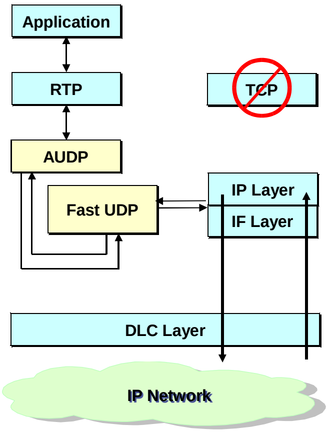
z/OS Communications Server

Intrusion detection services for Enterprise Extender

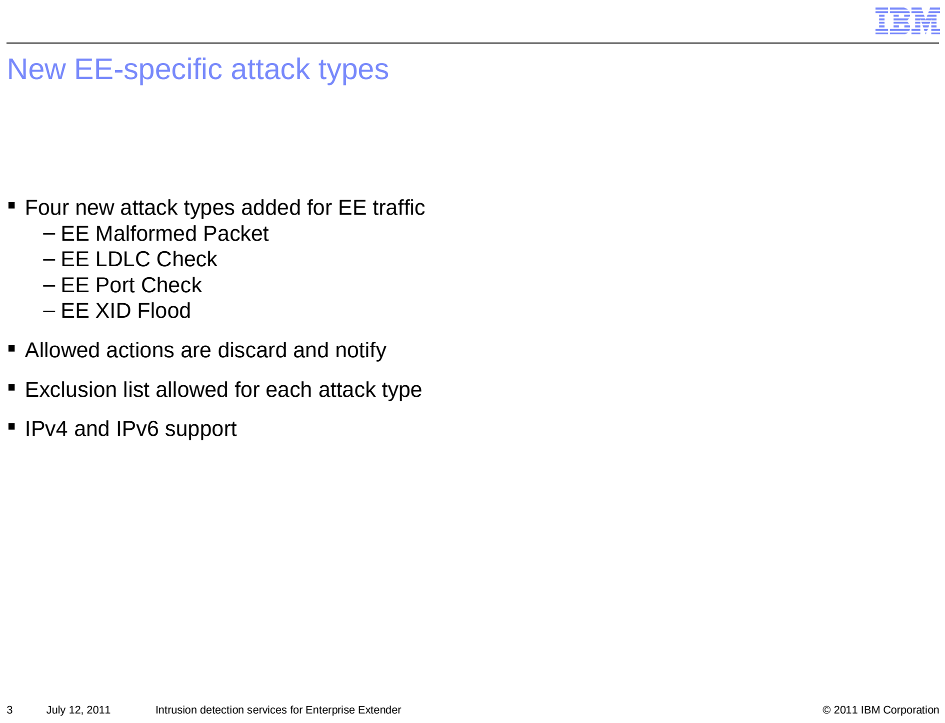
This presentation describes the Intrusion Detection Services for Enterprise Extender in z/OS® V1R13 Communications Server.

Intrusion detection services support for EE

- Enterprise Extender is a SNA over IP solution
- SNA data is transmitted as UDP datagrams through IP network
- Enterprise Extender is implemented in the SNA and TCPIP stacks



Enterprise Extender is a SNA over IP solution implemented in z/OS Communications Server. Enterprise Extender uses high performance routing (HPR) as the SNA transport protocol and UDP as the IP transport protocol. The SNA data is encapsulated into UDP datagrams and routed using IP protocols. The parts shaded in yellow (the AUDP and Fast UDP components) show how EE fits in the SNA and IP network protocols.



New EE-specific attack types

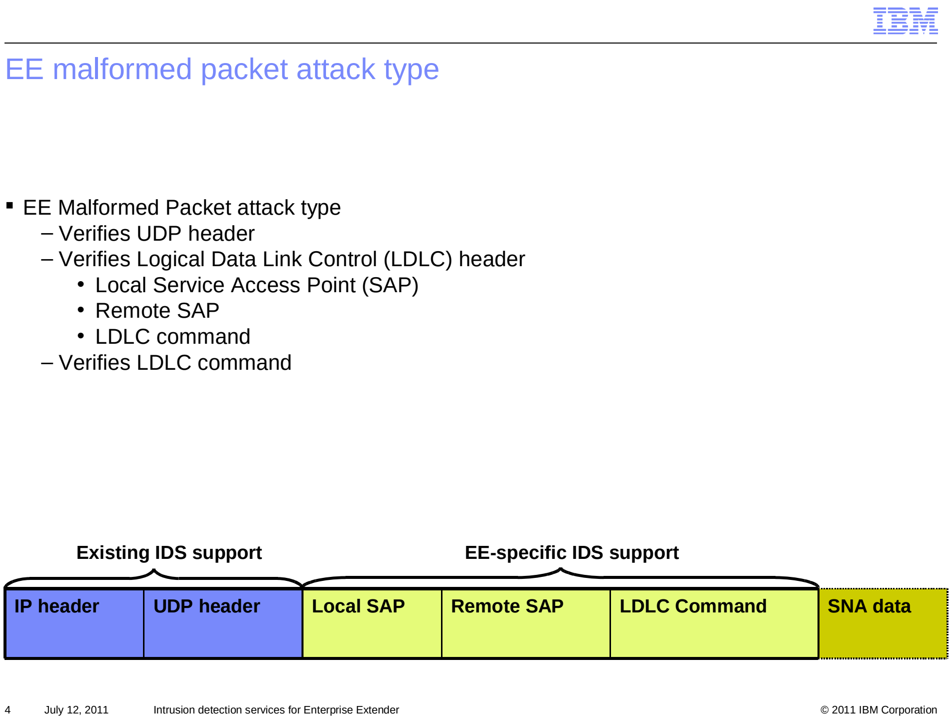
- Four new attack types added for EE traffic
  - EE Malformed Packet
  - EE LDLC Check
  - EE Port Check
  - EE XID Flood
- Allowed actions are discard and notify
- Exclusion list allowed for each attack type
- IPv4 and IPv6 support

3 July 12, 2011 Intrusion detection services for Enterprise Extender © 2011 IBM Corporation

Intrusion detection services (IDS) provides security to the IP stack from attacks.

To protect against packets that are not valid architecturally, four new EE-specific IDS attack types can be enabled. These attack types are supported for both IPv4 and IPv6 EE traffic. Each attack type is enabled separately. When an attack type is enabled, all inbound EE packets are checked for the conditions associated with the rule. If a suspicious packet is detected then the actions configured for the IDS rule are taken. The allowed actions are to discard the packet and to provide notification. The discard action is not allowed for the EE XID Flood attack type.

Each new EE attack type allows an exclusion list to be coded for the rule. If a packet is detected as an attack and it is determined that this is existing acceptable behavior, the source IP address can be put in an exclusion list to exclude it from detection as an attack.



