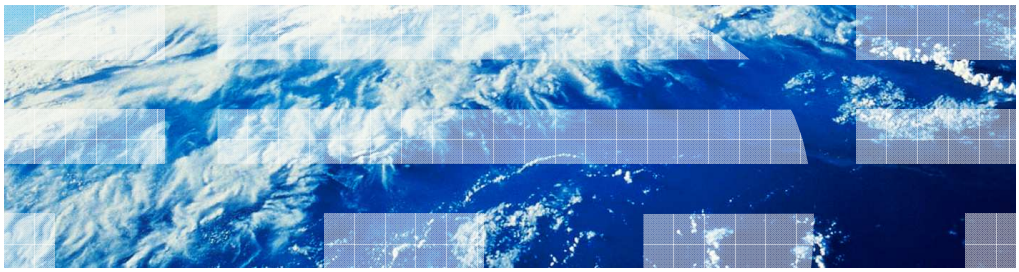
z/OS Communications Server

Intrusion detection services function externals

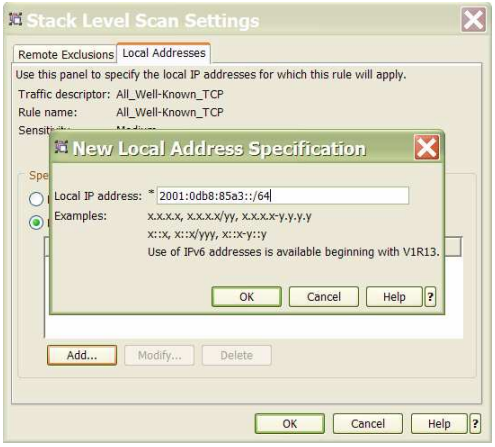


This presentation describes the external changes (configuration changes and command output) for the expansion of intrusion detection services in z/OS® V1R13 Communications Server. Background information, a description of the changes, migration information, diagnosis, and other information are described in a separate presentation.

IP addresses

- IP addresses used in a limited way in IDS policies

Optional for scan and TR
to identify a listening socket

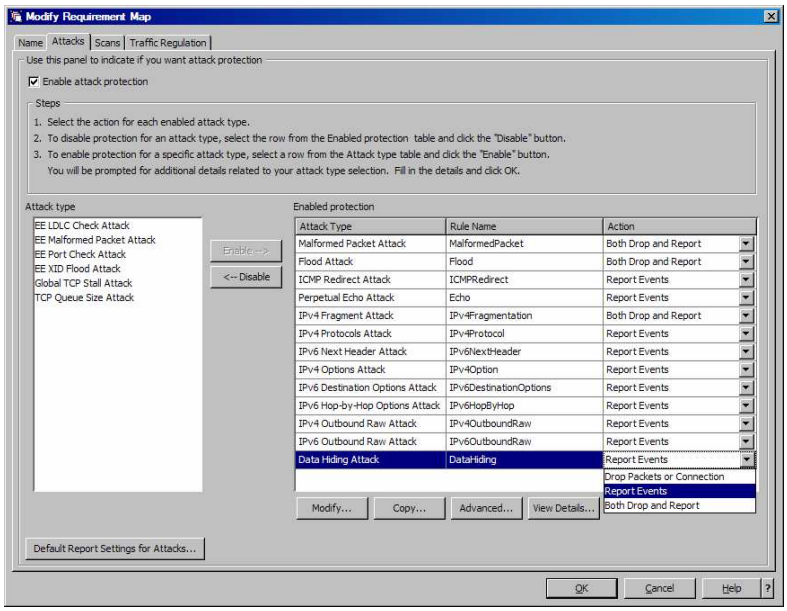


Optional for scan exclusion

2 Intrusion detection services function externals

The Configuration Assistant is updated to support the new IDS function. IP addresses are used in a limited way in IDS policies. In fact, you might even have IDS policies in place that don't specify any IP addresses. There are two places where IP addresses might be used in IDS policies. The first place is in specifying a local address for which the policy applies. For scan and traffic regulation policies, you can specify a listening socket by its IP address and port number, although it is typically identified by port number alone. The second place that IP addresses are used in IDS configuration is in specifying a remote address in the optional scan exclusion list.

Attacks



This slide shows the panel used to enable and disable attack types. Enabled attack types are shown in the list on the right of the panel. In this example, the enabled list includes the new IPv6-specific attack types, the new Data-Hiding attack type, and the existing attack types. Additionally, on the left you can see the new TCP-Queue-Size Attack and the Global TCP Stall attack. For each enabled attack type, the rule name and action is displayed. The action can be Report Events, Drop Packets or Connection, or Both Drop and Report.

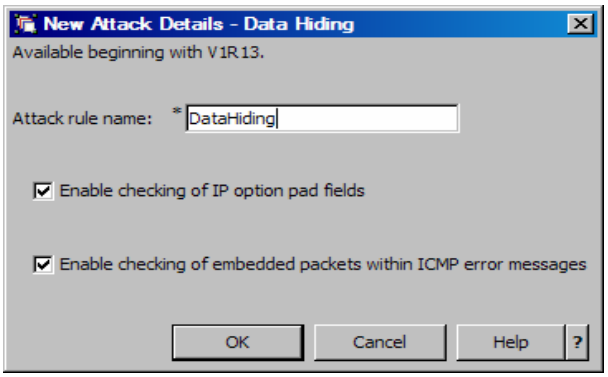
The next slides show specific information that can be configured for each of the new attack types.

