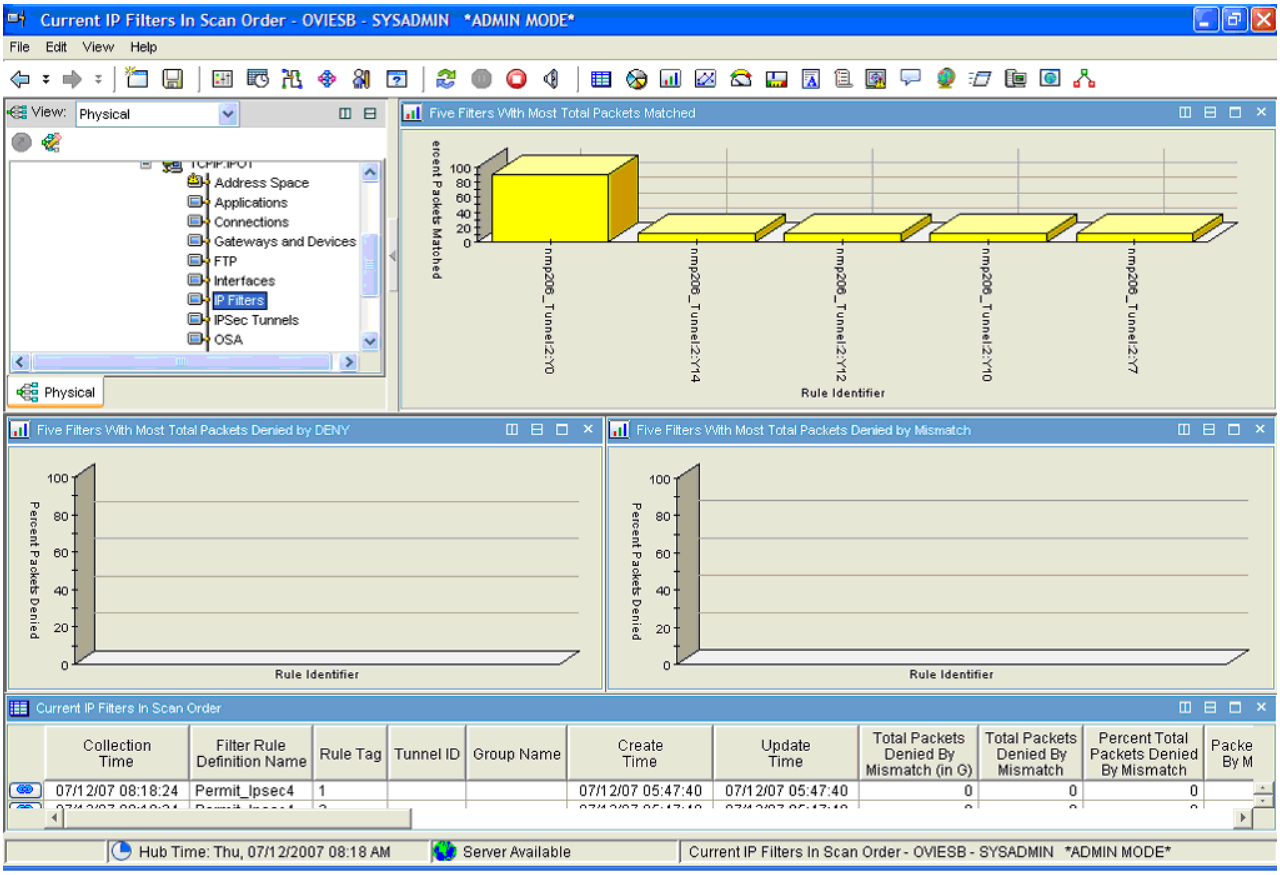


Figure 9. The Tivoli OMEGAMON XE for Mainframe Networks Current IP Filters in Scan Order workspace

The Current IP Filters in Scan Order workspace displays the following views:

Five Filters With Most Total Packets Matched
Displays the five filters that have the highest number of total packets that matched the filter's condition and action in the Current IP Filters table.

Five Filters With Most Total Packets Denied By DENY
Displays the five filters that have the highest number of total packets that matched the filter's condition and for which the action was DENY.

Five Filters With Most Total Packets Denied By Mismatch
Displays the five filters that have the highest number of total packets that matched the filter's condition but did not match the filter's action (for example, if a packet was sent "in the clear" but

the action was coded as IPSec). This view can provide an indication of a configuration problem such as packets flowing in the clear when they should be encrypted.

Current IP Filters in Scan Order summary table
This summary table provides performance and configuration data about the IP filters that are grouped on the same logical page. The filters are displayed in the order that they would be scanned by the TCP/IP stack when it compares them to packets.

Current IP Filters in Scan Order attributes: For a complete list of the attributes available in the Current IP Filters in Scan Order summary table, and a brief description of each, see the "Current IP Filters attributes" on page 77.

Dynamic IP Tunnels Statistics workspace

The Dynamic IP Tunnels Statistics workspace displays cumulative availability and performance statistics for the dynamic IP tunnels known to a TCP/IP stack.

The Dynamic IP Tunnels Statistics workspace can be displayed by clicking the **IPSec Tunnels** Navigator item of each monitored TCP/IP stack.

Additional Workspaces:
Right-click the **IPSec Tunnels** Navigator item to display the following additional workspaces:

- **Dynamic IP Tunnels Statistics** (default): Displays cumulative availability and performance statistics for the dynamic IP tunnels known to a TCP/IP stack.
- **Dynamic IP Tunnels**: Displays availability and performance statistics for dynamic IP tunnels known to the IKE daemon and the TCP/IP stack. Because of the large number of possible dynamic tunnels, this workspace has a predefined default filter when initially opened. The table view displays only those tunnels with a byte rate >= 2048
- **Manual IP Tunnels**: Displays availability and performance statistics for manual IP tunnels known to a specific TCP/IP stack.
- **IKE Tunnels Statistics**: Displays cumulative availability and performance statistics for all of the IKE tunnels known by the IKE daemon for a TCP/IP stack.
- **IKE Tunnels**: Displays availability and performance statistics for the IKE tunnels known to a specific TCP/IP stack.
- **Dynamic IP Tunnels with Byte Rate < 2048**: Displays availability and performance statistics for dynamic IP tunnels with a byte rate of less than 2048 bytes known to the IKE daemon and the TCP/IP stack.
- **IKE Tunnel with Byte Rate < 1024**: Displays availability and performance statistics for the IKE tunnels with a byte rate less than 1024 known to a specific TCP/IP stack.

Links to Other Workspaces:
Right-click the Link icon in the Dynamic IP Tunnels Statistics summary table to display a list of links to other workspaces. Left-click the Link icon to select the default link and navigate to its target workspace.

- **Dynamic IP Tunnels**: (default) Displays cumulative availability and performance statistics for the dynamic IP tunnels known to a TCP/IP stack.
- **Dynamic IP Tunnels With Byte Rate < 2048**: Displays availability and performance statistics for dynamic IP tunnels with a byte rate of less than 2048 bytes known to the IKE daemon and the TCP/IP stack.
- **Manual IP Tunnels**: Displays availability and performance statistics for manual IP tunnels know to a specific TCP/IP stack.

Data Source:
z/OS Communication Server Network Management Interface.

Default Filter:
None.

Figure 11 on page 96 shows the Dynamic IP Tunnels Statistics workspace.

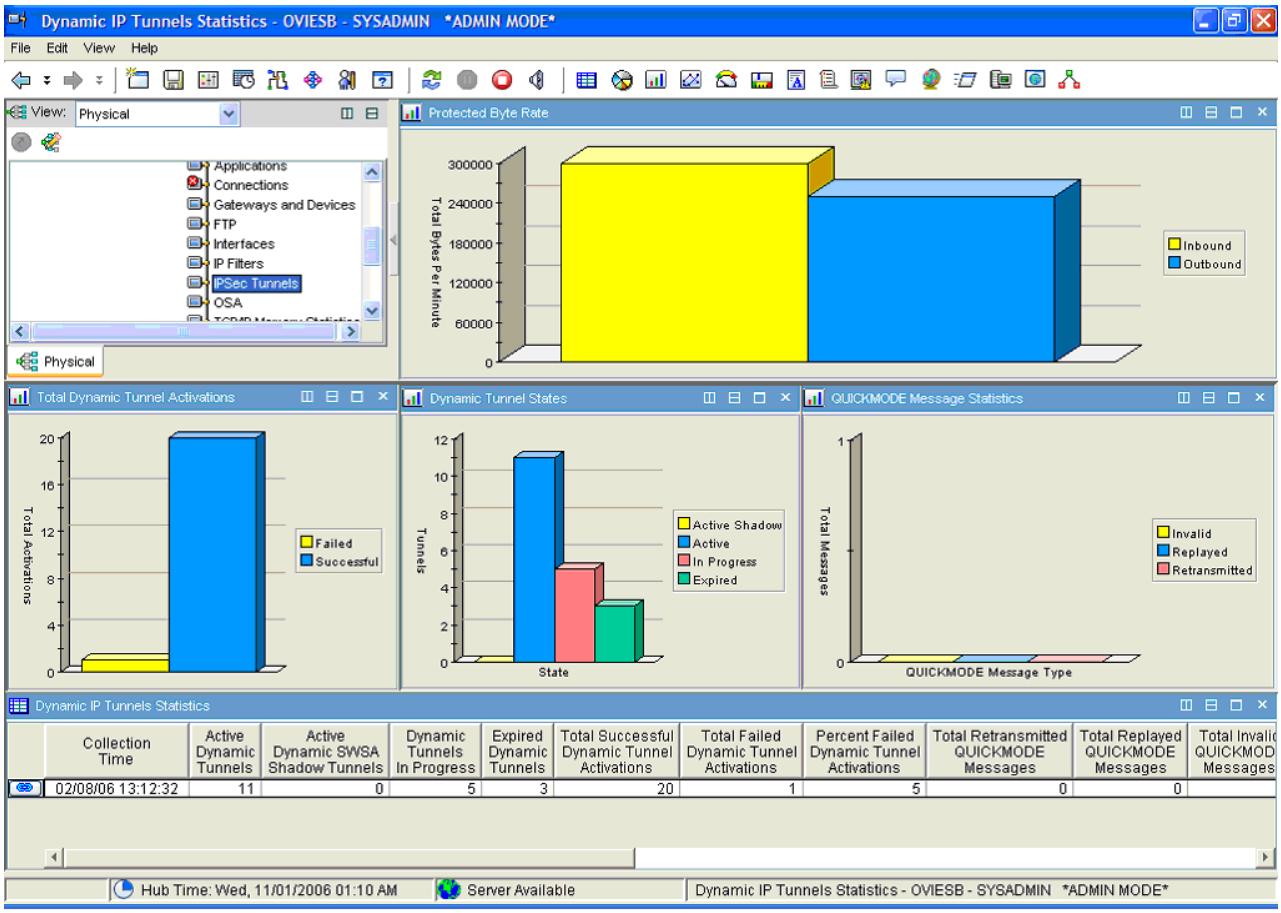


Figure 10. The Tivoli OMEGAMON XE for Mainframe Networks Dynamic IP Tunnels Statistics workspace

The Dynamic IP Tunnels Tunnels Statistics workspace displays the following views:

Protected Byte Rate

Shows the rate at which data is flowing through all of the dynamic IPSec tunnels on the stack. This view can be used to see which tunnels are being used the most. The graph is a bar chart where:

- Yellow represents the inbound byte rate expressed as number of bytes per minute.
- Blue represents the outbound byte rate expressed as number of bytes per minute.

Total Dynamic Tunnel Activations

Shows the cumulative number of successful and failed dynamic tunnel activations since the stack was started. The graph is a bar chart where:

- Yellow represents the number of dynamic tunnels that were successfully activated
- Blue represents the number of dynamic tunnels that failed to be activated.

Dynamic Tunnel States

Shows the dynamic IP tunnels known by the TCP/IP stack grouped by state. The graph is a bar chart where:

- Yellow represents the number of Active Shadow (SWSA) tunnels.
- Blue represents the number of Active tunnels.
- Pink represents the number of In Progress (either pending or in negotiation) tunnels.

- Green represents the number of Expired tunnels.

Quickmode Message Statistics

Provides cumulative statistics about QUICKMODE messages used to negotiate dynamic IPSec tunnels since the IKE daemon was started. High numbers of retransmits and replays may indicate a network problem between the security endpoints (IKEs). Non-zero values for invalid messages may indicate a possible attack. The graph is a bar chart where:

- Yellow represents the number Invalid QUICKMODE messages.
- Blue represents the number Replayed QUICKMODE messages.
- Pink represents the number of Retransmitted QUICKMODE messages.

Dynamic IP Tunnels Statistics summary table

Provides cumulative performance and availability data aggregated across all the dynamic IP tunnels known to the TCP/IP stack and the IKE daemon since the TCP/IP stack was started.

Dynamic IP Tunnels Statistics attributes

The following attributes are displayed in the Dynamic IP Tunnels Statistics summary table:

Collection Time

The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Active Dynamic Tunnels

The current number of active dynamic tunnels known to the TCP/IP stack. This number does not include Sysplex-Wide Security Associations (SWSA) shadow tunnels or manual tunnels. The format is an integer.

Active Dynamic SWSA Shadow Tunnels

The current number of active dynamic Sysplex-Wide Security Associations (SWSA) shadow tunnels known to the TCP/IP stack. The format is an integer.

Dynamic Tunnels In Progress

The number of dynamic tunnels in progress. The state of the tunnel is either PENDING or IN NEGOTIATION. The format is an integer where:

- 0 means PENDING
- 1 means IN NEGOTIATION

Expired Dynamic Tunnels
The number dynamic tunnels that are currently expired. This value includes shadow and non-shadow tunnels. The format is an integer.

Total Successful Dynamic Tunnel Activations
The cumulative number of successful dynamic tunnel activations since the TCP/IP stack was started. The format is an integer.

Total Failed Dynamic Tunnel Activations
The cumulative number of failed dynamic tunnel activations since the TCP/IP stack was started. The format is an integer.

Total Retransmitted QUICKMODE Messages
The cumulative number of retransmitted QUICKMODE (phase 2) messages sent since the Internet Key Exchange (IKE) daemon was started. The format is an integer.

Total Replayed QUICKMODE Messages
The cumulative number of replayed QUICKMODE (phase 2) messages received since the Internet Key Exchange (IKE) daemon was started. The format is an integer.

Total Invalid QUICKMODE Messages
The cumulative number of invalid QUICKMODE (phase 2) messages received since the Internet Key Exchange (IKE) daemon was started. The format is an integer.

IP Total Outbound Bytes Protected (in G)
The cumulative number of outbound bytes of IP traffic protected by dynamic tunnels since the start of the TCP/IP stack, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,823 and added to the value in the IP Outbound Bytes Protected column to calculate the cumulative number of IP outbound bytes protected. The format is an integer.

IP Total Outbound Bytes Protected
The cumulative number of outbound bytes of IP traffic protected by dynamic tunnels since the start of the TCP/IP stack. The value in this column can be added to the product of 1,073,741,823 and the value in the IP Outbound Bytes Protected (in G) column to calculate the cumulative number of IP Outbound Bytes Protected. The format is an integer.

IP Outbound Bytes Protected
The number of outbound bytes protected by IP tunnels in the last interval. The format is an integer.

IP Outbound Protected Byte Rate
The number of outbound bytes flowing through IP tunnels every minute. The format is an integer.

IP Total Inbound Bytes Protected (in G)
The cumulative number of inbound bytes of IP traffic protected by dynamic tunnels since the start of the TCP/IP stack, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,823 and added to the value in the IP Inbound Bytes Protected column to calculate the cumulative number of IP inbound bytes protected. The format is an integer.

IP Total Inbound Bytes Protected
The cumulative number of inbound bytes of IP traffic protected by dynamic tunnels since the start of the TCP/IP stack. The value in this column can be added to the product of 1,073,741,823 and the value in the IP Inbound Bytes Protected (in G) column to calculate the cumulative number of IP Inbound Bytes Protected. The format is an integer.

IP Inbound Bytes Protected
The number of inbound bytes protected by IP tunnels in the last interval. The format is an integer.

IP Inbound Protected Byte Rate
The number of inbound bytes flowing through IP tunnels every minute. The format is an integer.

Dynamic IP Tunnels workspace

The Dynamic IP tunnels workspace displays availability and performance statistics for dynamic IP tunnels known to the IKE daemon and the TCP/IP stack. Because of the large number of possible dynamic tunnels, this workspace has a predefined default filter when initially opened. These table views displays only those tunnels with a byte rate >= 2048 or = 0.

One of the ways to display the Dynamic IP Tunnels workspace is to right-click the **IPSec Tunnels** Navigator item for a specific TCP/IP stack, select **Workspaces** and select the **Dynamic IP Tunnels** workspace.

Links to Other Workspaces:

The following additional workspaces can be accessed by clicking the Link icon in the Dynamic IP Tunnels With Byte Rate >= 2048 or the Dynamic IP Tunnels with Byte Rate = 0 summary tables:

- **IKE Tunnels by Tunnel ID** (default): Navigates to the IKE Tunnels By Tunnel ID workspace and displays the IKE tunnel used to activate the selected tunnel.
- **Current IP Filters by Filter Rule Defintion Name**: Navigates to the Current IP Filters By Filter Rule Definition Name workspace and displays the IP filter used to activate the selected tunnel.
- **Dynamic IP Tunnels by Destination Address**: Navigates to the Current IP Tunnels By Destination Address workspace and displays tunnels that match the destination IP address you specified in the **Destination Address** dialog box. This dialog box prompts you for a destination IP address that is compared to the currently active tunnels for a TCP/IP stack. This field is filled in by default with the value from the **Destination Address** column for the selected tunnel, but you can change this value to be any IPv4 or IPv6 address. If the **Destination Address** column is blank, the field will display IP address that matches all addresses. With this address as input, this link navigates to the Dynamic IP Tunnels by Destination Address showing the IP tunnels that match the destination IP address that you provided.

Data Source:

z/OS Communications Server Network Management Interfaces

Default Filter:

There could be thousands of dynamic IP tunnels. This workspace must have a predefined default filter when initially opened. These table views display only tunnels with a byte rate >= 2048 or tunnels where the byte rate = 0.

Figure 11 on page 96 shows the Dynamic IP Tunnels workspace.

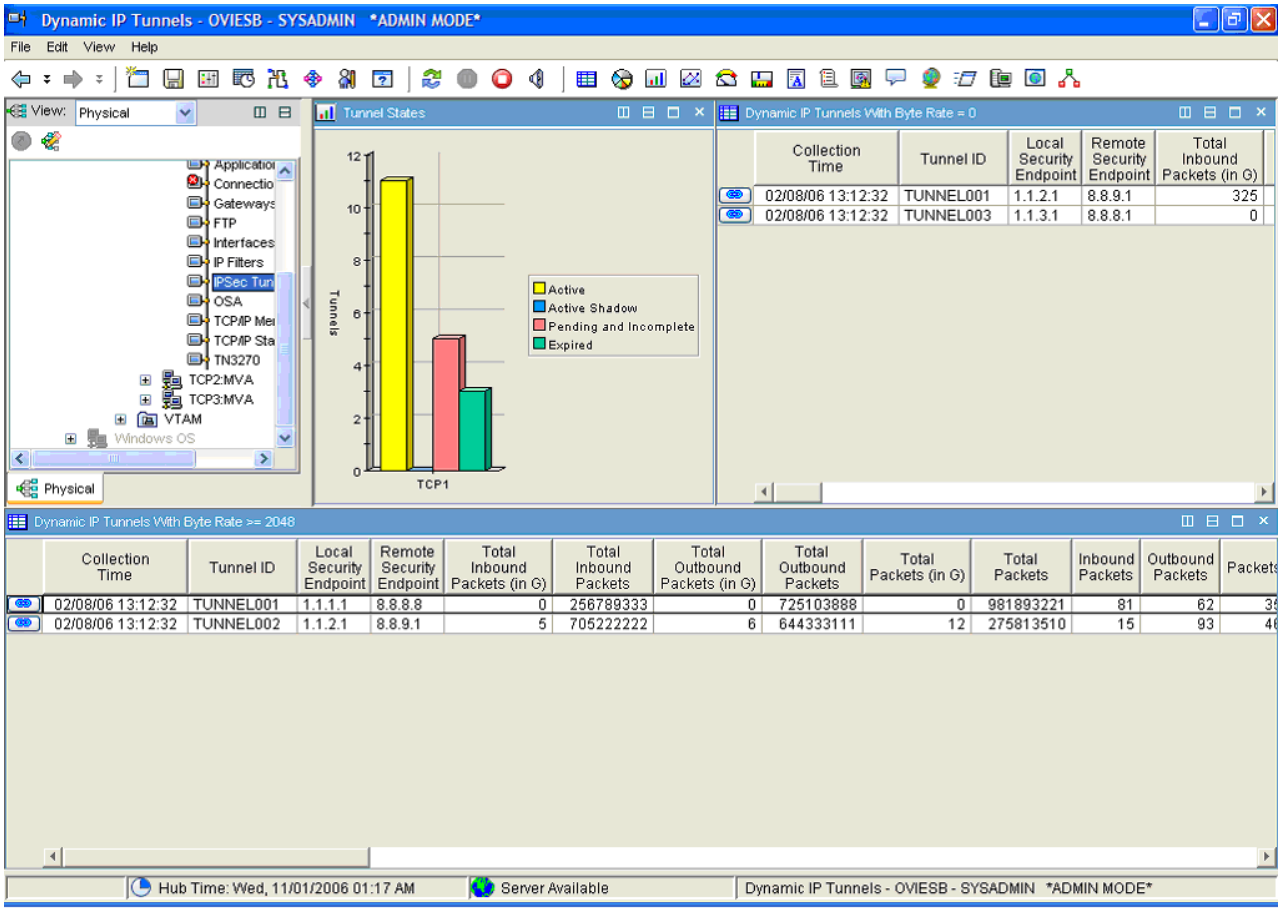


Figure 11. The Tivoli OMEGAMON XE for Mainframe Networks Dynamic IP Tunnels workspace

The Dynamic IP Tunnels workspace displays the following views:

Tunnel States
Shows the current number of dynamic IP tunnels in different states for the given TCP/IP stack. The query for this view uses the IPSec status table instead of the Dynamic IP tunnels table. The graph is a bar chart where:

- Yellow represents the number of Active tunnels.
- Blue represents the number of Active Shadow (SWSA) tunnels.
- Pink represents the number of Pending or Incomplete tunnels.
- Green represents the number of Expired tunnels.

Dynamic IP Tunnels with Byte Rate = 0 summary table
Provides performance and configuration information for dynamic IP tunnels that are active and had a byte rate of 0 in the most recent interval. A byte rate of 0 could be indicative of a problem with the tunnel. Each row in the table represents a single dynamic IP tunnel.

Dynamic IP Tunnels with Byte Rate >= 2048 summary table
Provides performance and configuration data about dynamic IP tunnels that had a byte rate >= 2048 in the most recent interval. Each row in the table represents a single dynamic IP tunnel.

Dynamic IP Tunnels attributes: The following attributes are displayed in the **Dynamic IP Tunnels with Byte Rate = 0** and **Dynamic IP Tunnels with Byte Rate >= 2048** summary tables.

Collection Time
The time and date of the data sampling. This time is displayed in the following format:

mm/dd/yy hh:mm:ss

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format CYYMMDDHHMMSSmmm (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Tunnel ID
Tunnel identifier. This identifier is generated by TCP/IP and is not unique. Multiple related tunnels may have the same tunnel ID. The format is an alphanumeric string of up to 48 characters.

Local Security Endpoint
The IP address of the local security endpoint responsible for negotiating the tunnel. The format is a character string of up to 45 characters.

