

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.

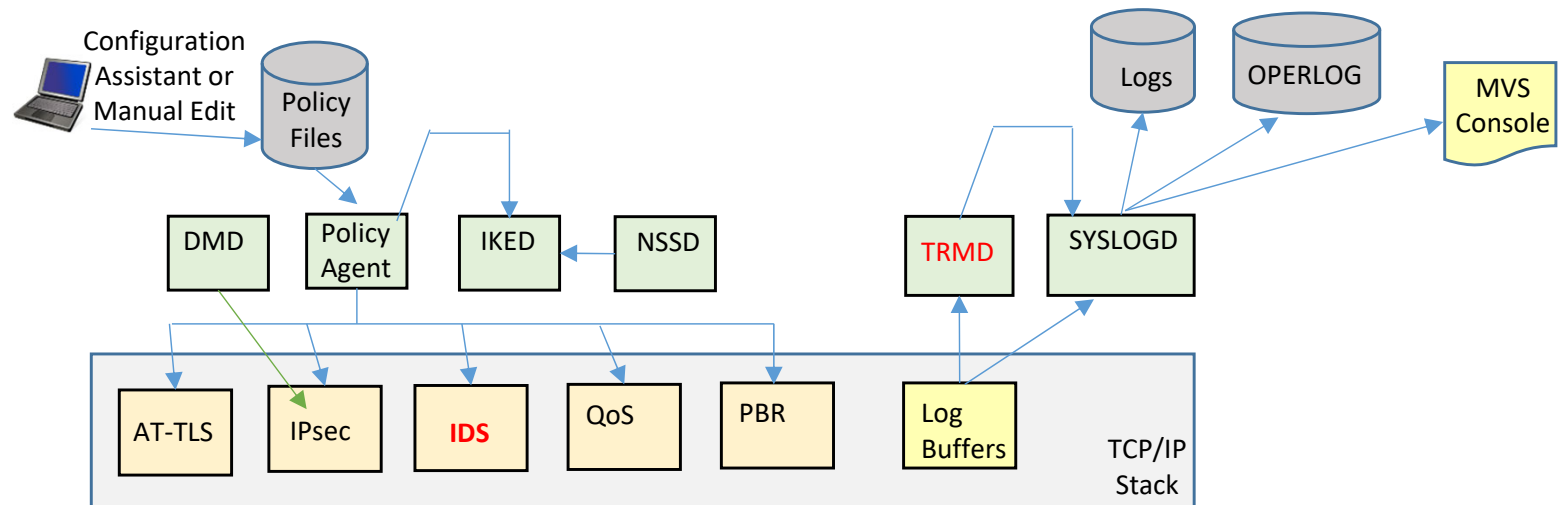
Agenda

- 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



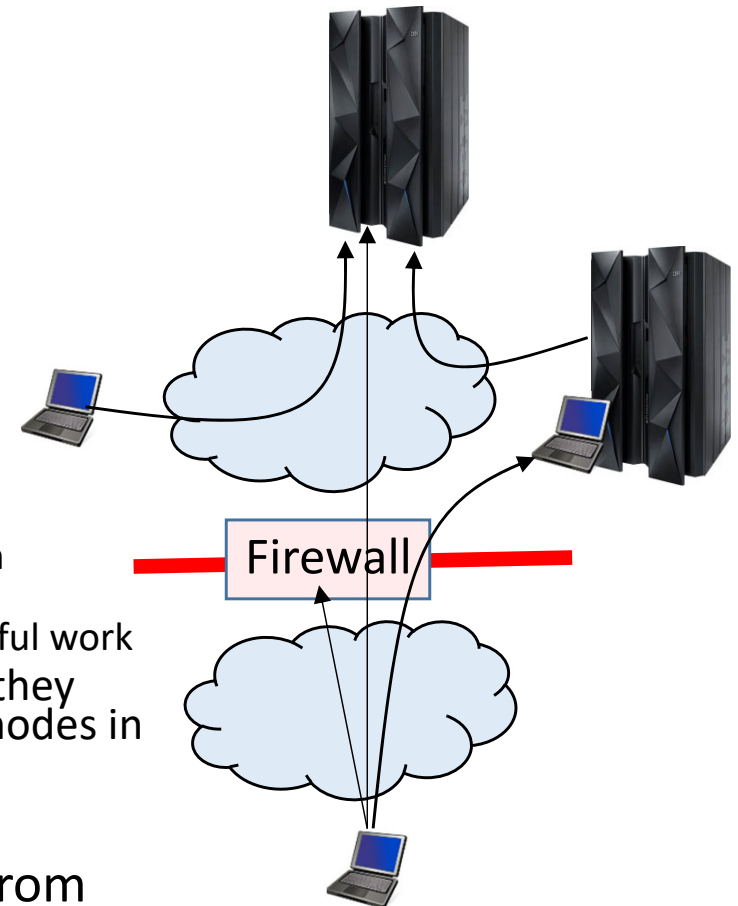
Lots of Different Policy Types and Started Tasks