EE malformed packet attack type

- EE Malformed Packet attack type
  - Verifies UDP header
  - Verifies Logical Data Link Control (LDLC) header
    - Local Service Access Point (SAP)
    - Remote SAP
    - LDLC command
  - Verifies LDLC command

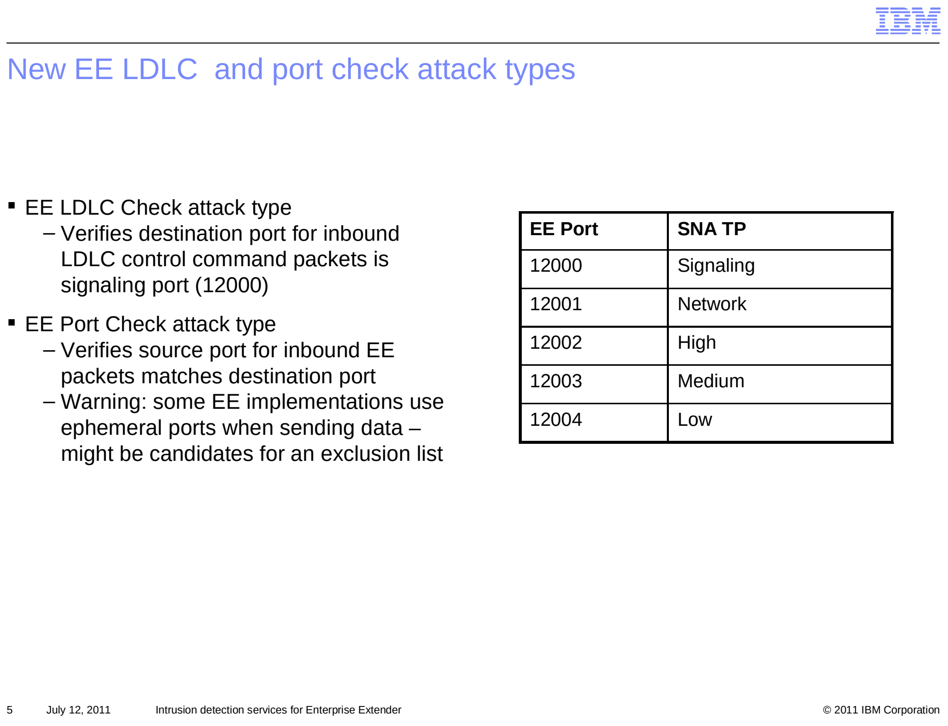
Existing IDS support		EE-specific IDS support			
IP header	UDP header	Local SAP	Remote SAP	LDLC Command	SNA data

4 July 12, 2011 Intrusion detection services for Enterprise Extender © 2011 IBM Corporation

Each packet sent or received on an EE connection uses a Logical Data Link Control (LDLC) header. The first two bytes are the local and remote SAP values for the connection. The third byte is the LDLC command. EE packets can be fixed length, consisting of the transport headers and the LDLC header, or variable length, containing the LDLC header in addition to SNA data such as an XID. The value of the LDLC command determines the SNA transmission priority and therefore the port used to send the packet.

The EE malformed packet IDS attack type detects malformed EE packets. When enabled, the EE malformed packet attack rule verifies the LDLC and UDP headers and flags any inconsistencies or problems found as a possible attack.

The general IDS malformed packet checking discards packets with malformed IP and transport headers, such as UDP and ICMP. The EE malformed packet attack type is separate from this, and specifically checks only the EE headers for malformed data. You can configure the EE malformed packet checking to notify for malformed packets, and additionally to discard these packets instead of forwarding them to VTAM®.



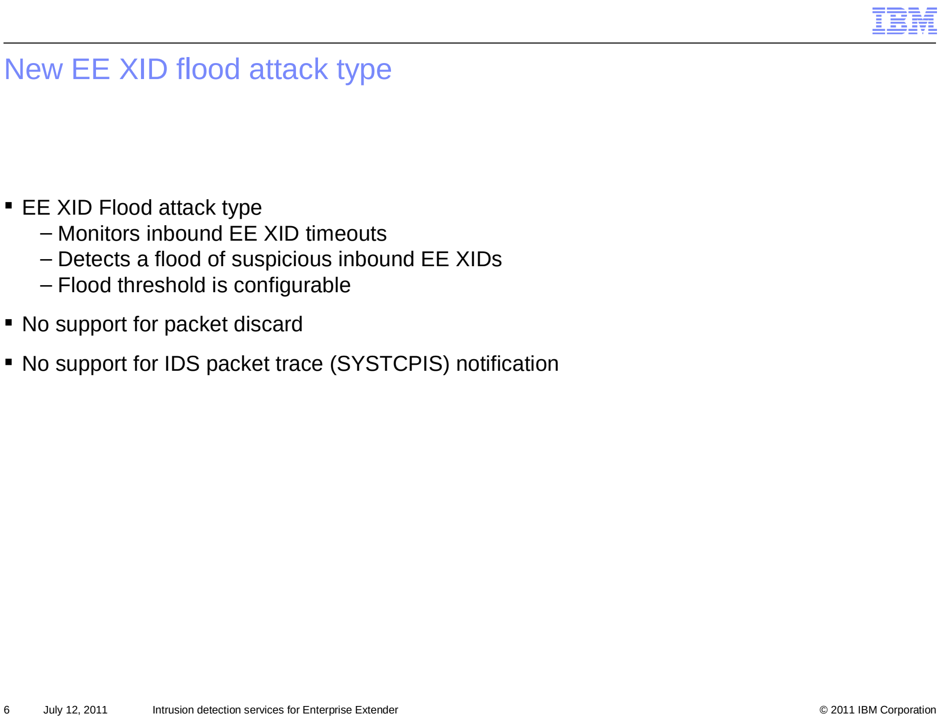
New EE LDLC and port check attack types

- EE LDLC Check attack type
  - Verifies destination port for inbound LDLC control command packets is signaling port (12000)
- EE Port Check attack type
  - Verifies source port for inbound EE packets matches destination port
  - Warning: some EE implementations use ephemeral ports when sending data – might be candidates for an exclusion list

EE Port	SNA TP
12000	Signaling
12001	Network
12002	High
12003	Medium
12004	Low

Enterprise extender data flows over five UDP ports corresponding to the five SNA data transmission priorities. The default ports are 12000 through 12004. The EE LDLC check attack type verifies that inbound EE packets are received on the correct destination port. When an EE LDLC attack rule is enabled, the value of the LDLC command type is checked to determine if the packet is received on the correct port. If the packet is received on the wrong port it is flagged as a possible attack.

The EE port check attack type checks the source port of the received packet. When an EE port check attack type rule is enabled, the source port must match the destination port. If the source and destination ports are not equal then the packet is flagged as a possible attack. But note that some EE implementations use ephemeral ports when sending EE data. These might be candidates to add to the exclusion list for an EE port check attack type rule.



