



Software Group | Enterprise Networking Solutions

# Integrated Intrusion Detection Services for z/OS Communications Server

## SHARE Session 8329

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®
- ▶ DB2 Connect
- ▶ DB2®
- ▶ DRDA®
- ▶ e-business on demand®
- ▶ e-business (logo)
- ▶ e business (logo)®
- ▶ ESCON®
- ▶ FICON®
- ▶ GDDM®
- ▶ HiperSockets
- ▶ HPR Channel Connectivity
- ▶ HyperSwap
- ▶ i5/OS (logo)
- ▶ i5/OS®
- ▶ IBM (logo)®
- ▶ IBM®
- ▶ IMS
- ▶ 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®
- ▶ PR/SM
- ▶ pSeries®
- ▶ RACF®
- ▶ Rational Suite®
- ▶ Rational®
- ▶ Redbooks
- ▶ Redbooks (logo)
- ▶ Sysplex Timer®
- ▶ System i5
- ▶ System p5
- ▶ System x
- ▶ System z
- ▶ System z9
- ▶ Tivoli (logo)®
- ▶ Tivoli®
- ▶ VTAM®
- ▶ WebSphere®
- ▶ xSeries®
- ▶ z9
- ▶ zSeries®
- ▶ z/Architecture
- ▶ z/OS®
- ▶ z/VM®
- ▶ z/VSE

- 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.
- Intel, Intel Inside (logos), MMX and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- Linux is a trademark of Linus Torvalds in the United States, other countries, or both.
- Red Hat is a trademark of Red Hat, Inc.
- SUSE® LINUX Professional 9.2 from Novell®
- Other company, product, or service names may be trademarks or service marks of others.
- This information is for planning purposes only. The information herein is subject to change before the products described become generally available.
- All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All performance data contained in this publication was obtained in the specific operating environment and under the conditions described and is presented as an illustration. Performance obtained in other operating environments may vary and customers should conduct their own testing.

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

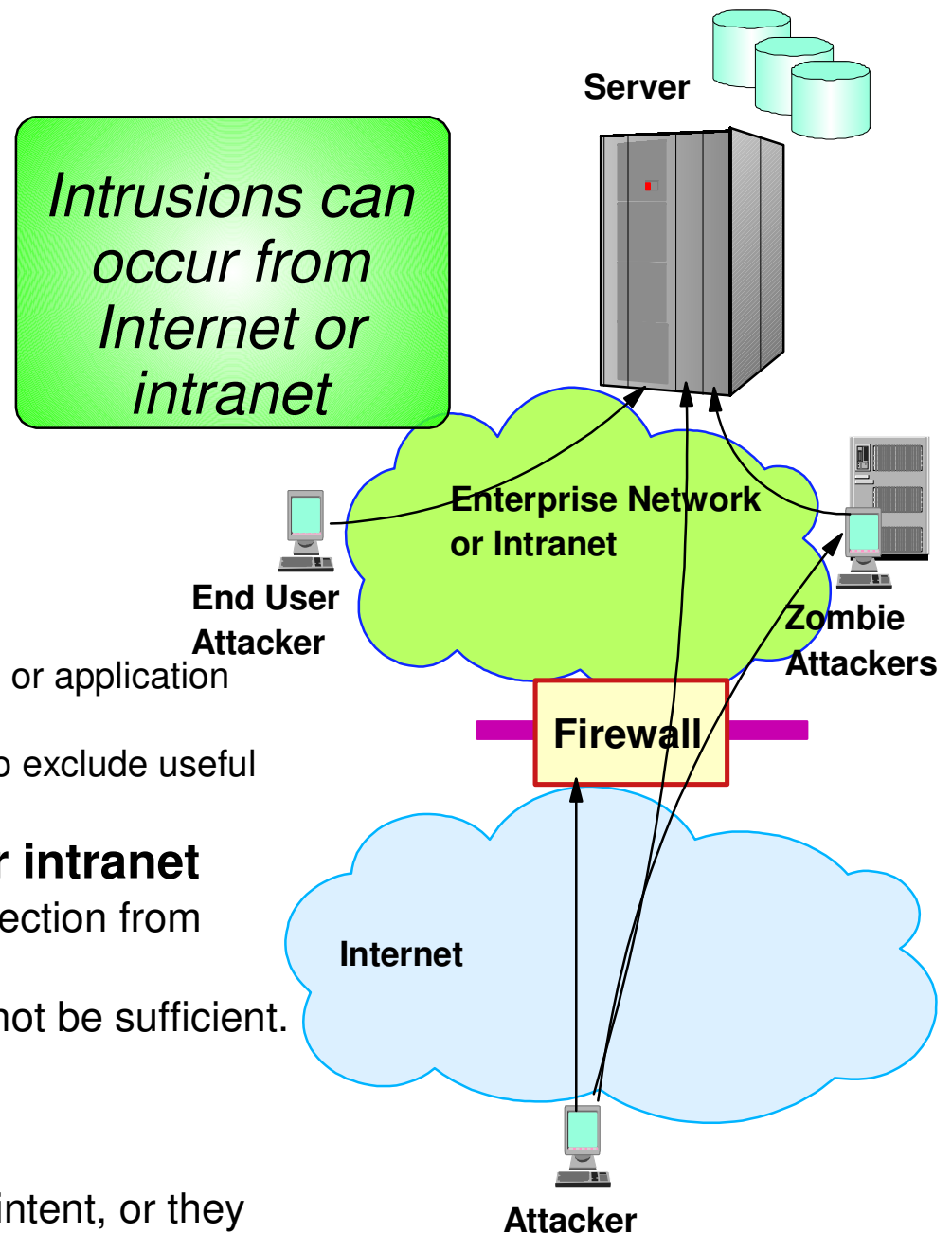
# The Intrusion Threat

## ■ What is an intrusion?

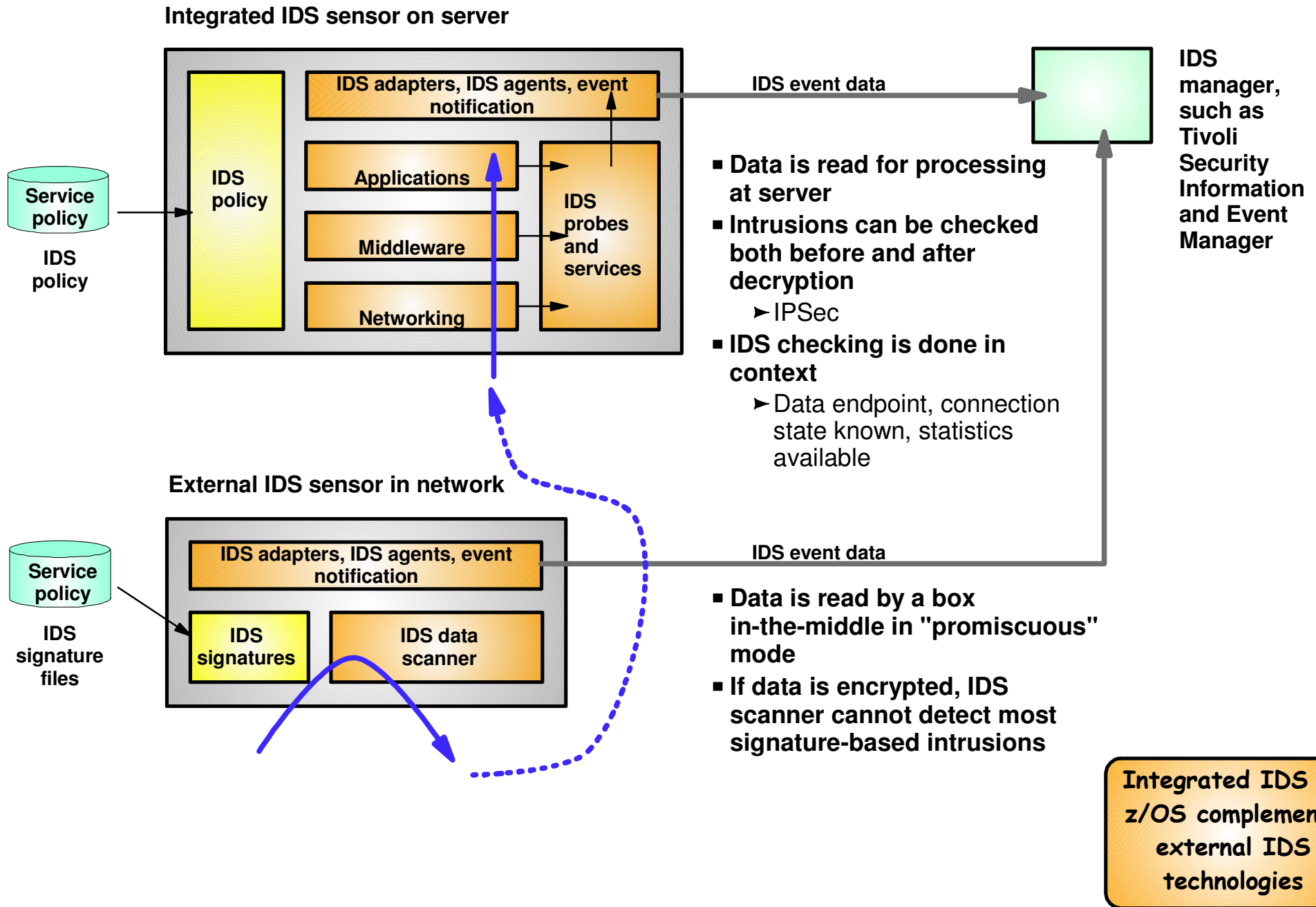
- ▶ Information Gathering
  - Network and system topology
  - Data location and contents
- ▶ Eavesdropping/Impersonation/Theft
  - On the network/on the server
  - Base for further attacks on others
    - ✓ Amplifiers
    - ✓ Robot or zombie
- ▶ Denial of Service
  - Attack on availability
    - ✓ Single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