- 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

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

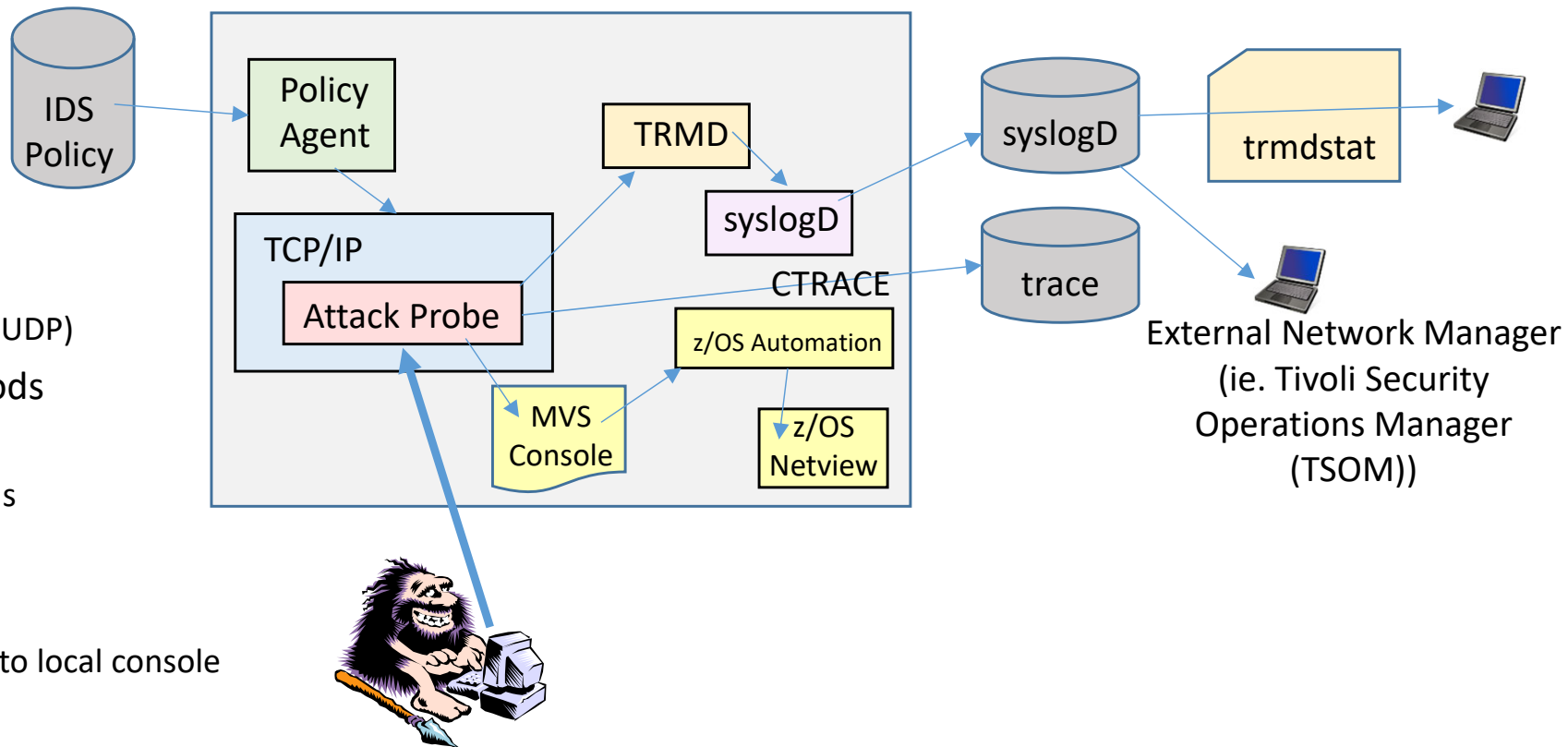


Firewall Definition

- 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.

z/OS IDS Capabilities

- Events detected
 - Scans
 - Attacks
 - Floods (TCP and UDP)
- Defensive methods
 - Packet discard
 - Limit connections
- Reporting
 - Logging
 - Event messages to local console
 - IDS packet trace
 - Notifications to Network Managers (ie. Tivoli NetView and Tivoli Security Operations Manager)
- z/OS IDS broadens intrusion detection coverage:
 - Evaluates inbound encrypted data - IDS applied after decryption
 - IDS policy checked after attack detected
 - Avoids overhead of per packet evaluation against table of known attacks
 - Detects statistical anomalies real-time
 - System has stateful data / internal thresholds that are unavailable to external IDSs
 - Policy can control prevention methods, such as connection limiting and packet discards