New IPv6 attacks

- IPv6 next-header attack
  - Allow or forbid upper-layer transport protocols
- IPv6 destination-options attack
  - Allow or forbid option types
- IPv6 hop-by-hop-options attack
  - Allow or forbid option types
- IPv6 outbound-raw attack
  - Allow or forbid upper-layer transport protocols

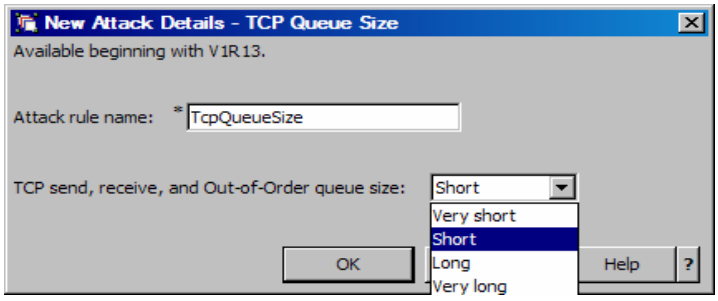
This slide shows the new IPv6 attack types that can be configured for IDS. Each attack lists the type of protocol or option values that you will configure to be allowed or forbidden.

Data hiding



When you enable the Data-Hiding attack type, this panel is displayed. By default all data-hiding checks are enabled. You can choose to disable one or more of the checks if false positives are being reported as a result of the checking. When this attack type is enabled and an inbound IPv4 or IPv6 packet has potential hidden data, the configured action is taken.

TCP-queue-size attack

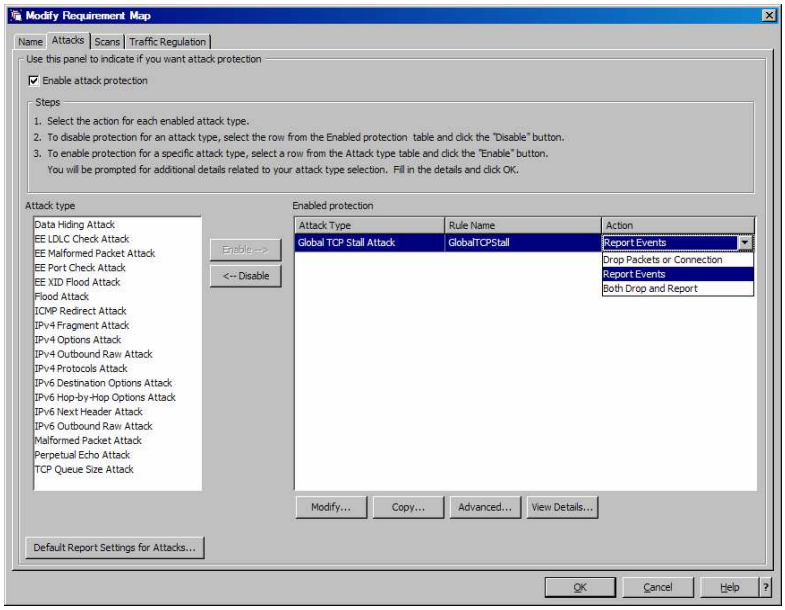


When you enable the TCP-queue-size attack type, this panel is displayed. A queue-size configuration value is provided. The default is Short. This attack can be configured with an action of Report Events, Drop Packets or Connection, or Both Drop and Report.

When this attack type is enabled and a TCP queue's size reaches the configured limit and the oldest data on the queue is at least 30 seconds old, the configured action is taken. Additionally, when this attack type is enabled and a TCP queue has *any* data that is at least 60 seconds old, the configured action is taken.

As with many attack types, you can configure an exclusion list for the TCP-Queue-Size attack. The exclusion list is used to exclude connections with a given remote IP address or port from *send* queue checking. Connections cannot be excluded from receive and out-of-order queue checks.

Global-TCP-stall attack



This slide shows the new global-TCP-stall attack type enabled. The rule name and action are displayed. The action can be Report Events, Drop Packets or Connection, or Both Drop and Report. No additional attack condition information is configured for this attack type.

Netstat IDS/–k report, scan detection

- ICMPv6 scan rule name added
- Displayed only for LONG format

```
NETSTAT IDS
MVS TCP/IP NETSTAT CS V1R13       TCPIP Name: TCPCS           11:51:44
Intrusion Detection Services Summary:
Scan Detection:
  GlobRuleName:   ScanGlobal-rule
  IcmpRuleName:   ScanEventIcmp-rule
  Icmpv6RuleName: ScanEventIcmpv6-rule
  TotDetected:  0           DetCurrPlc: 0
  DetCurrInt:   0           Interval:   60
  SrcIPsTrkd:   0           StrgLev:    00000
```


The Netstat IDS/-k report provides information about IDS policy and activity. The Scan Detection section of the report displays the name of the active scan global rule and the active ICMP scan rule. The name of the active ICMPv6 scan rule has been added to this section. Note that if IPv6 is not enabled on your system, you can display a SHORT format of the IDS/-k report. The ICMPv6 scan rule name is not included in the SHORT format report.

Netstat IDS/–k report, attack detection

```
Attack Detection:
. . .
   Data Hiding
     PlcRuleName: AttackDataHiding-rule
     TotDetected: 8           DetCurrPlc: 0
     DetCurrInt:  0           Interval:   0
   TCP Queue Size
     PlcRuleName: AttackTCPQueSz-rule
     TotDetected: 27          DetCurrPlc: 4
     DetCurrInt:  0           Interval:   0
   Global TCP Stall
     PlcRuleName: AttackTCPStall-rule
     TotDetected: 1           DetCurrPlc: 0
     DetCurrInt:  0           Interval:   0
. . .
   OutBound IPv6 RAW Restrictions
     PlcRuleName: AttackOutboundv6Raw-rule
     TotDetected: 0           DetCurrPlc: 0
     DetCurrInt:  0           Interval:   0
   Restricted IPv6 Next Headers
     PlcRuleName: AttackNextHdr-rule
     TotDetected: 30          DetCurrPlc: 4
     DetCurrInt:  0           Interval:   0
   Restricted IPv6 Destination Options
     PlcRuleName: AttackDestOpts-rule
     TotDetected: 15          DetCurrPlc: 2
     DetCurrInt:  0           Interval:   0
   Restricted IPv6 Hop-by-Hop Options
     PlcRuleName: AttackHopOpts-rule
     TotDetected: 3           DetCurrPlc: 1
     DetCurrInt:  0           Interval:   0
```


The Attack Detection section of the report has a subsection for each attack type. For each attack type, the name of the active rule is displayed. Several counts are also displayed that reflect detected attack activity. For each of the new attack types, a corresponding subsection has been added. Note that the IPv6-only attack types are not included in the SHORT format report. They are only displayed for the LONG format report.

