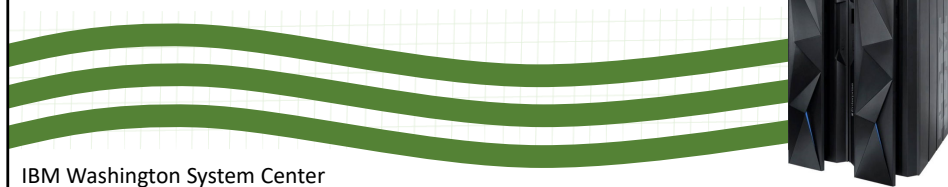


Securing and Encrypting Network Traffic
with z/OS Communications Server and
Policy Agent

Security Workshop

Intrusion Detection Services (IDS)



IBM Washington System Center
IBM Technical Sales Support

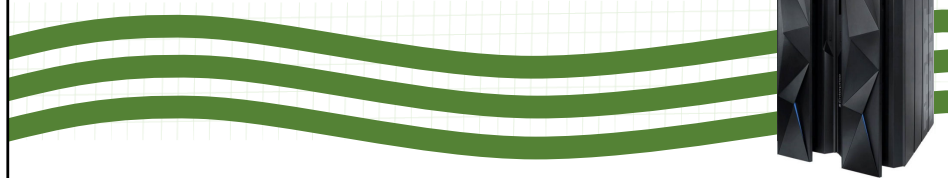
Trademarks

- **The following are Registered Trademarks of the International Business Machines Corporation in the United States and/or other countries.**
 - IBM
 - z/OS
- **The following are trademarks or registered trademarks of other companies.**
 - Microsoft is a registered trademark of Microsoft Corporation in the United States and other countries.
- All other products may be trademarks or registered trademarks of their respective companies.
- Refer to www.ibm.com/legal for further legal information.
- OSA-Express Features
- There are many different types of OSA-Express features. In this document where OSA is mentioned it refers to an OSA port on any of the OSA-Express features unless a specific OSA-Express feature is mentioned.

Agenda

- Intrusion Detection Services (IDS) Overview
- Detecting Scans
- Detecting Attacks
- Regulating Traffic (Traffic Regulation)
- Implementing IDS
- Policy Messages, Logs, Display Output
- Reports on Attacks
- Displaying IDS Policy with NETSTAT

Intrusion Detection Services (IDS) Overview

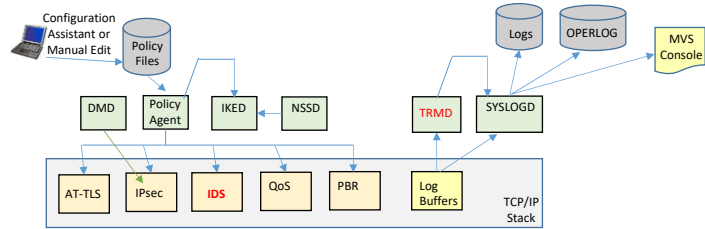


011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 4

Lots of Different Policy Types and Started Tasks



- Policy Agent
 - Installs Policies into the TCP/IP stack
- TCP/IP Stack
 - Enforces the Policies
- DMD (Defense Manager Daemon)
 - ipsec command can be used to install temporary IP Filter rules.
- IKED (Internet Key Exchange Daemon)
 - Required for IPsec Dynamic VPN (Virtual Private Network) Tunnels
- NSSD (Network Security Server Daemon)
 - Required for IKEv2
 - Provides central RACF certificate repository for remote IKED applications
 - Provides DataPower access to RACF
- TRMD (Traffic Regulation Management Daemon)
 - Required for log messages to syslogd for IP Filter, IPsec, and IDS
- SyslogD
 - Recommended for logging

011_ZCS301_IDS

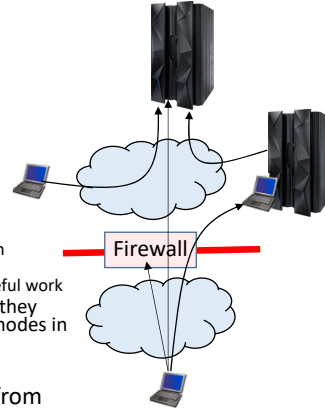
© Copyright IBM Corporation 2023

Page 5

Configuration Assistant can really help getting the whole environment setup.

Protect Against Intrusion Threats

- What is an intrusion?
 - Scan - Information Gathering
 - Network and system topology
 - Data location and contents
 - Attacks
 - Eavesdropping/Impersonation/Theft
 - On the network/on the host
 - Basis 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 be deliberate with malicious intent, or they can occur as a result of various forms of errors on nodes in the network
- 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



011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 6

What exposes critical services and sensitive data to loss of availability?

Attacks from the Internet and the intranet can attack critical internal resources, limit access to critical applications, and even compromise critical data. The vulnerability of organizations has increased with the promotion of remote employee and customer access to important systems. Thus e-business, e-commerce, and the increased mobility of employees has not only improved business efficiency but it has also increased security threats.

Perimeter security like Intrusion Detection Services (IDS) or Intrusion Prevention Systems (IPS) helps protect the network.. IDSs detect and alert when a known attack occurs. They depend on a list of known attack types (they maintain attack "signatures").

Intrusion Prevention Systems (IPSS) detect and protect against attacks, but also rely on a database of attack signatures and known attack symptoms. They rarely have reporting mechanisms attached to them that enable analysis of attacks or vulnerabilities.

z/OS Intrusion Detection Services provides: detection, mitigation, and reporting of attacks.

Firewall Definition

- According to Wikipedia ...
 - "A firewall is a device or set of devices configured to permit, deny, encrypt, or proxy all computer traffic between different security domains based upon a set of rules and other criteria."
 - A Firewall - when referring to network security - can be any device or application or process that defines security Rules to implement when traffic meets certain conditions:
 - Detecting and optionally reporting on Intrusions based upon knowledge of known intrusion types.
 - Permit or Deny (Block) Traffic based upon a set of conditions
 - Encryption in order to make data confidential
 - Network Address Translation (NAT) in order to mask IP addresses *
 - Relay the traffic after terminating it in a SOCKS or PROXY server *
 - Conditions can be:
 - Origin of Traffic
 - Destination of Traffic
 - Networking Protocol (TCP, UDP, etc)
 - Application Type
 - Time of Day
 - When PCI mentions "firewall" it can be referring to any of these security functions, but it is usually referring to IP Filtering and Intrusion Detection Services (IDS).
- * z/OS Communications server does not provide NAT, SOCKS server, or PROXY server.

011_ZCS301_IDS

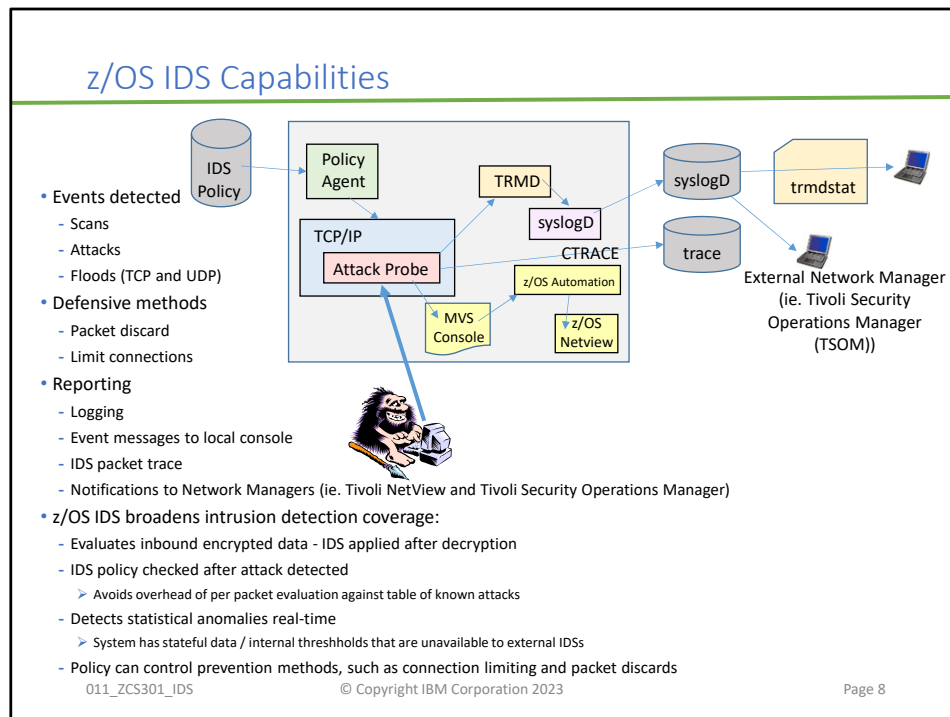
© Copyright IBM Corporation 2023

Page 7

z/OS Communications Server provides:

- IPSec
- IP packet filtering
- IDS

To satisfy the PCI Requirement 1.3.3, you need to implement an IP Filtering or IDS solution outside of z/OS that is capable of stateful inspection of packet flows.



Tivoli NetView z/OS V5R1, PTF UA11043

- Provides local z/OS management support for IDS

Tivoli Security Operations Manager

- Provides enterprise-wide 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

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

IDS Event Types

- Scans
 - Intent of scanning is to learn about the target in order to perform an attack against it (Subnet structure, addresses, masks, addresses in-use, system type, op-sys, application ports available, release levels)
 - Scan Types
 - TCP port scans
 - UDP port scans
 - ICMP scans
 - Sensitivity levels for all scans can be adjusted to control number of false positives recorded.
- Attacks
 - Intent of an attack is to crash or hang the system (Single or multiple packet)
 - Attack Types (See details in Attack section of this presentation)
 - Malformed packet events
 - Inbound fragment restrictions (IPv4)
 - IP protocol restrictions
 - IP option restrictions
 - UDP perpetual echo
 - ICMP redirect restrictions
 - Outbound raw restrictions
 - Flood events (physical interface flood detection, synflood, and connection flooding across multiple servers)
 - TCP Queue Size
 - Global TCP Stall
 - Enterprise Extender (EE) Attacks (EE Malformed Packet, LDLC Check, Port Check, XID Flood)
- Traffic Regulation (TR)
 - TR protects against traffic that could be intended to flood the system but the traffic could be an unexpected peak in valid requests
 - Traffic Regulation Limits
 - UDP backlog limit - management by port
 - TCP total connection and source percentage management by port
 - All TCP servers that use a UNIX process model to create a new process when a client connects to them should have a cap on the number of connections (FTP, otenetD, etc.)

011_ZCS301_IDS

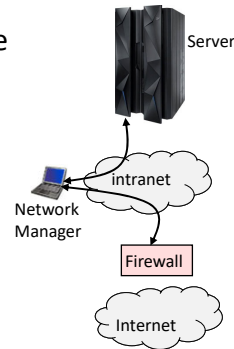
© Copyright IBM Corporation 2023

Page 9

Although at V1R13 protection has been extended to IPv6, some attack types continue to apply only to the IPv4 protocol. Three remaining IPv4 attack types (IP protocol restrictions, IP option restrictions, and Outbound RAW restrictions) are tied to the IPv4 header structure and so they continue to apply only to IPv4 packets. Other attack types are new and apply only to the IPv6 protocol. Please consult the TCP/IP documentation for more detail.

z/OS IDS versus External Firewall

- Not all problems perceived as Attacks are deliberate attacks by Hackers.
 - Hardware/Software bug may cause rogue machine
- Do you trust all intranet users?
 - Disgruntled employee
- When z/OS is encryption endpoint
 - Firewall IDS policies are not able to be applied to encrypted data.
- Network Managers may use external Firewall and z/OS IDS information concurrently.
 - ie. Tivoli Security Operations Manager



011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 10

We are not saying to get rid of external Firewalls. They are still serving their original purpose.

What we are saying is that the z/OS IDS is a useful tool in addition to all external Firewalls.

