z/OS Communications Server Intrusion Detection Services

SHARE Session 17986

Lin Overby - overbylh@us.ibm.com

Trademarks and notices

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

- Advanced Peer-to-Peer Networking®
- AIX®
- alphaWorks®
- AnyNet®
- AS/400®
- BladeCenter®
- Candle®
- CICS®
- DataPower®
- DB2 Connect
- DB2®
- DRDA®
- e-business on demand®
- e-business (logo)
- e business(logo)®
- ESCON®
- FICON®

- GDDM®
- GDPS®
- Geographically Dispersed Parallel Sysplex
- HiperSockets
- HPR Channel Connectivity
- HyperSwap
- i5/OS (logo)
- i5/OS®
- IBM eServer
- IBM (logo)®
- IBM®
- IBM zEnterprise™ System
- IMS
- InfiniBand ®
- IP PrintWay
- IPDS
- iSeries
- LANDP®

- Language Environment®
- MQSeries®
- MVS
- NetView®
- OMEGAMON®
- Open Power
- OpenPower
- Operating System/2®
- Operating System/400®
- OS/2®
- OS/390®
- OS/400®
- Parallel Sysplex®
- POWER®
- POWER7®
- PowerVM
- PR/SM
- pSeries®
- RACF®

- Rational Suite®
- Rational®
- Redbooks
- Redbooks (logo)
- Sysplex Timer®
- System i5
- System p5
- System x®
- System z®
- System z9®
- System z10
- Tivoli (logo)®
- Tivoli®
- VTAM®
- WebSphere®
- xSeries®
- z9®
- z10 BC
- z10 EC

- zEnterprise
- zSeries®
- z/Architecture
- z/OS®
- z/VM®
- z/VSE

* All other products may be trademarks or registered trademarks of their respective companies.

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

- Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
- Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license there from.
- Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
- InfiniBand is a trademark and service mark of the InfiniBand Trade Association.
- Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
- ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
- IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

Notes:

- Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
- IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
- All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
- This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
- All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
- Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
- Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

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

Integrated Intrusion Detection Services

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

This session will cover the following topics

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

The Intrusion Threat

■ **What is an intrusion?**
  ► Information Gathering
    - Network and system topology
    - Data location and contents
  ► Eavesdropping / Impersonation / Theft
    - On the network / on the server
    - Base 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 or unintentional**
  ► Deliberate: malicious intent from outside or internal bots
  ► Unintentional: various forms of errors on network nodes

■ **Attacks can occur from Internet or intranet**
  ► Firewalls can provide some level of protection from Internet
  ► Perimeter Security Strategy *alone* may not be sufficient.
    - Considerations:
      ✓ Access permitted from Internet
      ✓ Trust of intranet

Intrusions can occur from Internet or intranet

Server

Enterprise Network or Intranet

End User Attacker

Zombie Attackers

Firewall

Internet
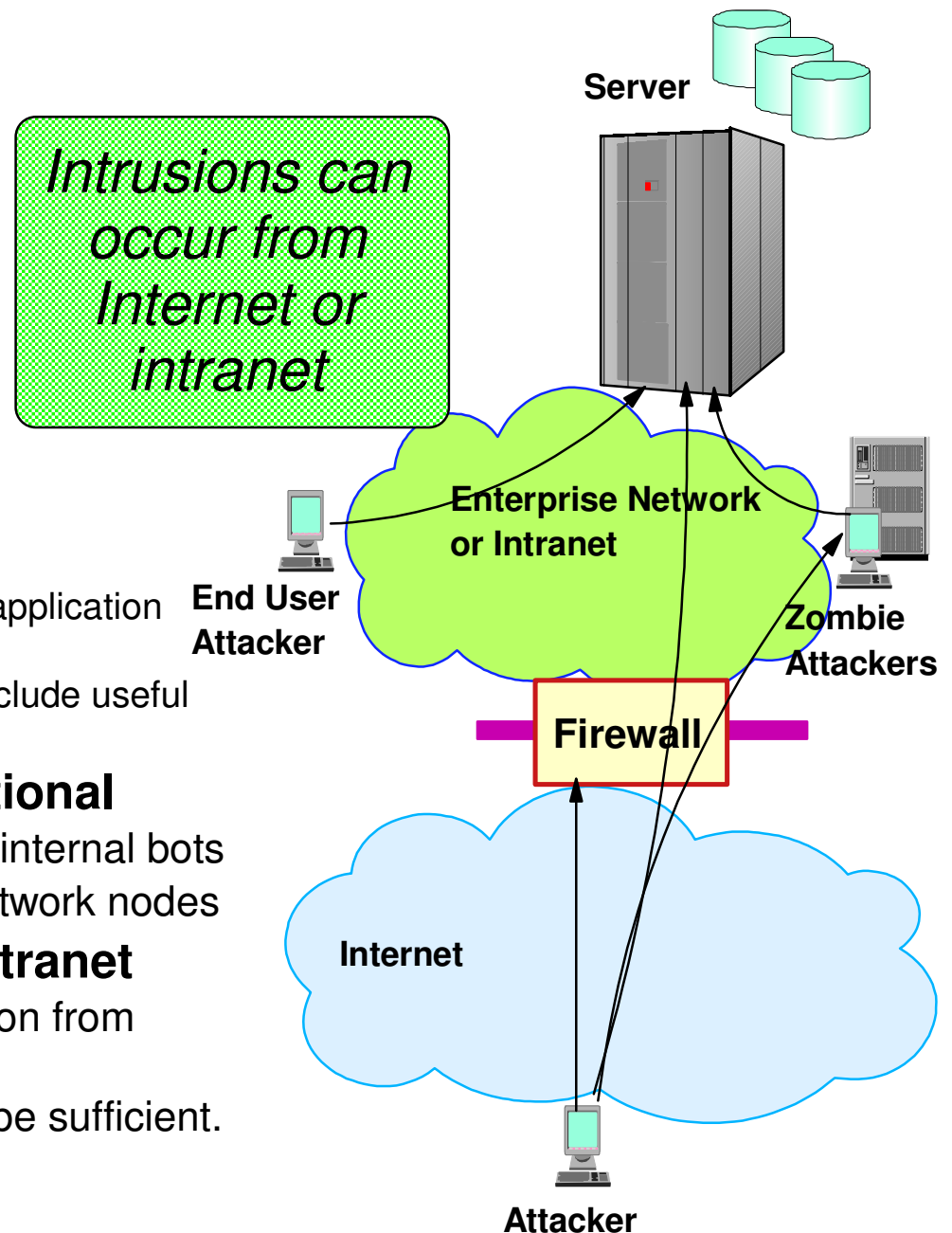
Attacker

Intrusion Detection Services Overview

IDS policy

IDS Policy administration

Policy Agent

TRMD

Log event and statistics

trmdstat utility

Detail and summary reports

Install IDS policies into TCP/IP stack

TCP/UDP/RAW

IP/ICMP

Attack probes

SyslogD

Intrusion event notification

Data Link

Security Administrator

z/OS NetView

Dynamic trace of suspicious activity

Trace

Event messages to MVS console

Attack!!!

