



Software Group | Enterprise Networking Solutions

# Integrated Intrusion Detection Services for z/OS Communications Server

## SHARE Session 15195

Lin Overby - [overbylh@us.ibm.com](mailto: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](http://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?

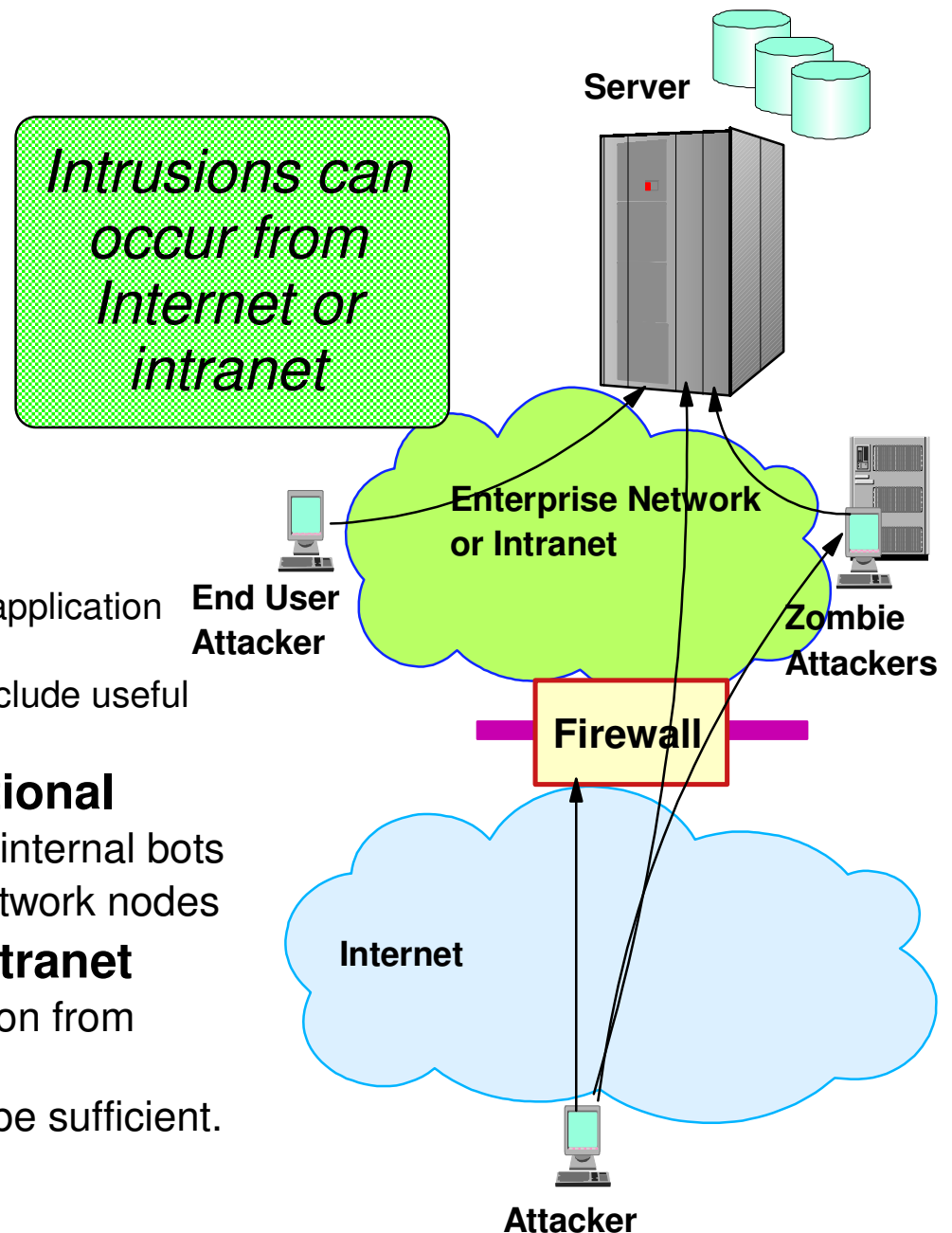
- ▶ Information Gathering
  - Network and system topology
  - Data location and contents
- ▶ Eavesdropping / Impersonation / Theft
  - On the network / on the server
  - Base for further attacks on others
    - ✓ Amplifiers
    - ✓ Robot or zombie
- ▶ Denial of Service
  - Attack on availability
    - ✓ Single Packet attacks - exploits system or application vulnerability
    - ✓ Multi-Packet attacks - floods systems to exclude useful work

## ■ Attacks can be deliberate or unintentional

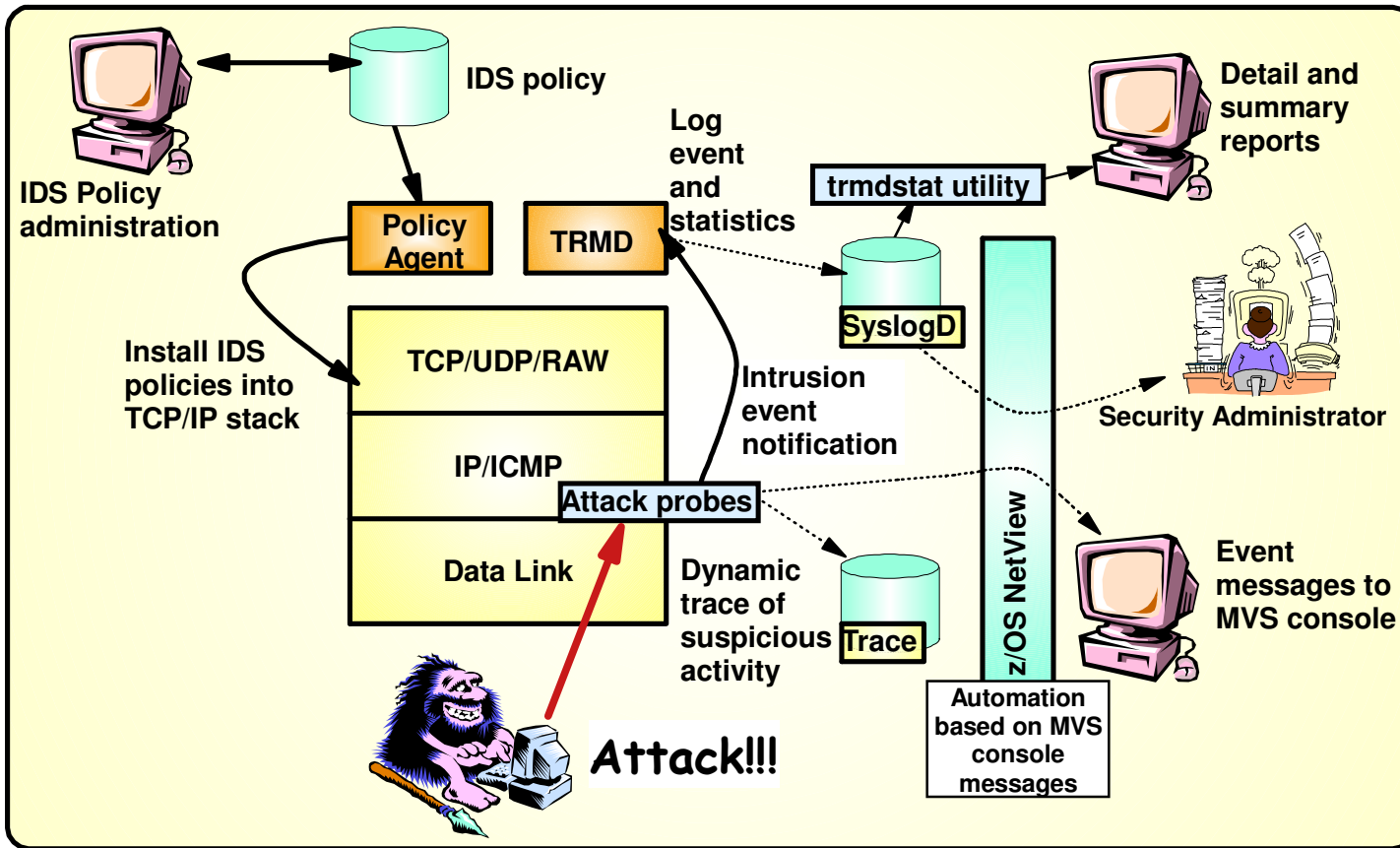
- ▶ Deliberate: malicious intent from outside or internal bots
- ▶ Unintentional: various forms of errors on network nodes