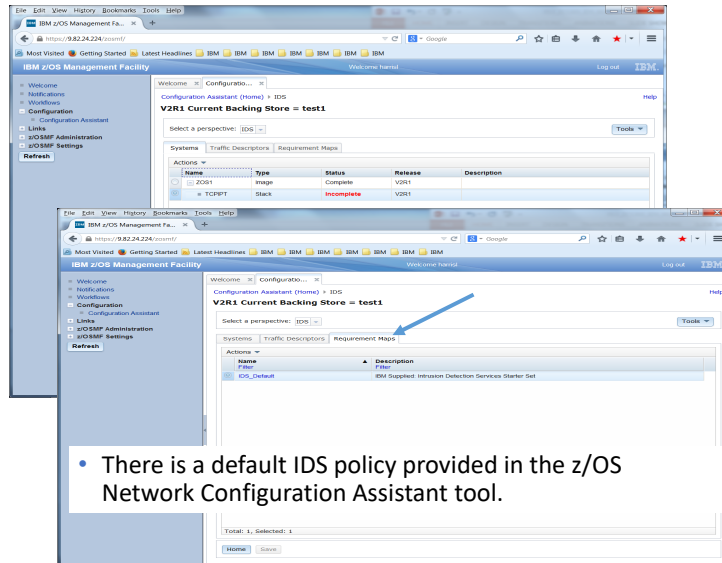
z/OS TCP/IP stack leverages existing error checking to avoid having to perform pattern matching on each packet for certain types of attacks: malformed packets, inbound fragment checking to detect whether there have been fragment overlays in the IP or transport header. SYN Flood protection.

External IDS's must perform pattern matching by scanning individual packets even for these attack types.

For cases in which a policy definition is required, the z/OS IDS policy is checked to determine whether the event represents an intrusion. However, even in such cases, the policy itself is used to update internal control blocks so that expensive lookups of each policy are still not required in order to determine policy violations.

IDS in z/OS is not looking for a specific known signature -- we're basing the detection more on protocol rules and on restrictions that the customer specifies in an IDS policy or in-context checking. We also do things like scan detection and traffic regulation that are very different from basic pattern matching.

IDS in Configuration Assistant tool



- There is a default IDS policy provided in the z/OS Network Configuration Assistant tool.

011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 11

Default IDS Policy

- The default only provides Attack protection.

The screenshot displays the IBM z/OS Management Facility Configuration Assistant interface. The left sidebar shows the navigation menu with options like Welcome, Notifications, Workflows, Configuration, and z/OSMF Settings. The main panel shows the 'View Details' for the 'IDS - View Details' configuration. A table titled 'Attack Protection Summary' lists various attack types and their default settings.

Enabled Attack Protection	Rule Name	Actions	Reports	Time Condition	Default Report Settings
	Data Hiding Attack¹	datahiding	Report Events	Use Default Report Settings	None
	IPv6 Outbound Raw Attack¹	ipv6OutboundRaw	Report Events	Use Default Report Settings	None
	IPv6 Destination Options Attack¹	ipv6DestinationOptions	Report Events	Use Default Report Settings	None
	IPv6 Hop-by-Hop Options Attack¹	ipv6HopbyHop	Report Events	Use Default Report Settings	None
	IPv6 Next Header Attack¹	ipv6NextHeader	Report Events	Use Default Report Settings	None
	TCP Queue Size Attack¹	tcpQueueSize	Report Events	Use Default Report Settings	None
	Global TCP Stall Attack¹	globalTCPStall	Report Events	Use Default Report Settings	None
	Flood Attack	Flood	Both Drop and Report	Use Default Report Settings	None
	Perpetual Echo Attack	Echo	Report Events	Use Default Report Settings	None
	IPv4 Protocols Attack	ipv4Protocol	Report Events	Use Default Report Settings	None
	IPv4 Options Attack	ipv4Option	Report Events	Use Default Report Settings	None
	ICMP Redirect Attack	icmpRedirect	Report Events	Use Default Report Settings	None
	Malformed Packet Attack	malformedPacket	Both Drop and Report	Use Default Report Settings	None
	IPv4 Outbound Raw Attack	ipv4OutboundRaw	Report Events	Use Default Report Settings	None

Console Parameters: No
 SYSLOG Parameters: SYSLOG: Yes, SYSLOG Level: 4 - Warning
 Statistics Parameters: Statistics: Yes, Statistics Interval: 60 Minutes
 Report Stat if no events: Yes
 Trace Parameters: No

011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 12

Scan Detection

Configurable with the IBM Configuration Assistant GUI.
However, the default IDS policy on the GUI does not include Scan policies.



Scan... Prelude to Attack

- A source host accessing multiple unique resources (ports or interfaces) over a specified period of time.
- Scan Policy: time interval, threshold, exclusion list, notification policy, tracing policy
- z/OS IDS Scan definition
 - Source host 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 (usually less than 5 minutes)
 - Slow scans
 - Different resources intermittently accessed over a longer time period (many hours)
- Scan event types supported
 - ICMP scans
 - TCP port scans
 - UDP port scans

011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 14

The majority of scanning is not done by people with malicious intent, but... the majority of people with malicious intent start with scanning.

Legitimate scans are done by an installation's network management software or users to determine the state of devices, systems and applications.

Many network search portals scan to discover new public information sites to add to their index.

For example, for either malicious or non-malicious intent, a SCAN may attempt to Map the following Network Resources:

- Subnet structure, addresses, masks
- Addresses in-use, system type, op-sys
- Application ports available, release levels

Scan Policy

- 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
 - ie. network management
 - Specify a scan sensitivity level
 - By port for UDP and TCP
 - Highest priority rule for ICMP

Scan Sensitivity

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

- Scan sensitivity determines whether an event is “counted” as a scan.
- Total number of scan events are tracked against an origin source IP address.
 - Total number of scan events for all scan event types is compared to the policy threshold.
 - If the threshold is exceeded for a single IP address, policy-directed notification and documentation is triggered.
- Balance between detecting every scan and limit the overhead.
 - Reserve low ports not explicitly in use to allow configuration of low sensitivity on low ports for both UDP and TCP.

011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 16

Scan Sensitivity can be set to Low, Medium or High.

This table shows how the policy-specified sensitivity affects the counting of scan events. The event suspicion level is determined by the stack and is documented in the reports that are produced.

The information in this and subsequent tables is extracted from the IP Configuration Guide.

High sensitivity considers any access to the resource as coming from a potential scanner and will start tracking the source host. For example, connections to listening TCP ports, read requests to bound UDP ports and non multicast pings without special options (such as record route and timestamp) would all be considered as coming from possible scanners. Since this level of monitoring results in tracking normal application users, the overhead is high.

Medium sensitivity only tracks possibly suspicious and very suspicious activity. For example, a user that attempts to connect to a closed port. This could be a scanner trying to determine which applications are installed or could be a legitimate user trying to connect into an application that is temporarily down.

Low sensitivity only tracks very suspicious activity (ie. activities that would normally be associated with a scanner.) For example, a user that attempts to connect to a RESERVED port or issues a ping to a multicast address.

Attack Detection

Configurable with the IBM Configuration Assistant GUI.
The default IDS policy on the GUI includes Attack policies.



011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 17

Attack

- Any activity to flood or crash the IP stack so as to deny service to legitimate users.
- The system already silently defends itself from attacks against the TCP/IP stack.
 - Malformed Packets
 - Syn Floods
 - Interface Floods
- IDS adds capability to control recording of intrusion events and supporting documentation.

011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 18

What's an Attack?

Any activity to flood or crash the IP stack so as to deny service to legitimate users.

z/OS already silently protects itself from many specific known attacks. IDS on z/OS adds notification.

Attack Policy:

- Use attack policy to set thresholds on legitimate activity.
- Use attack policy to obtain notification and documentation of attacks.

Attack Categories - Details

- 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 high percentage of packet discards on a physical interface. Detects flood of SYN packets from "spoofed" sources.
 - V1R13: Detects SYN floods against multiple servers.
- TCP Queue Size (V1R13)
 - Detects when the send or receive queue for an SMC-R link becomes constrained.
 - Data is available to be sent but cannot be sent.
 - Data is stored into the peer remote memory buffer that is not acknowledged (30 sec).
 - Data is available to be delivered but the application does not receive the data (30 sec).
- Global TCP Stall (V1R13)
 - Detects when at least 50% of the active TCP connections are stalled and at least 1000 TCP connections are active.
 - A TCP connection that traverses an SMC-R link is treated as a stalled connection when the TCB is write-blocked.
- Enterprise Extender Attacks (V1R13)
 - EE Malformed Packet, LDLC Check, Port Check, XID Flood

011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 19

Attack Policy

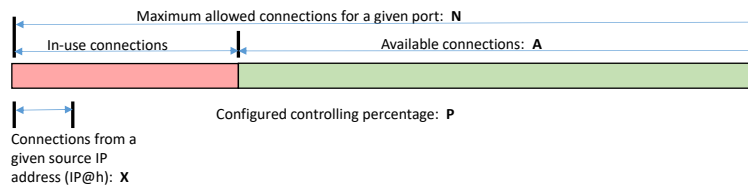
- Attack policy provides the ability to:
 - Control attack detection for one or more attack categories independently.
 - Obtain notification and documentation of attacks.
 - Notify the installation of a detected attack via console message or syslogd message.
 - Trace potential attack packets.
 - Request attack statistics on time interval basis
 - Normal or Exception
 - Control action when attack is detected.

Traffic Regulation (TR)

Configurable with the IBM Configuration Assistant GUI.
However, the default IDS policy on the GUI does not include Traffic Regulation policies.
Sample TR Policy is located in the /usr/lpp/tcpip/samples directory:
pagent_IDS.conf



TCP Connection Traffic Regulation



- 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.
- Also known as a "Fair Share 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 (in this example: IP@x), then:
 - If $X+1 < P*A$ then
 - Allow the new connection
 - Else
 - Deny the new connection

011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 22

The algorithm requires the customer to define the total number of connections allowed to a TCP port and a controlling percentage. The percentage is applied against the number of available connections (total allowed minus those already used). When few connections are established, many can come from the same host. When closer to the connection limit, a smaller percentage will be allowed to any one host. In that way, TCP flooding attacks from one host are prevented. Note: QoS policies also allow control over the maximum number of connections to a port. If a QoS policy is in effect that is more generous than the Traffic Regulation Management algorithm, the connection will be allowed.

Fair Share Algorithm Example

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

- 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.
- If the number of connections in use rises 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.

No active connection is dropped. Just new requests may be refused.

TCP Traffic Regulation Details

- Allows control over number of inbound connections from a single host
 - Can be specified for specific application ports
 - Including forking applications
 - Independent policies for multiple applications on the same port
 - ie. 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.
 - Client Concentrator
 - When clients pass through concentrator (web proxy server), all the clients are seen as a single client.
 - Use Port Limit without Individual Limit (Percentage for single client)

011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 24

TR TCP Policy Steps

- Start TCP/IP Stack, PAGENT, and TRMD.
- Create and install TR TCP policy.
 - Specify `ibm-idsTypeActions:STATISTICS`
- View TCP statistics messages.
- Using the statistics, decide upon an optimal policy.
 - Modify the policy to implement a suitable policy with logging.
 - Specify `ibm-idsTypeActions:LOG`
- Test policy over a period of time.
- Run `TRMDSTAT -T` to create a report of the logged messages.
 - For valid traffic - Adjust policy to accept
 - For invalid traffic - Investigate intrusions
- When you feel comfortable with the results, modify the policy to enforce the policy by refusing connections after the limit has been reached.
 - Specify `ibm-idsTypeActions:LIMIT`

011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 25

TCP/IP stack, PAGENT and TRMD active

Implement a TCP IDS policy

- Specify `ibm-idsTypeActions:STATISTICS`

View TCP statistics messages written by TRMD

Run `TRMDSTAT -T -S` for statistics reports

Modify the policy

- Specify `ibm-idsTypeActions:LOG` - Logs exceptions but allows the connection even if the policy thresholds are exceeded.