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

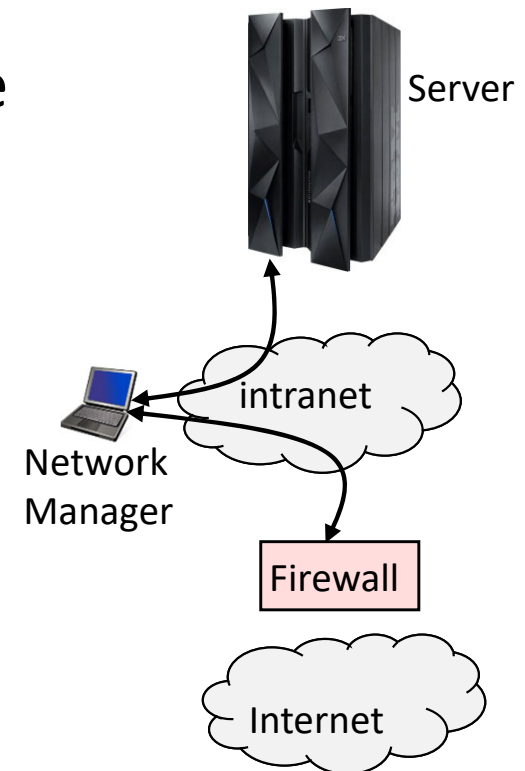
- Intent of an attack is to crash or hang the system (Single or multiple packet)
- Attack Types (See details in Attack section of this presentation)
 - Malformed packet events
 - Inbound fragment restrictions (IPv4)
 - IP protocol restrictions
 - IP option restrictions
 - UDP perpetual echo
 - ICMP redirect 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, otlenetD, etc.)

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



IDS in Configuration Assistant tool

The top screenshot shows the IBM z/OS Management Facility Configuration Assistant tool. The left sidebar contains a navigation menu with options: Welcome, Notifications, Workflows, Configuration (selected), Links, z/OSMF Administration, and z/OSMF Settings. The main content area displays the 'Configuration Assistant (Home) > IDS' page. It shows 'V2R1 Current Backing Store = test1' and a 'Select a perspective: IDS' dropdown. Below this, there are tabs for 'Systems', 'Traffic Descriptors', and 'Requirement Maps'. The 'Systems' tab is active, showing a table with columns: Name, Type, Status, Release, and Description. The table contains two rows: 'ZOS1' (Image, Complete, V2R1) and 'TCPIPT' (Stack, Incomplete, V2R1).

The bottom screenshot shows the same tool, but with the 'Requirement Maps' tab selected. A blue arrow points to the 'Requirement Maps' tab. The table in this tab has columns: Name, Description, and a 'Filter' column. It contains one row: 'IDS_Default' with the description 'IBM Supplied: Intrusion Detection Services Starter Set'. At the bottom of the page, it says 'Total: 1, Selected: 1' and has 'Home' and 'Save' buttons.

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

Default IDS Policy

- The default only provides Attack protection.

The screenshot displays the IBM z/OS Management Facility (zOSMF) Configuration Assistant interface. The left sidebar shows the navigation menu with options like Welcome, Notifications, Workflows, Configuration, and Links. The main content area is titled 'Configuration Assistant (Home) > IDS > View Details'. It shows the 'Requirement Map: IDS_Default - IBM Supplied: Intrusion Detection Services Starter Set' and an 'Attack Protection Summary' table.

| Enabled Attack Protection | Rule Name | Actions | Reports | Time Condition | Default Report Settings |
|--|------------------------|----------------------|-----------------------------|----------------|-------------------------|
| Data Hiding Attack ¹ | DataHiding | Report Events | Use Default Report Settings | None | |
| IPv6 Outbound Raw Attack ¹ | IPv6OutboundRaw | Report Events | Use Default Report Settings | None | |
| IPv6 Destination Options Attack ¹ | IPv6DestinationOptions | Report Events | Use Default Report Settings | None | |
| IPv6 Hop-by-Hop Options Attack ¹ | IPv6HopByHop | Report Events | Use Default Report Settings | None | |
| IPv6 Next Header Attack ¹ | IPv6NextHeader | Report Events | Use Default Report Settings | None | |
| TCP Queue Size Attack ¹ | TcpQueueSize | Report Events | Use Default Report Settings | None | |
| Global TCP Stall Attack ¹ | 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 | |
| IP Fragment Attack | Fragmentation | 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

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

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.

Attack Detection

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



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.