Automation based on MVS console messages

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

Defensive methods
- Packet discard
- Limit connections
- Reset connections

Reporting
- Logging,
- Event messages to local console,
- IDS packet trace
- Notifications to Tivoli NetView

IDS Policy
- Samples provided with Configuration Assistant for z/OS Communications Server

Integrated Intrusion Detection Services under policy control to identify, alert, and document suspicious activity

z/OS in-context IDS broadens overall intrusion detection coverage:
- Ability to evaluate inbound encrypted data - IDS applied after IPSec decryption on the target system
- Avoids overhead of per packet evaluation against table of known attacks - IDS policy checked after attack detected
- Detects statistical anomalies real-time - target system has stateful data / internal threshholds that are generally unavailable to external IDSs
- Policy can control prevention methods on the target, such as connection limiting and packet discard

z/OS Communications Server Security

Intrusion Events Types Detected

- **SCAN**

- **ATTACK**

- **TRAFFIC REGULATION**

Intrusion Event Types Supported

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

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

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

Scanning... the prelude to the attack

- z/OS IDS definition of a scanner
  - Source host that accesses <u>multiple unique resources</u> (ports or interfaces) over a <u>specified time period</u>
    - Installation can specify via policy number of unique events (Threshold) and scan time period (Interval)

- Categories of scan detection supported
  - Fast scan
    - Many resources rapidly accessed in a short time period (less than 5 minutes)
      - ✓ usually less than five minutes, program driven
  - Slow scans
    - Different resources intermittantly accessed over a longer time period (many hours)
      - ✓ scanner trying to avoid detection

- Scan event types supported
  - ICMP, ICMPv6 scans
  - TCP port scans
  - UDP port scans

Scan Policy Overview

Scan policy provides the ability to:

- Obtain notification and documentation of scanning activity
    - ➤ Notify the installation of a detected scan via console message or syslogd message
    - ➤ Trace potential scan packets

- Control the parameters that define a scan:
    - ➤ The time interval
    - ➤ The threshold number of scan events

- Reduce level of false positives
    - ➤ Exclude well known "legitimate scanners" via exclusion list
        - – e.g. network management
    - ➤ Specify a scan sensitivity level
        - – by port for UDP and TCP
        - – highest priority rule for ICMP, ICMPv6

Scan Event Counting and Scan Sensitivity

- Each scan event is internally classified as normal, suspicious or very suspicious
  - ➤ Socket state, ICMP, ICMPv6 type affect this classification
    - *Scan instance event classification by event type included in IP Configuration Guide.*
- Scan sensitivity determines whether a scan event is "countable"

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

- Countable scan events count against an origin source IP address
  - ➤ Total number of countable events for all scan event types is compared to policy thresholds
    - If threshold exceeded for a single IP address, policy-directed notification and documentation is triggered

Attacks Against The TCP/IP Stack

- The system already silently defends itself from many attacks against the TCP/IP stack.

- IDS adds capability to control recording of intrusion events and to provide supporting documentation.

- IDS adds controls to detect and disable uncommon or unused features which could be used in an attack.

Attack Categories

- **Malformed packet events**
  - ➤ Detects IPv4 and IPv6 packets with incorrect or partial header information
- **Inbound fragment restrictions**
  - ➤ Detects fragmentation in first 88 bytes of an IPv4 datagram
    - – *z/OS V2R1 changes the fragmentation attack probe to no longer consider fragment length as a criteria. Checks will be based purely on whether overlays occur and whether they change the packet content.*
- **IPv4 and IPv6 protocol restrictions**
  - ➤ Detects use of IP protocols you are not using that could be misused
  - ➤ Called "next header restrictions" for IPv6
- **IPv4 and IPv6 option restrictions**
  - ➤ Detects use of IP options you are not using that could be misused
  - ➤ Can restrict both destination and hop-by-hop options for IPv6
- **ICMP, ICMPv6 redirect restrictions**
  - ➤ Detects receipt of ICMP redirect to modify routing tables.

- **UDP perpetual echo**
  - ➤ Detects traffic between IPv4 and IPv6 UDP applications that unconditionally respond to every datagram received
- **Outbound RAW socket restrictions**
  - ➤ Detects z/OS IPv4 or IPv6 RAW socket application crafting invalid outbound packets
- **Flood Events**
  - ➤ Detects flood of SYN packets from "spoofed" IPv4 or IPv6 sources
  - ➤ Detects high percentage of packet discards on a physical IPv4 or IPv6 interface
- **Data hiding**
  - ➤ Detects attempts to pass hidden data in packet header and extension fields
- **TCP queue size**
  - ➤ Detects queue size constraints for individual connections
- **Global TCP stall**
  - ➤ Detects cases where large number and percentage of TCP connections are stalled
- **Enterprise Extender-specific attacks**
  - ➤ Malformed Packet
  - ➤ LDLC Check
  - ➤ Port Check
  - ➤ EE XID Flood

Attack Policy Overview

Attack policy provides the ability to:

- Control attack detection for one or more attack categories independently

- Generate notification and documentation of attacks
  - ➤ Notify the installation of a detected attack via console message or syslogd message
  - ➤ Trace potential attack packets

- Generate attack statistics on time interval basis
  - ➤ Normal or Exception

- Control defensive action when attack is detected

Interface Flood Detection

- Packet discard rate by physical interface is tracked to determine if there is a potential attack
  - A high percentage of discarded packets on a physical interface may indicate the interface is under attack.

- Notification and traces provided when a possible interface flood condition is occurring (according to the discard threshold value).

- Provides information to help determine the potential cause of the interface flood
  - Narrows flood condition to a local interface so you can
    - Vary the interface offline
      - ✓ This action not controlled with IDS policy
    - Start tracing flood back to source
  - Source MAC address of the "prior hop" (for OSA QDIO and LCS devices)
  - Source IP address from the outer IPSec header if the packet had been received as IPsec tunnel mode.
    - Source IP address could be a gateway or firewall
      - ✓ Could allow source tracking closer to the source than "prior hop"

Interface Flood Detection Process

- Policy related to interface flood detection
  - Specified on Attack Flood policy
  - 2 actions attributes provided
    - Flood minimum discard (default 1000)
    - Flood percentage (default 10)

- For each interface, counts are kept for
  - The number of inbound packets that arrived over the physical interface
  - The number of these packets that are discarded

- When the specified number of discards (flood minimum discard) is hit:
  - If the discards occurred within **one minute** or less:
    - the discard rate is calculated for the interval :
      - ✓ # discards during the interval / # inbound packets for the interval
    - If the discard rate equals or exceeds the specified flood percentage threshold, an interface flood condition exists
  - If discards occurred during period longer than 1 minute, not a flood condition

- Once an interface flood is detected, this data is collected and evaluated for the interface at 1 minute intervals. The interface flood is considered ended if
  - The discards for a subsequent interval fall below the minimum discard value   OR
  - Discard rate for the interval is less than or equal to 1/2 of the specified flood percentage threshold

Interface Flooding Example

- Assume the IDS flood policy specifies:
  - Flood minimum discard: 2000
  - Flood percentage:10%

- Consider the following sequence for interface X:

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

time

Traffic Regulation for TCP

- Allows control over number of inbound connections from a single host
  - ► Can be specified for specific application ports
    - – Especially useful for forking applications
  - ► Independent policies for multiple applications on the same port
    - – e.g. telnetd and TN3270

- Connection limit expressed as
  - ► Port limit for all connecting hosts AND
  - ► Individual limit for a single connecting host

- Fair share algorithm
  - ► Connection allowed if specified individual limit per single remote IP address does not exceed percent of available connections for the port
    - – All remote hosts are allowed at least one connection as long as port limit has not been exceeded
      - ✓ QoS connection limit used as override for concentrator sources (web proxy server)