Conduct network operation for a trial period.

At trial period end run `TRMDSTAT -T`

View TCP SYSLOG messages written by TRMD

Analyze logged events

- Valid traffic - Adjust policy to accept
- Invalid traffic - Investigate intrusions

Change the policy

- Specify `ibm-idsTypeActions:LIMIT` - Denies connections that exceed policy limits and logs the exceptions to syslogd.

UDP Traffic Regulation

- 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 global, applying to 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 supersedes 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

TR UDP Policy Steps

- Start TCP/IP Stack, PAGENT, and TRMD.
- Create and install TR UDP policy.
 - Specify `ibm-idsTypeActions:STATISTICS`
- View UDP statistics messages.
- Using the statistics, decide upon an optimal policy.
 - Modify the policy to implement a suitable policy with logging.
 - Specify `ibm-idsTypeActions:LOG`
 - Specify appropriate `ibm-idsTRudpQueueSize`
- Test policy over a period of time.
- Run `TRMDSTAT -U` to create a report of the logged messages.
- Adjust the policy as necessary
- When you feel comfortable with the results, modify the policy to enforce the policy by refusing connections after the limit has been reached.
 - Specify `ibm-idsTypeActions:LIMIT`

Implementing IDS

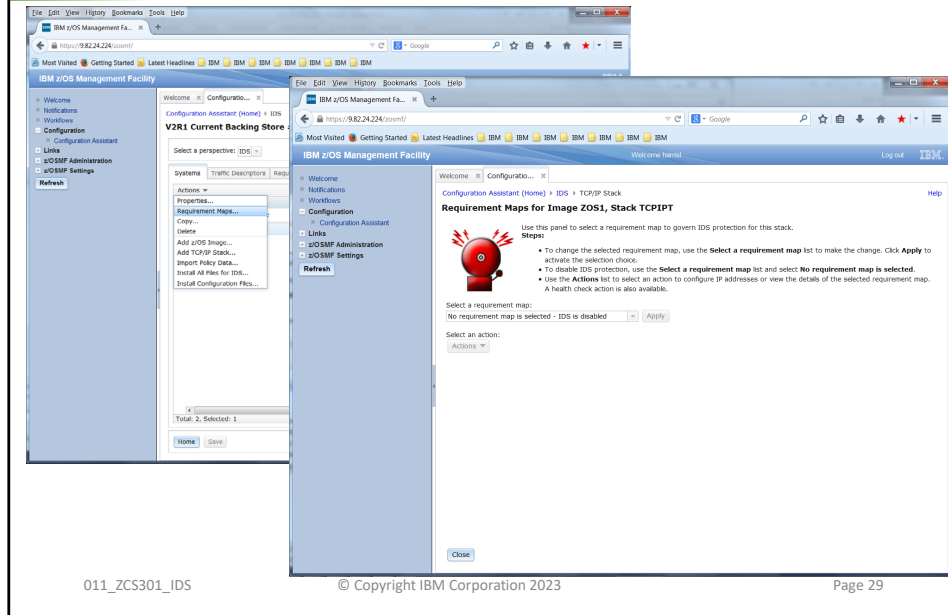


011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 28

IDS in Network Configuration Assistant

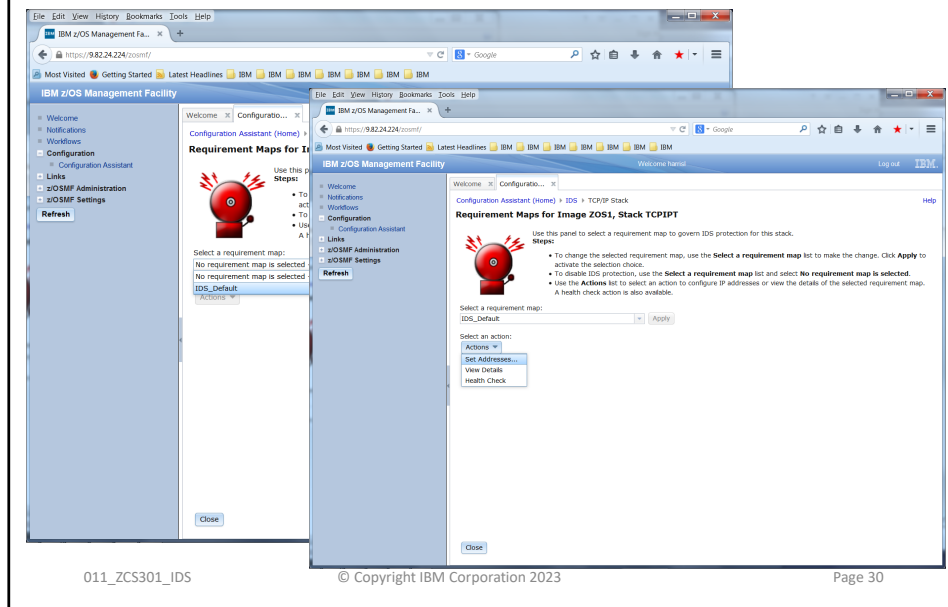


Policy Rules are mapped to Policy Actions.

Both may be defined in either an LDAP server or in a flat file that resides in the unix file system or in MVS.

IDS is the only policy type that may be defined in an LDAP server. However, the LDAP support is out of date and should not be used. The flat file repository is recommended.

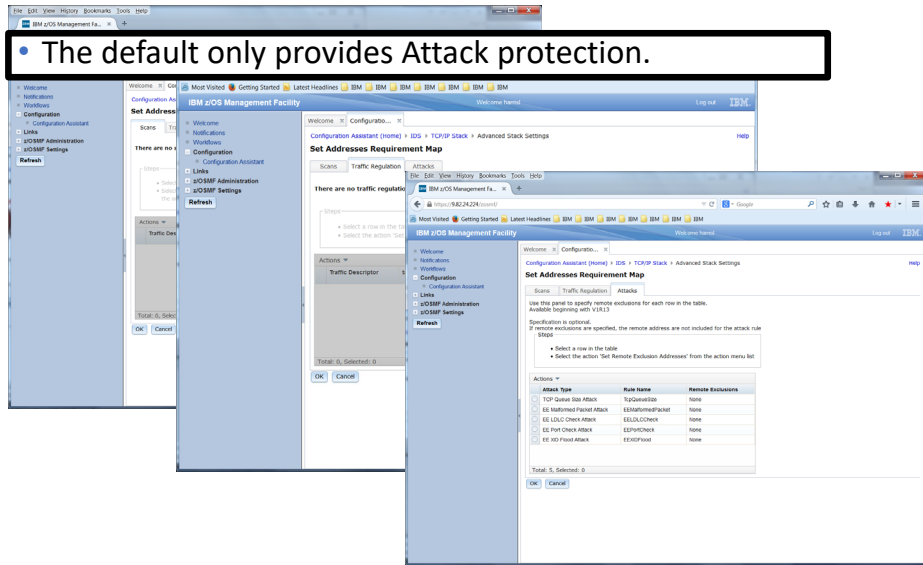
Select Default IDS Policy



“Set Addresses” allows you to specify local addresses that the rule should apply to (ie. which interfaces), and/or remote addresses to exclude from the rule being applied.

Customize IDS Policy

- The default only provides Attack protection.



011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 31

Policy Messages, Logs, and Displays



011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 32

Without TR Policy

- Proclib Unix settings:

BPXPRM00
MAXPROCUSER 200

- When a hacker is attempting connections to the port:

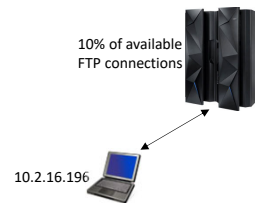
*BPXI040I PROCESS LIMIT MAXPROCUSER HAS REACHED 95% OF ITS CURRENT 708 CAPACITY OF 200 FOR PID=16777525 IN JOB FTPT214 RUNNING IN ADDRESS SPACE 0032

*BPXI040I PROCESS LIMIT MAXPROCUSER HAS REACHED 100% OF ITS CURRENT 709 CAPACITY OF 200 FOR PID=312 IN JOB FTPT215 RUNNING IN ADDRESS SPACE 00F4

- What the hacker sees on his side:

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>ftp 9.82.135.233
Connected to 192.168.135.233.
421 Open rejected due to insufficient resources.
Connection closed by remote host.



Although we have loaded the sample files from the unix sample directory on z/OS, the only TR policies in effect are those that collect statistics about TR activity -- not those that actually limit TR activity.

Thus, essentially with no TR controls in effect, the hacker is allowed to consume all of the available processes allocated to the FTP process. (NOTE: UNIX processes like FTP are not subject to the MAXUSER or ADDRESS SPACE Limitation that can be set in IEASYSxx.) Any user, legitimate or not, receives a message that there are no resources left.

You could modify this MAXPROCUSER value on the fly with a MODIFY OMVS, but the hacker would consume those resources as well. The best way to resolve this is to apply an IDS Traffic Regulation Policy with PAGENT.

With TR Policy – 10% per User

```
EZZ8761I IDS EVENT DETECTED 076
EZZ8762I EVENT TYPE: TCP SOURCE IP CONNECTION LIMIT REACHED
EZZ8763I CORRELATOR 37846 - PROBEID 01004042
EZZ8764I SOURCE IP ADDRESS 10.2.16.196 - PORT 0
EZZ8765I DESTINATION IP ADDRESS 0.0.0.0 - PORT 21
EZZ8766I IDS RULE FTPTR200
EZZ8767I IDS ACTION C200P10
```

10% of available
FTP connections

10.2.16.196

```
EZZ8761I IDS EVENT DETECTED 697
EZZ8762I EVENT TYPE: TCP SOURCE IP CONNECTION LIMIT REACHED
EZZ8763I CORRELATOR 37848 - PROBEID 01004042
EZZ8764I SOURCE IP ADDRESS 10.2.18.192 - PORT 0
EZZ8765I DESTINATION IP ADDRESS 0.0.0.0 - PORT 21
EZZ8766I IDS RULE FTPTR200
EZZ8767I IDS ACTION C200P10
```

10% of available
FTP connections

10.2.18.192

```
Connected to 192.168.135.233. 421
Service not available,
remote server has closed connection
```

011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 34

We have now implemented a TR policy that allows for a maximum of 200 connections on port 21, but note that it allows a single user to consume only 10% of the available connections.

The visual shows you two of the messages received on the z/OS system.

At the bottom of the visual you see the message at the hacker terminal.

This message indicates that the service is not available, very unlike the message when no TR policy is in effect.

Correlator numbers relate to tracing records.