## ■ Attacks can occur from Internet or intranet

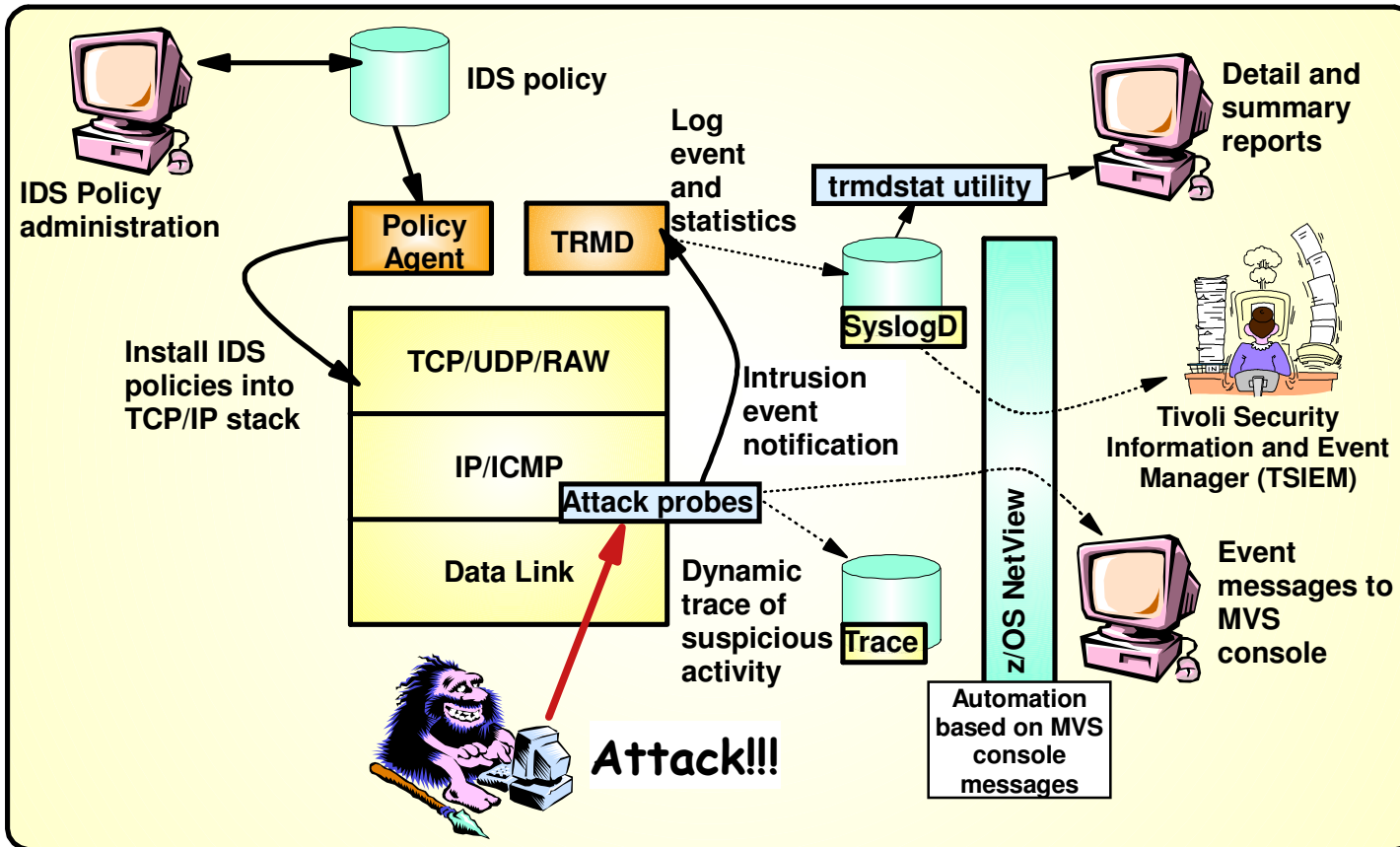
- ▶ Firewalls can provide some level of protection from Internet
- ▶ Perimeter Security Strategy *alone* may not be sufficient.
  - Considerations:
    - ✓ Access permitted from Internet
    - ✓ Trust of intranet
- ▶ Attack can be deliberate with malicious intent, or they can result from various forms of errors on nodes in the network



# Integrated vs. External Intrusion Detection Concepts



# 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 and Tivoli Security Information and Event Manager (TSIEM)

## IDS Policy

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

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

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

- Ability to evaluate inbound encrypted data - IDS applied after 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

# New Support Planned for z/OS V1R13

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

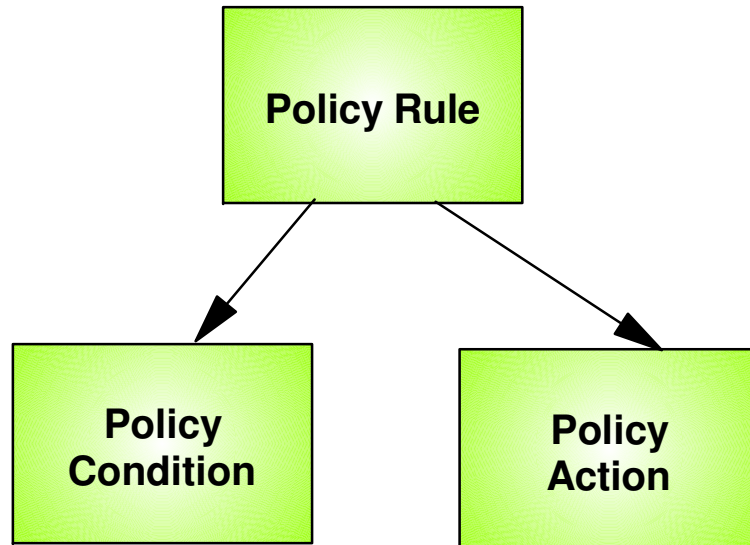
# IDS Configuration

- 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 events types supported
  - ▶ ICMP 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

# Scan Event Counting and Scan Sensitivity

- Each scan event is internally classified as normal, suspicious or very suspicious
  - ▶ Socket state, ICMP type affect this classification
- 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
- Scan instance event classification by event type included in appendix A

# 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 packets with incorrect or partial header information
- Inbound fragment restrictions
  - ▶ Detects fragmentation in first 88 bytes of a datagram
- IP protocol restrictions
  - ▶ Detects use of IP protocols you are not using that could be misused
- IP option restrictions
  - ▶ Detects use of IP options you are not using that could be misused
- UDP perpetual echo
  - ▶ Detects traffic between UDP applications that unconditionally respond to every datagram received
- ICMP redirect restrictions
  - ▶ Detects receipt of ICMP redirect to modify routing tables.
- Outbound RAW socket restrictions
  - ▶ Detects z/OS RAW socket application crafting invalid outbound packets
- Flood Events
  - ▶ Detects flood of SYN packets from "spoofed" sources
  - ▶ Detects high percentage of packet discards on a physical interface



# 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

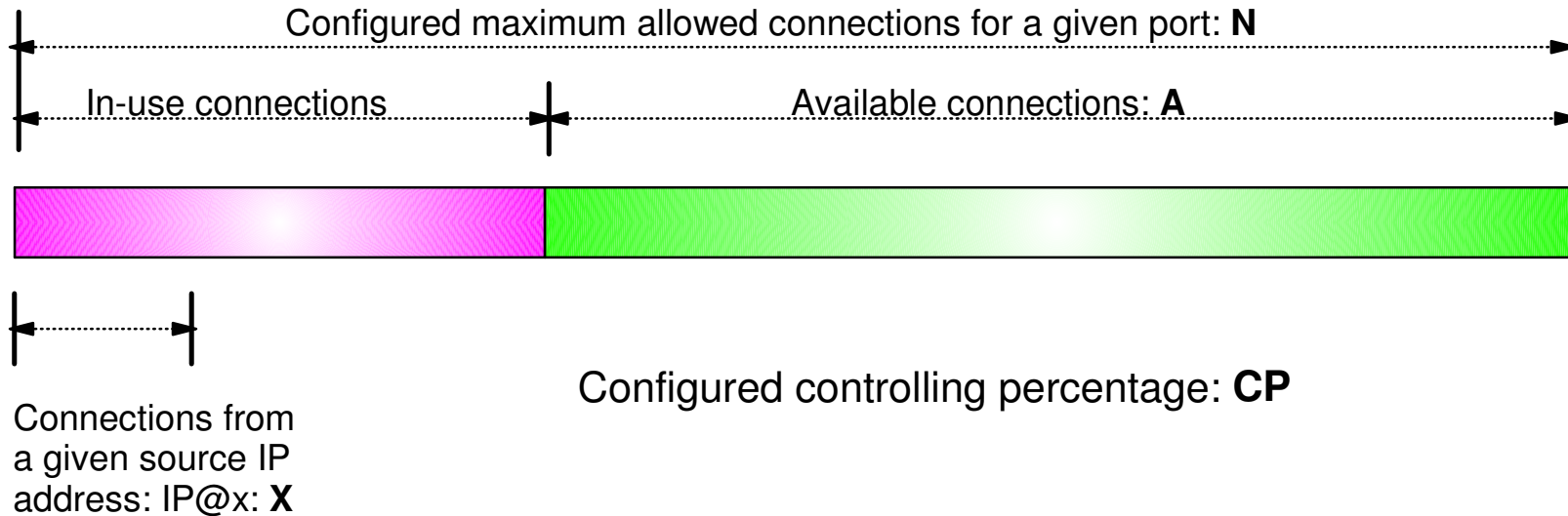


time interval	inbound cnt	discard cnt	discard rate	notes
> 1 min	13,000	2000	N/A	took longer than a minute to see the minimum discard count, so not a flood and discard rate not calculated.
< 1 min	30,000	2000	6.6%	not a flood, rate <10%
< 1 min	20,000	2000	10%	<b>interface flood start detected.</b> Run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

# 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	Allowed Rejected		
			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