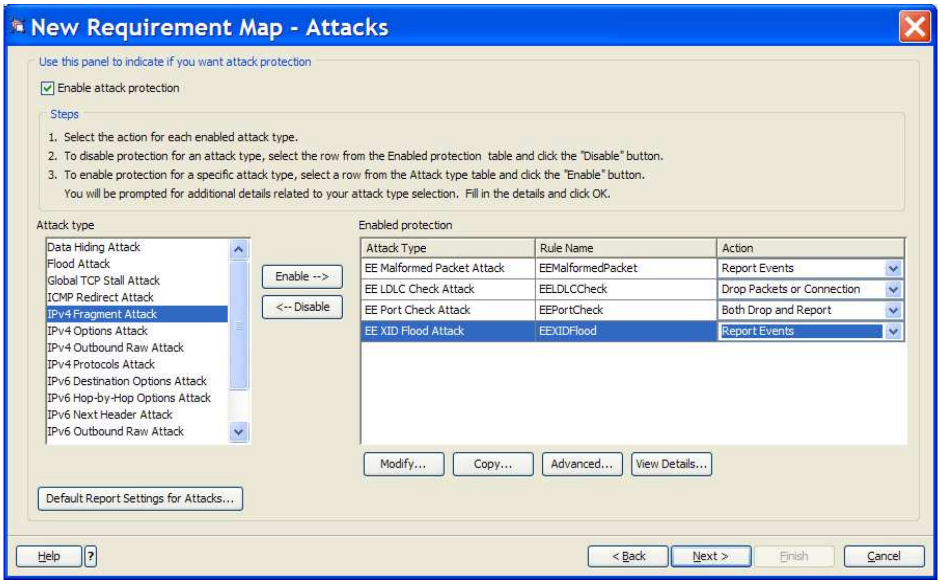
New EE XID flood attack type

- EE XID Flood attack type
  - Monitors inbound EE XID timeouts
  - Detects a flood of suspicious inbound EE XIDs
  - Flood threshold is configurable
- No support for packet discard
- No support for IDS packet trace (SYSTCPIS) notification

The EE XID flood attack type monitors inbound XID activity, which is analogous to the TCP SYN. When an EE XID flood rule is enabled, XID timeouts are flagged as a possible attack, similar to a TCP SYN flood. A flood threshold is coded that determines the number of XID timeouts that can be received in a one minute interval before a flood is detected. The default value is 100. If the number of timeouts in one minute is greater than the threshold, an XID flood is detected. When the number of XID timeouts falls below the threshold, the EE XID flood ends.

The EE XID flood attack rule will always forward the XID to VTAM. The rule cannot be configured to discard the packet. In addition, the EE XID flood attack type does not support IDS trace notification.

New attack types



Use this panel to indicate if you want attack protection

☑ Enable attack protection

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 a row from the Attack type 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.

Attack type

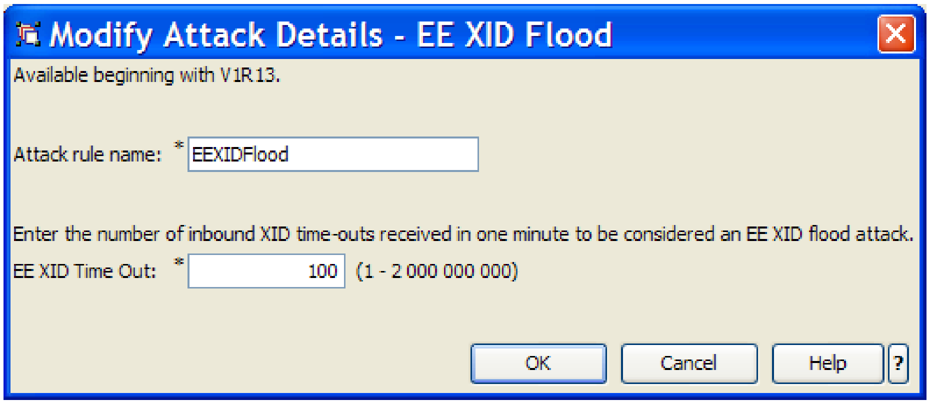
- Data Hiding Attack
- Flood Attack
- Global TCP Stall Attack
- ICMP Redirect Attack
- IPv4 Fragment Attack
- IPv4 Options Attack
- IPv4 Outbound Raw Attack
- IPv4 Protocols Attack
- IPv6 Destination Options Attack
- IPv6 Hop-by-Hop Options Attack
- IPv6 Next Header Attack
- IPv6 Outbound Raw Attack

Enabled protection

Attack Type	Rule Name	Action
EE Malformed Packet Attack	EEMalformedPacket	Report Events
EE LDLC Check Attack	EELDLCCheck	Drop Packets or Connection
EE Port Check Attack	EEPortCheck	Both Drop and Report
EE XID Flood Attack	EEXIDFlood	Report Events

The Configuration Assistant was updated to support the four new attack types. The window here shows a new requirement map with the four new EE attack types listed. You can disable an attack type by selecting it and clicking the disable button.

EE XID flood threshold



Modify Attack Details - EE XID Flood

Available beginning with V1R13.

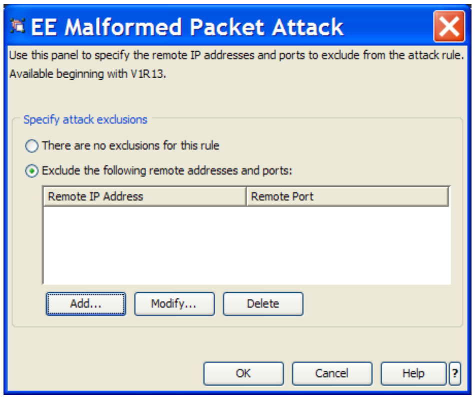
Attack rule name: * EEXIDFlood

Enter the number of inbound XID time-outs received in one minute to be considered an EE XID flood attack.

EE XID Time Out: * 100 (1 - 2 000 000 000)

The XID flood attack type allows a configurable value for the number of XID timeouts. This value represents the number of XID timeouts detected in one minute before entering an XID flood-detected state. The XID timeout has a default value of 100 and a range of one to 2,000,000,000.

Exclusion list



EE Malformed Packet Attack

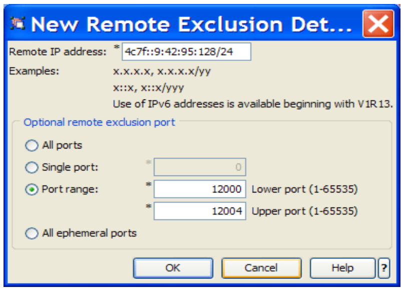
Use this panel to specify the remote IP addresses and ports to exclude from the attack rule. Available beginning with V1R13.

