



Software Group | Enterprise Networking Solutions

Integrated Intrusion Detection Services for z/OS Communications Server

SHARE Session 10829

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?

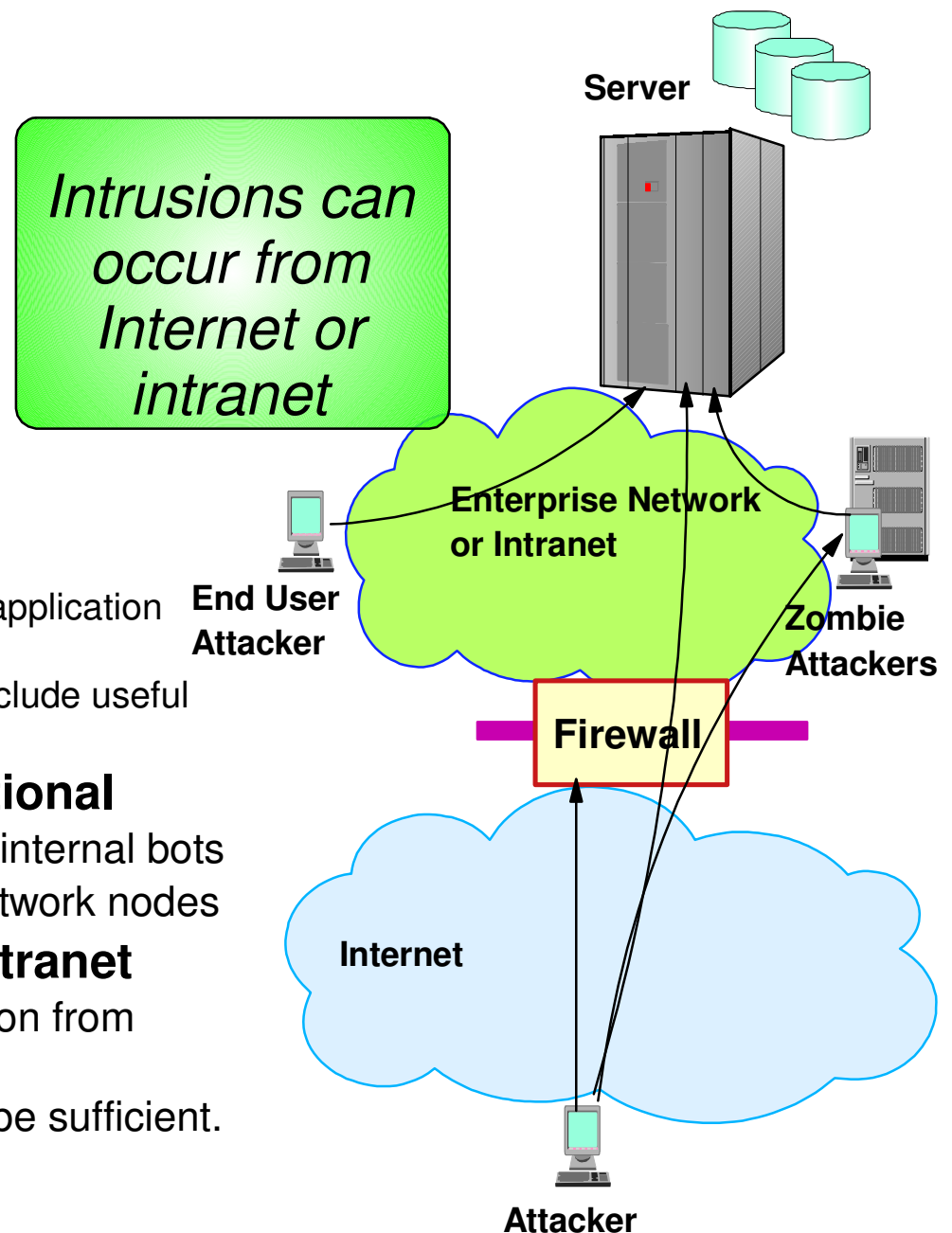
- ▶ Information Gathering
 - Network and system topology
 - Data location and contents
- ▶ Eavesdropping / Impersonation / Theft
 - On the network / on the server
 - Base for further attacks on others
 - ✓ Amplifiers
 - ✓ Robot or zombie
- ▶ Denial of Service
 - Attack on availability
 - ✓ Single Packet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

■ Attacks can be deliberate or unintentional

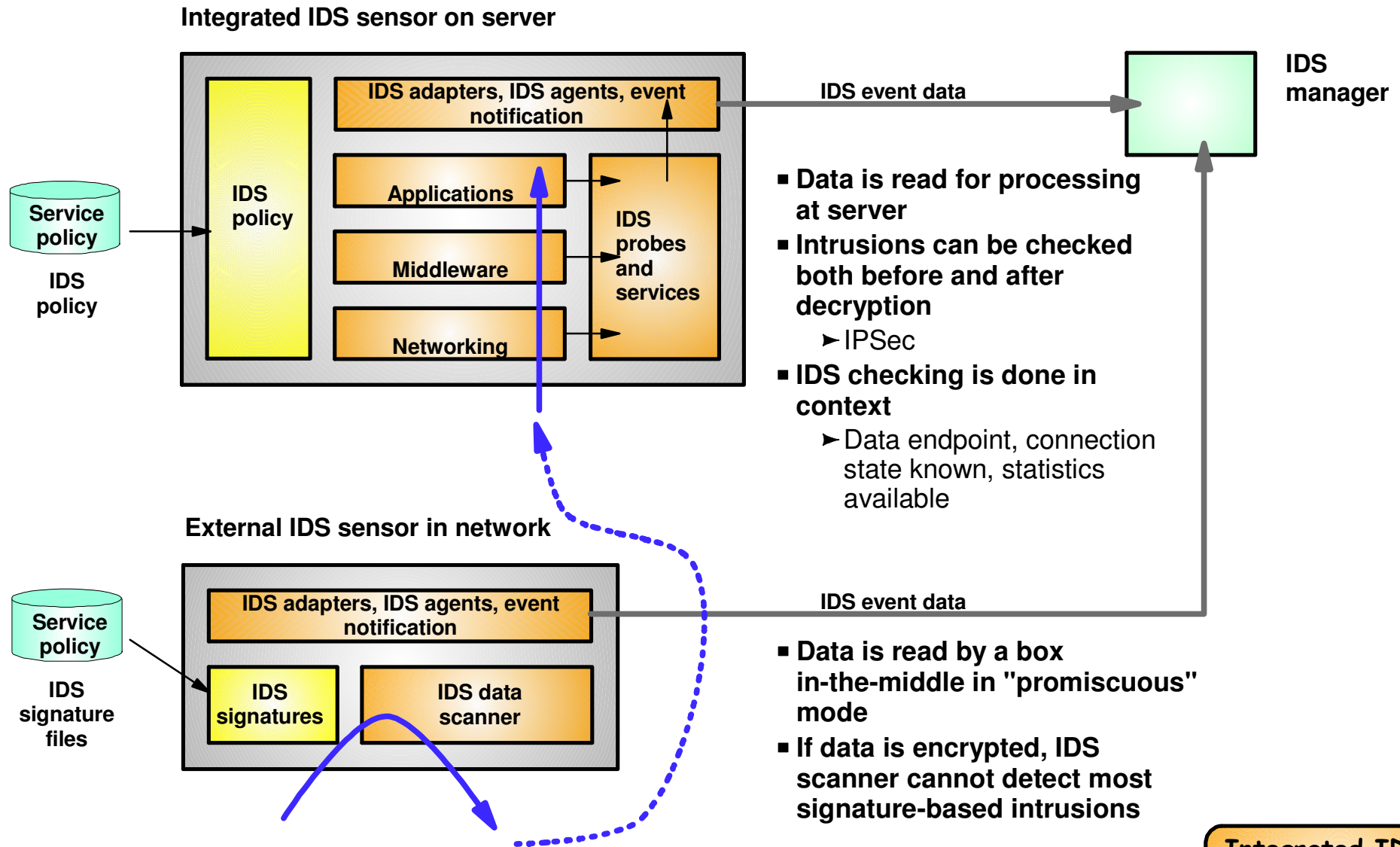
- ▶ Deliberate: malicious intent from outside or internal bots
- ▶ Unintentional: various forms of errors on network nodes

