Integrated Intrusion Detection Services for
z/OS Communications Server

SHARE Session 8329

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®
- 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 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

Intrusions can occur from Internet or intranet
Integrated vs. External Intrusion Detection Concepts

**Integrated IDS sensor on server**
- IDS adapters, IDS agents, event notification
- Applications
- Middleware
- Networking
- IDS probes and services

IDS event data

IDS manager, such as Tivoli Security Information and Event Manager

- Data is read for processing at server
- Intrusions can be checked both before and after decryption
  - IPSec
- IDS checking is done in context
  - Data endpoint, connection state known, statistics available

**External IDS sensor in network**
- IDS adapters, IDS agents, event notification
- IDS signatures
- IDS data scanner

IDS event data

- Data is read by a box in-the-middle in "promiscuous" mode
- If data is encrypted, IDS scanner cannot detect most signature-based intrusions

Integrated IDS on z/OS complements external IDS technologies

© Copyright International Business Machines Corporation 2011. All rights reserved.
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

*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 threshholds 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 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 Rule**
- **Policy Condition**
- **Policy 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

Policy objects relationship:
IF condition THEN action
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"

<table>
<thead>
<tr>
<th>Sensitivity (from policy)</th>
<th>Normal Event</th>
<th>Possibly Suspicious Event</th>
<th>Very Suspicious Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td>Count</td>
</tr>
<tr>
<td>Medium</td>
<td></td>
<td></td>
<td>Count</td>
</tr>
<tr>
<td>High</td>
<td>Count</td>
<td>Count</td>
<td>Count</td>
</tr>
</tbody>
</table>

- 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"
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:
    - \( \frac{\text{# discards during the interval}}{\text{# inbound packets for the interval}} \)
  - 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:

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

<table>
<thead>
<tr>
<th>Total Allowed</th>
<th>Connections</th>
<th>Available</th>
<th>CP=10%</th>
<th>CP=20%</th>
<th>CP=30%</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>20</td>
<td>80</td>
<td>8</td>
<td>16</td>
<td>24</td>
</tr>
<tr>
<td>100</td>
<td>40</td>
<td>60</td>
<td>6</td>
<td>12</td>
<td>18</td>
</tr>
<tr>
<td>100</td>
<td>60</td>
<td>40</td>
<td>4</td>
<td>8</td>
<td>12</td>
</tr>
<tr>
<td>100</td>
<td>80</td>
<td>20</td>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>100</td>
<td>90</td>
<td>10</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
</tbody>
</table>

**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
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
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

Enable dynamic defensive actions on z/OS
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
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
  - **TcpImage statement**
    - FLUSH | NOFLUSH  {PURGE | NOPURGE}
  - FLUSH and NOFLUSH take effect at Policy Agent initialization
    - FLUSH - specifies that any active policy should be deleted
    - NOFLUSH - specifies that active policy should not be deleted
  - PURGE and NOPURGE take effect at Policy Agent termination
    - PURGE - specifies that any active policy should be deleted
    - NOPURGE - specifies that active policy should not be deleted

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

- pasearch command
  ➤ Displays IDS policy read by Policy Agent

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

✓ Tip:
Restrict access to IDS policy displays using SAF SERVAUTH resources:
  ➤ EZB.PAGENT.sysname.tcpname.IDS
  ➤ EZB.NETSTAT.sysname.tcpname.IDS
Steps for Validating IDS Policy

1. 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

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\zCSConfigAssist\V1R12\files\sav...

Main Perspective

Navigation tree

z/OS Images

z/OS Communication Server technologies

Select the technology you want to configure and click Configure.