Remote Security Endpoint
The IP address of the remote security endpoint responsible for negotiating the tunnel. The format is a character string of up to 45 characters.

Total Inbound Packets (in G)
The total number of inbound packets for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Inbound Packets column to calculate the total inbound packets for the tunnel. For SWSA tunnels, the value is for packets that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Inbound Packets
The total number of inbound packets for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Inbound Packets (in G) column to calculate the total inbound packets for the tunnel. For SWSA tunnels, the value is for packets that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Outbound Packets (in G)
The total number of outbound packets for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Outbound Packets column to calculate the total outbound packets for the tunnel. For SWSA tunnels, the value is for packets that have traversed the tunnel since it was assigned to this stack only. The format is an integer

Total Outbound Packets
The total number of outbound packets for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Outbound

Packets (in G) column to calculate the total outbound packets for the tunnel. For SWSA tunnels, the value is for packets that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Packets (in G)
The total number of inbound and outbound packets for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Packets column to calculate the total packets for the tunnel. For SWSA tunnels, the value is for packets that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Packets
The total number of inbound and outbound packets for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Packets (in G) column to calculate the total packets for the tunnel. For SWSA tunnels, the value is for packets that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Inbound Packets
The number of inbound packets for this tunnel during the most recent time interval. The format is an integer.

Outbound Packets
The number of outbound packets for this tunnel during the most recent time interval. The format is an integer.

Packets
The number of inbound and outbound packets for this tunnel during the most recent time interval. The format is an integer.

Packet Rate
The number of inbound or outbound packets, per minute, for this tunnel during the most recent time interval. The format is an integer.

Total Inbound Bytes (in G)
The total number of inbound bytes for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Inbound Bytes column to calculate the total inbound bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Inbound Bytes
The total number of inbound bytes for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Inbound Bytes (in G) column to calculate the total inbound bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Outbound Bytes (in G)
The total number of outbound bytes for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Outbound Bytes column to calculate the total outbound bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Outbound Bytes
The total number of outbound bytes for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Outbound Bytes (in G) column to calculate the total outbound bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Bytes (in G)
The total number of inbound and outbound bytes for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Bytes column to calculate the total bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Total Bytes
The total number of inbound and outbound bytes for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Bytes (in G) column to calculate the total bytes for the tunnel. For SWSA tunnels, the value is for bytes that have traversed the tunnel since it was assigned to this stack only. The format is an integer.

Inbound Bytes
The number of inbound bytes for this tunnel during the most recent time interval. The format is an integer.

Outbound Bytes
The number of outbound bytes for this tunnel during the most recent time interval. The format is an integer.

Bytes The number of inbound and outbound bytes for this tunnel during the most recent time interval. The format is an integer.

Byte Rate
The number of inbound or outbound bytes, per minute, for this tunnel during the most recent time interval. The format is an integer.

State Current state of tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 2 = PENDING: Waiting for negotiation to start.
- 3 = INCOMPLETE: Negotiation in progress.
- 4 = ACTIVE: Tunnel is active and ready for use.
- 5 = EXPIRED: Expired and cannot be used.

Extended State
Indicates progress of tunnel negotiation. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = INIT: No key exchange messages have been initiated.
- 1 = KEP: Key exchange messages have been initiated.
- 2 = DONE: All key exchange messages have been completed, and the tunnel is usable for traffic.
- 3 = PENDING_NOTIFY: Key exchange messages have been completed, waiting to receive connection notification.
- 4 = PENDING_START: Waiting for the activation of an Internet Key Exchange (IKE) tunnel.

SWSA Shadow Indicator
Sysplex-Wide Security Associations (SWSA) shadow indicator. If this value is set, the tunnel is a SWSA shadow tunnel. This value is stored as an integer and displayed as a string.

- 0 = <blank>
- 1 = Yes

Pending New Indicator
Pending new activation indicator. If set, this field indicates that dynamic IP tunnel is in the pending state and it represents a new activation rather than a refresh. If it is not set, the tunnel is either not

in pending state or is not a new activation. For z/OS Communications Server Version 1.7, the value will always be 0. This value is stored as an integer and displayed as a string. Valid values are

- 0 = <blank>
- 1 = Yes

Source Address
Source IP address for data protected by this tunnel. This address may be any IPv4 or IPv6 address. If the traffic protected by the tunnel may have any source IP address, the address is blank. If the traffic protected by the tunnel is a range of source IP addresses, the value displayed is the lower address in the range. This value is represented as a 45-character string.

Note: For comparison, leading zeros are added for unspecified digits in IPv4 and IPv6 addresses when they are stored.

Upper Source Address
If the traffic protected by the tunnel is a range of source IP addresses, this is the upper address in the range. This may be any IPv4 or IPv6 address. If the traffic protected by the tunnel is not a range of addresses or is all addresses, this field is stored as blanks. This field is represented as a 45-character string.

Note: For comparison, leading zeros are added for unspecified digits in IPv4 and IPv6 addresses when they are stored.

Source Port
Source port for traffic protected by tunnel. If the tunnel protects data for all source ports, this value is 0. This field is represented by a 5-character string.

Destination Address
Destination IP address for data protected by the tunnel. This value may be any IPv4 or IPv6 address. If the traffic protected by the tunnel may have any destination IP address, this field is stored as blanks. If the traffic protected by the tunnel is a range of destination IP addresses, the value displayed is the lower address in the range. This value is represented as a 45-character string.

Note: For comparison, leading zeros are added for unspecified digits in IPv4 and IPv6 addresses when they are stored.

Upper Destination Address
If the traffic protected by the tunnel is a range of destination IP addresses, this is the upper address in the range. This value may be any IPv4 or IPv6 address. If the traffic protected by the tunnel is not a range of addresses or all addresses, this field is stored as blanks. This field is represented as a 45-character string.

Note: For comparison, leading zeros are added for unspecified digits in IPv4 and IPv6 addresses when they are stored.

Destination Port
Destination port for traffic protected by the tunnel. If the tunnel protects data for all destination ports, this value is 0. This field is represented by a 5-character string.

Protocol
The IP protocol number for the data to be carried in the tunnel. A value of zero (0) indicates that tunnel protects data for any protocol. The format is an integer representing an Internet Engineering Task Force (IETF)-defined protocol number.

Filter Rule Definition Name
The name specified for the filter rule definition that this tunnel is associated with. This column is stored as a 48-character string.

VPN Action Name
The name specified on a virtual private network (VPN) action definition statement. The VPN action

describes how to protect the traffic that flows through the tunnel. It specifies attributes of the tunnel, such as what type of encryption to use. The format of the name is a character string of up to 48 characters.

Local Dynamic VPN Rule Name
The name specified on a z/OS Communications Server Policy Agent `LocalDynVpnRule` configuration statement. The statement describes traffic that is to be protected by a tunnel that is activated on demand using the `ipsec` command or when the Internet Key Exchange (IKE) daemon or the TCP/IP stack is started or both. This field is blank if the tunnel is not associated with a local rule. The name is a character string of up to 48 characters.

Encapsulation Mode
Encapsulation mode to be used by the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = TUNNEL
- 2 = TRANSPORT

Authentication Protocol
The authentication protocol to be used by the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 51 = AH
- 50 = ESP

Authentication Algorithm
The authentication algorithm used for this tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 38 = MD5
- 39 = SHA1

Encryption Algorithm
Tunnel encryption algorithm. This field is undefined if the tunnel state is PENDING or INCOMPLETE. A value of 99 is assigned to the field in this case and blanks are displayed. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = NONE
- 3 = 3DES
- 11 = NULL
- 12 = AES
- 18 = DES
- 99 = <blank>

Inbound Authentication SPI
Tunnel inbound authentication security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This field is an unsigned 4-byte integer and is displayed in hexadecimal. This field is undefined and displayed as blanks if the state of the tunnel is PENDING or INCOMPLETE. This field is not displayed.

Outbound Authentication SPI
Tunnel outbound authentication security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This is an unsigned 4-byte integer and is displayed in hexadecimal. This field is undefined and displayed as blanks if the state of the tunnel is PENDING or INCOMPLETE. This field is not displayed.

Inbound Encryption SPI

Tunnel inbound encryption security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This is an unsigned 4-byte integer and is displayed in hexadecimal. This field is undefined and displayed as blanks if the state of the tunnel is PENDING or INCOMPLETE. This field is not displayed.

Outbound Encryption SPI

Tunnel outbound encryption security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This is an unsigned 4-byte integer and is displayed in hexadecimal. This field is undefined and displayed as blanks if the state of the tunnel is PENDING or INCOMPLETE. This field is not displayed

Parent IKE Tunnel ID

Tunnel ID for this tunnel's parent IKE (Phase 1) tunnel. The Internet Key Exchange (IKE) tunnel is used to negotiate the IP tunnel. This field is represented as a 48-character string.

Current Life Size

The number of bytes of data that have traversed the tunnel since the tunnel was activated. This value is zero (0) if no life size was negotiated for the tunnel. The format is an integer.

Life Size

The number of bytes of data that may traverse the tunnel over the life of the tunnel. This value is zero (0) if no life size was negotiated for the tunnel. The format is an integer.

Refresh Life Size

The number of bytes that may traverse the tunnel before a refresh is needed. This value is zero (0) if no life size was negotiated. The format is an integer.

Life Expiration Time

The time at which the tunnel will expire. This column is blank if no life time was negotiated. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Life Refresh Time

The time at which the tunnel is refreshed. This column is blank if no life time was negotiated. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

VPN Life Expiration Time

The time at which the tunnel should no longer be refreshed. This column is blank if no life time was negotiated for the VPN (security attributes implemented by the tunnel). This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Activation Method

Indicates how the tunnel was activated. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = USER: User activation from the command line.
- 2 = REMOTE: Remote activation from the IPSec peer.
- 3 = ONDEMAND: On-demand activation caused by IP traffic.

- 5 = TAKEOVER: Sysplex-Wide Security Associations (SWSA) activation as a result of a Dynamic Virtual IP Addressing (DVIPA) takeover.
- 6 = AUTOACT: Auto-activation.

Source NAT-OA Payload
The source network address translation original address (NAT-OA) payload. NAT-OA payloads are exchanged only for certain UDP-encapsulated tunnels. During NAT traversal negotiations, the Internet Key Exchange (IKE) peer sends the source IPv4 address that it is aware of. If NAT traversal negotiation did not occur, or if peer did not send a source NAT-OA payload, this column is blank. This column is stored as a 15-character string. This field is not displayed.

Dest NAT-OA Payload
The destination network address translation original address (NAT-OA) payload. NAT-OA payloads are exchanged only for certain UDP-encapsulated tunnels. During NAT traversal negotiations, the Internet Key Exchange (IKE) peer sends the known destination IPv4 address. If NAT traversal negotiation does not occur, or if peer does not send a source NAT-OA payload, this column is blank. This column is stored as a 15-character string. This field is not displayed.

Diffie-Hellman Group
Diffie-Hellman group used to generate keying material for the tunnel. Each group identifies the number of bits to be used in a prime number that is used to generate keying material. This column is blank if PFS (perfect forward security) was not negotiated for the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 99 = <blank>
- 0 = NONE
- 1 = GROUP1
- 2 = GROUP2
- 5 = GROUP5
- 14 = GROUP14

Remote IKE UDP Port
The IKE UDP port of the remote security endpoint. This column is blank when UDP encapsulation is not being used by the tunnel. This column is stored as a 5-character string.

Local NAT Indicator
Indicates if a NAT has been detected in front of the local security endpoint. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Remote NAT Indicator
Indicates if a NAT has been detected in front of the remote security endpoint. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Remote NAPT Indicator
Indicates if a network address port translation (NAPT) has been detected in front of the remote security endpoint. It is possible that an NAPT may exist but is detected only as a NAT. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Remote NAT Traversal Gateway Indicator
Indicates if the remote security endpoint is acting as a NAT traversal gateway. If the remote

security endpoint is acting as a NAT traversal gateway, the tunnel uses UDP encapsulation and the remote security endpoint is acting as an IPSec gateway. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Remote zOS Indicator

Indicates if the remote peer is a z/OS system. This can be detected only if NAT traversal is enabled. Even if NAT traversal is enabled, it is possible for the remote peer to be a z/OS system and this indicator not to be set. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Initiation Indicator

Indicates if the local security endpoint may initiate dynamic tunnel negotiations with the remote security endpoint. Either security endpoint may initiate refreshes regardless of the value of this indicator. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Local Client ID Type

Internet Security Associations Key Management Protocol (ISAKMP) identity type for the local client ID as defined in RFC 2407. If client IDs were not exchanged during negotiation, this column is blank. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = IPv4_ADDR
- 2 = FQDN
- 3 = USER_FQDN
- 4 = IPv4_ADDR_SUBNET
- 5 = IPv6_ADDR
- 6 = IPv6_ADDR_SUBNET
- 7 = IPv4_ADDR_RANGE
- 8 = IPv6_ADDR_RANGE
- 9 = DER_ASN1_DN
- 10 = DER_ASN1_GN
- 11 = KEY_ID

Local Client ID

Internet Security Associations Key Management Protocol (ISAKMP) identity of local client. A string containing an identifier as described by Local Client ID Type. Some of the ID strings can get as long as 2048 characters. The ID is always truncated at 100 characters. If no IDs are exchanged, this fields contains blanks. The format is a string of up to 100 characters. This field is not displayed.

Remote Client ID Type

Internet Security Associations Key Management Protocol (ISAKMP) identity type for the remote client ID as defined in RFC 2407. If the client IDs were not exchanged during negotiation, this column is blank. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = IPv4_ADDR
- 2 = FQDN
- 3 = USER_FQDN

- 4 = IPv4_ADDR_SUBNET
- 5 = IPv6_ADDR
- 6 = IPv6_ADDR_SUBNET
- 7 = IPv4_ADDR_RANGE
- 8 = IPv6_ADDR_RANGE
- 9 = DER_ASN1_DN
- 10 = DER_ASN1_GN
- 11 = KEY_ID

This field is not displayed.

Remote Client ID
Internet Security Associations Key Management Protocol (ISAKMP) identity of remote client. A string containing an identifier as described by Remote Client ID Type. Some of the ID strings can get as long as 2048 characters. The ID is always truncated at 100 characters. If no IDs are exchanged, this field contains blanks. The format is a string of up to 100 characters. This field is not displayed.

IP Address Version
The version of the IP addresses being used for the traffic descriptor and the security endpoints. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = IPv4: The traffic descriptor and the security endpoints are using IPv4 addresses.
- 1 = IPv6: The traffic descriptor and the security endpoints are using IPv6 addresses.

Dynamic IP Tunnels by Destination Address workspace

The Dynamic IP Tunnels by Destination Address workspace displays availability and performance statistics for dynamic IP tunnels known to the IKE daemon and the TCP/IP stack.

Summary information is displayed in the **Dynamic IP Tunnels With Byte Rate = 0** summary table and the **Dynamic IP Tunnels by Destination Address** summary table.

One of the ways to display the Dynamic IP Tunnels by Destination Address workspace is to do the following:

1. Right-click the **IPSec Tunnels** Navigator item for a specific TCP/IP stack.
2. Select **Workspaces** and select the **Dynamic IP Tunnels** workspace.
3. Click the Link icon by one of the rows of the **Dynamic IP Tunnels With Byte Rate >= 2048** summary table.
4. Select the **Dynamic IP Tunnels by Destination Address** link.

Links to Other Workspaces:
The following additional workspaces can be accessed by clicking the Link icon in the Dynamic IP Tunnels by Destination Address summary table:

- **IKE Tunnel by Tunnel ID** (default): Navigates to the IKE Tunnels By Tunnel ID workspace and displays the IKE tunnel used to activate the selected tunnel.
- **Current IP Filters by Filter Rule Definition Name**: Navigates to the Current IP Filters By Filter Rule Definition Name workspace and displays the IP filter used to activate the selected tunnel.
- **Dynamic IP Tunnels by Destination Address** (this workspace)

Data Source:
z/OS Communication Server Network Management Interface

Default Filter:
The table in this workspace is filtering using the following attributes:

- Byte Rate = 0
- Destination Address

Figure 12 shows the Dynamic IP Tunnels by Destination Address workspace.

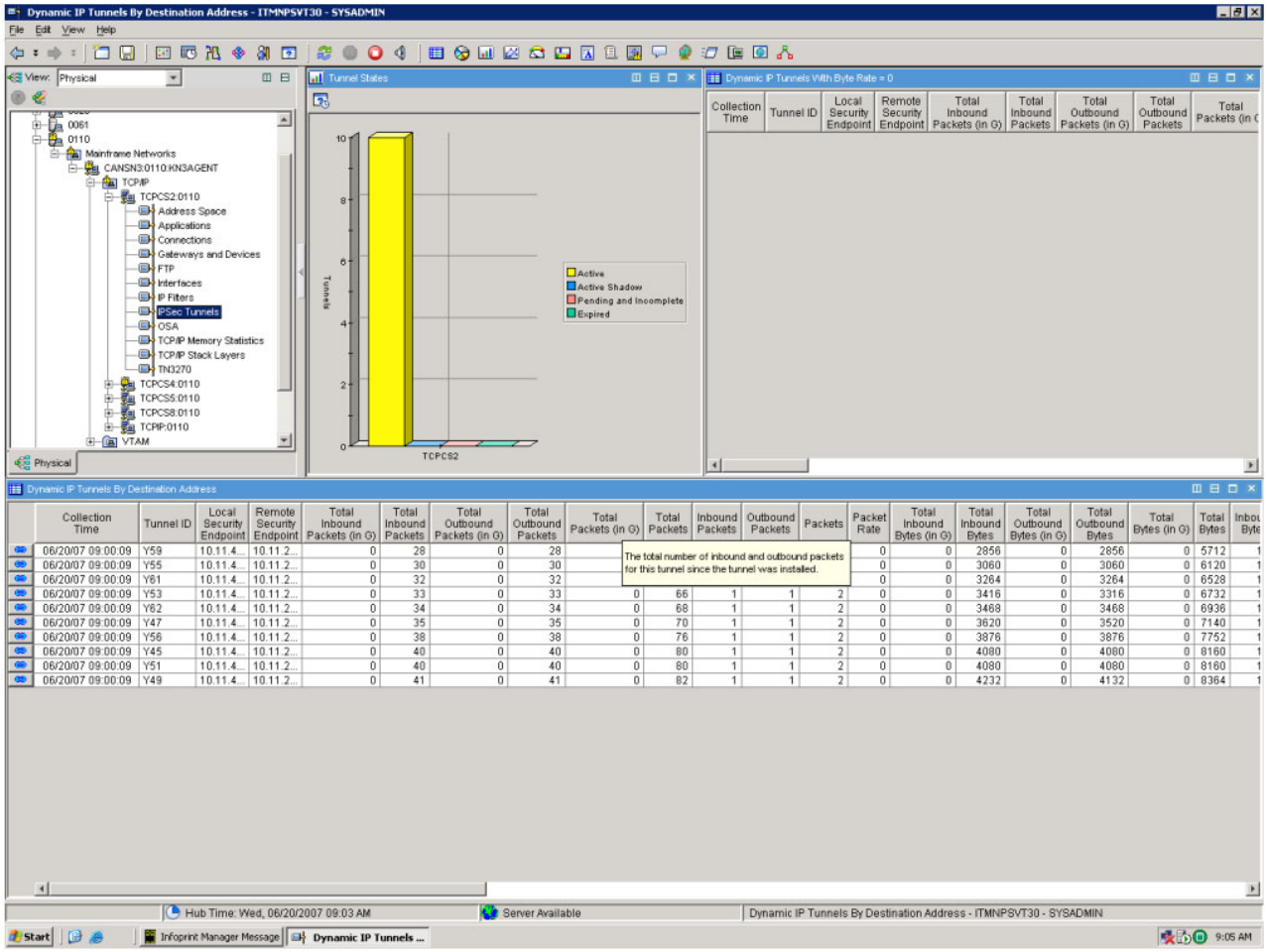


Figure 12. The Tivoli OMEGAMON XE for Mainframe Networks Dynamic IP Tunnels by Destination Address workspace

The Dynamic IP Tunnels by Destination Address Workspace contains the following views:

- **Tunnel States**: Shows the current number of dynamic IP tunnels in different states for the given TCP/IP stack. The query for this view uses the IPSec status table instead of the Dynamic IP tunnels table. The graph is a bar chart where:
  - Yellow represents the number of Active tunnels.
  - Blue represents the number of Active Shadow (SWSA) tunnels.
  - Pink represents the number of Pending or Incomplete tunnels.
  - Green represents the number of Expired tunnels.
- **Dynamic IP Tunnels with Byte Rate = 0** summary table: Provides performance and configuration information for dynamic IP tunnels to any destination address that are active and had a byte rate of 0 in the most recent interval. A byte rate of 0 could be indicative of a problem with the tunnel. Each row in the table represents a single dynamic IP tunnel.
- **Dynamic IP Tunnels by Destination Address** summary table: Provides performance and configuration data about dynamic IP tunnels that match the destination IP address you specified in the destination address dialog box. Each row in the table represents a single dynamic IP tunnel.

Dynamic IP Tunnels by Destination Address attributes: For a complete list of the attributes available in the **Dynamic IP Tunnels with Byte Rate = 0** and **Dynamic IP Tunnels by Destination Address** summary tables, and a brief description of each, see the “Dynamic IP Tunnels attributes” on page 96.

Dynamic IP Tunnels by Filter Rule Definition Name workspace

The Dynamic IP Tunnels by Filter Rule Definition Name workspace displays availability and performance statistics for dynamic IP tunnels that match a filter name passed in via a link.

One way to display the Dynamic IP Tunnels by Filter Rule Definition Name workspace is to do the following:

1. Right-click the **IP Filters** Navigator item for a specific TCP/IP stack.
2. Select **Workspaces** and select the **Current IP Filters** workspace.
3. Click the Link icon by one of the rows in the **Current IP Filters in Scan Order** summary table.
4. If you have selected a filter that is associated with a dynamic IP tunnel, the **Dynamic IP Tunnels by Filter Rule Definition Name** conditional link is displayed. This link is available only for filters with a **Type** value of DYNAMIC, NATTDYN or NRF.

Links to Other Workspaces:

The following additional workspaces can be accessed by right-clicking the Link icon in the Dynamic IP Tunnels by Filter Rule Definition Name summary table:

- **IKE Tunnels by Tunnel ID** (default): Navigates to the IKE Tunnels By Tunnel ID workspace and displays the IKE tunnel used to activate the selected tunnel.
- **Current IP Filters by Filter Rule Definition Name**: Navigates to the Current IP Filters By Filter Rule Definition Name workspace and displays the IP filter used to activate the selected tunnel.
- **Dynamic IP Tunnels by Destination Address**: Navigates to the Current IP Tunnels By Destination Address workspace and displays tunnels that match the destination IP address you specified in the **Destination Address** dialog box. This dialog box prompts you for a destination IP address that is compared to the currently active tunnels for a TCP/IP stack. This field is filled in by default with the value from the **Destination Address** column for the selected tunnel, but you can change this value to be any IPv4 or IPv6 address. If the Destination Address column is blank, the field will display IP address that matches all addresses. With this address as input, this link navigates to the Dynamic IP Tunnels By Destination Address showing the IP tunnels that match the destination IP address that you provided.

Data Source:

z/OS Communication Server Network Management Interface

Default Filter:

The table in this workspace is filtering using the following attributes:

- Filter Name
- Byte Rate = 0

Figure 13 on page 109 shows the Dynamic IP Tunnels by Filter Rule Definition Name workspace.