Probeids

```
'03xx'X Scan probeids
'0301'X Scan Very Suspicious
'0302'X Scan Possibly Suspicious
'0303'X Scan Normal
'03010001'X Scan Reserved Port
'03020002'X Scan Unbound Port
'03030003'X Scan QosPolicy Violation
```

Restrictions

```
'03020004'X Scan FW Violation
'03020005'X Scan NOConnFWdeny
'03020006'X Scan BadState
'03010011'X Scan ICMP Broadcast req
'03020012'X Scan ICMP Info req
'03020013'X Scan ICMP Netmask req
'03020014'X Scan ICMP Rec Route opt
'03020015'X Scan ICMP Time Stamp opt
'03020020'X Scan TCP half RST
'03010021'X Scan TCP half TmOut
'03030022'X Scan TCP sequence Window
'03030023'X Scan TCP SA SYN
'03020024'X Scan TCP final TmOut
'03010025'X Scan TCP flag problem
'03020026'X Scan TCP SYN dropped
```

Constrained

```
'03020027'X Scan TCP no peer conn
'03010028'X Scan TCP no Conn Flgs
```

```
'04'X Attack probeids
'0401'X Attack Malformed
'0402'X Attack OutboundRaw
'0403'X Attack IP Fragment
'0404'X Attack ICMP Redirect
'0405'X Attack IP Option Restrictions
'0406'X Attack IP Protocol
```

```
'0407'X Attack Flood
'0408'X Attack Perpetual Echo
```

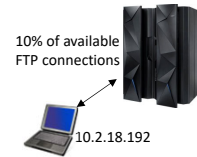
```
'0100'X TR TCP probeids
'0100xx00'X Start or End Constrained
xx identifies subreason
'01004014'X HOST_QOS_EXCP
'01004088'X PORT_ERROR
'01004084'X HOST_ERROR
'01004048'X MAX_APPL
'01004044'X MAX_HOST
'01004042'X MAX_QOS_HOST
```

```
'0200'X TR UDP probeids
'02000001'X Start or End
```

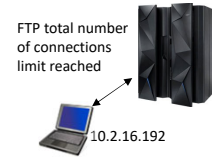
With TR Policy

CNZ3011I JOBNAME= TCPT21 JOBID= STC04051 ASID= 0032 HAS REACHED 50% OF THE WTO BUFFER LIMIT

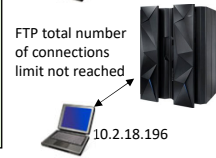
```
EZZ8761I IDS EVENT DETECTED 364
EZZ8762I EVENT TYPE: TCP SOURCE IP CONNECTION LIMIT REACHED
EZZ8763I CORRELATOR 152 - PROBEID 01004044
EZZ8764I SOURCE IP ADDRESS 10.2.18.192 - PORT 0
EZZ8765I DESTINATION IP ADDRESS 0.0.0.0 - PORT 23
EZZ8766I IDS RULE TN3270TR
EZZ8767I IDS ACTION C20P10
```



```
EZZ8761I IDS EVENT DETECTED 366
EZZ8762I EVENT TYPE: TCP PORT CONSTRAINED
EZZ8763I CORRELATOR 153 - PROBEID 01004400
EZZ8764I SOURCE IP ADDRESS 10.2.18.192 - PORT 0
EZZ8765I DESTINATION IP ADDRESS 0.0.0.0 - PORT 23
EZZ8766I IDS RULE TN3270TR
EZZ8767I IDS ACTION C20P10
```



```
EZZ8761I IDS EVENT DETECTED 365
EZZ8762I EVENT TYPE: TCP PORT UNCONSTRAINED
EZZ8763I CORRELATOR 150 - PROBEID 01002400
EZZ8764I SOURCE IP ADDRESS 10.2.16.196 - PORT 0
EZZ8765I DESTINATION IP ADDRESS 0.0.0.0 - PORT 23
EZZ8766I IDS RULE TN3270TR
EZZ8767I IDS ACTION C20P10
```



011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 35

TR generates messages to the console and will consume WTO buffers; make sure that you monitor WTO usage and adjust if necessary. TR TCP generates a Constrained Event when a port reaches about 90% of its Connection Limit. An Unconstrained Event is generated when the port falls below about 88% of its limit. An IDS correlator is assigned for the duration of each constrained state. If tracing is requested in the policy, the first 100 packets that exceed the limit in each constrained state are traced along with the correlator. TR TCP also generates events for each connection allowed because of a QoS override policy and for each connection denied for exceeding either the application's connection limit or the percent available limit.

SYNFLOOD LDAP, FTP, TN3270, Unix Telnet

EZZ8761I IDS EVENT DETECTED 176
EZZ8762I EVENT TYPE: ACCEPT QUEUE EXPANDED
EZZ8763I CORRELATOR 2 - PROBEID 04070008
EZZ8765I DESTINATION IP ADDRESS 0.0.0.0 - PORT 389
EZZ8766I IDS RULE AttackFlood-rule
EZZ8767I IDS ACTION AttackLog-action
EZZ4350I AN EXCESSIVE NUMBER OF HALF-OPEN CONNECTIONS ARE QUEUED FOR LISTENING PORT: 389

Attack on LDAP
389

EZZ8761I IDS EVENT DETECTED 178
EZZ8762I EVENT TYPE: SYN FLOOD STARTED
EZZ8763I CORRELATOR 3 - PROBEID 04070009
EZZ8765I DESTINATION IP ADDRESS 0.0.0.0 - PORT 389
EZZ8766I IDS RULE AttackFlood-rule
EZZ8767I IDS ACTION AttackLog-action

EZZ4350I AN EXCESSIVE NUMBER OF HALF-OPEN CONNECTIONS ARE QUEUED FOR LISTENING PORT: 21
EZZ4350I AN EXCESSIVE NUMBER OF HALF-OPEN CONNECTIONS ARE QUEUED FOR LISTENING PORT: 23
EZZ4350I AN EXCESSIVE NUMBER OF HALF-OPEN CONNECTIONS ARE QUEUED FOR LISTENING PORT: 2023

Attack on
FTP 21,
TN3270 23,
Unix Telnet
2023

EZZ8761I IDS EVENT DETECTED 611
EZZ8762I EVENT TYPE: SYN FLOOD STARTED
EZZ8763I CORRELATOR 19868 - PROBEID 04070009
EZZ8765I DESTINATION IP ADDRESS 0.0.0.0 - PORT 2023
EZZ8766I IDS RULE AttackFlood-rule
EZZ8767I IDS ACTION AttackLog-action

Policy was changed to notify CONSOLE and also to continue logging.

NOTE: IDS implements "Message Flooding Protection" for ATTACKS via the keyword "ibm-idsMaxEventMessage".

In addition, only 100 messages per attack category are logged within a five-minute period.

SYNFLOOD

EZZ4350I AN EXCESSIVE NUMBER OF HALF-OPEN CONNECTIONS ARE QUEUED FOR LISTENING PORT: 10007

EZZ8761I IDS EVENT DETECTED 823
EZZ8762I EVENT TYPE: SYN FLOOD STARTED
EZZ8763I CORRELATOR 21322 - PROBEID 04070009
EZZ8765I DESTINATION IP ADDRESS 0.0.0.0 - PORT 10007
EZZ8766I IDS RULE AttackFlood-rule
EZZ8767I IDS ACTION AttackLog-action

Message Flooding
Protection

IVT5562I CSM ECSA STORAGE AT CRITICAL LEVEL
IVT5564I CSM ECSA STORAGE SHORTAGE RELIEVED
IVT5563I CSM FIXED STORAGE AT CRITICAL LEVEL
EZZ7840I SENDTO() ERROR, ERRNO=1122:EDC8122I NO BUFFER SPACE AVAILABLE.,
ERRNO2=74420324
EZZ7921I OSPF ADJACENCY FAILURE, NEIGHBOR 172.17.0.12, OLD STATE 128 222,
NEW STATE 1, EVENT 12

CSM Storage Shortage
Relieved

IVT5562I CSM ECSA STORAGE AT CRITICAL LEVEL
IVT5564I CSM ECSA STORAGE SHORTAGE RELIEVED

IVT5563I CSM FIXED STORAGE AT CRITICAL LEVEL
IVT5565I CSM FIXED STORAGE SHORTAGE RELIEVED

011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 37

ibm-idsMaxEventMessage attribute specifies the maximum number of event messages to be displayed on the console during a 5 minute period for an IDS attack type (e.g. MALFORMED_PACKET). The format of this attribute is as follows: ibm-idsMaxEventMessage:<an integer number> . The default is 0, meaning that there is no maximum number of messages.

- To prevent flooding SYSLOGD with messages, an additional control is in place that only permits a maximum of 100 messages per attack category in in any five-minute period.

For the "CSM ECSA CRITICAL" message, TCPIP will detect that ECSA has gone critical, and will attempt to release any CSM storage that we may currently have cached but are not using. TCPIP caches CSM in the hopes that a near-term request for CSM can be satisfied by cache rather than going to CSM Services. After a certain time period, we will release the CSM storage if it has not been referenced in this time period. When CSM is critical, we release all of our cached storage immediately, rather than waiting the time period, thus you would normally see the "CSM SHORTAGE RELIEVED" message after we are done freeing our cached data.

For the "CSM FIXED CRITICAL" message, CSM Services detects this and will attempt to page free any fixed ECSA that was marked as "page-eligible". An example of when storage is marked "page-eligible" is when TCPIP transmits data for a TCP connection. The storage for the data packet needs to be fixed as it is used for I/O out the interface. TCP holds a copy of the packet in case we need to retransmit it. During this time (waiting for a SYN or retransmit timeout), we mark it page-eligible and if we need to retransmit, we fix it first. So, if there is enough of this "page-eligible" CSM lying around, CSM Services can pagefree it and you would see the "CSM SHORTAGE RELIEVED" message.


But what happened to OSPF? Well, we used the approach of giving it a high WLM service level, but it still got swapped out! You can make OMPROute non-swappable.

SYNFLOOD FOR TN3270

```

D TCPIP,,T,CONN
EZZ6064I TELNET CONNECTION DISPLAY 363
EN
CONN      TY  IPADDR..PORT      LUNAME  APPLID  TSP  LOGMODE
-----
000175EC   10.2.16.196..60382          ?N?
000175E9   10.2.16.196..60381          ?N?
000175E6   10.2.16.196..60380          ?N?
00017341   10.54.137.95..3351    TCPT2111  TPE
0001731F   10.54.137.95..3350    TCPT2110  TPE
00017305   10.54.137.95..3349    TCPT2109  TPE
000172E2   10.54.137.95..3348    TCPT2108  TPE
000172A6   10.54.137.95..3345    TCPT2107  TPE
0001726B   10.2.18.36..47233          ?N?
00017269   10.2.18.36..47232          ?N?
00017267   10.2.18.36..47231          ?N?
00017265   10.2.18.36..47230          ?N?
00017263   10.2.18.36..47229          ?N?
00017261   10.2.18.36..47228          ?N?
0001725F   10.2.18.36..47227          ?N?
0001725D   10.2.18.36..47226          ?N?
0001725B   10.2.18.36..47225          ?N?
00017259   10.2.18.36..47224          ?N?
----- PORT:      23      ACTIVE          PROF: CURR CONNS:      18
  
```

Session State = N
for negotiating



You notice from the column about Type (TP), Status (ST), and Protocol (PR) that the Telnet connections never went anywhere -- observe the question marks.

SYNFLOOD Ended Message Sent to Console

```
EZZ8761I IDS EVENT DETECTED 078
EZZ8762I EVENT TYPE: SYN FLOOD ENDED
EZZ8763I CORRELATOR 23800 - PROBEID 04070006
EZZ8765I DESTINATION IP ADDRESS 0.0.0.0 - PORT 10007
EZZ8766I IDS RULE AttackFlood-rule
EZZ8767I IDS ACTION AttackLog-action

EZZ8761I IDS EVENT DETECTED 079
EZZ8762I EVENT TYPE: SYN FLOOD ENDED
EZZ8763I CORRELATOR 24258 - PROBEID 04070006
EZZ8765I DESTINATION IP ADDRESS 0.0.0.0 - PORT 21
EZZ8766I IDS RULE AttackFlood-rule
EZZ8767I IDS ACTION AttackLog-action
```

If you are sending notification to the console, you receive a message that tells you the SYNFLOOD ended.