<table>
<thead>
<tr>
<th>Technology</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT-TLS</td>
<td>Application Transparent - Transport Layer Security</td>
</tr>
<tr>
<td>DMD</td>
<td>Defense Manager Daemon</td>
</tr>
<tr>
<td>IPSec</td>
<td>IP Security</td>
</tr>
<tr>
<td>IDS</td>
<td>Intrusion Detection Services</td>
</tr>
<tr>
<td>NSS</td>
<td>Network Security Services</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>PDP</td>
<td>Policy Based Routing</td>
</tr>
</tbody>
</table>

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...
Create IDS policy objects

![IDS Perspective](image)

Navigate to the Reusable Objects section and select Requirement Maps to 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
Requirement Map: IDS_Default - IBM Supplied: Intrusion Detection Services Starter Set

## Attack Protection Summary

<table>
<thead>
<tr>
<th>Enabled Attack Protection</th>
<th>Rule Name</th>
<th>Actions</th>
<th>Reports</th>
<th>Time Condition</th>
<th>Report Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flood Attack</td>
<td>Flood</td>
<td>Both Discard and Report</td>
<td>Inherited</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Perpetual Echo Attack</td>
<td>Echo</td>
<td>Report Events</td>
<td>Inherited</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Unwanted IP Protocols Att</td>
<td>IPProtocol</td>
<td>Report Events</td>
<td>Inherited</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Unwanted IP Options Att</td>
<td>IPOption</td>
<td>Report Events</td>
<td>Inherited</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>ICMP Redirect Attack</td>
<td>ICMPRedirect</td>
<td>Report Events</td>
<td>Inherited</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Malformed Packet Attack</td>
<td>MalformedPacket</td>
<td>Both Discard and Report</td>
<td>Inherited</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Outbound Raw Attack</td>
<td>OutboundRaw</td>
<td>Report Events</td>
<td>Inherited</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>IP Fragment Attack</td>
<td>IPFragmentation</td>
<td>Report Events</td>
<td>Inherited</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

**Console Parameters:** No

**SYSLOG Parameters:**
SYSLOG: Yes
SYSLOG Level: 4 - Warning

**Statistics Parameters:**
Statistics: Yes
Statistics Interval: 60
Report Stat if no events: No

**Trace Parameters:** No
### Attack Protection Details

#### Enabled Attack Protection: Flood Attack - Flood

<table>
<thead>
<tr>
<th>Flood Minimum Discard</th>
<th>Flood Percentage</th>
<th>Reports</th>
<th>Time Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>10</td>
<td>Inherited</td>
<td>None</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Traffic Descriptor</th>
<th>Port Location</th>
<th>Reports</th>
<th>Time Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>7 - Echo</td>
<td>Both Local and Remote</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13 - Time Of Day</td>
<td>Both Local and Remote</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17 - Quote Of The Day</td>
<td>Both Local and Remote</td>
<td>Inherited</td>
<td>None</td>
</tr>
<tr>
<td>19 - Char Gen</td>
<td>Both Local and Remote</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Details view of IDS_Default requirements map (3 of 4)


<table>
<thead>
<tr>
<th>Starting Protocol</th>
<th>Ending Protocol</th>
<th>Reports</th>
<th>Time Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>16</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>45</td>
<td>Inherited</td>
<td>None</td>
</tr>
<tr>
<td>48</td>
<td>49</td>
<td></td>
<td></td>
</tr>
<tr>
<td>52</td>
<td>88</td>
<td></td>
<td></td>
</tr>
<tr>
<td>90</td>
<td>93</td>
<td></td>
<td></td>
</tr>
<tr>
<td>95</td>
<td>255</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Starting Option</th>
<th>Ending Option</th>
<th>Reports</th>
<th>Time Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>67</td>
<td>Inherited</td>
<td>None</td>
</tr>
<tr>
<td>69</td>
<td>81</td>
<td></td>
<td></td>
</tr>
<tr>
<td>83</td>
<td>255</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Details view of IDS_Default requirements map (4 of 4)

**Enabled Attack Protection: Outbound Raw Attack - OutboundRaw**

<table>
<thead>
<tr>
<th>Starting Protocol</th>
<th>Ending Protocol</th>
<th>Reports</th>
<th>Time Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>88</td>
<td>Inherited</td>
<td>None</td>
</tr>
<tr>
<td>90</td>
<td>255</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Enabled Attack Protection: IP Fragment Attack - IPFragmentation**