Specify attack exclusions

○ There are no exclusions for this rule

● Exclude the following remote addresses and ports:

Remote IP Address	Remote Port



New Remote Exclusion Det...

Remote IP address: * 4c7f::9:42:95:128/24

Examples: x.x.x.x, x.x.x.x/yy
x::x, x::x/yyy
Use of IPv6 addresses is available beginning with V1R13.

Optional remote exclusion port

○ All ports

○ Single port: * 0

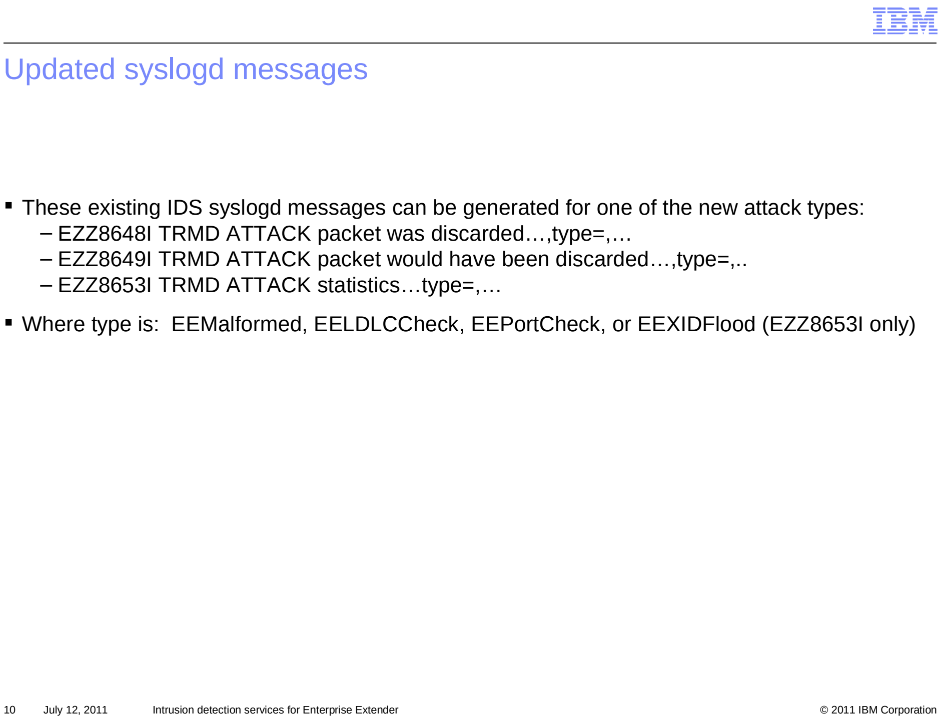
● Port range: * 12000 Lower port (1-65535)

* 12004 Upper port (1-65535)

○ All ephemeral ports

An exclusion list can be configured for each EE attack type. An exclusion list is used to exclude a source IP address or range of IP addresses from detection as an attack. Also a single or range of ports can be included in the exclusion list. Some EE implementations do not conform to all of the EE protocol rules, for example, in their choice of source ports for some EE packets. The exclusion list can be used to prevent detecting such partners as a source of malformed packets.

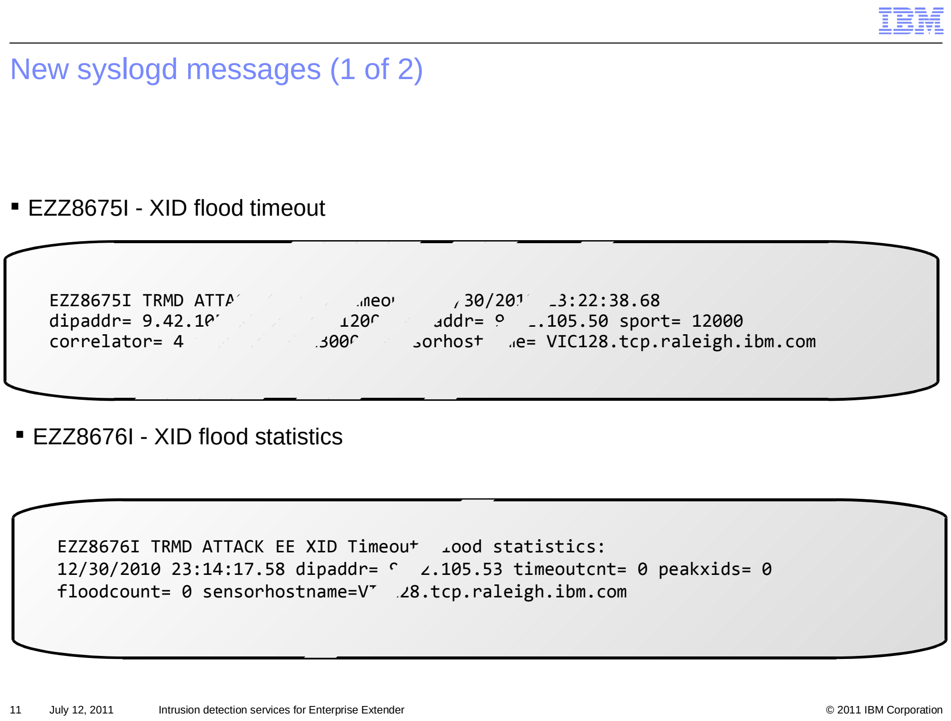
To code an exclusion list, on the first window select the Exclude radio button and click add and the second window will appear. The next window shows how to create an exclusion list. An exclusion list can be further refined by adding a source port or a range of ports.



Updated syslogd messages

- These existing IDS syslogd messages can be generated for one of the new attack types:
  - EZZ8648I TRMD ATTACK packet was discarded…,type=,…
  - EZZ8649I TRMD ATTACK packet would have been discarded…,type=,..
  - EZZ8653I TRMD ATTACK statistics…type=,…
- Where type is: EEMalformed, EELDLCCheck, EEPortCheck, or EEXIDFlood (EZZ8653I only)

Existing IDS messages were updated to document an attack for one of the new attack types. Each of the messages is updated to output the reason for the attack following the type field.



New syslogd messages (1 of 2)

- EZZ8675I - XID flood timeout

```
EZZ8675I TRMD ATTA          .meo      /30/201  3:22:38.68
dipaddr= 9.42.10           120     addr= 9  .105.50 sport= 12000
correlator= 4              300      sorhost  .e= VIC128.tcp.raleigh.ibm.com
```

- EZZ8676I - XID flood statistics

```
EZZ8676I TRMD ATTACK EE XID Timeout  lood statistics:
12/30/2010 23:14:17.58 dipaddr= 9  2.105.53 timeoutcnt= 0 peakxids= 0
floodcount= 0 sensorhostname=V  28.tcp.raleigh.ibm.com
```

The EZZ8675I message is written, using syslogd, when the EE XID flood attack type is enabled and an XID timeout occurs. This message documents the XID timeout which can lead to an XID flood condition. The message contains information to help identify the packet that caused the timeout.