- A** If we currently 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

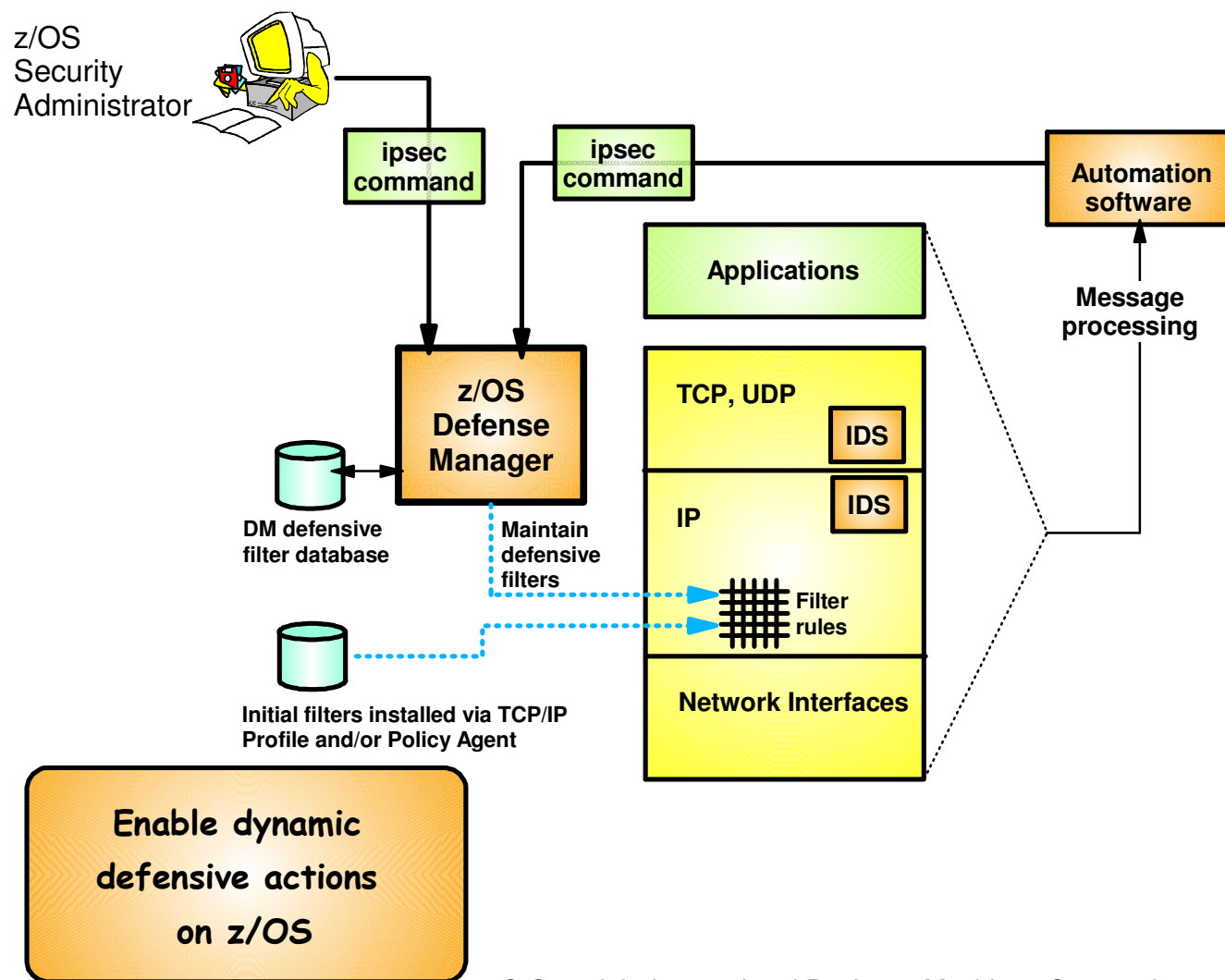
- Recording options controlled by IDS policy action specification
- Options
  - ▶ Event logging
    - Syslogd
      - ✓ Number of events per attack subtype recorded in a five minute interval can be limited
    - Local Console
      - ✓ Recording suppression provided if quantity of IDS console messages 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)
- 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

- Scan Events
  - ▶ No defensive action defined
- 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)
    - Some attack types controlled by IDS policy action
      - ✓ ICMP redirect restrictions
      - ✓ IP option restrictions
      - ✓ IP protocol restrictions
      - ✓ IP fragment
      - ✓ outbound raw restrictions
      - ✓ perpetual echo
  - ▶ No defensive action defined
    - ✓ flood (interface flood detection)
- 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
    - 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
  
- Tivoli Security Information and Event Manager (TSIEM) provides **enterprise-wide management** support for IDS
  - ▶ Automated aggregation and correlation of events, logs, and vulnerabilities
    - Broad device support for multi-vendor environments, including security, network, host, and applications
    - Support includes processing for z/OS Communications Server syslog messages for IDS events
  - ▶ Automates policy and regulatory compliance
    - Policy and Regulatory based policy monitoring and reporting

# 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



- **GUI-based approach to configuring:**
  - ▶ IDS
  - ▶ AT-TLS
  - ▶ IPsec and IP filtering
  - ▶ QoS
  - ▶ Policy-based Routing (PBR)
  - ▶ Defense Manager Daemon (V1R11)
- **Focus on high level concepts vs. low level file syntax**
- **Runs on Windows and under z/OSMF (V1R11)**
- **Builds and maintains**
  - ▶ Policy files
  - ▶ Related configuration files
  - ▶ JCL procedures and RACF directives ( V1R11)
- **Supports import of existing policy files (V1R10)**

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 12



(c) Licensed Materials - Property of IBM Corp. (c) Copyright by IBM Corp. and other(s) 2006, 2010. 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

V1R12 Configuration Assistant - Backing Store (Read-Write) = C:\Program Files\IBM\zCSCConfigAssist\V1R12\files\sav...

File Edit Perspective Help

## Main Perspective

Navigation tree

- z/OS Images

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
<b>IDS</b>	<b>Intrusion Detection Services</b>
NSS	Network Security Services
QoS	Quality of Service
PPR	Policy Based Routing

Configure

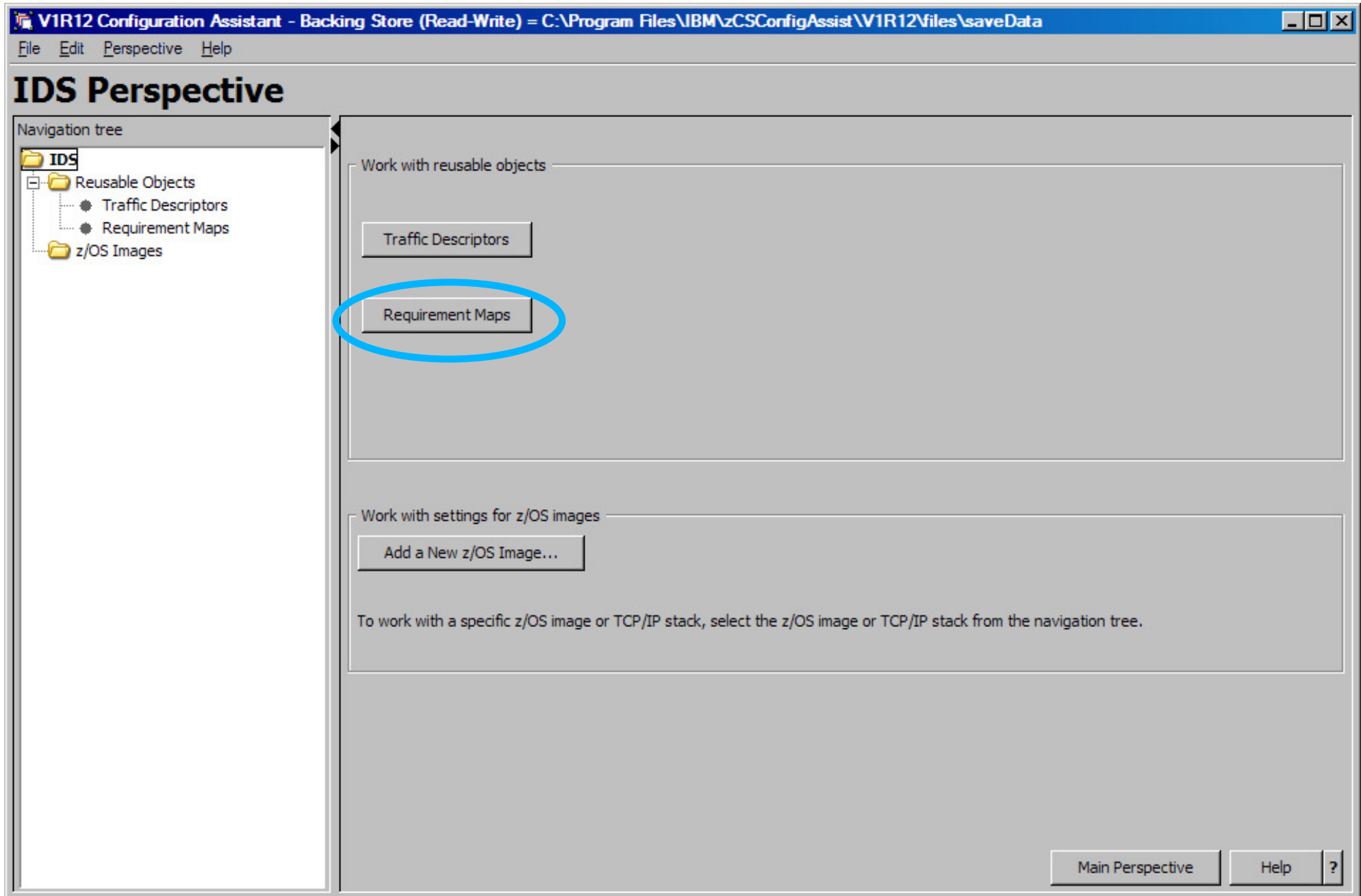
Work with settings for z/OS images

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 n...