Netstat IDS/–k report, miscellaneous

- Global conditions reports connection flooding and stalled connections
- IPv6 addresses might now appear for TCP and UDP sockets

```
Active Global Conditions:
  ServersInConnFlood: 5
  TCPStalledConns: 345         TCPStalledConnsPct: 14

Intrusion Detection Services TCP Port List:
. . .
TcpListeningSocket: 2001:db8::9:67:115:66..21
  ScStat: C  ScRuleName: ids-rule7
  TrStat: C  TrRuleName: ids-rule1
  TrPortInst: Y  TrCorr: 0           MxApp: 1           MxHst: 2
  SynFlood:   N  ConnFlood: N

Intrusion Detection Services UDP Port List:
. . .
UdpDestSocket: 2001:db8::9:67:115:78..911
  ScStat: C  ScRuleName: ids-rule7
  TrStat: C  TrRuleName: *NONE*
  TrCorr: 0           Discarded: 0
```


The Active Global Conditions now reports some additional counts. ServersInConnFlood indicates the number of TCP server sockets whose backlogs have been expanded to handle incoming connection requests. TCPStalledConns and TCPStalledConnsPct indicate the number and percentage of TCP connections whose send data flow is stalled. Refer to the earlier discussion of the global-TCP-stall attack for a discussion of when a connection is considered stalled. These fields are reported even when the global-TCP-stall attack is not configured.

The Intrusion Detection Services TCP Port List section has an entry for each TCP listening socket that is being monitored for scan event detection or traffic regulation. The name of the scan event and traffic regulation rules are displayed. Various statistics are also displayed. IDS policy can now apply to TCP sockets bound to IPv4 and IPv6 addresses so you might see both IPv4 and IPv6 addresses in this display. Additionally, the ConnFlood indicator shows whether a server's connection backlog has been expanded due to a potential SYN-flood attack.

Similarly, the Intrusion Detection Services UDP Port List section has an entry for each UDP socket that is being monitored for scan event detection or traffic regulation. The name of the scan event and traffic regulation rules and various statistics are displayed. IDS policy can now apply to UDP sockets bound to IPv4 and IPv6 addresses so you might see both IPv4 and IPv6 addresses in this display.

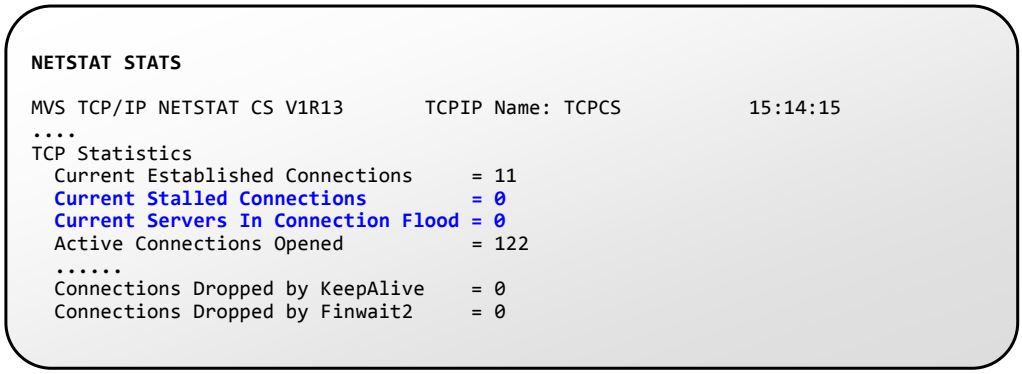
Netstat ALL/–A report

```
Client Name: FTPD1                    Client Id: 0000006D
  Local Socket: ::1..21
  Foreign Socket: ::1..1026
    .....
    Last Touched:       22:05:51        State:              Establsh
    .....
    ReceiveDataQueued:  0000000000
    SendDataQueued:     0000000000
    SendStalled:        No
    Ancillary Input Queue: Yes
      BulkDataIntfName: OSAQDIO4

Client Name: FTPD1                    Client Id: 000000F6
  Local Socket: 0.0.0.0..21             Foreign Socket: 0.0.0.0..0
  Foreign Socket: ::..0
    .....
    Last Touched:       21:41:09          State:              Listen
    .....
    ConnectionsIn:      0000000001        ConnectionsDropped: 0000000000
    MaximumBacklog:     0000000010        ConnectionFlood:    No
    CurrentBacklog:     0000000000
      ServerBacklog:    0000000000        FRCABacklog:        0000000000
```


The Netstat ALL/–A report displays information about all sockets. A new field, SendStalled, has been added to the Netstat ALL/–A report. This field indicates whether this connection's send data flow is stalled (Yes) or not (No). Refer to the earlier discussion of the global-TCP-stall attack for a discussion of when a connection is considered stalled. This field is reported whether the global TCP stall attack type is configured or not.

The ConnectionFlood field has also been added. This field indicates whether this server's connection backlog has been expanded due to a potential SYN-flood attack. This field is only displayed for a connection that is in listen state.