The EZZ8676I message is written, using syslogd, if the XID flood attack type enables the gathering of statistics. This message is written in addition to the existing EZZ8653I statistics message. This message provides additional information related to XID timeouts during the statistics interval.

New syslogd messages (2 of 2)

- EZZ8677I - XID flood start

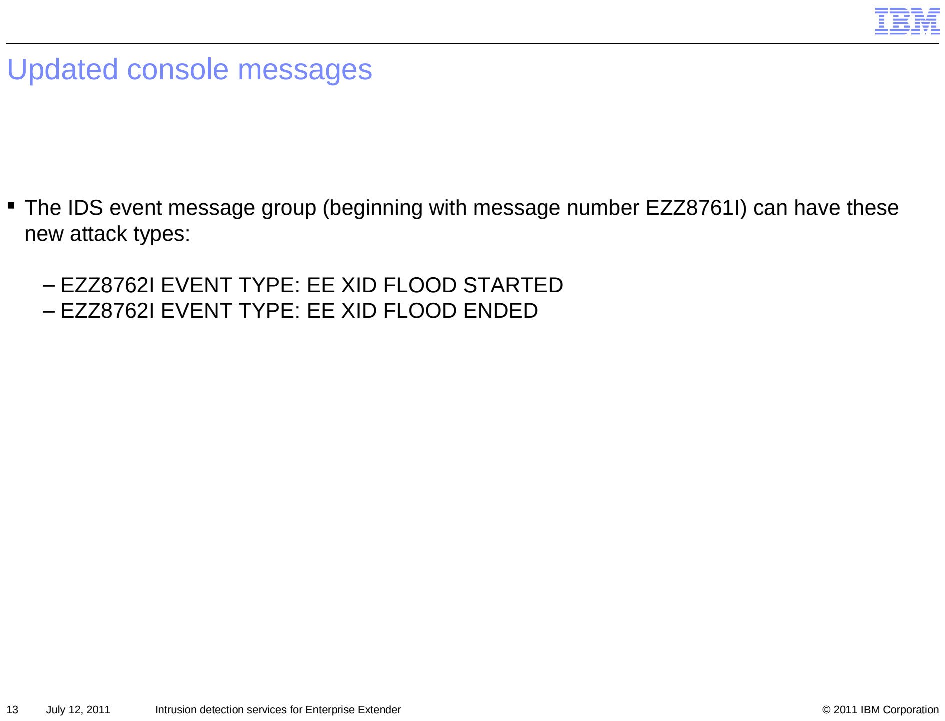
```
EZZ8677I TRMD ATTACK            meo          start:    30/2010 2   2:44.18
dipaddr= 9.42.105.5          chr          0 last   = 9.42.10   sipcnt= 2
correlator= 5 pr          300          hostnar   VIC128.tc   aleigh.ibm.com
```

- EZZ8678I - XID flood end

```
EZZ8678I TRMD ATTAC          im           end:    30/2010 23:26:42.71
dipaddr= 9.42.105          ion          eoutcnt   1 lastsip= 9.42.105.50
sipcnt= 12 corr          pr          130003
sensorhostnar          .tc          .ibm.c
```

EZZ8677I is a new message written using syslogd. This message is written when an XID flood is detected. This message contains information that can be used to determine the cause of the flood.

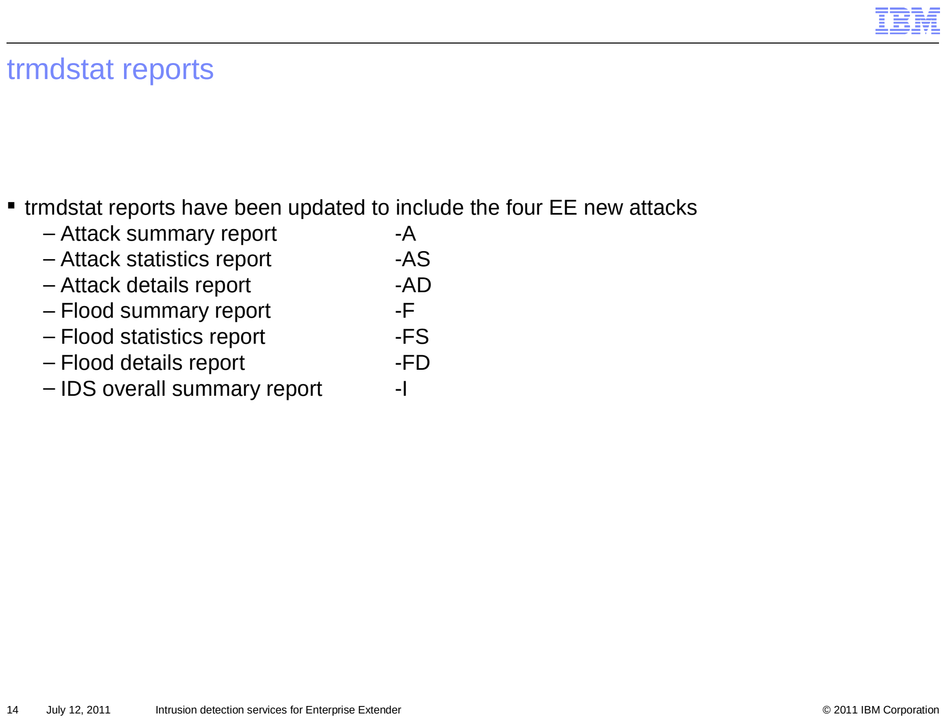
EZZ8678I is a new message written using syslogd. This message is written when an XID flood ends. The message contains information pertaining to the duration of the flood in addition to the number of XID timeouts that occurred during this timeframe.



Updated console messages

- The IDS event message group (beginning with message number EZZ8761I) can have these new attack types:
  - EZZ8762I EVENT TYPE: EE XID FLOOD STARTED
  - EZZ8762I EVENT TYPE: EE XID FLOOD ENDED

EZZ8762I is an existing message issued as a part of the EZZ8761I message group. The message group is written to the console when an attack type specifies logging messages to the console when an attack is detected. EZZ8762I was changed to include events to document EE flood start and EE flood end messages.

