



Software Group | Enterprise Networking and Transformation Solutions (ENTS)

Integrated Intrusion Detection Services for z/OS Communications Server

Lin Overby - overbylh@us.ibm.com

Trademarks and notices

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries or both:

- ▶ AIX⁷
- ▶ AnyNet⁷
- ▶ AS/400⁷
- ▶ Candle⁷
- ▶ CICS⁷
- ▶ CICSplex⁷
- ▶ CICS/ESA⁷
- ▶ DB2⁷
- ▶ DB2 Connect[™]
- ▶ DPI⁷
- ▶ DRDA⁷
- ▶ e business (logo)⁷
- ▶ ESCON⁷
- ▶ eServer[™]
- ▶ ECKD[™]
- ▶ FFST[™]
- ▶ GDDM⁷
- ▶ GDPS⁷
- ▶ HiperSockets[™]
- ▶ IBM⁷
- ▶ Infoprint⁷
- ▶ IMS[™]
- ▶ IP PrintWay[™]
- ▶ iSeries[™]
- ▶ Language Environment⁷
- ▶ MQSeries⁷
- ▶ MVS[™]
- ▶ MVS/ESA[™]
- ▶ NetView⁷
- ▶ OS/2⁷
- ▶ OS/390⁷
- ▶ Parallel Sysplex⁷
- ▶ PrintWay[™]
- ▶ PR/SM[™]
- ▶ pSeries⁷
- ▶ RACF⁷
- ▶ Redbooks[™]
- ▶ Redbooks (logo)[™]
- ▶ S/390⁷
- ▶ System/390⁷
- ▶ ThinkPad⁷
- ▶ Tivoli⁷
- ▶ Tivoli (logo)⁷
- ▶ VM/ESA⁷
- ▶ VSE/ESA[™]
- ▶ VTAM⁷
- ▶ WebSphere⁷
- ▶ xSeries⁷
- ▶ z/Architecture[™]
- ▶ z/OS⁷
- ▶ z/VM⁷
- ▶ zSeries⁷

- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- Intel, Intel Inside (logos), MMX and Pentium are trademarks of Intel 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.
- Linux is a trademark of Linus Torvalds in the United States, other countries, or both.
- Red Hat is a trademark of Red Hat, Inc.
- SUSE® LINUX Professional 9.2 from Novell®
- Other company, product, or service names may be trademarks or service marks of others.
- This information is for planning purposes only. The information herein is subject to change before the products described become generally available.
- All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All performance data contained in this publication was obtained in the specific operating environment and under the conditions described and is presented as an illustration. Performance obtained in other operating environments may vary and customers should conduct their own testing.

Refer to www.ibm.com/legal/us for further legal information.

Integrated Intrusion Detection Services

z/OS Communications Server provides an integrated Intrusion Detection Services (IDS) for TCP/IP . This session will describe the Communications Server IDS and how it can be used to detect intrusion attempts against z/OS.

This session will cover the following topics

- IDS Overview
- Intrusion events detected by z/OS IDS
- IDS Actions
 - ▶ Defensive Actions
 - ▶ Recording Actions
- IDS Reports
- Automation for IDS
- Working with IDS policy

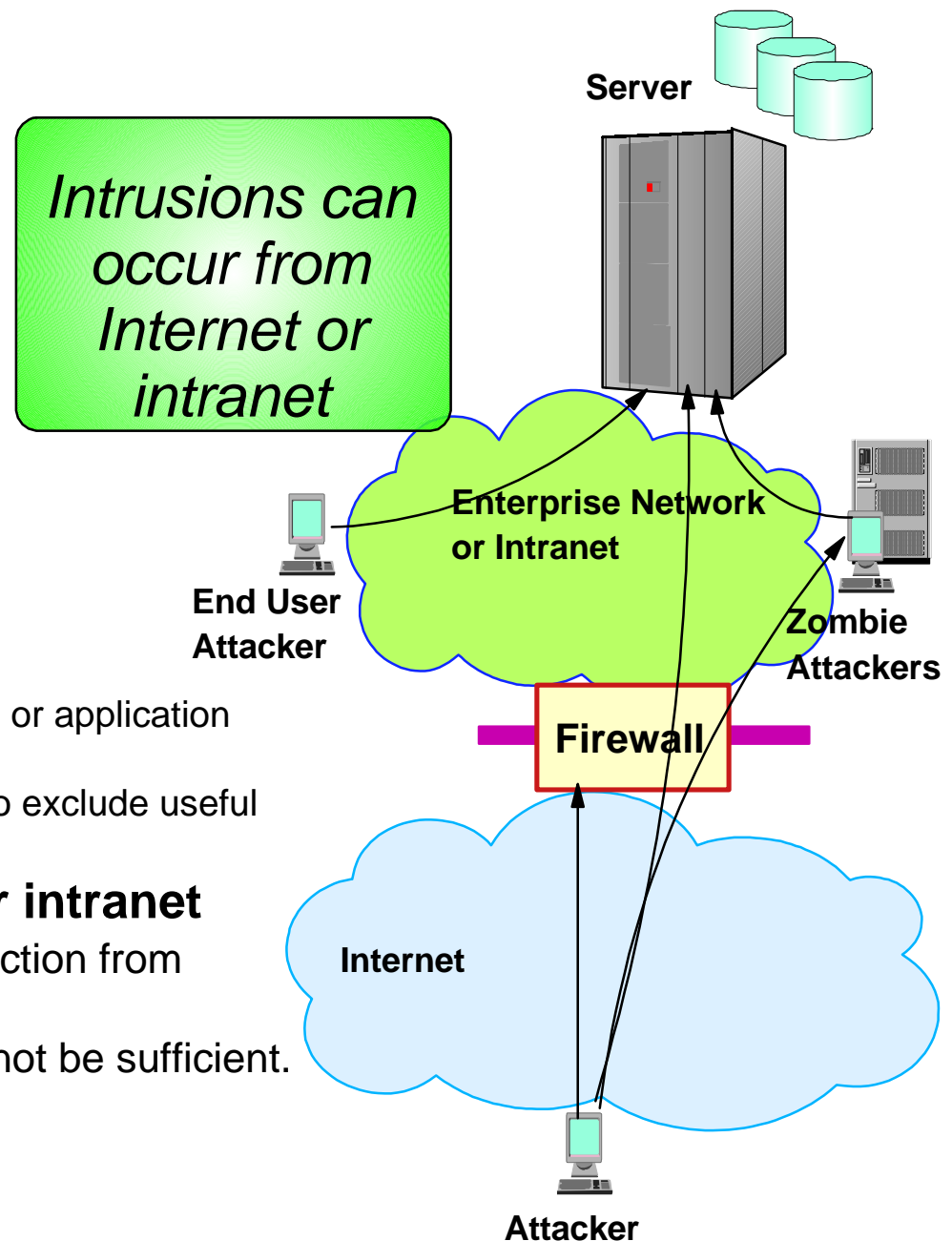
The Intrusion Threat

■ What is an intrusion?

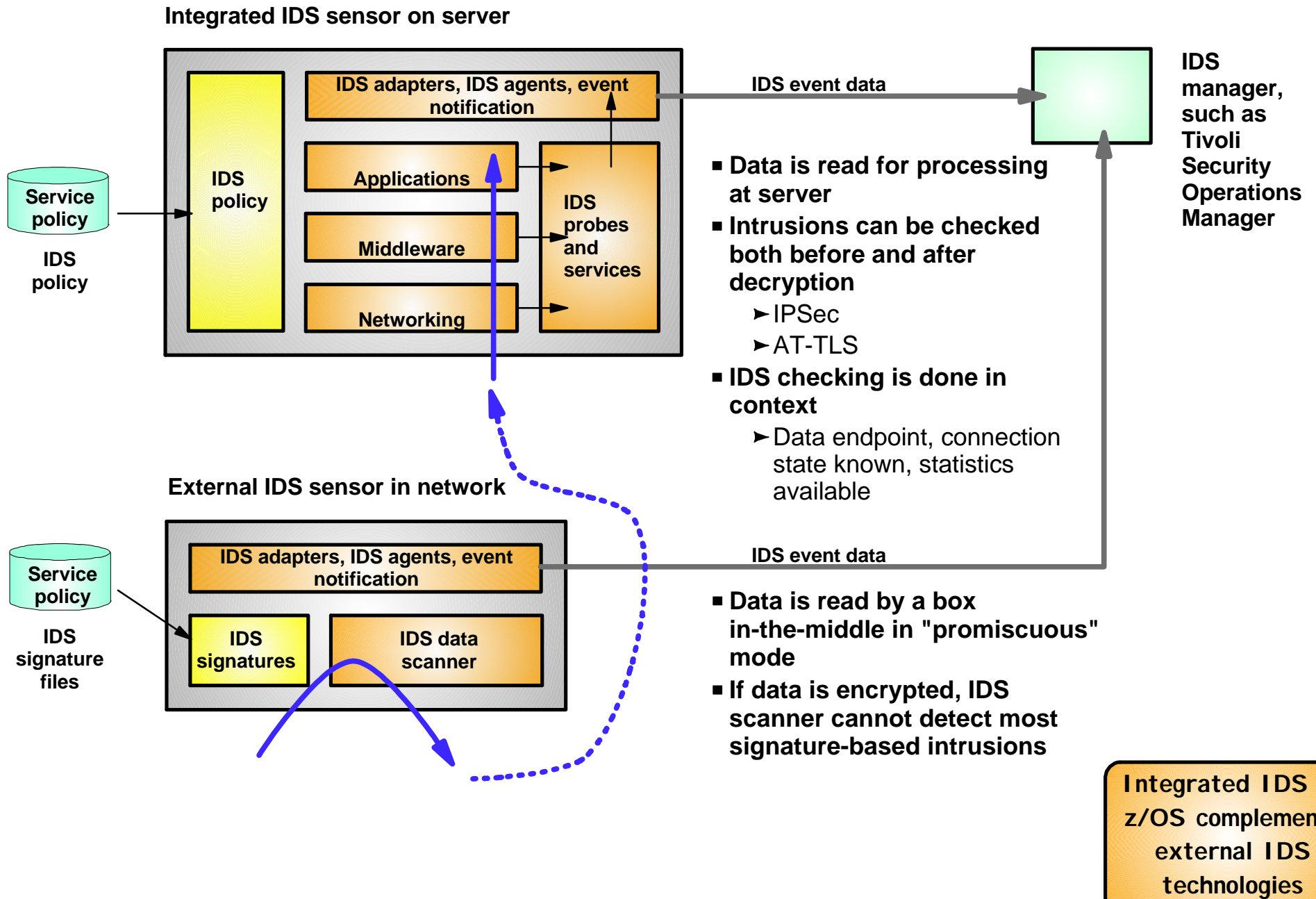
- ▶ Information Gathering
 - Network and system topology
 - Data location and contents
- ▶ Eavesdropping/Impersonation/Theft
 - On the network/on the host
 - Based for further attacks on others
 - ✓ Amplifiers
 - ✓ Robot or zombie
- ▶ Denial of Service
 - Attack on availability
 - ✓ Single Packet attacks - exploits system or application vulnerability
 - ✓ Multi-Packet attacks - floods systems to exclude useful work

■ Attacks can occur from Internet or intranet

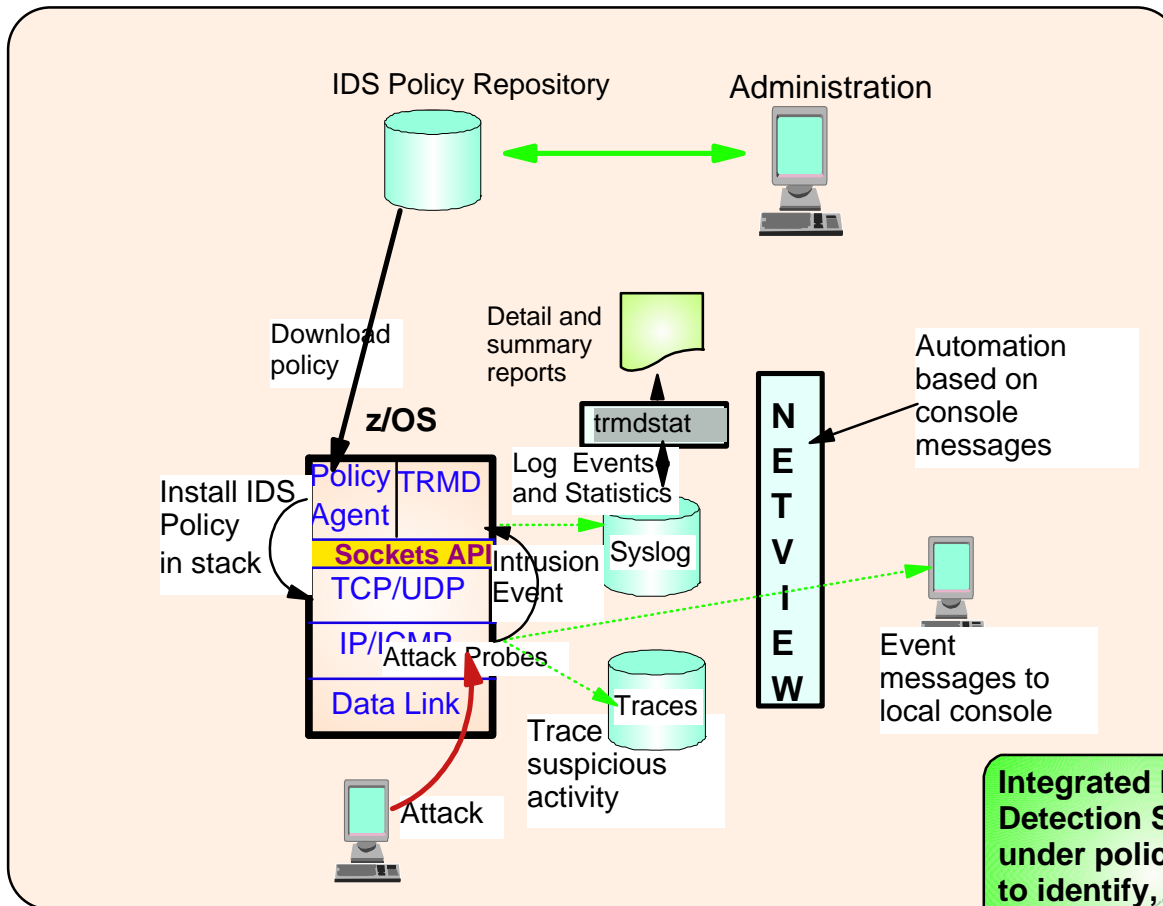
- ▶ Firewall can provide some level of protection from Internet
- ▶ Perimeter Security Strategy alone may not be sufficient.
 - Considerations:
 - ✓ Access permitted from Internet
 - ✓ Trust of intranet



Integrated vs. External Intrusion Detection Concepts



Intrusion Detection Services Overview



Events detected

- Scans
- Attacks Against Stack
- Flooding (both TCP and UDP)

Defensive methods

- Packet discard
- Limit connections

Reporting

- Logging,
- Event messages to local console,
- IDS packet trace
- Notifications to Tivoli NetView and Tivoli Security Operations Manager

IDS Policy Repositories

- LDAP
- Flat file support as LDAP alternative
- ▶ **New in V1R8**

z/OS IDS broadens intrusion detection coverage:

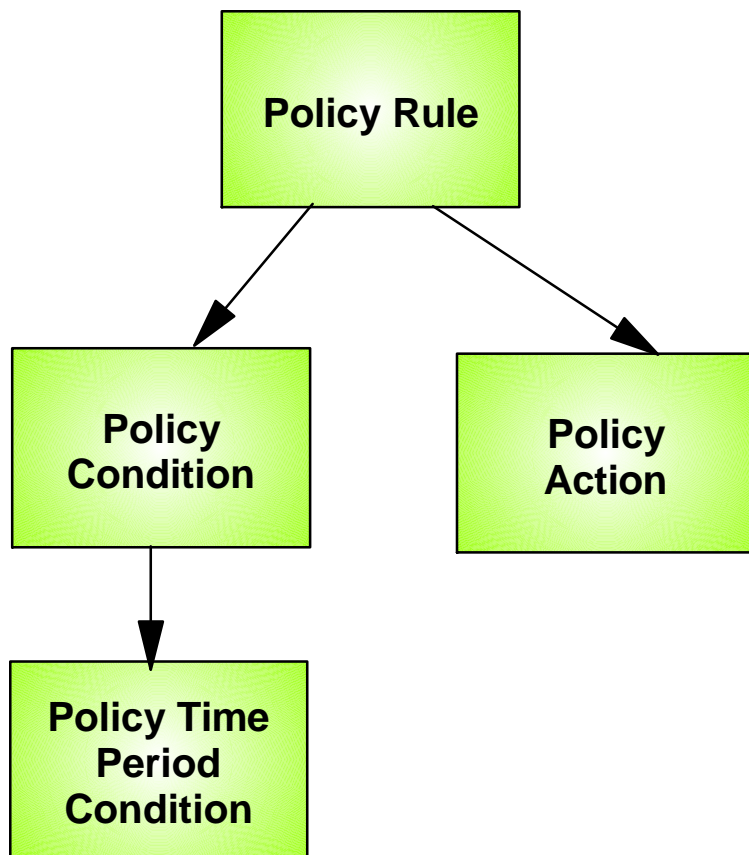
- Ability to evaluate inbound encrypted data - IDS applied after decryption on the target system
- Avoids overhead of per packet evaluation against table of known attacks - IDS policy checked after attack detected
- Detects statistical anomalies real-time - target system has stateful data / internal thresholds unavailable to external IDSs
- Policy can control prevention methods on the target, such as connection limiting and packet discard

IDS Configuration

- IDS is configured with IDS policy
 - ▶ IDS policy defines intrusion events to monitor and actions to take
- Policy definitions are stored in policy repository
 - ▶ LDAP
 - ▶ File or data set (V1R8)
- Policy Agent reads policy definitions from policy repository
 - ▶ Policy definitions are processed by Policy Agent and installed in the TCP/IP stack