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

Attack Policy

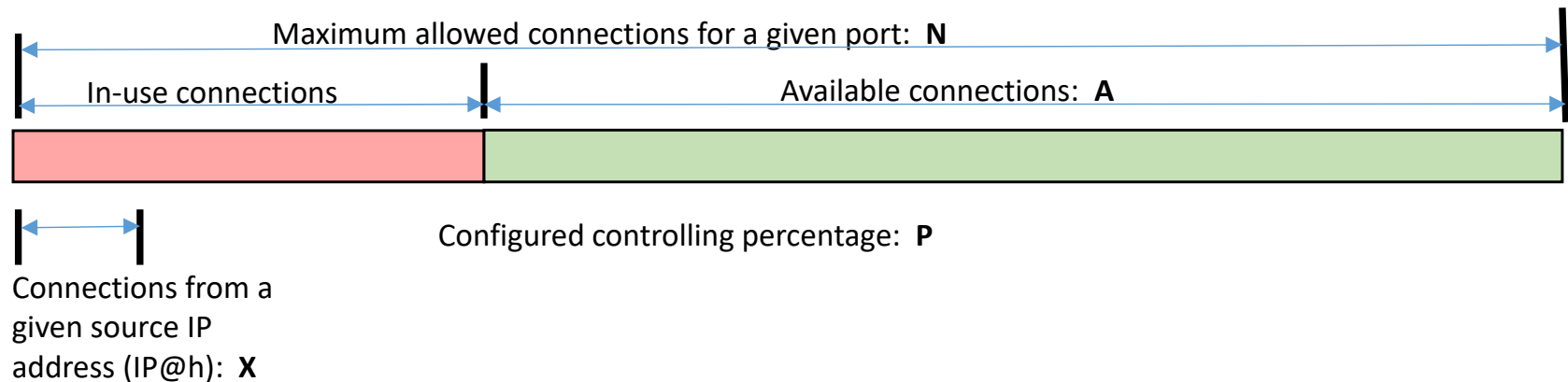
- Attack policy provides the ability to:
 - Control attack detection for one or more attack categories independently.
 - Obtain notification and documentation of attacks.
 - Notify the installation of a detected attack via console message or syslogd message.
 - Trace potential attack packets.
 - Request 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

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.

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)