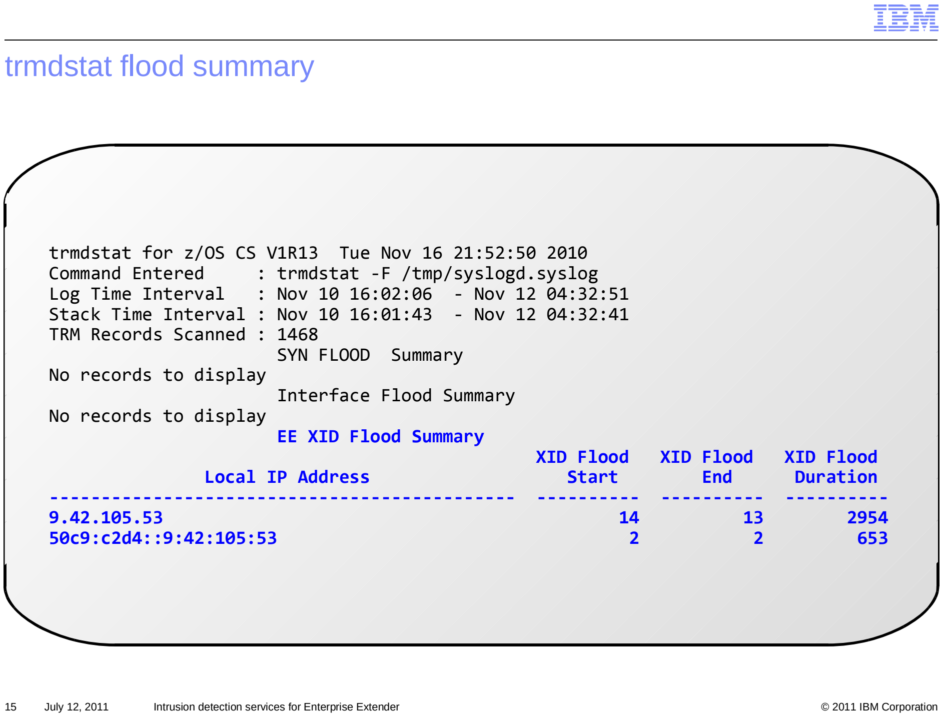


trmdstat reports

- trmdstat reports have been updated to include the four EE new attacks

– Attack summary report	-A
– Attack statistics report	-AS
– Attack details report	-AD
– Flood summary report	-F
– Flood statistics report	-FS
– Flood details report	-FD
– IDS overall summary report	-I

The z/OS UNIX® system services trmdstat command is used to create trmdstat reports. The trmdstat reports were updated to support the four new EE attack types. The XID flood attack type information was added to the existing flood reports. The remaining attack types were added to the attack reports. Also the IDS summary report was updated to include the four new attack types.



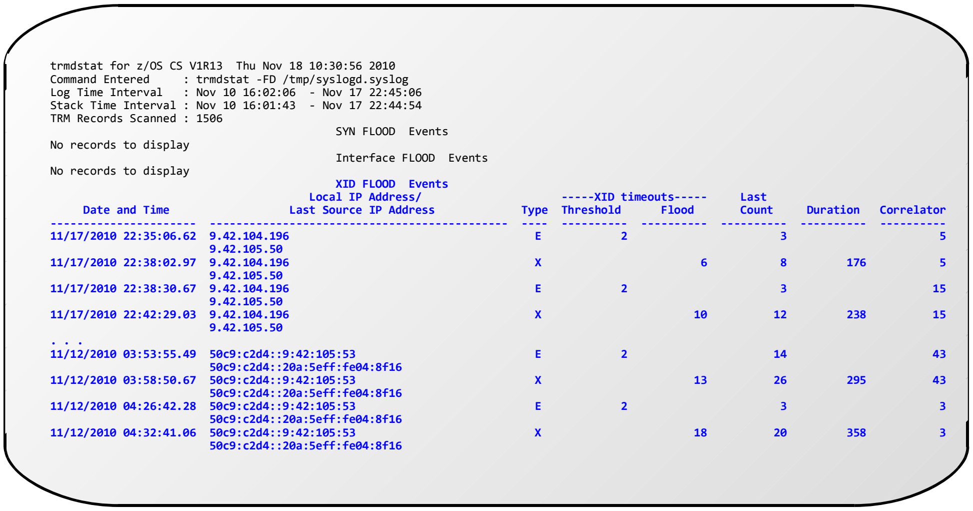
trmdstat flood summary

```
trmdstat for z/OS CS V1R13  Tue Nov 16 21:52:50 2010
Command Entered     : trmdstat -F /tmp/syslogd.syslog
Log Time Interval   : Nov 10 16:02:06  - Nov 12 04:32:51
Stack Time Interval : Nov 10 16:01:43  - Nov 12 04:32:41
TRM Records Scanned : 1468
                      SYN FLOOD  Summary
No records to display
                      Interface Flood Summary
No records to display
                      EE XID Flood Summary
                                               XID Flood   XID Flood   XID Flood
               Local IP Address                   Start        End      Duration
---------------------------------------------  ----------  ----------  ----------
9.42.105.53                                            14          13        2954
50c9:c2d4::9:42:105:53                                  2           2         653
```

15 July 12, 2011 Intrusion detection services for Enterprise Extender

The flood summary was written to provide information about the SYN and interface floods. The report was changed to include EE XID flood summary information. The EE XID flood information summarizes the activity for each local VIPA (virtual IP address) used for Enterprise Extender. The information shown for each is the number of flood starts and the number of flood ends. The XID flood duration provides the total number of seconds in XID flood state.