■ 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

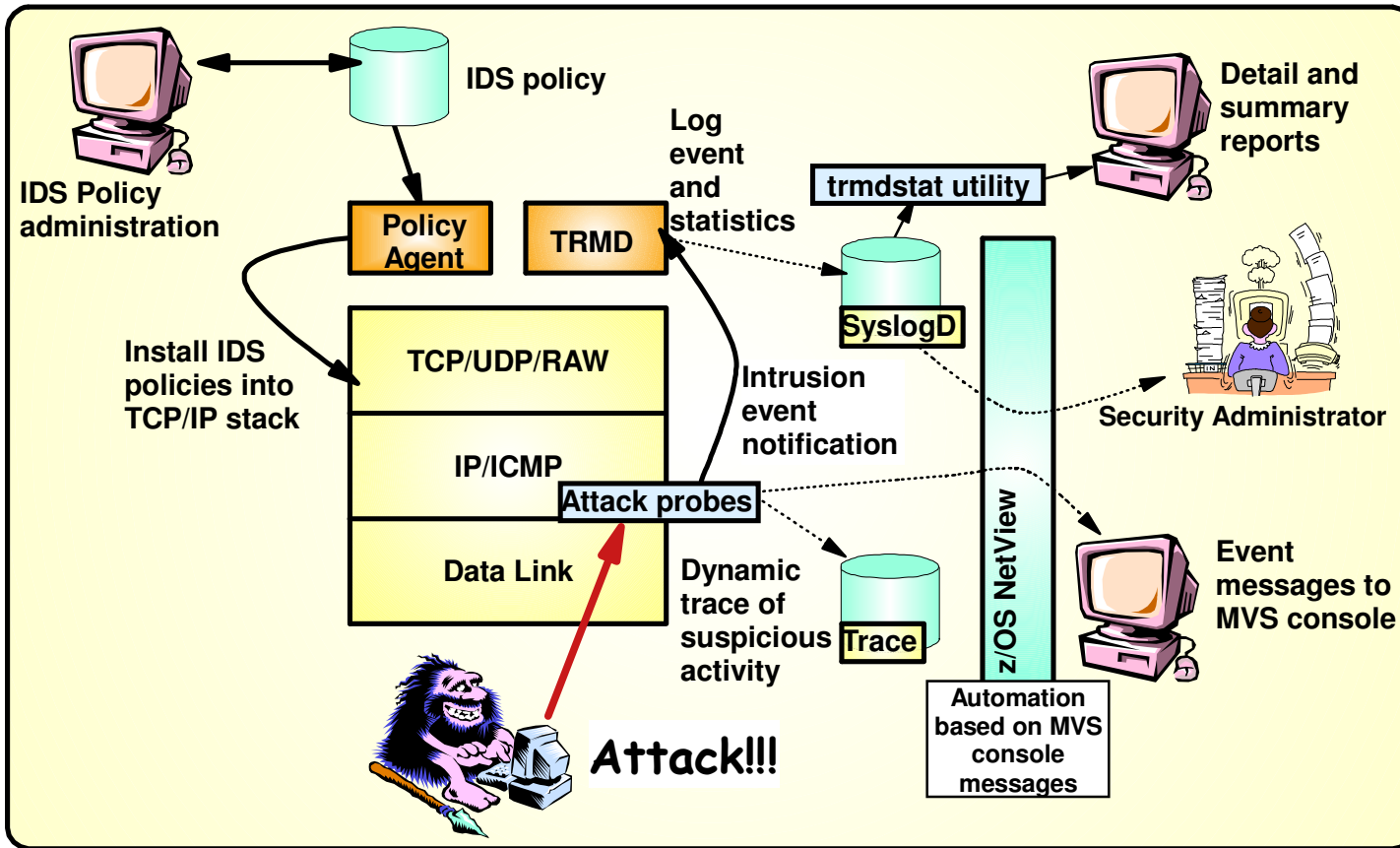


Integrated vs. External Intrusion Detection Concepts



Integrated IDS on z/OS complements external IDS technologies

Intrusion Detection Services Overview



Events detected

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

Defensive methods

- Packet discard
- Limit 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

New Support Added in z/OS V1R13

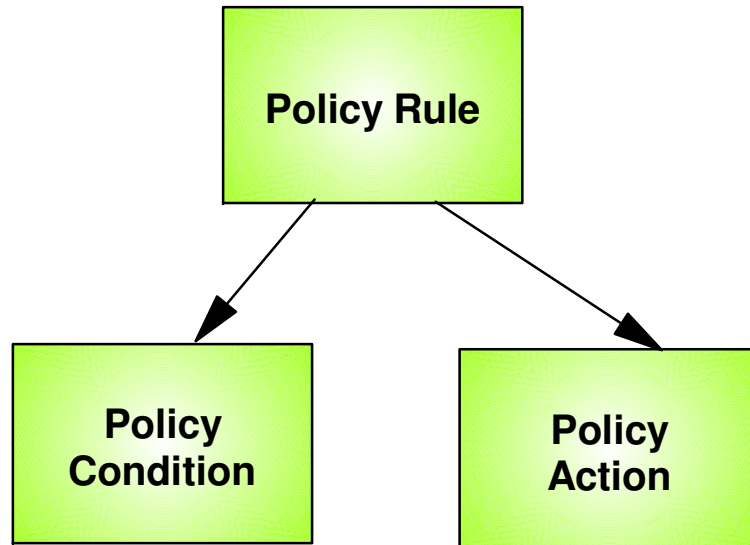
- Extend existing support to IPv6
- New attack types:
 - ▶ Data hiding
 - ▶ TCP Queue Size
 - ▶ Global TCP Stall
 - ▶ Enterprise Extender protections

IDS Configuration

- IDS is configured with IDS policy
 - ▶ IDS policy defines intrusion events to monitor and actions to take
- Policy definitions are stored in policy repository
 - ▶ File or data set
 - ▶ LDAP (no longer being enhanced)
- Policy Agent reads policy definitions from policy repository
 - ▶ Policy definitions are processed by Policy Agent and installed in the TCP/IP stack

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

* = New in V1R13

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*

* = New in V1R13

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

* = New in V1R13

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 (1 of 2)

- 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
- 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
- UDP perpetual echo
 - ▶ Detects traffic between IPv4 and IPv6* UDP applications that unconditionally respond to every datagram received
- ICMP, ICMPv6* redirect restrictions
 - ▶ Detects receipt of ICMP redirect to modify routing tables.
- 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

* = New in V1R13

Attack Categories (2 of 2)

New in V1R13, for both IPv4 and IPv6...

- Data hiding
 - ▶ Detects attempts to pass hidden data in packet header and extension fields

- TCP queue size
 - ▶ Provides IDS configuration for already-existing protection of TCP queues
 - ▶ Configurable "reset connection" provided in addition to usual notification actions
 - ▶ Exclusion list can be specified

- Global TCP stall
 - ▶ Detects cases where large number and percentage of TCP connections are stalled
 - ▶ Configurable "reset connection" provided in addition to usual notification actions

- Enterprise Extender-specific attacks
 - ▶ 4 different attack types (more on this later)
 - ▶ Exclusion list can be specified for each individual type
 - ▶ Appropriate defensive action available for each type

IPv6 support for pre-V1R13 Attacks

Existing IPv4 attack type	IPv6 implementation
<ul style="list-style-type: none">• Malformed packet• ICMP redirect restrictions• UDP perpetual echo• Flood (both interface flood and TCP SYN flood)	Existing IPv4 support extended to IPv6. No new configuration needed.
IP protocol restrictions (specifies a list of restricted IP protocol values)	IPv6 next header restrictions (specifies a list of restricted IPv6 next header values, which may include IP protocol values)
IP option restrictions (specifies a list of restricted IPv4 options)	<ul style="list-style-type: none">• IPv6 destination option restrictions (specifies a list of restricted IPv6 destination options)• IPv6 hop-by-hop option restrictions (specifies a list of restricted IPv6 hop-by-hop options)
Outbound RAW (specifies a list of restricted IP protocols for IPv4 and imposes other restrictions)	IPv6 outbound RAW (specifies a list of restricted IP protocols for IPv6 and imposes other restrictions)

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 (IfcFloodPercentage) 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:

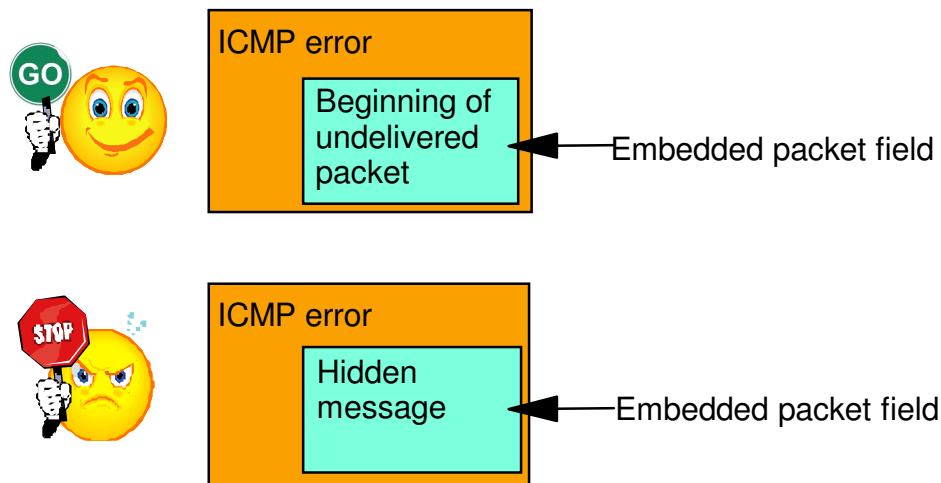
time interval	inbound cnt	discard cnt	discard rate	notes
> 1 min	13,000	2000	N/A	took longer than a minute to see the minimum discard count, so not a flood and discard rate not calculated.
< 1 min	30,000	2000	6.6%	not a flood, rate <10%
< 1 min	20,000	2000	10%	interface flood start detected. Run 1 minute 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.

Data Hiding Protection

V1R13

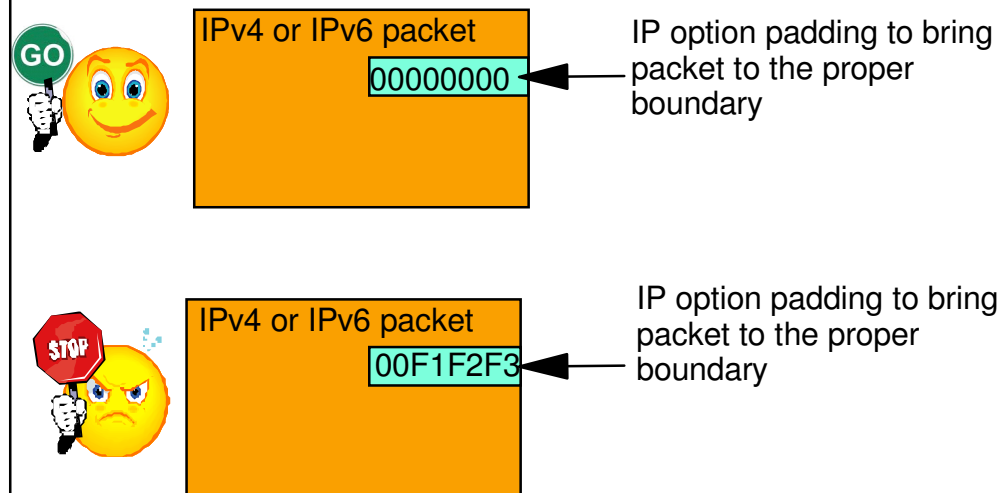
- The structure of protocol headers afford the opportunity embed "hidden data" in packets (at the source host / in the network)
- V1R13 introduces the Data Hiding attack type to protect against such hidden data
- In addition to notifications you can configure an optional packet discard action
- Two forms of data hiding protection can be independently enabled

Exploitation of ICMP and ICMPv6 error messages



Before processing an inbound ICMP or ICMPv6 error message Comm Server ensures the source address of the embedded message matches the destination address of the error message.

Exploitation of IPv4 and IPv6 option pad



Comm Server checks padding space for non-zero data.