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`

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

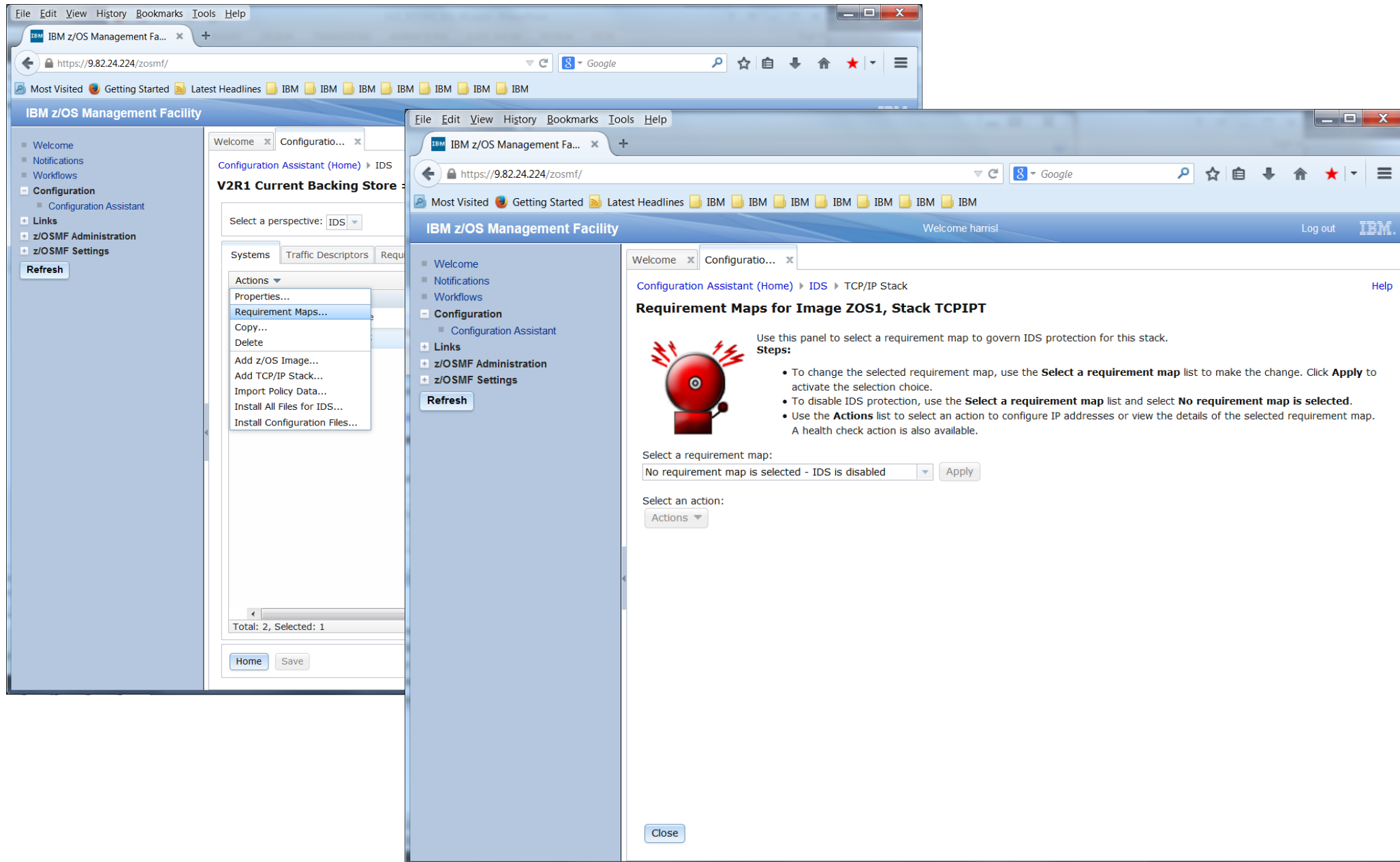
TR UDP Policy Steps

- 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



IDS in Network Configuration Assistant



Select Default IDS Policy

The image displays two overlapping screenshots of the IBM z/OS Management Facility Configuration Assistant web interface, illustrating the steps to select a default IDS policy.

Left Screenshot: The 'Configuration Assistant (Home)' page is shown. The 'Requirement Maps for Image ZOS1, Stack TCPIPT' section is active. A red alarm bell icon is displayed. The 'Select a requirement map:' dropdown menu is open, showing 'No requirement map is selected' and 'IDS_Default'. The 'IDS_Default' option is highlighted. A 'Refresh' button is visible below the dropdown.

Right Screenshot: The 'Configuration Assistant (Home)' page is shown, with the 'IDS' tab selected. The 'Requirement Maps for Image ZOS1, Stack TCPIPT' section is active. The 'Select a requirement map:' dropdown menu is set to 'IDS_Default'. The 'Apply' button is visible next to the dropdown. The 'Select an action:' dropdown menu is open, showing 'Actions', 'Set Addresses...', 'View Details', and 'Health Check'. The 'Set Addresses...' option is highlighted.

Customize IDS Policy

- The default only provides Attack protection.

The screenshot displays the IBM z/OS Management Facility Configuration Assistant interface. The main window is titled 'Set Addresses Requirement Map' and is divided into three tabs: 'Scans', 'Traffic Regulation', and 'Attacks'. The 'Attacks' tab is currently selected, showing a table of attack types and their remote exclusions. The table has columns for 'Attack Type', 'Rule Name', and 'Remote Exclusions'. The table lists five attack types: 'TCP Queue Size Attack', 'EE Malformed Packet Attack', 'EE LDLC Check Attack', 'EE Port Check Attack', and 'EE XID Flood Attack'. All have 'None' for Remote Exclusions. The page also includes instructions on how to specify remote exclusions and a 'Refresh' button.

| Attack Type | Rule Name | Remote Exclusions |
|--|-------------------|-------------------|
| <input type="radio"/> TCP Queue Size Attack | TcpQueueSize | None |
| <input type="radio"/> EE Malformed Packet Attack | EEMalformedPacket | None |
| <input type="radio"/> EE LDLC Check Attack | EELDLCCheck | None |
| <input type="radio"/> EE Port Check Attack | EETPortCheck | None |
| <input type="radio"/> EE XID Flood Attack | EEXIDFlood | None |

Policy Messages, Logs, and Displays



Without TR Policy

- Proclib Unix settings:

BPXPRM00
MAXPROCUSER 200

- When a hacker is attempting connections to the port:

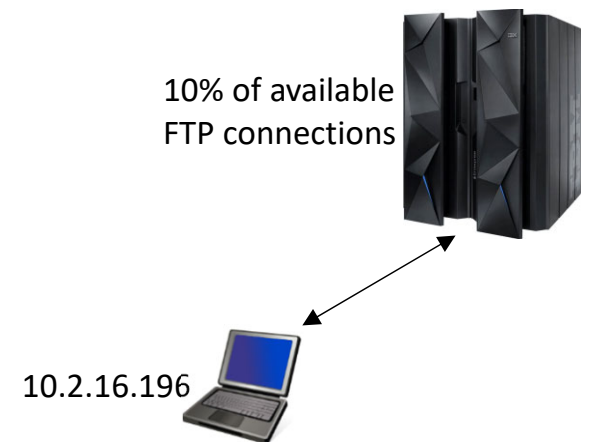
*BPXI040I PROCESS LIMIT MAXPROCUSER HAS REACHED 95% OF ITS CURRENT 708
CAPACITY OF 200 FOR PID=16777525 IN JOB FTPT214 RUNNING IN
ADDRESS SPACE 0032

*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.