Display that Show SYNFLOOD

```

D TCPIP, ,N,IDS
EZZ2500I NETSTAT CS VIR4 TCPT21 335
INTRUSION DETECTION SERVICES SUMMARY:
RESTRICTED IP OPTIONS
  RESTRICTED IP OPTIONS
    PLCRULENAME: ATTACKIPOPT-RULE
    TOTDETECTED: 10396      DETCURRPLC: 0
    DETCURRINT: 0          INTERVAL: 10
  ICMP REDIRECT RESTRICTIONS
    PLCRULENAME: ATTACKICMPREDIRECT-RULE
    TOTDETECTED: 4         DETCURRPLC: 4
    DETCURRINT: 0          INTERVAL: 60
  FLOODS
    PLCRULENAME: ATTACKFLOOD-RULE
    TOTDETECTED: 2         DETCURRPLC: 2
    DETCURRINT: 2          INTERVAL: 20
  TRAFFIC REGULATION:
    TCP
      CONNREJECTED: 12718    PLCACTIVE: Y
    UDP
      PCKDISCARDED: 0        PLCACTIVE: Y
  INTRUSION DETECTION SERVICES TCP PORT LIST:
  TCPLISTENINGSOCKET: 0.0.0.0..23
  SCSTAT: S  SCRULENAME: SCANEVENTLOW-RULE
  TRSTAT: S  TRRULENAME: TN3270TR
  TRPORTINST: Y  TRCORR: 0      MXAPP: 0      MXHST: 0
  SYNFLOOD: Y
  TCPLISTENINGSOCKET: 0.0.0.0..2023
  SCSTAT: S  SCRULENAME: *NONE*
  TRSTAT: S  TRRULENAME: OTELNETTR
  TRPORTINST: Y  TRCORR: 0      MXAPP: 0      MXHST: 0
  SYNFLOOD: Y
011_ZCS301_IDS

```

© Copyright IBM Corporation 2023

Page 40

For Scan Detection:

- GlobRuleName The Global Scan rule name or *NONE* if scan detection is not active.
- IcmpRuleName The Scan ICMP rule name or *NONE* if ICMP scan event policy is not active.
- TotDetected The number of scans detected since the TCP stack was started.
- DetCurrPlc The number of scans detected since the last Scan Global policy change.
- DetCurrInt The number of scans detected in the current scan interval.
- Interval The length of the internal scan interval used to detect scans. This value is either 30 seconds or 60 seconds depending on the fast scan interval specified in the policy.
- SrcIPsTrkd The number of source IP addresses currently being monitored by scan detection.
- StrgLev The amount of private storage, in megabytes, that scan detection is using. This value is calculated at each internal interval. If 0 is shown, this indicates that no storage is currently in use for scan detection. 0M indicates that less than 1 MB of storage is in use.

For Attack Detection:

- PlcRuleName The attack rule name or *NONE* if no policy is active for the attack type.
- TotDetected The number of attacks detected since the TCP stack was started.
- DetCurrPlc The number of attacks detected since the last policy change.
- DetCurrInt The number of attacks detected in the current statistics interval. If statistics or exceptstats is not specified in the policy, this field is 0.
- Interval The current statistics interval or 0 if statistics or exceptstats is not specified in the policy.

For Traffic Regulation:

- ConnRejected The number of TCP connections rejected by Traffic Regulation since the TCPIP stack was started.
- PckDiscarded The number of UDP packets discarded by Traffic Regulation since the TCPIP stack was started.
- PlcActive
- Y Indicates that TR policy is active for at least one port in the respective protocol.
- N Indicates that Traffic Regulation is not active for any ports in the respective protocol.

Display that Shows Related Problems

```
D TCPIP,,N,STATS
EZZ2500I NETSTAT CS V1R4 TCPT21 313
IP STATISTICS
  PACKETS RECEIVED                = 3957845
  INBOUND CALLS FROM DEVICE LAYER = 3382749
  INBOUND FRAME UNPACKING ERRORS  = 177
  INBOUND DISCARDS MEMORY SHORTAGE = 1745431
  RECEIVED HEADER ERRORS          = 18656
  RECEIVED ADDRESS ERRORS         = 3629
  DATAGRAMS FORWARDED             = 0
  UNKNOWN PROTOCOLS RECEIVED      = 0
  RECEIVED PACKETS DISCARDED       = 3633
  RECEIVED PACKETS DELIVERED       = 3939930
  OUTPUT REQUESTS                 = 6651958
...
ICMP STATISTICS
      RECEIVED      SENT
      -----      -
MESSAGES      389010      349280
  ERRORS      29597       1432
  DESTINATION UNREACHABLE 20157       1438
  TIME EXCEEDED          3298         0
  PARAMETER PROBLEMS      0        18543
  SOURCE QUENCHS          0         0
  REDIRECTS               0         0
  ECHOS                   330685       5
  ECHO REPLIES            22315      329294
...
```

Notification Set to Console

- Consider changing MaxEventMessage for Attack Policy (Default is 5).
- Additional Control for SYSLOGD: 100 msg. per 5 minutes

```
EZZ8761I IDS EVENT DETECTED 355
EZZ8762I EVENT TYPE: SUSPICIOUS PACKET RECEIVED
EZZ8763I CORRELATOR 2 - PROBEID 04020001
EZZ8764I SOURCE IP ADDRESS 172.17.0.121 - PORT 0
EZZ8765I DESTINATION IP ADDRESS 224.0.0.5 - PORT 0
EZZ8766I IDS RULE AttackOutboundRaw-rule
EZZ8767I IDS ACTION AttackLimit-action

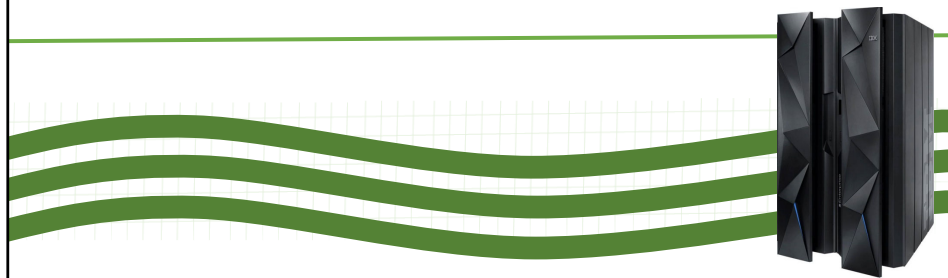
EZZ8761I IDS EVENT DETECTED 356
EZZ8762I EVENT TYPE: SUSPICIOUS PACKET RECEIVED
EZZ8763I CORRELATOR 37797 - PROBEID 04060001
EZZ8764I SOURCE IP ADDRESS 172.17.0.12 - PORT 0
EZZ8765I DESTINATION IP ADDRESS 172.17.0.121 - PORT 0
EZZ8766I IDS RULE AttackIPprot-rule
EZZ8767I IDS ACTION AttackLimit-action
```

This is a reminder that Attack policies enjoy Message Flooding protection.

ibm-idsMaxEventMessage attribute specifies the maximum number of event messages to be displayed on the console during a 5 minute period for an IDS attack type (e.g. MALFORMED_PACKET). The format of this attribute is as follows: ibm-idsMaxEventMessage:<an integer number>. The default is 0, meaning that there is no maximum number of messages.

To prevent flooding SYSLOGD with messages, an additional control is in place that only permits a maximum of 100 messages per attack category in in any five-minute period.

trmdstat Reports

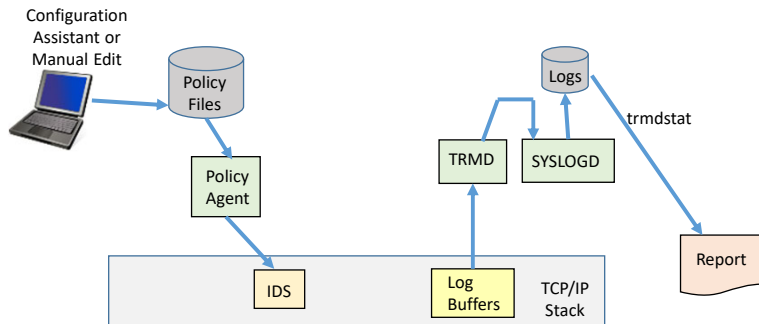


011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 43

trmdstat Command



- Create reports from IDS syslogd data.

011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 44

Traffic regulation policies are configured for the policy agent. The policy agent is responsible for reading configured policies and storing them into the stack.

TCP flooding attacks are very prevalent on the Internet. It is sometimes impossible to tell the difference between an attack and legitimate heavy traffic. There is no effective way to prevent them.

Traffic Regulation and Management Policy

- Control Over Number Of Inbound Connections from a single host
- Can Be Specified For Specific Application Ports

Possible Actions

- Collect Statistics For Tuning Purposes
- Log Limit Violation
- Deny New Connections Over Limit

Connection limit expressed as

- Port Limit
 - Total number for all connecting hosts
 - Available Connection Total = Total Connection Allowed - Total Connections Active
- Individual limit for a single host
 - Connection within individual limit if single host connection total + new connection request \leq specified percentage of available connection total

The stack enforces the configured policies.

- It determines whether a TR policy applies to a particular TCP port.
- It tracks the number of available connections to the port and calculates the number of connections allowed to a host at that time.
- It tracks the number of connections held by a particular host.
- It gathers statistical data and log data.

Traffic Regulation Management Daemon (trmd) communicates with the policy agent and the stack to retrieve statistics about the configured policies. It writes out logging and statistics messages to the syslog daemon.

The trmdstat command reads the records from the syslog daemon and generates reports on number of connections received, number of connections refused, etc.

The TCP/IP stack itself provides a mechanism to control true SYN Floods, which are TCP connections that have not completed the 3-way handshake of (SYN, ACK/SYN,ACK).

SYN Flood Protections: After there are 758 partially completed connections (SYN, followed by ACK/SYN), TCP/IP starts randomly discarding open connections for every newly arrived SYN. The stack chooses which to discard from among the oldest open connections.

Summary Report

```
trmdstat -I /tmp/dablog.log
trmdstat for z/OS CS V1R2          Wed Jan 31 15:51:45 2001

Log Time Interval   : Jan  9 12:16:24 - Jan  9 12:20:54
Stack Time Interval : Jan  9 16:09:06 - Jan  9 17:20:36
TRM Records Scanned : 3307
Port Range         : ALL

Traffic Regulation - TCP
-----
Connections would have been refused :    0
Connections refused                  :    0
Constrained entry logged             :    0
Constrained exit logged              :    0
Constrained entry                    :    1
Constrained exit                     :    1
QOS exceptions logged                 :    0
QOS exceptions made                   :    0

Traffic Regulation - UDP
-----
Constrained entry logged             :    0
Constrained exit logged              :    0
Constrained entry                    :    0
Constrained exit                     :    0

SCAN Detection
-----
Threshold exceeded                   :    0
Detection delayed                    :    0
Storage constrained entry            :    0
Storage constrained exit             :    0

ATTACK Detection
-----
Packet would have been discarded     :    0
Packet discarded                     :   593
Accept queue expanded                :    0

FLOOD Detection
-----
SYN Flood start                      :    0
SYN Flood end                        :    0

440 ATTACK messages lost at 01/09/2001 16:08:26.49

TRMD Started      : Jan  9 10:53:42
TRMD Ended        : Jan  9 11:05:14
TRMD Started      : Jan  9 12:16:22
```

011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 45

Connections would have been refused - Indicates the number of connections that would have been refused if "TypeActions Limit" had been specified. This count indicates the total number of EZZ9319I messages present in the log.

Connections refused - Indicates the number of connections refused by the system. This count indicates the total number of EZZ8499I messages present in the log.

Constrained entry logged - Indicates the number of times the system would have entered into a constrained state. This count indicates the total number of EZZ9320I messages present in the log.

Constrained exit logged - Indicates the number of times the system would have exited a constrained state. This count indicates the total number of EZZ9322I messages present in the log.

Constrained entry - Indicates the number of times the system entered into a constrained state. This count indicates the total number of EZZ9321I messages present in the log.

Constrained exit - Indicates the number of times the system exited a constrained state. This count indicates the total number of EZZ9323I messages present in the log.

QOS exceptions logged - Indicates the number of times a QOS exception was logged. If "TypeActions Limit" had been specified in the TR policy, the connection would have been refused by the percentage limit if the higher QoS limit for this source IP to this port didn't exist. This count indicates the total number of EZZ9318I messages present in the log.

QOS exceptions made - Indicates the number of times a QOS exception was made. This count indicates the total number of EZZ9317I messages present in the log.

SCAN Threshold exceeded - Indicates the number of times the SCAN policy threshold was exceeded by fast or slow scans. This count indicates the total number of EZZ8643I messages present in the log.

SCAN Detection delayed - Indicates the number of times the SCAN interval processing took more than an interval to complete. This count indicates the total number of EZZ8645I messages present in the log.