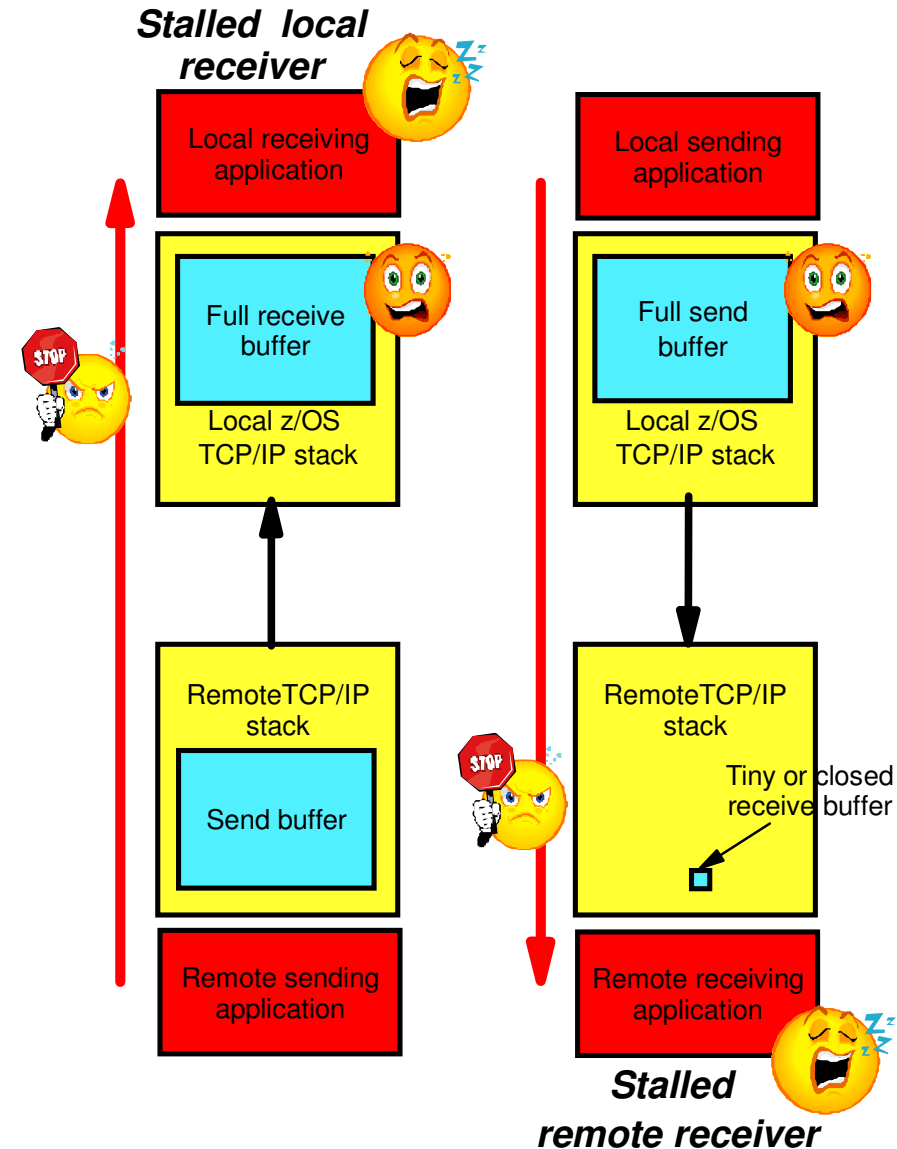
TCP Queue Size Protection

V1R13

- Builds upon V1R11 behavior. In that release, when a queue becomes constrained...
 - ▶ Data on that queue is marked "page eligible"
 - ▶ Syslogd message is issued to indicate constraint condition for that connection
 - ▶ A manual action can be taken to reset connection (netstat drop / -d) -- NO automated reset available

V1R13 IDS TCP queue size attack protection...

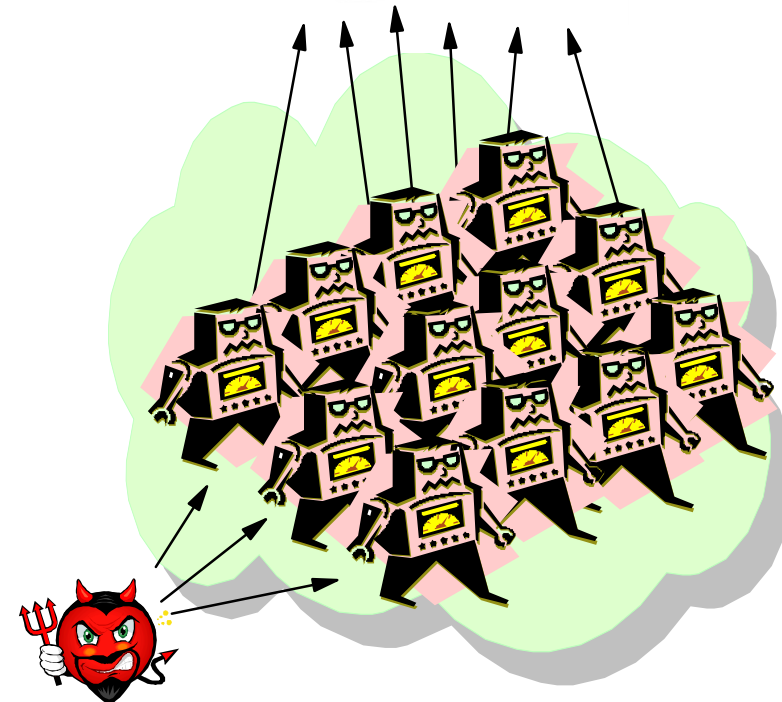
- Avoids/minimizes storage constraint conditions related to amount of storage consumed for TCP queues:
 - ▶ Receive queue (protection from stalled z/OS applications)
 - ▶ Out-of-order queue (protection from misbehaved remote senders)
 - ▶ Send queue (protection from stalled or misbehaved remote receivers)
- Evaluated on a per-connection basis
- Constraint condition triggered when:
 - ▶ Data is on queue for at least 60 seconds OR
 - ▶ A configurable threshold amount of data has been on queue for at least 30 seconds
 - very short / short / long / very long
 - this data amount is a fixed internal value in V1R11
- Constraint condition ends when data amount AND age falls below threshold.
- Exclusion list for z/OS send queue available for cases where such behavior is legitimate (like a printer that's out of paper):
 - ▶ Based on IP addr and port
 - ▶ Constrained queue storage still marked as "page eligible"



Global TCP Stall Protection

V1R13

- Protect 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 (which is set by the peer) < smaller of largest send window seen for this connection and Default MTU
 - ▶ 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
- Global TCP stall condition is exited when...
 - ▶ Number of stalled connections drops to < 25% of the total OR
 - ▶ Total number of connections drops to < 450



Comparing TCP queue size and TCP global stall attack types

V1R13

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

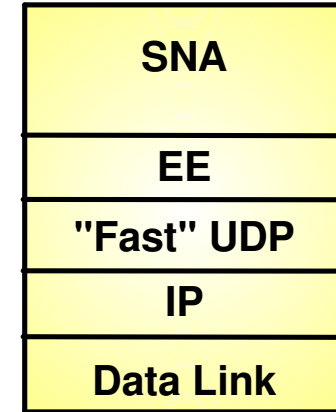
▶ **EE XID Flood**

- 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

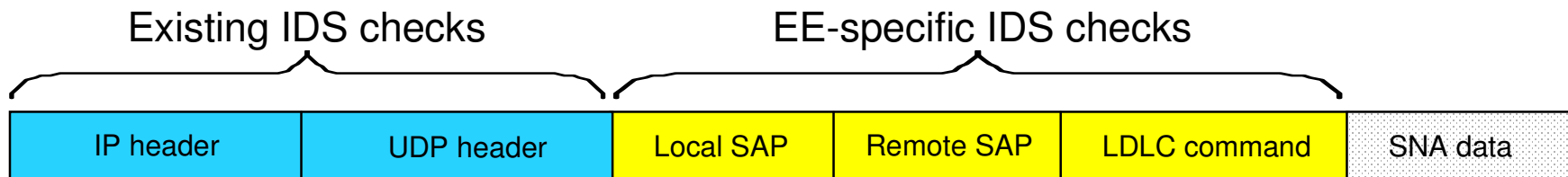
■ Usual IDS reporting options available (exception: no IDS trace for EE XID flood)



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



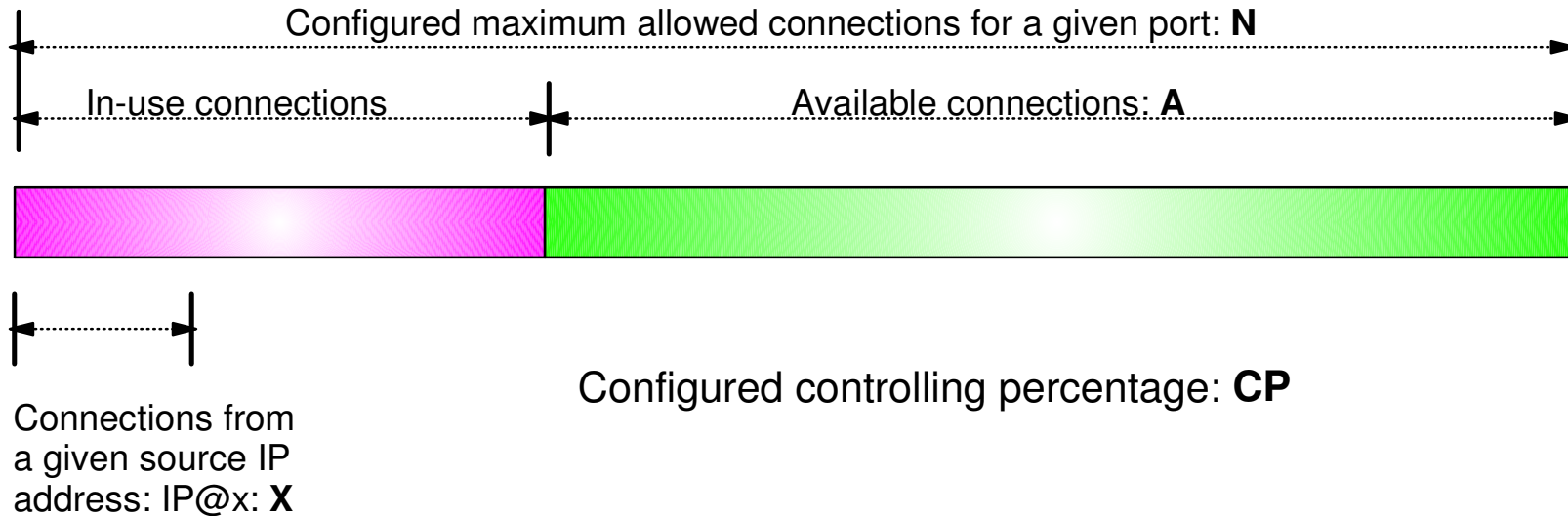
Traffic Regulation for TCP

- 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
 - ▶ VERY SHORT
 - ▶ SHORT
 - For applications that tend to receive data faster than they can process it
 - ▶ LONG
 - ▶ 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