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

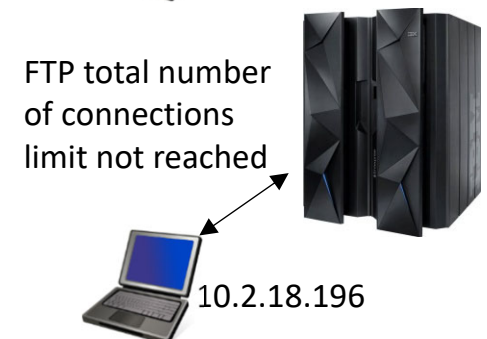
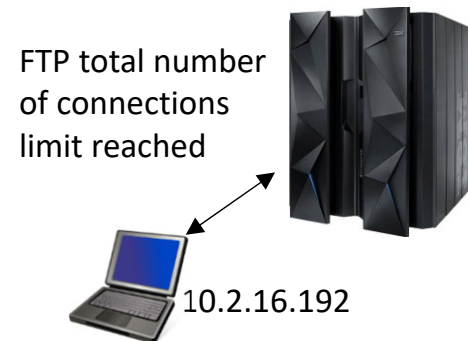
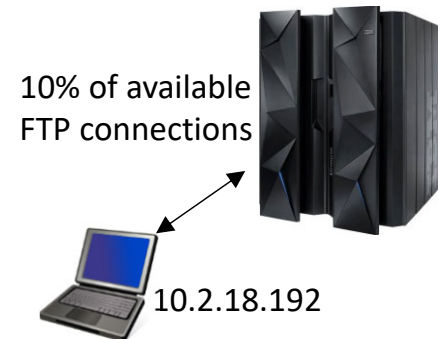
With TR Policy

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

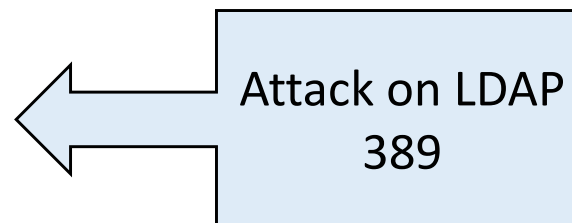
EZZ8761I IDS EVENT DETECTED 366
EZZ8762I EVENT TYPE: TCP PORT CONSTRAINED
EZZ8763I CORRELATOR 153 - PROBEID 01004400
EZZ8764I SOURCE IP ADDRESS 10.2.18.192 - PORT 0
EZZ8765I DESTINATION IP ADDRESS 0.0.0.0 - PORT 23
EZZ8766I IDS RULE TN3270TR
EZZ8767I IDS ACTION C20P10