<table>
<thead>
<tr>
<th>Reports</th>
<th>Time Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inherited</td>
<td>None</td>
</tr>
</tbody>
</table>

**Scan Protection Summary**

No Scan Protection Configured

**Traffic Regulation Summary**

No Traffic Regulation Configured
Use IDS_\_Default as a starting point

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

Modify Requirement Map

Name: IDS_Policy_Demo
Description: Show how to configure IDS policy

Use these panels to modify the requirement map:
1. Attack protection
2. Pre-attack scan monitoring
3. Traffic regulation
Modify copied default requirements map
Attack protection enabled by default
Customize report settings

Indicate where to report IDS events
- System console
- SYSLOGD
- IDS trace

Indicate if you want to log statistics at predefined intervals
- Log statistics to SYSLOGD
Enable scan policy

Enable scans to monitor for preattack scans:

1. 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: All_Well-Known_TCP, Rule Name: All_Well-Known_TCP, Sensitivity: Medium
- Enabled Traffic Descriptor: All_Well-Known_UDP, Rule Name: All_Well-Known_UDP, Sensitivity: Medium
- Enabled Traffic Descriptor: ICMP, Rule Name: ICMP, Sensitivity: High

Default Report Settings for Scans
- Modify Fast and Slow Scan Settings

next page
Modify Global Scan Settings

![Global Scan Settings dialog box]

- **Fast scan settings**
  - Fast scan interval: 1 minute
  - How many accesses within scan interval indicate an attack: 5

- **Slow scan settings**
  - Enable slow scans
  - Slow scan interval: 120 minutes
  - How many accesses within scan interval indicate an attack: 10
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

Use this panel to indicate if you want to implement traffic regulation (TR).

- **Enable traffic regulation**

**Steps**

1. To enable a traffic regulation for a particular traffic descriptor, select from the traffic descriptors table and click the "Enable" button.
2. Select the Action for each enabled traffic regulation.
3. To disable a traffic regulation for a traffic descriptor, select it from the Enabled traffic regulations table and click the "Disable" button.

**Traffic descriptors list**

- All_Well-Known_UDP
- Centralized_Policy_Server
- CICS
- DNS
- EE
- FTP-Server
- FTP-Server-SSL
- IKE
- IKE-NAT
- Kerberos
- LPD
- LBA-Advisor

**Enabled traffic regulations**

- Enabled Traffic Descriptor
- Rule Name
- Action

[Next page]
Set details for TR

[Image of the New Details window with the following configuration:

- **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:
    - 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 buttons]
Traffic regulation enabled

Use this panel to indicate if you want to implement traffic regulation (TR).

Steps:
1. To enable a traffic regulation for a particular traffic descriptor, select from the traffic descriptors table and click the "Enable" button.
2. Select the Action for each enabled traffic regulation.
3. To disable a traffic regulation for a traffic descriptor, select it from the Enabled traffic regulations table and click the "Disable" button.

Traffic descriptors list:
- All_Well-Known_UDP
- Centralized_Policy_Server
- CICS
- DNS
- EE
- IKE
- IKE-NAT
- Kerberos
- LPD
- LBA-Advisor
- LBA-Agent
- LDAP-Server

Enabled traffic regulations:

<table>
<thead>
<tr>
<th>Enabled Traffic Descriptor</th>
<th>Rule Name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP-Server-SSL</td>
<td>FTP-Server-SSL</td>
<td>Limit and Report</td>
</tr>
<tr>
<td>FTP-Server</td>
<td>FTP-Server</td>
<td>Limit and Report</td>
</tr>
</tbody>
</table>

Default Report Settings for Traffic Regulation...
IDS_Policy_Demo
requirements map now created
Create System Image
Create TCP/IP stack
Associate TCP/IP Stack with Requirements Map

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

- **IDS_Default**
  - IBM Supplied: Intrusion Detection Services Starter Set

- **IDS_Policy_Demo**
  - Show how to configure IDS policy
Perform application setup tasks
Install configuration files

IDS Perspective

- **Navigation tree**
  - IDS
    - Reusable Objects
      - Traffic Descriptors
      - Requirement Maps
    - z/OS Images
      - Image - SYSTEMA
        - Stack - TCP/IPA

- **Image Information**
  - z/OS image information
    - Enter a name for the z/OS image: **SYSTEMA**
    - Enter a description: **z/OS SYSTEMA**

- **Buttons**
  - 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.