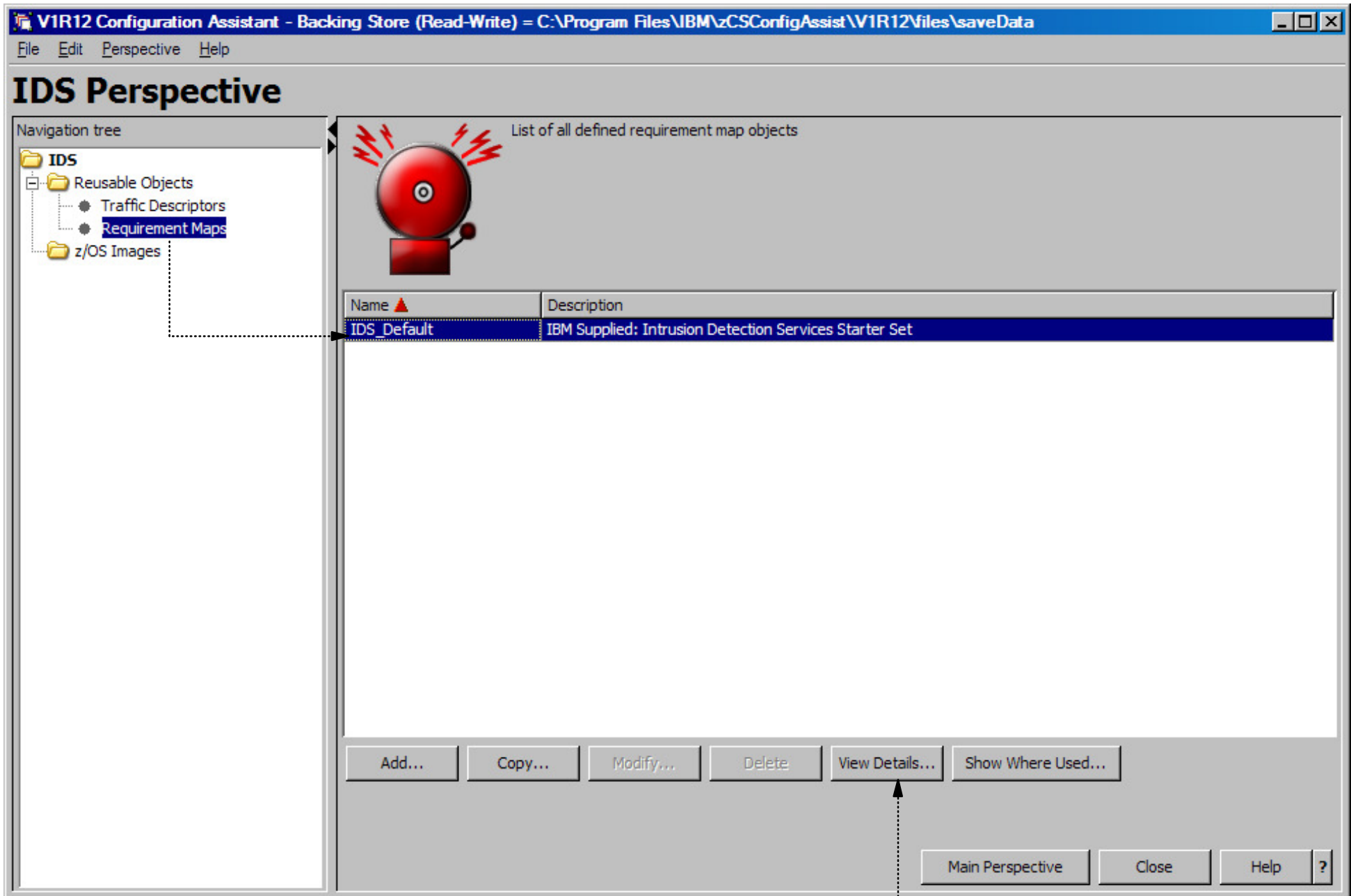
Save Exit Help

# Create IDS policy objects





# Evaluate IDS\_Default requirements map



## IDS\_Default provided as default requirement map

- Display details of the requirement map
- Evaluate whether they meet your requirements

# Details view of IDS\_Default requirements map (1 of 4)

Help

Requirement Map: IDS\_Default - IBM Supplied: Intrusion Detection Services Starter Set

## Attack Protection Summary

Enabled Attack Protection	Rule Name	Actions	Reports	Time Condition	Report Settings
Flood Attack	Flood	Both Discard and Report	Inherited	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 Report Stat if no events: No ----- <b>Trace Parameters:</b> No
Perpetual Echo Attack	Echo	Report Events	Inherited	None	
Unwanted IP Protocols Attack	IPProtocol	Report Events	Inherited	None	
Unwanted IP Options Attack	IPOption	Report Events	Inherited	None	
ICMP Redirect Attack	ICMPRedirect	Report Events	Inherited	None	
Malformed Packet Attack	MalformedPacket	Both Discard and Report	Inherited	None	
Outbound Raw Attack	OutboundRaw	Report Events	Inherited	None	
IP Fragment Attack	IPFragmentation	Report Events	Inherited	None	

# Details view of IDS\_Default requirements map (2 of 4)

Help



## Attack Protection Details

### Enabled Attack Protection: Flood Attack - Flood

Flood Minimum Discard	Flood Percentage	Reports	Time Condition
1000	10	Inherited	None

### Enabled Attack Protection: Perpetual Echo Attack - Echo

Traffic Descriptor	Port Location	Reports	Time Condition
7 - Echo	Both Local and Remote	Inherited	None
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 (3 of 4)

## Enabled Attack Protection: Unwanted IP Protocols Attack - IPProtocol

Starting Protocol	Ending Protocol	Reports	Time Condition
0	0	Inherited	None
3	3		
5	5		
7	16		
18	45		
48	49		
52	88		
90	93		
95	255		

---

## Enabled Attack Protection: Unwanted IP Options Attack - IPOption

Starting Option	Ending Option	Reports	Time Condition
2	6	Inherited	None
8	67		
69	81		
83	255		

# Details view of IDS\_Default requirements map (4 of 4)

## Enabled Attack Protection: Outbound Raw Attack - OutboundRaw

Starting Protocol	Ending Protocol	Reports	Time Condition
0	0	Inherited	None
2	88		
90	255		