Policy Model Overview

Basic Policy Objects



Policy objects relationship:
IF condition THEN action

Policies consist of several related objects

- Policy Rule is main object and refers to one or more objects:
 - ▶ Policy Condition
 - Defines IDS conditions which must be met to execute the Policy action
 - ▶ Policy Action
 - Defines IDS actions to be performed when Policy Condition is met
 - ▶ Policy Time Period Condition
 - Determines when a policy rule is active

z/OS Communications Server Security

Intrusion Events Types Detected

- **SCAN**
- **ATTACK**
- **TRAFFIC REGULATION**

Intrusion Event Types Supported

- Scan detection and reporting
 - ▶ Intent of scanning is to map the target of the attack
 - Subnet structure, addresses, masks, addresses in-use, system type, op-sys, application ports available, release levels

- Attack detection, reporting, and prevention
 - ▶ Intent is to crash or hang the system
 - Single or multiple packet

- Traffic regulation for TCP connections and UDP receive queues
 - ▶ Could be intended to flood system OR could be an unexpected peak in valid requests

Scanning... the prelude to the attack

- z/OS IDS definition of a scanner
 - ▶ Source host that accesses multiple unique resources (ports or interfaces) over a specified time period
 - Installation can specify via policy number of unique events (Threshold) and scan time period (Interval)
- Categories of scan detection supported
 - ▶ Fast scan
 - Many resources rapidly accessed in a short time period (less than 5 minutes)
 - ✓ usually less than five minutes, program driven
 - ▶ Slow scans
 - Different resources intermittently accessed over a longer time period (many hours)
 - ✓ scanner trying to avoid detection
- Scan events types supported
 - ▶ ICMP scans
 - ▶ TCP port scans
 - ▶ UDP port scans

Scan Policy Overview

Scan policy provides the ability to:

- Obtain notification and documentation of scanning activity
 - ▶ Notify the installation of a detected scan via console message or syslogd message
 - ▶ Trace potential scan packets
- Control the parameters that define a scan:
 - ▶ The time interval
 - ▶ The threshold
- Reduce level of false positives
 - ▶ Exclude well known "legitimate scanners" via exclusion list
 - e.g. network management
 - ▶ Specify a scan sensitivity level
 - by port for UDP and TCP
 - highest priority rule for ICMP

Scan Event Counting and Scan Sensitivity

- Scan sensitivity determines whether a scan event is "countable"

Sensitivity (from policy)	Normal Event	Possibly Suspicious Event	Very Suspicious Event
Low			Count
Medium		Count	Count
High	Count	Count	Count

- Countable scan events count against an origin source IP address
 - ▶ Total number of countable events for all scan event types is compared to policy thresholds
 - If threshold exceeded for a single IP address, policy-directed notification and documentation is triggered
- Balance between detecting every scan and limit overhead
 - ▶ Reserve low ports not explicitly in use to allow configuration of low sensitivity on low ports for both UDP and TCP
- Scan instance event classification by event type included in appendix A

Attacks Against The TCP/IP Stack

- The system already silently defends itself from many attacks against the TCP/IP stack.
- IDS adds capability to control recording intrusion events and supporting documentation.
- IDS adds controls to detect and disable uncommon or unused features which could be used in an attack.

Attack Categories

- Malformed packet events
 - ▶ Detects packets with incorrect or partial header information
- Inbound fragment restrictions
 - ▶ Detects fragmentation in first 256 bytes of a datagram
- IP protocol restrictions
 - ▶ Detects use of IP protocols you are not using that could be misused
- IP option restrictions
 - ▶ Detects use of IP options you are not using that could be misused
- UDP perpetual echo
 - ▶ Detects traffic between UDP applications that unconditionally respond to every datagram received
- ICMP redirect restrictions
 - ▶ Detects receipt of ICMP redirect to modify routing tables.
- Outbound RAW socket restrictions
 - ▶ Detects z/OS RAW socket application crafting invalid outbound packets
- Flood Events
 - ▶ Detects flood of SYN packets from "spoofed" sources
 - ▶ Detects high percentage of packet discards on a physical interface

Attack Policy Overview

Attack policy provides the ability to:

- Control attack detection for one or more attack categories independently
- Obtain notification and documentation of attacks
 - ▶ Notify the installation of a detected attack via console message or syslogd message
 - ▶ Trace potential attack packets
- Allows request for attack statistics on time interval basis
 - ▶ Normal or Exception
- Control defensive action when attack is detected

Interface Flood Detection

- Packet discard rate by physical interface is tracked to determine if there is a potential attack
 - ▶ A high percentage of discarded packets on a physical interface may indicate the interface is under attack.
- Notification and traces provided when a possible interface flood condition is occurring if the discard rate exceeds a specified limit.
- Provides information to help determine the potential cause of the interface flood
 - ▶ Narrows flood condition to a local interface so
 - Vary interface offline
 - ✓ This action not controlled with IDS policy
 - Start tracing flood back to source
 - ▶ Source MAC address of the "prior hop" for:
 - LCS devices
 - OSA QDIO with microcode level that supports providing the source MAC address
 - ▶ Source IP address from the outer IPSec header if the packet had been received as IPsec tunnel mode.
 - Source IP address could be a gateway or firewall
 - ✓ Could allow source tracking closer to the source than "prior hop"

Interface Flood Detection Process

- Policy related to interface flood detection
 - ▶ Part of Attack Flood support
 - ▶ 2 new actions attributes provided
 - ibm-idsIfcFloodMinDiscard (default 1000)
 - ibm-idsIfcFloodPercentage (default 10)
- For each interface, counts are tracked for
 - ▶ The number of inbound packets that arrived over the physical interface
 - ▶ The number of these packets that are discarded
- When the specified number of discards (ibm-idsIfcFloodMinDiscard) is hit:
 - ▶ If it took longer than 1 minute to accumulate the discards, doesn't qualify as a flood condition
 - ▶ If the discards occurred in a minute or less:
 - the discard rate is calculated for the interval :
 - ✓ # discards during the interval / # inbound packets for the interval
 - If the discard rate equals or exceeds the specified threshold, an interface flood condition exists
- Once an interface flood is detected, this data is collected and evaluated for the interface at 1 minute intervals. The interface flood is considered ended if the discards for a subsequent interval:
 - ▶ Fall below the minimum discard value OR
 - ▶ Discard rate for the interval is less than or equal to 1/2 of the specified threshold

Interface Flooding Example

- Assume the IDS flood policy specifies:
 - ▶ ibm-idslfcFloodMinDiscard:2000
 - ▶ ibm-idslfcFloodPercentage:10

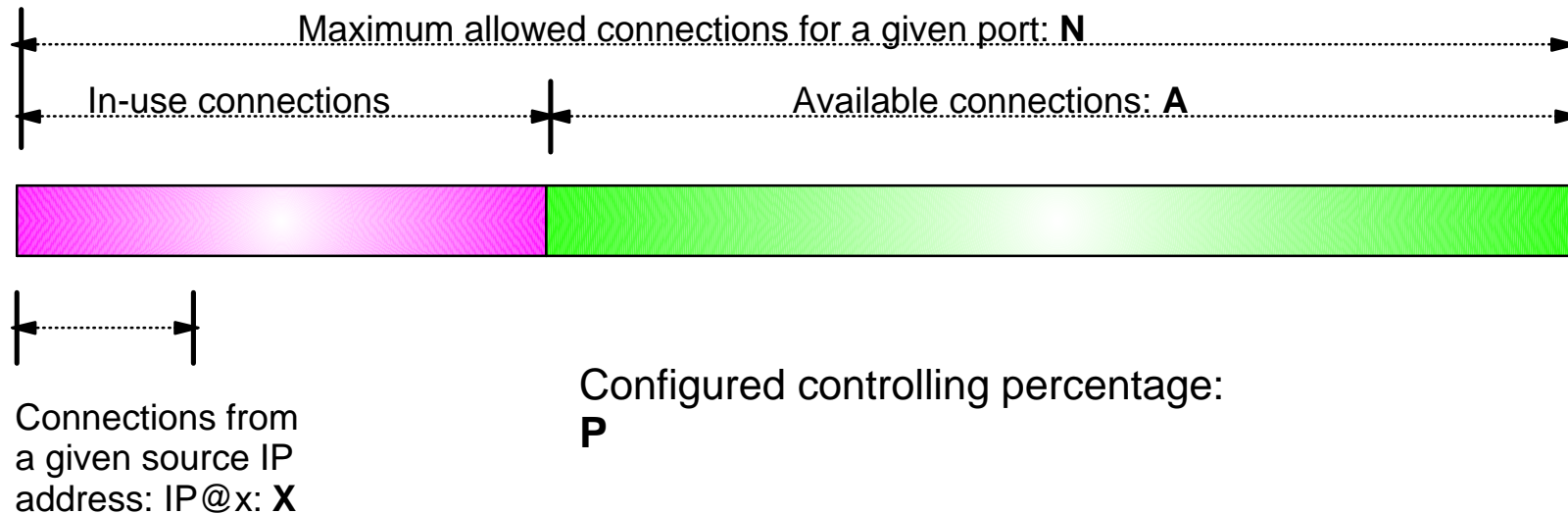
- The activity for interface X is as shown in the table below:

time interval	inbound cnt	discard cnt	discard rate	notes
> 1 min	13,000	2000	N/A	took longer than a minute to see the minimum discard count, so not a flood and discard rate not calculated.
< 1 min	30,000	2000	6.6%	not a flood, rate <10%
< 1 min	20,000	2000	10%	interface flood start detected. Run 1 minute timer until flood end detected.
1 min	40,000	3000	7.5%	flood condition still exists, reset 1 minute timer.
1 min	50,000	2500	5%	Interface flood end detected. Discard rate <= half of policy specified rate.

Traffic Regulation for TCP

- Allows control over number of inbound connections from a single host
 - ▶ Can be specified for specific application ports
 - Especially for forking applications
 - ▶ Independent policies for multiple applications on the same port
 - e.g. telnetd and TN3270
- Connection limit expressed as
 - ▶ Port limit for all connecting hosts
 - ▶ Individual limit for a single host
- Fair share algorithm
 - ▶ Connection allowed if specified individual limit per single remote IP address does not exceed percent of available connections for the port
 - All remote hosts are allowed at least one connection as long as port limit has not been exceeded
 - ✓ QoS connection limit used as override for concentrator sources (web proxy server)

TCP connection regulation algorithm



If a new connection request is received and $A=0$, the request is rejected.

If a new connection request is received and $A>0$ and the request is from a source that already has connections with this port number (in this example: IP@x), then:

If $X+1 < P*A$ then
 Allow the new connection
Else
 Deny the new connection

Purpose: If close to the connection limit, then a given source IP address will be allowed only a small number of the in-use connections..

Regulation algorithm example

Total Allowed	Available	10%	20%	30%	40%
100	80	8	16	24	32
100	60	6	12	18	24
100	40	4	A 8	12	16
100	20	2	4 B	6	8
100	10	1	2	3	4

- A** If we currently have 60 connections (40 available), the controlling percentage is 20%, and a source IP address tries to establish its connection number 6, it will be allowed.
- B** If the number of connections in use rise to 80 (20 available), the controlling percentage is again 20%, and the same source IP address tries to establish its connection number 6, it will be rejected.

Traffic Regulation for UDP

- Allows control over length of inbound receive queues for UDP applications
 - ▶ Can be specified for specific application ports
- Before TR for UDP, UDP queue limit control was requested globally for all queues
 - ▶ UDPQueueLimit ON | OFF in TCP/IP Profile
- If neither TR UDP or UDPQueueLimit is used, a stalled application or a flood against a single UDP port could consume all available buffer storage
 - ▶ TR UDP supercedes UDPQueueLimit specification
- TR UDP queue limit expressed as abstract queue length
 - ▶ VERY SHORT
 - ▶ SHORT
 - For applications that consistently receive data at higher rates than can be processed
 - ▶ LONG
 - ▶ VERY LONG
 - Useful for fast applications with bursty arrival rates

z/OS Communications Server Security

IDS Actions

- **Defensive actions**
- **Recording actions**

Defensive Actions by Event Type

- Scan Events
 - ▶ No defensive action defined
- Attack Events
 - ▶ Packet discard
 - Certain attack events always result in packet discard and are not controlled by IDS policy action
 - ✓ malformed packets
 - ✓ flood (synflood discard)
 - Some attack types controlled by IDS policy action
 - ✓ ICMP redirect restrictions
 - ✓ IP option restrictions
 - ✓ IP protocol restrictions
 - ✓ IP fragment
 - ✓ outbound raw restrictions
 - ✓ perpetual echo
 - ▶ No defensive action defined
 - ✓ flood (interface flood detection)
- Traffic Regulation Events
 - ▶ Controlled by IDS policy action
 - TCP - Connection limiting
 - UDP - Packet discard

Recording Actions

- Recording options controlled by IDS policy action specification
- Options
 - ▶ Event logging
 - Syslogd
 - ✓ Number of events per attack subtype recorded in a five minute interval is limited
 - Local Console
 - ✓ Recording suppression provided if quantity of IDS console messages reach policy-specified thresholds
 - ▶ Statistics
 - Syslogd
 - ✓ Normal, Exception
 - ▶ IDS packet trace
 - Activated after attack detected
 - ✓ Number of packets traced for multi-packet events are limited
 - ✓ Amount of data trace is configurable (header, full, byte count)
- All IDS events recorded in syslog and console messages, and packet trace records have probeid and correlator
 - ▶ Probeid identifies the specific event detected
 - ▶ Correlator allows events to be matched with corresponding packet trace records

z/OS Communications Server Security

Intrusion Detection Reports for Analysis

IDS Log Reports

trmdstat program produces reports based on IDS data recorded to syslog

- Types of reports generated for logged events
 - ▶ Overall summary reports
 - Connection and IDS
 - ▶ Event type summary reports
 - For Connection, Attack, Flood, Scan, TCP and UDP information
 - ▶ Event type detail reports
 - For Connection, Attack, Flood, Scan, TCP and UDP information
- Types of reports generated for statistics events
 - ▶ Details reports
 - Attack, TCP, and UDP reports

Tivoli Support for IDS Events

- Tivoli NetView z/OS V5R1, PTF UA11043, provides local z/OS management support for IDS
 - ▶ NetView provides ability to trap IDS messages from the system console or syslog and take predefined actions based on IDS event type such as:
 - Route IDS messages to designated NetView consoles
 - email notifications to security administrator
 - Run trmdstat and attach output to email
 - Issue pre-defined commands
- Tivoli Security Operations Manager provides enterprise-wide management support for IDS
 - ▶ Automated aggregation and correlation of events, logs, and vulnerabilities
 - Broad device support for multi-vendor environments, including security, network, host, and applications
 - Support includes processing for z/OS Communications Server syslog messages for IDS events
 - ▶ Automates policy and regulatory compliance
 - Policy and Regulatory based policy monitoring and reporting

z/OS Communications Server Security

Working with IDS Policy

- **Controlling, Displaying, and Validating Policy**
 - **Defining IDS Policy**
 - **IDS Policy Configuration with Configuration Assistant for z/OS**
- Examples**

Controlling Active IDS Policy

■ Configurable policy deletion controls

- ▶ Tcplmage statement in policy configuration file ..
 - FLUSH | NOFLUSH {PURGE | NOPURGE} 1800
- ▶ FLUSH and NOFLUSH take effect at Policy Agent initialization
 - FLUSH - specifies that any active policy should be deleted
 - NOFLUSH - specifies that active policy should not be deleted
- ▶ PURGE and NOPURGE take effect at Policy Agent termination
 - PURGE - specifies that any active policy should be deleted
 - NOPURGE - specifies that active policy should not be deleted

■ Refresh Policy

- At Interval (1800-second default)
- With MODIFY PAGENT command (REFRESH option)
- When Policy Agent configuration file (HFS only) is updated (refresh is automatic)

Displaying IDS Policy

- `pasearch` command
 - ▶ Displays IDS policy read by Policy Agent
- `netstat` command
 - ▶ Displays installed IDS policy in TCP/IP stack
 - ▶ Displays statistics by policy category

✓ Tip:

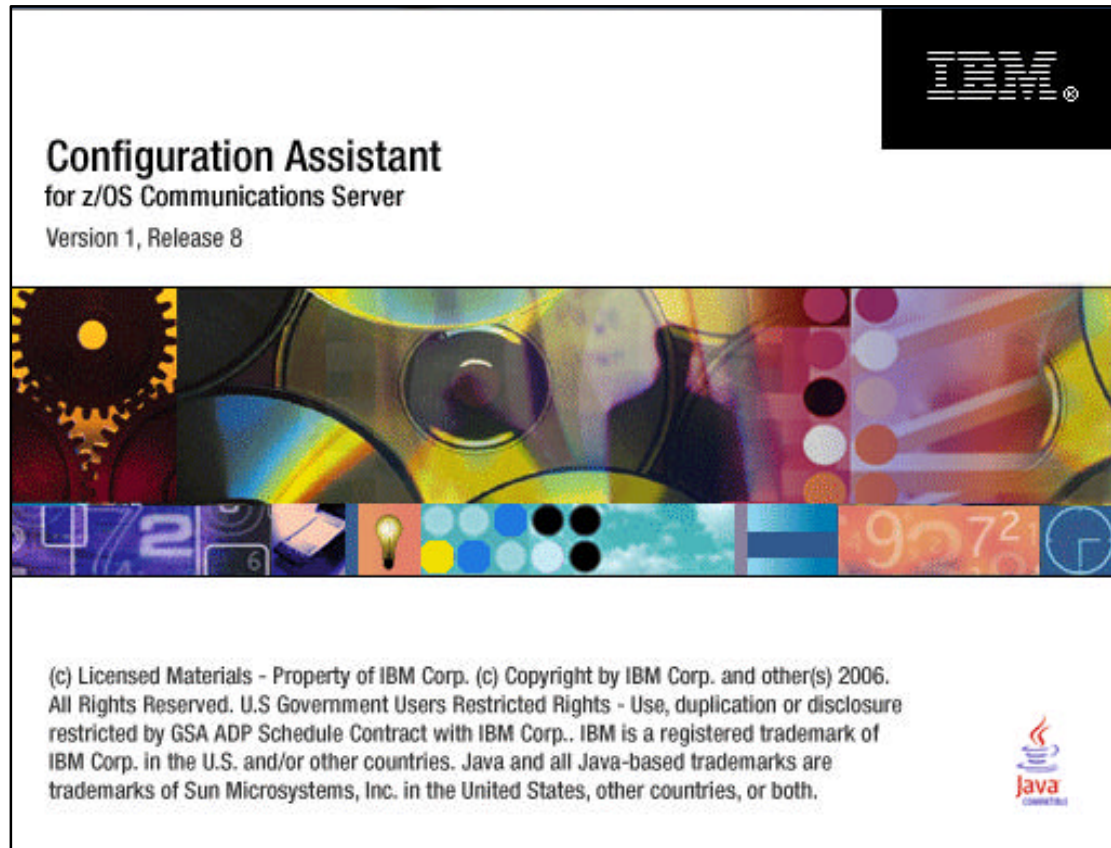
Restrict access to IDS policy displays using SAF SERVAUTH resources:

- ▶ `EZB.PAGENT.sysname.tcpname.IDS`
- ▶ `EZB.NETSTAT.sysname.tcpname.IDS`

Steps for Validating IDS Policy

1. Inspect configured IDS policy for correctness
2. Invoke PAGENT and TRMD
3. Issue PASEARCH
 - a. Verify the correct policy is installed
4. Keep policy in force for a trial period
5. Issue IDS netstat to view active IDS policy and statistics
6. Verify syslog messages document intrusions
 - a. Display syslog
 - b. Run TRMDSTAT reports
7. Adjust the policy as required

Defining IDS Policy



- In z/OS V1R8 the Policy Agent configuration tools are combined into one tool to manage policies for:
 - ▶ AT-TLS
 - ▶ IPsec and IP packet filtering
 - ▶ IDS
 - ▶ QoS
- Common approach for all policy types:
 - ▶ Master copy stored in binary file format (on workstation or file server)
 - ▶ Text-based configuration files to be parsed by Policy Agent are created and transferred to z/OS

Note: IDS policies may now be stored in a text file, just as the other policy types. There is no requirement for LDAP.