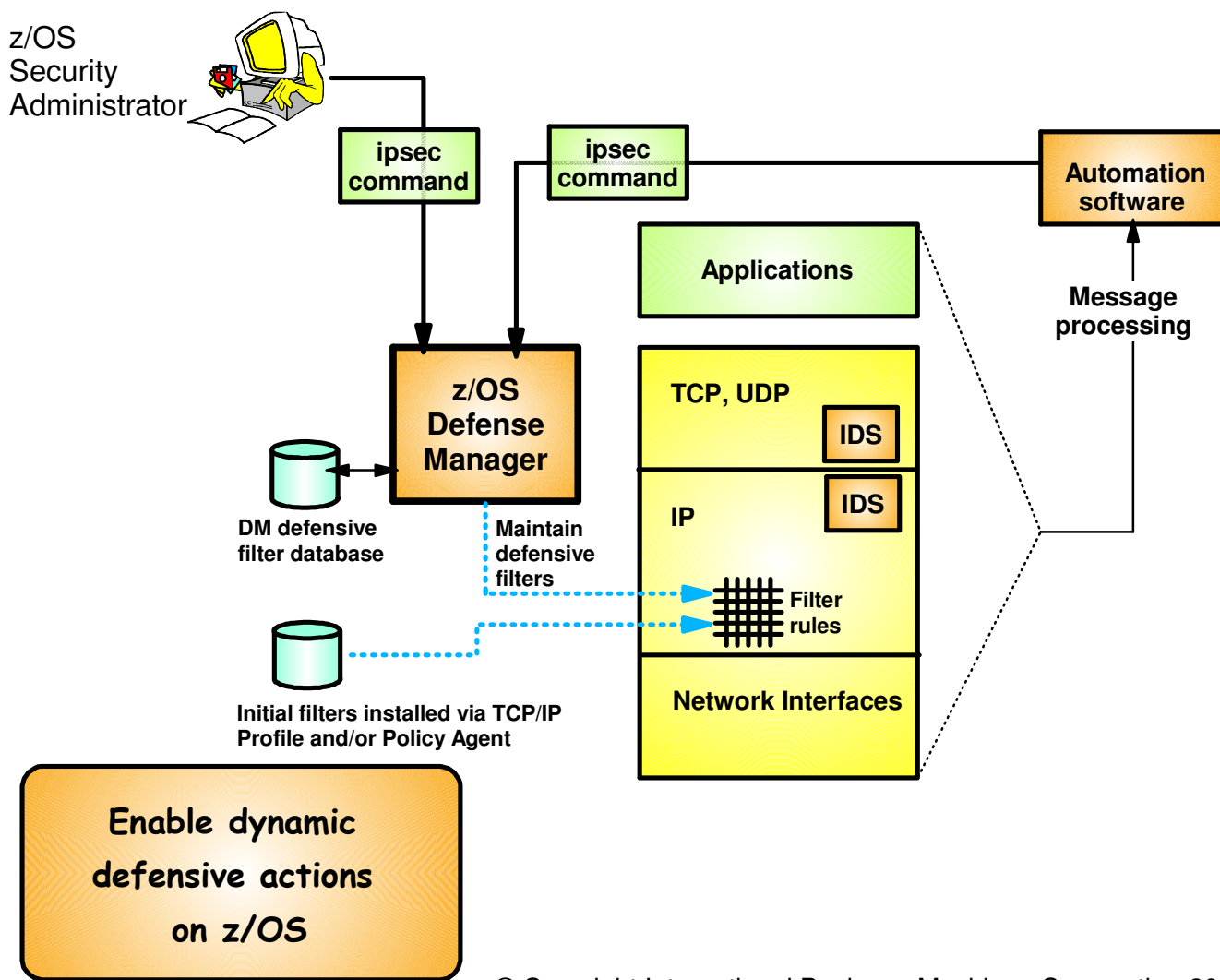
■ Traffic Regulation Events

- ▶ Controlled by IDS policy action
 - TCP - Connection limiting
 - UDP - Packet discard

* = New in V1R13

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**
- **Already supports IPv6**

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
 - Connection and IDS
 - ▶ Event type summary reports
 - For Connection, Attack, Flood, Scan, TCP and UDP TR information
 - ▶ Event type detail reports
 - For Connection, 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. Inspect configured IDS policy for correctness
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

Defining IDS Policy



Configuration Assistant

for z/OS Communications Server

Version 1, Release 13



(c) Licensed Materials - Property of IBM Corp. (c) Copyright by IBM Corp. and other(s) 2006, 2011. All Rights Reserved. U.S Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.. IBM is a registered trademark of IBM Corp. in the U.S. and/or other countries. Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.



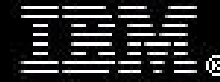
- **GUI-based approach to configuring:**
 - ▶ IDS
 - ▶ AT-TLS
 - ▶ IPSec and IP filtering
 - ▶ QoS
 - ▶ Policy-based Routing (PBR)
 - ▶ Defense Manager Daemon
- **Focus on high level concepts vs. low level file syntax**
- **Runs under z/OSMF (strategic) or as a Windows application**
- **Builds and maintains**
 - ▶ Policy files
 - ▶ Related configuration files
 - ▶ JCL procedures and RACF directives
- **Supports import of existing policy files**

Download the Windows-based Configuration Assistant at: <http://tinyurl.com/cgoqsa>

IDS Policy Configuration Steps with the Configuration Assistant

1. Download and install the Configuration Assistant configuration tool
<http://tinyurl.com/cgoqsa>
2. 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
3. Create system image and TCP/IP stack image
4. Associate new requirements map with TCP/IP stack
5. Perform policy infrastructure and application setup tasks
6. Transfer IDS policy to z/OS

Configuration Assistant for z/OS Communications Server



Configuration Assistant for z/OS Communications Server

Version 1, Release 13



(c) Licensed Materials - Property of IBM Corp. (c) Copyright by IBM Corp. and other(s) 2006, 2011.
All Rights Reserved. U.S Government Users Restricted Rights - Use, duplication or disclosure
restricted by GSA ADP Schedule Contract with IBM Corp.. IBM is a registered trademark of
IBM Corp. in the U.S. and/or other countries. Java and all Java-based trademarks are
trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.




Start a new IDS configuration

File Edit Perspective Help

Main Perspective

Navigation tree

- z/OS Images
 - Image - DEMOMVS



[z/OS Communication Server technologies](#)

Select the technology you want to configure and click Configure.

Technology	Description
AT-TLS	Application Transparent - Transport Layer Security
DMD	Defense Manager Daemon
IPSec	IP Security
IDS	Intrusion Detection Services
NSS	Network Security Services
QoS	Quality of Service
DRP	Policy Based Routing

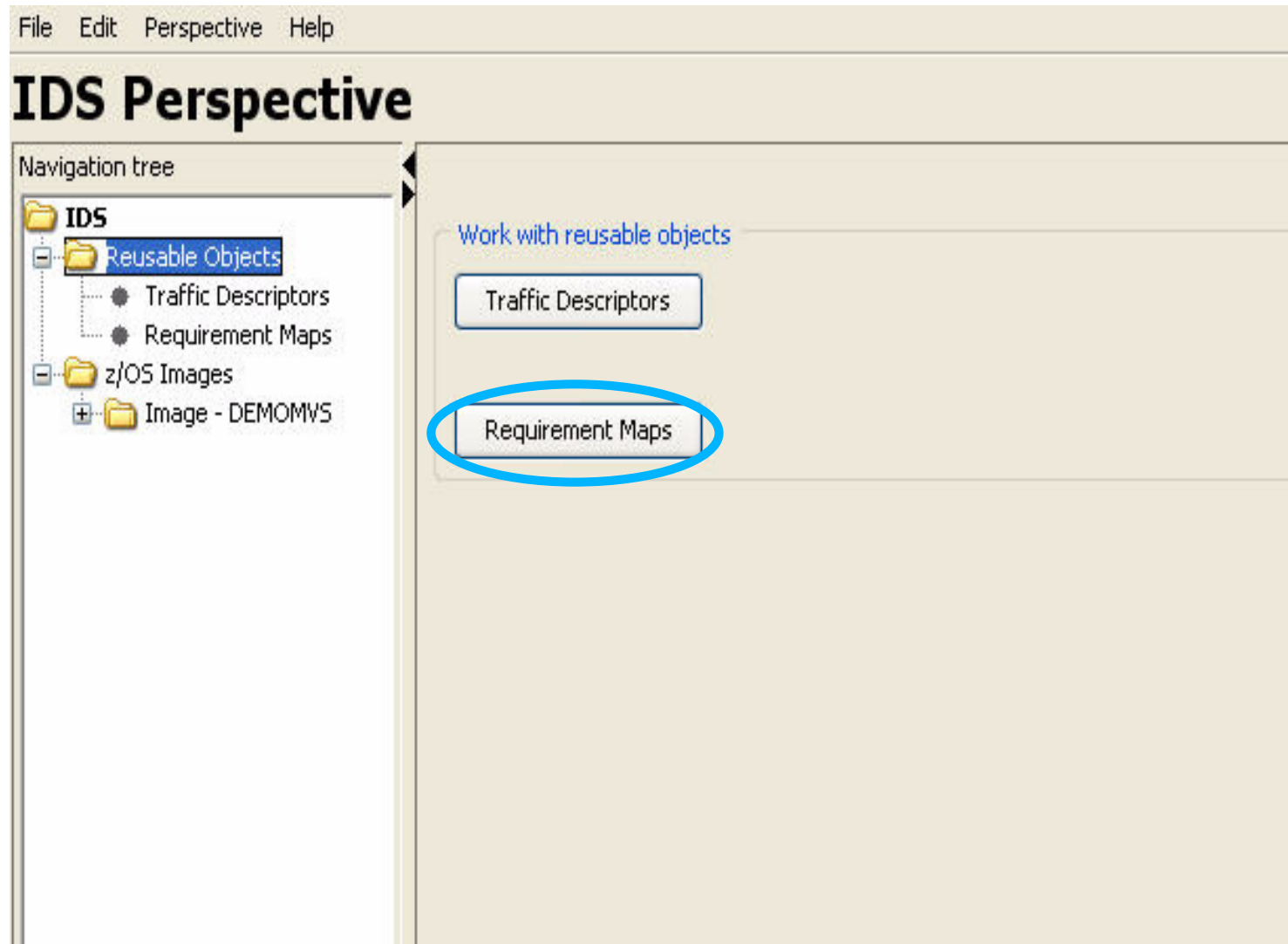
Configure

[Work with settings for z/OS images](#)

Add a New z/OS Image...