- **Buttons**
  - Main Perspective
  - Apply Changes
  - OK
  - Cancel
  - Help
  - ?

next page
Show the configuration file to be installed

```
# 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
  IDSAAttackCondition
  {
    AttackType FLOOD
    IfcFloodMinDiscard 1000
    IfcFloodPercentage 10
  }
  IDSAActionRef Flood
}

IDSRule Echo
{
  ConditionType Attack
  IDSAAttackCondition
  {
    AttackType PERPETUAL_ECHO
    LocalPortGroupRef LocalEchoPortGroup-1
    RemotePortGroupRef RemoteEchoPortGroup-1
  }
  IDSAActionRef Echo
}

IDSRule IPProtocol
```
Set up to transfer policy file to z/OS
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)
Appendix A

- Scan Probe Instance Event Classifications
## ICMP Scan Probe Instance Classification

<table>
<thead>
<tr>
<th><strong>Request Type</strong></th>
<th><strong>Destination Address</strong></th>
<th><strong>Event Classification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>subnet base or broadcast</td>
<td>very suspicious</td>
</tr>
<tr>
<td>Information req</td>
<td>single host</td>
<td>possibly suspicious</td>
</tr>
<tr>
<td>Subnet Mask req</td>
<td>single host</td>
<td>possibly suspicious</td>
</tr>
<tr>
<td>Echo with IP Option Record Route</td>
<td>single host</td>
<td>possibly suspicious</td>
</tr>
<tr>
<td>Echo with Record Timestamp</td>
<td>single host</td>
<td>possibly suspicious</td>
</tr>
<tr>
<td>Echo or Timestamp, denied by QOS policy</td>
<td>single host</td>
<td>normal</td>
</tr>
<tr>
<td>Echo or Timestamp</td>
<td>single host</td>
<td>normal</td>
</tr>
</tbody>
</table>
# UDP Scan Probe Instance Classification

<table>
<thead>
<tr>
<th>Socket State</th>
<th>Event</th>
<th>Event Classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>RESERVED to no one</td>
<td>recv any packet</td>
<td>very suspicious</td>
</tr>
<tr>
<td>Unbound, not RESERVED</td>
<td>recv any packet</td>
<td>possibly suspicious - app may be temporarily down</td>
</tr>
<tr>
<td>Bound</td>
<td>packet rejected by QOS policy</td>
<td>normal</td>
</tr>
<tr>
<td>Bound</td>
<td>packet rejected by FW filtering</td>
<td>possibly suspicious</td>
</tr>
<tr>
<td>Bound</td>
<td>recv any packet</td>
<td>normal</td>
</tr>
</tbody>
</table>
## TCP Scan Probe Instance Classification

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

<table>
<thead>
<tr>
<th>URL</th>
<th>Content</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.twitter.com/IBM_Commsserver">http://www.twitter.com/IBM_Commsserver</a></td>
<td>IBM Communications Server Twitter Feed</td>
</tr>
<tr>
<td><a href="http://www.facebook.com/IBMCommserver">http://www.facebook.com/IBMCommserver</a></td>
<td>IBM Communications Server Facebook Fan Page</td>
</tr>
<tr>
<td><a href="http://www.rfc-editor.org/rfcsearch.html">http://www.rfc-editor.org/rfcsearch.html</a></td>
<td>Requests For Comment (RFC)</td>
</tr>
</tbody>
</table>