trmdstat flood details



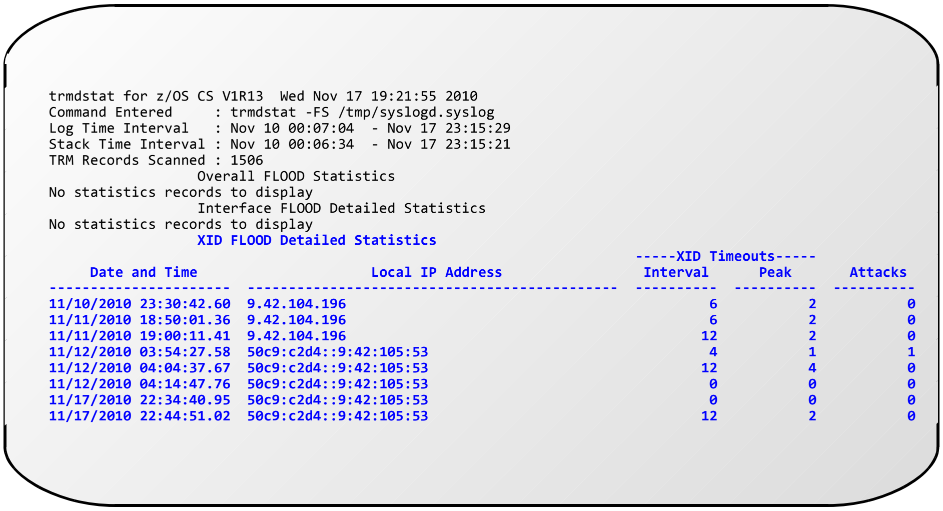
```
trmdstat for z/OS CS V1R13  Thu Nov 18 10:30:56 2010
Command Entered     : trmdstat -FD /tmp/syslogd.syslog
Log Time Interval   : Nov 10 16:02:06  - Nov 17 22:45:06
Stack Time Interval : Nov 10 16:01:43  - Nov 17 22:44:54
TRM Records Scanned : 1506
                                           SYN FLOOD  Events

No records to display
                                           Interface FLOOD  Events

No records to display
                                           XID FLOOD  Events
                                       Local IP Address/                     -----XID timeouts-----     Last
     Date and Time                  Last Source IP Address             Type  Threshold      Flood       Count     Duration   Correlator
----------------------  ---------------------------------------------  ----  ----------  ----------  ----------  ----------  ----------
11/17/2010 22:35:06.62  9.42.104.196                                     E            2                       3                       5
                        9.42.105.50
11/17/2010 22:38:02.97  9.42.104.196                                     X                        6           8         176           5
                        9.42.105.50
11/17/2010 22:38:30.67  9.42.104.196                                     E            2                       3                      15
                        9.42.105.50
11/17/2010 22:42:29.03  9.42.104.196                                     X                       10          12         238          15
                        9.42.105.50
. . .
11/12/2010 03:53:55.49  50c9:c2d4::9:42:105:53                           E            2                      14                      43
                        50c9:c2d4::20a:5eff:fe04:8f16
11/12/2010 03:58:50.67  50c9:c2d4::9:42:105:53                           X                       13          26         295          43
                        50c9:c2d4::20a:5eff:fe04:8f16
11/12/2010 04:26:42.28  50c9:c2d4::9:42:105:53                           E            2                       3                       3
                        50c9:c2d4::20a:5eff:fe04:8f16
11/12/2010 04:32:41.06  50c9:c2d4::9:42:105:53                           X                       18          20         358           3
                        50c9:c2d4::20a:5eff:fe04:8f16
```

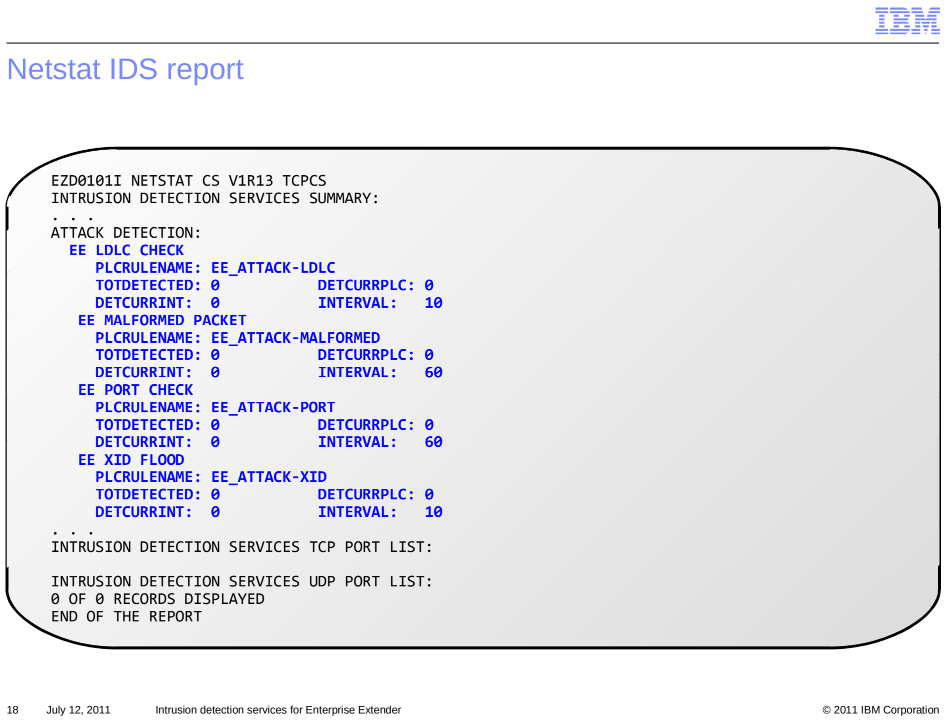
The trmdstat flood details report provides detailed information for the SYN and interface floods. The detailed information for the EE XID flood was added. The detailed output examines the flood start and flood end messages (EZZ8677I and EZZ8678I). The output provided helps determine what event started the flood and how the flood ended.

trmdstat flood statistics



```
trmdstat for z/OS CS V1R13  Wed Nov 17 19:21:55 2010
Command Entered     : trmdstat -FS /tmp/syslogd.syslog
Log Time Interval   : Nov 10 00:07:04  - Nov 17 23:15:29
Stack Time Interval : Nov 10 00:06:34  - Nov 17 23:15:21
TRM Records Scanned : 1506
                  Overall FLOOD Statistics
No statistics records to display
                  Interface FLOOD Detailed Statistics
No statistics records to display
                  XID FLOOD Detailed Statistics
                                                                       -----XID Timeouts-----
     Date and Time                     Local IP Address                 Interval      Peak       Attacks
----------------------  ---------------------------------------------  ----------  ----------  ----------
11/10/2010 23:30:42.60  9.42.104.196                                            6           2           0
11/11/2010 18:50:01.36  9.42.104.196                                            6           2           0
11/11/2010 19:00:11.41  9.42.104.196                                           12           2           0
11/12/2010 03:54:27.58  50c9:c2d4::9:42:105:53                                  4           1           1
11/12/2010 04:04:37.67  50c9:c2d4::9:42:105:53                                 12           4           0
11/12/2010 04:14:47.76  50c9:c2d4::9:42:105:53                                  0           0           0
11/17/2010 22:34:40.95  50c9:c2d4::9:42:105:53                                  0           0           0
11/17/2010 22:44:51.02  50c9:c2d4::9:42:105:53                                 12           2           0
```

The trmdstat flood statistics report provided information for the SYN and interface floods. The statistics information for XID flood was added. The trmdstat flood statistics provide information about the statistics logged for each VIPA. If statistics are enabled a statistics message, EZZ8676I, is written for each VIPA at the end of the logging interval. The flood statistics provide pertinent information from each of these messages.