To work with a specific z/OS image or TCP/IP stack, select the z/OS image or TCP/IP stack from the navigation tree.

Create IDS policy objects



Evaluate IDS_Default requirements map

The screenshot shows the 'IDS Perspective' window with a menu bar (File, Edit, Perspective, Help) and a navigation tree on the left. The tree includes 'IDS', 'Reusable Objects', 'Traffic Descriptors', 'Requirement Maps', 'z/OS Images', and 'Image - DEMOMVS'. The 'Requirement Maps' folder is selected, and a dotted arrow points to the 'IDS_Default' entry in the main table. The table has two columns: 'Name' and 'Description'. The 'IDS_Default' row is highlighted with a blue background. Below the table is a horizontal scrollbar and a row of buttons: 'Add...', 'Copy...', 'Modify...', 'Delete', 'View Details...', and 'Show Where Used...'. At the bottom right, there are buttons for 'Main Perspective', 'Close', 'Help', and a question mark icon. A red alarm bell icon with lightning bolts is positioned above the table, with the text 'List of all defined requirement map objects' next to it.

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

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)

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	Console Parameters: No <hr/> SYSLOG Parameters: SYSLOG: Yes SYSLOG Level: 4 - Warning
IPv6 Outbound Raw Attack ¹	IPv6OutboundRaw	Report Events	Use Default Report Settings	None	
IPv6 Destination Options Attack ¹	IPv6DestinationOptions	Report Events	Use Default Report Settings	None	
IPv6 Hop-by-Hop Options Attack ¹	IPv6HopByHop	Report Events	Use Default Report Settings	None	
IPv6 Next Header Attack ¹	IPv6NextHeader	Report Events	Use Default Report Settings	None	
TCP Queue Size Attack ¹	TcpQueueSize	Report Events	Use Default Report Settings	None	
Global TCP Stall Attack ¹	GlobalTCPStall	Report Events	Use Default Report Settings	None	
Flood Attack	Flood	Both Drop and Report	Use Default Report Settings	None	
Perpetual Echo Attack	Echo	Report Events	Use Default Report Settings	None	

Details view of IDS_Default requirements map (2 of 4)

Attack	Protocol	Action	Report Settings	Severity	Statistics Parameters:
IPv4 Protocols Attack	IPv4Protocol	Report Events	Use Default Report Settings	None	Statistics Parameters: Statistics: Yes Statistics Interval: 60 Minutes Report Stat if no events: Yes <hr/> Trace Parameters: No
IPv4 Options Attack	IPv4Option	Report Events	Use Default Report Settings	None	
ICMP Redirect Attack	ICMPRedirect	Report Events	Use Default Report Settings	None	
Malformed Packet Attack	MalformedPacket	Both Drop and Report	Use Default Report Settings	None	
IPv4 Outbound Raw Attack	IPv4OutboundRaw	Report Events	Use Default Report Settings	None	
IPv4 Fragment Attack	IPv4Fragmentation	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.

Details view of IDS_Default requirements map (3 of 4)

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.

Details view of IDS_Default requirements map (4 of 4)

(. . . several intervening pages...)

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

Use IDS_Default as a starting point

The screenshot shows the 'IDS Perspective' application window. The menu bar includes 'File', 'Edit', 'Perspective', and 'Help'. The title bar reads 'IDS Perspective'. On the left is a 'Navigation tree' with the following structure:

- IDS
 - Reusable Objects
 - Traffic Descriptors
 - Requirement Maps
 - z/OS Images
 - Image - DEMOMVS

The 'Requirement Maps' folder is selected. The main area displays a red alarm bell icon with the text 'List of all defined requirement map objects'. Below this is a table with the following content:

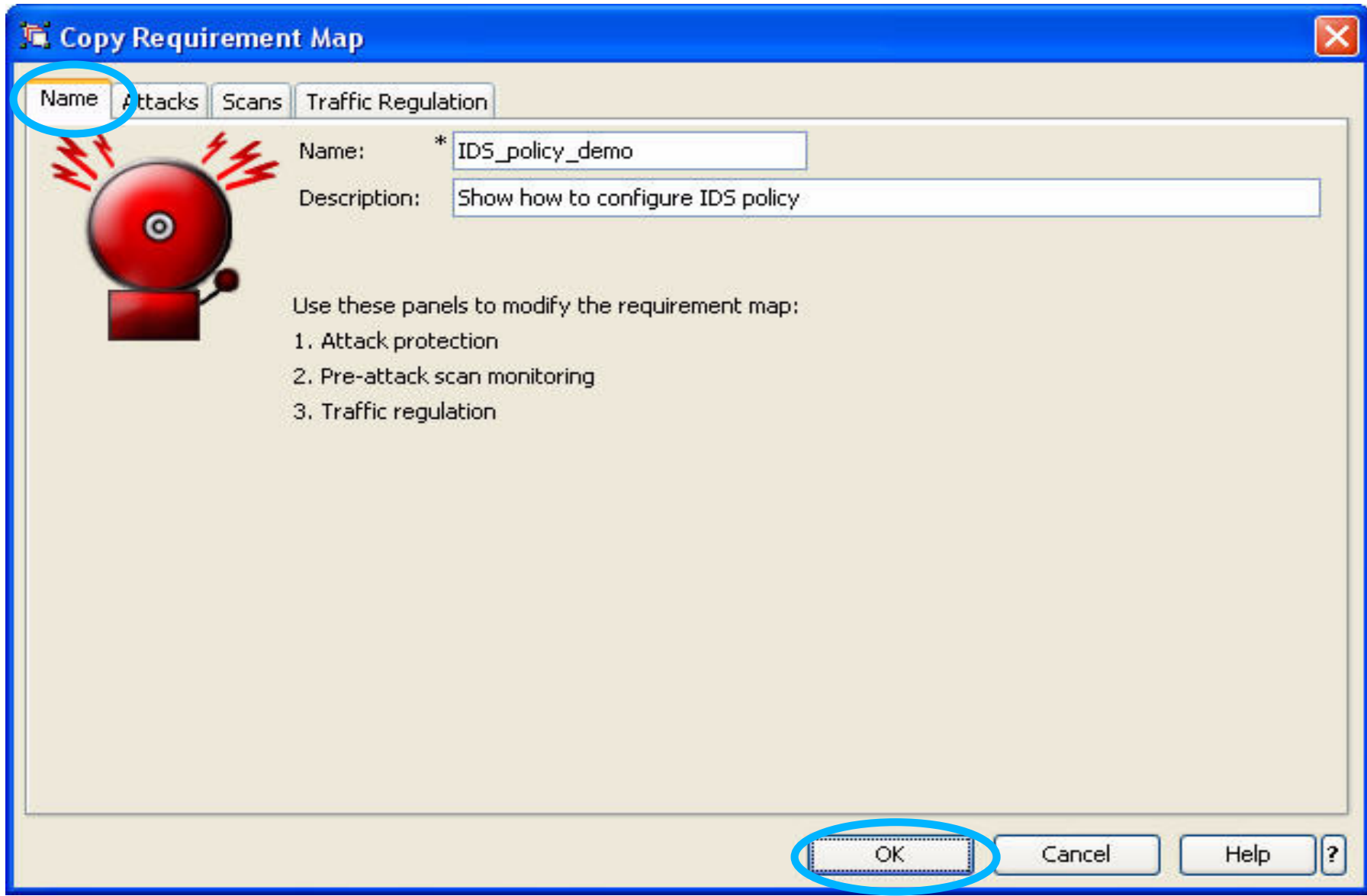
Name ▲	Description
IDS_Default	IBM Supplied: Intrusion Detection Services Starter Set

At the bottom of the table area are several buttons: 'Add...', 'Copy...', 'Modify...', 'Delete', 'View Details...', and 'Show Where Used...'. At the very bottom of the window are 'Main Perspective', 'Close', 'Help', and a question mark icon. A dotted arrow points from the 'Copy...' button to the text 'Using IDS_Default as a base' in the text block below.

Using IDS_Default as a base

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

Name new requirements map



Modify copied default requirements map

The screenshot shows the 'IDS Perspective' application window. On the left is a 'Navigation tree' with folders for 'IDS', 'Reusable Objects', 'Traffic Descriptors', 'Requirement Maps', 'z/OS Images', and 'Image - DEMOMVS'. The 'Requirement Maps' folder is selected. The main area displays a 'List of all defined requirement map objects' with a red alarm bell icon. Below this is a table with two columns: 'Name' and 'Description'. The table contains two rows: 'IDS_Default' (IBM Supplied: Intrusion Detection Services Starter Set) and 'IDS_policy_demo' (Show how to configure IDS policy). Below the table is a toolbar with buttons for 'Add...', 'Copy...', 'Modify...', 'Delete', 'View Details...', and 'Show Where Used...'. The 'Modify...' button is circled in red. At the bottom right of the toolbar are buttons for 'Main Perspective', 'Close', 'Help', and a question mark icon.

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

→ next page

Attack protection enabled by default

The screenshot shows the 'Modify Requirement Map' dialog box with the 'Attacks' tab selected. The 'Enable attack protection' checkbox is checked. Below it, a 'Steps' section provides instructions on how to manage attack protection. A table titled 'Enabled protection' lists various attack types and their corresponding protection actions. At the bottom left, a button labeled 'Default Report Settings for Attacks...' is circled in blue, with an arrow pointing to the text 'next page'.

Name: Attacks | Scans | Traffic Regulation

Use this panel to indicate if you want attack protection

Enable attack protection

Steps

1. Select the action for each enabled attack type.
2. To disable protection for an attack type, select the row from the Enabled protection table and click the "Disable" button.
3. To enable protection for a specific attack type, select a row from the Attack type table and click the "Enable" button.

You will be prompted for additional details related to your attack type selection. Fill in the details and click OK.