TCP connection regulation algorithm

Configured maximum allowed connections for a given port: **N**

In-use connections

Available connections: **A**

Configured controlling percentage: **CP**

Connections from
a given source IP
address: IP@x: **X**
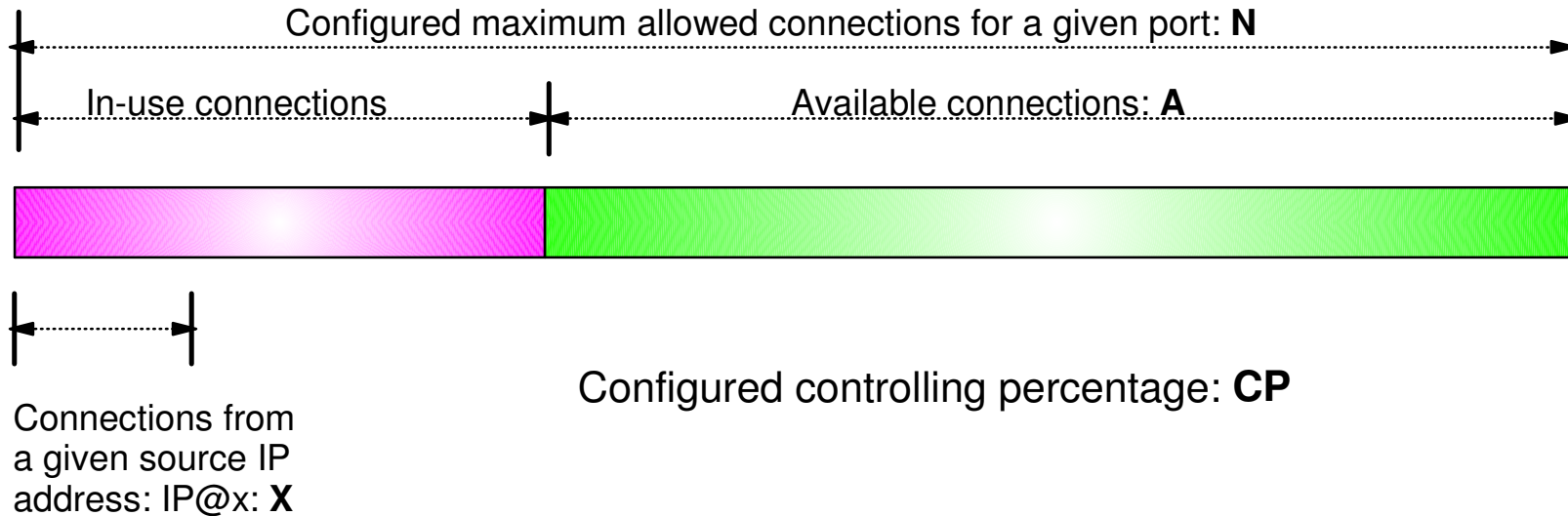
If a new connection request is received and A=0, the request is rejected.

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

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

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

Regulation algorithm example

Source IP address X attempts its fifth connection

Allowed   Rejected

Total Allowed	Connections	Available	CP=10%	CP=20%	CP=30%
100	20	80	8	16	24
100	40	60	6	12	18
100	60	40	4	(A) 8	12
100	80	20	2	4 (B)	6
100	90	10	1	2	3

(A) If we currently have 40 connections available (A=40) and a controlling percentage (CP) of 20%, when source IP address X tries to establish its fifth connection, it will be allowed (40 * 20% = 8, so 5 connections is within the acceptable range).

(B) If we have 20 connections available (A) and CP is again 20%, when source IP address X tries to establish its fifth connection, it will be rejected (20 * 20% = 4, so 5 would exceed the allowable number of connections).

Traffic Regulation for UDP

- Allows control over length of inbound receive queues for UDP applications
  - ➤ Specified on a per-port basis
  - ➤ Can be applied to ports of your choosing

- Before TR for UDP, UDP queue limit control was requested globally for all queues
  - ➤ UDPQueueLimit ON | OFF in TCP/IP Profile

- If neither TR UDP or UDPQueueLimit is used, a stalled application or a flood against a single UDP port could consume all available buffer storage
  - ➤ TR UDP supercedes UDPQueueLimit specification

- TR UDP queue limit expressed as abstract queue length
  - ➤ SHORT or VERY SHORT
    - For applications that tend to receive data faster than they can process it
  - ➤ LONG or VERY LONG
    - Useful for fast or high priority applications with bursty arrival rates

z/OS Communications Server Security

IDS Actions

- **Recording actions**

- **Defensive actions**

Recording Actions

- Recording options controlled by IDS policy action specification

- Possible options
  - Event logging
    - Syslogd
      - ✓ Number of events per <u>attack subtype</u> recorded in a five minute interval can be limited (for most attack subtypes)
    - Local Console
      - ✓ Recording suppression provided if quantity of IDS console messages reach policy-specified thresholds
  - Statistics
    - Syslogd
      - ✓ Normal and Exception conditions
  - IDS packet trace
    - Activated <u>after</u> attack detected
      - ✓ Number of packets traced for multipacket events are limited
      - ✓ Amount of data trace is configurable (header, full, byte count)
    - Not available for all attack types

- All IDS events recorded in syslog and console messages, and packet trace records have <u>probeid</u> and <u>correlator</u>
  - Probeid identifies the point at which the event detected
  - Correlator allows association of corresponding syslog and packet trace records

Defensive Actions by Event Type

- Attack Events
  - ➤ Packet discard
    - – Certain attack events always result in packet discard and are <u>not</u> controlled by IDS policy action
      - ✓ malformed packets
      - ✓ flood (synflood discard)
    - – Most attack types controlled by IDS policy action
      - ✓ ICMP redirect restrictions
      - ✓ IPv4 and IPv6 option restrictions
      - ✓ IPv4 and IPv6 protocol restrictions
      - ✓ IP fragment
      - ✓ outbound raw restrictions
      - ✓ perpetual echo
      - ✓ data hiding
      - ✓ EE malformed, LDLC and port checks
  - ➤ Reset connection
    - ✓ TCP queue size
    - ✓ Global TCP stall
  - ➤ No defensive action defined
    - ✓ flood (interface flood detection)

- Scan Events
  - ➤ No defensive action defined

- Traffic Regulation Events
  - ➤ Controlled by IDS policy action
    - – TCP - Connection limiting
    - – UDP - Packet discard