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



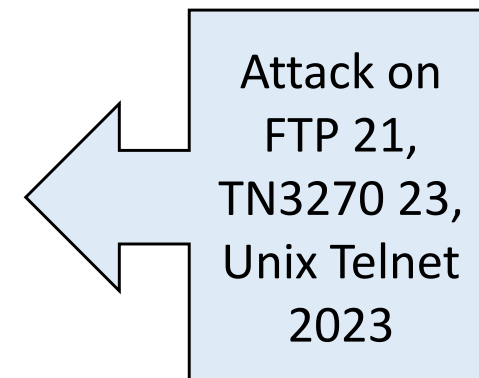
SYNFLOOD LDAP, FTP, TN3270, Unix Telnet

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



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



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

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

SYNFLOOD FOR TN3270

D TCPIP,,T,CONN

EZZ6064I TELNET CONNECTION DISPLAY 363


| CONN | EN | 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




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
```



Display that Show SYNFLOOD

D TCPIP,,N,IDS

EZZ2500I NETSTAT CS V1R4 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

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 msgs. per 5 minutes

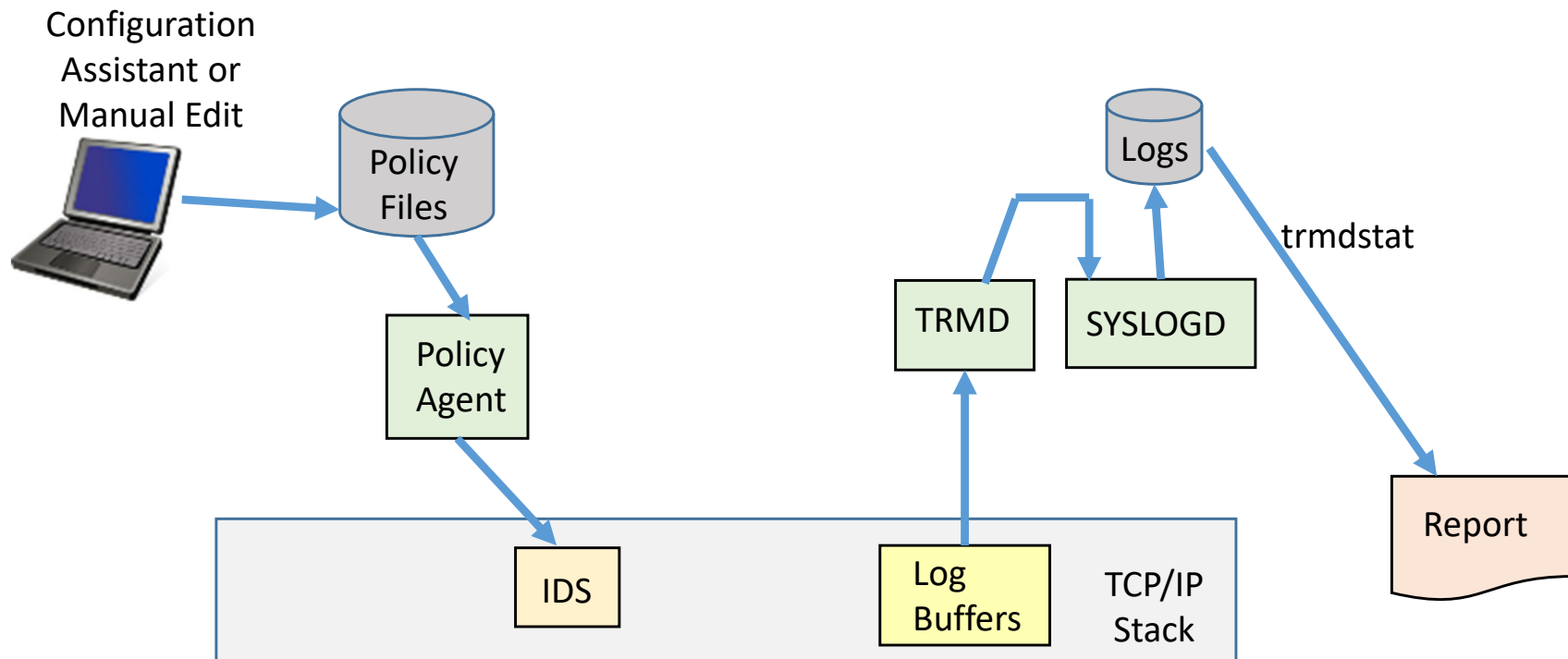
```
EZZ8761I  IDS EVENT DETECTED 355
EZZ8762I  EVENT TYPE: SUSPICIOUS PACKET RECEIVED
EZZ8763I  CORRELATOR 2 - PROBEID 04020001
EZZ8764I  SOURCE IP ADDRESS 172.17.0.121 - PORT 0
EZZ8765I  DESTINATION IP ADDRESS 224.0.0.5 - PORT 0
EZZ8766I  IDS RULE AttackOutboundRaw-rule
EZZ8767I  IDS ACTION AttackLimit-action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

```
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
```

trmdstat Reports



trmdstat Command



- Create reports from IDS syslogd data.

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
```

Flood Summary Report

```
trmdstat -F /tmp/tstlog.log
trmdstat for z/OS CS V1R2
```

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
```

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 | | 87591 |
| 8/21/2000 14:31:9.53 | 11.12.13.14 | 11000 | E | | 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
```

Attack Summary Report

```
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
```

| 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 |

```
Datagrams would have been Discarded
Source: 61.62.63.64      Destination: 31.32.33.34
Attacks
```

| Dst Port | Malf | ORaw | IPFr | ICMP | IPop | Prto | Perp | NoId |
|----------|------|------|------|------|------|------|------|------|
| 12001 | 0 | 2 | 0 | 0 | 0 | 0 | 0 | 0 |

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


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
```

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 |
| PRTO | 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
```

Scan Summary Report