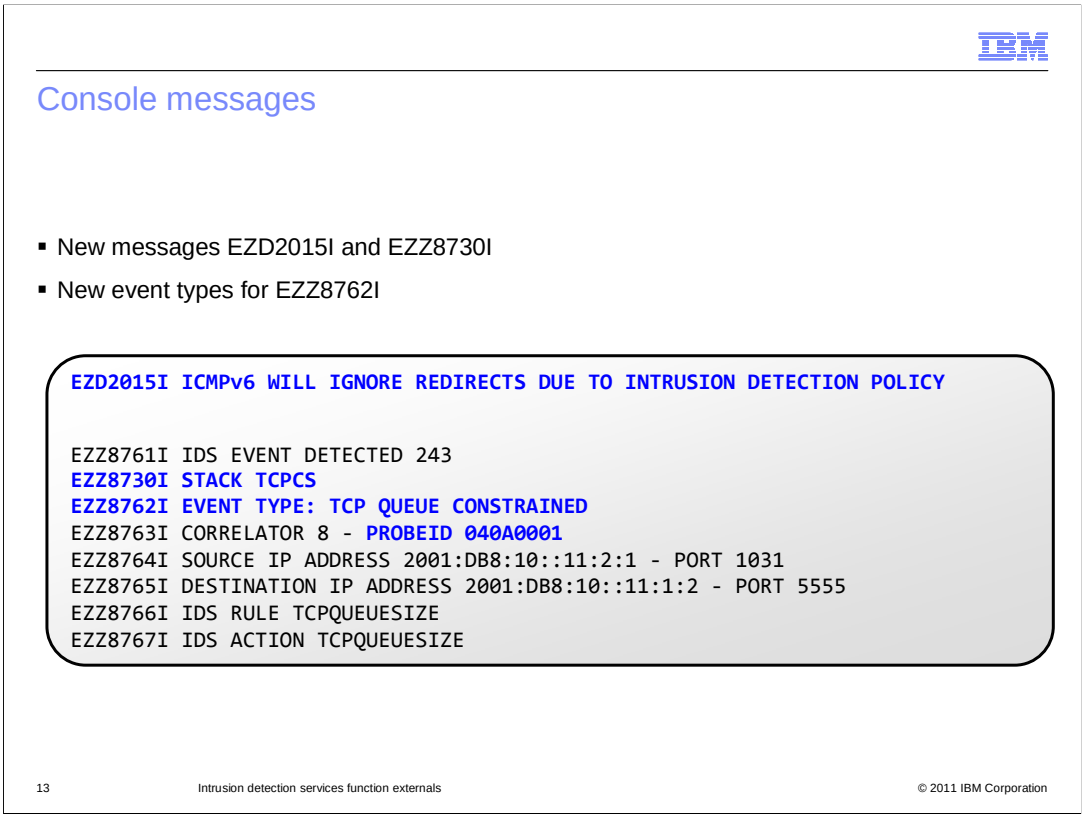
Netstat STATS/–S report



```
NETSTAT STATS

MVS TCP/IP NETSTAT CS V1R13       TCPIP Name: TCPCS           15:14:15
....
TCP Statistics
  Current Established Connections     = 11
  Current Stalled Connections         = 0
  Current Servers In Connection Flood = 0
  Active Connections Opened           = 122
  ......
  Connections Dropped by KeepAlive    = 0
  Connections Dropped by Finwait2     = 0
```


The Netstat STATS/–S report displays TCP/IP statistics. Current Stalled Connections is the number of TCP connections whose send data flow is stalled. Refer to the earlier discussion of the global-TCP-stall attack for a discussion of when a connection is considered stalled. This field is maintained and displayed whether the global TCP stall attack type is configured or not.

Current Servers In Connection Flood is the number of TCP servers under a potential connection-flood attack. A server is considered under a potential connection-flood attack when backlog-queue expansion is required to handle the incoming connection requests. When more than 25 servers are under a potential connection-flood attack, no server's backlog queue is allowed to expand.



This slide shows new and changed IDS messages that are written to the system console.

Message EZD2015I is a new message that is written to the console when policy is processed and there is an IDS policy rule that discards ICMP redirects (both IPv4 and IPv6). EZD2015I is not displayed if IPCONFIG6 IGNOREREDIRECT is configured in the TCP/IP profile or if ICMPv6 redirects are already being ignored due to OMPROUTE.

The multiline message beginning with EZZ8761I is written to the console when an IDS event is detected. Several other messages are included to describe the event. Some of the messages are always included, while others are optional. Message EZZ8730I is a new message. It identifies the name of the stack where the IDS event was detected. It is always included.

Message EZZ8762I identifies the event type. The new event types for this message are TCP QUEUE CONSTRAINED, TCP QUEUE UNCONSTRAINED, TCP CONN RESET - QUEUE CONSTRAINED, GLOBAL TCP STALL ENTERED, and GLOBAL TCP STALL EXITED.

For events related to TCP-queue constraint, the type of TCP queue that is constrained – send, receive, or out of order – can be identified by the value in PROBEID. For example, the value 040A0001 indicates the TCP receive queue is constrained. The probe ID values are documented in the *z/OS Communications Server: IP and SNA Codes* publication.

syslogd attack messages

```
EZZ8648I TRMD ATTACK packet was discarded:07/16/2010 20:19:43.52,
sipaddr=9.67.120.4,dipaddr=9.67.120.3,sport=0,dport=0,type=IPPROTO,
proto=89,option=0,fragsize=0,correlator=2905,probeid=04060001,
sensorhostname=HOST1.COMPANYA.COM,restrictval=89

EZZ8649I TRMD ATTACK packet would have been discarded:
08/13/2010 15:07:14.05,sipaddr=2001:db8::2,dipaddr=2001:db8::1:2:3:4,
sport=0,dport=0,type=IPv6HopOptions,proto=0,option=0,fragsize=0,
correlator=7,probeid=040F0001,sensorhostname=HOST1.COMPANYA.COM,
restrictval=5

EZZ8653I TRMD ATTACK statistics:07/16/2010 20:20:07.93,
type=TCPQueueSize,attacks=5,action=noresetconn,
sensorhostname=HOST1.COMPANYA.COM

EZZ9327I TRMD Attack log records suppressed:07/16/2010 20:19:43.52,
attack type=IPFragment,count=57,probeid=0403FFF0,
sensorhostname=HOST1.COMPANYA.COM
```


This slide shows examples of changes to syslogd messages. These messages might now report IPv6 addresses. Message EZZ8649I on this slide shows an example of a message with an IPv6 address.