SCAN Storage Constrained Entry - Indicates the number of times the storage required to track either a source IP addr or a scan event could not be obtained. This count indicates the total number of EZZ8646I messages present in the log.

SCAN Storage Constrained Exit - Indicates the number of times SCAN storage allocation constraints ended. This count indicates the total number of EZZ8647I messages present in the log.

ATTACK Packet would have been discarded - Indicates the number of times a packet would have been discarded if "TypeActions Limit" had been specified. This count indicates the total number of EZZ8649I messages present in the log.

ATTACK Packet discarded - Indicates the number of times a packet was discarded. This count indicates the total number of EZZ8648I messages present in the log.

ATTACK Accept queue expanded - Indicates the number of times accept queue expansion has occurred. This count indicates the total number of EZZ8648I messages present in the log.

FLOOD SYN Flood start - Indicates the number of times the server has come under SYN flood attack. This count indicates the total number of EZZ8650I messages present in the log.

FLOOD SYN Flood end - Indicates the number of times a SYN flood attack has ended. This count indicates the total number of EZZ8651I messages present in the log.

Flood Summary Report

```
trmdstat -F /tmp/tstlog.log
trmdstat for z/OS CS VIR2          Wed Nov  8 09:59:32 2000
Log Time Interval      : Aug 21 08:32:09 - Aug 21 10:32:09
Stack Time Interval    : Aug 21 14:31:09 - Aug 21 14:32:09
TRM Records Scanned    : 71
Port Range              : ALL
```

FLOOD Summary

IP Address	Port	SYN Flood Start	SYN Flood End	SYN Flood Duration
11.12.13.14	11000	2	2	80
61.62.63.64	12000	2	2	120
61.62.63.64	14000	1	1	120

TRMD Started : Aug 21 10:32:09

This report will be displayed when the -F option is specified with the trmdstat command. It will display the summary of all flood events.

IP Address: Indicates the bound IP address of the flood.

Port: Indicates the bound port number.

SYN Flood Start: Indicates the number of SYN flood starts.

SYN Flood End: Indicates the number of SYN flood ends.

SYN Flood Duration: Indicates the duration of SYN Flood in seconds.

Flood Detail Report

```
trmdstat -F -D /tmp/tstlog.log
trmdstat for z/OS CS V1R2                Wed Nov  8 10:00:37 2000

Log Time Interval      : Aug 21 08:32:09 - Aug 21 10:32:09
Stack Time Interval    : Aug 21 14:31:09 - Aug 21 14:32:09
TRM Records Scanned    : 71
Port Range             : ALL

                                FLOOD Events

  Date and Time      IP Address      Port  Type  Duration  Correlator
-----
8/21/2000 14:31:9.53 11.12.13.14 11000  E      40      87591
8/21/2000 14:31:9.53 11.12.13.14 11000  E      40      87704
8/21/2000 14:32:9.53 11.12.13.14 11000  X      40      87893
8/21/2000 14:32:9.53 11.12.13.14 11000  X      40      87997
8/21/2000 14:32:9.53 61.62.63.64 12000  X      60      87999

TRMD Started          : Aug 21 10:32:09
```

This report will be displayed when the -F and -D options are specified with the trmdstat command. It will display the contents of flood event records.

Date and Time: Indicates the date and time contained in the flood record.

IP Address: Indicates the bound IP address of the flood.

Port: Indicates the bound port number.

Type: Indicates the SYN Flood record type - 'E' for enter SYN Flood and 'X' for exit.

Duration: Indicates the SYN Flood duration in seconds.

Correlator: Indicates the trace correlator.

Attack Summary Report

<pre> trmdstat -A /tmp/tstlog.log trmdstat for z/OS CS V1R2 Wed Nov 8 10:14:11 2000 Log Time Interval : Aug 21 08:32:09 - Aug 21 10:32:09 Stack Time Interval : Aug 21 14:32:09 - Aug 21 14:32:09 TRM Records Scanned : 71 Port Range : ALL ATTACK Summary Datagrams Discarded Source: 31.32.33.34 Destination: 51.52.53.54 Attacks </pre>									
Dst	Port	Malf	ORaw	IPFr	ICMP	IPop	Prto	Perp	NoId
13001		1	0	0	0	0	0	0	0
14001		0	0	0	0	0	0	1	0
<pre> Datagrams would have been Discarded Source: 61.62.63.64 Destination: 31.32.33.34 Attacks </pre>									
Dst	Port	Malf	ORaw	IPFr	ICMP	IPop	Prto	Perp	NoId
12001		0	2	0	0	0	0	0	0
<pre> TRMD Started : Aug 21 10:32:09 </pre>									

This report will be displayed when the -A option is specified with the trmdstat command.

It will display the summary of all attack events.

Source: Indicates the IP address of the source host.

Destination: Indicates the IP address of the destination host.

Port: Indicates the port number.

Half: Indicates the number of datagrams discarded or would have been discarded if "TypeActions Limit" had been specified in the policy due to Malformed Packet attacks.

ORaw: Indicates the number of datagrams discarded or would have been discarded if "TypeActions Limit" had been specified in the policy due to OutBound Raw attacks.

IPFr: Indicates the number of datagrams discarded or would have been discarded if "TypeActions Limit" had been specified in the policy due to Fragmented Packet attacks.

ICMP: Indicates the number of datagrams discarded or would have been discarded if "TypeActions Limit" had been specified in the policy due to ICMP attacks.

IPop: Indicates the number of datagrams discarded or would have been discarded if "TypeActions Limit" had been specified in the policy due to IP Options attacks.

Prto: Indicates the number of datagrams discarded or would have been discarded if "TypeActions Limit" had been specified in the policy due to IP Protocol error attacks.

Perp: Indicates the number of datagrams discarded or would have been discarded if "TypeActions Limit" had been specified in the policy due to Perpetual Echo attacks.

Noid: Indicates the number of datagrams discarded or would have been discarded if "TypeActions Limit" had been specified in the policy due to unidentified attacks.

Attack Detail Report

```
trmdstat -A -D /tmp/tstlog.log
trmdstat for z/OS CS V1R2      Wed Nov  8 09:55:36 2000

Log Time Interval   : Aug 21 08:32:09 - Aug 21 10:32:09
Stack Time Interval : Aug 21 14:32:09 - Aug 21 14:32:09
TRM Records Scanned : 71
Port Range          : ALL

ATTACK Events
Packets Discarded
Attack Date and Time  Dst IpAddr  Src IpAddr  Dst Port  Src Port  Correlator  ProbeID
-----
Malf 8/21/2000 14:32:9.53 51.52.53.54 41.42.43.44 0          0          82334 04010009
IPFr 8/21/2000 14:32:9.53 51.52.53.54 41.42.43.44 0          0          82336 04030001
IPOp 8/21/2000 14:32:9.53 51.52.53.54 41.42.43.44 0          0          82338 04050001
PRTO 8/21/2000 14:32:9.53 51.52.53.54 41.42.43.44 0          0          82339 04060001
Perp 8/21/2000 14:32:9.53 51.52.53.54 41.42.43.44 13001      10001      82342 04080001
ICMP 8/21/2000 14:32:9.53 51.52.53.54 41.42.43.44 12001      10001      82337 04040009
Packets would have been Discarded
Attack Date and Time  Dst IpAddr  Src IpAddr  Dst Port  Src Port  Correlator  ProbeID
-----
ORAW 8/21/2000 14:32:9.54 41.42.43.44 71.72.73.74 0          0          87999 04020001
TRMD Started          : Aug 21 10:32:09
```

011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 49

This report will be displayed when the -A and -D options are specified on the trmdstat command.

It will display the contents of attack event records.

Attack: Indicates the ATTACK type causing the packet to be discarded or would have been discarded if "TypeActions Limit" had been specified in the policy:

- Malf - Malformed Packet
- ORaw - OutBound Raw
- IPFr - IP Fragment
- ICMP - ICMP
- IPOP - IP Options
- PRTO - IP Protocol error
- Flod - Flood
- NoID - Not identified

Date and Time: Indicates the date and time contained in the record written at the time of the attack.

Dst IpAddr: Indicates the destination IP address of the attack.

Src IpAddr: Indicates the source IP address of the attack.

Dst Port: Indicates the destination port number.

Src Port: Indicates the source port number.

Correlator: Indicates the trace correlator.

ProbeID: Indicates the probe ID.

Attack Statistics Report

```
trmdstat -A -S /tmp/statlog.log
trmdstat for z/OS CS V1R2      Tue Jan 16 13:13:30 2001
```

Log Time Interval	: Jan 9 10:54:15 - Jan 9 10:54:16
Stack Time Interval	: Jan 9 15:42:53 - Jan 9 15:45:58
TRM Records Scanned	: 27
Port Range	: ALL

ATTACK Statistics			
Attack	Date and Time	Attacks	Action
Malf	01/09/2001 15:42:53.20	11111	LIMIT
IPFr	01/09/2001 15:42:53.20	22222	LIMIT
ORAW	01/09/2001 15:43:54.84	33333	LIMIT
PRT0	01/09/2001 15:43:54.84	44444	LIMIT
ICMP	01/09/2001 15:44:56.52	55555	LIMIT
IPOP	01/09/2001 15:44:56.52	66666	NOLIMIT
Perp	01/09/2001 15:45:58.17	77777	NOLIMIT
Flod	01/09/2001 15:45:58.18	88888	LIMIT


```
TRMD Started      : Jan 9 10:53:42
```

This report will be displayed when the -A and -S options are specified on the trmdstat command. It will display the contents of attack statistics records (including Flood statistics).

Attack: Indicates the ATTACK type causing the packet to be discarded if the statistics record indicates LIMIT or would have been discarded if the statistics record indicates NOLIMIT.

- Malf - Malformed Packet
- ORaw - OutBound Raw
- IPFr - IP Fragment
- ICMP - ICMP
- IPOP - IP Options
- PRT0 - IP Protocol error
- Flod - Flood
- NoID - Not identified

Date and Time: Indicates the date and time at which the statistics information was collected by the TCP/IP stack.

Attacks: Indicates the number of attacks recorded.

Action: Indicates the action specified on the policy ibm-idsTypeActions statement.

- 'LIMIT' indicates LIMIT was specified.
- 'NOLIMIT' indicates no ibm-idsTypeActions LIMIT was specified.

Scan Summary Report

trmdstat -N /tmp/tstlog.log					
trmdstat for z/OS CS VIR2					
Wed Nov 8 09:06:56 2000					
Log Time Interval	:	Aug 21 08:32:09	-	Aug 21 10:32:09	
Stack Time Interval	:	Aug 21 14:32:09	-	Aug 21 14:32:09	
TRM Records Scanned	:	71			
Port Range	:	ALL			
SCAN TR Summary					
IP Address	Scans		Suspicion Level		
	Fast	Slow	Very	Possibly	Normal
11.12.13.14	2	2	20	20	20
22.33.44.55	2	0	200	400	600
TRMD Started : Aug 21 10:32:09					

- Exclude legitimate network management sources.
- Correlate with Access Control violations and Investigate unusual behavior:
- majority of losses reported to FBI are caused by current or recent employees
 - break-in attempts, successful or not, often are followed by denial of service attacks
- This report will be displayed when the -N option is specified on the trmdstat command. It will display the summary of scan events.
- IP Address - Indicates the source IP address causing the SCAN detection.
- Scans - Fast
- Indicates the number of fast scans detected.
- Scans - Slow
- Indicates the number of slow scans detected.
- Suspicion Levels:
- Very -Indicates the number of very suspicious unique events included in the scans
 - Possibly - Indicates the number of possibly suspicious events included.
 - Normal -Indicates the number of normal events included.