Attack type

Enabled protection

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
TCP Queue Size Attack	TcpQueueSize	Report Events
Global TCP Stall Attack	GlobalTCPStall	Report Events
Flood Attack	Flood	Both Drop and Report
Perpetual Echo Attack	Echo	Report Events
IPv4 Protocols Attack	IPv4Protocol	Report Events

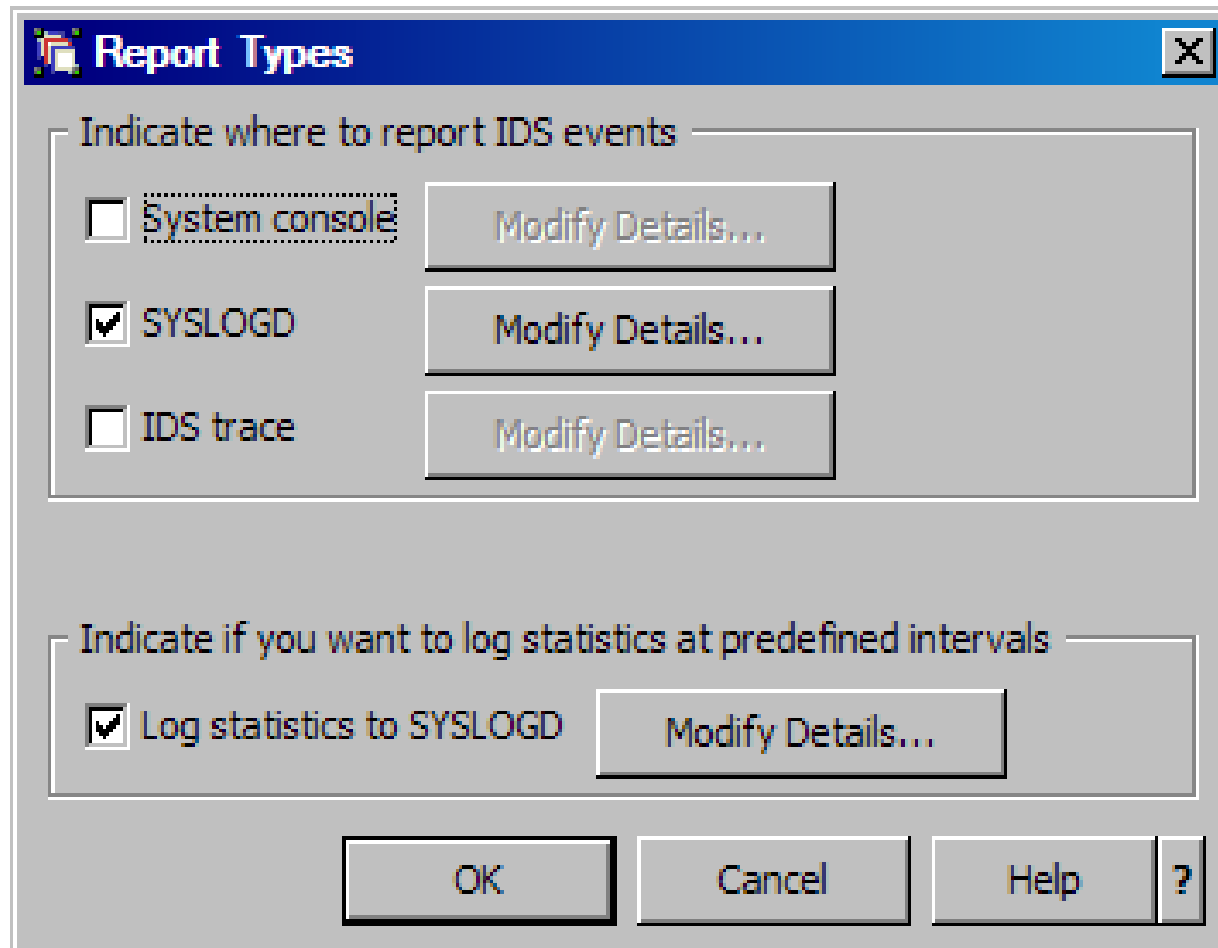
Enable --> | <-- Disable

Modify... | Copy... | Advanced... | View Details...

Default Report Settings for Attacks... → next page

OK | Cancel | Help ?

Customize report settings



Enable scan policy

Modify Requirement Map

Name Attacks **Scans** Traffic Regulation

Use this panel to indicate if you want to monitor for preattack scans

Enable scans

Steps

1. To enable a scan for a particular traffic descriptor, select from the traffic descriptors table and click the "Enable" button.
2. Select the monitor level for each enabled scan.
3. To disable scan protection for a traffic descriptor, select the row from the Enabled scans table and click the "Disable" button.

Traffic descriptors list

- Centralized_Policy_Server
- CICS
- DNS
- EE
- FTP-Server
- FTP-Server-SSL
- ICMP-IPv6
- IKE
- IKE-NAT
- Kerberos
- LBA-Advisor
- LBA-Agent
- LDAP-Server
- IPD

Enabled scans

Enabled Traffic Descriptor	Rule Name	Sensitivity
All_Well-Known_TCP	All_Well-Known_TCP	Medium
All_Well-Known_UDP	All_Well-Known_UDP	Medium
ICMP	ICMP	High

Traffic Descriptors... Modify... Copy Advanced... Move Up Move Down View Details...

Default Report Settings for Scans... **Modify Fast and Slow Scan Settings...** → next page

OK Cancel Help ?

Modify Global Scan Settings

Global Scan Settings [X]

Fast scan settings

Fast scan interval: * (minutes, 1-1440)

How many accesses within scan interval indicate an attack: * (1 - 64)

Slow scan settings

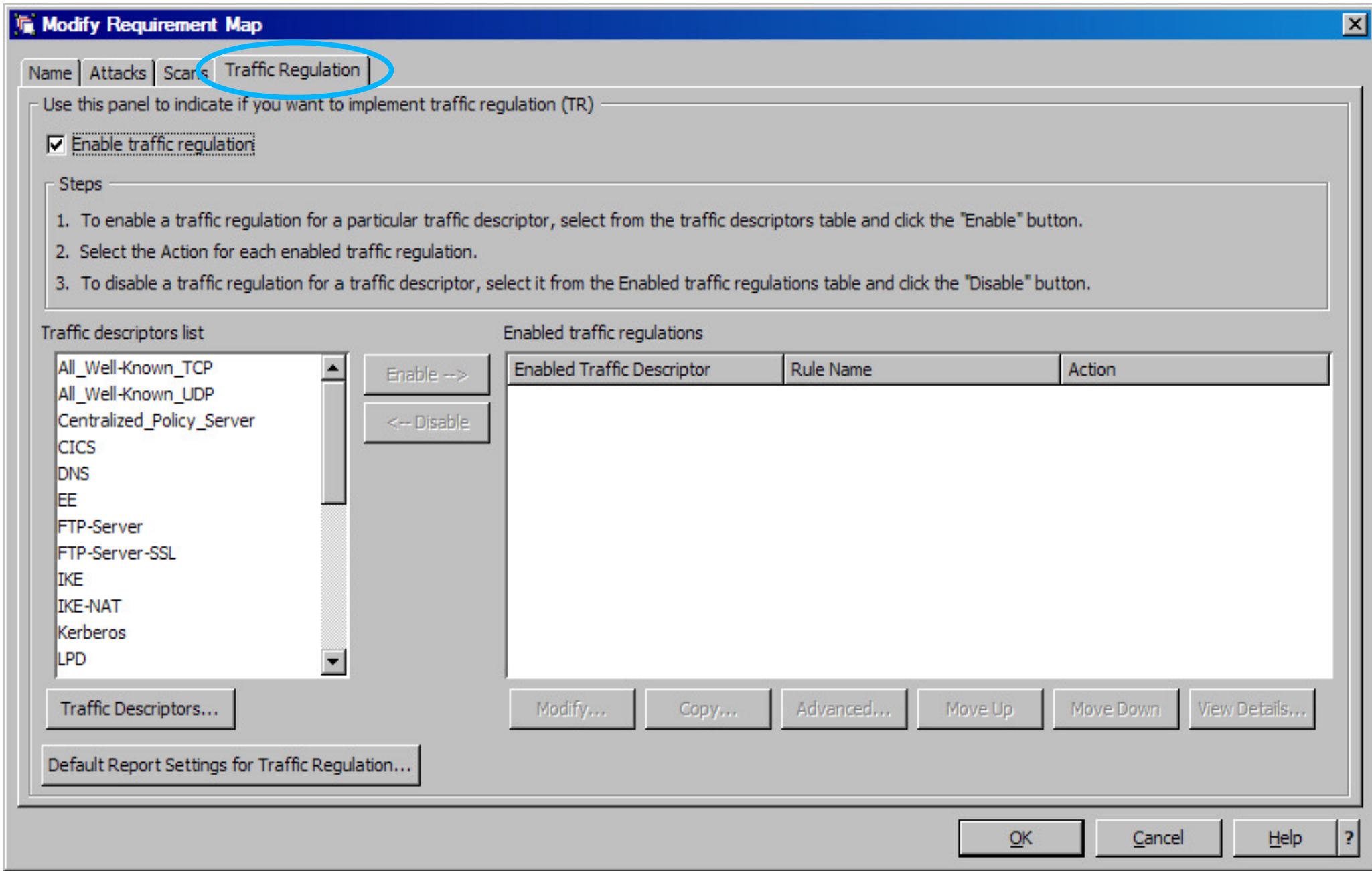
Enable slow scans

Slow scan interval: * (minutes, 1-1440)

How many accesses within scan interval indicate an attack: * (1 - 64)

OK Cancel Help ?