## ■ 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



# Intrusion Detection Services Overview



## 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

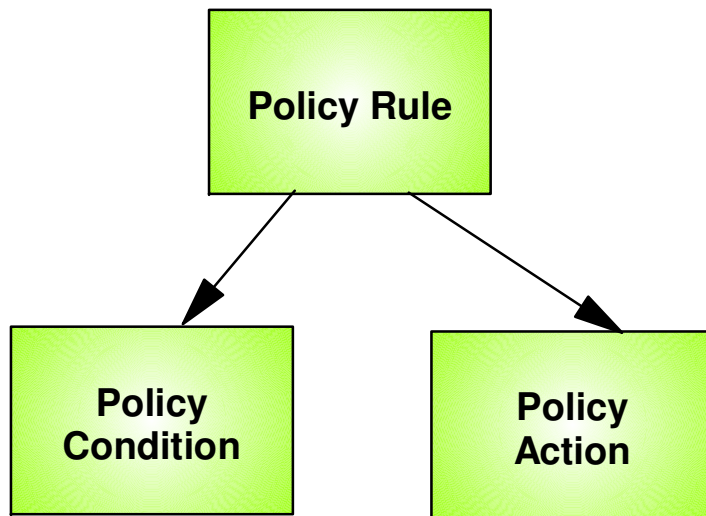
## z/OS in-context IDS broadens overall intrusion detection coverage:

- 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 thresholds that are generally unavailable to external IDSs
- Policy can control prevention methods on the target, such as connection limiting and packet discard

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

# Policy Model Overview

## Basic Policy Objects



Policy objects relationship:  
IF condition THEN action

Policies consist of several related objects

- Policy Rule is main object and refers to:
  - ▶ Policy Condition
    - Defines IDS conditions which must be met to execute the Policy action
  - ▶ Policy Action
    - Defines IDS actions to be performed when Policy Condition is met

# 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 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 (less than 5 minutes)
      - ✓ usually less than five minutes, program driven
  - ▶ Slow scans
    - Different resources intermittently 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"

<b>Sensitivity (from policy)</b>	<b>Normal Event</b>	<b>Possibly Suspicious Event</b>	<b>Very Suspicious Event</b>
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

- ▶ 4 different attack types (more on this later)

# 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
    - IfcFloodMinDiscard (default 1000)
    - IfcFloodPercentage (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 (IfcFloodMinDiscard) 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 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 threshold



# Interface Flooding Example

- Assume the IDS flood policy specifies:
  - ▶ IfcFloodMinDiscard: 2000
  - ▶ IfcFloodPercentage:10%
  
- Consider the following sequence for interface X:

time



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%	<b>interface flood start detected.</b> 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%	<b>Interface flood end detected.</b> Discard rate <= half of policy specified rate.

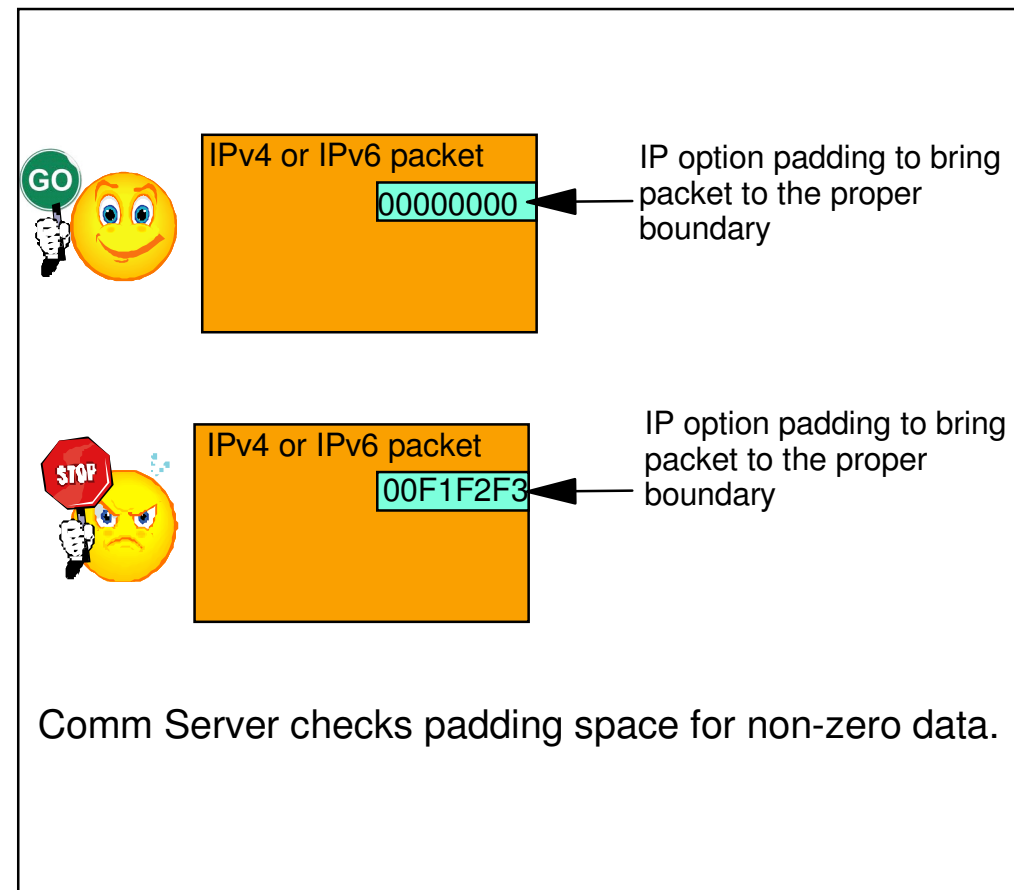
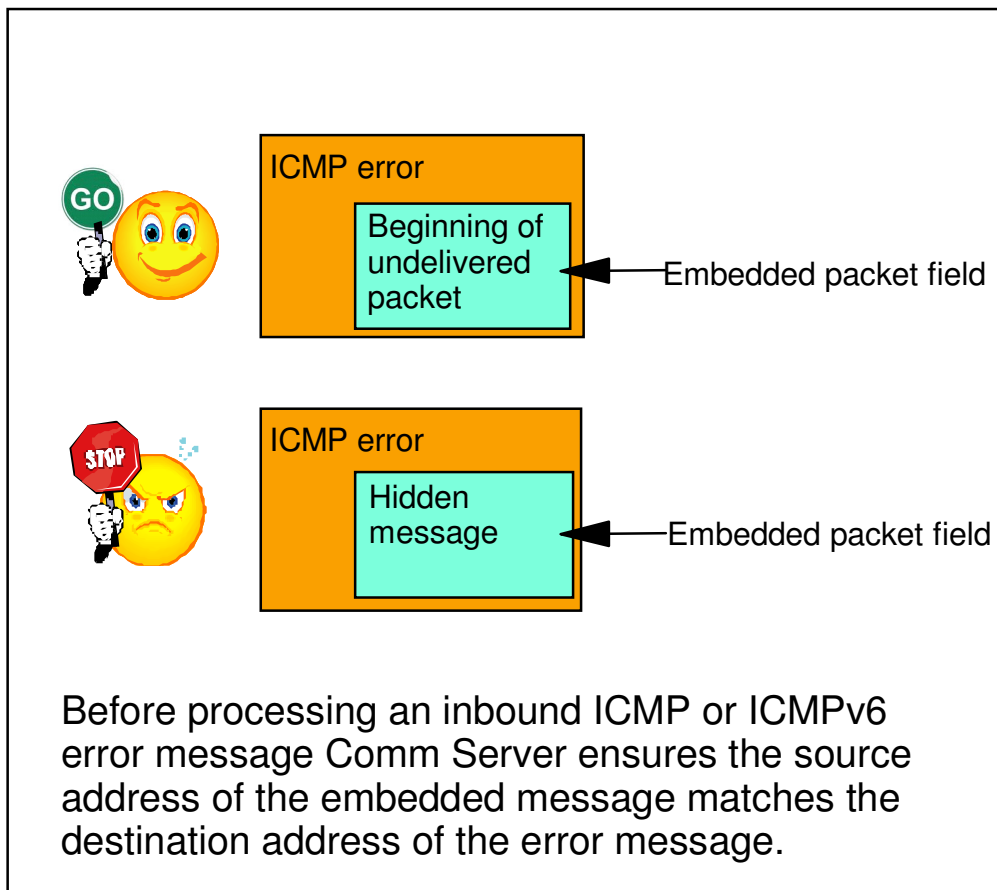
# Data Hiding Protection

- The structure of protocol headers afford the opportunity embed "hidden data" in packets (at the source host / in the network)
- The Data Hiding attack type can detect such hidden data

- Two forms of data hiding protection can be independently enabled:

Exploitation of ICMP and ICMPv6 error messages

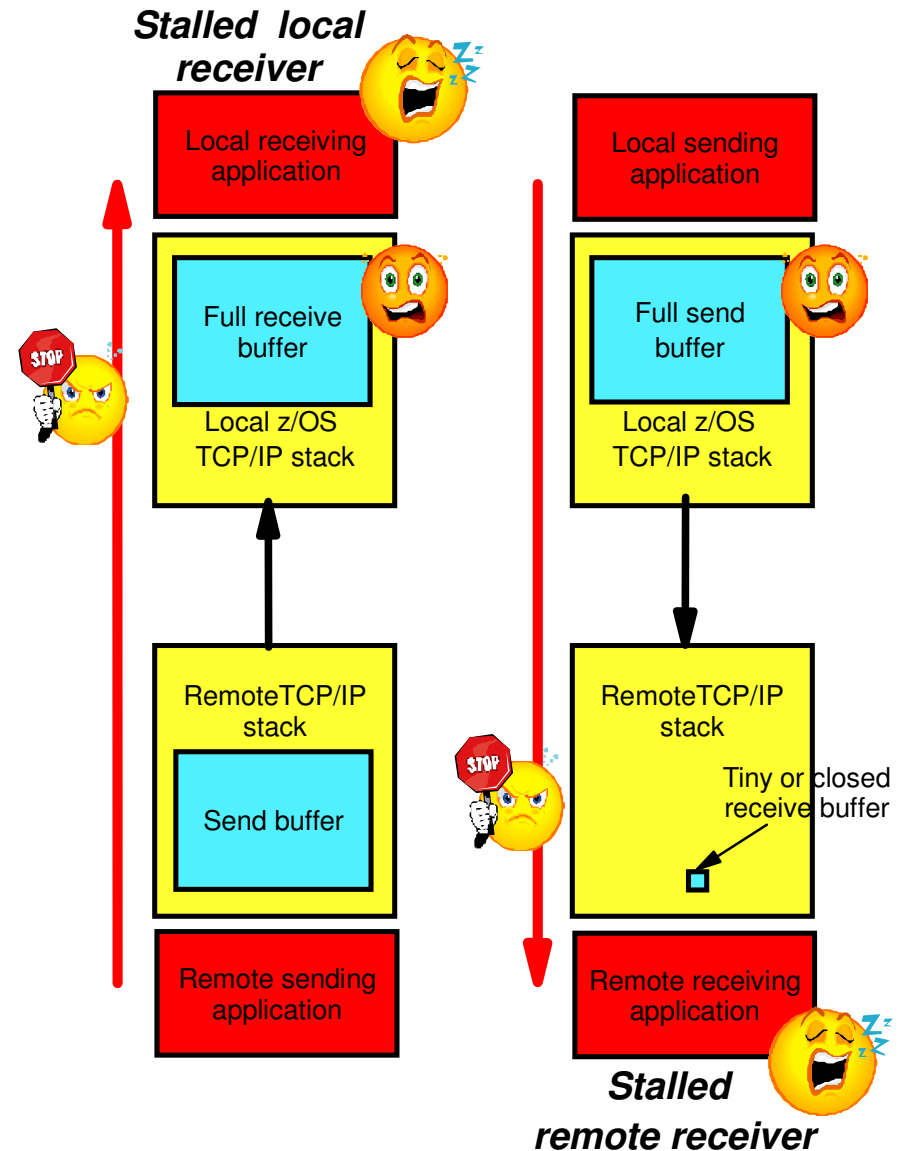
Exploitation of IPv4 and IPv6 option pad



# TCP Queue Size Protection

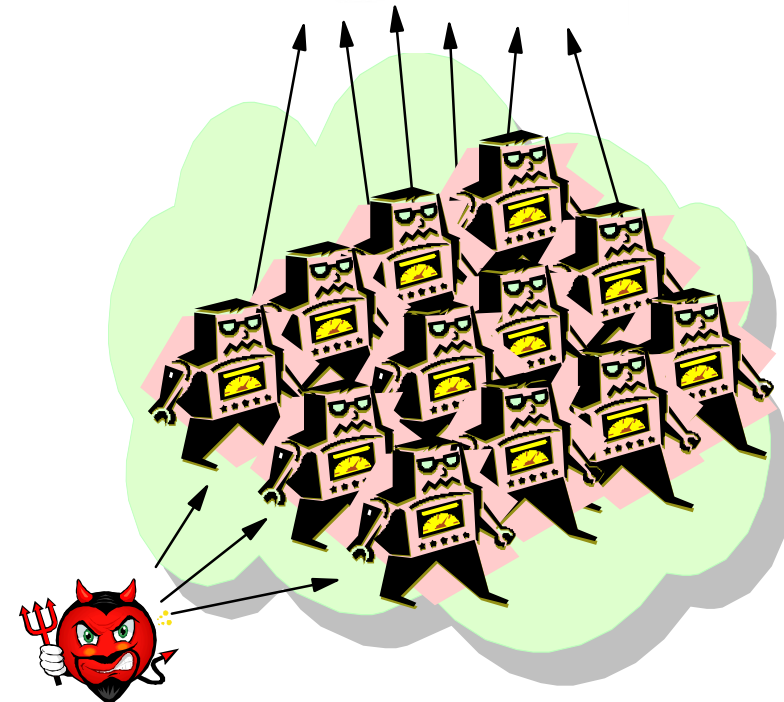
TCP queue size protection can be controlled with IDS policy...

- Protects TCP queues that become constrained
  - ▶ Send, receive and out-of-order queues
  - ▶ Mark data “page eligible” after 60 seconds, or after 30 seconds if limit exceeded
- IDS configuration provides
  - ▶ Configurable queue size and configurable action of reset connection
  - ▶ IDS logging and statistics
  - ▶ No IDS tracing for this attack type
- Exclusion list can limit reporting or reset of constrained send queue
  - ▶ Can be a legitimate condition, for example, a printer running out of paper
  - ▶ Data on send queue is still marked "page eligible"
- Evaluated on a per-connection basis



# Global TCP Stall Protection

- Global TCP Stall Protection protects against DoS attack where a large number of TCP connections are created and forced to stall, thereby consuming lots of TCP/IP resources
- A single connection is considered stalled when either...
  - ▶ TCP send window size is abnormally small
  - ▶ TCP send queue is full and data is not being retransmitted
- Global TCP stall condition is entered when...
  - ▶ At least 1000 TCP connections are active AND
  - ▶ At least 50% of those TCP connections are in a stalled state
- IDS reporting options (except IDS tracing) available
  - ▶ Two levels of logging - basic and detailed
  - ▶ Be careful with detailed syslogd logging - can generate 500+ messages per global stall detection
- Defensive action of "reset connection" may be configured
  - ▶ Resets all stalled connections when a global TCP stall condition is detected



# Comparing TCP queue size and TCP global stall attack types

TCP Queue Size Attack	Global TCP Stall Attack
Monitors individual connection's send queue for old or excessive data.	Monitors individual connection's send queue to detect stall condition.
No awareness of TCP/IP stack's overall state.	Aware of stack's overall state -- keeps count of stalled TCP send queues.
Attack detected based on individual send queue's state.	Attack detected based on overall state of stack -- large number of stalled connections.
Attack detected after at least 30 or 60 seconds.	Attack detection not based on time - can be detected much more quickly than 30 seconds.
Able to detect when a one or a few connections are stalled.	Triggered only when a large number of connections stall.

# EE Attack Types

- Four attack types:

- ▶ **EE Malformed Packet**

- Validates general form of LDLC packets
    - Discard and notify actions available

- ▶ **EE LDLC Check**

- Ensure LDLC control packets flow on EE signaling port
    - Discard and notify actions available

- ▶ **EE Port Check**

- Ensure source port matches destination port on inbound packets
    - Discard and notify actions available

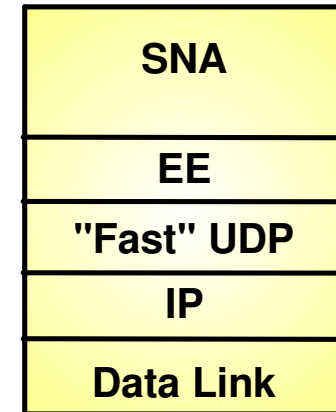
- ▶ **EE XID Flood**

- Raises flood condition if too many unique XID timeouts arrive within a one minute interval (flood threshold is configurable)
    - Condition ends when number of XID timeouts fall below threshold
    - Notify actions available

- Exclusion list can be configured for each attack type

- ▶ Some EE implementations observed to use ephemeral ports - may be exclusion candidates for LDLC, Port checks

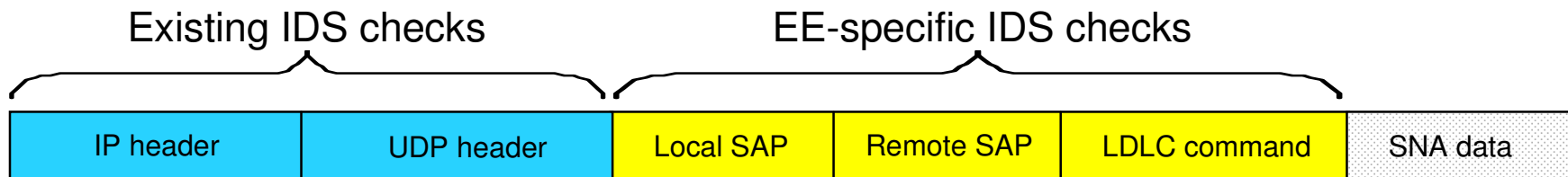
- Usual IDS reporting options available (exception: no IDS trace for EE XID flood)