Scan Detail Report

trmdstat -N -D /tmp/tstlog.log						
trmdstat for z/OS CS V1R2						
Wed Nov 8 09:08:54 2000						
Log Time Interval : Aug 21 08:32:09 - Aug 21 10:32:09						
Stack Time Interval : Aug 21 14:32:09 - Aug 21 14:32:09						
TRM Records Scanned : 71						
Port Range : ALL						
Date and Time	IP Address	SCAN TR Events	Suspicion Level			Type Correlator
			Very	Possibly	Normal	
8/21/2000 14:32:9.53	11.12.13.14	5	5	5	5	S 47113
8/21/2000 14:32:9.53	11.12.13.14	5	5	5	5	S 47212
8/21/2000 14:32:9.53	11.12.13.14	5	5	5	5	F 57287
8/21/2000 14:32:9.53	11.12.13.14	5	5	5	5	F 67333
8/21/2000 14:32:9.54	22.33.44.55	100	200	300	300	F 87433
8/21/2000 14:32:9.54	22.33.44.55	100	200	300	300	F 97500
TRMD Started : Aug 21 10:32:09						

This report will be displayed when the -N and -D options are specified trmdstat command. It will display the contents of individual scan event records.

Date and Time - Indicates the date and time the stack detected the scan.

IP Address - Indicates the source IP address triggering the scan.

Suspicion Levels:

- Very -Indicates the number of very suspicious unique events included in the scan.
- Possibly - Indicates the number of possibly suspicious events included.
- Normal -Indicates the number of normal events included.

Type - Indicates the type of scan detected - 'F' indicates a fast scan, 'S' indicates a slow scan.

Correlator - Indicates the trace correlator.

If SYSLOGDETAIL notification was specified in policy, the syslogd EZZ8644I message will also indicate the destination ports accessed. The correlator shown in the report above can be used to find the matching EZZ8644I message.

TR UDP Summary Report

trmdstat -U /tmp/tstlog.log						
trmdstat for z/OS CS V1R2						
Wed Nov 8 09:00:20 2000						
Log Time Interval : Aug 21 08:32:09 - Aug 21 10:32:09						
Stack Time Interval : Aug 21 14:32:09 - Aug 21 16:33:09						
TRM Records Scanned : 71						
Port Range : ALL						
UDP TR Summary						
Constrained State						
IP Address	Port	Entered	Exited	Duration	Datagrams Discarded	
05.16.17.18	2001	1	1	100	155	
05.16.17.18	5001	2	2	200	310	
Constrained State						
IP Address	Port	Entered	Exited	Duration	Datagrams Would have been Discarded	
05.16.17.18	1001	1	1	100	155	
05.16.17.18	2001	2	2	200	310	
TRMD Started : Aug 21 10:32:09						

Summary of UDP constrained state and datagram discard information.

This report will be displayed when the -U option is specified with the trmdstat command. It will display the summary of UDP constrained state and datagram discard information.

IP Address: Indicates the IP address of the destination host.

Port: Indicates the port number.

Constrained State Entered

- Indicates the number of times the UDP port receive queue became constrained.

Constrained State Exited

- Indicates the number of times the UDP port receive queue constraint ended.

Constrained State Duration

- Indicates the number of seconds the UDP port receive queue constraint condition existed.

Datagrams discarded

- Indicates the number of datagrams discarded.

Datagrams would have been discarded

- Indicates the number of datagrams that would have been discarded if "TypeActions Limit" had been specified in the TR policy.

TR UDP Detail Report

trmdstat -U -D /tmp/tstlog.log							
trmdstat for z/OS CS V1R2							
Wed Nov 8 09:03:34 2000							
Log Time Interval : Aug 21 08:32:09 - Aug 21 10:32:09							
Stack Time Interval : Aug 21 14:32:09 - Aug 21 16:33:09							
TRM Records Scanned : 71							
Port Range : ALL							
UDP TR Events							
IP Address : 05.16.17.18							
Date and Time							
Port							
Type							
Duration							
Discarded							
Qsize							
Correlator							
8/21/2000 14:32:9.53							
5001							
E							
100							
155							
VS							
87011							
8/21/2000 14:33:9.53							
2001							
X							
100							
155							
VS							
87232							
IP Address : 05.16.17.18							
Date and Time							
Port							
Type							
Duration							
Would have been Discarded							
Qsize							
Correlator							
8/21/2000 16:32:9.54							
1001							
E							
100							
155							
VS							
87887							
8/21/2000 16:33:9.54							
2001							
X							
100							
155							
VL							
87995							
TRMD Started : Aug 21 10:32:09							

Contents of individual UDP records.

This report will be displayed when the -U, and -D options are specified. It will display the contents of individual UDP records.

IP Address: Indicates the IP address of the destination host.

Date and Time: Indicates the date and time in the record written when the datagram was discarded or would have been discarded.

Port: Indicates the port number.

Type: Indicates the constraint type of the record -

- 'E' indicates constraint entry,
- 'X' indicates constraint exit.

Duration

- Indicates the number of seconds the UDP receive queue was constrained.

Discarded

- Indicates the number of datagrams discarded.

Would have been Discarded

- Indicates the number of datagrams that would have been discarded if "TypeActions Limit" had been specified in the UDP policy.

Qsize: Indicates the queue size specified in the policy.

Correlator: Indicates the trace correlator.

TR UDP Statistics Report

trmdstat -U -S /tmp/statlog.log									
trmdstat for z/OS CS V1R2									
Tue Jan 16 13:17:08 2001									
Log Time Interval : Jan 9 10:54:17 - Jan 9 10:55:45									
Stack Time Interval : Jan 9 15:47:00 - Jan 9 15:55:15									
TRM Records Scanned : 27									
Port Range : ALL									
UDP Statistics									
IP Address : 127.0.0.1									
Date and Time									
Port									
Datagrams Received									
Datagrams Discarded									
Dgs Peak									
01/09/2001 15:47:00.11									
8000									
12345670									
1230									
111									
Bytes Received									
Bytes Discarded									
Bytes Peak									
12345671									
1231									
1111									
Duration									
Constraints									
Qsize									
Action									
10									
50									
VS									
NOLIMIT									
Date and Time									
Port									
Datagrams Received									
Datagrams Discarded									
Dgs Peak									
01/09/2001 15:49:03.63									
8002									
33333330									
3330									
333									
Bytes Received									
Bytes Discarded									
Bytes Peak									
33333333									
3333									
3333									
TRMD Started									
: Jan 9 10:53:42									
TRMD Ended									
: Jan 9 11:05:14									

Contents of individual UDP statistics records.

This report will be displayed when the -U, and -S options are specified. It will display the contents of individual UDP statistics records.

IP Address: Indicates the IP address of the destination host.

Date and Time: Indicates the date and time at which the statistics information was collected by the TCP/IP stack.

Port: Indicates the port number.

Datagrams Received: Indicates the number of UDP datagrams received during the statistics interval.

Datagrams Discarded: Indicates the number of UDP datagrams discarded during the statistics interval.

DatagramsPeak : Indicates the maximum concurrent number of UDP datagrams attached to the receive queue during the statistics interval.

Bytes Received: Indicates the number of bytes received during the statistics interval.

Bytes Discarded: Indicates the number of bytes discarded during the statistics interval.

Bytes Peak: Indicates the maximum concurrent number of bytes within UDP datagrams attached to the receive queue during the statistics interval.

Duration: Indicates the number of seconds the port was in a constrained state during the statistics interval.

Constraints: Indicates the number of times a constrained state was entered during the statistics interval.

Qsize: Indicates the queue size specified in the policy.

Action: Indicates the action specified on the policy ibm-idsTypeActions statement.

- 'LIMIT' indicates LIMIT was specified.
- 'NOLIMIT' indicates no ibm-idsTypeActions LIMIT was specified.

TR TCP Summary Report

```

trmdstat -T /tmp/tstlog.log
trmdstat for z/OS CS V1R2
Wed Nov 8 10:42:41 2000
Log Time Interval : Aug 21 09:32:09 - Aug 21 12:32:09
Stack Time Interval : Aug 21 09:32:09 - Aug 21 12:32:09
TRM Records Scanned : 71
Port Range : ALL
TCP TR Summary
Local Host: 00.01.02.03 Host: 10.11.12.13
Constrained States
Port Enter Limited Exit Duration Excp QOS Connections Refused Host
-----
7001 0 0 0 1 0 0
Local Host: 20.21.22.23 Host: 11.12.13.14
Constrained States
Port Enter Logged Exit Duration Excp QOS Would have been Refused Host
-----
2001 1 1 100 0 0 0
9001 0 0 0 0 1 1
TRMD Started : Aug 21 10:32:09

```

011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 56

Summary of TCP constrained state and datagram discard information.

This report will be displayed when the -T option is specified with the trmdstat command. It will display the summary of TCP constrained state and datagram discard information.

Local Host Indicates the destination host IP address.

Host Indicates the source host IP address.

Port number Indicates the port number.

Enter constrained state

- Limited - Indicates the number of times the available connections for this port has fallen to ten percent under a TCP TR policy specifying LIMIT.
- Logged - Indicates the number of times the available connections for this port has fallen to ten percent under a TCP TR policy specifying LOG.

Exit constrained state

- Limited - Indicates the number of times the available connections for this port has exceeded twelve percent under a TCP TR policy specifying LIMIT.
- Logged - Indicates the number of times the available connections for this port has exceeded twelve percent under a TCP TR policy specifying LOG.

Duration

- Limit - Indicates the number of seconds connections have been constrained state(s) under a TCP TR policy specifying LIMIT.
- Logged - Indicates the number of seconds connections have been constrained state(s) under a TCP TR policy specifying LOG.

Excp QOS - Indicates the number of times a QOS exception has occurred.

Connections Refused

- Appl - Indicates the number of times connections were refused because an application was constrained.
- Host - Indicates the number of times connections were refused because the host was constrained.

Connections would have been Refused

- Appl - Indicates the number of times connections would have been refused because an application was constrained if "TypeActions Limit" had been specified in the TR policy.
- Host - Indicates the number of times connections would have been refused because the host was constrained if "TypeActions Limit" had been specified in the TR policy.

TR TCP Extended Summary Report

```

trmdstat -T -E /tmp/tstlog.log
trmdstat for z/OS CS V1R2          Wed Dec 20 17:02:50 2000
Log Time Interval   : Aug 21 08:32:09 - Aug 21 08:32:09
Stack Time Interval : Aug 21 09:32:09 - Aug 21 12:32:09
TRM Records Scanned : 70
Port Range         : ALL
TCP Extended TR Summary

```

Local Host: 00.01.02.03		Host: ALL		Constrained States		Excp		Connections		Refused	
Port	Host	Enter	Limited	Exit	Duration	QOS		Appl	Host		
3001	11.12.13.14	1		1	100	0		0		0	0
7001	10.11.12.13	0		0	0	1		0		0	0
8001	11.12.13.14	0		0	0	0		1		0	0

```

Local Host: 20.21.22.23

```

Local Host: 20.21.22.23		Host: ALL		Constrained States		Excp		Connections		Refused	
Port	Host	Enter	Logged	Exit	Duration	QOS		Would have been	Appl	Host	
2001	11.12.13.14	1		1	100	0		0		0	0
7001	10.11.12.13	0		0	0	1		0		0	0
9001	11.12.13.14	0		0	0	0		1		1	1

```

TRMD Ended          : Aug 21 08:32:09

```

011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 57

Extended summary of TCP constrained state and datagram discard information.

This report will be displayed when the -T and the -E options are specified with the trmdstat command. It will display the extended summary of TCP constrained state and datagram discard information.

Local Host: Indicates the destination host IP address.

Host: Indicates the source host IP address.

Port number: Indicates the port number.

Enter constrained state

- Limited - Indicates the number of times the available connections for this port has fallen to ten percent under a TCP TR policy specifying LIMIT.
- Logged - Indicates the number of times the available connections for this port has fallen to ten percent under a TCP TR policy specifying LOG.

Exit constrained state

- Limited - Indicates the number of times the available connections for this port has exceeded twelve percent under a TCP TR policy specifying LIMIT.
- Logged - Indicates the number of times the available connections for this port has exceeded twelve percent under a TCP TR policy specifying LOG.