IDS and Defensive Filtering

- **The Defense Manager component allows authorized users to dynamically install time-limited, defensive filters:**
  - ➤ A local security administrator can install filters based on information received about a pending threat
  - ➤ Enables filter installation through automation based on analysis of current attack conditions
- **Defensive filtering is an extension to IDS capabilities**
  - ➤ Adds additional defensive actions to protect against attacks

z/OS
Security
Administrator

ipsec command

z/OS Defense Manager

DM defensive filter database

Maintain defensive filters

Initial filters installed via TCP/IP Profile and/or Policy Agent

Applications

TCP, UDP **IDS**

IP **IDS**

Filter rules

Network Interfaces

Enable dynamic defensive actions on z/OS
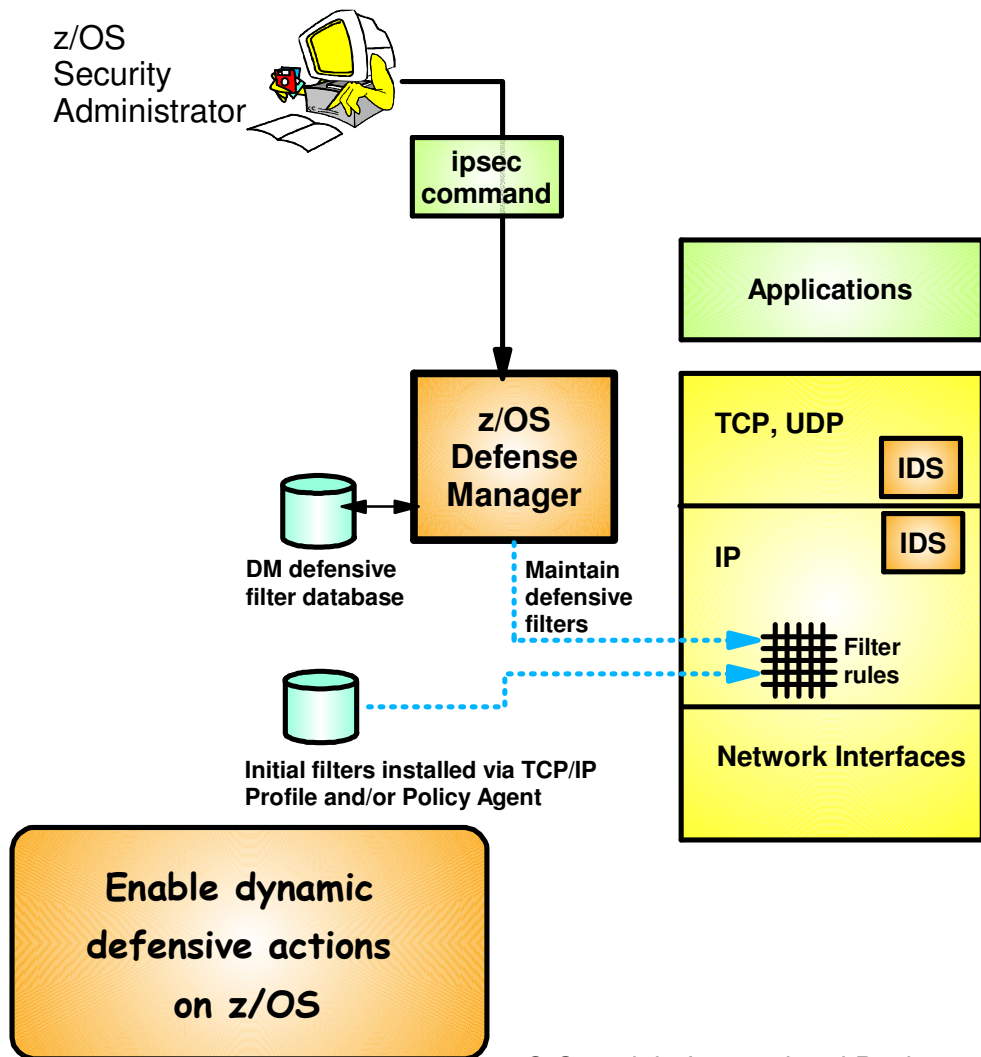
- **Requires minimal IP Security configuration to enable IP packet filtering function**
  - ➤ Uses ipsec command to control and display defensive filters
- **Defense Manager**
  - ➤ Manages installed defensive filters in the TCP/IP stack
  - ➤ Maintains record of defensive filters on DASD for availability in case of DM restart or stack start/restart
- **Defensive filter scope may be:**
  - ➤ Global - all stacks on the LPAR where DM runs
  - ➤ Local - apply to a specific stack
- **Defensive filter are installed "in-front" of configured/default filters**

z/OS Communications Server Security

Intrusion Detection Reports for Analysis

IDS Log Reports

trmdstat command produces reports based on IDS data recorded in syslog

- Types of reports generated for logged events
  - Overall summary reports
    - IDS
  - Event type <u>summary</u> reports
    - For Attack, Flood, Scan, TCP and UDP TR information
  - Event type <u>detail</u> reports
    - For Attack, Flood, Scan, TCP and UDP TR information

- Types of reports generated for statistics events
  - Details reports
    - Attack, Flood, TCP and UDP TR reports

Tivoli Support for IDS Events

- Tivoli NetView provides local z/OS management support for IDS

- NetView provides ability to trap IDS messages from the system console or syslog and take predefined actions based on IDS event type such as:

  - ➤ Route IDS messages to designated NetView consoles

  - ➤ email notifications to security admistrator

  - ➤ Run trmdstat and attach output to email

  - ➤ Issue pre-defined comands

z/OS Communications Server Security

Working with IDS Policy

- **Controlling, displaying, and validating policy**

- **Defining IDS policy**

- **IDS policy configuration with Configuration Assistant for z/OS Communications Server example**

Controlling Active IDS Policy

- **Configurable** <u>policy deletion controls</u> in Policy Agent configuration file
  - ➤ TcpImage statement
    - – FLUSH | NOFLUSH {PURGE | NOPURGE}
  - ➤ FLUSH and NOFLUSH take effect at Policy Agent initialization
    - – FLUSH - specifies that any active policy should be deleted
    - – NOFLUSH - specifies that active policy should not be deleted
  - ➤ PURGE and NOPURGE take effect at Policy Agent termination
    - – PURGE - specifies that any active policy should be deleted
    - – NOPURGE - specifies that active policy should not be deleted

- **Refresh Policy**
  - – At Interval (1800-second default) specified on TcpImage statement
  - – With MODIFY PAGENT command (REFRESH option)
  - – When Policy Agent configuration file (HFS only) is updated (refresh is automatic)

Displaying IDS Policy

- **pasearch command**
  - ➤ Displays IDS policy read by Policy Agent

- **netstat command**
  - ➤ Displays installed IDS policy in TCP/IP stack
  - ➤ Displays statistics by policy category

✓Tip:

Restrict access to IDS policy displays using SAF SERVAUTH resources:
  - ➤ EZB.PAGENT.sysname.tcpname.IDS
  - ➤ EZB.NETSTAT.sysname.tcpname.IDS