## Enabled Attack Protection: IP Fragment Attack - IPFragmentation

Reports	Time Condition
Inherited	None

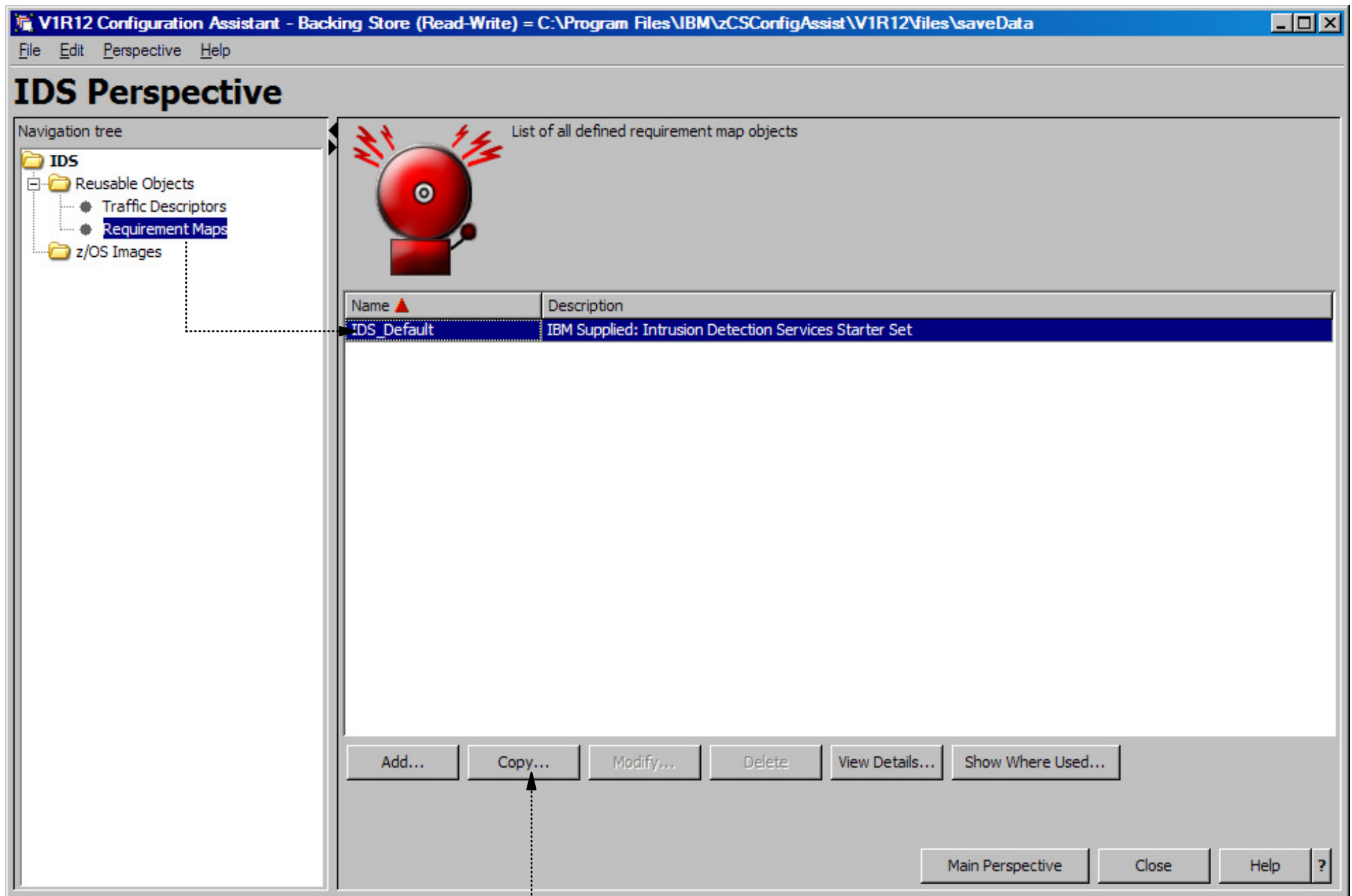
## Scan Protection Summary

No Scan Protection Configured

## Traffic Regulation Summary

No Traffic Regulation Configured

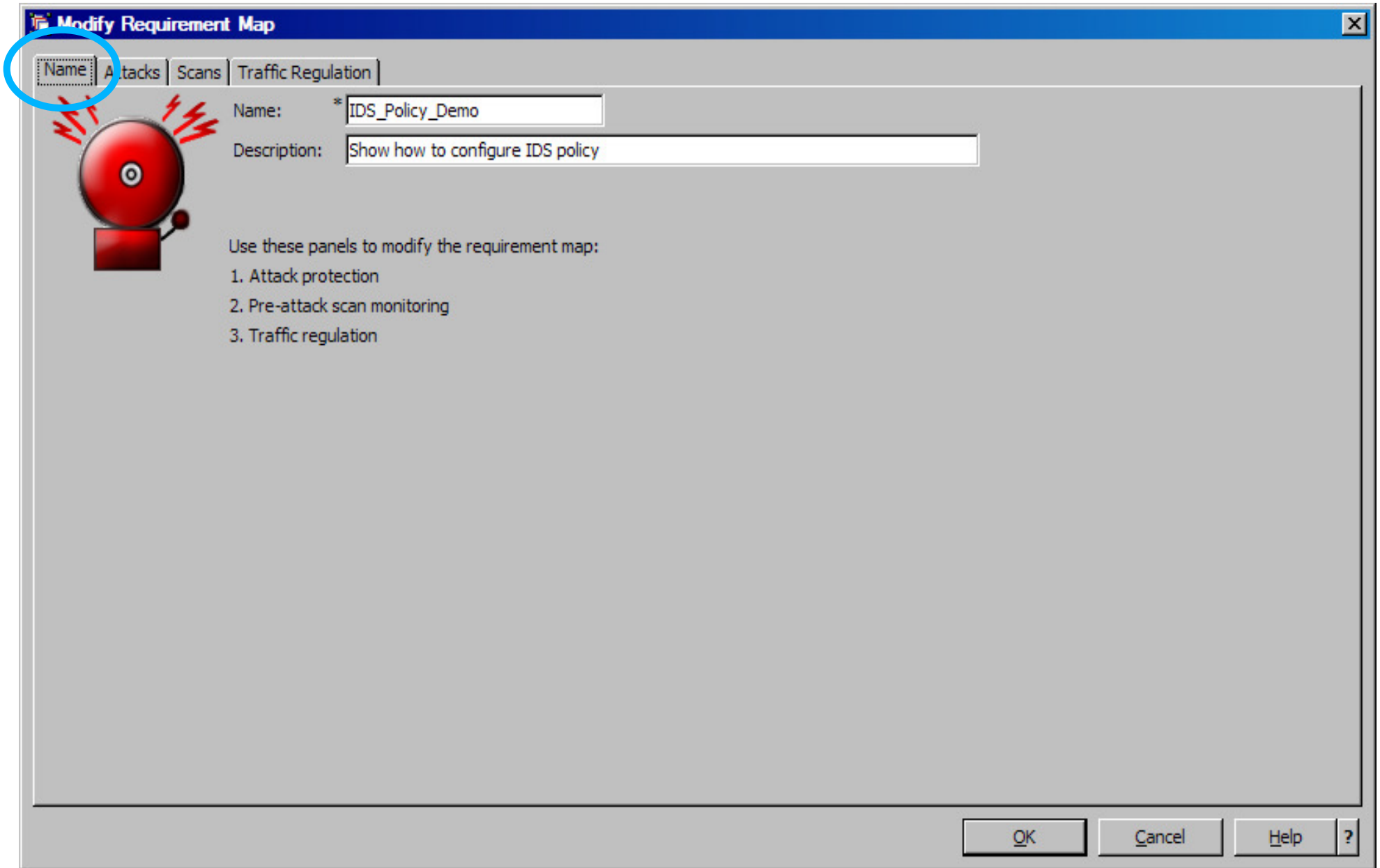
# Use IDS\_Default as a starting point



## Using IDS\_Default as a base

- Copy IDS\_Default
- Create new requirements map using copied IDS\_Default as a base

# Name new requirements map



# Modify copied default requirements map

V1R12 Configuration Assistant - Backing Store (Read-Write) = C:\Program Files\IBM\zCSConfigAssist\V1R12Files\saveData


File Edit Perspective Help

## IDS Perspective

Navigation tree

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

List of all defined requirement map objects



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

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

next page

Main Perspective Close Help ?



# Attack protection enabled by default

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

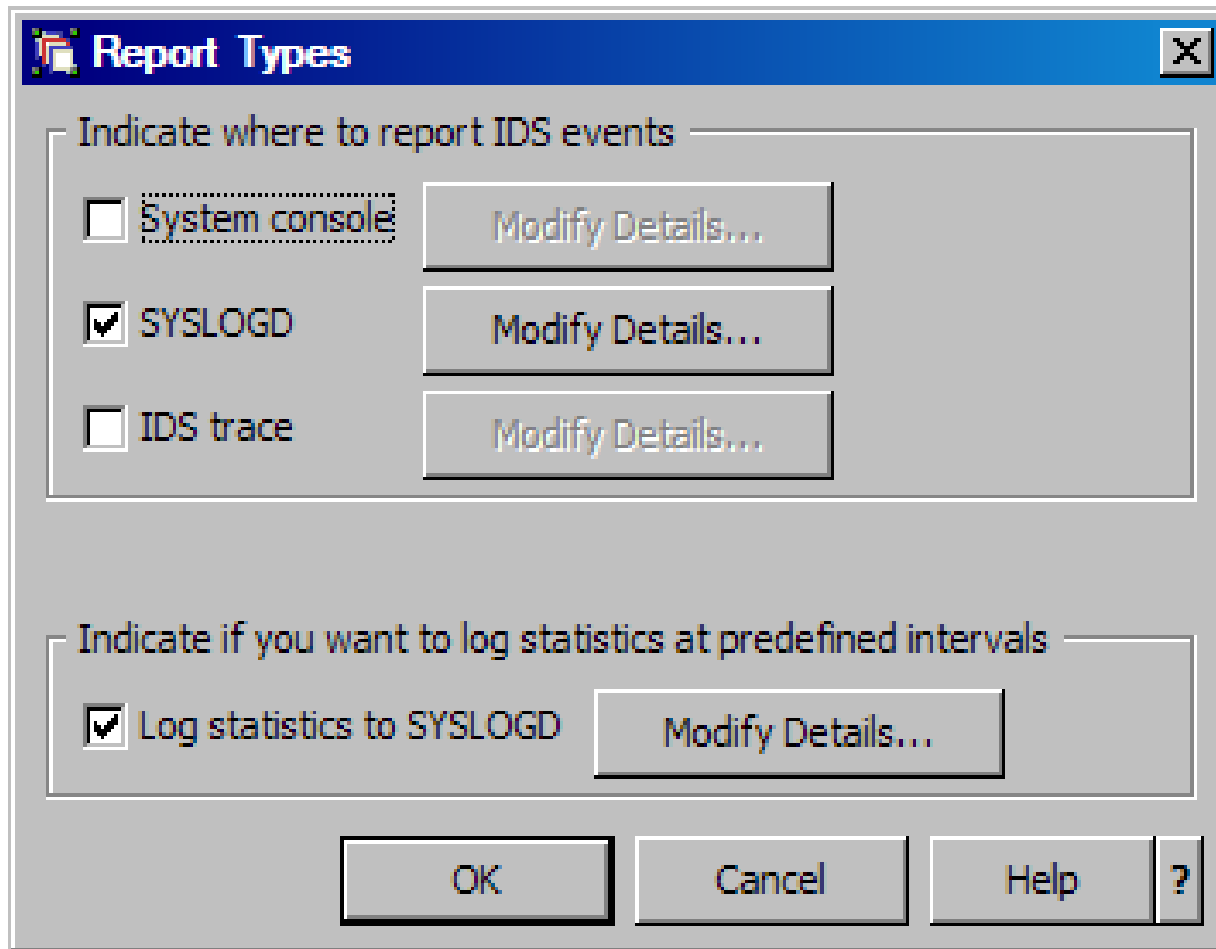
Enabled protection

Attack Type	Rule Name	Action
Flood Attack	Flood	Both Discard ...
Perpetual Echo Attack	Echo	Report Events
Unwanted IP Protocols Attack	IPProtocol	Report Events
Unwanted IP Options Attack	IPOption	Report Events
ICMP Redirect Attack	ICMPRedirect	Report Events
Malformed Packet Attack	MalformedPacket	Both Discard ...
Outbound Raw Attack	OutboundRaw	Report Events
IP Fragment Attack	IPFragmentation	Report Events

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 scan**

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
- IKE
- IKE-NAT
- Kerberos
- LBA-Advisor
- LBA-Agent
- LDAP-Server