Duration

- Limit - Indicates the number of seconds connections have been constrained state(s) under a TCP TR policy specifying LIMIT.
- Logged - Indicates the number of seconds connections have been constrained state(s) under a TCP TR policy specifying LOG.

Excp QOS: Indicates the number of times a QOS exception has occurred.

Connections Refused -

- Appl - Indicates the number of times connections were refused because an application was constrained.
- Host - Indicates the number of times connections were refused because the host was constrained.

Connections would have been Refused

- Appl - Indicates the number of times connections would have been refused because an application was constrained if "TypeActions Limit" had been specified in the TR policy.
- Host - Indicates the number of times connections would have been refused because the host was constrained if "TypeActions Limit" had been specified in the TR policy.

TR TCP Detail Report

trmdstat -T -D /tmp/tstlog.log									
trmdstat for z/OS CS V1R2									
Wed Nov 8 10:45:08 2000									
Log Time Interval : Aug 21 09:32:09 - Aug 21 12:32:09									
Stack Time Interval : Aug 21 09:32:09 - Aug 21 12:32:09									
TRM Records Scanned : 71									
Port Range : ALL									
TCP TR Events									
Events Limited									
Local Host: 00.01.02.03 Source Host: ALL									
Date and Time Port Source Host Rec Cns									

Typ Typ Connections									

Current Available Total Conn Policy									

8/21/2000 10:32:9.53 1001 11.12.13.14 C 411 500 1000 25 ...									
8/21/2000 10:32:9.53 2001 21.22.23.24 C 411 500 1000 25 ...									
.....									
Events Logged									
Local Host: 00.01.02.03 Source Host: ALL									
Date and Time Port Source Host Rec Cns									

Typ Typ Connections									

Current Available Total Conn Policy									

8/21/2000 10:32:9.54 1001 11.12.13.14 C 222 500 1000 25 0									
TRMD Started : Aug 21 10:32:09									

This report will be displayed when the -T, and -D options are specified. It will display the contents of individual TCP records.

Local Host: Indicates the destination host IP address.

Source Host: Indicates the source host IP address.

Date and Time: Indicates the date and time in the record written when the connection was refused or logged.

Port number: Indicates the port number.

Rec Typ: Indicates the record type -

- 'C' indicates connection,
- 'S' indicates constraint and
- 'Q' indicates QOS exception.

Cns Typ: Indicates the constraint type -

- 'E' indicates entering constraint,
- 'X' indicates exiting constraint.

Connections current: Indicates the number of current connections.

Connections available: Indicates the number of available connections.

- Note: if this count is negative more connections exist than are allowed by the policy.

Policy Total Conn: Indicates the number of total connections allowed by the TCP TR policy.

Policy Pct: Indicates the percentage of total connections allowed under the TCP TR policy.

Policy QOS limit: Indicates the number of connections allowed under the QOS policy.

Correlator: Indicates the trace correlator.

Probeid: Indicates the probe ID contained in the record written when the connection was refused or logged.

TR TCP Statistics Report

```
trmdstat -T -S /tmp/statlog.log
trmdstat for z/OS CS VIR2      Thu Jan 18 16:28:59 2001

Log Time Interval : Jan 9 10:54:15 - Jan 9 10:54:15
Stack Time Interval : Jan 9 15:42:53 - Jan 9 15:42:53
TRM Records Scanned : 27
Port Range : ALL
```

TCP TR Statistics									
Local Host: 127.0.0.1	Port	Peak Host: ALL	Action	Peak Host	Requests	Warnings	QosExcepts	Terminates	
Date and Time		Peak Host		Host	Current	Duration	SugLimit	SugPercent	
01/09/2001 15:42:53.20	8054	112.122.132.142	NOLIMIT	1	1	1111	111	1	
01/09/2001 15:42:53.20	8055	2.2.2.2	LIMIT	2	222	2222	222	2	
01/09/2001 15:42:53.20	8056	3.3.3.3	LIMIT	3	333	3333	333	3	
TRMD Started	: Jan 9 10:53:42								
TRMD Ended	: Jan 9 11:05:14								

011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 59

This report will be displayed when the -T, and -S options are specified. It will display the contents of individual TCP statistics records.

Local Host: Indicates the destination host IP address.

Peak Host: Indicates the peak host IP address.

Date and Time: Indicates the date and time at which the statistics information was gathered by the TCP/IP stack.

Port number: Indicates the port number.

Action: Indicates the action specified on the policy ibm-idsTypeActions statement

- 'LIMIT' indicates LIMIT was specified.
- 'NOLIMIT' indicates no TypeAction LIMIT was specified.

Peak: Indicates the maximum number of concurrent connections to this port held during the statistics interval.

Requests: Indicates the number of connections requested during the statistics interval.

Warnings: Indicates the number of connections refused if Action=LIMIT was indicated in the statistics message; the number of connections that would have been refused if Action=NOLIMIT was indicated.

QosExcepts: Indicates the number of connections that would have been refused by Traffic Regulation policy but allowed by QOS policy if the ibm-idsTypeActions policy specification is LIMIT.

Terminates: Indicates the number of connections that were disconnected during the statistics interval.

Peak Host: Indicates the peak host IP address.

HostPeak: Indicates the maximum number of concurrent connections held by a source host at any time during the statistics interval.

Current: Indicates the number of connections currently active on the port.

Duration: Indicates the number of seconds the port was in a constrained state during the statistics interval.

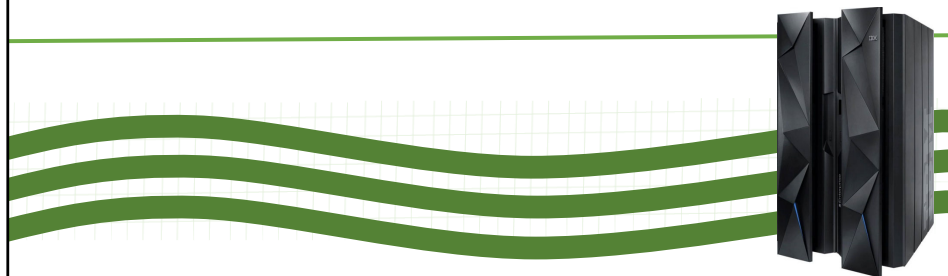
SugLimit: Indicates the suggested value for the ibm-idsTRtcpTotalConnections policy specification based on traffic during this statistics interval.

- If ibm-idsTypeActions LIMIT is specified the value will be zero.

SugPercent: Indicates the suggested value for the ibm-idsTRtcpPercentage policy specification based on the traffic during this statistics interval.

- If ibm-idsTypeActions LIMIT is specified the value will be zero.

IDS Policy Displays



011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 60

NETSTAT IDS Display

- NETSTAT IDS command is supported from operator console, TSO and Unix (-k).
 - netstat ids summary (from tso)
 - netstat -k summary (from OE)
 - Options:
 - Summary
 - Protocol (TCP or UDP)
- RACF resource (EZB.NETSTAT.mvsname.tcprocname.IDS) can be used to restrict access to command.
- Syntax documented in the IP System Administrator's Command manual.

011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 61

If neither Summary or Protocol specified, summary and protocol reports for tcp and udp are displayed.

Summary information shows global information (for example scan globals and attack rule) and overall totals by IDS type.

Protocol information shows data for TCP or UDP by port if the tcb or ucb has IDS related information (for example, an IDS rule or is undergoing a syn flood).

See the IP System Administrator's Command manual for command syntax and additional information.

NETSTAT IDS Summary Display

```
onetstat -k SUM
MVS TCP/IP onetstat CS V1R2          TCPIP Name: TCPCS
Intrusion Detection Services Summary:
Scan Detection:
  GlobRuleName: ScanGlobal-rule
  IcmpRuleName: ScanEventMedium-rule
  TotDetected: 0                      DetCurrPlc: 0
  DetCurrInt: 0                      Interval: 60
  SrcIPsTrkd: 1                      StrgLev: 00000M
Attack Detection:
  Malformed Packets
  PlcRuleName: AttackMalformed-rule
  TotDetected: 0                      DetCurrPlc: 0
  DetCurrInt: 0                      Interval: 60
  OutBound RAW Restrictions
  PlcRuleName: AttackOutboundRaw-rule
  TotDetected: 1200                  DetCurrPlc: 1200
  DetCurrInt: 1200                  Interval: 60
  ...
Traffic Regulation:
  TCP
  ConnRejected: 0                    PlcActive: N
  UDP
  PckDiscarded: 0                    PlcActive: N
```

NETSTAT IDS Protocol Display

```
netstat -k PROTOCOL TCP
MVS TCP/IP onetstat CS V1R2          TCPIP Name:
TCPCS 10:57:46
Intrusion Detection Services TCP Port List:
TcpListeningSocket: 0.0.0.0..21
  ScStat: C   ScRuleName: ScanEvent-rule
  TrStat: C   TrRuleName: TRtcp-rule
  TrPortInst: Y   TrCorr: 0           MxApp: 0
MxHst: 0
  SynFlood:    N
TcpListeningSocket: 0.0.0.0..623
  ScStat: C   ScRuleName: ScanEvent-rule
  TrStat: C   TrRuleName: TRtcp-rule
  TrPortInst: Y   TrCorr: 0           MxApp: 0
MxHst: 0
  SynFlood:    N
```

Note: Only applications with IDS-related information are displayed.

pasearch IDS Display

```
'pasearch -i'
MVS TCP/IP pasearch CS V1R2      TCP/IP Image:  NM1ATCP
Date: 01/28/2002                Time: 19:31:43

Policy:  Profile:  routed
Version: 1
Permission: Allowed
Direction: Outgoing
ServiceClass: networkcontrol
LocalInterface: 0.0.0.0
SourceIpFrom: 0.0.0.0
SourcePortFrom: 520
DestIpFrom: 0.0.0.0
DestPortFrom: 0

ServiceClass: networkcontrol
Version: 1
Scope: DataTraffic

Status: Active
Protocol: UDP
No. ServiceClass: 1

SourceIpTo: 0.0.0.0
SourcePortTo: 520
DestIpTo: 0.0.0.0
DestPortTo: 0

Status: Active
OutgoingTOS: 11100000
```

011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 64

Pasearch command options:

- -n to display only policy names, no policy details
- -i to display only IDS policy actions (and rules)
- -q to display only QoS policy actions (and rules)
- Policies with PolicyScope TR are converted into IDS TR policies. This means the TR value on the pasearch -s parameter is no longer valid - the pasearch -i option must be used to display these policies.

Usage: pasearch <options>

options:

- A - Display only Active Policy Entries
- I - Display only Inactive Policy Entries
- d - Display Debug Information
- a - Display only Policy Actions
- e - Display every Policy Entry (Policy Rules and/or Policy Actions) that matches pasearch <options>
- f <PolicyFilterName>
 - Display only Policy Entries that are an exact or wildcard match for Policy Rule <PolicyFilterName>
 - Use -w option for wildcard matches
 - Use -g option for <PolicyFilterName> to be matched to Policy Rule and Policy Action
 - <PolicyFilterName> is case sensitive
- g - Matches the <PolicyFilterName> to both Policy Rule and Policy Action.
- i - Display all Ids Policy entries that match the input option for pasearch
 - This Option is incompatible with other Action Types (ie. -q)
- n - Display policy names only.
- o - Display Condition Original Level and Condition Original Arrays
- p <TcpImage>
 - Display only Policy Entries associated with <TcpImage> value
 - <TcpImage> is case insensitive
- q - Display all Qos Policy entries that match the input option for pasearch
 - This Option is incompatible with other Action Types (ie. -i)
- r - Display only Policy Rules
- s <PolicyScopeName>
 - Display all Qos Policy Actions that match the <PolicyScopeName> value
 - Valid values are 'RSVP', 'DataTraffic' or 'Both'
 - <PolicyScopeName> is case insensitive
- w - Display Policy Entries for all matched <PolicyFilterName> as a wildcard
- ? - Displays command syntax information

End of Topic



011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 65

End of Topic



011_ZCS301_IDS

© Copyright IBM Corporation 2023

Page 66