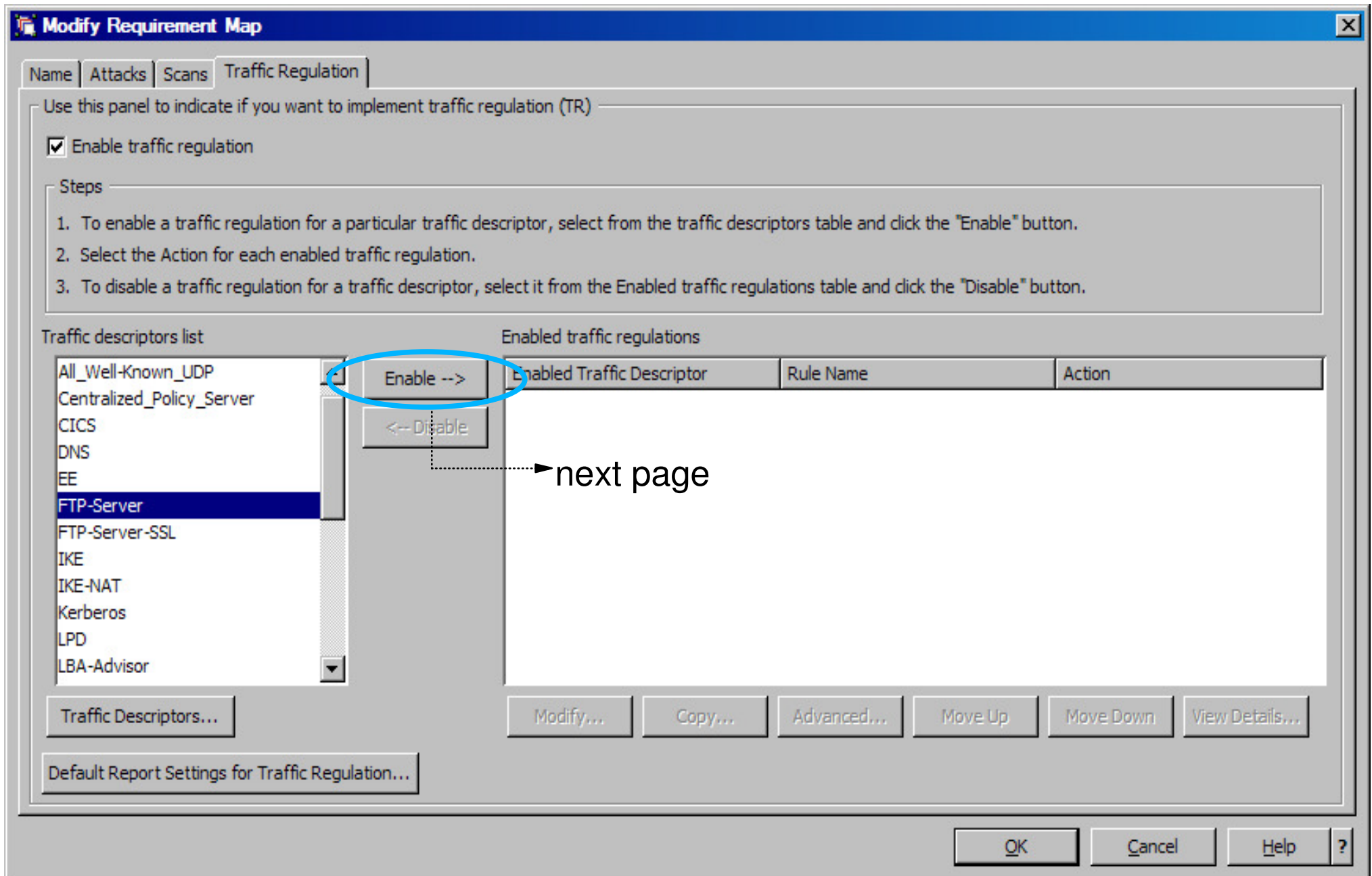
Enable traffic regulation protection



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 Details [X]

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

Traffic regulation identification

Name: *

Traffic descriptor: FTP-Server

Action: Limit and Report

Enter parameters for TCP traffic

Limit by total connections

Maximum number of connections: * (0-65535)

Limit by percentage of total connections

No limit per host

Limit each host to the following percentage of the maximum connections:

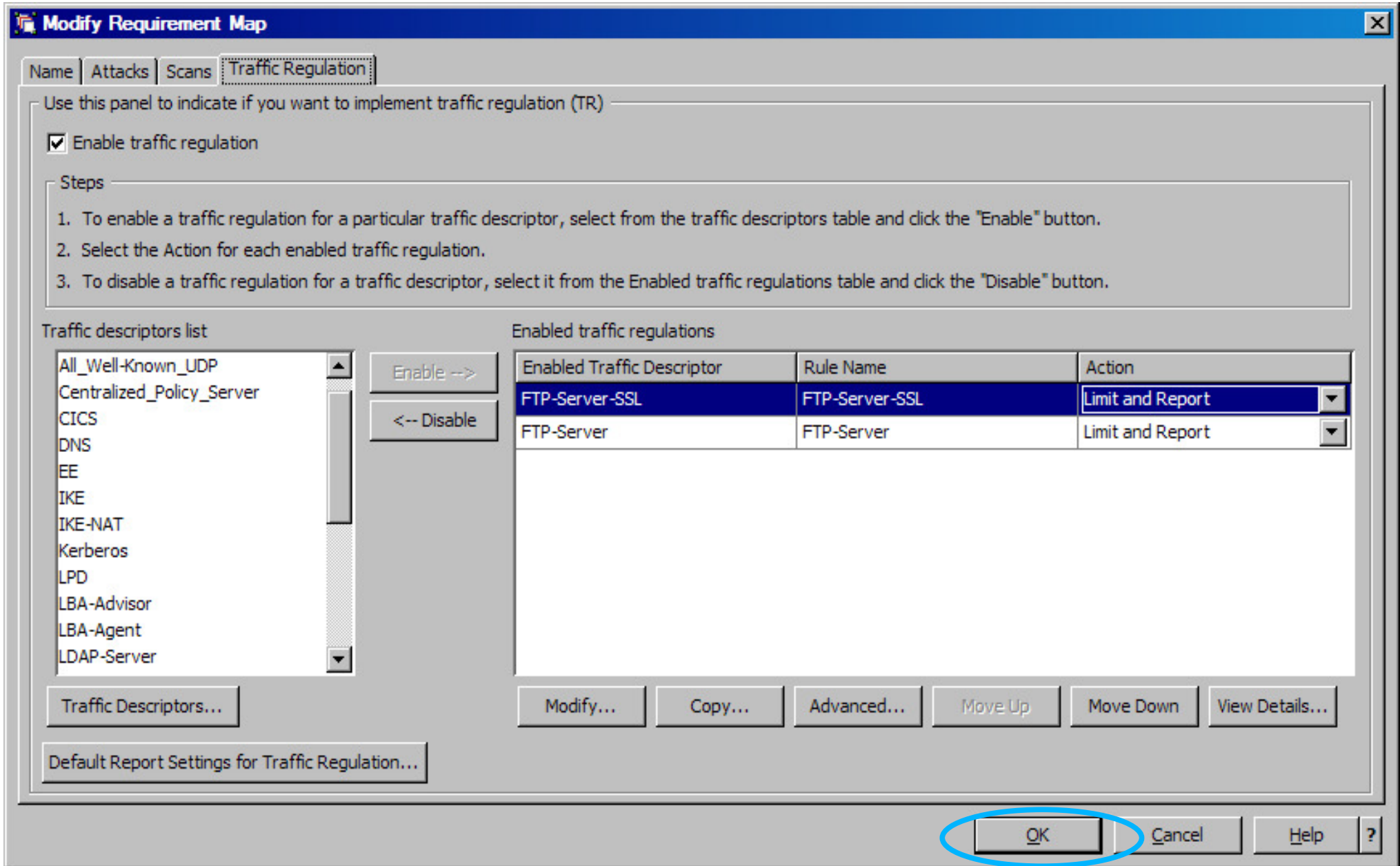
* (percent)

Limit by socket or by all sockets

Limit scope: ▼

OK Cancel Help ?

Traffic regulation enabled



IDS_Policy_Demo

requirements map now created


File Edit Perspective Help

IDS Perspective

Navigation tree

- IDS
 - Reusable Objects
 - Traffic Descriptors
 - Requirement Maps
 - z/OS Images
 - Image - DEMOMVS

List of all defined requirement map objects



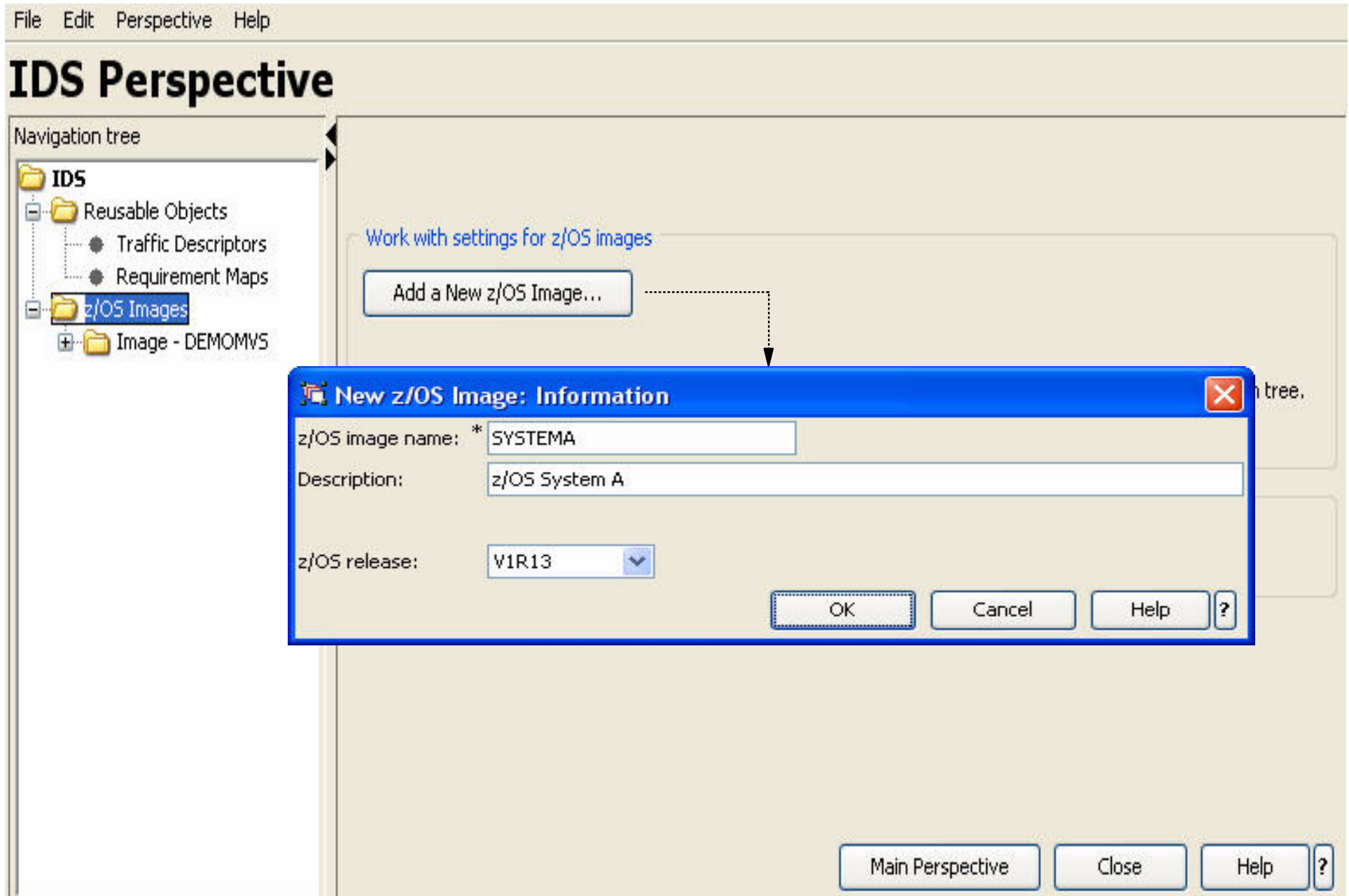
Name ▲	Description
IDS_Default	IBM Supplied: Intrusion Detection Services Starter Set
IDS_policy_demo	Show how to configure IDS policy