- V1R7 - Network Security Configuration Assistant
 - ▶ Configured policy for IPsec, IP packet filtering, and AT-TLS
- V1R8 - (Name change) Configuration Assistant for z/OS Communications Server
 - ▶ Adds policy configuration support for IDS and QoS

Downloadable policy configuration tool:

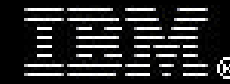
<http://www-1.ibm.com/support/docview.wss?rs=206&uid=swg21181698>

Note: Policy in LDAP can continue to be configured with the zIDS Configuration Manager

IDS Policy Configuration Steps with the Configuration Assistant

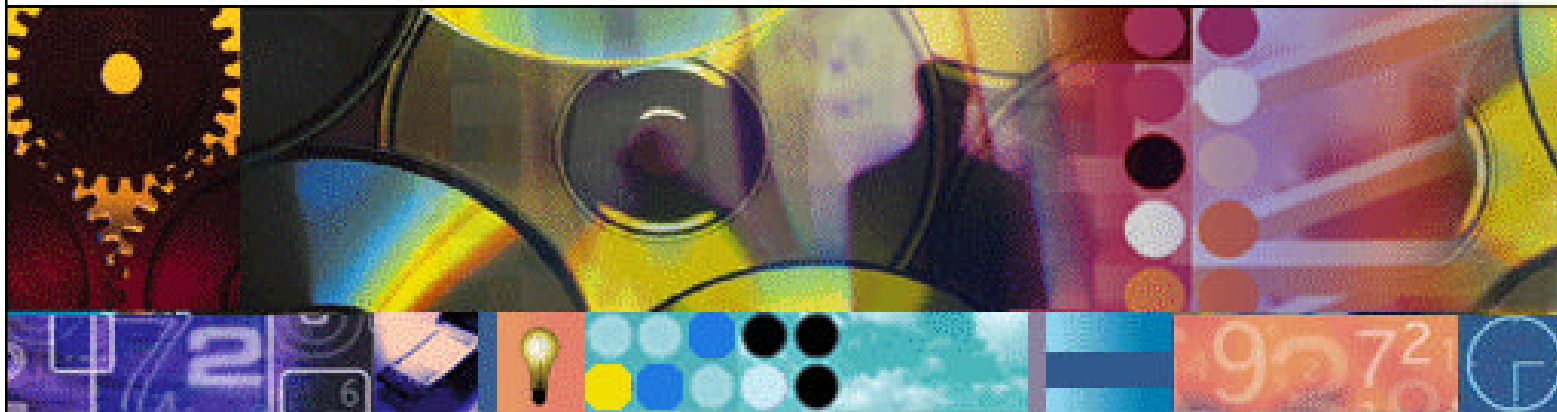
1. Download and install the Configuration Assistant configuration tool
<http://www.ibm.com/software/network/commserver/zos/support/>
2. Configure IDS policies
 - a. Examine IDS defaults and base policy on defaults
 - b. Copy IDS defaults into a new IDS requirements map
 - c. Make changes to new requirements map as needed
3. Create system image and TCP/IP stack image
4. Associate new requirements map with TCP/IP stack
5. Transfer IDS policy to z/OS

Configuration Assistant for z/OS Communications Server



Configuration Assistant for z/OS Communications Server

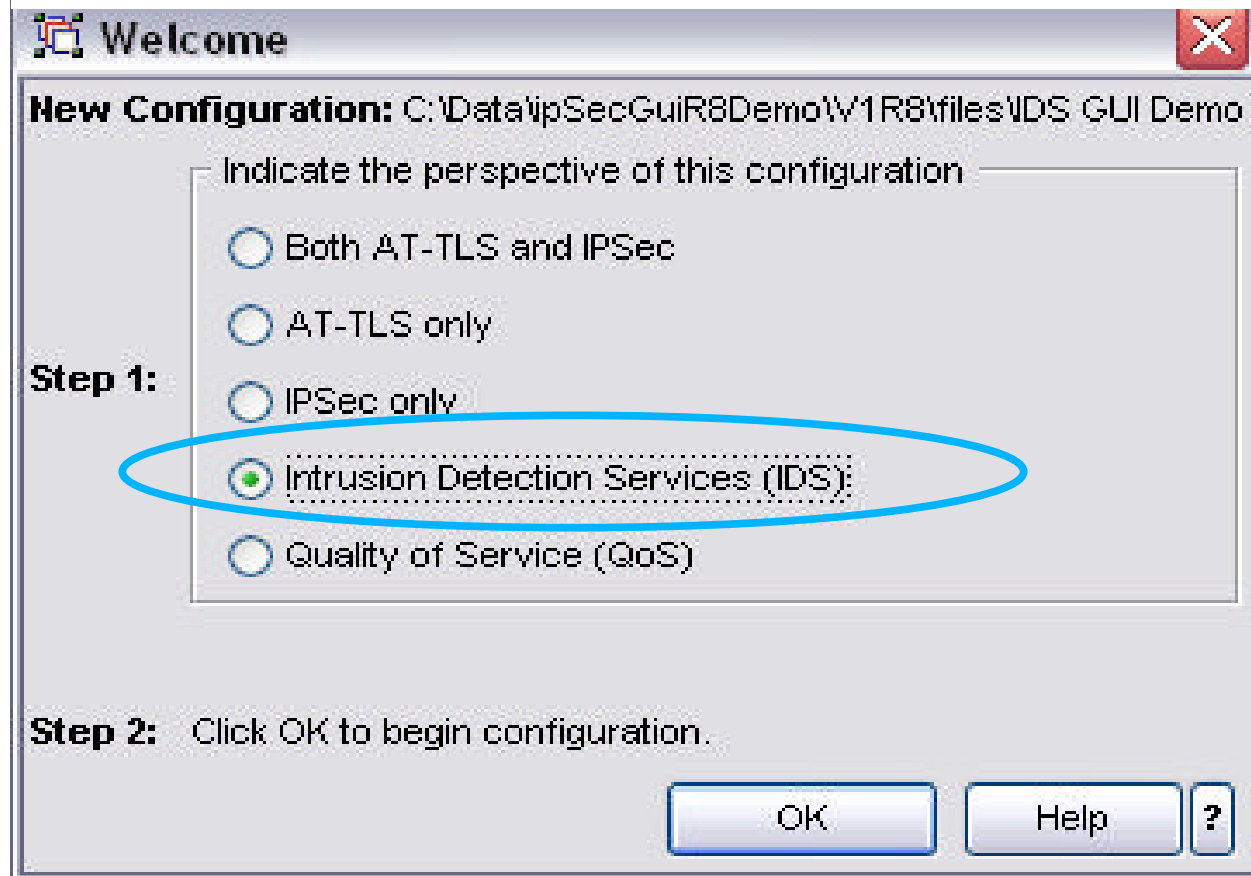
Version 1, Release 8



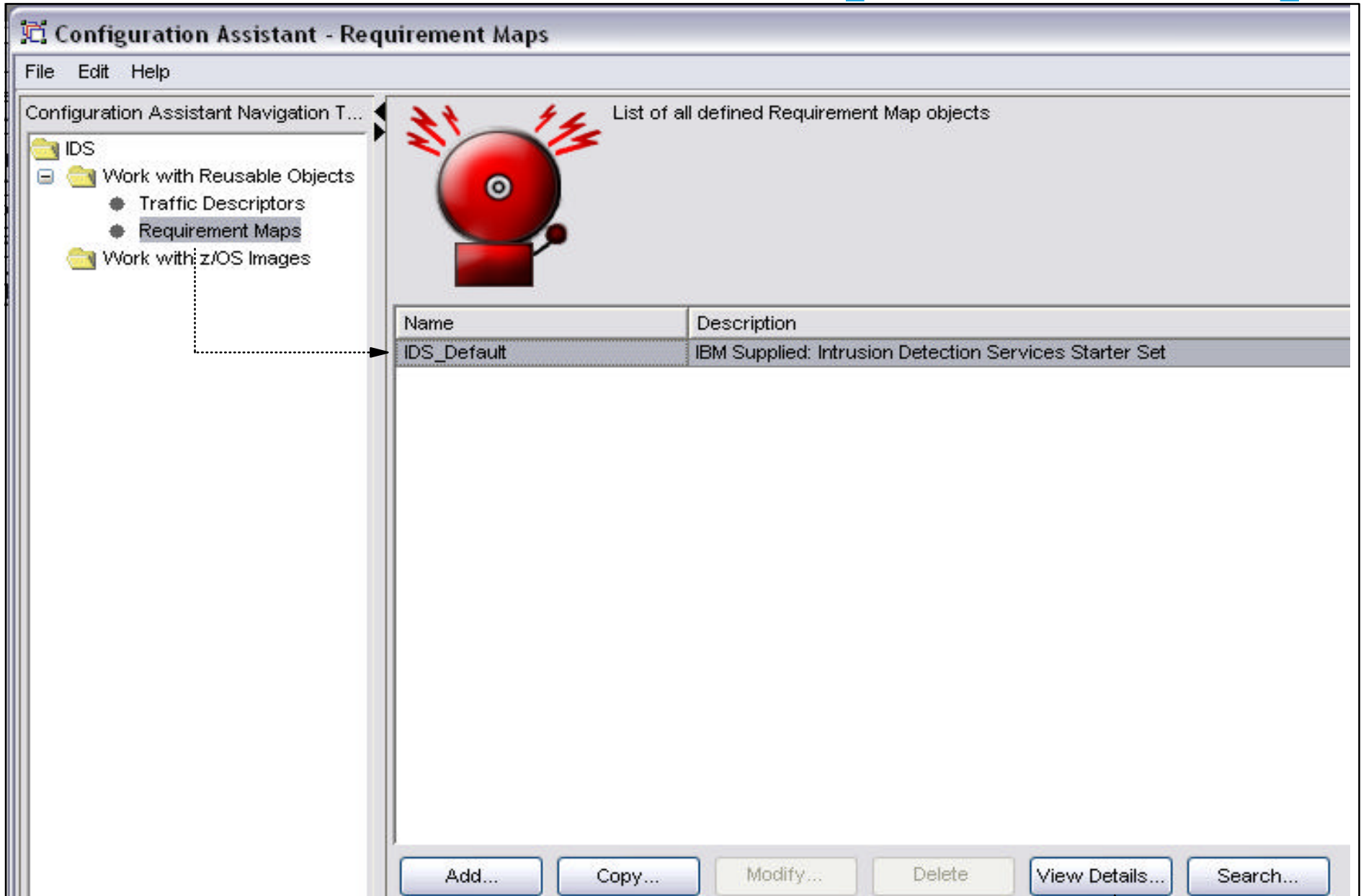
(c) Licensed Materials - Property of IBM Corp. (c) Copyright by IBM Corp. and other(s) 2006.
All Rights Reserved. U.S Government Users Restricted Rights - Use, duplication or disclosure
restricted by GSA ADP Schedule Contract with IBM Corp.. IBM is a registered trademark of
IBM Corp. in the U.S. and/or other countries. Java and all Java-based trademarks are
trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.



Start a new IDS configuration



Evaluate IDS_Default Requirements Map



IDS_Default provided as default requirement map

- Display details of the requirement map
- Evaluate whether they meet your requirements

Details View of IDS_Default Requirements Map (1 of 4)

Help

Requirement Map: IDS_Default - IBM Supplied: Intrusion Detection Services Starter Set

Attack Protection Summary

Enabled Attack Protection	Rule Name	Actions	Reports	Time Condition	Report Settings
Flood Attack	Flood	Both Discard and Report	Inherited	None	Console Parameters: No ----- SYSLOG Parameters: SYSLOG: Yes SYSLOG Level: 4 - Warning ----- Statistics Parameters: Statistics: Yes Statistics Interval: 60 Report Stat if no events: No ----- Trace Parameters: No
Perpetual Echo Attack	Echo	Report Events	Inherited	None	
Unwanted IP Protocols Attack	IPProtocol	Report Events	Inherited	None	
Unwanted IP Options Attack	IPOption	Report Events	Inherited	None	
ICMP Redirect Attack	ICMPRedirect	Report Events	Inherited	None	
Malformed Packet Attack	MalformedPacket	Both Discard and Report	Inherited	None	
Outbound Raw Attack	OutboundRaw	Report Events	Inherited	None	
IP Fragment Attack	IPFragmentation	Report Events	Inherited	None	

Details View of IDS_Default Requirements Map (2 of 4)

Help

< >

Attack Protection Details

Enabled Attack Protection: Flood Attack - Flood

Flood Minimum Discard	Flood Percentage	Reports	Time Condition
1000	10	Inherited	None

Enabled Attack Protection: Perpetual Echo Attack - Echo

Traffic Descriptor	Port Location	Reports	Time Condition
7 - Echo	Both Local and Remote	Inherited	None
13 - Time Of Day	Both Local and Remote		
17 - Quote Of The Day	Both Local and Remote		
19 - Char Gen	Both Local and Remote		

Details View of IDS_Default Requirements Map (3 of 4)

Enabled Attack Protection: Unwanted IP Protocols Attack - IPProtocol

Starting Protocol	Ending Protocol	Reports	Time Condition
0	0	Inherited	None
3	3		
5	5		
7	16		
18	45		
48	49		
52	88		
90	93		
95	255		

Enabled Attack Protection: Unwanted IP Options Attack - IPOption

Starting Option	Ending Option	Reports	Time Condition
2	6	Inherited	None
8	67		
69	81		
83	255		

Details View of IDS_Default Requirements Map (4 of 4)

Enabled Attack Protection: Outbound Raw Attack - OutboundRaw

Starting Protocol	Ending Protocol	Reports	Time Condition
0	0	Inherited	None
2	88		
90	255		