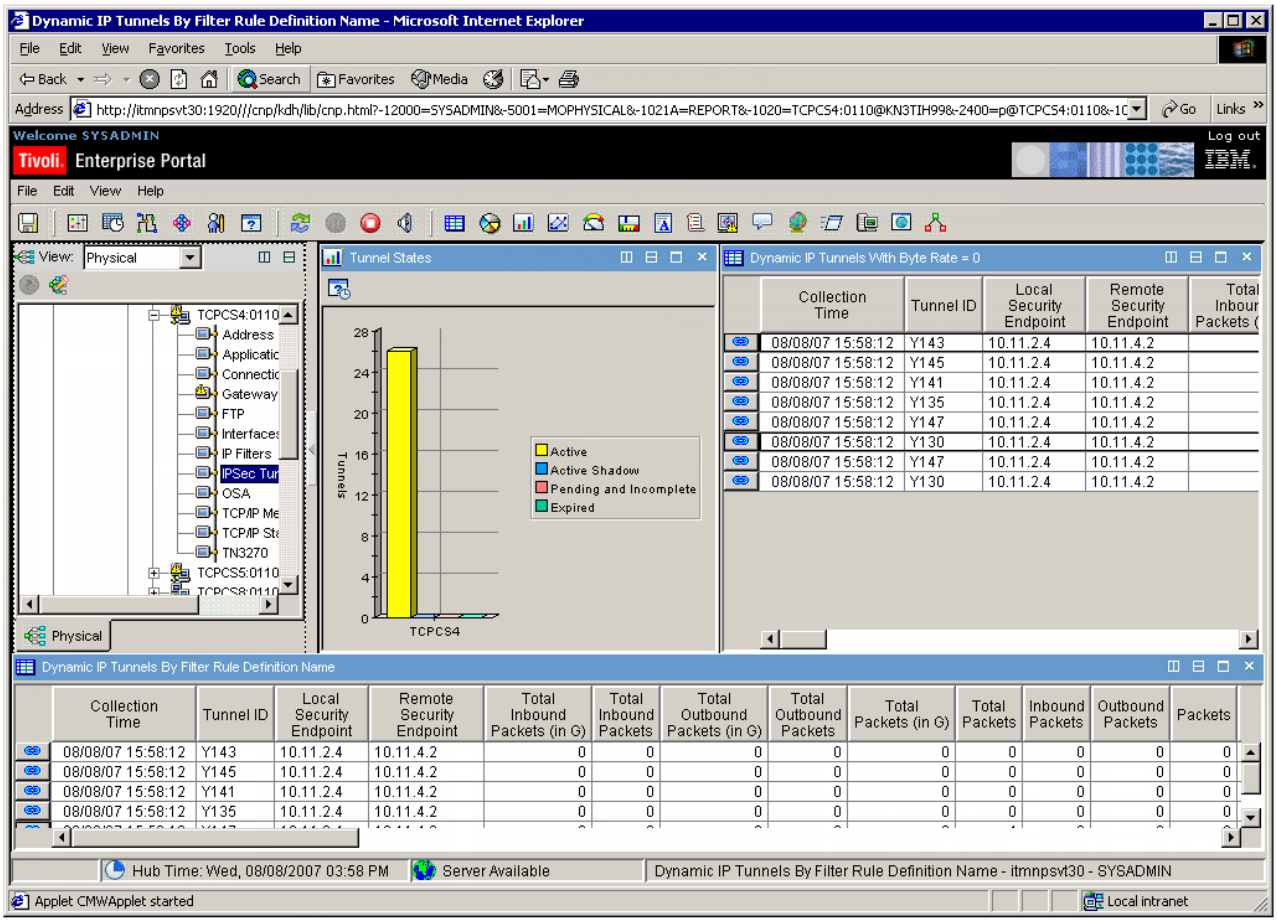


Figure 13. The Tivoli OMEGAMON XE for Mainframe Networks Dynamic IP Tunnels by Filter Rule Definition Name workspace

The Dynamic IP Tunnels by Filter Rule Definition Name Workspace contains the following views:

- **Tunnel States**: Shows the current number of dynamic IP tunnels in different states for the given TCP/IP stack. The query for this view uses the IPSec status table instead of the Dynamic IP tunnels table. The graph is a bar chart where:
  - Yellow represents the number of Active tunnels.
  - Blue represents the number of Active Shadow (SWSA) tunnels.
  - Pink represents the number of Pending or Incomplete tunnels.
  - Green represents the number of Expired tunnels.
- **Dynamic IP Tunnels with Byte Rate = 0** summary table: Provides performance and configuration information for dynamic IP tunnels to any destination address that are active and had a byte rate of 0 in the most recent interval. A byte rate of 0 could be indicative of a problem with the tunnel. Each row in the table represents a single dynamic IP tunnel.
- **Dynamic IP Tunnels by Filter Rule Definition Name** summary table: Provides performance and configuration data about dynamic IP tunnels that matched the filter rule definition name query in the most recent interval. Each row in the table represents a single dynamic IP tunnel.

Dynamic IP Tunnels by Filter Rule Definition Name attributes: For a complete list of the attributes available in the **Dynamic IP Tunnels with Byte Rate = 0** and **Dynamic IP Tunnels by Filter Rule Definition Name** summary tables, and a brief description of each, see the “Dynamic IP Tunnels attributes” on page 96.

Dynamic IP Tunnels by Tunnel ID workspace

The Dynamic IP Tunnels by Tunnel ID workspace displays availability and performance statistics for dynamic IP tunnels that match the value specified for the Tunnel ID attribute.

Summary information is displayed in the **Dynamic IP Tunnels with Byte Rate = 0** summary table and the **Dynamic IP Tunnels by Tunnel ID** summary table.

One way to display the Dynamic IP Tunnels by Tunnel ID workspace is to do the following:

1. Right-click the **IP Filters** Navigator item for a specific TCP/IP stack.
2. Select **Workspaces** and select the **Current IP Filters** workspace.
3. Right-click the Link icon by one of the rows of the **Current IP Filters in Scan Order** summary table.
4. If you have selected a filter that is associated with a dynamic IP tunnel, the **Dynamic IP Tunnels by Tunnel ID** conditional link is displayed. This link is available only for filters with a **Type** value of **DYNAMIC**, **NATTDYN** or **NRF**.

Links to Other Workspaces:

The following additional workspaces can be accessed by clicking the Link icon in the Dynamic IP Tunnels With Byte Rate = 0 or the Dynamic IP Tunnels by Tunnel ID summary tables:

- **IKE Tunnels by Tunnel ID** (default): Navigates to the IKE Tunnels By Tunnel ID workspace and displays the IKE tunnel used to activate the selected tunnel.
- **Current IP Filters by Filter Rule Definition Name**: Navigates to the Current IP Filters By Filter Rule Definition Name workspace and displays the IP filter used to activate the selected tunnel.
- **Dynamic IP Tunnels by Destination Address**: Navigates to the Dynamic IP Tunnels By Destination Address workspace and displays tunnels that match the destination IP address you specified in the **Destination Address** dialog box. This dialog box prompts you for a destination IP address that is compared to the currently active tunnels for a TCP/IP stack. This field is filled in by default with the value from the **Destination Address** column for the selected tunnel, but you can change this value to be any IPv4 or IPv6 address. If the Destination Address column is blank, the field will display IP address that matches all addresses. With this address as input, this link navigates to the Dynamic IP tunnels By Destination Address showing the IP tunnels that match the destination IP address that you provided.

Data Source:

z/OS Communication Server Network Management Interface

Default Filter:

The table in this workspace is filtering using the following filters:

- Tunnel ID
- Byte Rate = 0

Figure 14 on page 111 shows the Dynamic IP Tunnels by Tunnel ID workspace.

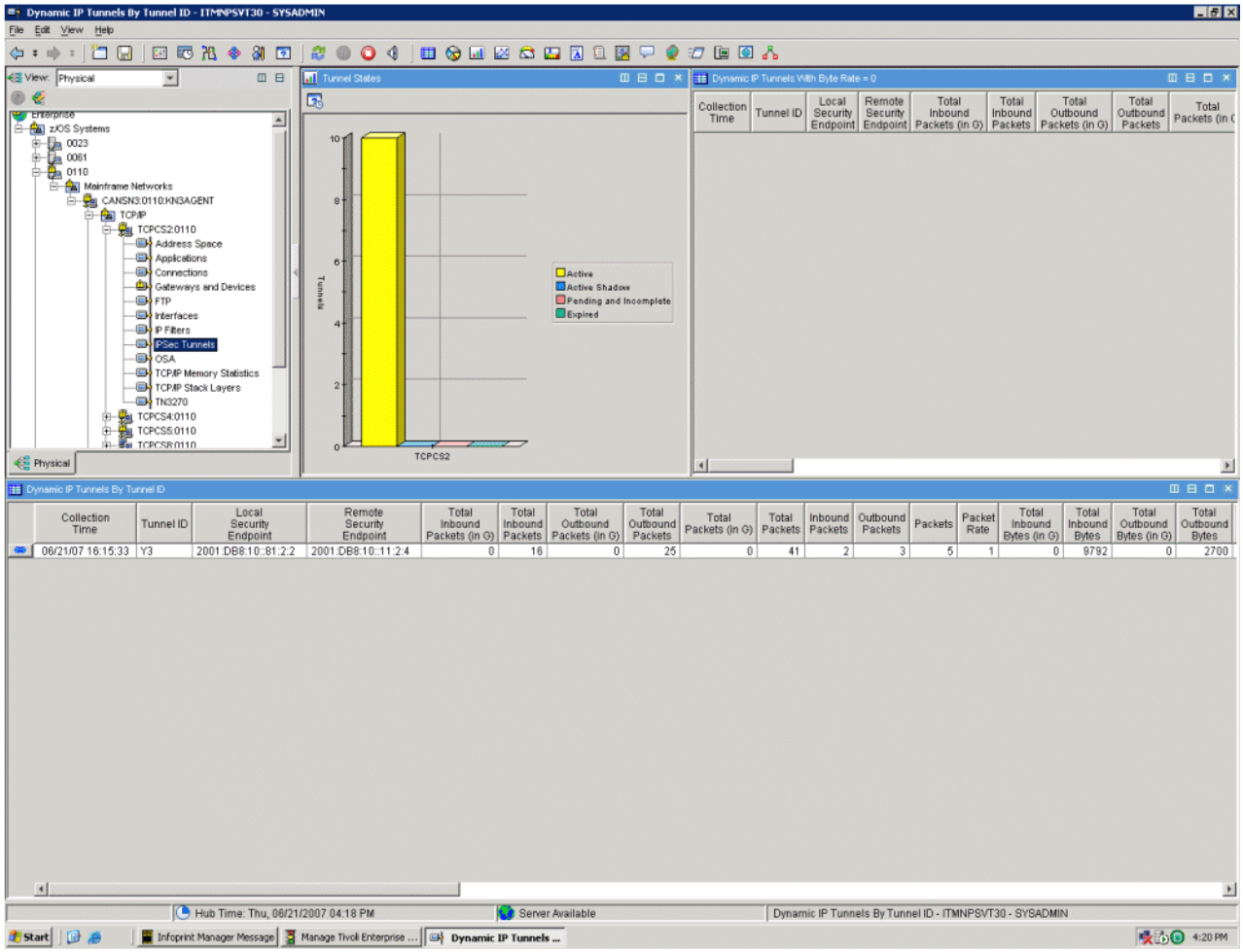


Figure 14. The Tivoli OMEGAMON XE for Mainframe Networks Dynamic IP Tunnels by Tunnel ID workspace

The Dynamic IP Tunnels by Tunnel ID Workspace contains the following views:

- **Tunnel States**: Shows the current number of dynamic IP tunnels in different states for the given TCP/IP stack. The query for this view uses the IPSec status table instead of the Dynamic IP tunnels table. The graph is a bar chart where:
  - Yellow represents the number of Active tunnels.
  - Blue represents the number of Active Shadow (SWSA) tunnels.
  - Pink represents the number of Pending or Incomplete tunnels.
  - Green represents the number of Expired tunnels.
- **Dynamic IP Tunnels with Byte Rate = 0** summary table: Provides performance and configuration information for dynamic IP tunnels that are active and had a byte rate of 0 in the most recent interval. A byte rate of 0 could be indicative of a problem with the tunnel. Each row in the table represents a single dynamic IP tunnel.
- **Dynamic IP Tunnels by Tunnel ID** summary table: Provides performance and configuration data about dynamic IP tunnels that match the tunnel ID passed using the link.

Dynamic IP Tunnels by Tunnel ID attributes: For a complete list of the attributes available in the **Dynamic IP Tunnels with Byte Rate = 0** and **Dynamic IP Tunnels by Tunnel ID** summary tables, and a brief description of each, see the “Dynamic IP Tunnels attributes” on page 96.

Dynamic IP Tunnels with Byte Rate < 2048 workspace

The Dynamic IP Tunnels with Byte Rate < 2048 workspace displays availability and performance statistics for dynamic IP tunnels with a byte rate of less than 2048 bytes.

One way to display the Dynamic IP Tunnels by Destination Address workspace is to do the following:

1. Click the **IPSec Tunnels** Navigator item for a specific TCP/IP stack to access the **Dynamic IP Tunnels Statistics** workspace.
2. Click the Link icon by one of the rows of the **Dynamic IP Tunnels Statistics** summary table.
3. Select the **Dynamic IP Tunnels with Byte Rate < 2048** link.

Links to Other Workspaces:

The following additional workspaces can be accessed by clicking the Link icon in the Dynamic IP Tunnels With Byte Rate = 0 and the Dynamic IP Tunnels by Filter Rule Definition Name summary tables:

- **IKE Tunnels by Tunnel ID** (default): Navigates to the IKE Tunnels By Tunnel ID workspace and displays the IKE tunnel used to activate the selected tunnel.
- **Current IP Filters by Filter Rule Definition Name**: Navigates to the Current IP Filters By Filter Rule Definition Name workspace and displays the IP filter used to activate the selected tunnel.
- **Dynamic IP Tunnels by Destination Address**: Navigates to the Dynamic IP Tunnels By Destination Address workspace and displays tunnels that match the destination IP address you specified in the **Destination Address** dialog box. This dialog box prompts you for a destination IP address that is compared to the currently active tunnels for a TCP/IP stack. This field is filled in by default with the value from the **Destination Address** column for the selected filter, but you can change this value to be any IPv4 or IPv6 address. If the **Destination Address** column is blank, the field will display IP address that matches all addresses. With this address as input, this link navigates to the Dynamic IP Tunnels by Destination Addres showing the IP tunnels that match the destination IP address that you provided.

Data Source:

z/OS Communications Server Network Management Interfaces

Default Filter:

The table in this workspace is filtering using the following attributes:

- Tunnel ID
- Byte Rate < 2048

Figure 15 on page 113 shows the Dynamic IP Tunnels with Byte Rate < 2048 workspace.

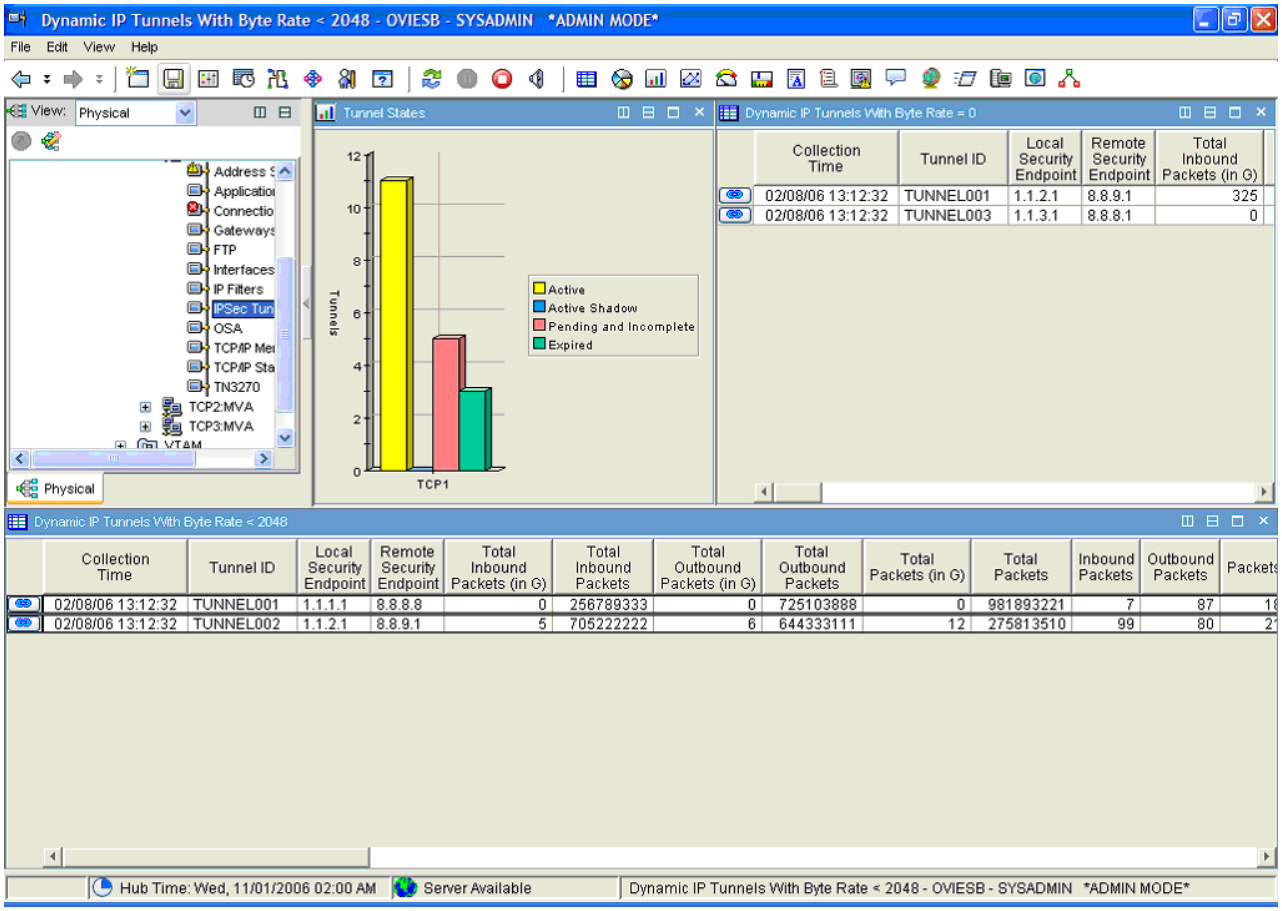


Figure 15. The Tivoli OMEGAMON XE for Mainframe Networks Dynamic IP Tunnels with Byte Rate < 2048 workspace

The Dynamic IP Tunnels with Byte Rate < 2048 workspace displays the following views:

Tunnel States
Shows the current number of dynamic IP tunnels in different states for the given TCP/IP stack. The query for this view uses the IPSec status table instead of the Dynamic IP tunnels table. The graph is a bar chart where:

- Yellow represents the number of Active tunnels.
- Blue represents the number of Active Shadow (SWSA) tunnels.
- Pink represents the number of Pending or Incomplete tunnels.
- Green represents the number of Expired tunnels.

Dynamic IP Tunnels with Byte Rate = 0 summary table
Provides performance and configuration information for dynamic IP tunnels that are active and had a byte rate of 0 in the most recent interval. A byte rate of 0 could be indicative of a problem with the tunnel. Each row in the table represents a single dynamic IP tunnel.

Dynamic IP Tunnels with Byte Rate < 2048 summary table
Provides performance and configuration data about dynamic IP tunnels that had a byte rate of less than 2048 bytes in the most recent interval. Each row in the table represents a single dynamic IP tunnel.

Dynamic IP Tunnels with Byte Rate < 2048 attributes: For a complete list of the attributes available in the **Dynamic IP Tunnels With Byte Rate = 0** and **Dynamic IP Tunnels with Byte Rate < 2048** summary tables, and a brief description of each, see the “Dynamic IP Tunnels attributes” on page 96.

IKE Tunnels Statistics workspace

The IKE Tunnels Statistics workspace displays cumulative availability and performance statistics for all of the IKE tunnels known by the IKE daemon for a TCP/IP stack.

To display the IKE Tunnels Statistic workspace is to right-click the **IPSec Tunnels** Navigator item for a specific TCP/IP stack, select **Workspaces**, and select the **IKE Tunnels Statistics** workspace.

Links to Other Workspaces:

Right-click the IPSec Tunnels navigator item to display the following additional workspaces:

- **IKE Tunnels** (default): Displays availability and performance statistics for IKE tunnels known to the IKE daemon for a specific stack.
- **IKE Tunnels with Byte Rate < 1024:** Displays availability and performance statistics for IKE tunnels with a byte rate of less than 1024 bytes known to the IKE daemon for a specific stack.

Data Source:

z/OS Communications Server Network Management Interface

Default Filter:

None.

Figure 16 shows the IKE Tunnels Statistics workspace.

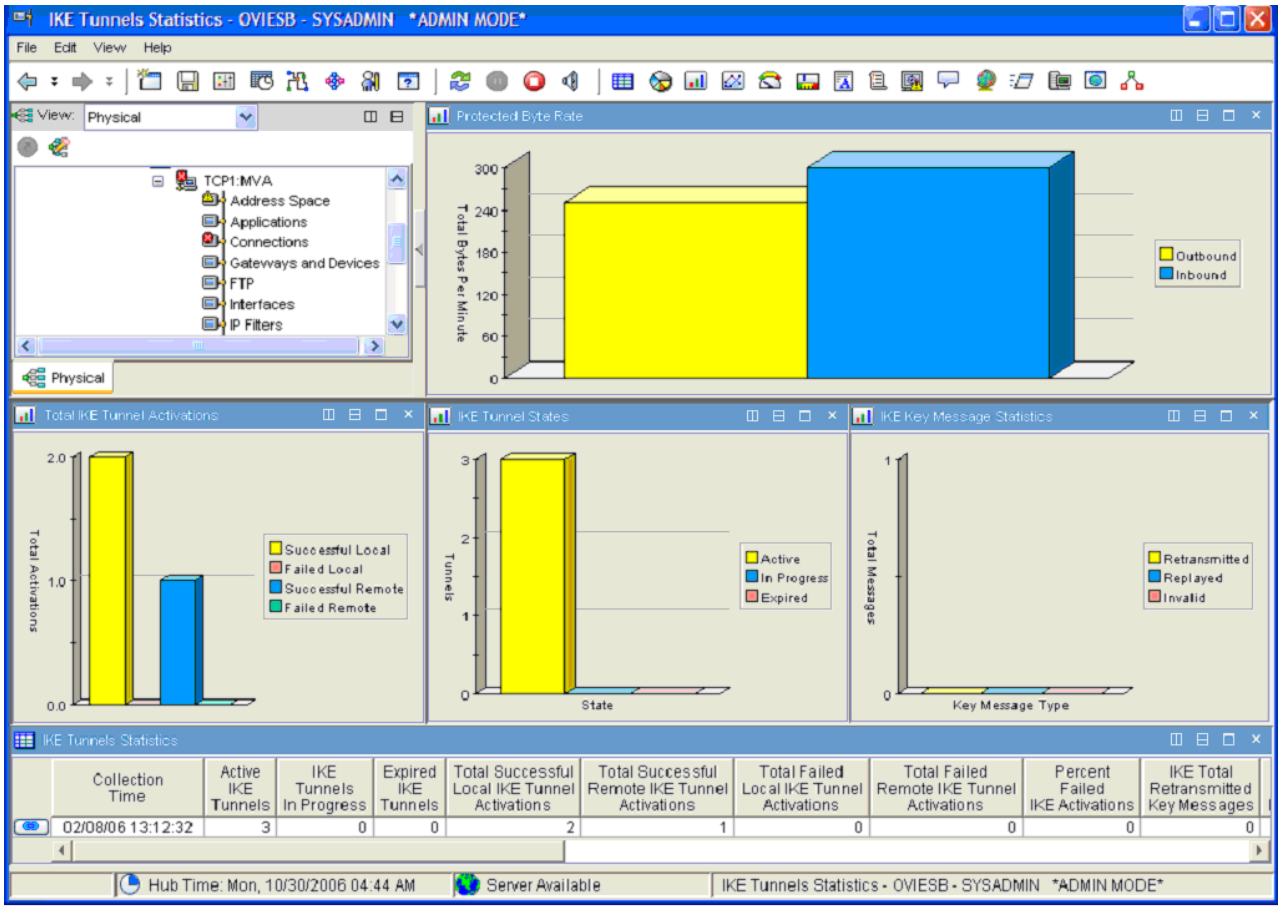


Figure 16. The Tivoli OMEGAMON XE for Mainframe Networks IKE Tunnels Statistics workspace

The IKE Tunnels Statistics workspace displays the following views:

Protected Byte Rate

Shows the rate at which data is flowing through all of the IKE tunnels on the stack. Use this view to determine which tunnels are being used the most. The graph is a bar chart where:

- Yellow represents the number of bytes per minute flowing through outbound IKE tunnels.
- Blue represents the number of bytes per minute flowing through inbound IKE tunnels.