EE is based on UDP

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

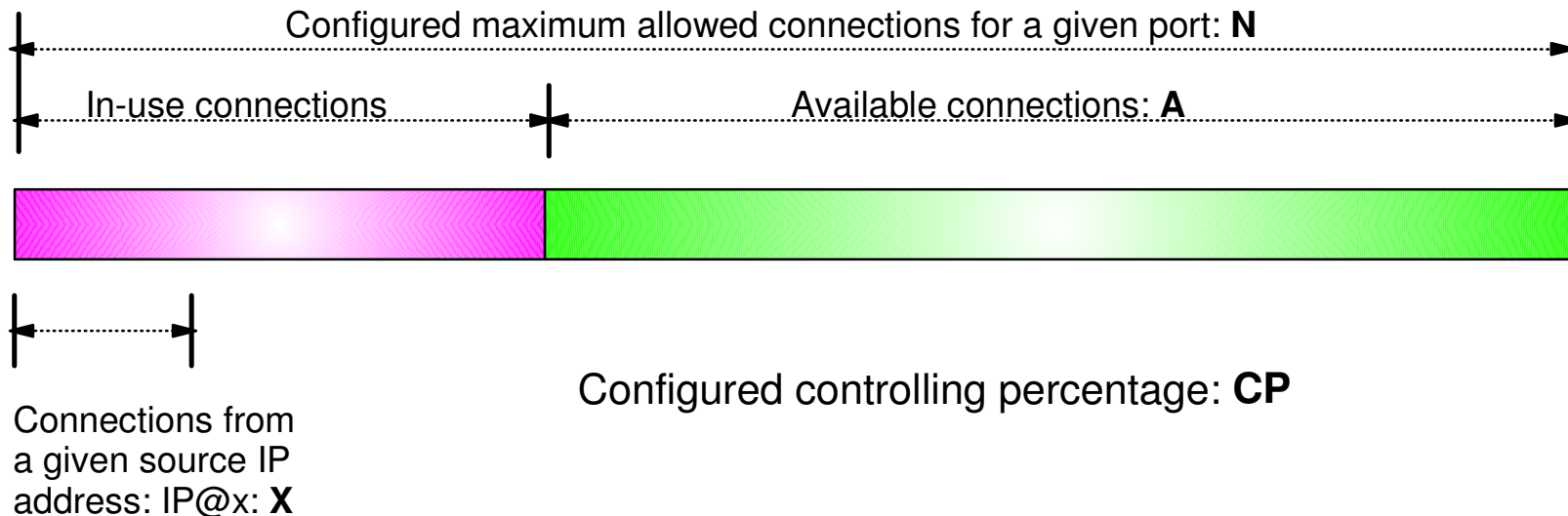
Uses 5 pre-defined ports



# 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



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

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	8	12
100	80	20	2	4	6
100	90	10	1	2	3

Allowed      Rejected

- 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 attack subtype 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 after 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 probeid and correlator
  - ▶ 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 not 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

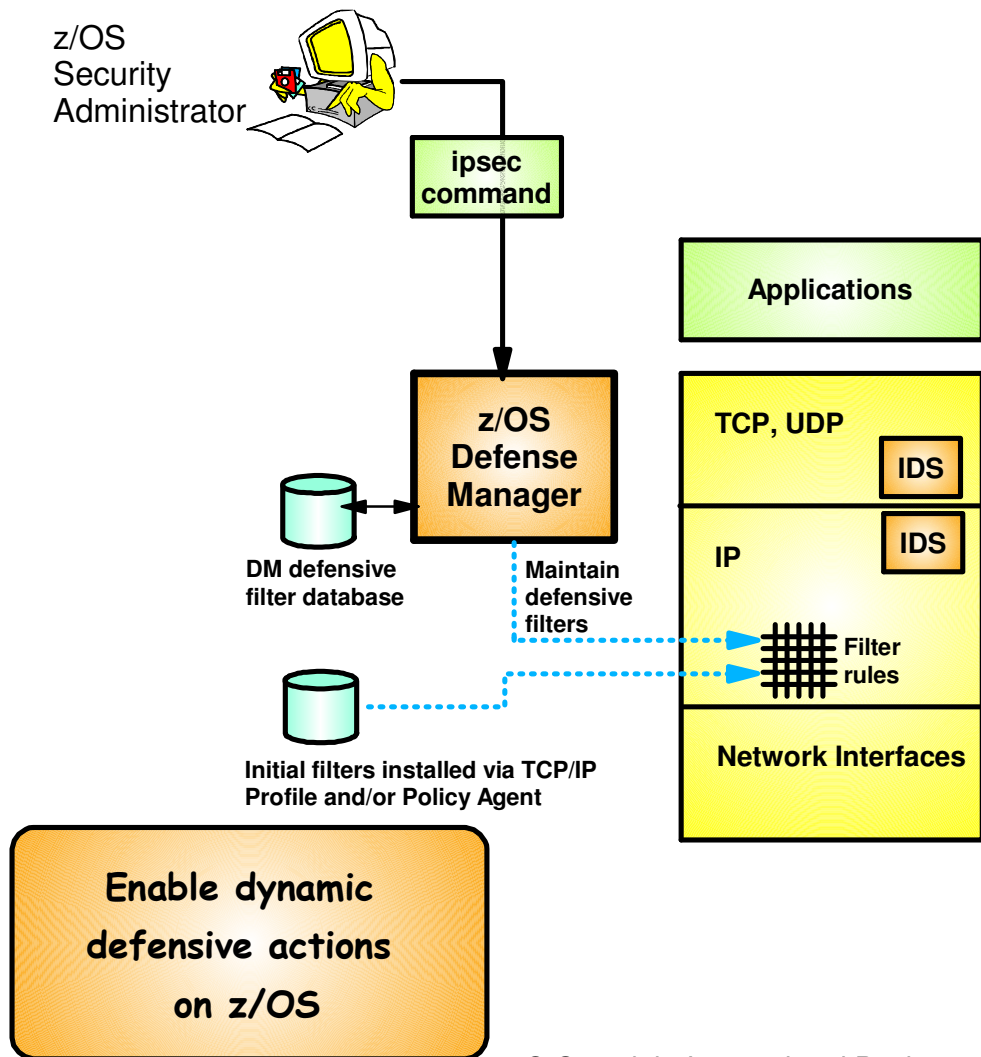
## ■ Traffic Regulation Events

- ▶ 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



- **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 summary reports
    - For Attack, Flood, Scan, TCP and UDP TR information
  - ▶ Event type detail 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 administrator
  - ▶ Run trmdstat and attach output to email
  - ▶ Issue pre-defined commands

# 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 policy deletion controls in Policy Agent configuration file
  - ▶ Tcplmage 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 Tcplmage 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:

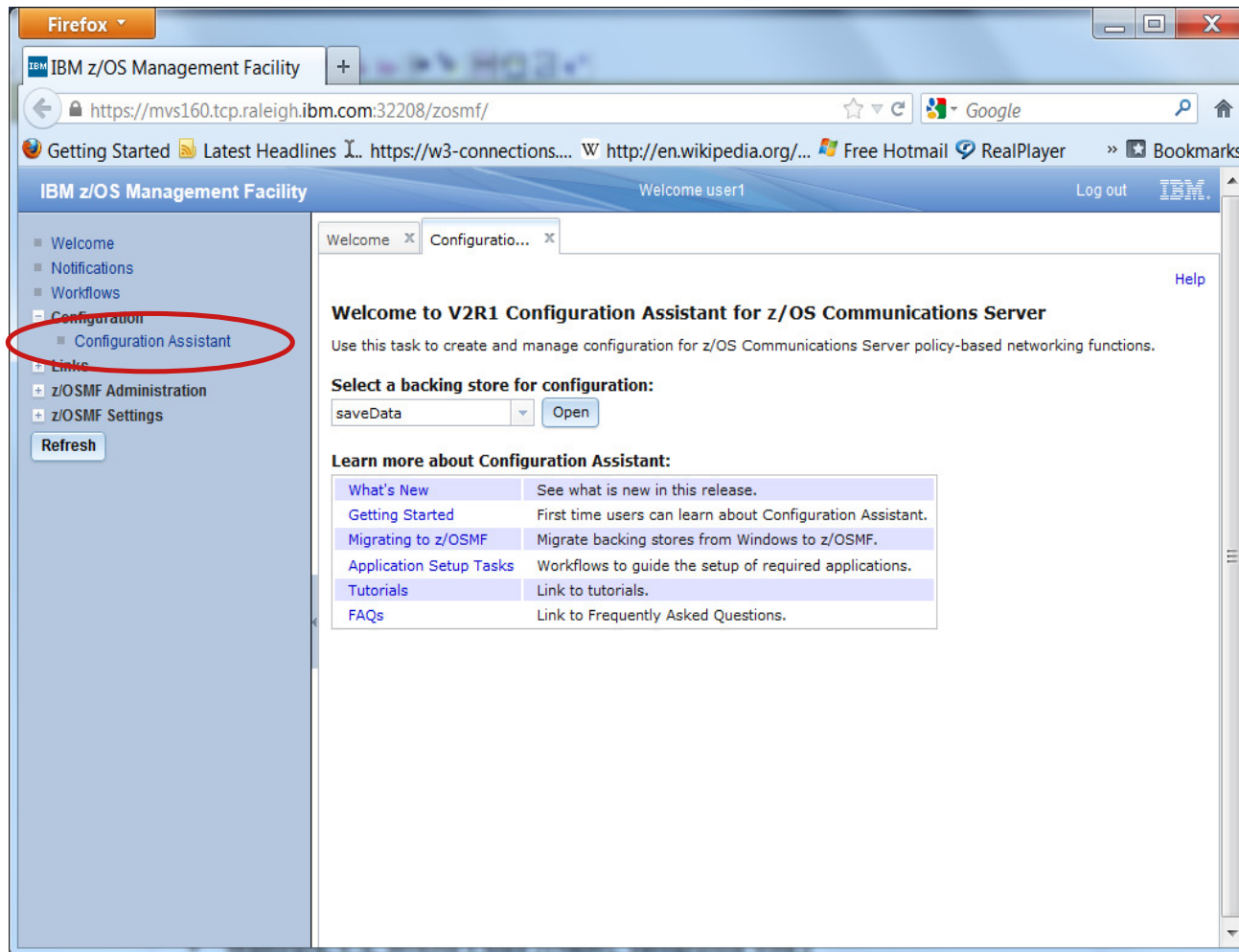
Restrict access to IDS policy displays using SAF SERVAUTH resources:

- ▶ `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

The screenshot shows a Firefox browser window displaying the IBM z/OS Management Facility Configuration Assistant. The browser's address bar shows the URL <https://mvs160.tcp.raleigh.ibm.com:32208/zosmf/>. The page title is "IBM z/OS Management Facility" and the user is logged in as "user1".

The left sidebar contains a navigation menu with the following items:

- Welcome
- Notifications
- Workflows
- Configuration
  - Configuration Assistant** (highlighted with a red circle)
- Links
- z/OSMF Administration
- z/OSMF Settings

A "Refresh" button is located below the sidebar menu.

The main content area displays the "Welcome to V2R1 Configuration Assistant for z/OS Communications Server" page. It includes a "Help" link in the top right corner. The main heading is "Welcome to V2R1 Configuration Assistant for z/OS Communications Server". Below the heading, it states: "Use this task to create and manage configuration for z/OS Communications Server policy-based networking functions."

The section "Select a backing store for configuration:" contains a dropdown menu with "saveData" selected and an "Open" button.

The section "Learn more about Configuration Assistant:" contains a table of links:

Learn more about Configuration Assistant:	
<a href="#">What's New</a>	See what is new in this release.
<a href="#">Getting Started</a>	First time users can learn about Configuration Assistant.
<a href="#">Migrating to z/OSMF</a>	Migrate backing stores from Windows to z/OSMF.
<a href="#">Application Setup Tasks</a>	Workflows to guide the setup of required applications.
<a href="#">Tutorials</a>	Link to tutorials.
<a href="#">FAQs</a>	Link to Frequently Asked Questions.



# Start a new IDS configuration - create a new backing store

Firefox

IBM z/OS Management Facility

https://mvs160.tcp.raleigh.ibm.com:32208/zosmf/

Getting Started Latest Headlines https://w3-connections... http://en.wikipedia.org/... Free Hotmail RealPlayer Bookmarks

IBM z/OS Management Facility Welcome user1 Log out IBM

Welcome x Configuratio... x

Help

**Welcome to V2R1 Configuration Assistant for z/OS Communications Server**

Use this task to create and manage configuration for z/OS Communications Server policy-based networking functions.

**Select a backing store for configuration.**

idsdemoLHO Open

**Learn more about Configuration Assistant:**

<a href="#">What's New</a>	See what is new in this release.
<a href="#">Getting Started</a>	First time users can learn about Configuration Assistant.
<a href="#">Migrating to z/OSMF</a>	Migrate backing stores from Windows to z/OSMF.
<a href="#">Application Setup Tasks</a>	Workflows to guide the setup of required applications.
<a href="#">Tutorials</a>	Link to tutorials.
<a href="#">FAQs</a>	Link to Frequently Asked Questions.

# Create IDS policy objects - select the IDS policy perspective

The screenshot shows the IBM z/OS Management Facility Configuration Assistant interface. The browser address bar indicates the URL `https://mvs160.tcp.raleigh.ibm.com:32208/zosmf/`. The page title is "IBM z/OS Management Facility" and the user is logged in as "user1".

The main content area displays the "Configuration Assistant (Home) > IDS" view. The current backing store is identified as "V2R1 Current Backing Store = idsdemoLHO". A dropdown menu labeled "Select a perspective:" is open, showing the following options: AT-TLS, IDS (highlighted), IPsec, NSS, PBR, and QoS. The "IDS" option is circled in red.

Below the dropdown, there are tabs for "Systems", "Traffic De...", "DMD", and "Requirement Maps". An "Actions" dropdown is also visible. A table with columns "Name", "Status", "Release", and "Description" is shown, but it is empty with the message "There is no data to display." Below the table, it says "Total: 0, Selected: 0".

At the bottom of the configuration area, there are "Home" and "Save" buttons.

# Traffic Descriptors

Welcome x Configuratio... x

Configuration Assistant (Home) > IDS H

**V2R1 Current Backing Store = idsdemoLHO**

Select a perspective: IDS Tools

Systems **Traffic Descriptors** Requirement Maps

Actions

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

Total: 28, Selected: 0

# Evaluate IDS\_Default requirements map

The screenshot shows the IBM z/OS Management Facility Configuration Assistant interface. The browser address bar indicates the URL is <https://mvs160.tcp.raleigh.ibm.com:32208/zosmf/>. The page title is "IBM z/OS Management Facility" and it says "Welcome user1". The main content area is titled "V2R1 Current Backing Store = idsdemoLHO". Below this, there is a "Select a perspective:" dropdown menu set to "IDS" and a "Tools" button. The "Requirement Maps" tab is selected and circled in red. Below the tabs, there is an "Actions" dropdown menu, also circled in red, with a dashed arrow pointing to the "View Details" option, which is also circled in red. The main table displays a single requirement map entry:

Name Filter	Description Filter
IDS_Default	IBM Supplied: Intrusion Detection Services Starter Set

At the bottom of the table, it says "Total: 1, Selected: 0".

## 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 x Configuratio... x

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
<b>Data Hiding Attack<sup>1</sup></b>	DataHiding	Report Events	Use Default Report Settings	None	<b>Console Parameters:</b> No ----- <b>SYSLOG Parameters:</b> SYSLOG: Yes SYSLOG Level: 4 - Warning ----- <b>Statistics Parameters:</b> Statistics: Yes Statistics Interval: 60 Minutes Report Stat if no events: Yes ----- <b>Trace Parameters:</b> No
<b>IPv6 Outbound Raw Attack<sup>1</sup></b>	IPv6OutboundRaw	Report Events	Use Default Report Settings	None	
<b>IPv6 Destination Options Attack<sup>1</sup></b>	IPv6DestinationOptions	Report Events	Use Default Report Settings	None	
<b>IPv6 Hop-by-Hop Options Attack<sup>1</sup></b>	IPv6HopByHop	Report Events	Use Default Report Settings	None	
<b>IPv6 Next Header Attack<sup>1</sup></b>	IPv6NextHeader	Report Events	Use Default Report Settings	None	
<b>TCP Queue Size Attack<sup>1</sup></b>	TcpQueueSize	Report Events	Use Default Report Settings	None	
<b>Global TCP Stall Attack<sup>1</sup></b>	GlobalTCPStall	Report Events	Use Default Report Settings	None	
<b>Flood Attack</b>	Flood	Both Drop and Report	Use Default Report Settings	None	
<b>Perpetual Echo Attack</b>	Echo	Report Events	Use Default Report Settings	None	
<b>IPv4 Protocols Attack</b>	IPv4Protocol	Report Events	Use Default Report Settings	None	
<b>IPv4 Options Attack</b>	IPv4Option	Report Events	Use Default Report Settings	None	
<b>ICMP Redirect Attack</b>	ICMPRedirect	Report Events	Use Default Report Settings	None	
<b>Malformed Packet Attack</b>	MalformedPacket	Both Drop and Report	Use Default Report Settings	None	
<b>IPv4 Outbound Raw Attack</b>	IPv4OutboundRaw	Report Events	Use Default Report Settings	None	
<b>IP Fragment Attack</b>	Fragmentation	Report Events	Use Default Report Settings	None	
<b>EE Malformed Packet Attack<sup>1</sup></b>	EEMalformedPacket	Report Events	Use Default Report Settings	None	
<b>EE LDLC Check Attack<sup>1</sup></b>	EELDLCCheck	Report Events	Use Default Report Settings	None	
<b>EE Port Check Attack<sup>1</sup></b>	EETPortCheck	Report Events	Use Default Report Settings	None	
<b>EE XID Flood Attack<sup>1</sup></b>	EEXIDFlood	Report Events	Use Default Report Settings	None	