Steps for Validating IDS Policy

1. Initially configure policy for reporting actions only (no defensive actions)

2. Invoke PAGENT and TRMD

3. Issue PASEARCH and verify that the correct policy is installed

4. Keep policy in force for a trial period

5. Issue IDS netstat to view active IDS policy and statistics

6. Run TRMDSTAT reports to verify syslog messages for intrusion events

7. Adjust the policy as required

8. Add defensive actions

Configuration Assistant for z/OS Communications Server
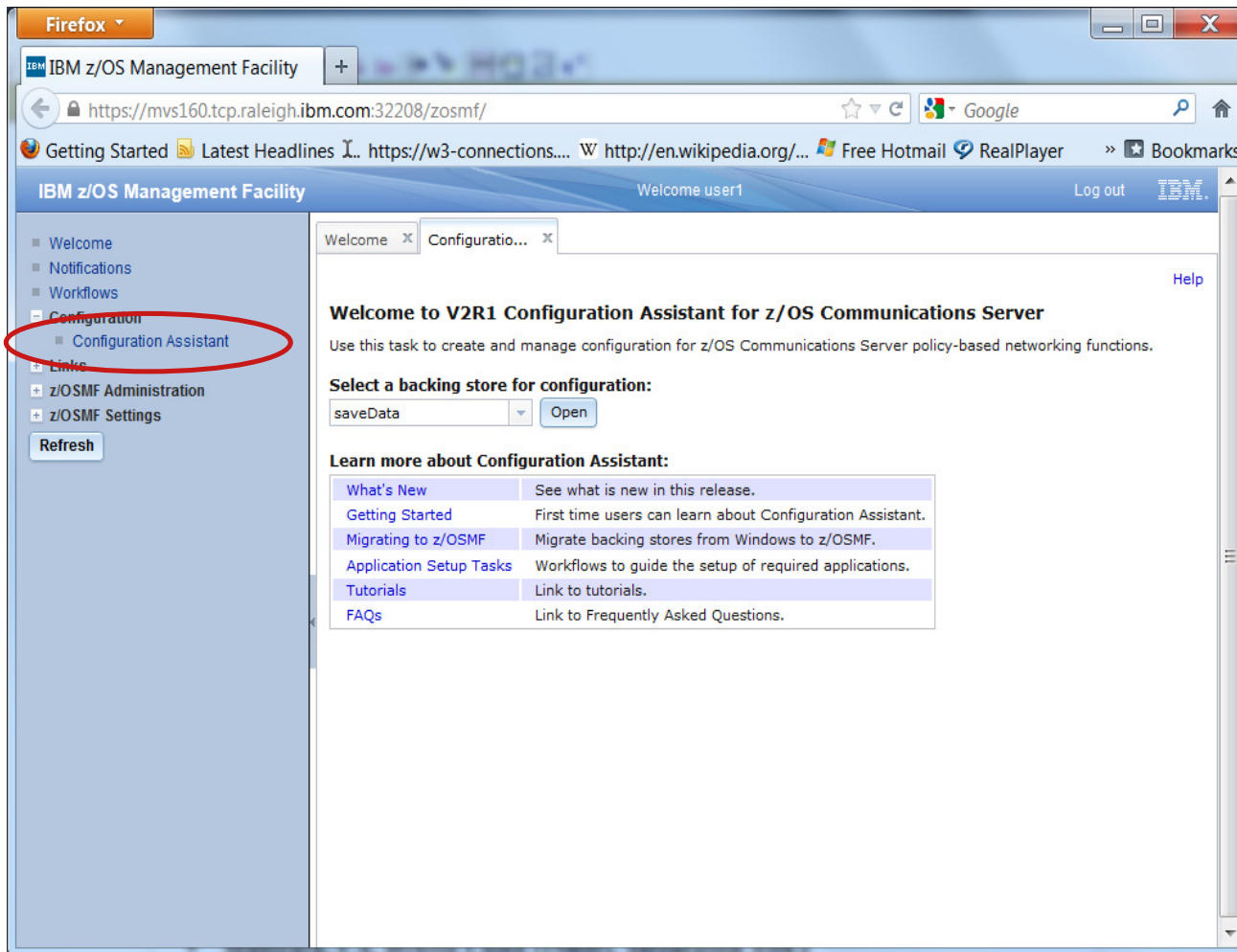
- **GUI-based approach to configuring:**
  - ➤ IDS
  - ➤ AT-TLS
  - ➤ IPSec and IP filtering
  - ➤ QoS
  - ➤ Policy-based Routing
- **Focus on high level concepts vs. low level file syntax**
- **Available through z/OSMF-based web interface**
  - ➤ Standalone Windows application
    - – Not supported after z/OS V1R13
- **Builds and maintains**
  - ➤ Policy files
  - ➤ Related configuration files
  - ➤ JCL procedures and RACF directives
- **Supports import of existing policy files**

IDS Policy Configuration Steps with the Configuration Assistant

1. Configure IDS policies
   a. Examine IDS defaults and base policy on defaults
   b. Copy IDS defaults into a new IDS requirements map
   c. Make changes to new requirements map as needed

2. Create system image and TCP/IP stack image

3. Associate new requirements map with TCP/IP stack

4. Transfer IDS policy to z/OS

5. Perform policy infrastructure and application setup tasks

Configuration Assistant for z/OS Communications Server

Start a new IDS configuration - create a new backing store

Create IDS policy objects -
select the IDS policy perspective

Traffic Descriptors

Welcome ✕ | Configuratio... ✕

Configuration Assistant (Home) ▶ IDS

V2R1 Current Backing Store = idsdemoLHO

Select a perspective: IDS ▾   Tools ▾

System | **Traffic Descriptors** | Requirement Maps

Actions ▾

Name Filter	▲	Description Filter
○ All_Well-Known_TCP		IBM supplied: All Well-Known TCP Traffic
○ All_Well-Known_UDP		IBM supplied: All Well-Known UDP Traffic
○ Centralized_Policy_Server		(VERIFY) IBM supplied: Centralized Policy Server
○ CICS		(VERIFY) IBM supplied: CICS traffic
○ DNS		(VERIFY) IBM supplied: Domain Name Server traffic
○ EE		IBM supplied: Enterprise Extender (EE) traffic
○ FTP-Server		(VERIFY) IBM supplied: FTP Server traffic
○ FTP-Server-SSL		(VERIFY) IBM supplied: FTP Server SSL traffic using port 990
○ ICMP		IBM supplied: ICMP IPv4 traffic
○ ICMP-IPv6		IBM supplied: ICMP IPv6 traffic
○ IKE		IBM supplied: Internet Key Exchange daemon traffic
○ IKE-NAT		IBM supplied: NAT - Internet Key Exchange daemon traffic
○ Kerberos		(VERIFY) IBM supplied: Kerberos Server traffic
○ LBA-Advisor		(VERIFY) IBM supplied: z/OS Load Balancing Advisor traffic
○ LBA-Agent		(VERIFY) IBM supplied: z/OS Load Balancing Advisor - Agent traffic
○ LDAP-Server		(VERIFY) IBM supplied: LDAP Server traffic
○ LPD		IBM supplied: LPD Server traffic
○ NSS_Server		(VERIFY) IBM supplied: Network Security Services server traffic
○ Portmap-Server		IBM supplied: Portmap Server traffic
○ REXEC-Server		IBM supplied: REXEC - Remote Execution Server
○ RSH-Server		IBM supplied: RSH - Remote Shell Server
○ SMTP		IBM supplied: Simple Mail Transfer Protocol (SMTP) Server
○ SNMP-Agent		IBM supplied: Simple Network Management Protocol (SNMP) Agent traffic

Total: 28, Selected: 0

Evalute IDS_Default requirements map

IDS_Default provided as default requirement map
- Display details of the requirement map
- Evaluate whether they meet your requirements

Details view of IDS_Default requirements map (1 of 4)

Welcome ✕   Configuratio... ✕

Configuration Assistant (Home) ▸ IDS ▸ View Details

View Details

[Close]

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

Attack Protection Summary

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	**Console Parameters:** No
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	**SYSLOG Parameters:** SYSLOG: Yes SYSLOG Level: 4 - Warning
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	**Statistics Parameters:** Statistics: Yes
IPv4 Options Attack	IPv4Option	Report Events	Use Default Report Settings	None	Statistics Interval: 60 Minutes
ICMP Redirect Attack	ICMPRedirect	Report Events	Use Default Report Settings	None	Report Stat if no events: Yes
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	**Trace Parameters:** No
IP Fragment Attack	Fragmentation	Report Events	Use Default Report Settings	None	
EE Malformed Packet Attack[1]	EEMalformedPacket	Report Events	Use Default Report Settings	None	
EE LDLC Check Attack[1]	EELDLCCheck	Report Events	Use Default Report Settings	None	
EE Port Check Attack[1]	EEPortCheck	Report Events	Use Default Report Settings	None	
EE XID Flood Attack[1]	EEXIDFlood	Report Events	Use Default Report Settings	None	

Footnotes:
1 The attack is not available for V1R12 stacks. The requirement map is configured with this attack, but if the stack is mapped to a V1R12 stack, the attack will be ignored.
===

Attack Protection Details

Enabled Attack Protection: Data Hiding Attack - DataHiding

Enabled Options	Reports	Time Condition	Action
Checking of IP option pad fields: Enabled Checking of embedded packets within ICMP error messages: Enabled	Use Default Report Settings	None	Report Events

The attack is not available for V1R12 stacks. The requirement map is configured with this attack, but if the stack is mapped to a V1R12 stack, the attack will be ignored.