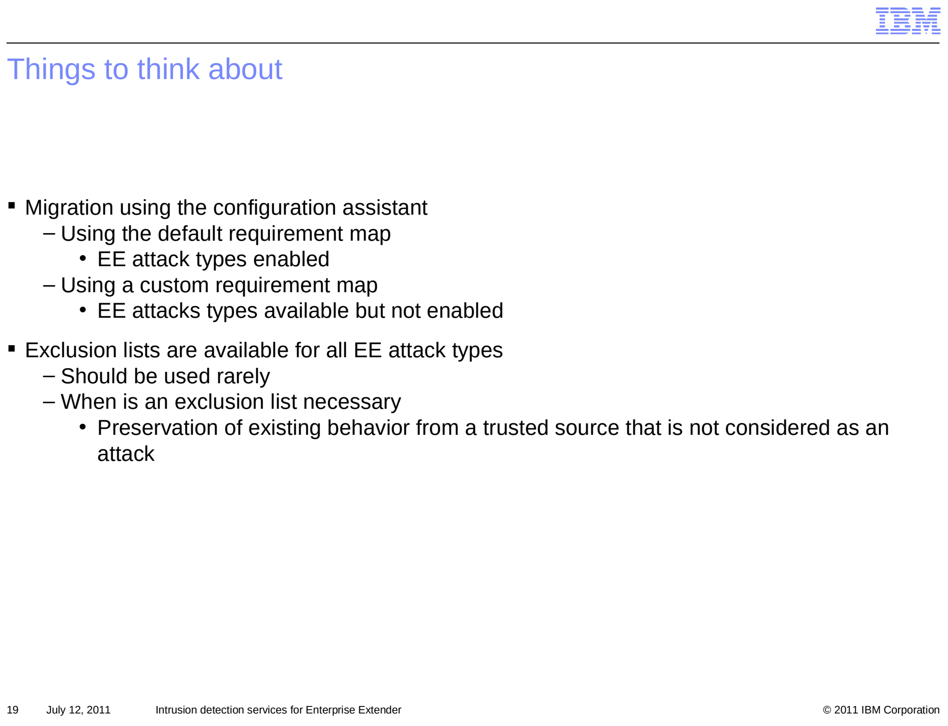
Netstat IDS report

```
EZD0101I NETSTAT CS V1R13 TCPCS
INTRUSION DETECTION SERVICES SUMMARY:
. . .
ATTACK DETECTION:
  EE LDLC CHECK
     PLCRULENAME: EE_ATTACK-LDLC
     TOTDETECTED: 0           DETCURRPLC: 0
     DETCURRINT:  0           INTERVAL:   10
   EE MALFORMED PACKET
     PLCRULENAME: EE_ATTACK-MALFORMED
     TOTDETECTED: 0           DETCURRPLC: 0
     DETCURRINT:  0           INTERVAL:   60
   EE PORT CHECK
     PLCRULENAME: EE_ATTACK-PORT
     TOTDETECTED: 0           DETCURRPLC: 0
     DETCURRINT:  0           INTERVAL:   60
   EE XID FLOOD
     PLCRULENAME: EE_ATTACK-XID
     TOTDETECTED: 0           DETCURRPLC: 0
     DETCURRINT:  0           INTERVAL:   10
. . .
INTRUSION DETECTION SERVICES TCP PORT LIST:

INTRUSION DETECTION SERVICES UDP PORT LIST:
0 OF 0 RECORDS DISPLAYED
END OF THE REPORT
```

18 July 12, 2011 Intrusion detection services for Enterprise Extender © 2011 IBM Corporation

The Netstat IDS command can be used to display IDS information. The command can be issued from the console, TSO, or OMVS. The output was updated to include the attack information for the four new EE attack types.

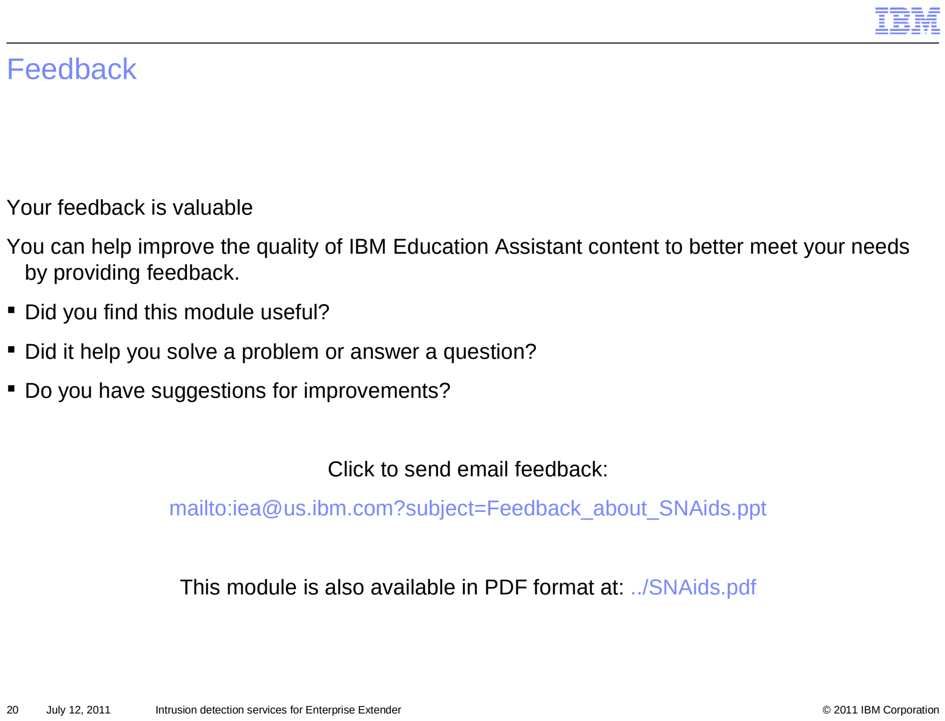


Things to think about

- Migration using the configuration assistant
  - – Using the default requirement map
    - EE attack types enabled
  - – Using a custom requirement map
    - EE attacks types available but not enabled
- Exclusion lists are available for all EE attack types
  - – Should be used rarely
  - – When is an exclusion list necessary
    - Preservation of existing behavior from a trusted source that is not considered as an attack

The new EE attack types can be enabled by using the Configuration Assistant. If the Configuration Assistant is used to migrate an existing policy the new policy generated is different based on the type of old policy. If the old policy was the default policy, then the new migrated policy adds the new EE attack types with notification enabled. If the migrated policy is a customized policy then the new policy will not have the new EE IDS attack types enabled. The new attack types can then be enabled by updating the policy.

The EE IDs rules should be defined without any exclusion lists. The exclusion list should be used to exclude packets from source IP addresses and the attack has been determined to not be harmful. This is commonly used to protect against existing behavior from adjacent Enterprise Extender endpoints.



Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send email feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_SNAids.ppt

This module is also available in PDF format at: ../SNAids.pdf

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

Trademarks, disclaimer, and copyright information

THE INFORMATION CONTAINED IN THIS PRESENTATION IS PROVIDED FOR INFORMATIONAL PURPOSES ONLY. Other company, product, or service names may be trademarks or service marks of others.

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.