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**

**Fast scan settings**

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

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

**Slow scan settings**

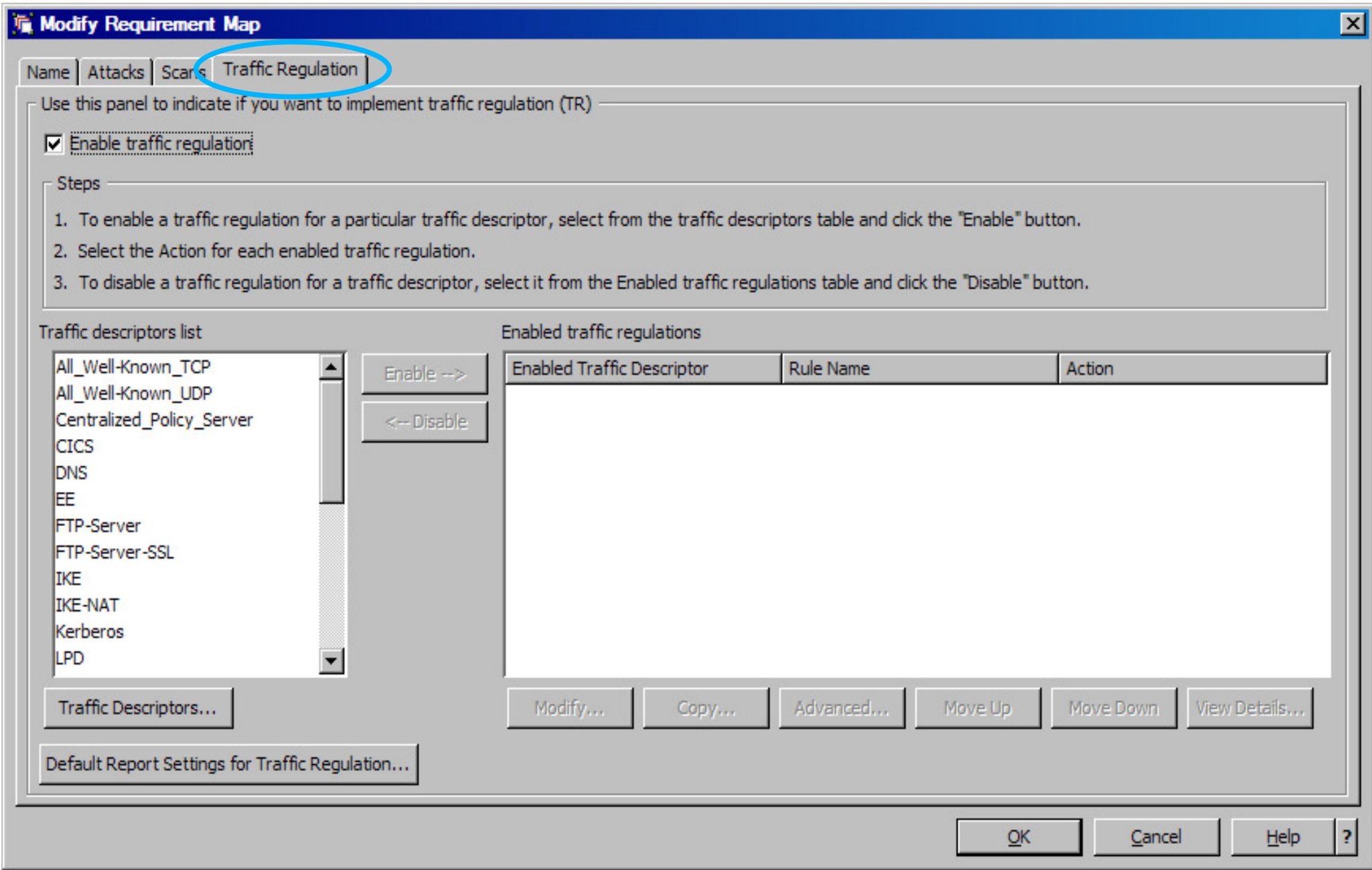
Enable slow scans

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

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

OK Cancel Help ?

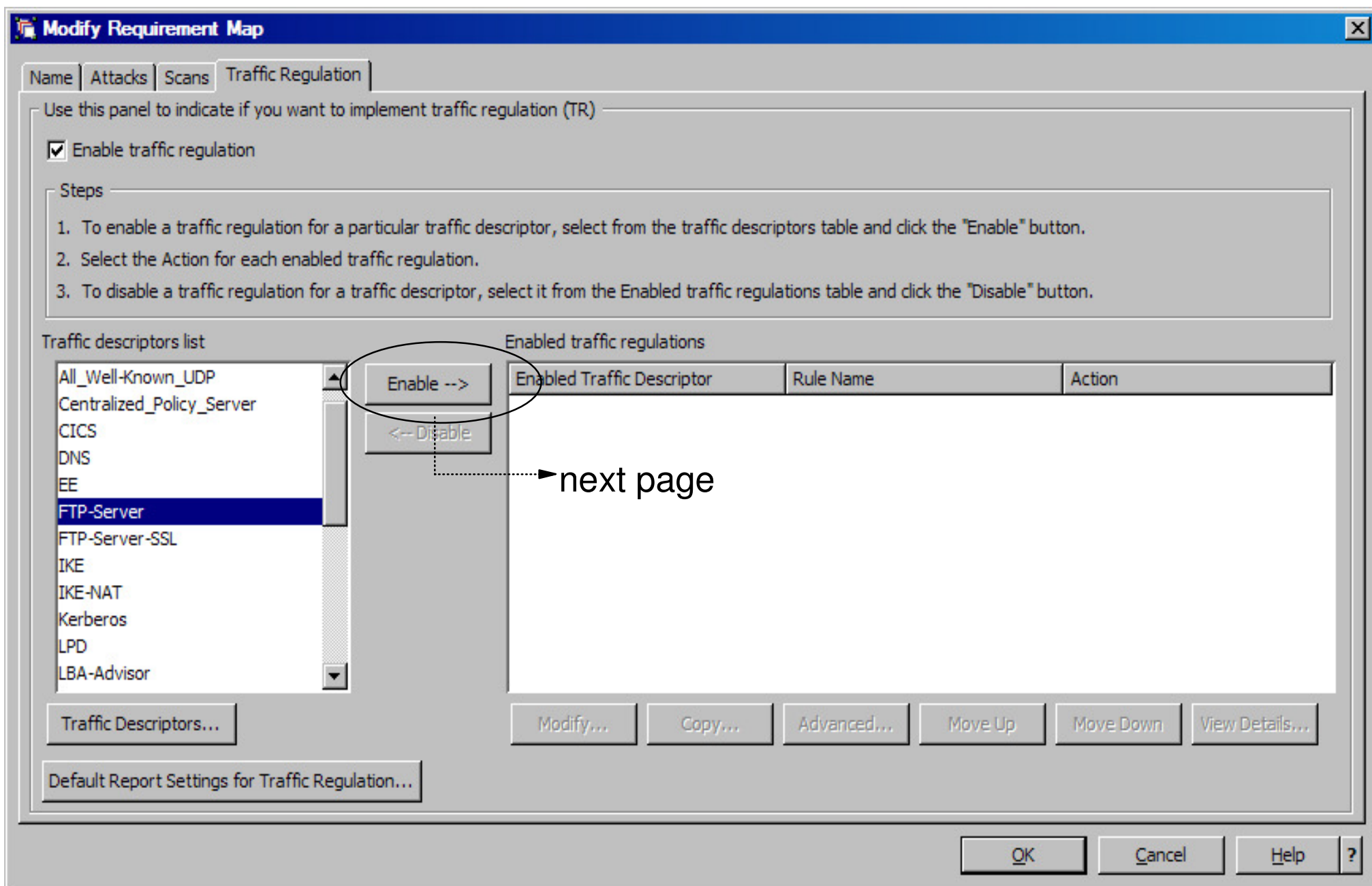
# Enable traffic regulation protection



## 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: \* FTP-Server

Traffic descriptor: FTP-Server

Action: Limit and Report

Enter parameters for TCP traffic

Limit by total connections

Maximum number of connections: \* 100 (0-65535)

Limit by percentage of total connections

No limit per host

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

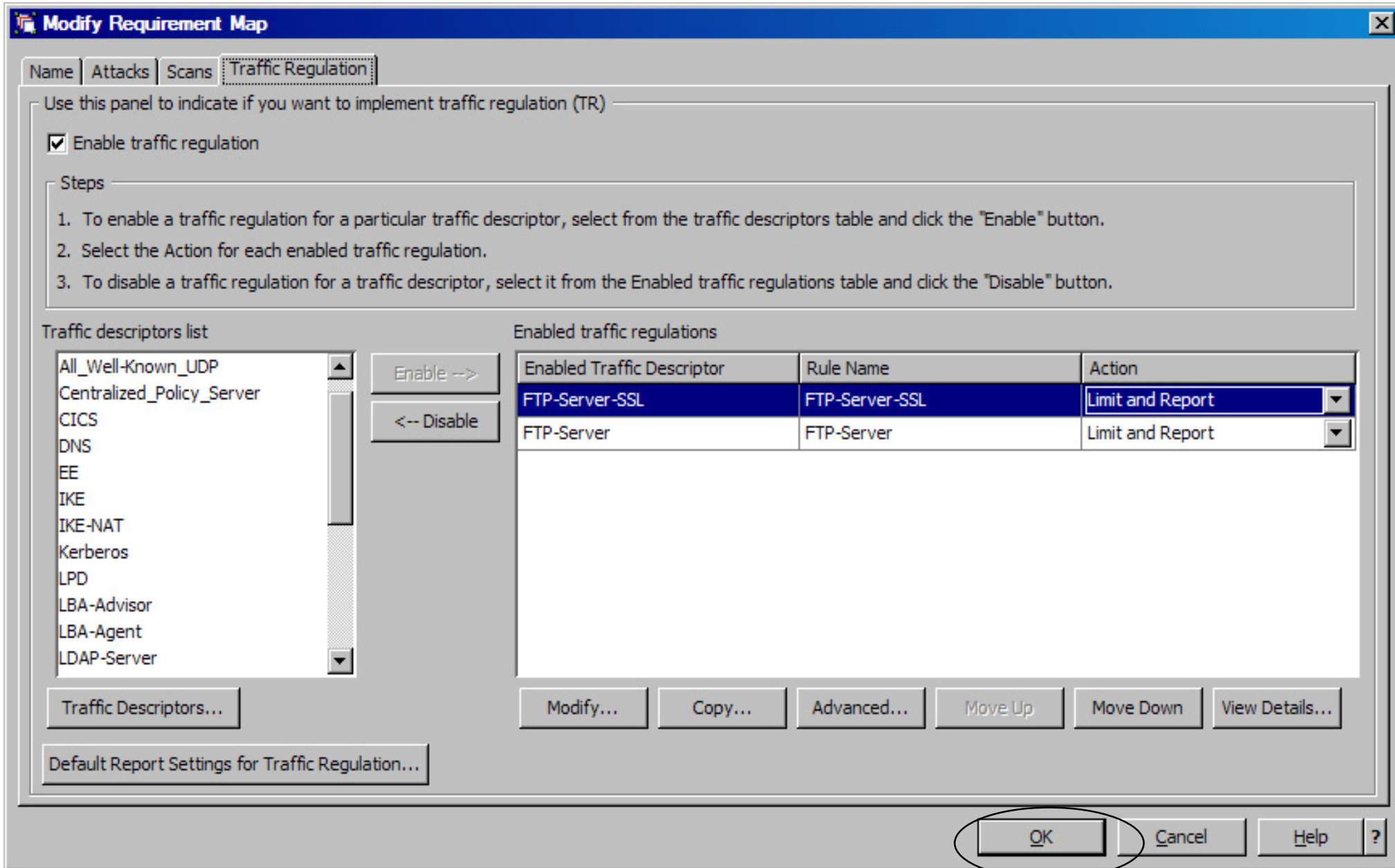
\* 20 (percent)

Limit by socket or by all sockets

Limit scope: All sockets

OK Cancel Help ?