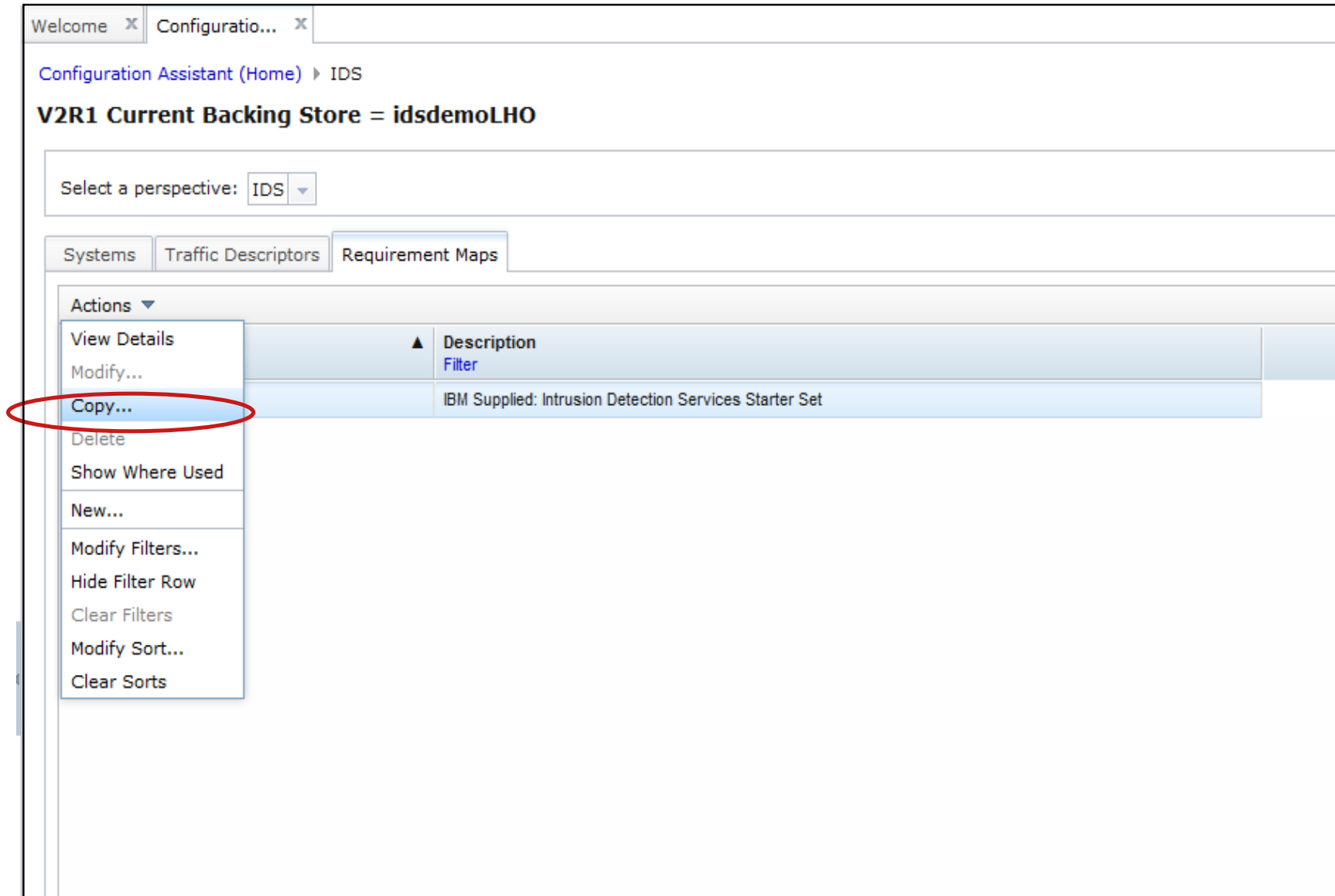# Details view of IDS_Default requirements map (2 of 4)

Configuration Assistant (Home) ▸ IDS ▸ View Details

View Details

Attack Protection Details

Enabled Attack Protection: Data Hiding Attack - DataHiding

Enabled Options	Reports	Time Condition	Action
Checking of IP option pad fields: Enabled Checking of embedded packets within ICMP error messages: Enabled	Use Default Report Settings	None	Report Events

The attack is not available for V1R12 stacks. The requirement map is configured with this attack, but if the stack is mapped to a V1R12 stack, the attack will be ignored.

Enabled Attack Protection: IPv6 Outbound Raw Attack - IPv6OutboundRaw

Starting Protocol	Ending Protocol	Reports	Time Condition	Action
0	16			
18	57			
59	88	Use Default Report Settings	None	Report Events
90	255			

The attack is not available for V1R12 stacks. The requirement map is configured with this attack, but if the stack is mapped to a V1R12 stack, the attack will be ignored.

Enabled Attack Protection: IPv6 Destination Options Attack - IPv6DestinationOptions

Starting Option	Ending Option	Reports	Time Condition	Action
2	3			
8	137			
139	193	Use Default Report Settings	None	Report Events
195	200			
202	255			

The attack is not available for V1R12 stacks. The requirement map is configured with this attack, but if the stack is mapped to a V1R12 stack, the attack will be ignored.

Enabled Attack Protection: IPv6 Hop-by-Hop Options Attack - IPv6HopByHop

Starting Option	Ending Option	Reports	Time Condition	Action
2	3			
8	137			
139	193	Use Default Report Settings	None	Report Events
195	200			
202	255			

The attack is not available for V1R12 stacks. The requirement map is configured with this attack, but if the stack is mapped to a V1R12 stack, the attack will be ignored.

Details view of IDS_Default requirements map (3 of 4)

Welcome ×   Configuratio... ×

Configuration Assistant (Home) ▸ IDS ▸ View Details

View Details

Enabled Attack Protection: IPv6 Next Header Attack - IPv6NextHeader

Starting Next Header	Ending Next Header	Reports	Time Condition	Action
1	5			
7	16			
18	40			
42	42			
45	49	Use Default Report Settings	None	Report Events
52	57			
61	88			
90	134			
136	255			

The attack is not available for V1R12 stacks. The requirement map is configured with this attack, but if the stack is mapped to a V1R12 stack, the attack will be ignored.