Enabled Attack Protection: IP Fragment Attack - IPFragmentation

Reports	Time Condition
Inherited	None

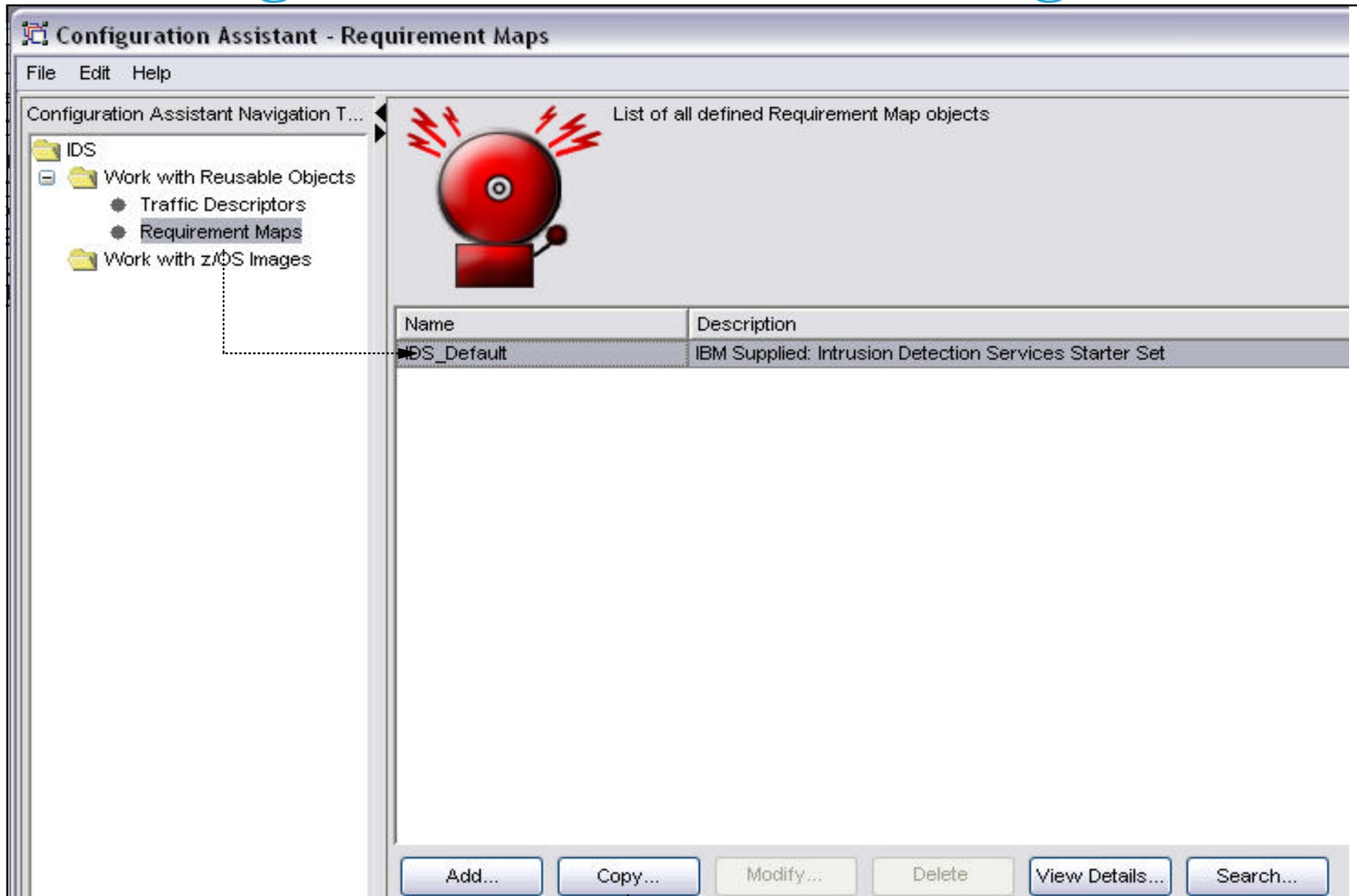
Scan Protection Summary

No Scan Protection Configured

Traffic Regulation Summary

No Traffic Regulation Configured

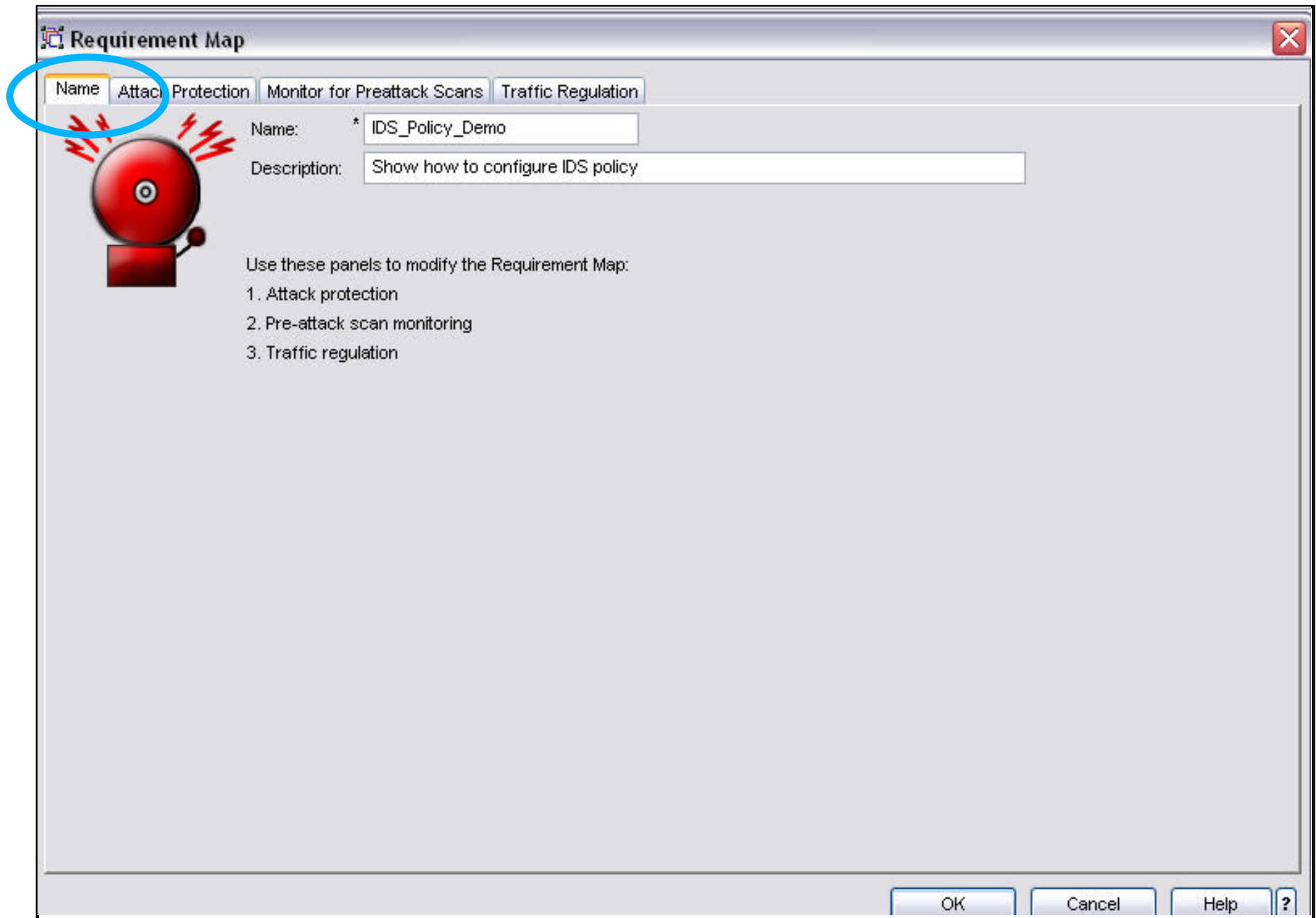
Using IDS_Default as a Starting Point



Using IDS_Default as a base

- Copy IDS_Default
- Create new requirements map using copied IDS_Default as a base

Name new requirements map



Attack protection enabled by default

ion Assistant - Requirement Maps

Requirement Map

Name: **Attack Protection** | Monitor for Preattack Scans | Traffic Regulation

Use this panel to indicate if you want attack protection

Enable attack protection

Attack protection requirements

Steps

1. Select the action for each enabled attack type.
2. To disable protection for an attack type, select the row from the Enabled protection table and click the "Disable" button.
3. To enable protection for a specific attack type, select from the Disabled protection table and click the "Enable..." button.

You will be prompted for additional details related to your attack type selection. Fill in the details and click OK.

Enabled protection			Disabled protection	
Attack Type	Rule Name	Action	<-- Enable	Attack Type
Flood Attack	Flood	Both Discard and Report	Disable -->	
Perpetual Echo Attack	Echo	Report Events		
Unwanted IP Protocols Attack	IPProtocol	Report Events		
Unwanted IP Options Attack	IPOption	Report Events		
ICMP Redirect Attack	ICMPRedirect	Report Events		
Malformed Packet Attack	MalformedPacket	Both Discard and Report		
Outbound Raw Attack	OutboundRaw	Report Events		
IP Fragment Attack	IPFragmentation	Report Events		

Modify... Copy... Advanced... View Details...

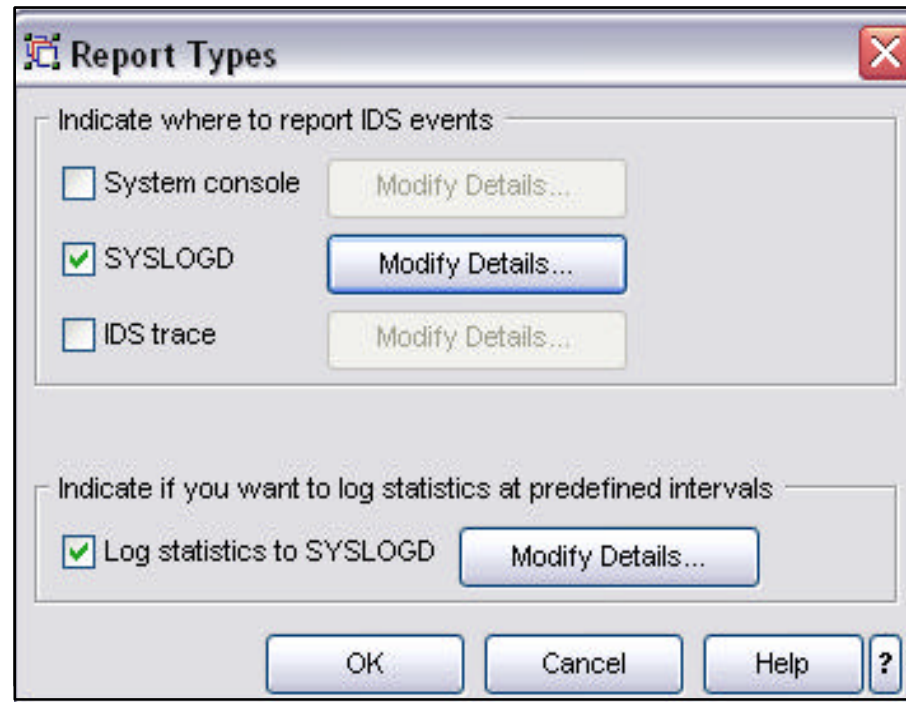
Customized report settings for attack protection

Default Report Settings for Attacks...

next page

Page 45

Customize report settings



Enable Scan Policy

Requirement Map

Name: Attack Protection, **Monitor for Preattack Scans**, Traffic Regulation

Use this panel to indicate if you want to monitor for preattack scans

Enable scan

Scan requirements

Steps

1. To enable a scan for a particular Traffic Descriptor, select from the Traffic Descriptors table and click the "Enable" button.
2. Select the monitor level for each enabled scan.
3. To disable scan protection for a Traffic Descriptor, select the row from the Enabled scans table and click the "Disable" button.

Enabled scans

Traffic Descriptor	Rule Name	Sensitivity
All_Well-Known_TCP	All_Well-Known_TCP	Medium
All_Well-Known_UDP	All_Well-Known_UDP	Medium
ICMP	ICMP	High

Buttons: <-- Enable, Disable -->

Traffic Descriptors

- CICS
- DNS
- EE
- FTP-Server
- FTP-Server-SSL
- IVE

Buttons: Work with Traffic Descriptors

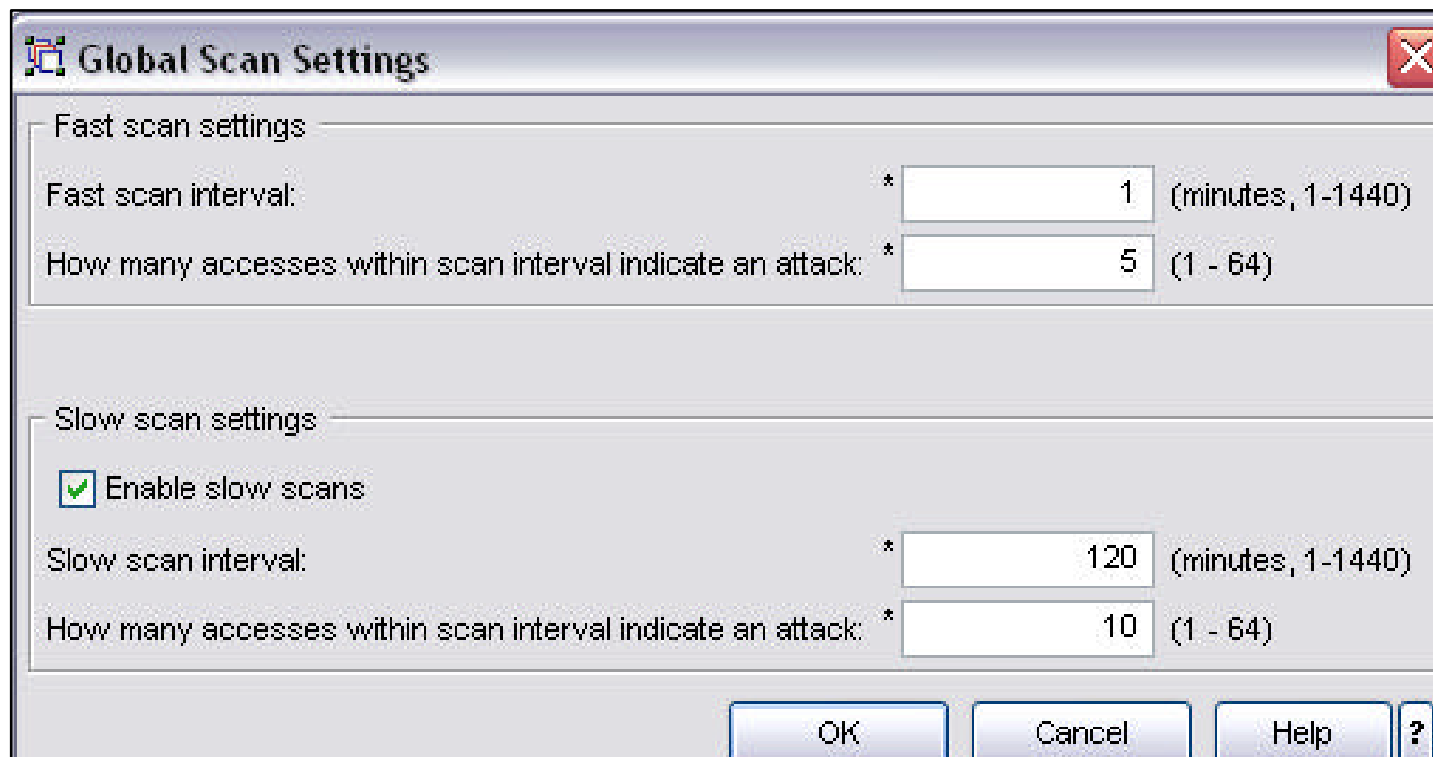
Additional scan protection parameters

Modify Fast and Slow Scan Settings... → next page

Default Report Settings for Scans...

Buttons: OK, Cancel, Help, ?

Modify Global Scan Settings



The image shows a dialog box titled "Global Scan Settings" with a close button (X) in the top right corner. The dialog is divided into two sections: "Fast scan settings" and "Slow scan settings".

Fast scan settings

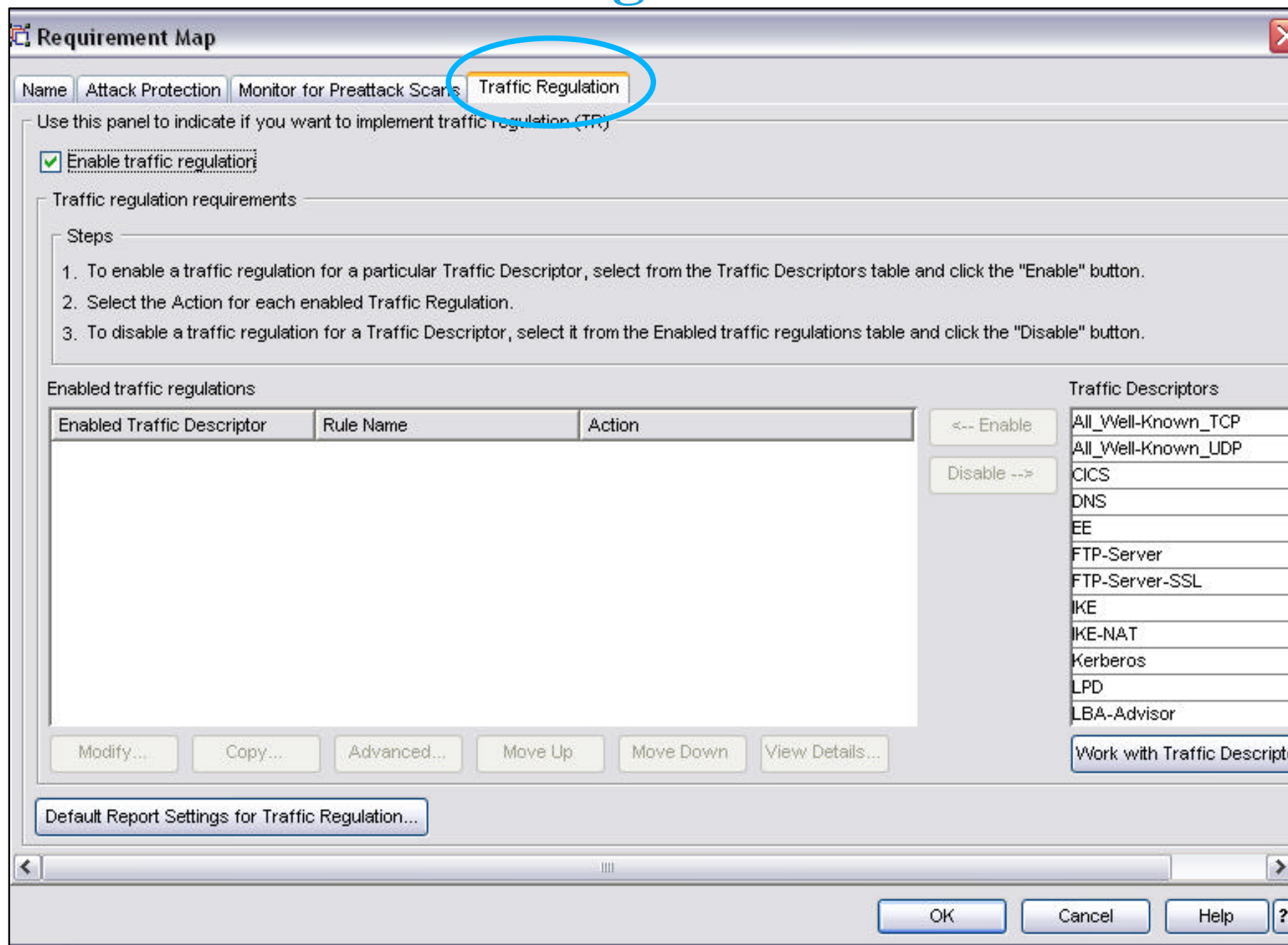
- Fast scan interval: * (minutes, 1-1440)
- How many accesses within scan interval indicate an attack: * (1 - 64)

Slow scan settings

- Enable slow scans
- Slow scan interval: * (minutes, 1-1440)
- How many accesses within scan interval indicate an attack: * (1 - 64)

At the bottom of the dialog, there are four buttons: "OK", "Cancel", "Help", and a question mark icon.

Enable Traffic Regulation Protection



No traffic regulation defaults

- Policy selections are very system dependant
- System capacity a consideration in setting maximum limits

Define TCP TR Policy for FTP

Requirement Map

Name: Attack Protection | Monitor for Preattack Scans | **Traffic Regulation**

Use this panel to indicate if you want to implement traffic regulation (TR)

Enable traffic regulation

Traffic regulation requirements

Steps

1. To enable a traffic regulation for a particular Traffic Descriptor, select from the Traffic Descriptors table and click the "Enable" button.
2. Select the Action for each enabled Traffic Regulation.
3. To disable a traffic regulation for a Traffic Descriptor, select it from the Enabled traffic regulations table and click the "Disable" button.