Total IKE Tunnel Activation

Provides a snapshot of the cumulative number of successful and failed IKE tunnel activations since the IKE daemon was started. The bars on the graph differentiate between IKE tunnels that were initiated locally and IKE tunnels that were initiated remotely. The graph is a bar chart where:

- Yellow represents the number of Successful Local tunnel activations.
- Pink represents the number of Failed Local tunnel activations.
- Blue represents the number of Successful Remote tunnel activations.
- Green represents the number of Failed Remote tunnel activations.

IKE Tunnel States

Provides a snapshot of the state of the all the IKE tunnels known by the IKE daemon. The graph is a bar chart where:

- Yellow represents the number of tunnels that are Active.
- Blue represents the number of tunnels that are In Progress (either pending or in negotiation).
- Pink represents the number of tunnels that are Expired.

IKE Key Message Statistics

Provides statistics about key exchange messages that are used to activate IKE tunnels between security endpoints. High number of key exchange messages could indicate that a problem exists. The graph is a bar chart where:

- Yellow represents the number of key exchange messages that were Retransmitted.
- Blue represents the number of key exchange messages that were Replayed.
- Pink represents the number of key exchange messages that were Invalid.

A high number of retransmitted or replayed messages over several collection intervals may indicate a problem in the network between the two security endpoints. Invalid messages may indicate an attack or an incompatibility between the security endpoints.

IKE Tunnels Statistics summary table

Provides performance and configuration data about all IKE tunnels known by the IKE daemon for a TCP/IP stack.

IKE Tunnels Statistics attributes

The following attributes are displayed in the IKE Tunnels Statistics summary table:

Collection Time

The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Active IKE Tunnels
The number of Internet Key Exchange (IKE) tunnels that are currently active. The format is an integer.

IKE Tunnels in Progress
The number of Internet Key Exchange (IKE) tunnels currently in progress. The format is an integer where:

- 0 means PENDING
- 1 means IN NEGOTIATION

Expired IKE Tunnels
The number of Internet Key Exchange (IKE) tunnels that are currently expired. The format is an integer

Total Successful Local IKE Tunnel Activations
The cumulative number of successful locally initiated Internet Key Exchange (IKE) tunnel activations since the IKE daemon was started. The format is an integer.

Total Successful Remote IKE Tunnel Activations
The cumulative number of successful Internet Key Exchange (IKE) tunnel activations that were initiated locally or remotely since the IKE daemon was started. The format is an integer.

Total Failed Local IKE Tunnel Activations
The cumulative number of failed Internet Key Exchange (IKE) tunnel activations that were initiated locally since the IKE daemon was started. The format is an integer.

Total Failed Remote IKE Tunnel Activations
The cumulative number of failed remote Internet Key Exchange (IKE) tunnel activations since the IKE daemon was started. The format is an integer.

IKE Total Retransmitted Key Messages
The cumulative number of failed remote Internet Key Exchange (IKE) tunnel activations since the IKE daemon was started. The format is an integer.

IKE Total Replayed Key Messages
The cumulative number of replayed key exchange (phase 1) messages received since the Internet Key Exchange (IKE) daemon was started. The format is an integer.

IKE Total Invalid Key Messages
Cumulative number of invalid key exchange (phase 1) messages received since the Internet Key Exchange (IKE) daemon was started. This does not include message authentication failures. The format is an integer.

IKE Total Key Message Authentication Failures
The cumulative number of key exchange (phase 1) message authentication failures since the Internet Key Exchange (IKE) daemon was started. The format is an integer.

IKE Total Outbound Bytes Protected (in G)
The cumulative number of outbound bytes of IKE traffic protected by dynamic tunnels since the start of the IKE daemon, divided by 1,073,741,824. The value in this column can be multiplied by

1,073,741,824 and added to the value in the IKE Outbound Bytes Protected column to calculate the cumulative number of IKE outbound bytes protected. The format is an integer.

IKE Total Outbound Bytes Protected
The cumulative number of outbound bytes of IKE traffic protected by IKE tunnels since the IKE daemon was started. The value in this column can be added to the product of 1,073,741,824 and the value in the IKE Outbound Bytes Protected (in G) column to calculate the cumulative number of IKE Outbound Bytes Protected. The format is an integer

IKE Outbound Bytes Protected
The number of outbound bytes protected by Internet Key Exchange (IKE) tunnels in the last interval. The format is an integer.

IKE Outbound Protected Byte Rate
The number of outbound bytes flowing through Internet Key Exchange (IKE) tunnels every minute. The format is an integer.

IKE Total Inbound Bytes Protected (in G)
The cumulative number of inbound bytes of IKE traffic protected by dynamic tunnels since the start of the IKE daemon, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the IKE Inbound Bytes Protected column to calculate the cumulative number of IKE inbound bytes protected. The format is an integer.

IKE Total Inbound Bytes Protected
The cumulative number of inbound bytes of IKE traffic protected by IKE tunnels since the IKE daemon was started. The value in this column can be added to the product of 1,073,741,824 and the value in the IKE Inbound Bytes Protected (in G) column to calculate the cumulative number of IKE Inbound Bytes Protected. The format is an integer.

IKE Inbound Bytes Protected
The number of inbound bytes protected by IKE tunnels in the last interval. The format is an integer.

IKE Inbound Protected Byte Rate
The number of inbound bytes flowing through Internet Key Exchange (IKE) tunnels every minute. The format is an integer.

IKE Tunnels workspace

The Internet Key Exchange (IKE) Tunnels workspace displays availability and performance statistics for IKE tunnels known to the IKE daemon for a specific stack. IKE tunnels are used by a security endpoint (IKE daemon) to negotiate dynamic IP tunnels. Since there could be thousands of IKE tunnels this workspace has a predefined default filter when initially opened. The query used to initially open the workspace will request IKE tunnels with a byte rate >= 1024.

One way to display the IKE Tunnels workspace, right-click the **IPSec Tunnels** Navigator item for a specific TCP/IP stack is to select **Workspaces** and select the **IKE Tunnels** workspace.

Summary information is displayed in the IKE Tunnels summary tables.

Links to Other Workspaces:
The following can be accessed by clicking the Link icon in the **IKE Tunnels with Byte Rate >= 1024** summary table:

- **IKE Tunnels by Security Endpoint Workspace** (default): Navigates to the IKE Tunnels By Security Endpoint workspace and displays the IKE tunnels matching the remote security endpoint of the IKE tunnels you would like displayed. When you select the link to the IKE Tunnels By Security Endpoint workspace, a dialog box prompts you to identify the remote security endpoint of the tunnels you would like displayed. This value is requested: .
  - Remote Security Endpoint: The IP address of the remote security endpoint. This may be an IPv4 address in dotted decimal notation or an IPv6 address in colon hexadecimal notation

Entries in the stored table are compared to the values provided in the dialog box. All entries in the table that match are displayed in the table view requested.

Data Source:

z/OS Communications Server Network Management Interface

Default Filter:

The table in this workspace is filtering using the Byte Rate >= 1024 attribute.

Figure 17 shows the IKE Tunnels workspace.

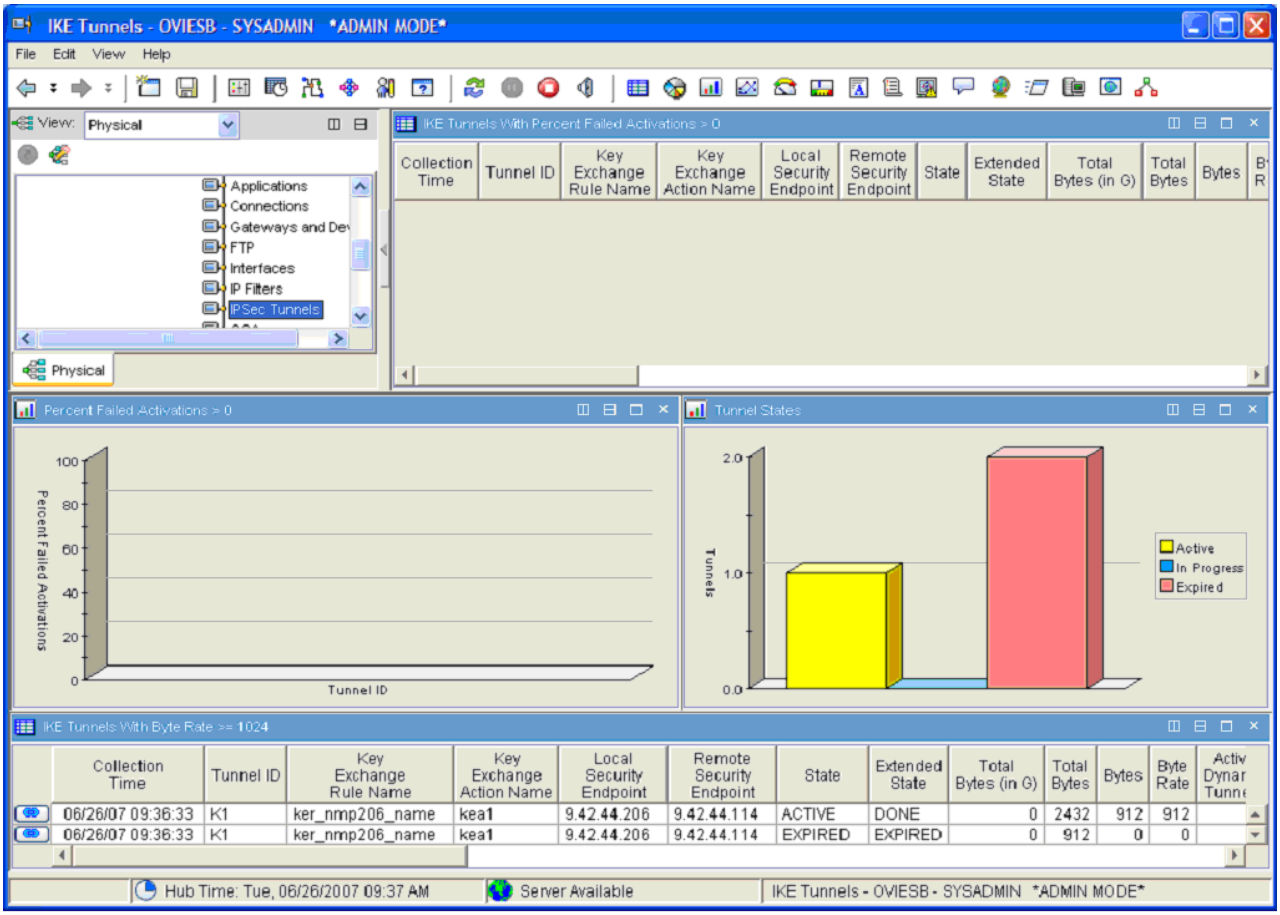


Figure 17. The Tivoli OMEGAMON XE for Mainframe Networks IKE Tunnels workspace

The IKE Tunnels workspace displays the following views:

IKE Tunnels with Percent Failed Activations > 0 summary table

Displays performance and configuration information for IKE tunnels that are experiencing failures when activating dynamic IP tunnels. No links are available from this view.

Percent Failed Activations > 0

Shows IKE tunnels that have experienced dynamic tunnel activation failures. This bar chart shows the percentage of dynamic tunnel activations that have failed by Tunnel ID.

Tunnel States

Shows the current number of IKE tunnels in different states for the given TCP/IP stack. The query for this view uses the IPSec statistics table instead of the IKE Tunnels table. The graph is a bar chart where:

- Yellow represents the number of tunnels in an Active state.

- Blue represents the number of tunnels in an In Progress state.
- Pink represents the number of tunnels in an Expired state.

IKE Tunnels with Byte Rate >= 1024 summary table
Displays performance and configuration data about the IKE tunnels with a byte rate greater than or equal to 1024. Each row in the table represents a single IKE tunnel. The data in this table can be filtered based on criteria that you provide.

IKE Tunnels attributes: The following attributes are displayed in the **IKE Tunnels with Percent Failed Activations > 0** and **IKE Tunnels with Byte Rate >= 1024** summary tables:

Collection Time
The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss
```

Where:
- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:
- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Tunnel ID
Tunnel identifier. This identifier is generated by the Internet Key Exchange (IKE) daemon and is not unique. Multiple related tunnels may have the same tunnel ID. This value is a character string of up to 48 characters.

Key Exchange Rule Name
The name specified on a z/OS Communications Server Policy Agent KeyExchangeRule configuration statement. This name identifies the rule being used to activate this Internet Key Exchange (IKE) tunnel. Key exchange rules identify the security endpoints for an IKE tunnel and the policy to be used for the tunnel by referencing a key exchange action. This field is stored as a 48-character string.

Key Exchange Action Name
The name specified on a z/OS Communications Server Policy Agent KeyExchangeAction configuration statement. This name identifies the action being used to activate this Internet Key Exchange (IKE) tunnel. Key exchange actions describe how key exchanges between security endpoints should be protected. This field is stored as a 48-character string.

Local Security Endpoint
The IP address of the local security endpoint (IKE) responsible for negotiating the tunnel. The format is a character string of up to 45 characters.

Remote Security Endpoint
The IP address of the remote security endpoint (IKE) responsible for negotiating the tunnel. The format is a character string of up to 45 characters.

Initiator Cookie
A string of hexadecimal digits that, when combined with the Responder Cookie, uniquely identifies the SA for the tunnel. This value is stored as a 16-character string. This field is not displayed.

Responder Cookie
A string of hexadecimal digits that, when combined with the Initiator Cookie, uniquely identifies the SA for the tunnel. This value is stored as a 16-character string. This field is not displayed.

State Current state of the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 3 = INCOMPLETE: Tunnel negotiation is in progress.
- 4 = ACTIVE: Tunnel is active and ready for use.
- 5 = EXPIRED: Tunnel has expired and cannot be used.

Extended State
Indicates the progress of the tunnel negotiation. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = INIT: No key exchange messages have been initiated.
- 1 = WAIT_SA: The first key exchange message has been sent and the endpoint is waiting for a response.
- 2 = IN_KE: A key exchange response has been sent.
- 3 = WAIT_KE: A key exchange message has been sent and the endpoint is waiting on a response.
- 4 = DONE: All key exchange messages have been completed and the tunnel is ready for data traffiic.
- 5 = EXPIRED: Tunnel has exceeded its life time or life size and is not available for data traffic.

Total Bytes (in G)
The cumulative number of bytes protected by this tunnel since the tunnel was activated, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,823 and added to the value in the Total Bytes column to calculate the total bytes for the tunnel. The format is an integer.

Total Bytes
The cumulative number of bytes protected by this tunnel since the tunnel was activated. The value in this column can be added to the product of 1,073,741,823 and the value in the Total Bytes (in G) column to calculate the total bytes for the tunnel. The format is an integer.

Bytes The number of bytes protected by this tunnel during the most recent time interval. The format is an integer.

Byte Rate
The number of bytes protected, per minute, for this tunnel during the most recent time interval. The format is an integer.

Active Dynamic Tunnels
Current count of active dynamic tunnels associated with this Internet Key Exchange (IKE) tunnel. The format is an integer.

In Progress Dynamic Tunnels
Current count of in-progress dynamic tunnels associated with this Internet Key Exchange (IKE) tunnel. The format is an integer.

Percent In Progress Dynamic Tunnels
The percentage of dynamic tunnels in progress compared to active dynamic tunnels. The format is a number between 0 and 100 inclusive.

Percent Failed Activations
The percent of dynamic tunnel activations that have failed for this Internet Key Exchange (IKE) tunnel. The format is a number between 0 and 100 inclusive.

Total Successful Local Activations
The cumulative count of successful locally initiated dynamic tunnel activations for this Internet Key Exchange (IKE) tunnel. The format is an integer.

Total Successful Remote Activations
The cumulative count of successful remotely initiated dynamic tunnel activations for this Internet Key Exchange (IKE) tunnel. The format is an integer.

Total Failed Local Activations
The cumulative count of failed locally initiated dynamic tunnel activations for this Internet Key Exchange (IKE) tunnel. The format is an integer.

Total Failed Remote Activations
The cumulative count of failed remotely initiated dynamic tunnel activations for this Internet Key Exchange (IKE) tunnel. The format is an integer.

Exchange Mode
Exchange mode used by a tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 2 = MAIN
- 4 = AGGRESSIVE

Role Role of the local security endpoint in the activation of the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = INITIATOR
- 2 = RESPONDER

Authentication Algorithm
The authentication algorithm used for this tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 38 = MD5
- 39 = SHA1

Encryption Algorithm
Encryption algorithm used by the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 3 = 3DES
- 12 = AES
- 18 = DES

Diffie Hellman Group
Diffie-Hellman group used to generate keying material for the tunnel. Each group identifies the number of bits to be used in a prime number that is used to generate keying material. This column is blank if PFS (perfect forward security) was not negotiated for the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = NONE
- 1 = GROUP1
- 2 = GROUP2
- 5 = GROUP5
- 14 = GROUP14

Peer Authentication Method

Peer authentication method. This value is stored as an integer and displayed as a string. Valid values are:

- 3 = PRESHAREDKEY
- 2 = RSASIGNATURE

Life Size

The number of bytes of data that may traverse the tunnel over the life of the tunnel. This value is 0 if no life size was negotiated for the tunnel. The format is an integer.

Life Time

The amount of time, in seconds, that the tunnel is to remain active. The format is an integer.

Life Refresh Time

The time at which the tunnel is refreshed. This column is blank if no life time was negotiated. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Life Expiration Time

The time at which the tunnel will expire. This column is blank if no life time was negotiated. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)

- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Remote IKE UDP Port
Remote UDP port used for Internet Key Exchange (IKE) negotiations. This column is stored as a 5-character string.

NAT Traversal Indicator
Indicates if the network address translation (NAT) traversal function is enabled for the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

NAT Traversal Support Level
Indicates the type of network address translation (NAT) traversal support being used. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = NONE: No NAT traversal support. Support is either not configured or not negotiated.
- 1 = RFCD2: RFC 3947 draft 2 support.
- 3 = RFCD3: RFC 3947 draft 3 support.
- 4 = RFC: RFC 3947 support with non-z/OS peer.
- 5 = ZOS: RFC 3947 support with z/OS peer.

Local NAT Indicator
Indicates if network address translation (NAT) has been detected in front of the local security endpoint. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Remote NAT Indicator
Indicates if a NAT has been detected in front of the remote security endpoint. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Remote NAPT Indicator
Indicates if a network address port translation (NAPT) has been detected in front of the remote security endpoint. It is possible that a NAPT may exist but is detected only as a NAT. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Initiation Indicator
Indicates if the local security endpoint may initiate Internet Key Exchange (IKE) tunnel negotiations with the remote security endpoint. Either security endpoint may initiate refreshes regardless of the value of this indicator. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = Yes

Local Security Endpoint ID Type

Internet Security Associations Key Management Protocol (ISAKMP) identity type for the local security endpoint as defined in RFC 2407. If client IDs were not exchanged during negotiation, this column is blank. ISAKMP peers exchange and verify each other's identities as part of the Internet Key Exchange (IKE) tunnel (Phase 1) negotiation. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = IPv4_ADDR
- 2 = FQDN
- 3 = USER_FQDN
- 4 = IPv4_ADDR_SUBNET
- 5 = IPv6_ADDR
- 6 = IPv6_ADDR_SUBNET
- 7 = IPv4_ADDR_RANGE
- 8 = IPv6_ADDR_RANGE
- 9 = DER_ASN1_DN
- 10 = DER_ASN1_GN
- 11 = KEY_ID

This field is not displayed.

Local Security Endpoint ID

Internet Security Associations Key Management Protocol (ISAKMP) identity of local security endpoint. This field is a string containing an identifier, as described by local security endpoint ID type. Some ID strings can be as long as 2048 characters. The ID is always truncated at 100 characters. If no IDs are exchanged, this field is stored as blanks. This field is not displayed.

Remote Security Endpoint ID Type

Internet Security Associations Key Management Protocol (ISAKMP) identity type for the remote security endpoint as defined in RFC 2407. If client IDs were not exchanged during negotiation, this column is blank. ISAKMP peers exchange and verify each other's identities as part of the Internet Key Exchange (IKE) tunnel (Phase 1) negotiation. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = IPv4_ADDR
- 2 = FQDN
- 3 = USER_FQDN
- 4 = IPv4_ADDR_SUBNET
- 5 = IPv6_ADDR
- 6 = IPv6_ADDR_SUBNET
- 7 = IPv4_ADDR_RANGE
- 8 = IPv6_ADDR_RANGE
- 9 = DER_ASN1_DN
- 10 = DER_ASN1_GN
- 11 = KEY_ID

This field is not displayed.

Remote Security Endpoint ID

Internet Security Associations Key Management Protocol (ISAKMP) identity of remote security endpoint. This field is a string containing an identifier, as described by remote security endpoint ID

type. Some ID strings can be as long as 2048 characters. The ID is always truncated at 100 characters. If no IDs are exchanged, this field is stored as blanks. This field is not displayed.

IP Address Version

The version of the IP addresses being used for the security endpoints.This value is stored as an integer and displayed as a string. Valid values are:

- 0 = IPv4: The traffic descriptor and the security endpoints are using IPv4 addresses.
- 1 = IPv6: The traffic descriptor and the security endpoints are using IPv6 addresses.

This value is not displayed.

IKE Tunnels by Security Endpoint Workspace

The Internet Key Exchange (IKE) Tunnels by Security Endpoint workspace displays availability and performance statistics for IKE tunnels known to the IKE daemon for the specified remote security endpoint. IKE tunnels are used by a security endpoint (IKE daemon) to negotiate dynamic IP tunnels.

One way to display the IKE Tunnels by Security Endpoint workspace is to do the following:

1. Right-click the **IPSec Tunnels** Navigator item for a specific TCP/IP stack.
2. Select **Workspaces** and select the **IKE Tunnels** workspace.
3. Click the Link icon by one of the rows of the **IKE Tunnels With Byte Rate >= 1024** summary table.
4. Select the **IKE Tunnels by Security Endpoint** link.

Summary information is displayed in the IKE Tunnels summary tables.

Links to Other Workspaces:

The following additional workspace can be accessed by right-clicking the Link icon in the IKE Tunnels by Security Endpoint summary table:

- **IKE Tunnels by Security Endpoint Workspace** (default): Navigates to the IKE Tunnels By Security Endpoint workspace and displays the IKE tunnels matching the remote security endpoint of the IKE tunnels you would like displayed. When you select the link to the IKE Tunnels By Security Endpoint workspace, a dialog box prompts you to identify the remote security endpoint of the tunnels you would like displayed. This value is requested: .
  - Remote Security Endpoint: The IP address of the remote security endpoint. This may be an IPv4 address in dotted decimal notation or an IPv6 address in colon hexadecimal notation

  Entries in the stored table are compared to the values provided in the dialog box. All entries in the table that match are displayed in the table view requested.

Data Source:

z/OS Communications Server Network Management Interface

Default Filter:

The table in this workspace is filtering using the specified local or remote security endpoint.

Figure 18 on page 126 shows the IKE Tunnels by Security Endpoint workspace.

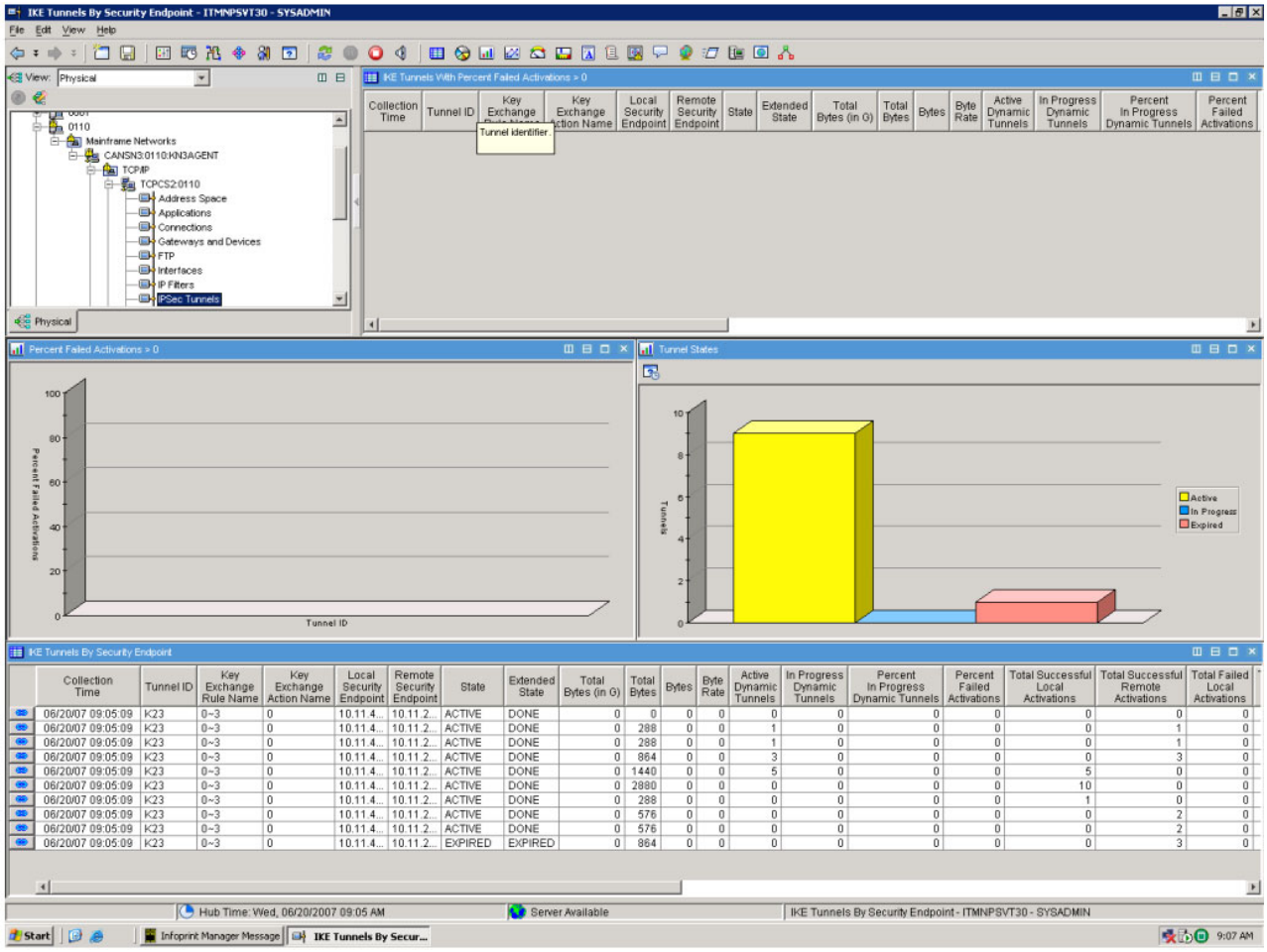


Figure 18. The Tivoli OMEGAMON XE for Mainframe Networks IKE Tunnels by Security Endpoint workspace

The IKE Tunnels IKE Tunnels by Security Endpoint workspace displays the following views:

IKE Tunnels with Percent Failed Activations > 0 summary table
Displays performance and configuration information for IKE tunnels that are experiencing failures when activating dynamic IP tunnels.

Percent Failed Activations > 0
Shows tunnels that have experienced dynamic tunnel activation failures. This bar chart shows the percentage of dynamic tunnel activations that have failed by Tunnel ID.

Tunnel States
Shows the current number of IKE tunnels in different states for the given TCP/IP stack. The query for this view uses the IPSec statistics table instead of the IKE Tunnels table. The graph is a bar chart where:

- Yellow represents the number of tunnels in an Active state.
- Blue represents the number of tunnels in an In Progress state.
- Pink represents the number of tunnels in an Expired state.

IKE Tunnels By Security Endpoint summary table
Provides performance and configuration data about the IKE tunnels known to the IKE daemon for the specified security endpoints.

IKE Tunnels by Security Endpoint attributes: For a complete list of the attributes available in the **IKE Tunnels with Percent Failed Activations > 0** and **IKE Tunnels By Security Endpoint** summary tables, and a brief description of each, see the "IKE Tunnels attributes" on page 119.

IKE Tunnels by Tunnel ID Workspace

The IKE Tunnels by Tunnel ID workspace displays availability and performance statistics for IKE tunnels with a tunnel ID that matches the one passed by the link. IKE tunnels are used by a security endpoint (IKE daemon) to negotiate dynamic IP tunnels.

To display the IKE Tunnels by Tunnel ID workspace, do the following:

1. Right-click the **IPSec Tunnels** Navigator item for a specific TCP/IP stack.
2. Select **Workspaces** and select the **Dynamic IP Tunnels** workspace.
3. Click the Link icon by one of the rows of the **Dynamic IP Tunnels With Byte Rate >= 2048** or **Dynamic IP Tunnels With Byte Rate = 0** summary tables.
4. Select the **IKE Tunnels by Tunnel ID** link.

Summary information is displayed in the IKE Tunnels summary tables.

Links to Other Workspaces:

The following additional workspace can be accessed by clicking the Link icon in the IKE Tunnels by Tunnel ID summary table:

- **IKE Tunnels by Security Endpoint Workspace** (default): Navigates to the IKE Tunnels By Security Endpoint workspace and displays the IKE tunnels matching the remote security endpoint of the IKE tunnels you would like displayed. When you select the link to the IKE Tunnels By Security Endpoint workspace, a dialog box prompts you to identify the remote security endpoint of the tunnels you would like displayed. This value is requested: .
  - Remote Security Endpoint: The IP address of the remote security endpoint. This may be an IPv4 address in dotted decimal notation or an IPv6 address in colon hexadecimal notation

  Entries in the stored table are compared to the values provided in the dialog box. All entries in the table that match are displayed in the table view requested.

Data Source:

z/OS Communications Server Network Management Interface

Default Filter:

The table in this workspace is filtering using the Tunnel ID attribute.

Figure 19 on page 128 shows the IKE Tunnels by Tunnel ID workspace.

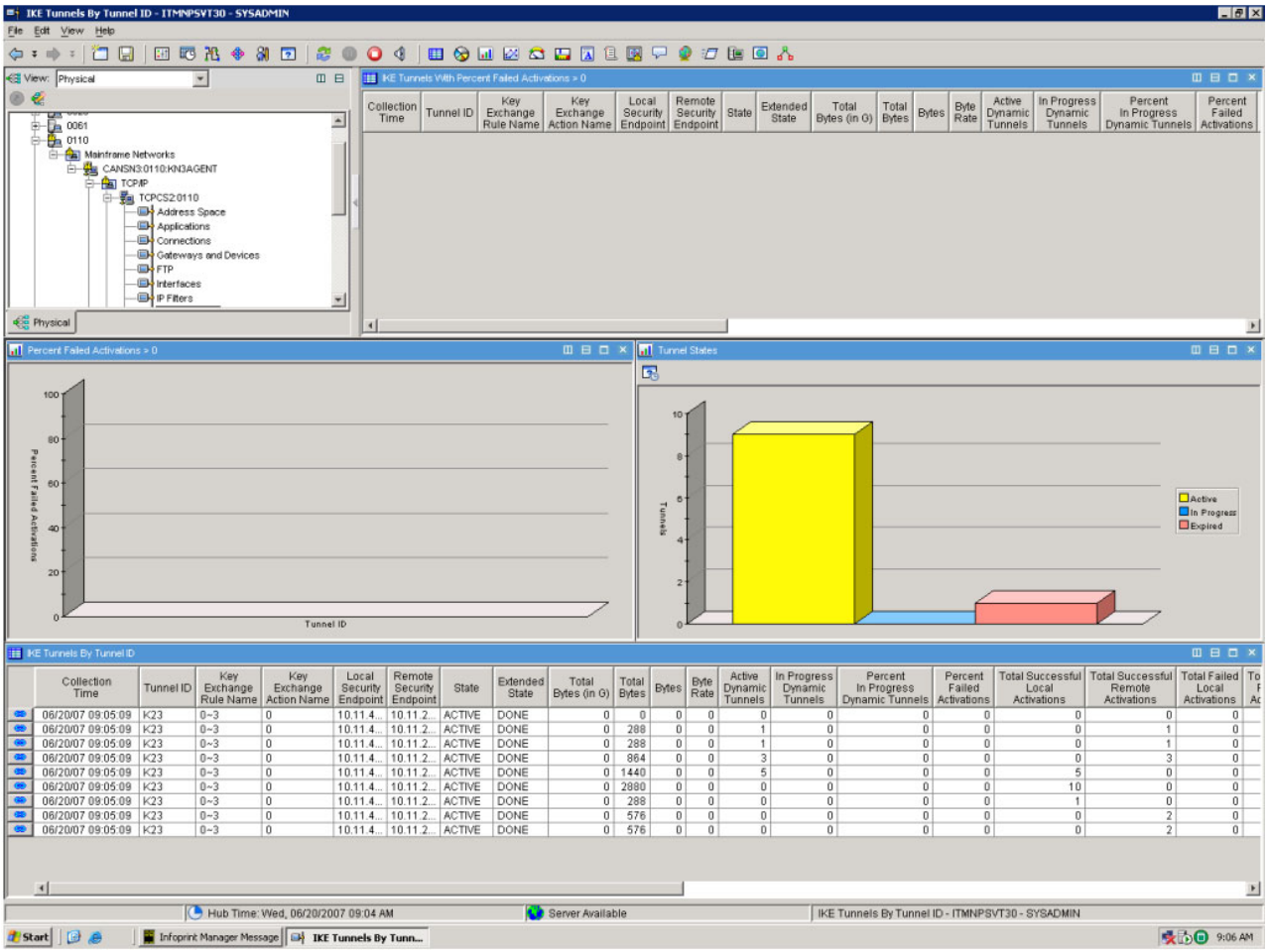


Figure 19. The Tivoli OMEGAMON XE for Mainframe Networks IKE Tunnels by Tunnel ID workspace

The IKE Tunnels IKE Tunnels by Tunnel ID workspace displays the following views:

IKE Tunnels with Percent Failed Activations > 0 summary table
Displays performance and configuration information for IKE tunnels that are experiencing failures when activating dynamic IP tunnels.

Percent Failed Activations > 0
Shows tunnels that have experienced dynamic tunnel activation failures. This bar chart shows the percentage of dynamic tunnel activations that have failed by Tunnel ID.

Tunnel States
Shows the current number of IKE tunnels in different states for the given TCP/IP stack. The query for this view uses the IPSec statistics table instead of the IKE Tunnels table. The graph is a bar chart where:

- Yellow represents the number of tunnels in an Active state.
- Blue represents the number of tunnels in an In Progress state.
- Pink represents the number of tunnels in an Expired state.

IKE Tunnels by Tunnel ID summary table
Displays availability and performance statistics for IKE tunnels with a tunnel ID that matches the one passed by the link. IKE tunnels are used by a security endpoint (IKE daemon) to negotiate dynamic IP tunnels.

IKE Tunnels by Tunnel ID attributes: For a complete list of the attributes available in the **IKE Tunnels with Percent Failed Activations > 0** and **IKE Tunnels by Tunnel ID** summary tables, and a brief description of each, see the "IKE Tunnels attributes" on page 119.

IKE Tunnels with Byte Rate < 1024 Workspace

The IKE Tunnels with Byte Rate < 1024 workspace displays availability and performance statistics for IKE tunnels with a byte rate of less than 1024 bytes known to the IKE daemon for a specific stack. IKE tunnels are used by a security endpoint (IKE daemon) to negotiate dynamic IP tunnels. A low byte rate could be indicative of a problem and this workspace allows users to examine information about IKE tunnels with lower byte rates. This view may be used to see if there is a large number of expired IKE tunnels using up system resources.

One way to display the IKE Tunnels workspace is to right-click the **IPSec Tunnels** Navigator item for a specific TCP/IP stack, select **Workspaces** and select the **IKE Tunnels with Byte Rate < 1024** workspace.

Links to Other Workspaces:

The following additional workspace can be accessed by clicking the Link icon in the IKE Tunnels With Percent Failed Activations > 0 summary table:

- **IKE Tunnels by Security Endpoint Workspace** (default): Navigates to the IKE Tunnels By Security Endpoint workspace and displays the IKE tunnels matching the remote security endpoint of the IKE tunnels you would like displayed. When you select the link to the IKE Tunnels By Security Endpoint workspace, a dialog box prompts you to identify the remote security endpoint of the tunnels you would like displayed. This value is requested: .
  - Remote Security Endpoint: The IP address of the remote security endpoint. This may be an IPv4 address in dotted decimal notation or an IPv6 address in colon hexadecimal notation

  Entries in the stored table are compared to the values provided in the dialog box. All entries in the table that match are displayed in the table view requested.

Data Source:

z/OS Communications Server Network Management Interface

Default Filter:

The table in this workspace is filtering using the Byte Rate < 1024 attribute.

Figure 20 on page 130 shows the IKE Tunnels with Byte Rate < 1024 workspace.

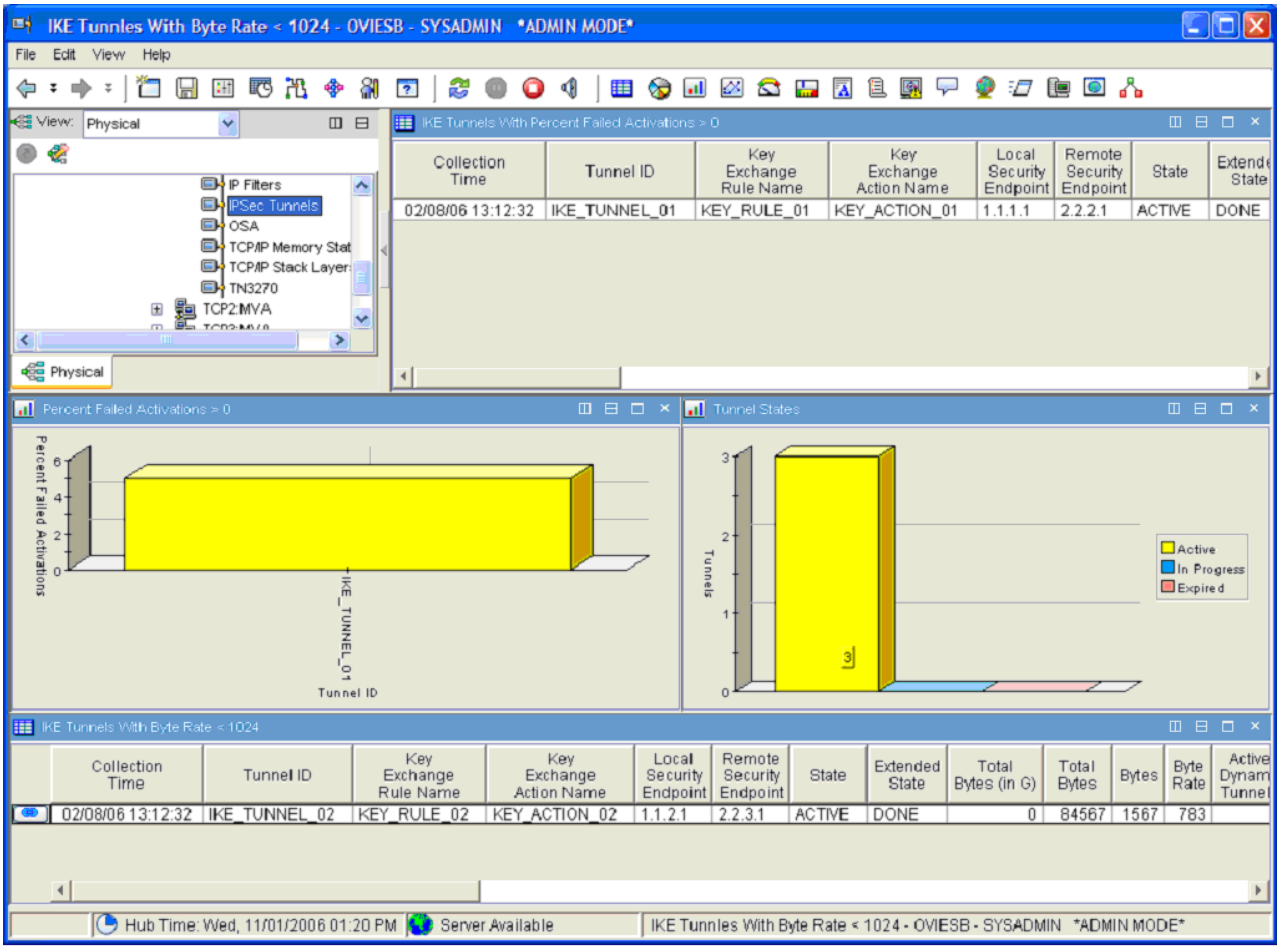


Figure 20. The Tivoli OMEGAMON XE for Mainframe Networks IKE Tunnels with Byte Rate < 1024 workspace

The IKE Tunnels with Byte Rate < 1024 workspace displays the following views:

IKE Tunnels with Percent Failed Activations > 0 summary table
Displays performance and configuration information for IKE tunnels that are experiencing failures when activating dynamic IP tunnels.

Percent Failed Activations > 0
Shows IKE tunnels that have experienced dynamic tunnel activation failures. This bar chart shows the percentage of dynamic tunnel activations that have failed by Tunnel ID.

Tunnel States
Shows the current number of IKE tunnels in different states for the given TCP/IP stack. The query for this view uses the IPSec statistics table instead of the IKE Tunnels table. The graph is a bar chart where:

- Yellow represents the number of tunnels in an Active state.
- Blue represents the number of tunnels in an In Progress state.
- Pink represents the number of tunnels in an Expired state.

IKE Tunnels with Byte Rate < 1024 summary table
Displays performance and configuration data about the IKE tunnels with byte rates less than 1024 bytes. Each row in the table represents a single IKE tunnel. The data in this table can be filtered based on criteria that you provide.

IKE Tunnels with Byte Rate < 1024 attributes: For a complete list of the attributes available in the **IKE Tunnels with Percent Failed Activations > 0** and **IKE Tunnels with Byte Rate < 1024** summary table summary tables, and a brief description of each, see the “IKE Tunnels attributes” on page 119.

Manual IP Tunnels workspace

The Manual IP Tunnels workspace displays availability and performance statistics for manual IP tunnels known to a specific TCP/IP stack.

One way to display the Manual IP Tunnels workspace is to right-click the **IPSec Tunnels** Navigator item for a specific TCP/IP stack, select **Workspaces** and select the **Manual IP Tunnels** link.

Links to Other Workspaces:
None.

Data Source:
z/OS Communication Server Network Management Interface

Default Filter:
None.

Figure 21 shows the Manual IP Tunnels workspace.

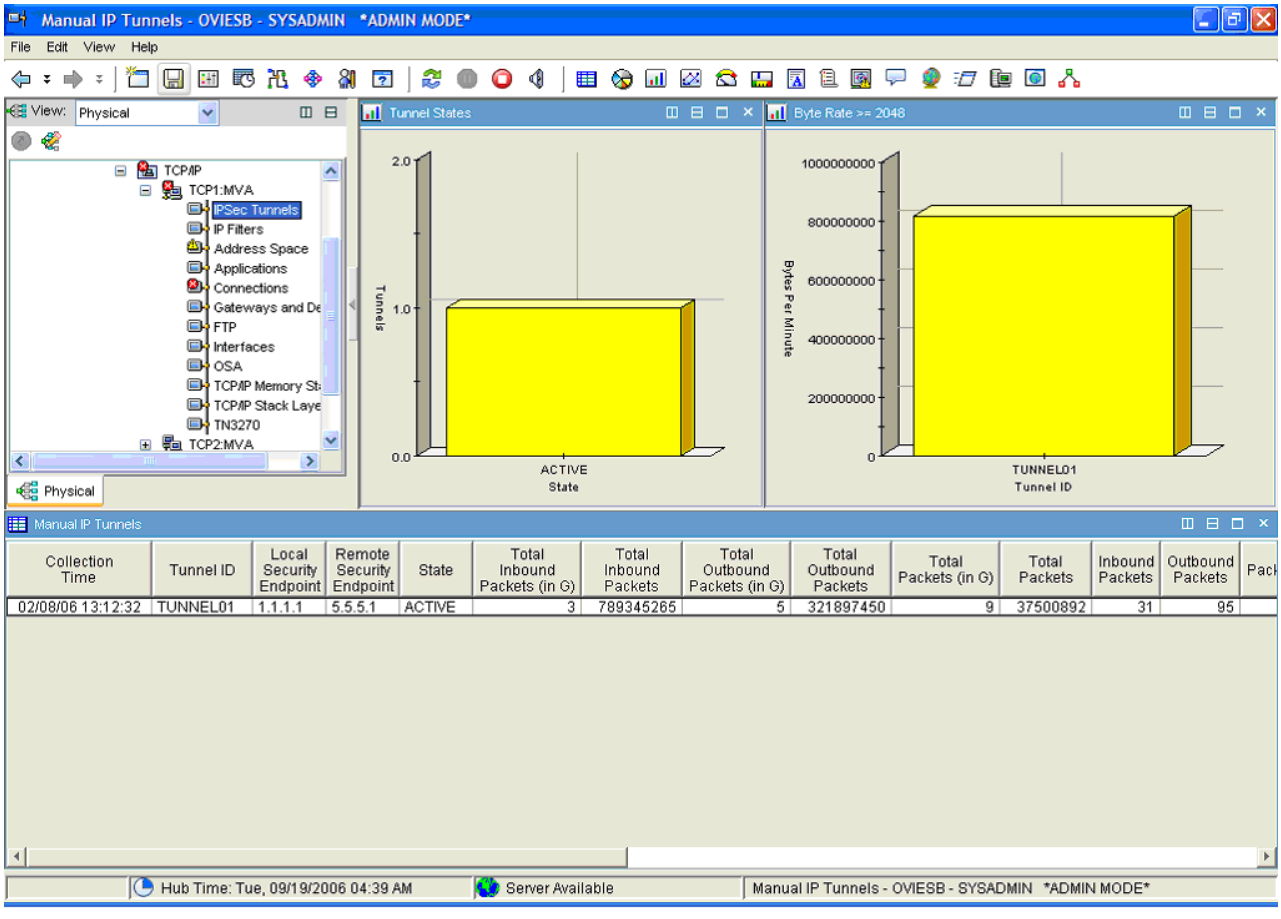


Figure 21. The Tivoli OMEGAMON XE for Mainframe Networks Manual IP Tunnels workspace

The Manual IP Tunnels workspace displays the following views:

Tunnel States
Provides a snapshot of the current number of manual tunnels in different states for the given TCP/IP stack. Each bar in the graph represents the number of tunnels in a particular state. The graph is a bar chart where:

- Yellow represents the number of Active tunnels.
- Blue represents the number of Inactive tunnels.

Byte Rate >= 2048
Shows tunnels that have an inbound or outbound byte rate of 2048 or greater during the most recent collection interval. The bar chart displays number of bytes per minute for each tunnel ID.

Manual IP Tunnels summary table
Provides performance and configuration data about the manual IP tunnels. Each row in the table represents a single manual IP tunnel.

Manual IP Tunnels attributes

The following attributes are displayed in the Manual IP Tunnels summary table:

Collection Time
The time and date of the data sampling. This time is displayed in the following format:

```
mm/dd/yy hh:mm:ss
```

Where:

- mm = Month
- dd = Day of the month
- yy = Year
- hh = Hour
- mm = Minute
- ss = Seconds

The stored format is a string no longer than 16 characters in the format `CYYMMDDHHMMSSmmm` (as in 1020315064501000 for 03/15/02 06:45:01) where:

- C = Century (0 for 20th, 1 for 21st)
- Y = Year
- M = Month
- D = Day
- H = Hour
- M = Minute
- S = Second
- m = Millisecond

Tunnel ID
Tunnel identifier. This identifier is generated by TCP/IP and is not unique. Multiple related tunnels may have the same tunnel ID. The format is an alphanumeric string of up to 48 characters.

Local Security Endpoint
The IP address of the local security endpoint responsible for negotiating the tunnel. The format is an alphanumeric string of up to 45 characters.

Remote Security Endpoint
The IP address of the remote security endpoint responsible for negotiating the tunnel. The format is an alphanumeric string of up to 45 characters.

State Current tunnel state. This value is stored as an integer and displayed as a string. Valid values are:

- 1 = INACTIVE

- 4 = ACTIVE

Total Inbound Packets (in G)
The total number of inbound packets for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Inbound Packets column to calculate the total inbound packets for the tunnel. The format is an integer.

Total Inbound Packets
The total number of inbound packets for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Inbound Packets (in G) column to calculate the total inbound packets for the tunnel. The format is an integer.

Total Outbound Packets (in G)
The total number of outbound packets for this tunnel since the tunnel was established, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,823 and added to the value in the Total Outbound Packets column to calculate the total outbound packets for the tunnel. The format in an integer.

Total Outbound Packets
The total number of outbound packets for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Outbound Packets (in G) column to calculate the total outbound packets for the tunnel. The format is an integer.

Total Packets (in G)
The total number of inbound and outbound packets for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Packets column to calculate the total packets for the tunnel. The format is an integer.

Total Packets
The total number of inbound and outbound packets for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Packets (in G) column to calculate the total packets for the tunnel. The format is an integer.

Inbound Packets
The number of inbound packets for this tunnel during the most recent collection interval. The format is an integer.

Outbound Packets
The number of outbound packets for this tunnel during the most recent collection interval. The format is an integer.

Packets
The number of inbound and outbound packets for this tunnel during the most recent collection interval. The format is an integer.

Packet Rate
The number of inbound or outbound packets, per minute, for this tunnel during the most recent collection interval. The format is an integer.

Total Inbound Bytes (in G)
The total number of inbound bytes for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Inbound Bytes column to calculate the total inbound bytes for the tunnel. The format is an integer.

Total Inbound Bytes
The total number of inbound bytes for this tunnel since the tunnel was installed. The value in this

column can be added to the product of 1,073,741,824 and the value in the Total Inbound Bytes (in G) column to calculate the total inbound bytes for the tunnel. The format is an integer.

Total Outbound Bytes (in G)
The total number of outbound bytes for this tunnel since the tunnel was installed, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,824 and added to the value in the Total Outbound Bytes column to calculate the total outbound bytes for the tunnel. The format is an integer.

Total Outbound Bytes
The total number of outbound bytes for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Outbound Bytes (in G) column to calculate the total outbound bytes for the tunnel. The format is an integer.

Total Bytes (in G)
The total number of inbound and outbound bytes for this tunnel since the tunnel was established, divided by 1,073,741,824. The value in this column can be multiplied by 1,073,741,823 and added to the value in the Total Bytes column to calculate the total bytes for the tunnel. The format is an integer.

Total Bytes
The total number of inbound and outbound bytes for this tunnel since the tunnel was installed. The value in this column can be added to the product of 1,073,741,824 and the value in the Total Bytes (in G) column to calculate the total bytes for the tunnel. The format is an integer.

Inbound Bytes
The number of inbound bytes for this tunnel during the most recent collection interval. The format is an integer.

Outbound Bytes
The number of outbound bytes for this tunnel during the most recent collection interval. The format is an integer.

Bytes The number of inbound and outbound bytes for this tunnel during the most recent collection interval The format is an integer.

Byte Rate
The number of inbound or outbound bytes, per minute, for this tunnel during the most recent collection interval. The format is an integer.

VPN Action Name
The VPN Action Name is the name associated with the definition of a security association. The security association describes the attributes of the tunnel. An example is the encryption algorithm to be used. The name is a character string of up to 48 characters.

Encapsulation Mode
Tunnel encapsulation mode to be used by the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 1 = TUNNEL
- 2 = TRANSPORT

Authentication Protocol
The authentication protocol to be used by the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 51 = AH
- 50 = ESP

Authentication Algorithm

The authentication algorithm used for this tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = <blank>
- 38 = MD5
- 39 = SHA1

Encryption Algorithm

Encryption algorithm to be used by the tunnel. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = NONE
- 3 = 3DES
- 11 = NULL
- 12 = AES
- 18 = DES
- 99 = <blank>

Inbound Authentication SPI

Tunnel inbound authentication security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This is an unsigned 4-byte integer and displayed in hexadecimal. This value is not displayed.

Outbound Authentication SPI

Tunnel outbound authentication security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This field is an unsigned 4-byte integer and displayed in hexadecimal. This value is not displayed.

Inbound Encryption SPI

Tunnel inbound encryption security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This is an unsigned 4-byte integer and displayed in hexadecimal. This value is not displayed.

Outbound Encryption SPI

Tunnel outbound encryption security parameter index (SPI). This SPI, combined with the other three SPIs, uniquely identifies a tunnel. This field is an unsigned 4-byte integer and displayed in hexadecimal. This value is not displayed.

IP Address Version

The version of the IP addresses being used for the security endpoints. This value is stored as an integer and displayed as a string. Valid values are:

- 0 = IPv4: The traffic descriptor and the security endpoints are using IPv4 addresses.
- 1 = IPv6: The traffic descriptor and the security endpoints are using IPv6 addresses.

This value is not displayed.

Manual IP Tunnels by Tunnel ID workspace

The Manual IP Tunnels by Tunnel ID workspace displays availability and performance statistics for manual IP tunnels known to a specific TCP/IP stack sorted by Tunnel ID.

One way to display the Manual IP Tunnels by Tunnel ID workspace is to do the following:

1. Right-click the **IP Filters** Navigator item for a specific TCP/IP stack.
2. Select **Workspaces** and select the **Current IP Filters** link.
3. Click the Link icon in the **Current IP Filters in Scan Order** summary table and select the **Manual IP Tunnels by Tunnel ID** link. This link is available only for filters with a **Type** value of **MANUAL**.

Links to Other Workspaces:

None.

Data Source:
z/OS Communication Server Network Management Interface

Default Filter:
None.

Figure 22 shows the Manual IP Tunnels by Tunnel ID workspace.

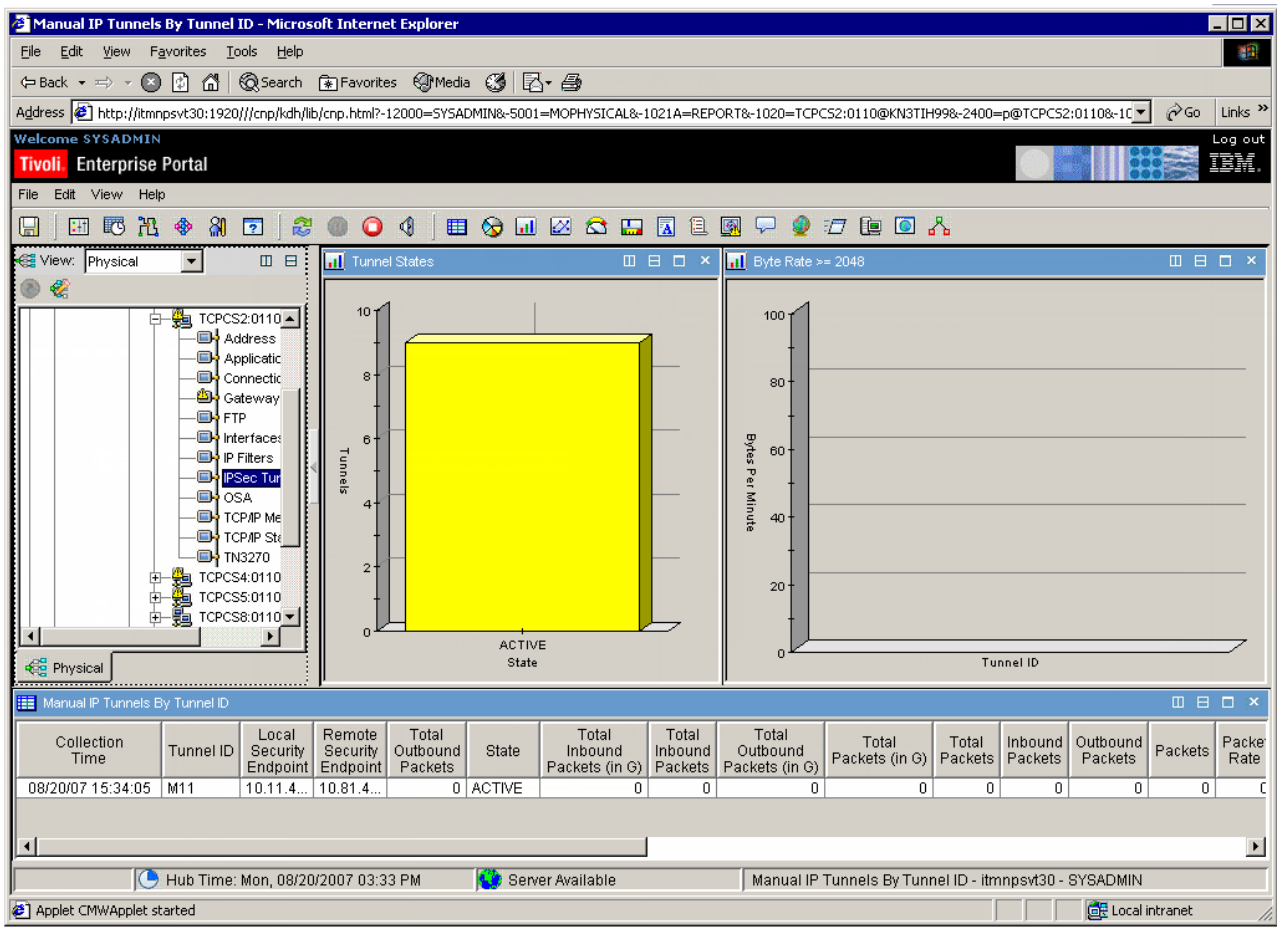


Figure 22. The Tivoli OMEGAMON XE for Mainframe Networks Manual IP Tunnels by Tunnel ID workspace

The Manual IP Tunnels by Tunnel ID workspace displays the following views:

Tunnel States
Provides a snapshot of the current number of manual tunnels in different states for the given TCP/IP stack. Each bar in the graph represents the number of tunnels in a particular state. The graph is a bar chart where:

- Yellow represents the number of Active tunnels.
- Blue represents the number of Inactive tunnels.

Byte Rate >= 2048
Shows tunnels that have an inbound or outbound byte rate of 2048 or greater during the most recent collection interval. The bar chart displays number of bytes per minute for each tunnel ID.

Manual IP Tunnels by Tunnel ID summary table
Provides performance and configuration data about the manual IP tunnel selected.

Manual IP Tunnels by Tunnel ID attributes: For a complete list of the attributes available in the Manual IP Tunnels by Tunnel ID summary table, and a brief description of each, see the “Manual IP Tunnels attributes” on page 132.

Updates to the Connections, Applications Connections, and TCP Connections workspaces

The Connections, Applications Connections, and TCP Connections workspaces have been updated to add a new conditional link to the **Current IP Filters by Destination Address** workspace shown when the Connection Type is TCP. There is also a new conditional link to the IBM Tivoli NetView for z/OS **DVIPA Definition and Status Workspace**. This link is displayed when the value for the DVIPA attribute in the Current IP Filters by Destination Address workspace is **Yes (1)**.

The following attributes were added to the TCPIP Connections Summary table displayed in all three workspaces:

Local IP Address
The local IP address for this connection. For UDP end points, a value of 0.0.0.0 (or ::) in this field indicates that the UDP end point will accept datagrams from any local IP address. For TCP listeners, this IP address will be 0.0.0.0 (or ::) when the application will accept connections to any local IP address. The format is a string up to 45 characters in length.

Note: This attribute was changed for the Connections Workspace only.

Application Name and Port
The Application Name and Local Port are combined in this attribute, separated by a colon. The format is a string up to 15 characters in length.

DVIPA Identifies when the Local IP Address is a DVIPA address. This value is stored as an integer and displayed as a string. The following are valid values:

- 0 = [blank] - Not available.
- 1 = Yes
- 2 = No

These new links to other workspaces are available for these three workspaces:

Links to Other Workspaces:
These following additional workspaces can be accessed by left-clicking the Link icon for a row in the Connections summary table:

- **Current IP Filters by Destination Address**: If the Connection Type is TCP, this link causes a dialog box to be displayed that prompts you for a destination IP address that is compared to the currently active filters for a TCP/IP stack. This field is filled in by default with the value from the **Foreign Address** column for the selected connection, but you can change this value to be any IPv4 or IPv6 address. If the Foreign Address column is blank, the field will display IP address that matches all addresses. With this address as input, this link navigates to the Current IP Filters By Destination Address Workspace showing the IP filters that match the IP address that you provided.
- IBM Tivoli NetView for z/OS **DVIPA Definition and Status Workspace**: This link uses the IP address specified by the **Local IP Address** attribute to link to the NetView DVIPA Definition and Status Workspace. This conditional link is available only if the DVIPA attribute in these workspaces has the value of **Yes (1)**.

For a full list of all the attributes available from these workspaces, refer to the online help or the user's guide.

Updates to the Interfaces and Interfaces History workspaces

In APAR OA21641, a user discovered that the Physical Address attribute in the Interfaces and Interfaces History workspaces was not returning the intended data. In Fix Pack 1, this problem has been corrected.

Interfaces attributes

The old Physical Address definition has been deprecated, and a new definition has been added.

Old Value:

Physical Address
(deprecated) The address of the interface at the protocol sub-layer. The format is a string up to four characters in length.

New Value:

Physical Address
The address of the interface at the protocol sub-layer or blank. The format is a string up to 12 characters in length. This field will be blank when the interface is not active or is not one of the following types:

- ATM
- HYPERchannel
- LCS Ethernet
- MPCIPA OSA Express QDIO

Updates to the Gateways and Devices workspace

In Fix Pack 1, the method by which the TCP/IP Gateways summary table in the Gateways and Devices workspaces retrieves gateway information has changed for monitoring agents running on z/OS 1.5 and higher. For these monitoring agents, the TCP/IP stack creates an “implicit route” for every IP address defined to the stack. These “implicit routes” are not reflected in the inetCidrRouteTable, As a result, the inetCidrRouteIfIndex does not return as many gateways as ipForwardIfIndex.

TCP/IP Gateways attributes

Changes were made to the to the TCP/IP Gateways attributes group to accommodate IPv6 addresses. The following attributes are involved in this change:

- First Hop
- Network Address
- Subnet Mask
- Subnet Value

The existing attributes are deprecated. New attributes with the same name but a longer length have been added to accommodate the longer IPv6 addresses. The Packet Size attribute is no longer displayed.

The new definitions for these attributes follow:

First Hop
The first router in the path to the remote network. The format is an alphanumeric string no longer than 45 characters. This special value may be displayed:

```
<direct> – First Hop is a host IP address
```

Network Address
The network address of this gateway. The format is an alphanumeric string no longer than 45 characters. Special values may be displayed as follows:

- *Defaultnet* – the Network Address is a host IP address

- *Default* – the Network Address is 0

Link-local IPv6 addresses will be displayed in the following format:

FE80::<interface ID>%<interface name>

Subnet Mask

The 32-bit (for IPv4 addresses) or 128-bit (for IPv6 addresses) mask for the subnetwork address in the IP address host portion. The format is an alphanumeric string no longer than 45 characters. These special values might be displayed:

- <none> – Subnet Mask contains zeros.
- HOST – Subnet Mask is a host IP address.

Subnet Value

The subnet identifier. A subnet composes a group of nodes within the same network ID. The format is an alphanumeric string no longer than 45 characters.

Chapter 7. New IPSec situations

IBM Tivoli OMEGAMON XE for Mainframe Networks offers a set of situations that help you to identify some of the most common mainframe network problems. You can use these situations to begin monitoring immediately, or modify them to meet the needs of your enterprise.

The situations in Table 27 on page 142 were added to exploit IPSec functionality.

Table 27. Summary of situations provided by Tivoli OMEGAMON XE for Mainframe Networks

Navigator Item	Attribute table name	Situation name	Column name and initial conditional value	State	Run at startup?
IPSec Tunnels	KN3ITI	N3T_IPSec_Dyn_Act_Fail_IKE_Tnl	The number of failed local activations since the situation was last evaluated is > 0.	Warning	No
		N3T_IPSec_Dyn_Act_Fail_IKE_TnR	The number of failed remote activations since the situation was last evaluated is > 0.	Warning	No
	KN3ISS	N3T_IPSec_Dyn_Act_Fail	The number of failed IKE activations since the situation was last evaluated is > 0.	Warning	No
		N3T_IPSec_IKE_Act_Fail	The number of failed IKE activations since the situation was last evaluated is > 0.	Warning	No
		N3T_IPSec_Key_Msgs_Auth_Fail	IKE key message authentication failures since the situation was last evaluated is > 0. **Note:** This is most likely due to a configuration error.	Warning	No
		N3T_IPSec_Key_Msgs_Invalid	IKE invalid key messages received during the last interval is > 0. **Note:** This is an ISAKMP protocol error.	Warning	No
		N3T_IPSec_Key_Msgs_Replayed	The total number of replayed key messages since the situation was last evaluated is > 5 for 3 consecutive intervals.	Warning	No
		N3T_IPSec_Key_Msgs_Rtrnsmttd	The total number of retransmitted key messages since the situation was last evaluated is > 5 for 3 consecutive intervals.	Warning	No
		N3T_IPSec_QUICKMODE_Invalid	The number of invalid QUICKMODE messages received since the situation was last evaluated is > 0.	Warning	No
		N3T_IPSec_QUICKMODE_Replayed	The total number of replayed QUICKMODE messages since the situation was last evaluated is > 5 for 3 consecutive intervals.	Warning	No
		N3T_IPSec_QUICKMODE_Rtrnsmttd	The total number of retransmitted QUICKMODE messages since the situation was last evaluated is > 5 for 3 consecutive intervals.	Warning	No

Table 27. Summary of situations provided by Tivoli OMEGAMON XE for Mainframe Networks (continued)

Navigator Item	Attribute table name	Situation name	Column name and initial conditional value	State	Run at startup?
IPSec Filters	KN3ISS	N3T_IPSec_Pkts_Denied_DENY	The percentage of packets denied by DENY is > 5.	Warning	No
	KN3IFC	N3T_IPSec_Pkts_Denied_Mismatch	Packets denied by mismatch is > 0.	Warning	No

New IPSec provided situation details

N3T_IPSec_Dyn_Act_Fail

Dynamic IP tunnel activations have failed.

Evaluate the IKE daemon logs to understand the nature of the failures. Failures could be due to either a configuration mismatch where one of the peers is rejecting the other peer's proposals or a network problem such as retransmissions.

Refer to the *z/OS Communication Server: IP Diagnosis* manual for additional information.

This warning situation uses the CHANGE function and the Total Failed Dynamic Tunnel Activations attribute to determine if any dynamic IP tunnel activations have failed since the situation was last evaluated. An attribute is not highlighted when the CHANGE function is used, and the Current Situation Value Table may not display data.

By default, this situation is evaluated every 15 minutes and is not run at startup.

N3T_IPSec_Dyn_Act_Fail_IKE_Tnl

Locally initiated dynamic IP tunnel activations using a particular IKE tunnel have failed.

Evaluate the IKE daemon logs to understand the nature of the failures. Failures could be due to either a configuration mismatch where one of the peers is rejecting the other peer's proposals or a network problem such as retransmissions.

Refer to the *z/OS Communication Server: IP Diagnosis* manual for additional information.

This warning situation uses the CHANGE function and the Total Failed Local Activations attribute to determine if any dynamic IP tunnel local activations using a specific IKE tunnel have failed since the situation was last evaluated. An attribute is not highlighted when the CHANGE function is used, and the Current Situation Value Table may not display data.

By default, this situation is evaluated every 15 minutes and is not run at startup.

N3T_IPSec_Dyn_Act_Fail_IKE_TnR

Remotely initiated dynamic IP tunnel activations using a particular IKE tunnel have failed.

Evaluate the IKE daemon logs to understand the nature of the failures. Failures could be due to either a configuration mismatch where one of the peers is rejecting the other peer's proposals or a network problem such as retransmissions.

Refer to the *z/OS Communication Server: IP Diagnosis* manual for additional information.

This warning situation uses the CHANGE function and the Total Failed Remote Activations attribute to determine if any dynamic IP tunnel remote activations using a specific IKE tunnel have failed since the situation was last evaluated. An attribute is not highlighted when the CHANGE function is used, and the Current Situation Value Table may not display data.

By default, this situation is evaluated every 15 minutes and is not run at startup.

N3T_IPSec_IKE_Act_Fail

Internet Key Exchange (IKE) tunnel activations have failed.

Evaluate the IKE daemon logs to understand the nature of the failures. Failures could be due to either a configuration mismatch where one of the peers is rejecting the other peer's proposals or a network problem such as retransmissions.

Refer to the *z/OS Communication Server: IP Diagnosis* manual for additional information.

This warning situation uses the CHANGE function and the Total Failed IKE Tunnel Activations attribute to determine if any IKE tunnel activations have failed since the situation was last evaluated. An attribute is not highlighted when the CHANGE function is used, and the Current Situation Value Table may not display data.

By default, this situation is evaluated every 15 minutes and is not run at startup.

N3T_IPSec_Key_Msgs_Auth_Fail

Authentication failures have occurred during the negotiation of Internet Key Exchange (IKE) tunnels.

This condition can occur when using shared keys if the shared keys on the peers do not match. Otherwise, this problem is likely an indication of network data corruption.

This warning situation uses the CHANGE function and the IKE Total Key Message Authentication Failures attribute to determine if the total number of IKE key message authentication failures has increased since the situation was last evaluated. An attribute is not highlighted when the CHANGE function is used, and the Current Situation Value Table may not display data.

By default, this situation is evaluated every 15 minutes and is not run at startup.

N3T_IPSec_Key_Msgs_Invalid

Invalid key exchange messages have been received from the remote security endpoint.

This condition can occur either because of an Internet Security Association and Key Management Protocol (ISAKMP) error (check the service levels on both peers) or, when using shared keys, if the shared keys on the peers do not match.

This warning situation uses the CHANGE function and the IKE Total Invalid Key Messages attribute to determine if the total number of invalid key messages has increased since the situation was last evaluated. An attribute is not highlighted when the CHANGE function is used, and the Current Situation Value Table may not display data.

By default, this situation is evaluated every 15 minutes and is not run at startup.

N3T_IPSec_Key_Msgs_Replayed

Key exchange messages used to negotiate Internet Key Exchange (IKE) tunnels have been replayed by the remote security endpoint.

This situation is an indication of a networking problem or a configuration mismatch problem. Evaluate the UNIX® syslog and identify the reason for IKE daemon dropping messages.

This warning situation uses the CHANGE function and the IKE Total Replayed Key Messages attribute to determine if the total number of replayed key messages was more than five for three consecutive evaluations for the situation. During IKE tunnel negotiation the IKE daemon replays 10 messages before declaring a failed activation attempt. Key messages will be replayed periodically for an activation attempt. The five replayed messages may or may not be for the same activation attempt. An attribute is not highlighted when the CHANGE function is used, and the Current Situation Value Table may not display data.

By default, this situation is evaluated every 15 minutes and is not run at startup.

N3T_IPSec_Key_Msgs_Rtrnsmttd

Key exchange messages used to negotiate Internet Key Exchange (IKE) tunnels have been retransmitted by the local security endpoint.

This situation is an indication of a networking problem or a configuration mismatch problem. Evaluate the UNIX syslog and identify the reason for the IKE daemon dropping messages.

This warning situation uses the CHANGE function and the IKE Total Retransmitted Key Messages attribute to determine if the total number of retransmitted key messages was more than five for three consecutive evaluations for the situation. During IKE tunnel negotiation the IKE daemon retransmits 10 messages before declaring a failed activation attempt. Key messages will be retransmitted periodically for an activation attempt. The five retransmitted messages may or may not be for the same activation attempt. An attribute is not highlighted when the CHANGE function is used, and the Current Situation Value Table may not display data.

By default, this situation is evaluated every 15 minutes and is not run at startup.

N3T_IPSec_Pkts_Denied_DENY

The number of packets being denied by the DENY action associated with one or more filters may be high.

This situation could indicate attempted suspicious activity. Enable logging for the filters with DENY actions and monitor the traffic using the UNIX syslog.

This warning situation is based on the Percent Packets Denied By DENY attribute. By default, this situation is evaluated every 15 minutes and is not run at startup.

N3T_IPSec_Pkts_Denied_Mismatch

The number of packets being denied due to a mismatch with the filter's action may be high.

First identify which filters are causing the mismatch alert. This problem could indicate a policy mismatch between the peer and this TCP/IP stack. Another possibility is attempted suspicious activity. Enable logging for the associated filter rule and monitor the traffic using the UNIX syslog.

This warning situation is based on the Packets Denied By Mismatch attribute. By default, this situation is evaluated every 15 minutes and is not run at startup.

N3T_IPSec_QUICKMODE_Invalid

Invalid QUICKMODE messages have been received from the remote security endpoint.

This situation indicates an Internet Security Association and Key Management Protocol (ISAKMP) error. Check the service levels on both peers.

This warning situation uses the CHANGE function and the Total Invalid QUICKMODE Messages attribute to determine if the total number of invalid QUICKMODE messages received (from the remote security endpoint) has increased since the situation was last evaluated. An attribute is not highlighted when the CHANGE function is used, and the Current Situation Value Table may not display data.

By default, this situation is evaluated every 15 minutes and is not run at startup.

N3T_IPSec_QUICKMODE_Replayed

QUICKMODE messages used to negotiate dynamic IP tunnels have been replayed by the remote security endpoint.

This situation indicates a networking problem or a configuration mismatch problem. Evaluate the UNIX syslog and identify the reason for the Internet Key Exchange (IKE) daemon dropping messages.

This warning situation uses the CHANGE function and the Total Replayed QUICKMODE Messages attribute to determine if the total number of replayed QUICKMODE messages was more than five for three consecutive evaluations for the situation. During dynamic tunnel negotiation the IKE daemon replays 10 messages before declaring a failed activation attempt. QUICKMODE messages will be replayed periodically for an activation attempt. The five replayed messages may or may not be for the same activation attempt. An attribute is not highlighted when the CHANGE function is used, and the Current Situation Value Table may not display data.

By default, this situation is evaluated every 15 minutes and is not run at startup.

N3T_IPSec_QUICKMODE_Rtrnsmttd

QUICKMODE messages used to negotiate dynamic IP tunnels have been retransmitted by the local security endpoint.

This situation indicates a networking problem or a configuration mismatch problem. Evaluate the UNIX syslog and identify the reason for the IKE daemon dropping messages.

This warning situation uses the CHANGE function and the Total Retransmitted QUICKMODE Messages attribute to determine if the total number of retransmitted QUICKMODE messages was more than five for three consecutive evaluations for the situation. During dynamic tunnel negotiation the IKE daemon retransmits 10 messages before declaring a failed activation attempt. QUICKMODE messages will be retransmitted periodically for an activation attempt. The five retransmitted messages may or may not be for the same activation attempt. An attribute is not highlighted when the CHANGE function is used, and the Current Situation Value Table may not display data.

By default, this situation is evaluated every 15 minutes and is not run at startup.

Chapter 8. New and changed KN3FCCMD commands

This chapter is an addendum to the "KN3FCCMD Command Reference" appendix in the *IBM Tivoli OMEGAMON XE for Mainframe Networks: Configuration Guide*.

KN3FCCMD z/OS `MODIFY` commands support the IBM Tivoli OMEGAMON XE for Mainframe Networks monitoring agent. This monitoring agent is made up of components that map to data types. By default, each of the components is enabled except IPSec. The default collection interval is 5 minutes.

You can enable or disable data collection by component, providing more granular control over which types of data are collected. These actions can be specified at the time you configure the IBM Tivoli OMEGAMON XE for Mainframe Networks monitoring agent (the preferred method) or through the z/OS MODIFY command. The z/OS `MODIFY` command is issued when the IBM Tivoli OMEGAMON XE for Mainframe Networks monitoring agent is running. You can use the z/OS `MODIFY` command to initialize, start, stop, and display the status of components.

The command appendix in the *IBM Tivoli OMEGAMON XE for Mainframe Networks: Configuration Guide* has been updated to add this new command type:

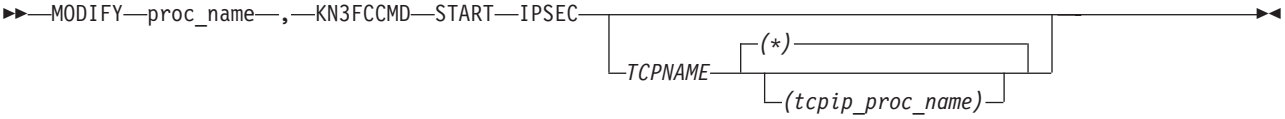
- **IPSec** for IPSec security extensions to the Internet Protocol. You can start or stop collection of IPSec data. To collect IPSec data, the OMEGAMON XE for Mainframe Networks monitoring agent must be at version 4.1.0 with Fix Pack 1 or higher and must be running on a z/OS version 1.8 system or higher.

New commands

New commands have been added to start and stop IPSec. Unlike other components, the default for this component is not to be started at startup.

KN3FCCMD START IPSEC

Format



Where:

TCPNAME
Identifies which TCP/IP address spaces this command applies to.

***** Indicates that this applies to all TCP/IP address spaces.

tcpip_proc_name
Is the name of a TCP/IP address space in your environment.

Purpose

Starts collection of IPSec data.

Usage

Sample output of this command using the default value of all TCP/IP address spaces is provided in the following section:

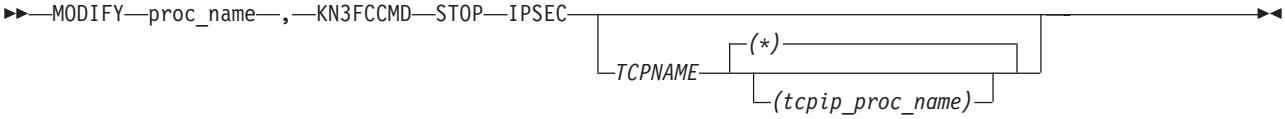
```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START IPSEC'
KN3C110I START FOR COMPONENT IPSEC ACCEPTED. TCPNAME: *
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

Sample output of this command using a specific TCP/IP address space is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD START IPSEC  TCPNAME(TCPIP)'
KN3C110I START FOR COMPONENT IPSEC ACCEPTED. TCPNAME: TCPIP
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD STOP IPSEC

Format



Where:

TCPNAME
Identifies which TCP/IP address spaces this command applies to.

***** Indicates that this applies to all TCP/IP address spaces.

tcpip_proc_name
Is the name of a TCP/IP address space in your environment.

Purpose

Stops collection of IPSec data.

Usage

Sample output of this command using the default value of all TCP/IP address spaces is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP IPSEC'
KN3C110I STOP FOR COMPONENT IPSEC ACCEPTED. TCPNAME: *
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

Sample output of this command using a specific TCP/IP address space is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STOP IPSEC  TCPNAME(TCPIP)'
KN3C110I STOP FOR COMPONENT IPSEC ACCEPTED. TCPNAME: TCPIP
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

Updated commands

Because of the addition of IPSec function, the output for the following two commands has changed:

KN3FCCMD STATUS TCPC

Format

Purpose

Displays the status of the TCP/IP and VTAM statistics component.

Usage

Sample output of this command is provided in the following section:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STATUS TCPC'
KN3FC095 TCPC COLLECTOR STATUS IS ACTIVE
KN3FC095 KONAYTGA ADDRESS IS ED9F900, KONAYFCV ADDRESS IS ED93798
KN3FC095 SAMPLE INTERVAL IS 1 MINUTES
KN3FC095 NUMBER OF TIMES COLLECTOR HAS ABENDED IS 0
KN3FC095 TCPC COLLECTION IS ACTIVE FOR TCPC, CONN, FTP, TN3270, ROUTE
KN3FC095 FTP DISPLAY INTERVAL IS 2 HOURS
KN3FC095 TN3270 DISPLAY INTERVAL IS 2 HOURS
KN3FC095 ROUTE COLLECTION FREQUENCY IS ONCE EVERY 10 INTERVALS
KN3FC095 TCPC COLLECTION FROM TCPIP IS ACTIVE FOR TCPC, CONN, IPSEC, FTP, TN3270
KN3FC095 FTP DISPLAY INTERVAL FOR TCPIP IS 2 HOURS
KN3FC095 TN3270 DISPLAY INTERVAL FOR TCPIP IS 2 HOURS
KN3FC095 ROUTE COLLECTION FREQUENCY FOR TCPIP IS ONCE EVERY 10 INTERVALS
KN3FC095 VTAM COLLECTION IS ACTIVE FOR SNA, CSM, EEHPR
KN3FC095 EEHPR OPTIONS: ALLHPR(N)
KN3FC095 TCPC STATUS DISPLAY COMPLETE
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

Sample output for a system with three TCP/IP address spaces:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD STATUS TCPC'
KN3FC095 TCPC COLLECTOR STATUS IS ACTIVE
KN3FC095 KONAYTGA ADDRESS IS 116A59F0, KONAYFCV ADDRESS IS 116A4760
KN3FC095 SAMPLE INTERVAL IS 5 MINUTES
KN3FC095 NUMBER OF TIMES COLLECTOR HAS ABENDED IS 0
KN3FC095 TCPC COLLECTION IS ACTIVE FOR TCPC, CONN, IPSEC, FTP, TN3270, ROUTE
KN3FC095 FTP DISPLAY INTERVAL IS 2 HOURS
KN3FC095 TN3270 DISPLAY INTERVAL IS 2 HOURS
KN3FC095 ROUTE COLLECTION FREQUENCY IS ONCE EVERY 10 INTERVALS
KN3FC095 TCPC COLLECTION FROM TCPCS2 IS ACTIVE FOR TCPC, CONN, IPSEC, FTP, TN3270, ROUTE
KN3FC095 FTP DISPLAY INTERVAL FOR TCPCS2 IS 2 HOURS
KN3FC095 TN3270 DISPLAY INTERVAL FOR TCPCS2 IS 2 HOURS
KN3FC095 ROUTE COLLECTION FREQUENCY FOR TCPCS2 IS ONCE EVERY 10 INTERVALS
KN3FC095 TCPC COLLECTION FROM TCPCS4 IS ACTIVE FOR TCPC, CONN, IPSEC, FTP, TN3270, ROUTE
KN3FC095 FTP DISPLAY INTERVAL FOR TCPCS4 IS 2 HOURS
KN3FC095 TN3270 DISPLAY INTERVAL FOR TCPCS4 IS 2 HOURS
KN3FC095 ROUTE COLLECTION FREQUENCY FOR TCPCS4 IS ONCE EVERY 10 INTERVALS
KN3FC095 TCPC COLLECTION FROM TCPIP IS ACTIVE FOR TCPC, CONN, IPSEC, FTP, TN3270, ROUTE
KN3FC095 FTP DISPLAY INTERVAL FOR TCPIP IS 2 HOURS
KN3FC095 TN3270 DISPLAY INTERVAL FOR TCPIP IS 2 HOURS
KN3FC095 ROUTE COLLECTION FREQUENCY FOR TCPIP IS ONCE EVERY 10 INTERVALS
KN3FC095 VTAM COLLECTION IS ACTIVE FOR SNA, CSM, EEHPR
KN3FC095 EEHPR OPTIONS: ALLHPR(N)
KN3FC095 TCPC STATUS DISPLAY COMPLETE
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

KN3FCCMD HELP

Format

Purpose

Displays the actions and options provided on the KN3FCCMD commands.

Usage

Sample output of this command is provided below:

```
KLVOP191 REPLY FROM *MASTER*:
KLVOP191    'KN3FCCMD HELP'
KN3FC005 --------+-------------------------------------------------------------+
KN3FC005 COMMAND | DESCRIPTION                                                 |
KN3FC005 --------+-------------------------------------------------------------+
KN3FC005 STATUS  | DISPLAY STATUS INFORMATION ABOUT INSTALLED COMPONENTS       |
KN3FC005 HELP    | HELP INFORMATION FOR KN3FCCMD                               |
KN3FC005 INSTALL | INSTALL COMPONENT(S) FOR PRODUCT ENVIRONMENT                |
KN3FC005 START   | START INSTALLED COMPONENTS                                  |
KN3FC005 STOP    | STOP INSTALLED COMPONENTS                                   |
KN3FC005 SEND    | SEND COMMAND MESSAGES                                       |
KN3FC005 --------+-----------------------------------+-----------------------+
KN3FC005 OPTION  | DESCRIPTION                       | COMMANDS              |
KN3FC005 --------+-----------------------------------+-----------------------+
KN3FC005 FPON    | OMEGAMON PRODUCT FEATURES         | INSTALL,STATUS        |
KN3FC005 FPCT    | CMS DATA SERVER FEATURES          | INSTALL,STATUS        |
KN3FC005 SEVT    | VTAM ENVIRONMENT FEATURES         | INSTALL,STATUS        |
KN3FC005 SEMV    | MVS ENVIRONMENT FEATURES          | INSTALL,STATUS        |
KN3FC005 SNAC    | SNA STATISTICS COLLECTOR          | START,STATUS          |
KN3FC005 TCPC    | TCP/IP STATISTICS COLLECTOR       | INSTALL,START,        |
KN3FC005         |                                   | STOP,STATUS           |
KN3FC005 TRACE   | DIAGNOSTICS TRACE FACILITY        | START,STOP,STATUS     |
KN3FC005 TRAP    | DIAGNOSTICS TRAP FACILITY         | START,STOP,STATUS     |
KN3FC005 DBUG    | EXTENDED DIAGNOSTICS MODE         | START,STOP,STATUS     |
KN3FC005 SNACINTV| SNA COLLECTOR INTERVAL            | START                 |
KN3FC005 TCPCVIOU| TCP/IP COLLECTOR DYNALLOC VIOUNIT | INSTALL,START         |
KN3FC005 TCPCINTV| TCP/IP COLLECTOR INTERVAL         | INSTALL,START         |
KN3FC005 TCPCTCPC| TCP/IP COLLECTOR NAME/PROFILE/COM | INSTALL,START         |
KN3FC005 EEHPR   | NMI EE/HPR DATA COLLECTION        | START,STOP            |
KN3FC005 CSM     | NMI CSM DATA COLLECTION           | START,STOP            |
KN3FC005 CONN    | NMI TCP CONN/APPL DATA COLLECTION | START,STOP            |
KN3FC005 IPSEC   | NMI IPSEC DATA COLLECTION         | START,STOP            |
KN3FC005 FTP     | NMI FTP DATA COLLECTION           | START,STOP            |
KN3FC005 TN3270  | NMI TN3270 DATA COLLECTION        | START,STOP            |
KN3FC005 ROUTE   | SNMP ROUTE DATA COLLECTION        | START,STOP            |
KN3FC005 TCPNAME | TCP/IP STACK SUBCMD               | START,STOP            |
KN3FC005         | (CONN,IPSEC,FTP,TN3270,ROUTE)     |                       |
KN3FC005 DSPINTV | NMI DATA DISPLAY INTERVAL SUBCMD  | START                 |
KN3FC005         | (FTP,TN3270)                      |                       |
KN3FC005 FREQ    | ROUTE COLLECTION FREQUENCY SUBCMD | START                 |
KN3FC005         | (ROUTE)                           |                       |
KN3FC005 ALLHPR  | OPTION ON THE EEHPR SUBCMD        | START                 |
KN3FC005         | N=HPR FLOWING OVER EE CONNECTIONS |                       |
KN3FC005         | Y=ALL HPR CONNECTIONS             |                       |
KN3FC005 --------+-----------------------------------+-----------------------+
KN3FC000 KN3FCCMD PROCESSING COMPLETE
```

Chapter 9. New and changed messages and problem determination

This chapter contains the new messages added to support IPSec and a new problem determination scenario.

Messages

The following messages are either new or updated because of additions made in this fix pack.

KN3FC005 <help text>

Explanation: This is a prefix for feature control command (KN3FCCMD) HELP output. To see a listing of the text that can be displayed in the *<help text>* field, see Chapter 8, "New and changed KN3FCCMD commands," on page 147 in this book and the Command Reference appendix in the *IBM Tivoli OMEGAMON XE for Mainframe Networks: Configuration Guide*.

System action: None.

Programmer response: None.

Message type: Informational.

KN3FC095 <status text>

Explanation: This is a prefix for feature control command (KN3FCCMD) STATUS TCPC output. To see a listing of the text that can be displayed in the *<status text>* field, see Chapter 8, "New and changed KN3FCCMD commands," on page 147 in this book and the Command Reference appendix in *IBM Tivoli OMEGAMON XE for Mainframe Networks: Configuration Guide*. This message may now also include IPSec status.

System action: None.

Programmer response: None.

Message type: Informational.

KN3N024E THE *netmgmt_interface* INTERFACE IN THE *interface_path* PATH CANNOT BE INITIALIZED. ERRNO=*errno* AND ERRNOJR=0x*errnoJr*. LOCATION: *location_code*.

Explanation: An attempt to initialize the z/OS Communications Server network management interface was not successful for the identified reason.

The *location_code* identifies the location within the monitor code where this message is issued. It is used by IBM Software Support.

Operator response: Verify that the TCP/IP stack is active. Verify that the z/OS Communications Server network management interface is active. Issue the `DISPLAY NET,VTAMOPTS,OPTION=SNAMGMT` command for the SNAMGMT interface. Issue the `DISPLAY TCPIP,tcpip_procname,NETSTAT,CONFIG` command for the network monitoring interfaces.

If you have enabled IPSec data collection on a z/OS version 1.8 or later system, confirm that the IKE daemon and Policy Agent daemon have been started by issuing this command: `D A,L`. If the daemons have not started, start them. Refer to the *z/OS Communications Server IP Configuration Guide* (SC31-8775) for more information about the IKE daemon and Policy Agent daemon.

Programmer response: Verify that the user ID running the monitor is authorized to access the z/OS Communications Server network management interface.

See *z/OS UNIX System Services Messages and Codes* for errno (displayed in decimal) and errnoJr codes.

KN3N031E AN UNEXPECTED MESSAGE TYPE WAS RECEIVED, *msgTypeReceived*. LOCATION: *location_code*.

Explanation: The data collection server received data that was not expected. Some IPSec data cannot be collected. The interface to the z/OS Communications Server network management data was closed, and resources were released. The data collection server attempts to establish this data collection again. The *location_code* identifies the location within the monitor code where this message is issued. It is used by IBM Software Support.

Operator Response: Notify the System Programmer if the problem persists.

Programmer response: Verify that the installed versions of Tivoli OMEGAMON XE for Mainframe Networks and z/OS Communications Server are compatible.

KN3N032E THE IPSEC INTERFACE CANNOT BE INITIALIZED. LOCATION: *location_code*.

Explanation: The program attempted to initialize a z/OS Communications Server network management interface to prepare for collecting z/OS Communications

Server IPSEC data. The initialization was not successful.

Operator Response: Confirm that the IKE daemon and Policy Agent daemon have been started by issuing this command:

```
D A,L
```

If the daemons have not started, start them. Refer to the *z/OS Communications Server IP Configuration Guide* (SC31-8775) for more information about the IKE daemon and Policy Agent daemon.

Programmer response: Verify that the installed versions of Tivoli OMEGAMON XE for Mainframe Networks and z/OS Communications Server are compatible. Verify that the user ID running the monitor is authorized to access the z/OS Communications Server network management interface.

KN3N033W THE Z/OS COMMUNICATIONS SERVER STOPPED THE IPSEC INTERFACE. LOCATION: *location_code***.**

Explanation: The monitor attempted to communicate using the z/OS Communications Server network management interface, but the z/OS Communications Server ended the connection. The monitor attempted to collect IPSEC data. The collection was not successful. The *location_code* identifies the location within the monitor code where this message is issued. It is used by IBM Software Support.

Operator Response: Determine if the IKE daemon and Policy Agent daemon are running by issuing this command:

```
D A,L
```

If the daemons are not running, start them. Refer to the *z/OS Communications Server IP Configuration Guide* (SC31-8775) for more information about the IKE daemon and Policy Agent daemon. Notify the System Programmer if the problem persists.

Programmer response: Determine why the IKE daemon and Policy Agent daemon are not running. Correct the problem and start the daemons.

KN3N035W INVALID STATE FOR DYNAMIC TUNNEL IN GET_IPTUNDYNSTACK RESPONSE. LOCATION: *location_code*

Explanation: The data collection server received data that was not expected. A record for a dynamic tunnel in the pending or incomplete state was received among record from a TCP/IP stack. All dynamic tunnels known to a TCP/IP stack are expected to be in active state. This record is ignored. Data collection continues.

Operator Response: Notify the System Programmer if the problem persists.

Programmer response: Verify that the installed versions of Tivoli OMEGAMON XE for Mainframe Networks and z/OS Communications Server are compatible.