Enabled Attack Protection: TCP Queue Size Attack - TcpQueueSize

TCP Queue Size	Reports	Time Condition	Action
Short	Use Default Report Settings	None	Report Events

The attack is not available for V1R12 stacks. The requirement map is configured with this attack, but if the stack is mapped to a V1R12 stack, the attack will be ignored.

Enabled Attack Protection: Global TCP Stall Attack - GlobalTCPStall

Reports	Time Condition	Action
Use Default Report Settings	None	Report Events

The attack is not available for V1R12 stacks. The requirement map is configured with this attack, but if the stack is mapped to a V1R12 stack, the attack will be ignored.

Enabled Attack Protection: Flood Attack - Flood

Flood Minimum Discard	Flood Percentage	Reports	Time Condition	Action
1000	10	Use Default Report Settings	None	Both Drop and Report

Enabled Attack Protection: Perpetual Echo Attack - Echo

Traffic Descriptor	Port Location	Reports	Time Condition	Action
7 - Echo	Both Local and Remote			
13 - Time Of Day	Both Local and Remote	Use Default Report Settings	None	Report Events
17 - Quote Of The Day	Both Local and Remote			
19 - Char Gen	Both Local and Remote			

Details view of IDS_Default requirements map (4 of 4)

(... several intervening pages)

Use IDS_Default as a starting point

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

Name new requirements map

Configuration Assistant (Home) ▶ IDS ▶ Requirement Map

Copy Requirement Map

Name	Attacks	Scans	Traffic Regulation

* Name:

IDS_policy_demo

Description:

Show how to configure IDS policy

The wizard will guide you through the required configuration steps and collect the following information:

- Attack protection
- Pre-attack scan monitoring
- Traffic regulation

OK   Cancel

Modify copied default requirements map
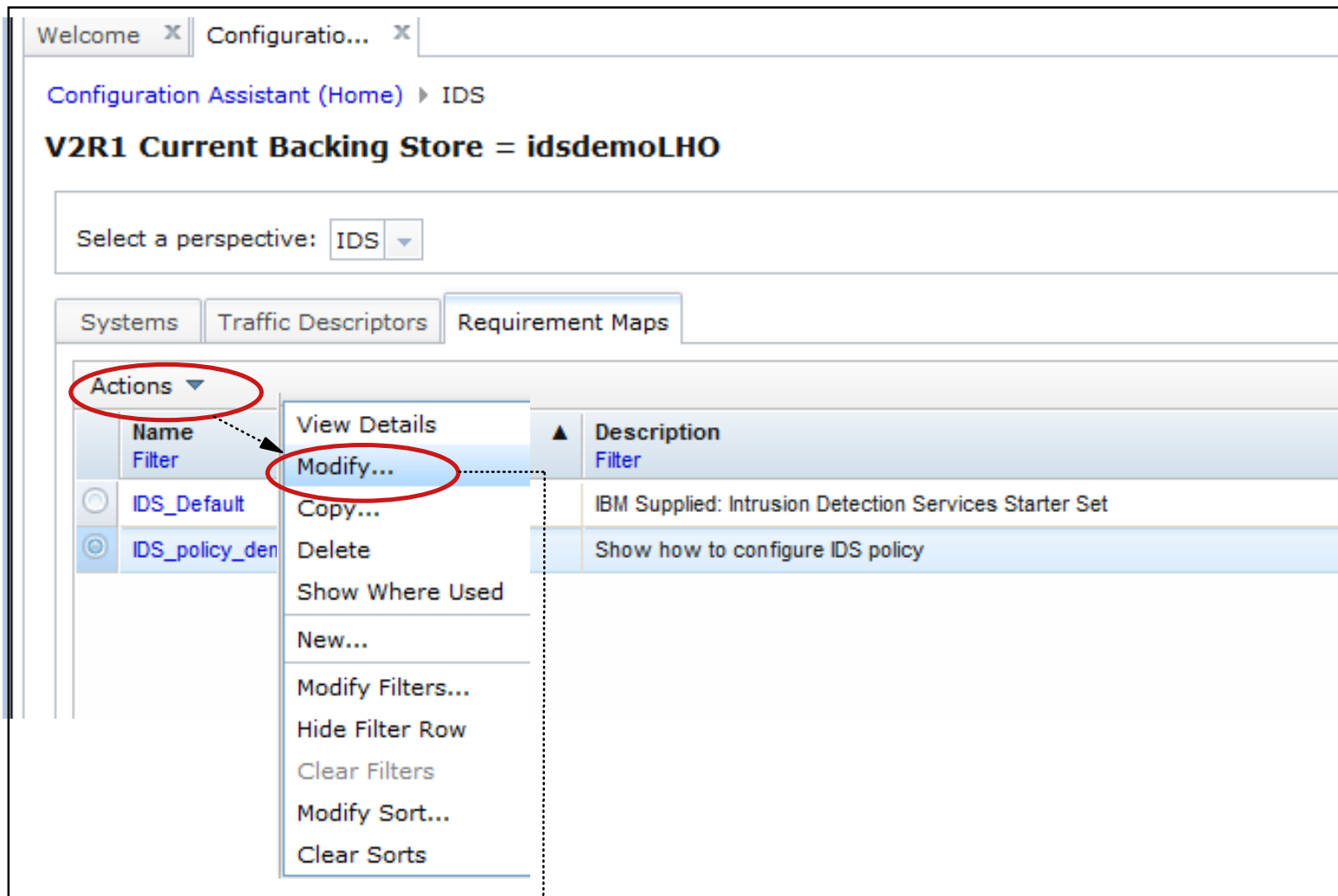
next page

Attack protection enabled by default

Welcome | Configuratio...

Configuration Assistant (Home) ▸ IDS ▸ Requirement Map

Modify Requirement Map

Name | **Attacks** | Scans | Traffic Regulation

☑ Enable attack protection

▸ **Steps**

Actions ▾

	Attack Type	Rule Name	Action
○	Data Hiding Attack	DataHiding	Report Events
○	IPv6 Outbound Raw Attack	IPv6OutboundRaw	Report Events
○	IPv6 Destination Options Attack	IPv6DestinationOptions	Report Events
○	IPv6 Hop-by-Hop Options Attack	IPv6HopByHop	Report Events
○	IPv6 Next Header Attack	IPv6NextHeader	Report Events

Total: 19, Selected: 0

Default report settings for Attacks... ┄┄► next page

OK   Cancel

Customize report settings

Enable scan policy

next page

Modify global scan settings

Enable traffic regulation protection

No traffic regulation defaults
- Policy selections are system dependant
- System capacity a consideration in setting maximum limits

Define TCP TR policy for FTP

Set details for TR

New Traffic Regulation Details

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

Traffic regulation identification

* Name   FTP-Server
* Traffic Descriptor   FTP-Server
Action   Limit and Report

Enter parameters for TCP traffic

*Max number of connections: 100   (0-65535)
*Limit each host to the following percentage of the available connections: 20
Limit scope: All sockets

OK   Cancel

Traffic regulation enabled

IDS_policy_demo requirements map now created

Welcome ✕ | Configuratio... ✕

Configuration Assistant (Home) ▶ IDS

V2R1 Current Backing Store = idsdemoLHO

Select a perspective: IDS ▾

| Systems | Traffic Descriptors | **Requirement Maps** |

Actions ▾

	Name ▲ Filter	Description Filter
○	IDS_Default	IBM Supplied: Intrusion Detection Services Starter Set
◉	IDS_policy_demo	Show how to configure IDS policy

Create system image

Create TCP/IP stack

Welcome X | Configuratio... X

Configuration Assistant (Home) ▸ IDS

V2R1 Current Backing Store = idsdemoLHO

Select a perspective: IDS ▾

| Systems | Traffic Descriptors | Requirement Maps |

Actions ▾

Name	Type	Status	Release	Description
▪ IDSDEMO	Image	Complete	V2R1	IDS Demo System

Proceed to the Next Step?