Enabled traffic regulations

Enabled Traffic Descriptor	Rule Name	Action
FTP-Server-SSL	FTP-Server-SSL	Limit and Report
FTP-Server	FTP-Server	Limit and Report

Traffic Descriptors

- All_Well-Known_TCP
- All_Well-Known_UDP
- CICS
- DNS
- E
- IKE
- IKE-NAT
- Kerberos
- LPD
- LBA-Advisor
- LBA-Agent
- LDAP-Server

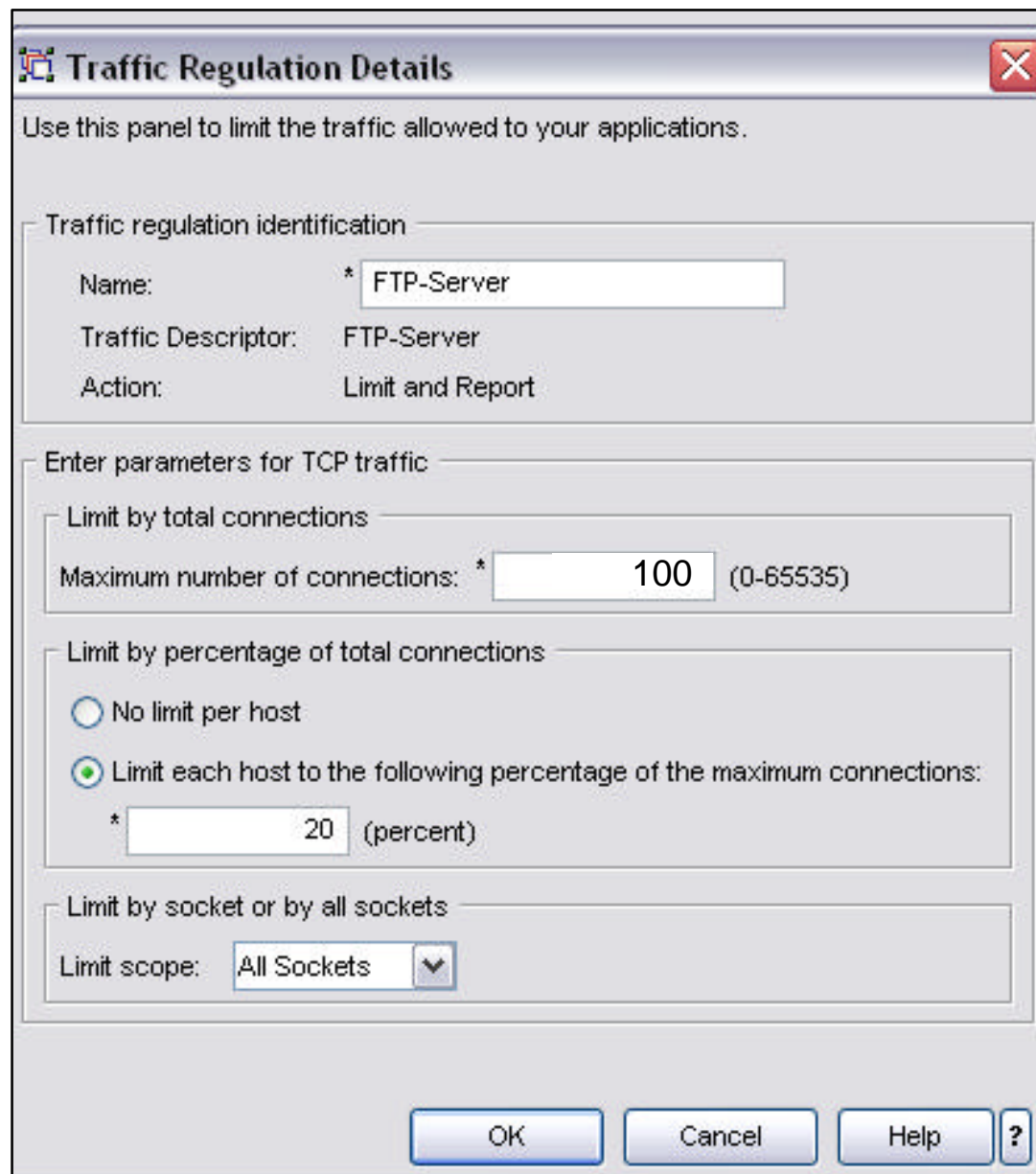
Buttons: Modify... | Copy... | Advanced... | Move Up | Move Down | View Details... | Work with Traffic Descriptors

Default Report Settings for Traffic Regulation...

OK | Cancel | Help | ?

next page

Set details for TR



Traffic Regulation Details [Close]

Use this panel to limit the traffic allowed to your applications.

Traffic regulation identification

Name: *

Traffic Descriptor: FTP-Server

Action: Limit and Report

Enter parameters for TCP traffic

Limit by total connections

Maximum number of connections: * (0-65535)

Limit by percentage of total connections

No limit per host

Limit each host to the following percentage of the maximum connections:

* (percent)

Limit by socket or by all sockets

Limit scope: [v]

OK Cancel Help ?

IDS_Policy_Demo

Requirements Map Now Created


Configuration Assistant - Requirement Maps

File Edit Help

Configuration Assistant Navigation T...

- IDS
 - Work with Reusable Objects
 - Traffic Descriptors
 - Requirement Maps
 - Work with z/OS Images

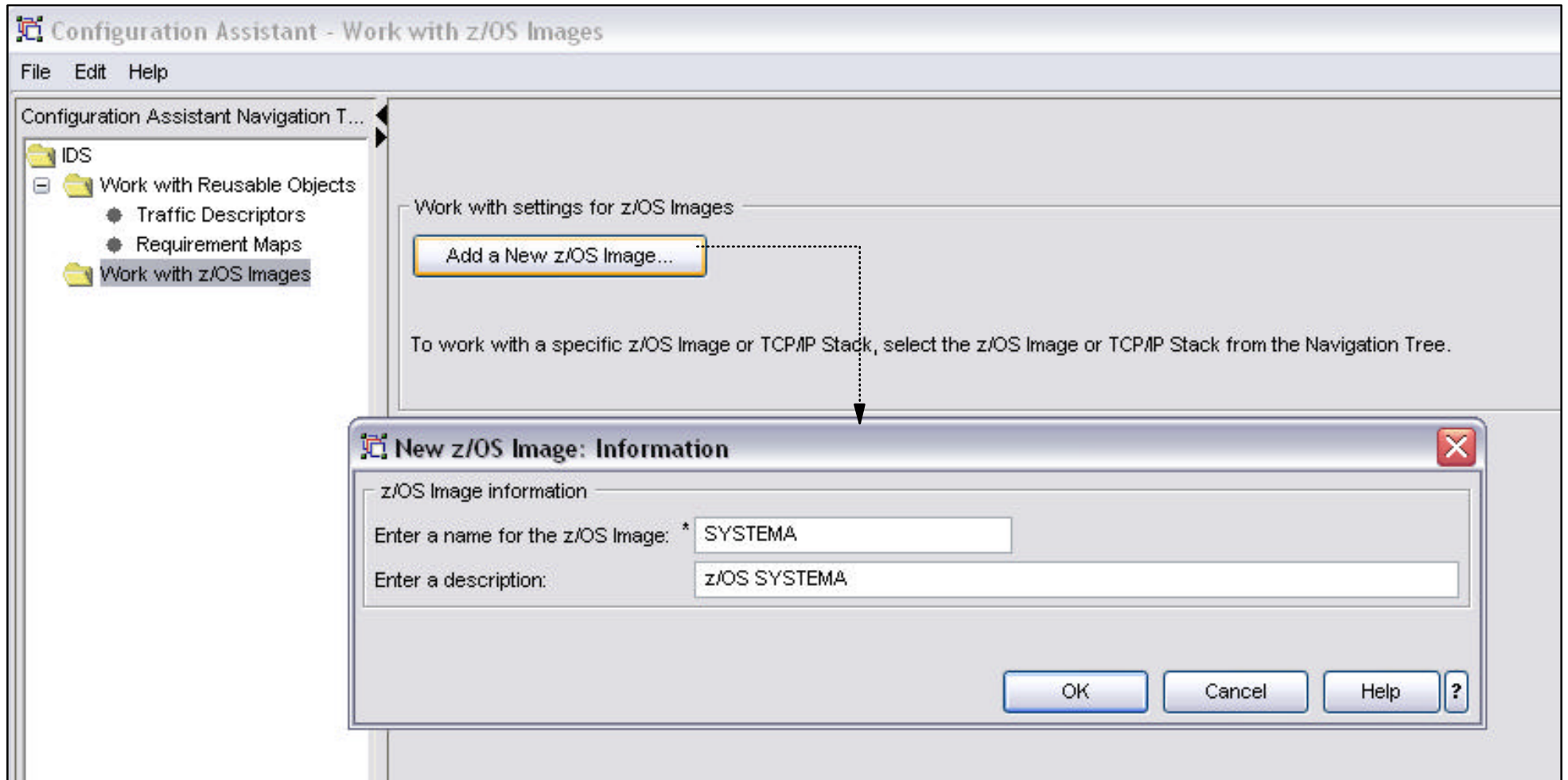
List of all defined Requirement Map objects



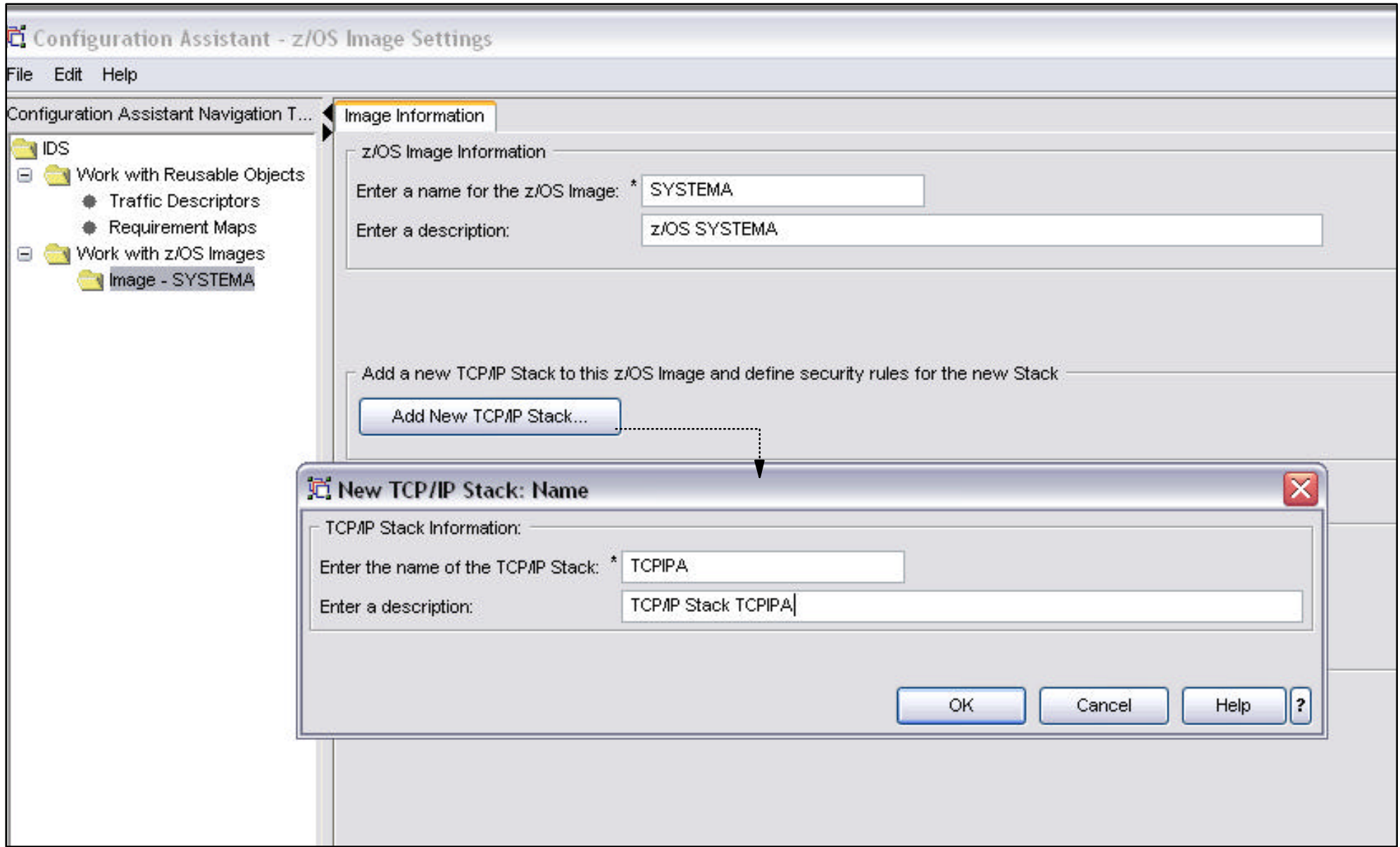
Name	Description
IDS_Policy_Demo	Show how to configure IDS policy
IDS_Default	IBM Supplied: Intrusion Detection Services Starter Set

Add... Copy... Modify... Delete View Details... Search...

Create System Image



Create TCP/IP Stack



Associate TCP/Stack with Requirements Map

The screenshot shows the 'Configuration Assistant - Requirement Maps' window. The left pane displays a tree view with 'Stack - TCPIPA' selected. The main area is titled 'TCP/IP Stack Information:' and contains the following fields:

- Enter the name of the TCP/IP Stack: * TCPIPA
- Enter a description: TCP/IP Stack TCPIPA
- Select a Requirement Map to govern IDS protection for this Stack.

A blue oval highlights the 'Select a Requirement Map...' instruction. Below it is a table with two columns: 'Name' and 'Description'.

Name	Description
IDS_Policy_Demo	Show how to configure IDS policy
IDS_Default	IBM Supplied: Intrusion Detection Services Starter Set

At the bottom of the window, there are several buttons: Add..., Copy..., Modify..., View Details..., Search..., Set Addresses..., and Health Check.

Install Configuration Files

Configuration Assistant - Requirement Maps

File Edit Help

Conf

- Add new z/OS Image...
- Copy the z/OS Image...
- Delete the z/OS Image
- Add new TCP/IP Stack...
- Copy the TCP/IP Stack...
- Delete the TCP/IP Stack
- Install Configuration Files...**
- Add Priority Level...
- Add Requirement Map...
- Add Security Level...
- Add Traffic Descriptor...
- Add Traffic Shaping Level...

TCP/IP Stack Information:

Enter the name of the TCP/IP Stack: * TCPIPA

Enter a description: TCP/IP Stack TCPIPA

Select a Requirement Map to govern IDS protection for this Stack.

Name	Description
IDS_Policy_Demo	Show how to configure IDS policy
IDS_Default	IBM Supplied: Intrusion Detection Services Starter Set

next page

Add... Copy... Modify... View Details... Search... Set Addresses... Health Check...

Show the configuration file to be installed

The image shows two windows from the IBM Configuration Assistant. The left window, titled "Installation - Stack= 'TCPIPA'", displays a tree view under "Install Configuration" with "Image - SYSTEMA" expanded to show "Stack - TCPIPA". The right window, titled "IDS: Policy Agent Stack Configuration", shows the configuration file content. A button labeled "Show Configuration File..." in the left window has a dotted arrow pointing to the configuration file content in the right window.

Installation - Stack= "TCPIPA"