A new field, restrictval, has been added to messages EZZ8648I and EZZ8649I. For attack types that restrict protocols, options or next-header values, restrictval will contain the restricted value that was detected.

New attack types might be reported in these messages, for example, OutboundRaw6, IPv6NextHeader, IPv6HopOptions, IPv6DestOptions, DataHiding, TCPQueueSize, GlobalTCPStall.

New action types might be reported. The set of possible action types is: discard, nodiscard, resetconn, noresetconn.

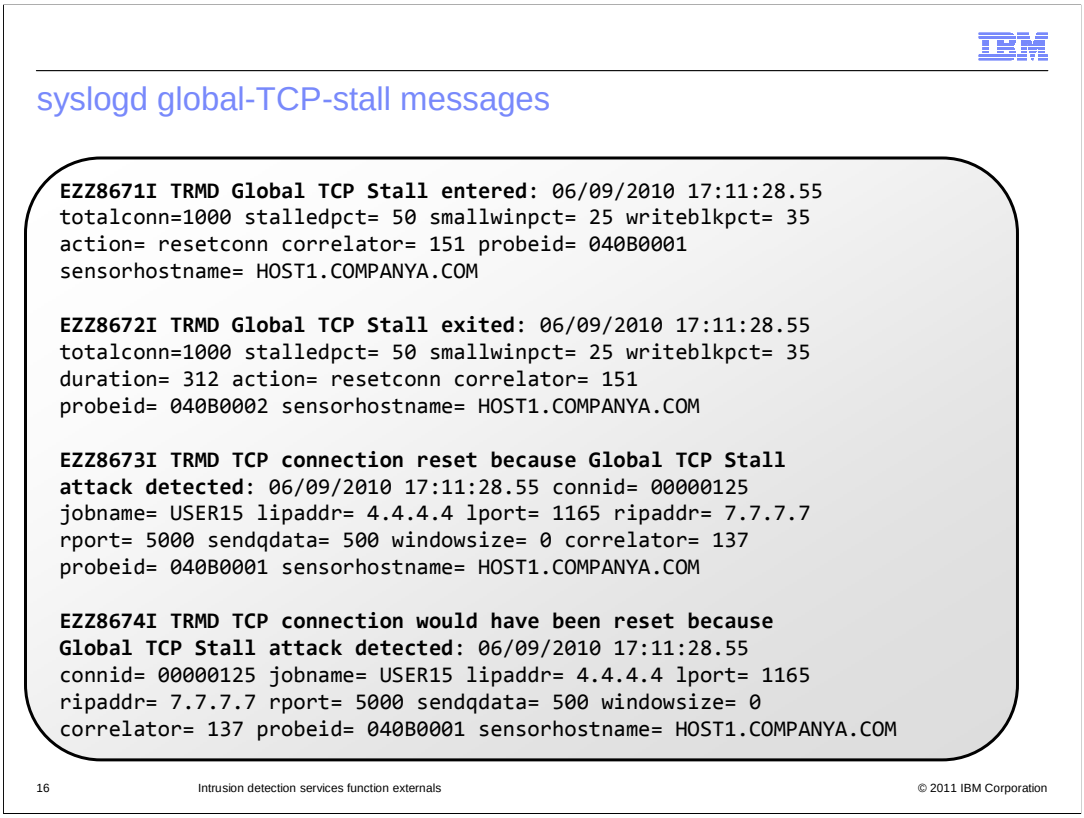
syslogd TCP-queue messages

```
EZZ8662I TRMD TCP receive queue constrained entry logged:
09/09/2008 17:11:28.55 , connid= 00000125 , jobname= USER15 ,
lipaddr= 4.4.4.4 , lport= 1165 , ripaddr= 7.7.7.7 , rport= 5000 ,
correlator= 137 , probeid= 01000001 , sensorhostname= HOST1.COMPANYA.COM ,
trigger= DataAge , dataage= 60 , bytesqueued= 576 , queuesize= S

EZZ8663I TRMD TCP receive queue constrained exit logged:
09/09/2008 17:11:33.55 , connid= 00000125 , jobname= USER15 ,
lipaddr= 4.4.4.4 , lport= 1165 , ripaddr= 7.7.7.7 , rport= 5000 ,
correlator= 137 , duration= 5 , probeid= 01000002 ,
sensorhostname= HOST1.COMPANYA.COM ,
dataage= 5 , bytesqueued= 256 , queuesize= S

EZZ8668I TRMD TCP connection reset due to constrained receive queue
detected: 09/09/2008 17:11:28.55 connid= 00000125 jobname= USER15
lipaddr= 4.4.4.4 lport= 1165 ripaddr= 7.7.7.7 rport= 5000
trigger= DataAge dataage= 60 bytesqueued= 576 queuesize= S
correlator= 137 probeid= 040A0003 sensorhostname= HOST1.COMPANYA.COM
```


This slide shows example messages that are written to syslogd relating to a constrained TCP receive queue. Messages EZZ8662I and EZZ8663I are existing messages, but additional information is now reported on these messages. Message EZZ8668I is a new message.