< [Progress Bar] >

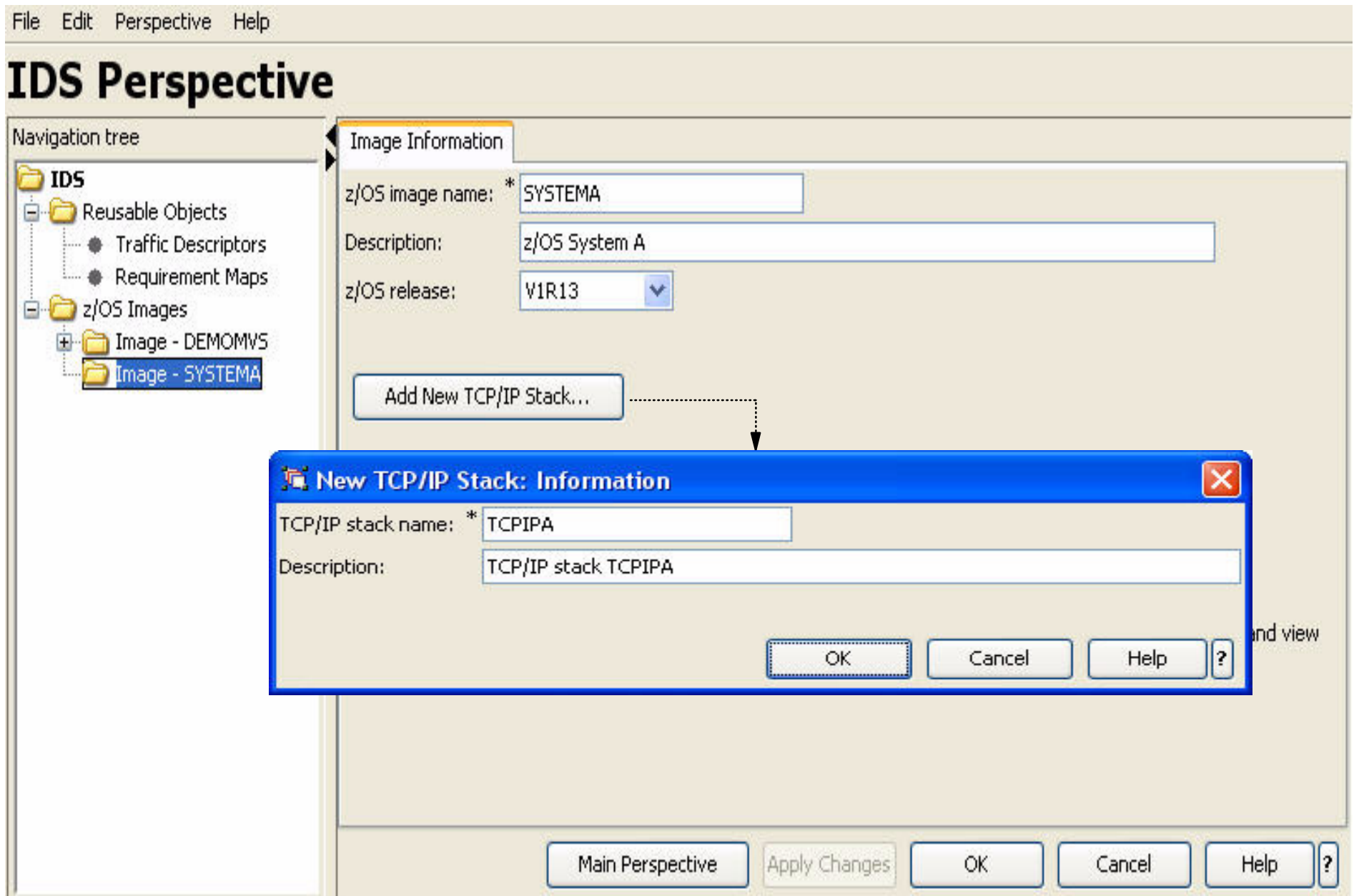
Add... Copy... Modify... Delete View Details... Show Where Used...

Main Perspective Close Help ?

Create System Image



Create TCP/IP stack



Associate TCP/IP Stack with Requirements Map

File Edit Perspective Help

IDS Perspective

Navigation tree

- IDS
 - Reusable Objects
 - Traffic Descriptors
 - Requirement Maps
 - z/OS Images
 - Image - DEMOMVS
 - Image - SYSTEMA
 - Stack - TCPIPA

TCP/IP stack name: * TCPIPA

Description: TCP/IP stack TCPIPA

z/OS release: V1R13

Select a requirement map to govern IDS protection for this stack.

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

Buttons: Add... Copy... Modify... View Details... Show Where Used... Set Addresses... Health Check... Main Perspective Apply Changes OK Cancel Help ?

next page

Perform application setup tasks

The screenshot shows the 'IDS Perspective' application window. On the left is a 'Navigation tree' with a folder structure: 'IDS' containing 'Reusable Objects' (with sub-items 'Traffic Descriptors' and 'Requirement Maps') and 'z/OS Images' (with sub-items 'Image - DEMOMVS', 'Image - SYSTEMA', and 'Stack - TCPIPA'). The main area is titled 'Image Information' and contains fields for 'z/OS image name: * SYSTEMA', 'Description: z/OS System A', and 'z/OS release: V1R13'. Below these are three buttons: 'Add New TCP/IP Stack...', 'Application Setup Tasks...' (highlighted with a dashed box and an arrow pointing to the dialog), and 'Install Configuration Files...'. The 'Application Setup Tasks...' dialog box is open, titled 'Application Setup Tasks for Image SYSTEMA'. It contains instructions: 'This panel contains tasks to enable Intrusion Detection Services for z/OS image SYSTEMA.', '- Select the task and click **Task Details**.', and 'Steps: - Follow the instructions on the panel. - As you finish each task, change its status to **Complete**.'. Below the instructions is a table titled 'List of setup tasks' with columns 'Task name', 'Last completion date', 'Status', and 'Cor'. The table lists ten tasks, all with a status of 'Incomplete'. At the bottom of the dialog are buttons for 'Task Details...' and 'Display All Instructions', and a checked checkbox for 'Permanently save backing store after performing these tasks'.

File Edit Perspective Help

IDS Perspective

Navigation tree

- IDS
 - Reusable Objects
 - Traffic Descriptors
 - Requirement Maps
 - z/OS Images
 - Image - DEMOMVS
 - Image - SYSTEMA
 - Stack - TCPIPA

Image Information

z/OS image name: * SYSTEMA

Description: z/OS System A

z/OS release: V1R13

Add New TCP/IP Stack...

Application Setup Tasks... Perform initial configuration

Install Configuration Files... View the product documentation

Application Setup Tasks for Image SYSTEMA

This panel contains tasks to enable Intrusion Detection Services for z/OS image SYSTEMA.

- Select the task and click **Task Details**.

Steps:

- Follow the instructions on the panel.
- As you finish each task, change its status to **Complete**.

List of setup tasks

Task name	Last completion date	Status	Cor
Installation Location Setup		Incomplete	
Policy Agent - RACF Directives		Incomplete	
Policy Agent - RACF Directives for data...		Incomplete	
Syslogd - RACF Directives		Incomplete	
TRMD - RACF Directives		Incomplete	
Policy Agent Configuration - Image SYS...		Incomplete	
Syslogd - Configuration		Incomplete	
Syslogd - Start Procedure		Incomplete	
Policy Agent - TCPIP Sample Profile		Incomplete	

Task Details... Display All Instructions

Permanently save backing store after performing these tasks

Install configuration files

File Edit Perspective Help

IDS Perspective

Navigation tree

- IDS
 - Reusable Objects
 - Traffic Descriptors
 - Requirement Maps
 - z/OS Images
 - Image - DEMOMVS
 - Image - SYSTEMA
 - Stack - TCPIPA

Image Information

z/OS image name: * SYSTEMA

Description: z/OS System A

z/OS release: V1R13

Add New TCP/IP Stack...

Application Setup Tasks... Perform initial setup tasks including RACF directives and start procedures.

Install Configuration Files... View the produced configuration files, install the files to the z/OS system, and view a configuration summary.

Main Perspective Apply Changes OK Cancel Help ?

next page

Show the configuration file to be installed

List of Configuration Files for Image SYSTEMA

Tip: Not all application setup tasks are marked complete. These tasks are not complete. Click Help for more information.

List of Configuration Files for Image SYSTEMA

Stack	Configuration	File Name (may be modified)
TCPIPA	IDS Policy	/etc/cfgasst/v1r13/SYSTEMA

Buttons: Show Configuration File, Install, Configuration Summary

Permanently save backing store after install

IDS: Policy Agent Stack Configuration

Contents of the flat file:

```
##
## IDS Policy Agent Configuration file for:
##   Image: SYSTEMA
##   Stack: TCPIPA
##
## Created by the IBM Configuration Assistant for z/OS Communications Server
## Version 1 Release 13
## Backing Store = C:\Program Files\IBM\zCSConfigAssist\V1R13\saveData
## FTP 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
)
```

Buttons: Save As..., Print..., Close

Set up to transfer policy file to z/OS

The image shows two overlapping windows from the IBM System Manager interface. The background window is titled "List of Configuration Files for Image SYSTEMA" and contains a table with the following data:

Stack	Configuration	File Name (may be modified)
TCPIPA	IDS Policy	/etc/cfgasst/v1r13/SYSTEMA/TCPIPA/idsPol

Below the table are buttons for "Show Configuration File", "Install", and "Configuration Summary". A checkbox labeled "Permanently save backing store after install" is checked. A dotted arrow points from the "Install" button to the "Install Files to Remote Host" dialog box in the foreground.

The foreground dialog box is titled "Install Files to Remote Host" and contains the following fields and options:

- Install file:**
- FTP login information:**
 - Host name:
 - Port number:
 - User ID:
 - Password: Save password
 - Use SSL
- Data transfer mode:**
 - Default Passive Active
- Comment for the configuration file prologue (optional):**
Comment:

At the bottom of the dialog box are buttons for "Go", "Close", "View FTP Log", "Help", and a question mark icon.

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/atmastr.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