Install Configuration

- Install Stack
 - Image - SYSTEMA
 - Stack - TCPIPA

Configuration Files Installation

To complete installation for Stack TCPIPA - Configuration Files

File

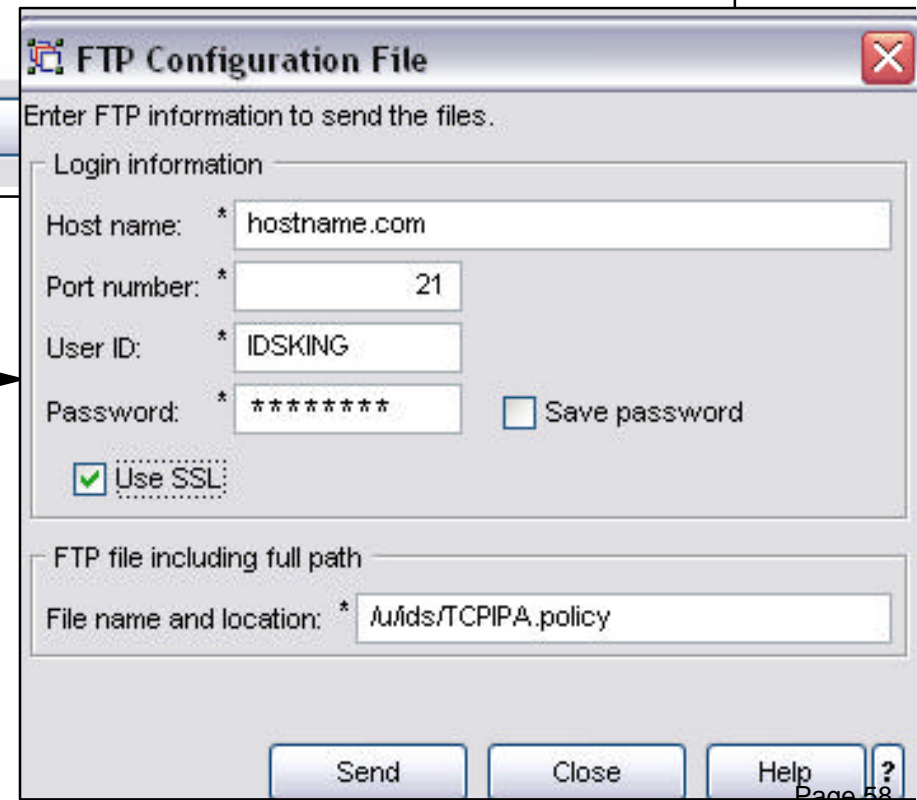
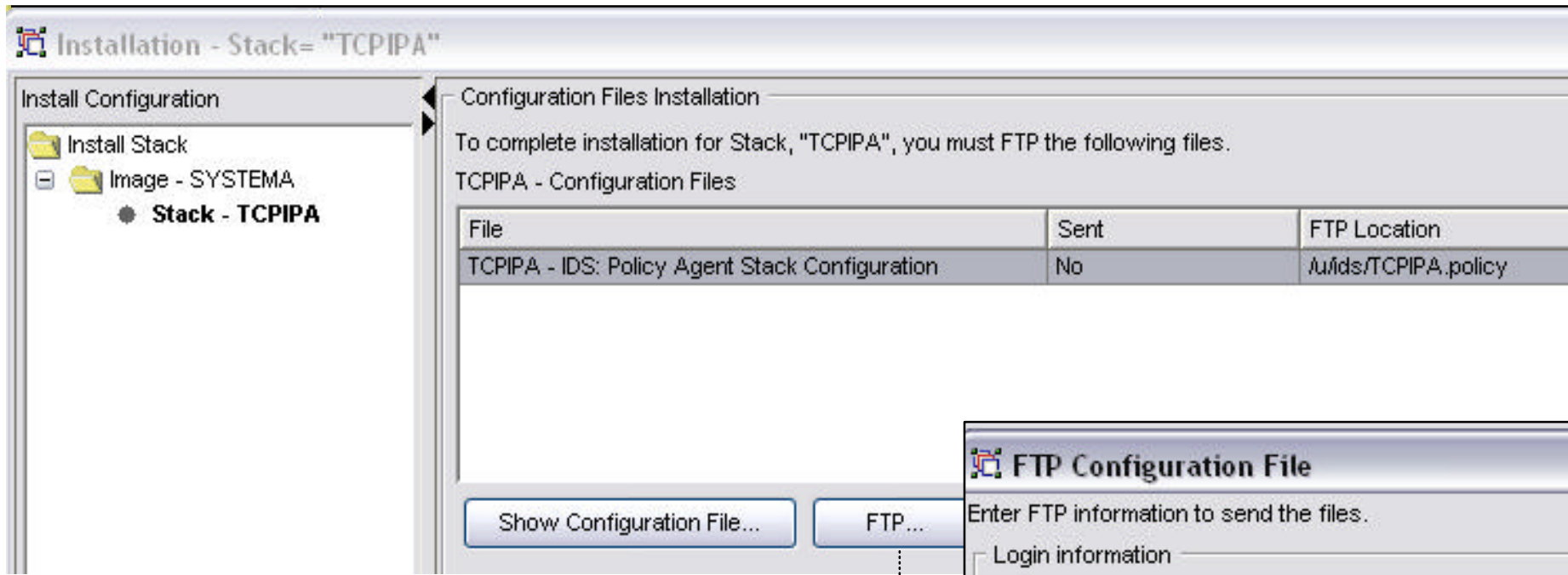
TCPIPA - IDS: Policy Agent Stack Configuration

Show Configuration File...

IDS: Policy Agent Stack Configuration

```
##
## IDS Policy Agent Configuration file for:
##   Image: SYSTEMA
##   Stack: TCPIPA
##
## Created by the IBM Configuration Assistant for z/OS
## Version 1 Release 8
## Date Created = Mon Jul 17 16:03:47 EDT 2006
##
#####
#####
# Attack Policies
#####
#-----
# Attack - IDSRule
#-----
IDSRule          Flood
(
  ConditionType  Attack
  IDSAttackCondition
  {
    AttackType    FLOOD
    IfcFloodMinDiscard 1000
    IfcFloodPercentage 10
  }
  IDSActionRef   Flood
)
IDSRule          Echo
(
  ConditionType  Attack
  IDSAttackCondition
```


Set up to transfer policy file to z/OS



z/OS Communications Server Security

Features Summary

IDS Features Summary

- **IDS events detected include:**
 - ▶ **Scan detection**
 - TCP port scans
 - UDP port scans
 - ICMP scans
 - ✓ Sensitivity levels for all scans can be adjusted to control number of false positives recorded.
 - ▶ **Attack detection**
 - Malformed packet events
 - Outbound raw restrictions
 - Inbound fragment restrictions
 - IP option restrictions
 - IP protocol restrictions
 - ICMP redirect restrictions
 - Flood events (Synflood, Interface flood)
 - UDP perpetual echo
 - ▶ **Traffic Regulation (Flood detection and prevention)**
 - UDP backlog management by port
 - ✓ Packets discard
 - TCP total connection and source percentage management by port
 - ✓ Connection limiting
- **IDS recording options**
 - ▶ **Event logging**
 - syslogd, local console
 - ▶ **Statistics**
 - syslogd
 - ✓ normal, exception
 - ▶ **IDS packet trace after attack detected for offline analysis**
 - Number of packets traced for multi-packet events are limited
- **Reports and event handling**
 - ▶ **trmdstat produces reports from IDS syslogd records**
 - Summary and detailed
 - ▶ **IDS event handling by**
 - Tivoli NetView
 - Tivoli Security Operations Manager

z/OS Communications Server Security

Appendix A

- **Scan Probe Instance Event Classifications**

ICMP Scan Probe Instance Classification

<i>Request Type</i>	<i>Destination Address</i>	<i>Event Classification</i>
any	subnet base or broadcast	very suspicious
Information req	single host	possibly suspicious
Subnet Mask req	single host	possibly suspicious
Echo with IP Option Record Route	single host	possibly suspicious
Echo with Record Timestamp	single host	possibly suspicious
Echo or Timestamp, denied by QOS policy	single host	normal
Echo or Timestamp	single host	normal

UDP Scan Probe Instance Classification

Socket State	Event	Event Classification
RESERVED to no one	recv any packet	very suspicious
Unbound, not RESERVED	recv any packet	possibly suspicious - app may be temporarily down
Bound	packet rejected by QOS policy	normal
Bound	packet rejected by FW filtering	possibly suspicious
Bound	recv any packet	normal

TCP Scan Probe Instance Classification

Socket State	Event	Event Classification
Any state	recv unexpected flags (SYN+FIN...)	very suspicious
RESERVED	recv any packet	very suspicious
Unbound, not RESERVED	recv any packet	possibly suspicious - app may be temporarily down
Listen	recv SYN	classification deferred if syn queued.
Half open connection	recv ACK	normal - connection handshake completed
Half open connection	recv RST	possibly suspicious - scanner covering tracks?
Half open connection	final time out (and not syn flood)	very suspicious - scanner abandoning handshake?
Any connected state	seq# out of window	normal - perhaps duplicate packet
Any connected state	recv standalone SYN	normal - perhaps peer reboot
Any connected state	final time-out	possibly suspicious - peer abandoned connection

z/OS Communications Server Security

Appendix B

- **IDS configuration with zIDS Manager**

(This method of configuration is used if IDS policy stored in LDAP)

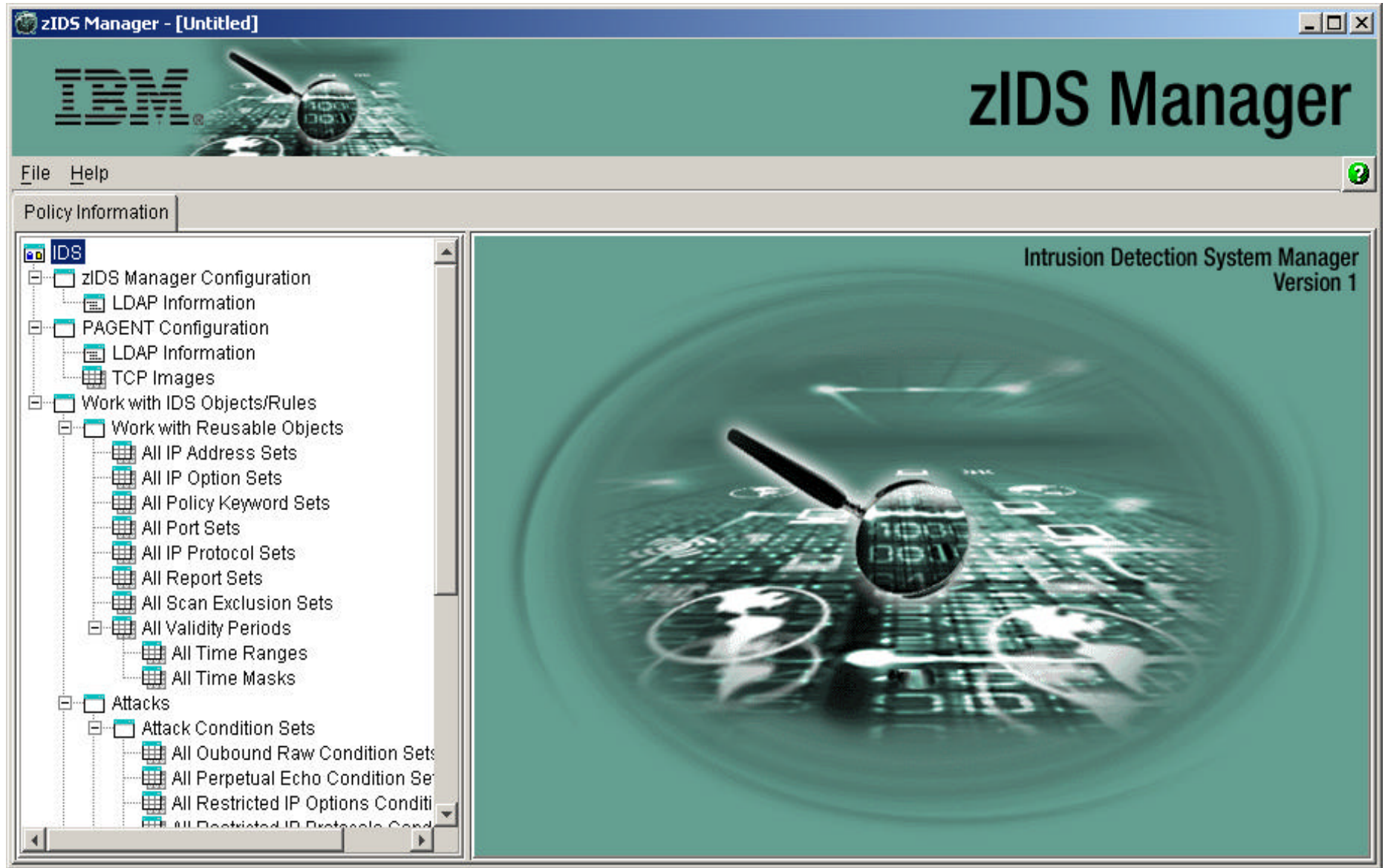
IDS Policy Configuration Steps with zIDS Manager

1. Download and install the zIDS Manager configuration tool
2. Configure the zIDS Manager for communications with LDAP server
3. Configure the Policy Agent configuration file
4. Configure IDS policies
 - a. Configure reusable objects
 - b. Create condition and action sets
 - c. Build policy rules from the condition and action sets
5. Upload policy agent configuration file and IDS policy

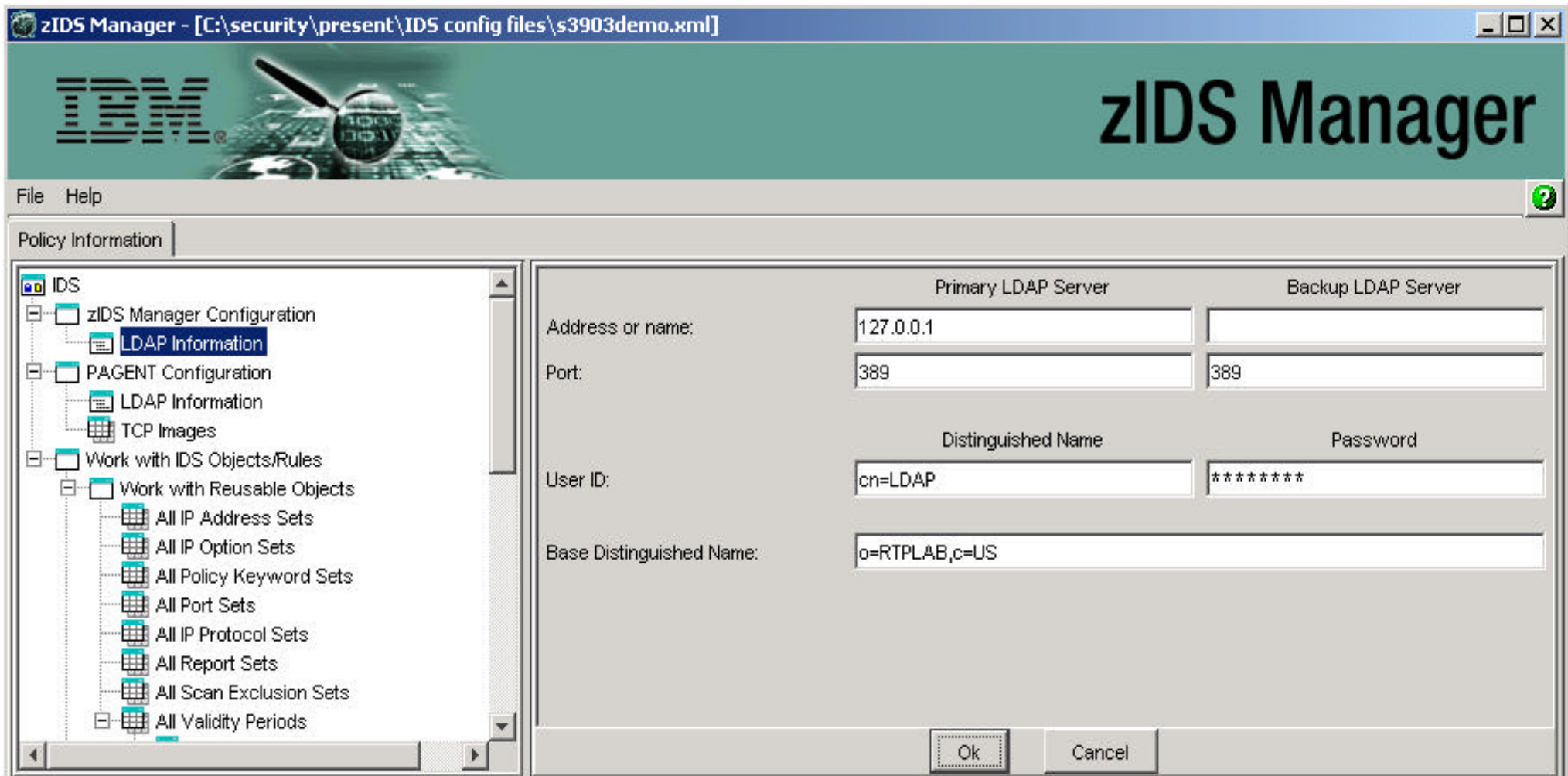
Download and Installation of zIDS Manager

1. Download and installation instructions are located at:
<http://www.ibm.com/software/network/commserver/zos/support/>
2. Instructions are written for Windows 2000 and Linux
3. Windows 2000 steps
 - a. Download this file to your Windows system: zIDSManager.zip
 - b. Use an unzip program to extract zIDSManager.zip
 - c. Execute zIDSManager.exe
 - d. Go to Start->Programs-zIDS Manager
4. Linux steps
 - a. Download this file to your Linux system: zidsmgr.tar
 - b. Untar the file with tar-xvf zidsmgr.tar
 - c. Execute ./zidsmgr
5. Sample XML File
 - a. Download this file to your system: zIDSSample.xml
 - b. Launch the zIDS Manager
 - c. Select File->Open from the zIDS Manager menubar and select the sample XML file

zIDS Manager



Configure zIDS Manager for Communications with LDAP

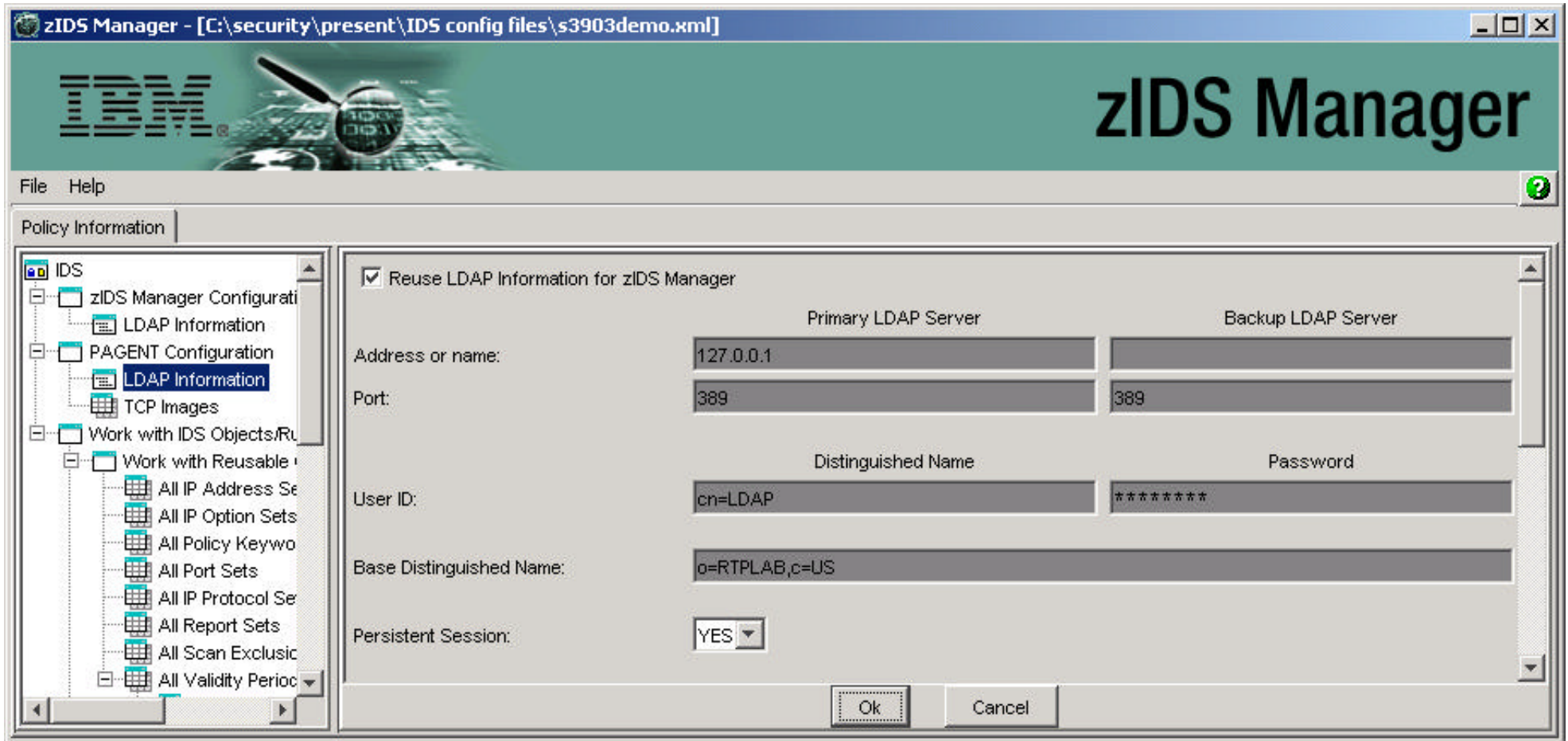


Defines LDAP server settings so that zIDS Manager can communicate with LDAP server