Similar messages are reported for a constrained TCP send queue: entry (EZZ8664I), exit (EZZ8665I) and reset (EZZ8669I). The first two messages report additional information, and the last message is a new message.

Similar messages are reported for a constrained TCP out-of-order queue: entry (EZZ8666I), exit (EZZ8667I) and reset (EZZ8670I). All three of these are new messages.



Messages EZZ8671I and EZZ8672I are added to report when a global-TCP-stall condition is entered or exited. If you have enabled detailed logging for global TCP stalls, message EZZ8673I or EZZ8674I is logged for each stalled connection depending on whether the configured action is to reset the connection.

trmdstat –A report

```
>trmdstat -A /tmp/tstlog.log
trmdstat for z/OS CS V1R13  Wed Nov 24 09:12:26 2010

Command Entered     : trmdstat -A /tmp/tstlog.log
...
                          ATTACK Summary

                          Packets Discarded

Destination IP Address: 192.168.105.53
Source IP Address:      192.168.105.50

Dest  Malform/   OutRaw4/   Redirect/  DestOpts/  IPProto/   PerpEcho/  EELDLC/
Port  Fragment   OutRaw6    IPOption   HopOpts    NextHdrs   DataHide   EEPort     EEMalfmd   NoId
----- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
    0         55          0          0          0          0          0          0          0          0
              0          0          0          0          0          0          0
    7          0          0          0          0          0         39          0          0          0
               0          0          0          0          0          0          0

                          Packets Would Have Been Discarded

Destination IP Address: 2001:db8:0:3:9:42:103:132
Source IP Address:      2001:db8:0:3:20a:5eff:fe04:8f16

Dest  Malform/   OutRaw4/   Redirect/  DestOpts/  IPProto/   PerpEcho/  EELDLC/
Port  Fragment   OutRaw6    IPOption   HopOpts    NextHdrs   DataHide   EEPort     EEMalfmd   NoId
----- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
    0          0          0          0          2          0          0          0          0          0
               0          0          0          1          1          0          0
```


This slide shows a sample trmdstat –A “attack” report. The information in this report is derived from attack messages EZZ8648I and EZZ8649I. The format of this report has changed to include all the new single packet attack types and to accommodate IPv6 source and destination addresses. The new attack types are OutRaw6, DestOpts, HopOpts, NextHdrs, and DataHide.

trmdstat –A –D report

```
>trmdstat -AD /tmp/tstlog.log
trmdstat for z/OS CS V1R13  Wed Nov 24 09:13:17 2010

Command Entered     : trmdstat -AD /tmp/tstlog.log
Log Time Interval   : Nov 12 04:36:51  - Nov 29 19:55:50
Stack Time Interval : Nov 12 04:36:47  - Nov 29 19:55:46
TRM Records Scanned : 227

                                     ATTACK Events

                                     Packets Discarded

                                       Destination IP Address/            DestPort/
 Attack      Date and Time               Source IP Address                 SrcPort   Correlator ProbeID
-------- ---------------------- ---------------------------------------- ---------  ---------- --------
NextHdrs 11/18/2010 16:02:53.51 2001:db8:0:3:9:42:103:132                         0          32 040D0001
                                2001:db8:0:3:20a:5eff:fe04:8f16                   0

Malform  11/13/2010 15:06:51.12 2001:db8:0:3:9:42:103:132                         0          12 0401003D
                                2001:db8:0:3:20a:5eff:fe04:8f16                   0


                                     Packets Would Have Been Discarded

                                       Destination IP Address/            DestPort/
 Attack      Date and Time               Source IP Address                 SrcPort   Correlator ProbeID
-------- ---------------------- ---------------------------------------- ---------  ---------- --------
OutRaw4  11/29/2010 19:24:27.02 192.168.0.5                                       0          63 04020001
                                192.168.101.3                                     0
```


This slide shows a sample trmdstat –A –D “attack-detail” report. The information in this report is derived from attack syslogd messages EZZ8648I and EZZ8649I. The format of this report has changed to accommodate IPv6 source and destination addresses. These new attack types can appear in this report: OutRaw6, DestOpts, HopOpts, NextHdrs, and DataHide.

trmdstat –A –S report

```
>trmdstat -AS /tmp/tstlog.log
trmdstat for z/OS CS V1R13  Wed Nov 24 09:19:06 2010

Command Entered     : trmdstat -AS /tmp/tstlog.log
Log Time Interval   : Sep 22 15:08:32  - Nov 29 15:24:28
Stack Time Interval : Sep 22 15:08:22  - Nov 29 19:24:23
TRM Records Scanned : 227

                          ATTACK  Statistics

 Attack           Date and Time              Attacks           Action
--------      ---------------------        ----------        -----------
TCPStall      09/22/2010 15:08:22.06                0        noresetconn
TCPQueSz      09/22/2010 15:08:22.07                0        resetconn
TCPStall      09/22/2010 15:18:14.49                0        resetconn
XIDFlood      11/12/2010 04:34:02.05                1        nodiscard
EEMalfmd      11/12/2010 05:24:52.34                3        discard
EEPortCk      11/12/2010 05:24:52.34                1        discard
Redirect      11/12/2010 18:52:16.19                0        nodiscard
PerpEcho      11/14/2010 16:03:09.07                1        nodiscard
NextHdrs      11/18/2010 16:04:59.46                2        discard
NextHdrs      11/18/2010 18:28:20.17                1        nodiscard
Flood         11/23/2010 14:46:27.18                7        discard
OutRaw6       11/29/2010 19:24:23.33                1        discard
```


This slide shows a sample trmdstat –A –S “attack-summary” report. The information in this report is derived from attack syslogd EZZ8653I messages. This report can display statistics information for all new attack types. The action field will display the configured action value for the attack type.