# Traffic regulation enabled





# IDS\_Policy\_Demo

## requirements map now created

V1R12 Configuration Assistant - Backing Store (Read-Write) = C:\Program Files\IBM\zCSConfigAssist\V1R12Files\saveData


File Edit Perspective Help

### IDS Perspective

Navigation tree

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

List of all defined requirement map objects

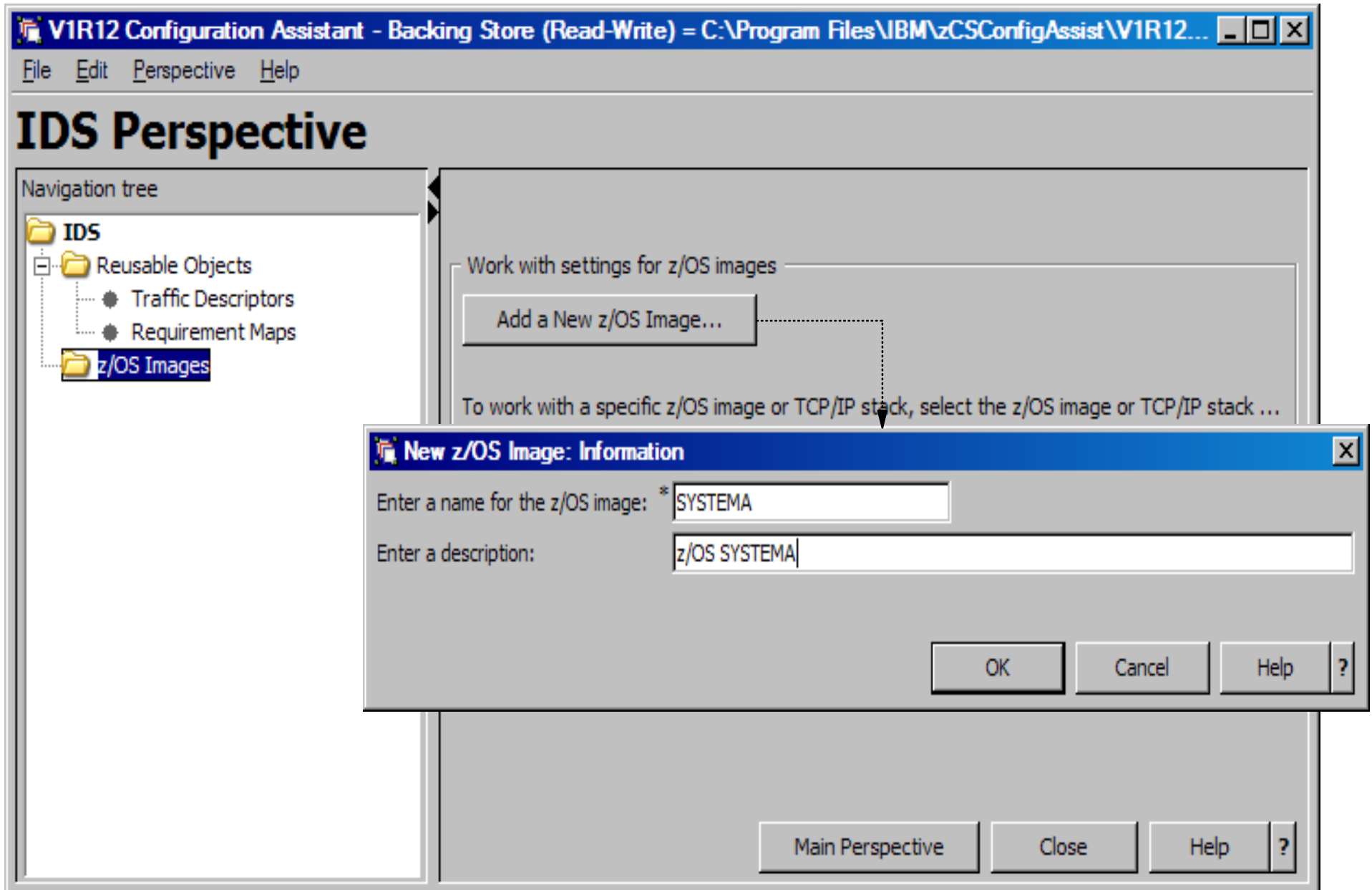


Name ▲	Description
IDS_Default	IBM Supplied: Intrusion Detection Services Starter Set
<b>IDS_Policy_Demo</b>	Show how to configure IDS policy

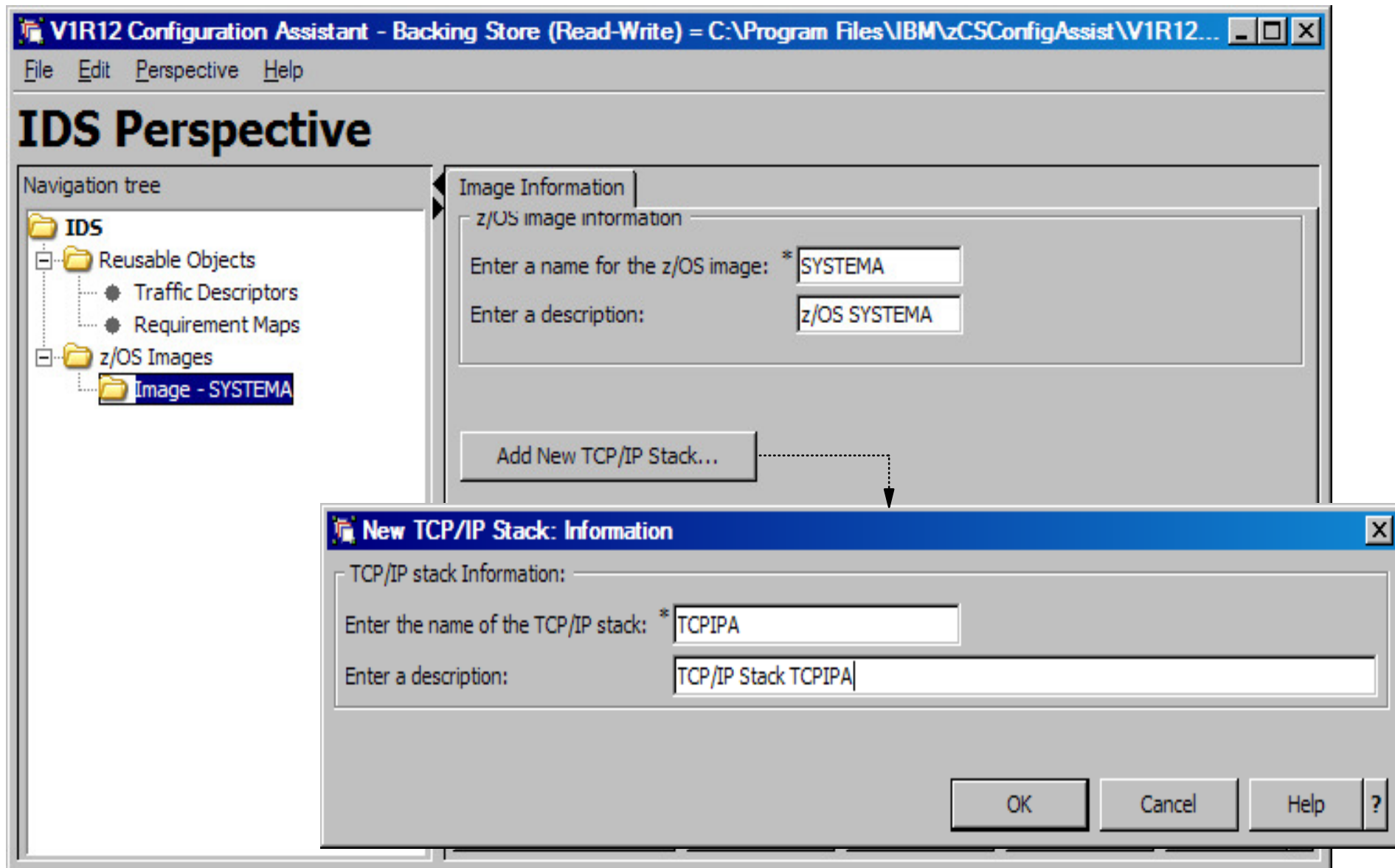
Buttons: Add... Copy... **Modify...** Delete View Details... Show Where Used...

Buttons: Main Perspective Close Help ?

# Create System Image



# Create TCP/IP stack



# Associate TCP/IP Stack with Requirements Map

The screenshot shows the V1R12 Configuration Assistant window. The title bar reads "V1R12 Configuration Assistant - Backing Store (Read-Write) = C:\Program Files\IBM\zCSConfigAssist\V1R12Vfiles\saveData". The menu bar includes "File", "Edit", "Perspective", and "Help". The main window is titled "IDS Perspective".

On the left is a "Navigation tree" with the following structure:

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

The "Stack - TCPIPA" item is selected and highlighted in blue. A dashed line connects it to the "Select a requirement map to govern IDS protection for this stack." section of the main configuration area.

The main configuration area is titled "TCP/IP stack information:" and contains the following fields:

- Enter the name of the TCP/IP stack: \*TCPIPA
- Enter a description: TCP/IP Stack TCPIPA

Below these fields is a section titled "Select a requirement map to govern IDS protection for this stack." which contains a table with two columns: "Name" and "Description".

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

The "IDS\_Policy\_Demo" row is selected and highlighted in blue. A blue oval highlights the text "Select a requirement map to govern IDS protection for this stack." and the table above it.

At the bottom of the main configuration area are several buttons: "Add...", "Copy...", "Modify...", "View Details...", "Show Where Used...", "Set Addresses...", and "Health Check...".