- Primary and backup LDAP Server IP address or domain name and port numbers
- Userid with write authority to the LDAP server
- Base distinguished name, which is the root of the LDAP subtree, where policy is to be stored

Configure Policy Agent Configuration File

Pagent LDAP Information (part 1)

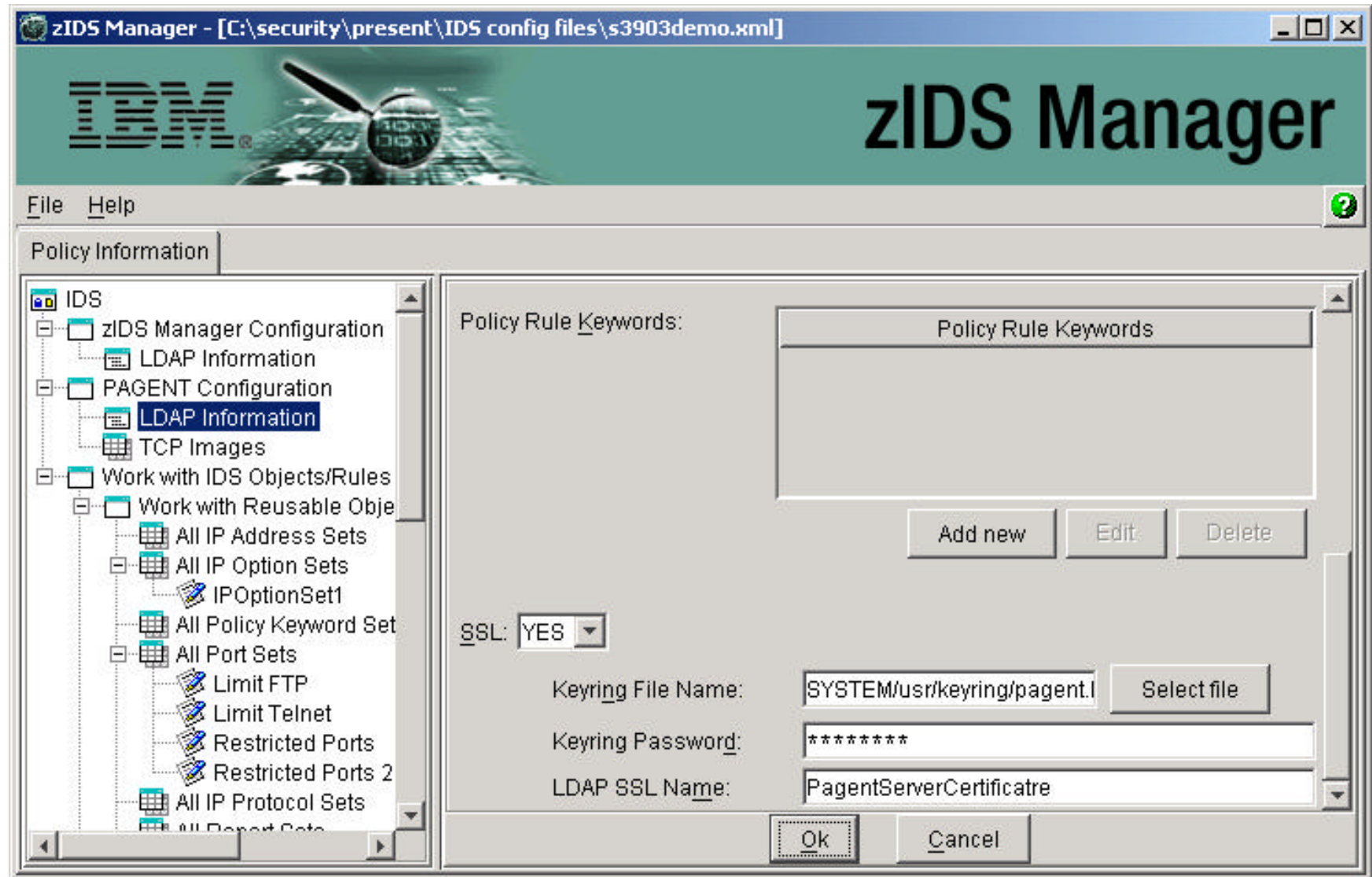


Defines LDAP server settings for the Pagent configuration file

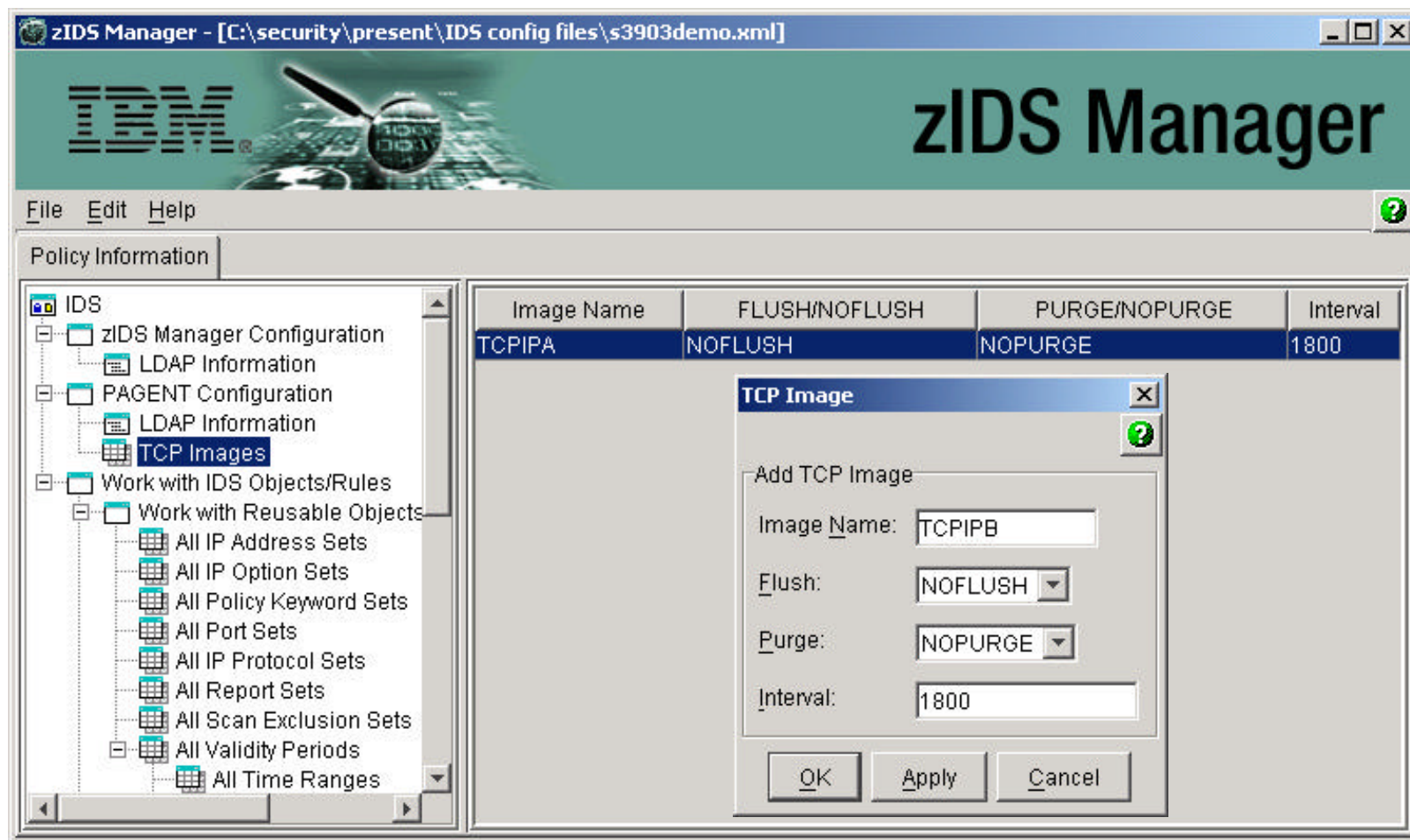
- Can reuse LDAP information entered in the zIDS Configuration panel for LDAP
- Can specify policy keywords to control which IDS policies are downloaded by the Policy Agent (next page)
 - ✓ Policy keywords can be specified at the policy rule level and are defined as a reusable object (policy keyword set)
- Can specify information to allow SSL protection between the Policy Agent and the LDAP server (next page)

Configure Policy Agent Configuration File

Pagent LDAP Information (part 2)



Configure Policy Agent Configuration File TCP Image Information



Defines information for each TCP stack using policy agent

- Stack name
- Defines policy control information for each stack
 - ✓ Flush / Purge values
 - ✓ Time interval for policy refresh

Configure Policy Agent Configuration File

Text Output

```
ReadFromDirectory
{
  LDAP_Server          127.0.0.1
  LDAP_Port            389
  LDAP_DistinguishedName  cn=LDAP
  LDAP_Password        sslkjl8
  LDAP_SessionPersistent Yes
  LDAP_ProtocolVersion  3
  LDAP_SchemaVersion   3
  SearchPolicyBaseDN   o=RTPLAB,c=US
  LDAP_SSL
  {
    LDAP_SSLKeyringFile  SYSTEM/usr/keyring/pagent.kdb
    LDAP_SSLKeyringPassword dfdfdfdf
    LDAP_SSLName         PagentServerCertificate
  }
}

TcplImage TCPIPA NOFLUSH NOPURGE 1800
TcplImage TCPIPB NOFLUSH NOPURGE 1800
```

"Save as" file type .conf

- File is Pagent Configuration file

File must be manually transferred (e.g. ftp, cut & paste, or retype) to configuration file on z/OS system

- File typically located at /etc/pagent.conf

Example IDS Policy Rule Configuration using zIDS Manager

1. Policy Types

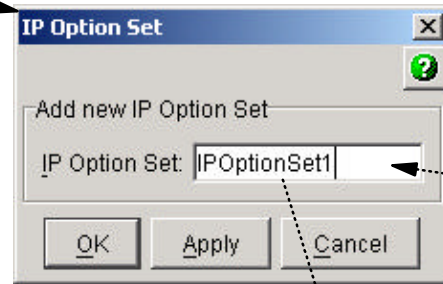
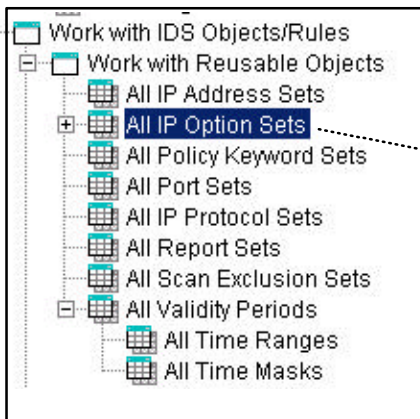
- a. Scan Global policy
- b. Scan Event policies
 - ✓ For selected TCP and UDP ports that are "Reserved" on PORT statement in TCP Profile
- c. Attack Policies
 - ✓ Flood
 - ✓ Malformed Packet
 - ✓ Restricted IP Options
 - ✓ IP Fragment
- d. Traffic Regulation policies
 - ✓ TCP ports for Telnet and FTP

2. Reusable Objects defined

- a. IP options sets
 - ✓ Referenced by Restricted IP Options
- b. Port sets
 - ✓ Referenced by Scan Event and TCP Traffic Regulation
- c. Report sets
 - ✓ Referenced by Action objects

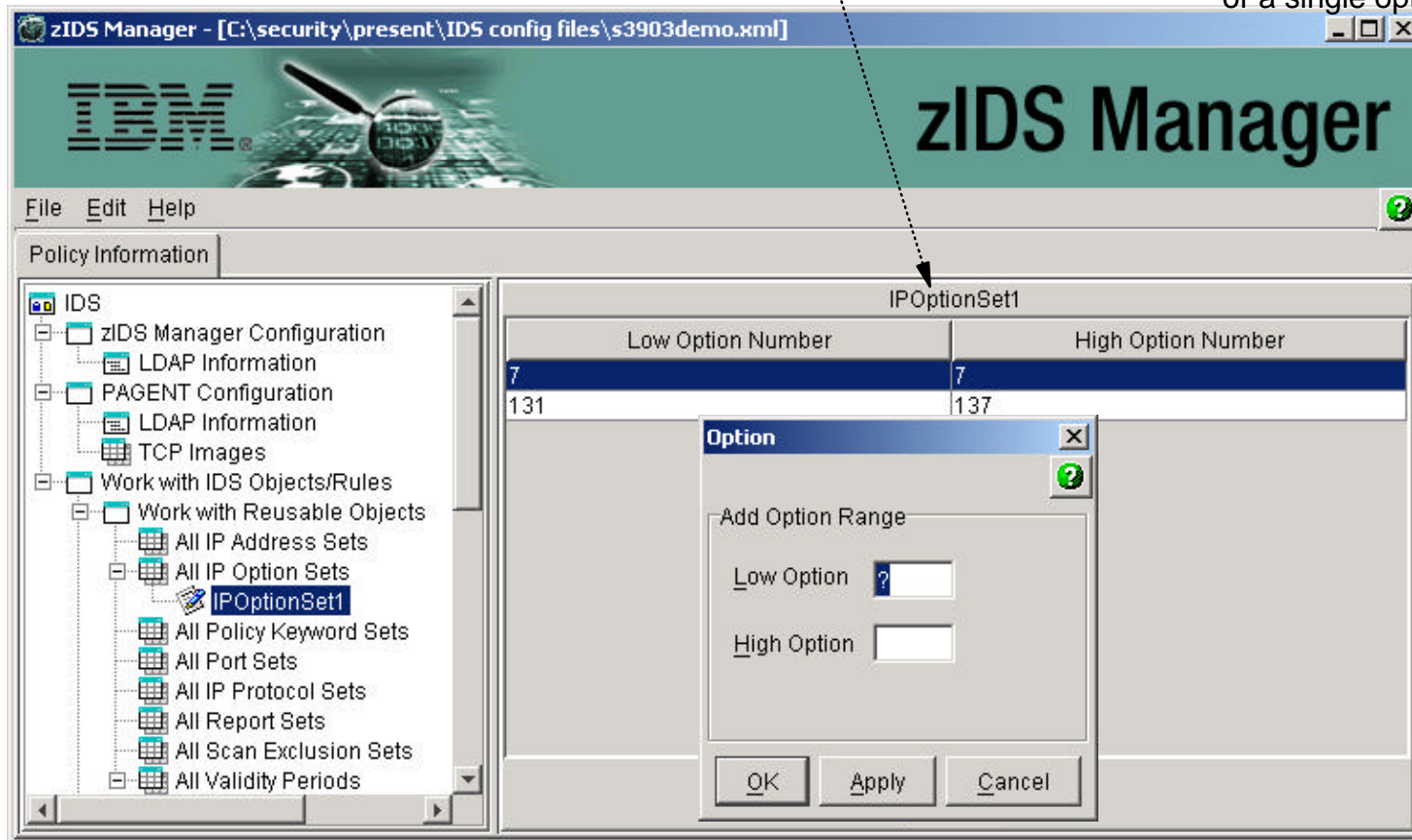
Configuring Reusable Objects

IP Option Set

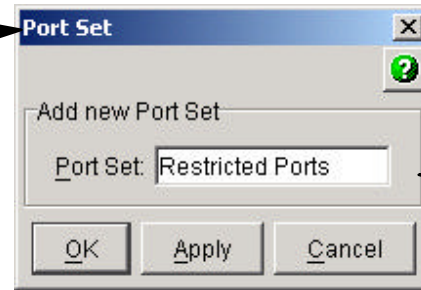
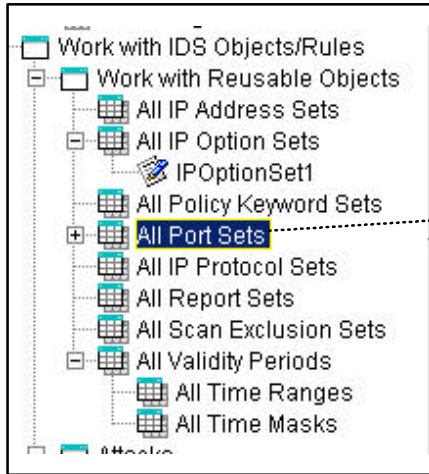


Define a set of IP Options which will be restricted through the Restricted IP Options Attack condition

- Option set name to be referenced
- Options in the option set
- Options can be specified as a range or a single option value