```
trmdstat -N /tmp/tstlog.log
trmdstat for z/OS CS V1R2          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
```

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 | | | Type | Correlator |
|----------------------|-------------|----------------|----------|--------|------|------------|
| | | Very | Possibly | Normal | | |
| 8/21/2000 14:32:9.53 | 11.12.13.14 | 5 | 5 | 5 | S | 47113 |
| 8/21/2000 14:32:9.53 | 11.12.13.14 | 5 | 5 | 5 | S | 47212 |
| 8/21/2000 14:32:9.53 | 11.12.13.14 | 5 | 5 | 5 | F | 57287 |
| 8/21/2000 14:32:9.53 | 11.12.13.14 | 5 | 5 | 5 | F | 67333 |
| 8/21/2000 14:32:9.54 | 22.33.44.55 | 100 | 200 | 300 | F | 87433 |
| 8/21/2000 14:32:9.54 | 22.33.44.55 | 100 | 200 | 300 | F | 97500 |

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

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

| IP Address | Port | Entered | Constrained State Exited | Duration | Datagrams Discarded |
|-------------|------|---------|-----------------------------|----------|------------------------|
| 05.16.17.18 | 2001 | | 1 | 1 | 100 |
| 05.16.17.18 | 5001 | | 2 | 2 | 200 |

| IP Address | Port | Entered | Constrained State Exited | Duration | Datagrams Would have been Discarded |
|-------------|------|---------|-----------------------------|----------|--|
| 05.16.17.18 | 1001 | | 1 | 1 | 100 |
| 05.16.17.18 | 2001 | | 2 | 2 | 200 |

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

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 | | | 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 | | | VS | 87887 |
| 8/21/2000 16:33:9.54 | 2001 | X | 100 | 155 | VL | 87995 |

TRMD Started : Aug 21 10:32:09

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
```

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      Connections
              QOS      Refused
-----
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      Would have been Refused
              QOS      Appl      Host
-----
2001             1             1            100             0             0             0
9001             0             0             0             0             1             1

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


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

| Port | Host | Enter | Limited Exit | Duration | Excp QOS | Connections Refused Appl | Host |
|------|-------------|-------|-----------------|----------|-------------|--------------------------------|------|
| 3001 | 11.12.13.14 | 1 | 1 | 100 | 0 | 0 | 0 |
| 7001 | 10.11.12.13 | 0 | 0 | 0 | 1 | 0 | 0 |
| 8001 | 11.12.13.14 | 0 | 0 | 0 | 0 | 1 | 0 |

Local Host: 20.21.22.23

Host: ALL
Constrained States

| Port | Host | Enter | Logged Exit | Duration | Excp QOS | Would have been Refused Appl | Host |
|------|-------------|-------|----------------|----------|-------------|------------------------------------|------|
| 2001 | 11.12.13.14 | 1 | 1 | 100 | 0 | 0 | 0 |
| 7001 | 10.11.12.13 | 0 | 0 | 0 | 1 | 0 | 0 |
| 9001 | 11.12.13.14 | 0 | 0 | 0 | 0 | 1 | 1 |

TRMD Ended : Aug 21 08:32:09

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 | | Connections | | | Policy | |
|-------------------------|------|------------------|--------------------|-------------|-----------|------------|--------|--|
| Date and Time | Port | Source Host | Rec Cns Typ Typ | Current | Available | Total Conn | Pct | |
| 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 | | Connections | | | Policy | |
|-------------------------|------|------------------|--------------------|-------------|-----------|------------|--------|--|
| Date and Time | Port | Source Host | Rec Cns Typ Typ | Current | Available | Total Conn | Pct | |
| 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

TR TCP Statistics Report

```
trmdstat -T -S /tmp/statlog.log
trmdstat for z/OS CS V1R2          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 Date and Time | Port | Peak Host: ALL Action Peak Host | Peak Host | Requests Current | Warnings Duration | QosExcepts SugLimit | Terminates SugPercent |
|--|-------------------|---------------------------------------|--------------|---------------------|----------------------|------------------------|--------------------------|
| 01/09/2001 15:42:53.20 | 8054 | NOLIMIT 112.122.132.142 | 1 1 | 1 111 | 1111 11111 | 111 10 | 1 11 |
| 01/09/2001 15:42:53.20 | 8055 | LIMIT 2.2.2.2 | 2 2 | 2 222 | 2222 22222 | 222 20 | 2 22 |
| 01/09/2001 15:42:53.20 | 8056 | LIMIT 3.3.3.3 | 3 3 | 3 333 | 3333 33333 | 333 30 | 3 33 |
| TRMD Started | : Jan 9 10:53:42 | | | | | | |
| TRMD Ended | : Jan 9 11:05:14 | | | | | | |

IDS Policy Displays



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.tcpprocname.IDS) can be used to restrict access to command.
- Syntax documented in the IP System Administrator's Command manual.

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
```

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 | Status: Active | |
| Version: 1 | Protocol: UDP | |
| Permission: Allowed | No. ServiceClass: 1 | |
| Direction: Outgoing | | |
| ServiceClass: networkcontrol | | |
| LocalInterface: 0.0.0.0 | SourceIpTo: 0.0.0.0 | |
| SourceIpFrom: 0.0.0.0 | SourcePortTo: 520 | |
| SourcePortFrom: 520 | DestIpTo: 0.0.0.0 | |
| DestIpFrom: 0.0.0.0 | DestPortTo: 0 | |
| DestPortFrom: 0 | | |
| ServiceClass: networkcontrol | Status: Active | |
| Version: 1 | OutgoingTOS: 11100000 | |
| Scope: DataTraffic | | |

End of Topic



End of Topic