At the bottom of the window are five buttons: "Main Perspective", "Apply Changes", "OK", "Cancel", and "Help".

next page

# Perform application setup tasks

**VIR12 Configuration Assistant - Backing Store (Read-Write) = C:\Program Files\IBM\zCSConfigAssist\V1R12\files\saveData**

File Edit Perspective Help

## IDS Perspective

Navigation tree

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

**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**.

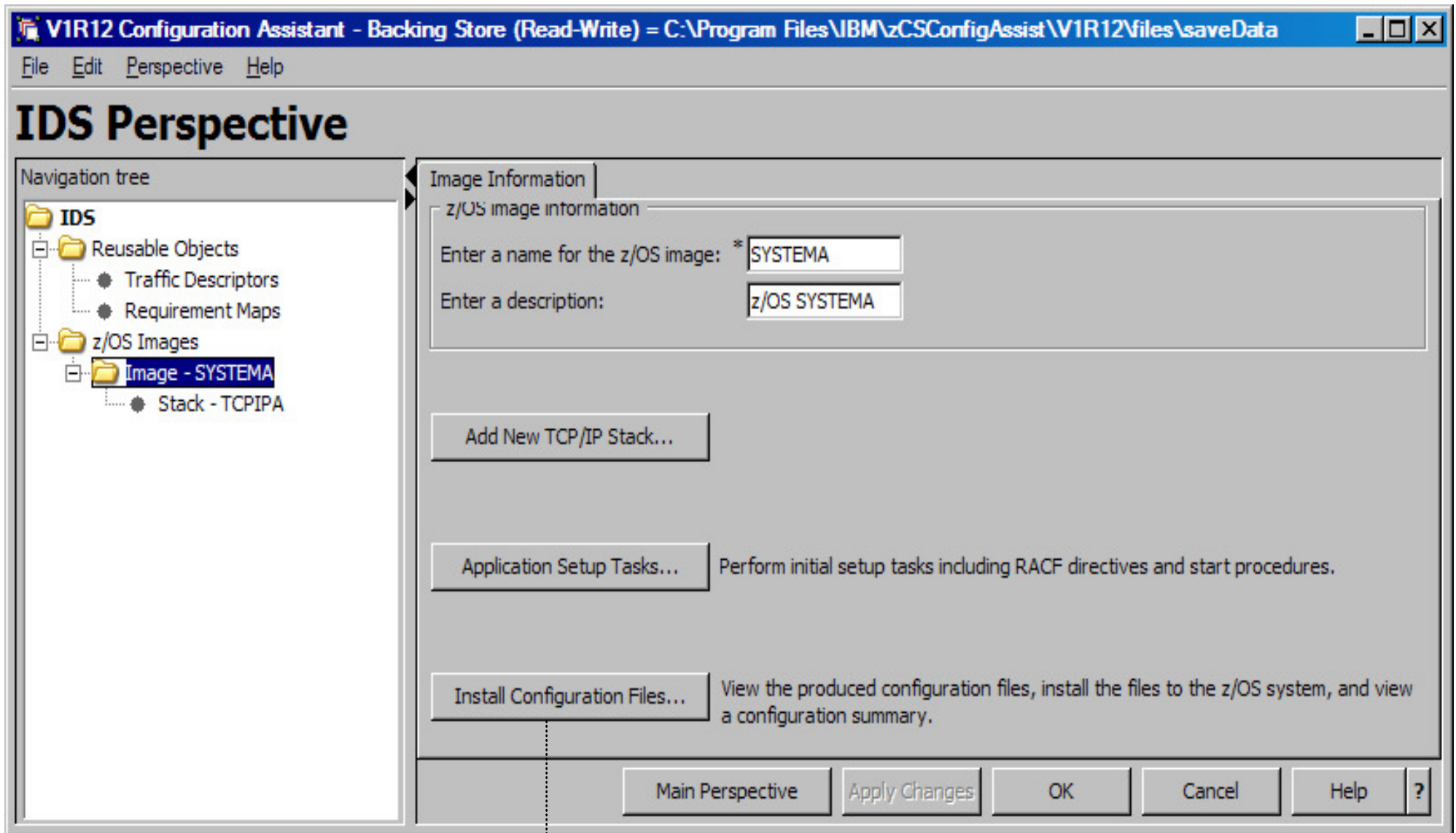
List of setup tasks

Task name	Last completion date	Status
Installation Location Setup		Incomplete
Policy Agent - RACF Directives		Incomplete
Policy Agent - RACF Directives for Polic...		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



▶ next page

# Show the configuration file to be installed

The image shows two windows from the IBM Configuration Assistant. The left window, titled "List of Configuration Files for Image SYSTEMA", contains a table with the following data:

Stack	Configuration	File Name (m
TCPIPA	IDS Policy	/etc/cfgasst/

Below the table are buttons for "Show Configuration File", "Install", and "Configurati". A checkbox labeled "Permanently save backing store after install" is checked. A dashed arrow points from the "Show Configuration File" button to the right window.

The right window, titled "IDS: Policy Agent Stack Configuration", displays the "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 12
## Backing Store = .\files\saveData
## FTP History:
##
## End of Configuration Assistant information

IDSRule                Flood
{
  ConditionType          Attack
  IDSAttackCondition
  {
    AttackType            FLOOD
    IfcFloodMinDiscard    1000
    IfcFloodPercentage     10
  }
  IDSActionRef           Flood
}

IDSRule                Echo
{
  ConditionType          Attack
  IDSAttackCondition
  {
    AttackType            PERPETUAL_ECHO
    LocalPortGroupRef     LocalEchoPortGroup~1
    RemotePortGroupRef    RemoteEchoPortGroup~1
  }
  IDSActionRef           Echo
}

IDSRule                IPProtocol
{
```

# Set up to transfer policy file to z/OS

The screenshot displays two windows from the IBM Configuration Assistant. The background window, titled "List of Configuration Files for Image SYSTEMA", contains a table with the following data:

Stack	Configuration	File Name (may be modified)	Host Name (may be modified)	Last Install	Status
TCPIPA	IDS Policy	/etc/cfgasst/v1r12/SYSTEMA...		Never	Needs install

Below the table are buttons for "Show Configuration File", "Install", and "Configuration S...", along with a checked checkbox for "Permanently save backing store after install".

The foreground window, titled "Install Files to Remote Host", is open over the "Install" button. It contains the following fields and options:

- Install file: \*/etc/cfgasst/v1r12/SYSTEMA/TCPIPA/idsPol
- FTP login information:
  - Host name: \* hostname.com
  - Port number: \* 21
  - User ID: \* IDSKING
  - Password: \* \*\*\*\*\*
  - Save password
  - Use SSL
- Data transfer mode:
  - Default
  - Passive
  - Active
- Comment for the configuration file prologue (optional):  
Comment: [Empty text box]

At the bottom of the "Install Files to Remote Host" window 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**
    - TCP port scans
    - UDP port scans
    - ICMP scans
      - ✓ Sensitivity levels for all scans can be adjusted to control number of false positives recorded.
  - **Attack detection**
    - Malformed packet events
    - Outbound raw restrictions
    - Inbound fragment restrictions
    - IP option restrictions
    - IP protocol restrictions
    - ICMP redirect restrictions
    - Flood events (Synflood, Interface flood)
    - UDP perpetual echo
  - **Traffic Regulation**
    - UDP backlog management by port
      - ✓ Packets discard
    - TCP total connection and source percentage management by port
      - ✓ Connection limiting
- **IDS recording options**
  - **Event logging**
    - syslogd, local console
  - **Statistics**
    - syslogd
      - ✓ normal, exception
  - **IDS packet trace after attack detected for offline analysis**
    - Number of packets traced for multi-packet events are limited
- **Reports and event handling**
  - **trmdstat produces reports from IDS syslogd records**
    - Summary and detailed
  - **IDS event handling by**
    - Tivoli NetView
    - Tivoli Security Information and Event Manager
- **Defensive filtering (z/OS V1R10)**
  - **Installed through ipsec command**
  - **Manually (by human being) or through automation (via external security event manager)**

# z/OS Communications Server Security

## Appendix A

- **Scan Probe Instance Event Classifications**

# ICMP Scan Probe Instance Classification

<b><i>Request Type</i></b>	<b><i>Destination Address</i></b>	<b><i>Event Classification</i></b>
any	subnet base or broadcast	very suspicious
Information req	single host	possibly suspicious
Subnet Mask req	single host	possibly suspicious
Echo with IP Option Record Route	single host	possibly suspicious
Echo with Record Timestamp	single host	possibly suspicious
Echo or Timestamp, denied by QOS policy	single host	normal
Echo or Timestamp	single host	normal



# UDP Scan Probe Instance Classification

<b><i>Socket State</i></b>	<b><i>Event</i></b>	<b><i>Event Classification</i></b>
RESERVED to no one	recv any packet	very suspicious
Unbound, not RESERVED	recv any packet	possibly suspicious - app may be temporarily down
Bound	packet rejected by QOS policy	normal
Bound	packet rejected by FW filtering	possibly suspicious
Bound	recv any packet	normal

# TCP Scan Probe Instance Classification

<b>Socket State</b>	<b>Event</b>	<b>Event Classification</b>
Any state	recv unexpected flags (SYN+FIN...)	very suspicious
RESERVED	recv any packet	very suspicious
Unbound, not RESERVED	recv any packet	possibly suspicious - app may be temporarily down
Listen	recv SYN	classification deferred if syn queued.
Half open connection	recv ACK	normal - connection handshake completed
Half open connection	recv RST	possibly suspicious - scanner covering tracks?
Half open connection	final time out (and not syn flood)	very suspicious - scanner abandoning handshake?
Any connected state	seq# out of window	normal - perhaps duplicate packet
Any connected state	recv standalone SYN	normal - perhaps peer reboot
Any connected state	final time-out	possibly suspicious - peer abandoned connection

# 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/servers/eserver/zseries/networking">http://www.ibm.com/servers/eserver/zseries/networking</a>	Networking: IBM zSeries Servers
<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>	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>	Communications Server for Linux on zSeries
<a href="http://www.ibm.com/software/network/ccl">http://www.ibm.com/software/network/ccl</a>	Communication Controller for Linux on zSeries
<a href="http://www.ibm.com/software/network/commserver/library">http://www.ibm.com/software/network/commserver/library</a>	Communications Server products - white papers, product documentation, etc.
<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>	Requests For Comment (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