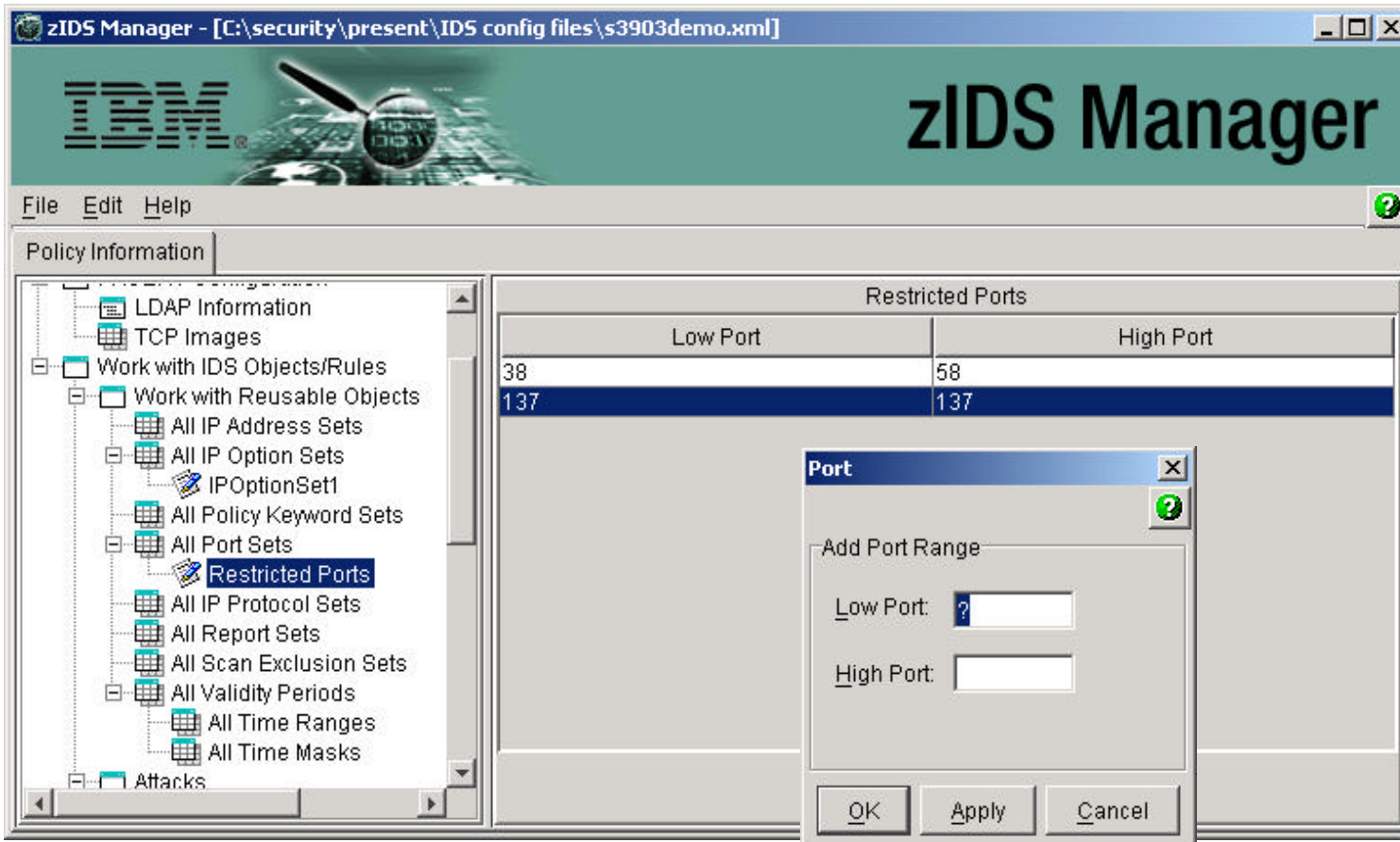


Configure Reusable Objects Port Sets



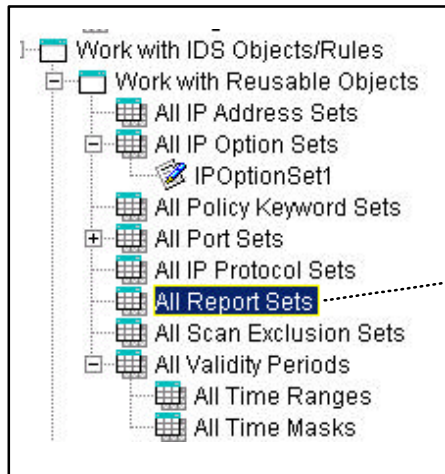
Define a set of ports which will be included in various IDS conditions

- Ports to monitor for Scan Events
- Ports to monitor for Traffic Regulation
- Port set name to be referenced
- Ports in the port set
- Ports can be specified as a range or a single port value



Configure Reusable Objects

Report Set



Define a set of report options which can be included in various IDS actions

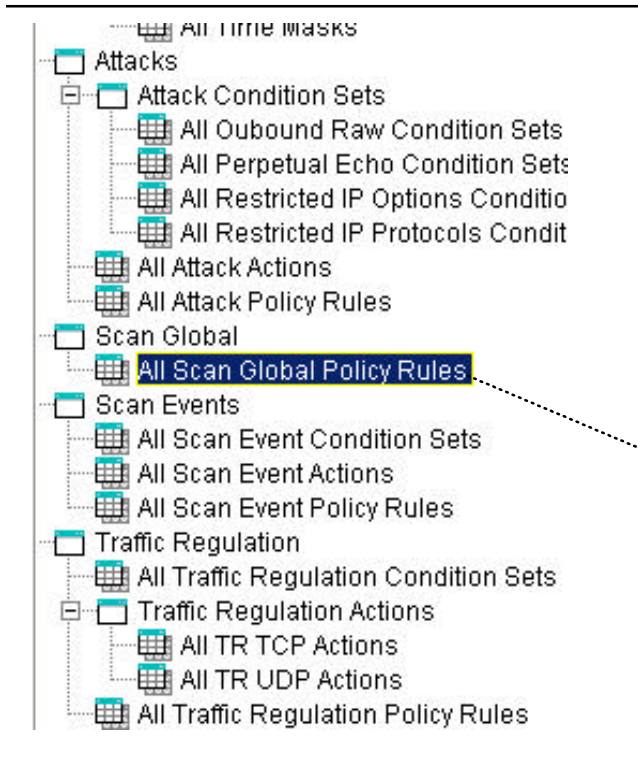
- Set up a report set with notification only - no defensive actions
- Set up a report set with notification and defensive actions

Action Type Options

- Limit (packet discard or connection limit - depending on action)
- Write IDS events to syslog
- Write IDS events to console
- Exception statistics records
- Trace packet data

Report Set Name	Type Action	Notification	Statistic Interval	Logging Level	Trace Data	Trace Record Size
Defend1	Exception Statistics Limit Log	SYSLOG Detail	60	1	Record Size	100
Notify1	Exception Statistics Log	SYSLOG Detail	60	1	Record Size	100

Set Scan Global Policy



Define the Scan Global Policy for the system which determines when a scan condition is reached

Scan Global Policy Rule

Add New Scan Global Policy Rule

Policy Rule Name: GlobalScan1

Fast Scan Interval: 1

Fast Scan Threshold: 5

Slow Scan Interval: 120

Slow Scan Threshold: 10

Report Set Name: Notify1

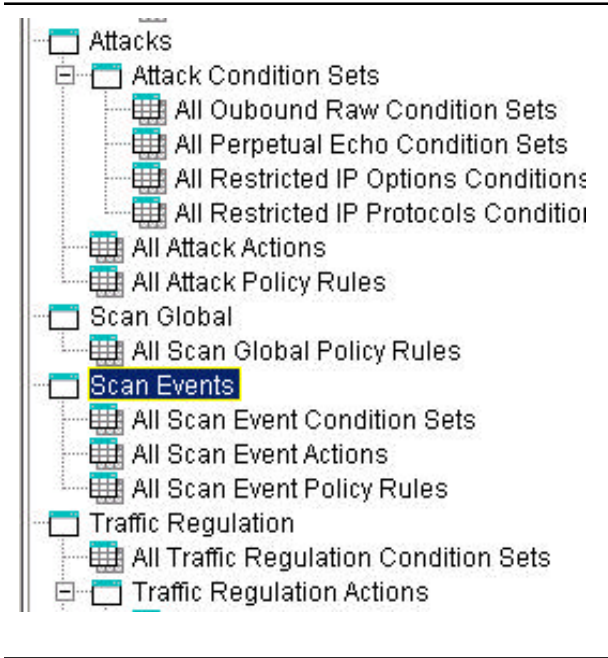
Validity Period Name: []

Policy Keyword Set Name: []

Buttons: OK, Apply, Cancel

- Fast Scan Interval - time period to evaluate for a fast scan
- Fast Scan Threshold - number of scan events required for fast scan event
- Slow Scan Interval - time period to evaluate for a slow scan
- Slow Scan Threshold - number of scan events required for slow scan event
- Reference to report set name (Notify1 - notify only - no defensive action)

Set Scan Event Policy



1

Scan Event Condition Set

Add Scan Event Condition Set

Set Name: ScanSetUDP

Protocol: UDP

Local Port Set: Restricted Ports 2

Local IP Address Set:

OK Apply Cancel

Scan Event Condition Set

Add Scan Event Condition Set

Set Name: ScanSetTCP

Protocol: TCP

Local Port Set: Restricted Ports

Local IP Address Set:

OK Apply Cancel

2

Scan Event Action

Add new Scan Event Action

Action Name: ScanAction1

Sensitivity: Low

Scan Exclusion Set:

OK Apply Cancel

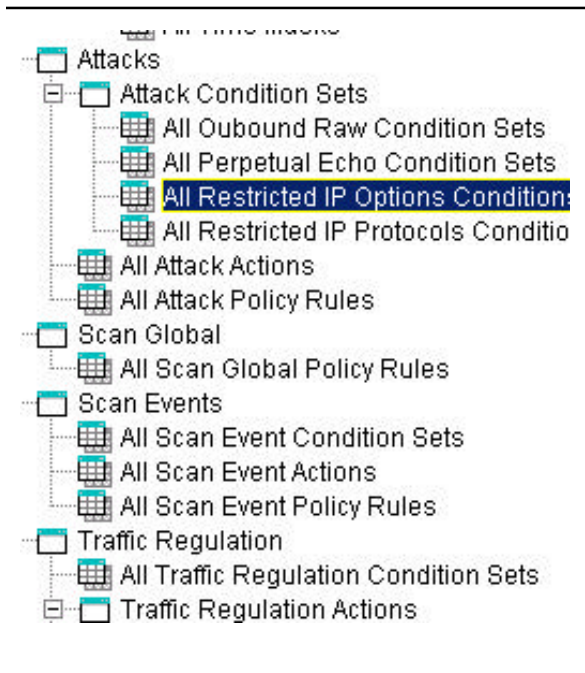
Define policies on a port basis (referencing local port set) which will determine when a scan event should count towards the Global Scan Policy

1. Define scan event conditions
2. Define scan event action which will be reused by multiple policy rules
3. Define policy rule and tie to condition sets and action

3

Policy Rule Name	Condition Set Name	Action Name	Validity Period Name	Policy Keyword Set name
ScanUDP	ScanSetUDP	ScanAction1		
ScanTCP	ScanSetTCP	ScanAction1		

Set Attack Policy



1

Restricted IP Options Condition Set

Modify Restricted IP Options Condition Set

Set Name:

Restricted option Set:

2

Attack Action

Modify Attack Action

Action Name:

Report Set:

Max Events Message:

Attack Action

Add new Attack Action

Action Name:

Report Set:

Max Events Message:

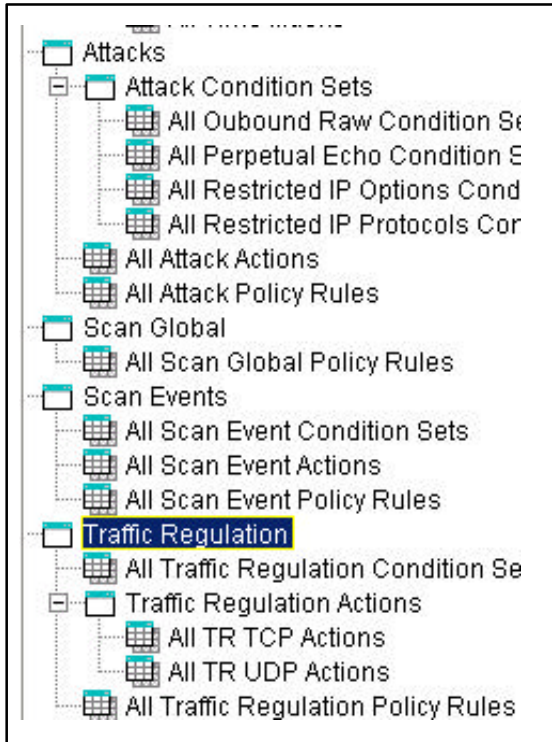
Define separate policy for each attack type

1. Define condition set for Restricted IP Options referencing an Option Set
2. Define reusable attack actions referencing a Report Set
3. Define policy rule and tie to condition sets and action

3

Policy Rule Name	Attack Type	Condition Set Name	Action Name	Validity Period Name	Policy Keyword Set Name
Flood	Flood		Attack Action 1		
Bad Option	Restricted IP Options	Restrict IP Options 1	Attack Action 2		
Malformed	Malformed Packet		Attack Action 1		
Fragment	IP Fragment		Attack Action 1		

Set Traffic Regulation Policy



1

2

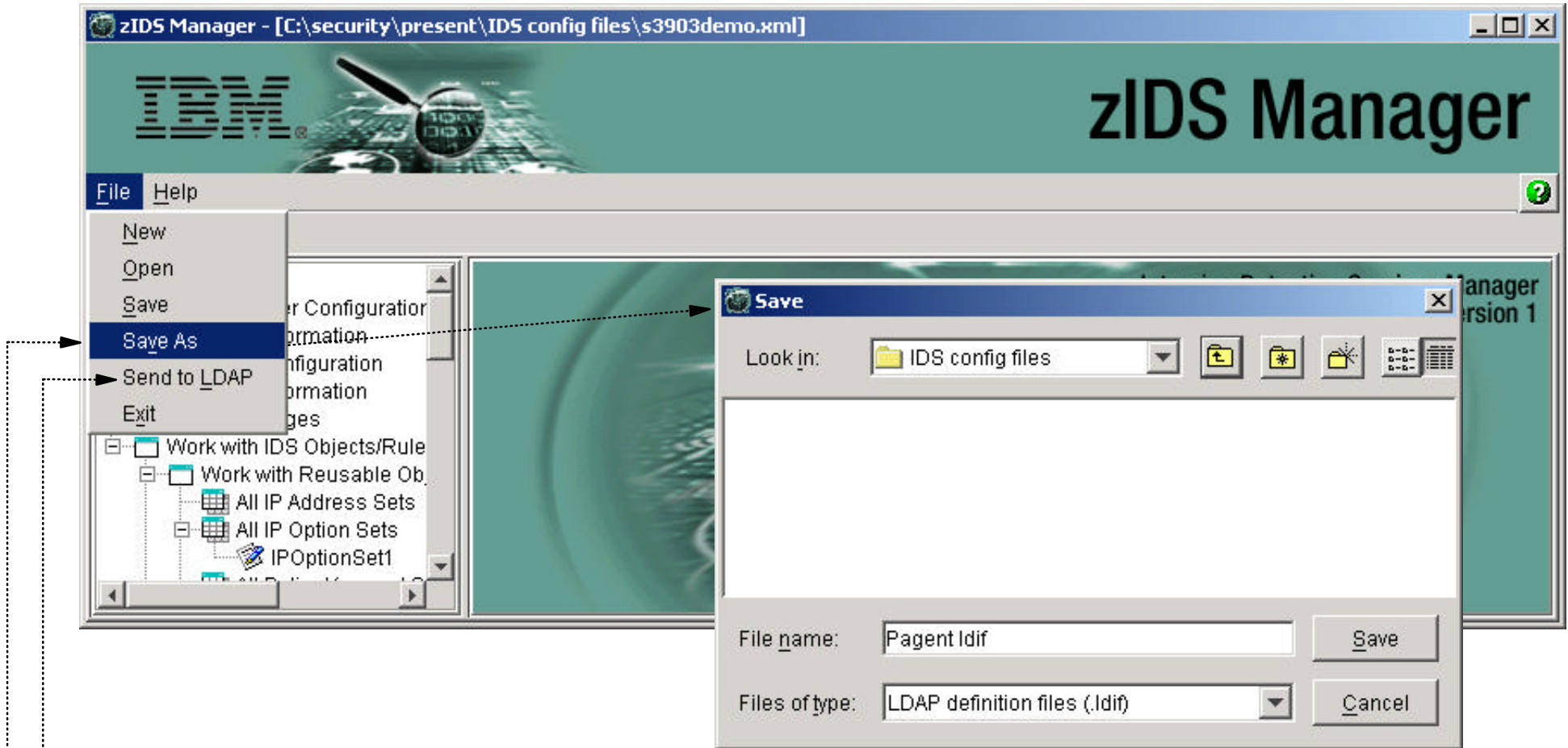
Define policies for TCP Traffic Regulation

1. Define condition set for each Port Set to be monitored for Traffic Regulation
2. Define reusable Traffic Regulation Action
3. Define policy rules for each Port Set to be monitored for Traffic Regulation

3

Policy Rule Name	Condition Set Name	Action Name	Validity Period Name	Policy Keyword Set Name
TCP FTP	TCP FTP	TR Action1		
TCP Telnet	TCP Telnet	TR Action1		

Transfer IDS Policy to LDAP Server



After IDS policy configuration is complete at zIDS Manager

1. Save policy as .ldif type file
 - ✓ .ldif file will be created from XML file that zIDS Manager uses
2. Send policy (ldif) file to LDAP Server
 - ✓ LDAP Server defined in first step - z/IDS Manager Configuration - LDAP information

For More Information....

URL	Content
http://www.ibm.com/servers/eserver/zseries	IBM eServer zSeries Mainframe Servers
http://www.ibm.com/servers/eserver/zseries/networking	Networking: IBM zSeries Servers
http://www.ibm.com/servers/eserver/zseries/networking/technology.html	IBM Enterprise Servers: Networking Technologies
http://www.ibm.com/software/network/commserver	Communications Server product overview
http://www.ibm.com/software/network/commserver/zos/	z/OS Communications Server
http://www.ibm.com/software/network/commserver/z_lin/	Communications Server for Linux on zSeries
http://www.ibm.com/software/network/ccl	Communication Controller for Linux on zSeries
http://www.ibm.com/software/network/commserver/library	Communications Server products - white papers, product documentation, etc.
http://www.redbooks.ibm.com	ITSO redbooks
http://www.ibm.com/software/network/commserver/support	Communications Server technical Support
http://www.ibm.com/support/techdocs/	Technical support documentation (techdocs, flashes, presentations, white papers, etc.)
http://www.rfc-editor.org/rfcsearch.html	Request For Comments (RFC)