Problem determination

No data appears in the new workspaces added for IPSec

If no data appears in your IPsec workspaces, do the following:

1. Verify that IPSEC collection is configured and enabled:
   a. Examine the RKLVLOG for the Mainframe Networks agent. If IPSEC collection was started at agent initialization, there should be a message KN3FC095 message that lists IPSEC in the list of active collection types:

      ```
      KN3FC095 TCPC COLLECTION IS ACTIVE FOR TCPC, CONN, IPSEC, FTP, TN3270, ROUTE
      ```

   b. Follow the procedures in Chapter 3, “New configuration required for IPSec,” on page 19 to invoke the Configuration Tool and verify that IPSec is enabled in the panel shown in Figure 3 on page 20.
2. Examine the KN3ANMON log for the Mainframe Networks agent to determine if any of the following error messages appear:

   ```
   KN3N024E THE IPSEC INTERFACE IN THE interface_path PATH CANNOT BE INITIALIZED.
     ERRNO=errno AND ERRNOJR=0xerrnoJr. LOCATION: location_code

   OR

   KN3N031E AN UNEXPECTED MESSAGE TYPE WAS RECEIVED, msgTypeReceived.  LOCATION:  location_code.

   OR

   KN3N035W INVALID STATE FOR DYNAMIC TUNNEL IN GET_IPTUNDYNSTACK RESPONSE.  LOCATION:  location code.
   ```

3. Verify that the IKE Daemon (IKED) and Policy Agent (PAGENT) tasks are active and initialized correctly. Examples of successful initialization messages follow:

   Policy agent example:

   ```
   EZZ8432I PAGENT INITIALIZATION COMPLETE
   EZZ8771I PAGENT CONFIG POLICY PROCESSING COMPLETE FOR TCPIP : IPSE
   ```

   IKE daemon example:

   ```
   EZD0911I IKE CONFIG PROCESSING COMPLETE USING FILE //'USER.PARMLIB(IKEDC)'
   EZD1061I IKE CONNECTING TO PAGENT
   EZD1059I IKE CONNECTED TO PAGENT
   EZD1058I IKE STATUS FOR STACK TCPIP IS UP
   EZD1068I IKE POLICY UPDATED FOR STACK TCPIP
   EZD1046I IKE INITIALIZATION COMPLETE
   ```

Appendix A. Known issues with information the version 4.1.0 documentation

This appendix documents known issues with the OMEGAMON XE for Mainframe Networks documentation. The following links explain these issues:

Online help changes for OSA Express Ports and OSA Express Port attribute groups

In the online help for the OSA Express Ports Attribute Group, two additional values can be returned by the Port Type attribute: oneThousandBaseTEthernet (97) and tenGigabitEthernet (145). The rewritten description of the Port Type attribute in the online help and the user's guide is as follows:

Port Type

The physical port type. The format is an integer. Possible port types are:

- 65 = gigabitEthernet
- 81 = fastEthernet
- 97 = oneThousandBaseTEthernet
- 145 = tenGigabitEthernet

This addition should also be made in the User Guide description of this attribute on page 114.

In the online help for the OSA Express Channels Attribute Group, these same two additional values can be returned by the Subtype attribute: oneThousandBaseTEthernet (97) and tenGigabitEthernet (145).

The rewritten description of the Subtype attribute in the online help and the user guide is as follows:

Subtype

The type of OSA feature present. The possible values are:

- 1 = Unknown
- 2 = Gigabit
- 3 = FastEthernet
- 4 = ATMNative

- 5 = ATMLanEmulation
- 6 = NoPortsDefined
- 7 = OneLogicalEthPort
- 8 = OneLogicalTokenRingPort
- 9 = TwoLogicalEthPorts
- 10 = TwoLogicalTokenRingPorts
- 11 = LogicalEthernetAndTokenRingPorts
- 12 = LogicalTokenRingAndEthPorts
- 65 = GigabitEthernet
- 81 = FastEthernet
- 82 = TokenRing
- 97 = OneThousandBaseTEthernet
- 145 = TenGigabitEthernet
- 2304 = ATMEmulatedEthernet

This addition should also be made in the User Guide description of this attribute on page 107.

Use of the configuration guide to complete the OMEGAMON XE agent configuration

Some steps required to complete the configuration of the OM XE agent are not found in the online help for the Configuration Tool. To ensure that you perform all the steps required and perform them in the correct order, use the *IBM Tivoli OMEGAMON XE for Mainframe Networks: Configuration Guide* for product configuration, not the Configuration Tool online help.

Clarification that Tivoli Data Warehouse and warehouse proxy run on platforms other than Windows

In the *IBM Tivoli OMEGAMON XE for Mainframe Networks: Planning Guide*, page 31 incorrectly states that the Tivoli Data Warehouse and warehouse proxy run only on Windows® and that these two components must be on the same Windows system.

Replace this paragraph:

The Tivoli Data Warehouse and warehouse proxy run on Windows. The Tivoli Enterprise™ Portal Server retrieves data from the Tivoli Data Warehouse through an ODBC connection. The warehouse proxy communicates with the Tivoli Enterprise Portal Server and with the systems where the short-term history is stored (either the monitoring agents or the Tivoli Enterprise Monitoring Server). The Tivoli Data Warehouse and warehouse proxy must be on the same Windows system. The placement of the Tivoli Data Warehouse in your network should consider the location of both the Tivoli Enterprise Portal Server and the short-term history files.

With this paragraph:

The Tivoli Data Warehouse and warehouse proxy run on a number of platforms. For the most current list of platforms, refer to the fix pack document for the most current version of IBM Tivoli Monitoring. The Tivoli Enterprise Portal Server retrieves data from the Tivoli Data Warehouse through an ODBC connection. The warehouse proxy communicates with the Tivoli Enterprise Portal Server and with the systems where the short-term history is stored (either the monitoring agents or the Tivoli Enterprise Monitoring Server). The placement of the Tivoli Data Warehouse in your network should consider the location of both the Tivoli Enterprise Portal Server and the short-term history files.

Likewise, in the *IBM Tivoli OMEGAMON XE for Mainframe Networks: Configuration Guide*, page 89 incorrectly states the following:

Tivoli Enterprise Portal and Tivoli Enterprise Portal Server are installed on a Windows system.

This has been changed as follows:

Tivoli Enterprise Portal and Tivoli Enterprise Portal Server run on a number of platforms. For the most current list of platforms, refer to the documentation for the most current fix pack for IBM Tivoli Monitoring.

Clarification that the summarization and pruning agent runs on a distributed monitoring server, not on z/OS monitoring server

In the *IBM Tivoli OMEGAMON XE for Mainframe Networks: Configuration Guide*, page 98 incorrectly describes this process for enabling summarization and pruning is for the hub Tivoli Enterprise Monitoring Server on z/OS. This process is for distributed platforms only, not for z/OS. Thus, in this explanation on page 98:

Enabling summarization and pruning on a hub Tivoli Enterprise Monitoring Server on z/OS

If the hub Tivoli Enterprise Monitoring Server on z/OS does not reside on the same machine as the Tivoli Enterprise Portal Server, you must enable summarization and pruning manually. To enable the Summarization and Pruning Agent to run against OMEGAMON XE for Mainframe Networks tables in the Tivoli Data Warehouse, you must install the catalog and attribute data files on the hub Tivoli Enterprise Monitoring Server on z/OS. These files are not automatically installed on a hub Tivoli Enterprise Monitoring Server if that component does not reside on the same machine as the Tivoli Enterprise Portal Server.

The word ″If″ should be replaced with ″Since.″

Configuration Tool screens and help may be more up-to-date than the configuration guide screens

Be aware that the Configuration Tool is updated constantly because it is updated as new products are shipped and new requirements are introduced. Therefore, the screens in the Configuration Guide may not exactly match those in the Configuration Tool.

ITMS: Engine MINIMUM statement has additional parameters

On page 120 of the configuration guide, the following tuning information is found:

ITMS:Engine MINIMUM parameter

The MINIMUM parameter is used to specify the minimum amount (in KB) of extended storage storage that can be allocated. This value is specified with this syntax:

`MINIMUM(8192,X | n,X)`

Where *n* represents the minimum amount of extended storage (in KB) that can be allocated. For example, to specify a 16MB above-the-line region, code `MINIMUM(16384,X)`. When managing a large number of resources, a value of `MINIMUM (500000,X)` is recommended.

This section has been rewritten as follows:

ITMS:Engine MINIMUM parameter

The MINIMUM parameter is used to specify the minimum amount (in KB) of extended or below-the-line private storage that can be allocated. This value is specified with this syntax:

```
MINIMUM(n,P | X)
```

Where:

n Is the size of a block of storage in KB

P Represents the amount of below-the-line private storage (in KB) that can be allocated .

X Represents the minimum amount of extended storage (in KB) that can be allocated.

For example, to specify a 16MB above-the-line region, code `MINIMUM(16384,X)`. When managing a large number of resources, a value of `MINIMUM (500000,X)` is recommended.

To use extended storage, you must do both of the following:

- Code the MINIMUM parameter.
- Make sure that MINIMUM + RESERVE is less than or equal to MAXIMUM

Note the following about the default over the line region:

- Specified in the IEFUSI and IEALIMIT z/OS(R) modules.
- Distributed by IBM(R) as 32 megabytes.
- If smaller than the amount specified for the MINIMUM parameter, do one of the following:
  - Alter the default
  - Use the REGION parameter as follows:

    0K or 0M
    All primary and extended storage is available for GETMAIN.

    Up to 16M
    Primary region equals the specified value; extended region equals the default.

    Up to 32M
    All available region goes to primary storage; extended region equals the default.

    Over 32M
    All available region goes to primary storage; specified value goes to extended storage.

In general, for example, REGION=0M.

Note: The MINIMUM parameter can be set from the Configuration Tool using the ″Specify Advanced Agent Configuration Values″ panel.

FTP Data Display Interval defined incorrectly in the configuration guide

The Configuration Tool help for the FTP Data Display Interval that is part of the SPECIFY COMPONENT CONFIGURATION (PAGE 2) panel is misleading. This same misleading information is found on page 65 of the configuration guide. It currently says:

FTP Data Display Interval
Determines how long FTP data will be displayed on the Tivoli Enterprise Portal. A value of ″1″ means that FTP data is displayed for one hour. This value is expressed as a whole number in hours from 1 to 24. The default is 2 hours.

It should say:

FTP Data Display Interval
Determines the size of the sliding window that displays all FTP transfers that were completed or

became active within the display interval. A value of ″1″ means the window displays all data from present until 1 hour ago. This value is expressed as a whole number in hours from 1 to 24. The default is 2 hours.

When the configuration guide says RC must be 0, there may be other valid returns found in the JCL job

In some instances, the configuration guides for monitoring agents on z/OS state that all return codes from the JCL job performed form the Configuration Tool must be zero. However, the comments inside the generated ICAT jobs sometimes state that other return codes are acceptable. Where there is a conflict between the JCL job comments and the configuration guide, accept the information in the JCL job since it may have been created later than the information in the book.

New problem determination issue: SNMP data collection fails with message KN3IR926

This problem description should be added to the *IBM OMEGAMON XE for Mainframe Networks: Problem Determination Guide*.

SNMP data collection fails with message KN3IR926 in your RKLVLOG: TCP MONITOR COLLECTION FAILED in v 4.1.0

This message most likely indicates a configuation issue with SNMP data collection. In OMEGAMON XE for Mainframe Networks version 4.1.0 the way you configure SNMP was changed from previous releases. In version 4.1.0, the Configuration Tool generates a sample SNMP configuration file during configuration. To collect SNMP-derived data, the SNMP configuration file must be customized to your environment. The sample started task procedures that are generated by the Configuration Tool for OMEGAMON XE and OMEGAMON II® for Mainframe networks contain DD statements that point to the SNMP configuration file that you identified during configuration. Refer to the SNMP appendix in the IBM Tivoli Monitoring: Configuration Guide for details about this file.

If the OMEGAMON XE or OMEGAMON II for Mainframe Networks SNMP configuration file is correct, then the problem could be caused by a more obscure SNMP agent configuration issue.

In OMEGAMON XE for Mainframe Networks version 3.1.0, the ″home″ IP address was used with the `sendto()` function when sending a PDU (datagram) to an SNMP agent associated with a TCP/IP stack whose data is being collected. This ″home″ interface is returned by an EZASMI TYPE=GETHOSTID request. As a result, the SNMP agent uses that ″home″ IP address as the source IP address for the datagram. A further com- plication is that this source IP address is also subjected to the IP address masking to determine if it is a source from which the SNMP agent will ″accept″ datagrams.

In OMEGAMON XE for Mainframe Networks version 4.1.0 with its new SNMP manager, the IP address used with `sendto()` is the loopback address. With this new solution, the loopback address is seen by the SNMP agent as the source IP address for the datagram. If the IP address-masking specified with the applicable COMMUNITY (or SNMP_COMMUNITY) definition in the SNMP agent configuration file (or perhaps in PW.SRC) is such that loopback is not allowed, that may explain an apparent change in the ability to communicate.

OMEGAMON II for Mainframe Networks version 560 is not affected by this change. This component continues to work as it did in version 550.

To address this issue, you must change the SNMP agent configuration to allow a request whose source IP address is loopback. Use one of the following three methods, based on your agent configuration.

1. Add a loopback statement in the PW.SRC file.

2. Add or change a COMMUNITY statement in the SNMP agent configuration file (for example, snmpd.conf).
3. Coordinate the SNMP_COMMUNITY and TARGET_ADDRESS statements in the SNMP agent configuration file (for example, snmpd.conf).

Information about how to make these changes is described in the *z/OS Communications Server: IP Configuration Reference*. All three alternatives could involve the addition to or a change in an IP address, an IP address mask, or both.

Telnet Pool Size and Data Source Level attributes summarized data is misleading

If you have configured both the Tivoli Data Warehouse and the Summarization and Pruning agent, you will find that summarized data for the Telnet Pool Size attribute is misleading. Therefore, summarized data for this attribute in the TCP/IP Summary and the TCP/IP Address Space workspaces is misleading.

To get around this issue, if you create or modify a view to show the summarized data, you could change the filter for that data. Right-click on the view, select **Properties**, click on the **Filter** tab, and select the LAT_ attribute (last value) instead of the TOT_ attribute (total value) for the summarized attribute.

Incorrect information configuration guide Appendix E: Disk space requirements for historical data table

The space requirement worksheets for some of the attribute tables in this appendix contain incorrect information. Refer to “Updates to historical data storage tables for new and changed attribute tables” on page 13 for specific changes in this appendix.

Undocumented OMEGAMON II for Mainframe Networks messages

These OMEGAMON II for Mainframe Networks messages were recently found to be undocumented.

KONAF162 (*module*) - TCP/IP COMMAND FAILED - COMMAND SERVICE TASK NOT ACTIVE

Explanation: The specified *module* needs the TCP/IP Collector Service Thread task to be active in order to issue a command but the task is not active.

System action: The request is terminated.

User response: Log the diagnostic information and contact IBM Software Support.

Message type: Error

KONAF163 (*module*) - EXTENDED MCS CONSOLE NOT ACTIVE

Explanation: The specified *module* expected to find an active EMCS console in order to issue a command. However, no EMCS console is active for this instance of OMEGAMON II for Mainframe Networks.

System action: The request is terminated.

User response: Log the diagnostic information and contact IBM Software Support.

Message type: Error

KONAF164 (*module*) - UNABLE TO LOCATE RESOURCE

Explanation: The specified *module* expected to find a resource associated with a chain of elements being processed. However, the resource was not found.

System action: The request to update the table is terminated.

User response: Log the diagnostic information and contact IBM Software Support.

Message type: Error

KONAF165 (*module*) - MIB BROWSER LINE LIMIT EXCEEDED

Explanation: The response to a MIB browser request exceeded the maximum number of lines that could be displayed on the OMEGAMON II for Mainframe Networks console.

System action: The request for the MIB data is terminated.

User response: None.

Message type: Informational

KONAF166 (*module*) - MIB BROWSER IS NOT ACTIVE

Explanation: The specified *module* issued a request to the MIB browser task, but the MIB browser task was not active.

System action: The request for the MIB data is terminated.

User response: Log the diagnostic information and contact IBM Software Support.

Message type: Error

KONAF167 (*module*) - TCP/IP COMMAND FAILED - RC(*return_code*)

Explanation: The specified *module* issued a TCP/IP command and received a non-zero return code.

System action: The request is terminated.

User response: Log the diagnostic information and contact IBM Software Support.

Message type: Error

Appendix B. Support for problem solving

If you have a problem with your IBM software, you want to resolve it quickly. This section describes the following options for obtaining support for IBM software products:

- "Using IBM Support Assistant"
- "Obtaining fixes"
- "Receiving weekly support updates" on page 166
- "Contacting IBM Software Support" on page 166

Using IBM Support Assistant

The IBM Support Assistant is a free, stand-alone application that you can install on any workstation. You can then enhance the application by installing product-specific plug-in modules for the IBM products you use.

The IBM Support Assistant saves you the time it takes to search the product, support, and educational resources. The IBM Support Assistant helps you gather support information when you need to open a problem management record (PMR), which you can then use to track the problem.

The product-specific plug-in modules provide you with the following resources:

- Support links
- Education links
- Ability to submit problem management reports

For more information, and to download the IBM Support Assistant Version 3, see http://www.ibm.com/software/support/isa. After you download and install the IBM Support Assistant, folow these steps to install the plug-in for IBM Tivoli Monitoring:

1. Start the IBM Support Assistant application.
2. Select **Updater** on the Welcome page.
3. Select **New Properties and Tools**.
4. Under Tivoli, select **IBM Tivoli OMEGAMON XE for Mainframe Networks**, and then click **Install**. Be sure to read the license and description.
5. Restart the IBM Support Assistant.

Obtaining fixes

A product fix might be available to resolve your problem. To determine which fixes are available for your IBM software product, follow these steps:

1. Go to the IBM Software Support Web site at http://www.ibm.com/software/support.
2. Click **Downloads and drivers** in the **Support topics** section.
3. Select the **Software** category.
4. Selet a product in the **Sub-category** list.
5. In the **Find downloads an drivers by product** section, select one software category from the **Category** list.
6. Select one product from the **Sub-category** list.
7. Type more search terms in the **Search within results** if you want to refine your search.
8. Click **Search**.
9. From the list of downloads returned by your search, click the name of a fix to read the description of the fix and to optionally download the fix.

For more information about the types of fixes that are available, see the *IBM Software Support Handbook* at http://techsupport.services.ibm.com/guides/handbook.html.

Receiving weekly support updates

To receive weekly e-mail notifications about fixes and other software support news, follow these steps:

1. Go to the IBM Software Support Web site at http://www.ibm.com/software/support.
2. Click **My support** in the upper- right corner of the page.
3. If you have already registered for **My support**, sign in and skip to the next step.

   If you have not registered, click **register now**, and complete the registration form using your e-mail address as your IBM ID and click **Submit**.
4. Click **Edit profile**.
5. In the **Products** list, select **Software**. A second list is displayed.
6. In the second list, select a product segment, for example, **Systems management**. A third list is displayed.
7. In the third list, select **Application Performance & Availability**. A list of applicable products is displayed.
8. Select **IBM Tivoli Monitoring**, **IBM Tivoli OMEGAMON XE for Mainframe Networks**, and any other products for which you want to receive updates.
9. Click **Add products**.
10. After selecting all products that are of interest to you, click **Subscribe to email** on the **Edit profile** tab.
11. Select **Please send these documents by weekly email**.
12. Update your e-mail address as needed.
13. In the **Documents** list, select **Software**.
14. Select the types of documents that you want to receive information about.
15. Click **Update**.

If you experience problems with the **My support** feature, you can obtain help in one of the following ways:

- Online

  Send an e-mail message to erchelp@ca.ibm.com, describing your problem.
- By phone

  Call 1-800-IBM-4You (1-800-426-4968).

Contacting IBM Software Support

IBM Software Support provides assistance with product defects. The easiest way to obtain that assistance is to open a PMR or ETR directly from the IBM Support Assistant (see “Using IBM Support Assistant” on page 165).

Before contacting IBM Software Support, your company must have an active IBM software maintenance contract, and you must be authorized to submit problems to IBM. The type of software maintenance contract that you need depends on the type of product you have:

- For IBM distributed software products (including, but not limited to, Tivoli, Lotus, and Rational products, as well as DB2 and WebSphere products that run on Windows or UNIX operating systems), enroll in Passport Advantage in one of the following ways:

  Online

  Go to the Passport Advantage Web site at http://www-306.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm.

By phone

For the phone number to call in your country, go to the IBM Software Support Web site at http://techsupport.services.ibm.com/guides/contacts.html and click the name of your geographic region.

- For customers with Subscription and Support (S & S) contracts, go to the Software Service Request Web site at https://techsupport.services.ibm.com/ssr/login.
- For customers with IBMLink, CATIA, Linux, OS/390, iSeries, pSeries, zSeries, and other support agreements, go to the IBM Support Line Web site at http://www.ibm.com/services/us/index.wss/so/its/a1000030/dt006.
- For IBM eServer software products (including, but not limited to, DB2 and WebSphere products that run in zSeries, pSeries, and iSeries environments), you can purchase a software maintenance agreement by working directly with an IBM sales representative or an IBM Business Partner. For more information about support for eServer software products, go to the IBM Technical Support Advantage Web site at http://www.ibm.com/servers/eserver/techsupport.html.

If you are not sure what type of software maintenance contract you need, call 1-800-IBMSERV (1-800-426-7378) in the United States. From other countries, go to the contacts page of the *IBM Software Support Handbook* on the Web at http://techsupport.services.ibm.com/guides/contacts.html and click the name of your geographic region for phone numbers of people who provide support for your location.

To contact IBM Software support, follow these steps:

1. "Determining the business impact"
2. "Describing problems and gathering information"
3. "Submitting problems" on page 168

Determining the business impact

When you report a problem to IBM, you are asked to supply a severity level. Use the following criteria TO understand and assess the business impact of the problem that you are reporting:

Severity 1

The problem has a *critical* business impact. You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.

Severity 2

The problem has a *significant* business impact. The program is usable, but it is severely limited.

Severity 3

The problem has *some* business impact. The program is usable, but less significant features (not critical to operations) are unavailable.

Severity 4

The problem has *minimal* business impact. The problem causes little impact on operations, or a reasonable circumvention to the problem was implemented.

Describing problems and gathering information

When describing a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Software Support specialists can help you solve the problem efficiently. To save time, know the answers to these questions:

- Which software versions were you running when the problem occurred?
- Do you have logs, traces, and messages that are related to the problem symptoms? IBM Software Support is likely to ask for this information.
- Can you re-create the problem? If so, what steps were performed to re-create the problem?
- Did you make any changes to the system? For example, did you make changes to the hardware, operating system, networking software, and so on.

- Are you currently using a workaround for the problem? If so, be prepared to explain the workaround when you report the problem.

Submitting problems

You can submit your problem to IBM Software Support in one of two ways:

Online

Click **Submit and track problems** on the IBM Software Support site at http://www.ibm.com/software/support/probsub.html. Type your information into the appropriate problem submission form.

By phone

For the phone number to call in your country, go to the contacts page of the *IBM Software Support Handbook* at http://techsupport.services.ibm.com/guides/contacts.html and click the name of your geographic region.

If the problem you submit is for a software defect or for missing or inaccurate documentation, IBM Software Support creates an Authorized Program Analysis Report (APAR). The APAR describes the problem in detail. Whenever possible, IBM Software Support provides a workaround that you can implement until the APAR is resolved and a fix is delivered. IBM publishes resolved APARs on the Software Support Web site daily, so that other users who experience the same problem can benefit from the same resolution.

Appendix C. Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION ″AS IS″ WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not display.

Trademarks

IBM, the IBM logo, DB2®, developerWorks®, eServer™, ETE, IBMLink™, , iSeries™, MVS™, NetView, OMEGAMON, OMEGAMON II, Passport Advantage®, pSeries®, Rational®, Redbooks®, S/390®, Tivoli, Tivoli Enterprise, Tivoli Enterprise Console®, VTAM, WebSphere®, z/OS, and zSeries® are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux® is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft®, Windows, and Windows NT® are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Index

G

H

I

K

L

M

N

O

P

R

S

T

V

W

Z

Printed in USA

GI11-8116-00