Footnotes:

<sup>1</sup> 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	Use Default Report Settings	None	Report Events
Checking of embedded packets within ICMP error messages: Enabled			

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)

Welcome x Configuratio... x

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	Use Default Report Settings	None	Report Events
18	57			
59	88			
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	Use Default Report Settings	None	Report Events
8	137			
139	193			
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	Use Default Report Settings	None	Report Events
8	137			
139	193			
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 x Configuratio... x

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	Use Default Report Settings	None	Report Events
7	16			
18	40			
42	42			
45	49			
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	Use Default Report Settings	None	Report Events
13 - Time Of Day	Both Local and Remote			
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)

Welcome x Configuratio... x

Configuration Assistant (Home) > IDS > View Details

### View Details

Attack - EEMalformedPacket

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: EE LDLC Check Attack - EELDLCCheck

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: EE Port Check Attack - EEPortCheck

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: EE XID Flood Attack - EEXIDFlood

EE XID TimeOut	Reports	Time Condition	Action
100	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.

-----

### Scan Protection Summary

No Scan Protection Configured

-----

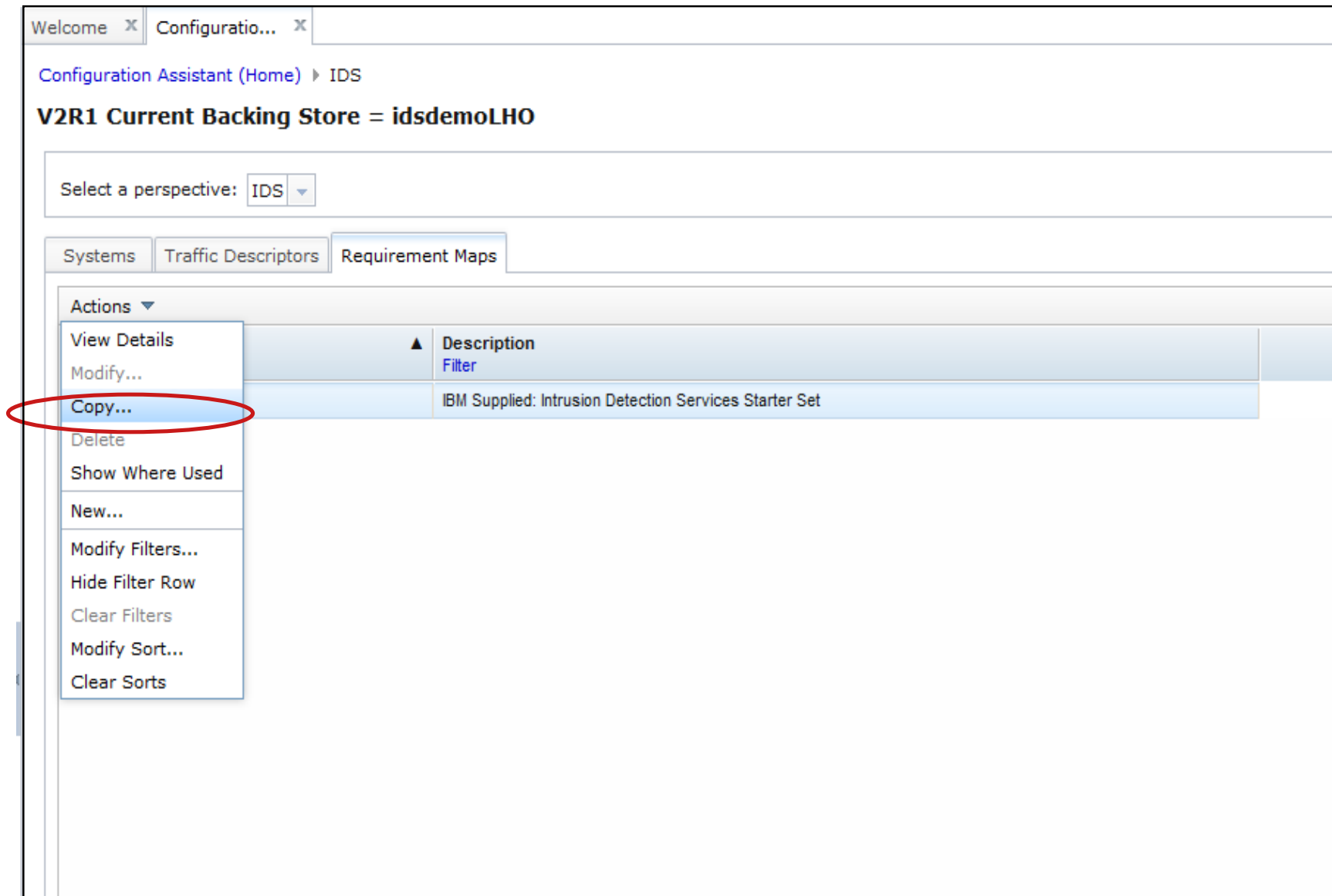
### Traffic Regulation Summary

No Traffic Regulation Configured

Close



# 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

Welcome x Configuratio... x

Configuration Assistant (Home) > IDS > Requirement Map

## Copy Requirement Map

Name Attacks Scans Traffic Regulation



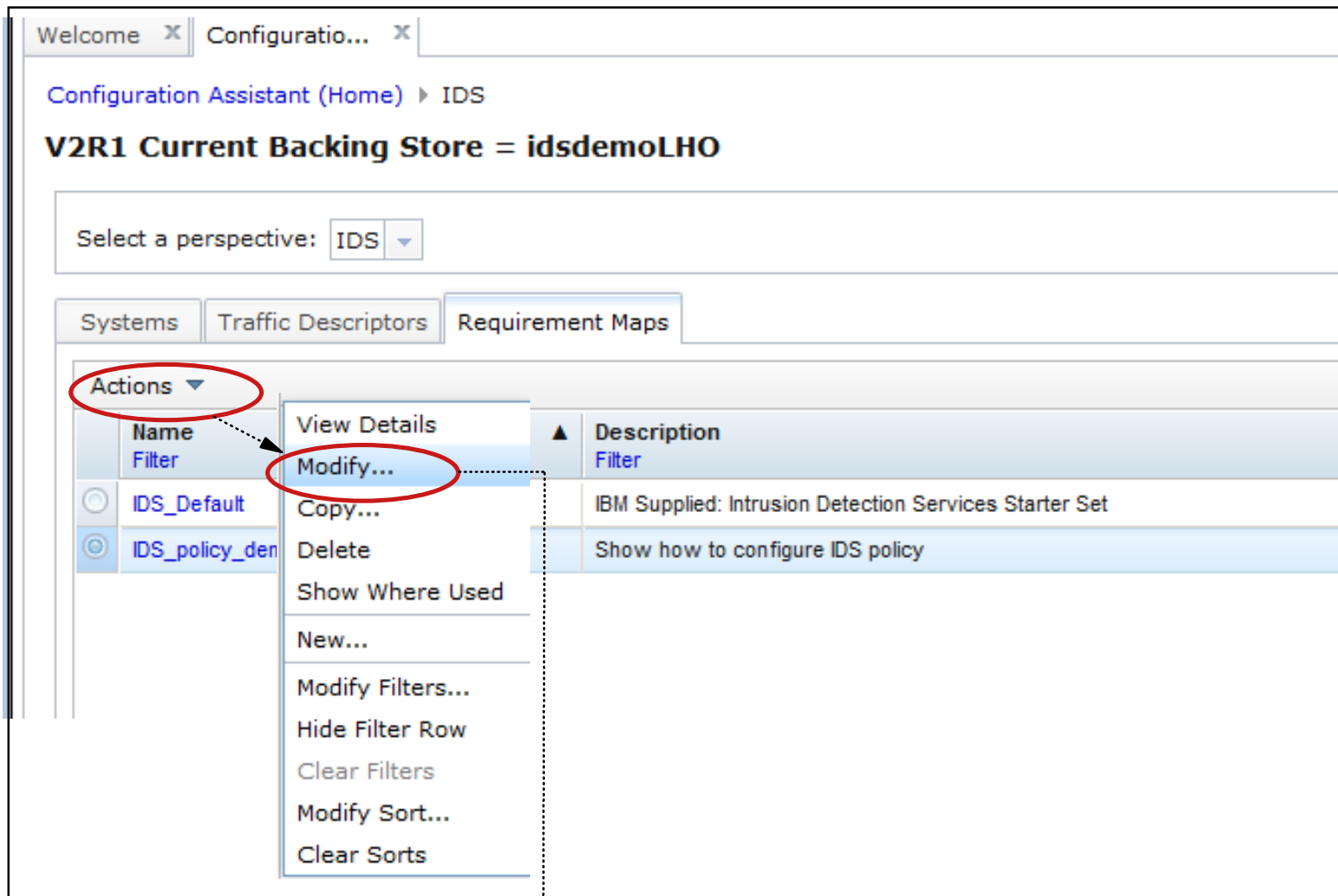
\* Name:

Description:

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

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

# Modify copied default requirements map



next page

# Attack protection enabled by default

Welcome x Configuratio... x

Configuration Assistant (Home) > IDS > Requirement Map

## Modify Requirement Map

Name **Attacks** Scans Traffic Regulation

Enable attack protection

▶ **Steps**

Actions ▼

	Attack Type	Rule Name	Action
<input type="radio"/>	Data Hiding Attack	DataHiding	Report Events
<input type="radio"/>	IPv6 Outbound Raw Attack	IPv6OutboundRaw	Report Events
<input type="radio"/>	IPv6 Destination Options Attack	IPv6DestinationOptions	Report Events
<input type="radio"/>	IPv6 Hop-by-Hop Options Attack	IPv6HopByHop	Report Events
<input type="radio"/>	IPv6 Next Header Attack	IPv6NextHeader	Report Events

Total: 19, Selected: 0

[Default report settings for Attacks...](#) → next page

OK Cancel

# Customize report settings

Welcome x Configuratio... x

Configuration Assistant (Home) > IDS > Requirement Map > Report Types

## Report Types

Indicate where to report IDS events

- System console [Modify Details...](#)
- SYSLOGD [Modify Details...](#)
- IDS trace [Modify Details...](#)

Indicate if you want to log statistics at predefined intervals

- Log statistics to SYSLOGD [Modify Details...](#)

[OK](#) [Cancel](#)

# Enable scan policy

Welcome x Configuratio... x

Configuration Assistant (Home) > IDS > Requirement Map

### Modify Requirement Map

Name Attacks **Scans** Traffic Regulation

Enable scan

▼ Steps

1. To enable a scan for a particular traffic descriptor, select from the 'Enable' action sub-menu items
2. Select the monitor level for each enabled scan
3. To disable scan protection for a traffic descriptor, select the row in the enabled scans table and click the 'Disable' action

Actions ▼ | Move Up Move Down

	Enabled Traffic Descriptor	Rule Name	Sensitivity
<input type="radio"/>	All_Well-Known_TCP	All_Well-Known_TCP	Medium
<input type="radio"/>	All_Well-Known_UDP	All_Well-Known_UDP	Medium
<input type="radio"/>	ICMP	ICMP	High

Total: 3, Selected: 0

Default report settings for Scans...

[Modify Fast and Slow Scan Settings...](#) → next page

OK Cancel

# Modify global scan settings

The screenshot shows a configuration window titled "Global Scan Settings" with two tabs: "Welcome" and "Configuratio...". The breadcrumb path is "Configuration Assistant (Home) > IDS > Requirement Map > Global Scan Settings". The window is divided into two sections: "Fast scan settings" and "Slow scan settings".

**Fast scan settings**

- \*Fast scan interval: 1 (minutes, 1-1440)
- \*How many accesses within scan interval indicate an attack: 5 (1 - 64)

**Slow scan settings**

- Enable slow scans
- \*Slow scan interval: 120 (minutes, 1-1440)
- \*How many accesses within scan interval indicate an attack: 10 (minutes, 1-1440)

At the bottom left, there are "OK" and "Cancel" buttons.

# Enable traffic regulation protection

The screenshot shows a web interface for configuring traffic regulation. The breadcrumb path is 'Configuration Assistant (Home) > IDS > Requirement Map'. The main heading is 'Modify Requirement Map'. There are four tabs: 'Name', 'Attacks', 'Scans', and 'Traffic Regulation', with the last one selected. A checkbox labeled 'Enable traffic regulation' is checked. Below this, a 'Steps' section lists three instructions. At the bottom, there is an 'Actions' menu with 'Move Up' and 'Move Down' options, and a table with columns 'Enabled Traffic Descriptor', 'Rule Name', and 'Action'. The table is currently empty, displaying 'There is no data to display.' and 'Total: 0, Selected: 0'.

## 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

Welcome x Configuratio... x

Configuration Assistant (Home) > IDS > Requirement Map > Traffic Regulation Details

## New Traffic Regulation Details

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

Traffic regulation identification

\* Name

\* Traffic Descriptor  ▼

Action

Enter parameters for TCP traffic

\*Max number of connections:  (0-65535)

\*Limit each host to the following percentage of the available connections:

Limit scope:  ▼

# Traffic regulation enabled

Welcome x Configuratio... x

Configuration Assistant (Home) > IDS > Requirement Map

## Modify Requirement Map

Name Attacks Scans **Traffic Regulation**

Enable traffic regulation

▼ **Steps**

1. To enable a traffic regulation for a particular traffic descriptor, select from the 'Enable' action sub-menu items
2. Select the Action for each enabled traffic regulation
3. To disable a traffic regulation for a traffic descriptor, select the row in the enabled traffic regulation table and click the 'Disable' action

Actions ▼   Move Up Move Down		
Enabled Traffic Descriptor	Rule Name	Action
<input checked="" type="radio"/> FTP-Server	FTP-Server	Limit and Report

Total: 1, Selected: 1

[Default report settings for Traffic Regulation...](#)

**OK** Cancel

# IDS\_policy\_demo requirements map now created

Welcome x Configuratio... x

Configuration Assistant (Home) > IDS

**V2R1 Current Backing Store = idsdemoLHO**

Select a perspective: IDS ▾

Systems Traffic Descriptors Requirement Maps

Actions ▾

	Name Filter	▲	Description Filter
<input type="radio"/>	IDS_Default		IBM Supplied: Intrusion Detection Services Starter Set
<input checked="" type="radio"/>	IDS_policy_demo		Show how to configure IDS policy

# Create system image

The image shows two overlapping screenshots of the Configuration Assistant interface. The top screenshot shows the main configuration screen with the breadcrumb 'Configuration Assistant (Home) > IDS' and the title 'V2R1 Current Backing Store = idsdemoLHO'. A dropdown menu is open under the 'Systems' tab, with 'Add z/OS Image...' highlighted in blue and circled in red. A dashed arrow points from this menu item to the dialog box shown in the bottom screenshot.

The dialog box, titled 'Add z/OS Image', contains the following fields and controls:

- \* Name: IDSDemo
- Description: IDS Demo System
- z/OS Release: V2R1
- Buttons: OK, Cancel

# 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

OK Cancel

next page ←

# Associate TCP/IP stack with requirements map

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
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 x Configuratio... x

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

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

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
IDSSTACK	Stack	Complete	V2R1	IDS Demo Stack

- Properties...
- Requirement Maps...
- Copy...
- Delete
- Add z/OS Image...
- Add TCP/IP Stack...
- Import Policy Data...
- Install All Files for IDS...
- Install Configuration Files...