trmdstat –Q report

```
>trmdstat -Q /tmp/tstlog.log
trmdstat for z/OS CS V1R13  Wed Nov 24 09:30:03 2010

Command Entered     : trmdstat -Q /tmp/tstlog.log
...
                 TCP Queue Size Summary

                   Connections Reset

Remote IP Address: 2001:db8::20a:5eff:fe04:8f16

Local
Port  SendQReset RecvQReset OofOQReset
----- ---------- ---------- ----------
 1000          0          0          1

...
                   TCP Queue Constraints

Remote IP Address: 2001:db8::20d:60ff:fe24:32ae

Local ------- SendQ Constraint ------- ------- RecvQ Constraint ------- ------- OofOQ Constraint -------
Port    Enter       Exit     Duration    Enter       Exit     Duration    Enter       Exit     Duration
----- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
 1000          0          0          0          1          1       3541          1          1       1044
```


This slide shows a sample of the new trmdstat –Q “queue-size” report. The information in this report is derived from TCP queue size syslogd messages EZZ8662I, EZZ8663I, EZZ8664I, EZZ8665I, EZZ8666I, EZZ8667I, EZZ8668I, EZZ8669I, and EZZ8670I.

trmdstat –Q –D report

```
>trmdstat -QD /tmp/tstlog.log
trmdstat for z/OS CS V1R13  Wed Nov 24 09:31:27 2010

...
                                        TCP Queue Size Events

                                          Connections Reset

Remote IP Address: 2001:db8::20a:5eff:fe04:8f16

                         Local                                          Remote ConnID/  QueueSize/  DageAge/
    Date and Time      Queue Port              Local IP Address          Port   JobName   Trigger    BytesQed  Correlator
---------------------- ----- ----- ---------------------------------------- ------ -------- ---------- ---------- ----------
11/10/2010 24:39:34.18 OofO   1000 2001:db8::9:42:105:17                    54224 000000D1     S              30          26
                                                                                 IBMUSER1  BytesQed       25600

...
                                        TCP Queue Constraints

Remote IP Address: 2001:db8::20d:60ff:fe24:32ae

                      Type/ Local                                       Remote ConnID/  QueueSize/  DageAge/   Duration/
    Date and Time      Queue Port              Local IP Address          Port   JobName   Trigger    BytesQed  Correlator
---------------------- ----- ----- ---------------------------------------- ------ -------- ---------- ---------- ----------
11/10/2010 17:33:27.02 Enter  1000 2001:db8::9:42:105:17                  61572 000000A5     S             132
                       OofO                                                      IBMUSER3  DataAge         6840           5
11/10/2010 17:51:41.87 Exit   1000 2001:db8::9:42:105:17                  61572 000000A5     S               0        1044
                       OofO                                                      IBMUSER3                  0           5
11/10/2010 18:38:27.35 Enter  1000 2001:db8::9:42:105:17                  60468 0000012E     S              97
                       Recv                                                      IBMUSER8  DataAge         4080          12
11/10/2010 19:40:20.24 Exit   1000 2001:db8::9:42:105:17                  60468 0000012E     S               0        3541
                       Recv                                                      IBMUSER8                  0          12
```


This slide shows a sample of the new trmdstat –Q –D “queue-size-detail” report. The information in this report is derived from TCP queue size syslogd messages EZZ8662I, EZZ8663I, EZZ8664I, EZZ8665I, EZZ8666I, EZZ8667I, EZZ8668I, EZZ8669I, and EZZ8670I.

trmdstat –G report

```
>trmdstat -G /tmp/tstlog.log
trmdstat for z/OS CS V1R13  Mon Dec  6 13:16:37 2010

Command Entered     : trmdstat -G /tmp/tstlog.log
Log Time Interval   : Oct 29 18:02:33  - Oct 29 18:53:33
Stack Time Interval : Oct 29 18:02:19  - Oct 29 18:53:21
TRM Records Scanned : 504

               Global TCP Stall Summary

Global TCP Stall Entered:  1
Global TCP Stall Exited:   1
Global TCP Stall Duration: 2920

               Connections Reset

No records to display

               Connections Would Have Been Reset

            Remote IP Address             Count
------------------------------------ ----------
10.11.2.1                                   126
10.12.2.1                                   125
2001:db8:10::11:2:1                         126
2001:db8:10::12:2:1                         125
```


This slide shows a sample of the new trmdstat –G “global-TCP-stall” report. The information in this report is derived from global TCP stall syslogd messages EZZ8671I, EZZ8672I, EZZ8673I, and EZZ8674I.

trmdstat –G –D report

```
>trmdstat -GD /tmp/tstlog.log
trmdstat for z/OS CS V1R13  Mon Dec  6 13:16:51 2010

Command Entered     : trmdstat -GD /tmp/tstlog.log
...

                          Global TCP Stall Events

                                                 Small    Write
                             Stalled             Window   Block
    Date and Time        Type   Percent TotalConns Percent Percent  Duration  Correlator   Action
----------------------- -------- ------- ---------- ------- ------- ---------- ---------- -----------
10/29/2010 18:02:19.08 Enter        50%       1004     49%      0%                     3 noresetconn
10/29/2010 18:53:21.22 Exit         25%       2008     25%      0%       2920          3 noresetconn

...
                          Connections Would Have Been Reset

Remote IP Address: 10.11.2.1

                     Local                                          Remote ConnID/  SendQSize/
    Date and Time    Port              Local IP Address             Port   JobName  WindowSize Correlator
---------------------- ----- ---------------------------------------- -----  -------- ---------- ----------
10/29/2010 18:02:19.08 20000 10.11.1.2                                 1119  00000091       8000          3
                                                                             USER13            0
10/29/2010 18:02:19.08 20000 10.11.1.2                                 1140  000000A5      20000          3
                                                                             USER13            0
```