? IDS requirement maps are configured for each TCP/IP stack. To continue with configuration you need to add a TCP/IP stack to the new z/OS image. Do you want to add a TCP/IP stack now?

Cancel | Proceed

Welcome X | Configuratio... X

Configuration Assistant (Home) ▸ IDS ▸ TCP/IP Stack

Add TCP/IP Stack

* Name:

IDSSTACK

Description:

IDS Demo Stack

next page ◂

OK | Cancel

Associate TCP/IP stack with requirements map

Welcome ✕ | Configuratio... ✕

V2R1 Current Backing Store = idsdemoLHO

Select a perspective: IDS ▾

| Systems | Traffic Descriptors | Requirement Maps |

Actions ▾

	Name	Type	Status	Release	Description
◯	⊟ IDSDEMO	Image	Complete	V2R1	IDS Demo System
◉	▪ IDSSTACK	Stack	Complete	V2R1	IDS Demo Stack

Proceed to the Next Step?

? The stack is now configured to use the IDS_Default requirement map protection. To change the level of protection you can select a different requirement map for this stack. Click Proceed if you would like to be directed to the stack requirement map panel

Cancel | Proceed

Welcome ✕ | Configuratio... ✕

Help

Requirement Maps for Image IDSDEMO, Stack IDSSTACK

Use this panel to select a requirement map to govern IDS protection for this stack.

Steps:

- To change the selected requirement map, use the **Select a requirement map** list to make the change. Click **Apply** to activate the selection choice.
- To disable IDS protection, use the **Select a requirement map** list and select **No requirement map is selected**.
- Use the **Actions** list to select an action to configure IP addresses or view the details of the selected requirement map. A health check action is also available.

Select a requirement map:

IDS_Default ▾ | Apply

No requirement map is selected - IDS is disabled
IDS_Default
IDS_policy_demo

Install configuration files

next page

Show the configuration file to be installed

Configuration Assistant (Home) ▸ IDS ▸ Configuration Files

List of Configuration Files for All Images

List of Configuration Files for All Images

Actions ▼			
Show Configuration File...	ration	**File Name**	**Host N**
Install...	K - IDS Policy	/etc/cfgasst/v2r1/IDSDEMO/IDSSTACK/idsPol	
Configuration Summary...			

Welcome ✕ | Configuratio... ✕

Configuration Assistant (Home) ▸ IDS ▸ Configuration Files ▸ Configuration File

Configuration File

[Close]

```
##
## IDS Policy Agent Configuration file for:
##     Image: IDSDEMO
##     Stack: IDSSTACK
##
## Created by the IBM Configuration Assistant for z/OS Communications Server
## Version 2 Release 1
## Backing Store = idsdemoLHO
## Install History:
##
## End of Configuration Assistant information

IDSRule              DataHiding
{
ConditionType        Attack
IDSAttackCondition
{
    AttackType           DATA_HIDING
    OptionPadChk         Enable
    IcmpEmbedPktChk      Enable
}
IDSActionRef         DataHiding
}

IDSRule              IPv6OutboundRaw
{
ConditionType        Attack
IDSAttackCondition
{
    AttackType           OUTBOUND_RAW_IPv6
    ProtocolGroupRef     IpProtGroup~1
}
IDSActionRef         IPv6OutboundRaw
}

IDSRule              IPv6DestinationOptions
{
ConditionType        Attack
IDSAttackCondition
{
    AttackType           RESTRICTED_IPV6_DST_OPTIONS
    RestrictedIpv6OptionGroupRef IpOptGroup~1
}
IDSActionRef         IPv6DestinationOptions
}

IDSRule              IPv6HopByHop
{
ConditionType        Attack
IDSAttackCondition
```

Set up to install configuration files on target z/OS system

List of Configuration Files for All Images

Welcome ✕ | Configuratio... ✕

Configuration Assistant (Home) ▶ IDS ▶ Configuration Files

List of Configuration Files for All Images

List of Configuration Files for All Images

Actions ▼		
Show Configuration File...	ration	File Name
Install...	K - IDS Policy	/etc/cfgasst/\
Configuration Summary...		

Install File

Welcome ✕ | Configuratio... ✕

Configuration Assistant (Home) ▶ IDS ▶ Configuration Files ▶ Install

Install File

* Install file name:

`/etc/cfgasst/v2r1/IDSDEMO/IDSSTACK/idsPol`

Select installation method
- ◉ Save to disk
- ○ FTP

FTP information

    * Host name: [_____]

    * Port number: [21_____]

    * User ID: [_____]

    * Password: [_____] ☑ Save password

    ☐ Use SSL

    ☐ Create the directories if they do not exist

Data transfer mode
◉ Default ○ Passive ○ Active

Comment for the configuration file prologue (optional)

[_____]

[Go] [Close] [View FTP Log]

Perform application setup tasks - All workflows view

next page

Perform application setup tasks - Specific workflow view

z/OS Communications Server Security

Features Summary

IDS Features Summary

- **IDS events detected include:**
  - ➤ Scan detection
  - ➤ Attack detection
  - ➤ Traffic Regulation
  - ... for both IPv4 and IPv6 traffic

- **IDS recording options**
  - ➤ Event logging to syslogd or console
  - ➤ Statistics to syslogd
  - ➤ IDS packet trace after attack detected for offline analysis

- **Reports and event handling**
  - ➤ trmdstat produces reports from IDS syslogd records
    - – Summary and detailed
  - ➤ IDS event handling by Tivoli NetView

- **Defensive filtering**
  - ➤ Installed through ipsec command
  - ➤ Manually (by human being) or through automation (via external security event manager)

For more information ...

URL	Content
http://www.twitter.com/IBM_Commserver	IBM Communications Server Twitter Feed
http://www.facebook.com/IBMCommserver	IBM Communications Server Facebook Fan Page
http://www.ibm.com/systems/z/	IBM System z in general
http://www.ibm.com/systems/z/hardware/networking/	IBM Mainframe System z networking
http://www.ibm.com/software/network/commserver/	IBM Software Communications Server products
http://www.ibm.com/software/network/commserver/zos/	IBM z/OS Communications Server
http://www.ibm.com/software/network/commserver/z_lin/	IBM Communications Server for Linux on System z
http://www.ibm.com/software/network/ccl/	IBM Communication Controller for Linux on System z
http://www.ibm.com/software/network/commserver/library/	IBM Communications Server library
http://www.redbooks.ibm.com	ITSO Redbooks
http://www.ibm.com/software/network/commserver/zos/support/	IBM z/OS Communications Server technical Support – including TechNotes from service
http://www.ibm.com/support/techdocs/atsmastr.nsf/Web/TechDocs	Technical support documentation from Washington Systems Center (techdocs, flashes, presentations, white papers, etc.)
http://www.rfc-editor.org/rfcsearch.html	Request For Comments (RFC)
http://www.ibm.com/systems/z/os/zos/bkserv/	IBM z/OS Internet library – PDF files of all z/OS manuals including Communications Server