Welcome x Configuratio... x

Configuration Assistant (Home) > IDS > Configuration Files [Help](#)

**List of Configuration Files for All Images**

List of Configuration Files for All Images

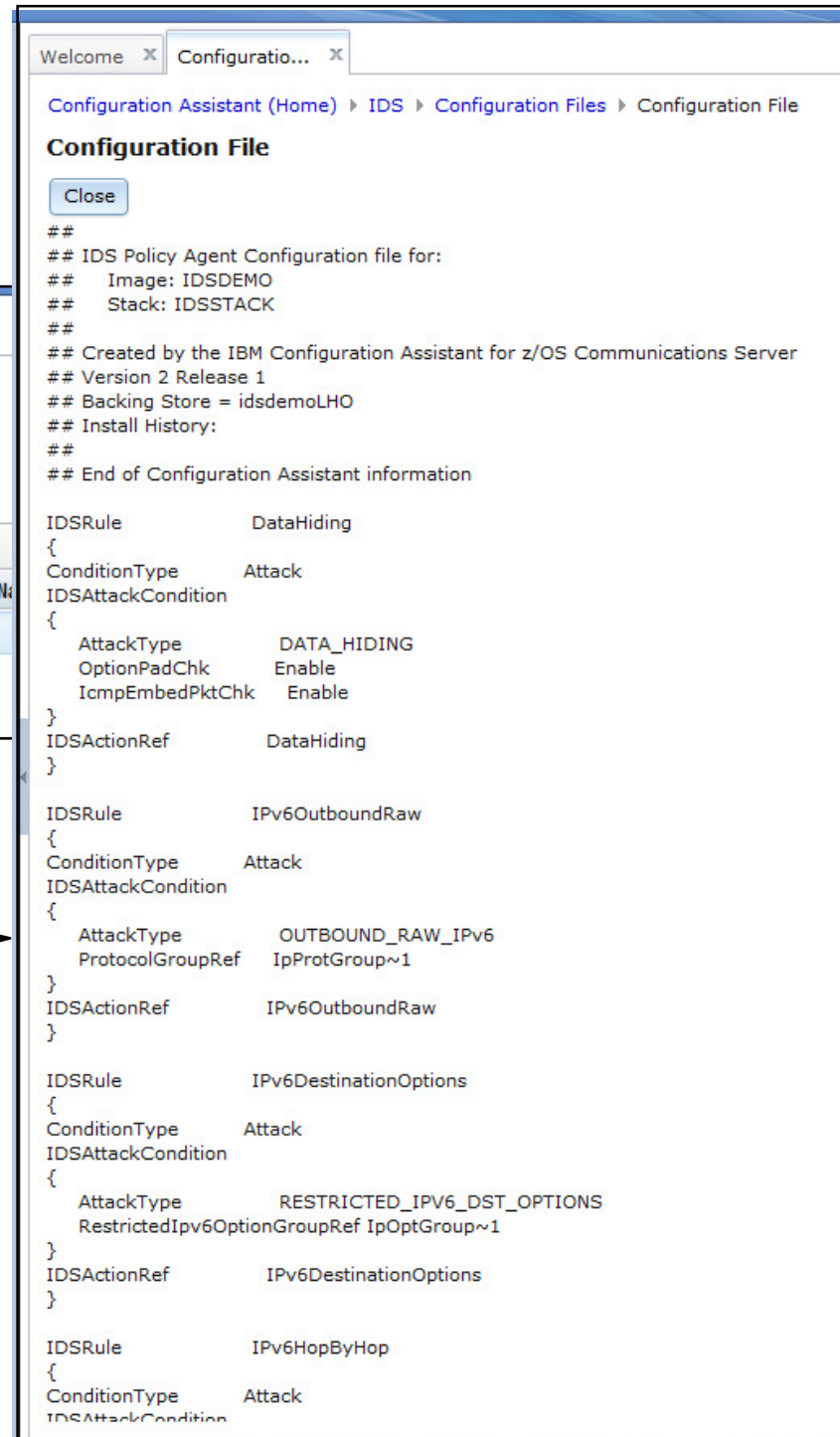
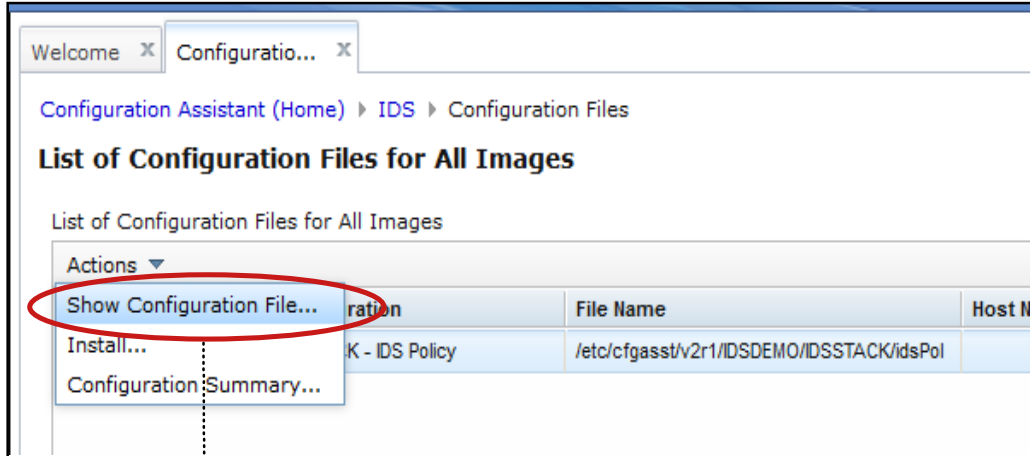
Actions

Image	Configuration	File Name	Host Name	Last Install
IDSDEMO	IDSSTACK - IDS Policy	/etc/cfgasst/v2r1/IDSDEMO/IDSSTACK/idsPol		Never

next page



# Show the configuration file to be installed



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

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

## Install File

\* Install file name:

Select installation method

Save to disk  
 FTP

FTP information

\* Host name:

\* Port number:

\* 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)

Configuration	File Name
K - IDS Policy	/etc/cfgasst/v2r1/IDSDEMO/IDSSTACK/idsPol

# Perform application setup tasks - All workflows view

IBM z/OS Management Facility Welcome user1 Log out IBM

Welcome x Configuratio... x Workflows x Help

### Workflows

Simplifies tasks through guided step-based workflows, and provides administrative functions for assigning workflow responsibilities and tracking progress.

Workflow Name Filter	Description Filter	Version Filter	Vendor Filter	Owner Filter	System Filter
<input checked="" type="checkbox"/> z/OS Communications Server: Setup to run Traffic Regulation Management Daemon (TRMD) - Workflow_0	z/OS Communications Server: Setup to run Traffic Regulation Management Daemon (TRMD)	1.0	IBM	user1	XESDEV.MVS160 (MVS160_00)
<input checked="" type="checkbox"/> z/OS Communications Server: Setup for Syslogd - Workflow_0	z/OS Communications Server: Setup for Syslogd	1.0	IBM	user1	XESDEV.MVS160 (MVS160_00)
<input checked="" type="checkbox"/> Setting up to run IP Defensive Filters with Defense Manager Daemon (DMD) - Workflow_0	Setting up to run IP Defensive Filters with Defense Manager Daemon (DMD)	1.0	IBM	user1	XESDEV.MVS160 (MVS160_00)
<input type="checkbox"/> Set up to run Network Security Services (NSS) - Workflow_0	Set up to run Network Security Services (NSS)	1.0	IBM	user1	XESDEV.MVS160 (MVS160_00)
<input type="checkbox"/> z/OS Communications Server: IP Security with IKE - Workflow_0	z/OS Communications Server: IP Security with IKE	1.0	IBM	user1	XESDEV.MVS160 (MVS160)
<input type="checkbox"/> z/OS Communications Server: Install Sample Profiles for TCP/IP Components - Workflow_0	z/OS Communications Server: Install Sample Profiles for TCP/IP Components	1.0	IBM	user1	XESDEV.MVS160 (MVS160)
<input checked="" type="checkbox"/> z/OS Communications Server: Setup to run Policy Agent - Workflow_0	z/OS Communications Server: Setup to run Policy Agent	1.0	IBM	user1	XESDEV.MVS160 (MVS160)

next page

# Perform application setup tasks - Specific workflow view

Welcome x Configuratio... x Workflows x

Workflows > z/OS Communications Server: Setup to run Policy Agent - Workflow\_0 Help

## z/OS Communications Server: Setup to run Policy Agent - Workflow\_0

[Notes](#) | [History](#)

Description: z/OS Communications Server: Setup to run Policy Agent

Owner: user1      System: XESDEV.MVS160 (MVS160)

Percent complete:

Steps complete: 0 of 7

Workflow Steps

Actions ▾  Search

	State Filter	No. Filter	Title Filter	Owner Filter	Skill Category Filter	Assignees Filter
<input type="checkbox"/>	Unassigned	1	■ Define the RACF user ID for Policy Agent		Basic JCL	
<input type="checkbox"/>	Unassigned	2	■ Setup for Policy Agent to execute operator commands		Basic JCL	
<input type="checkbox"/>	Unassigned	3	■ Setup for Policy Agent to have access to the BPX.DAEMON RACF profile		Basic JCL	
<input type="checkbox"/>	Unassigned	4	■ Permit the display of policies, access to policies by Configuration Assistant and policy clients		Basic JCL	
<input type="checkbox"/>	Unassigned	5	■ Sample Policy Agent Configuration for Image		Basic JCL	
<input type="checkbox"/>	Unassigned	6	■ Sample Policy Agent Configuration for Stack		Basic JCL	
<input type="checkbox"/>	Unassigned	7	■ Sample started procedure for the Policy Agent		Basic JCL	

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

- **Integrated Intrusion Detection Services for z/OS Communications Server**

- **Session # 15195**

- **QR Code:**