This slide shows a sample of the new trmdstat –G –D “global-TCP-stall-detail” report. The information in this report is derived from global TCP stall syslogd messages EZZ8671I, EZZ8672I, EZZ8673I, and EZZ8674I.

trmdstat miscellany

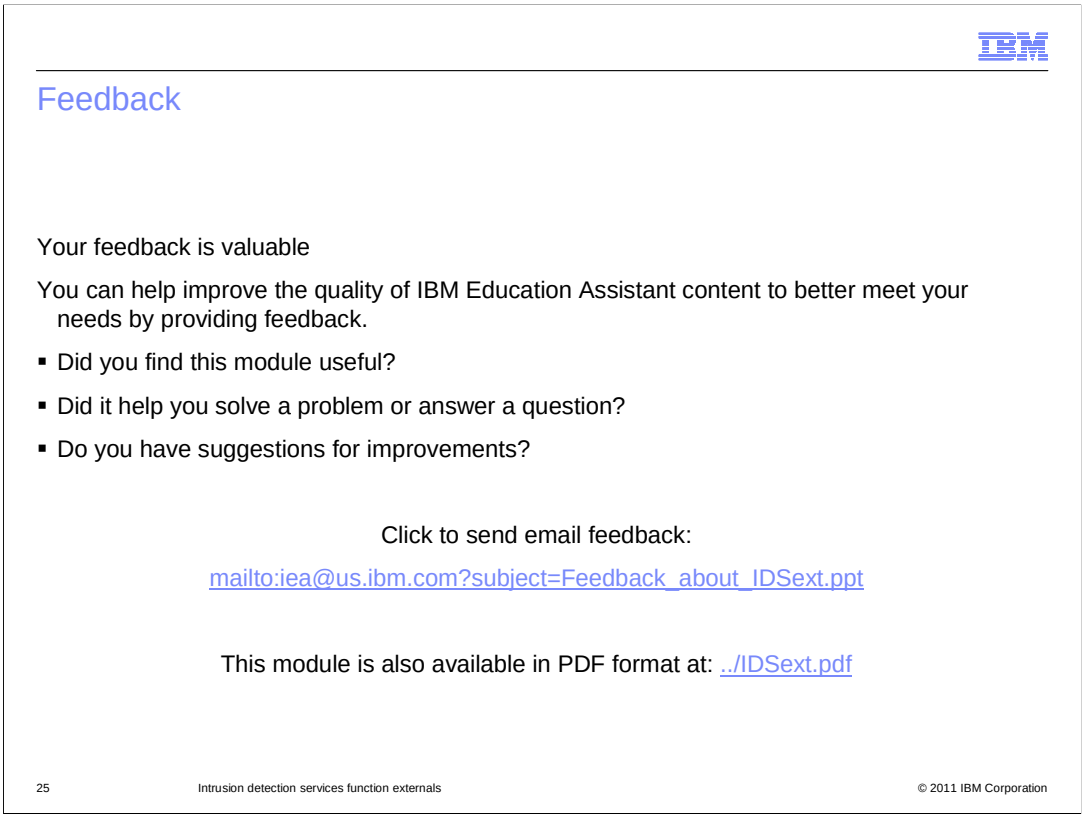
- Additional reports updated for IPv6 addresses
  - Flood reports: flood summary and detail
  - Scan reports: scan summary and detail
  - TCP TR reports: summary, extended summary, detail and statistics
  - UDP TR reports: UDP TR summary and detail
  - Connection report: connection detail
- IDS overall summary report
- UDP TR statistics report
- trmdstat default report

Several of the existing trmdstat reports are updated to accommodate IPv6 addresses. The flood summary (-F) and detail (-F –D) scan reports now include IPv6 addresses. The scan summary (-N) and detail (-N –D) reports include IPv6 addresses. The TCP TR summary (-T), extended summary (-T –E), detail (-T –D) and statistics (-T –S) reports now include IPv6 addresses. Also the UDP TR summary (-U) and detail (-U –D) reports and the connection detail (-C –D) report now include IPv6 addresses.

The IDS overall summary report is updated to include summary information for new IDS messages.

Formatting for the UDP TR statistics report is updated to consolidate heading information and data, for a more usable report.

The trmdstat default report, provided when the trmdstat command is issued with no report option, is changed to the –I “IDS-summary report.” The IDS summary report provides a summary of all IDS information.



You can help improve the quality of IBM Education Assistant content by providing feedback.

Trademarks, disclaimer, and copyright information

IBM, the IBM logo, ibm.com, and z/OS are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of other IBM trademarks is available on the web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY.
THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. WHILE EFFORTS WERE MADE TO VERIFY THE COMPLETENESS AND ACCURACY OF THE INFORMATION CONTAINED IN THIS PRESENTATION, IT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. IN ADDITION, THIS INFORMATION IS BASED ON IBM'S CURRENT PRODUCT PLANS AND STRATEGY, WHICH ARE SUBJECT TO CHANGE BY IBM WITHOUT NOTICE. IBM SHALL NOT BE RESPONSIBLE FOR ANY DAMAGES ARISING OUT OF THE USE OF, OR OTHERWISE RELATED TO, THIS PRESENTATION OR ANY OTHER DOCUMENTATION. NOTHING CONTAINED IN THIS PRESENTATION IS INTENDED TO, NOR SHALL HAVE THE EFFECT OF, CREATING ANY WARRANTIES OR REPRESENTATIONS FROM IBM (OR ITS SUPPLIERS OR LICENSORS), OR ALTERING THE TERMS AND CONDITIONS OF ANY AGREEMENT OR LICENSE GOVERNING THE USE OF IBM PRODUCTS OR SOFTWARE.