Integrated Intrusion Detection Services
for
z/OS Communications Server

SHARE Session 12847

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®
- Geographically Dispersed Parallel Sysplex
- HyperSwap
- i5/OS (logo)
- i5/OS®
- 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 8®
- System z9®
- System z10
- Tivoli (logo)®
- Tivoli®
- VTAM®
- WebSphere®
- xSeries®
- z9®
- z10 BC
- z10 EC

* 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 sensor on server

- 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

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

IDS manager

IDS event data

IDS adapters, IDS agents, event notification

Applications

Middleware

Networking

IDS policy

Service policy

IDS signatures

IDS data scanner

IDS event data

IDS manager

IDS adapters, IDS agents, event notification

Integrated IDS on z/OS complements external IDS technologies

IDS policy

IDS policy

IDS signatures files

IDS policy

IDS policy
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
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
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 intermittantly accessed over a longer time period (many hours)
      - scanner trying to avoid detection

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

* = 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"

<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>Count</td>
<td>Count</td>
<td>Count</td>
</tr>
<tr>
<td>Medium</td>
<td>Count</td>
<td>Count</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

* = 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.
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

<table>
<thead>
<tr>
<th>Existing IPv4 attack type</th>
<th>IPv6 implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Malformed packet</td>
<td>Existing IPv4 support extended to IPv6. No new configuration needed.</td>
</tr>
<tr>
<td>- ICMP redirect restrictions</td>
<td></td>
</tr>
<tr>
<td>- UDP perpetual echo</td>
<td></td>
</tr>
<tr>
<td>- Flood (both interface flood and TCP SYN flood)</td>
<td></td>
</tr>
<tr>
<td>IP protocol restrictions (specifies a list of restricted IP protocol values)</td>
<td>IPv6 next header restrictions (specifies a list of restricted IPv6 next header values, which may include IP protocol values)</td>
</tr>
<tr>
<td>IP option restrictions (specifies a list of restricted IPv4 options)</td>
<td>- IPv6 destination option restrictions (specifies a list of restricted IPv6 destination options)</td>
</tr>
</tbody>
</table>
|                                                               | - 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:

<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>
Data Hiding Protection

- 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
- Two forms of data hiding protection can be independently enabled:
  - Exploitation of ICMP and ICMPv6 error messages
  - Exploitation of IPv4 and IPv6 option pad

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.

Comm Server checks padding space for non-zero data.
TCP Queue Size Protection

- Builds upon V1R11 behavior. In that release, when a TCP 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

In V1R13, TCP queue size protection can be controlled with IDS policy...

- Protects TCP queues
  - Send, receive and out-of-order queues
  - Mark data “page eligible” after 60 seconds, or after 30 seconds if limit exceeded

- IDS configuration provides
  - Configurable queue size and configurable action of reset connection
  - IDS logging and statistics
  - No IDS tracing for this attack type

- Exclusion list can limit reporting or reset of constrained send queue
  - Can be a legitimate condition, for example, a printer running out of paper
  - Data on send queue is still marked "page eligible"

- Evaluated on a per-connection basis
V1R13 introduces the Global TCP Stall Protection to 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 is abnormally small
  - TCP send queue is full and data is not being retransmitted

- Global TCP stall condition is entered when...
  - At least 1000 TCP connections are active AND
  - At least 50% of those TCP connections are in a stalled state

- IDS reporting options (except IDS tracing) available
  - Two levels of logging - basic and detailed
  - Be careful with detailed syslogd logging - can generate 500+ messages per global stall detection

- Defensive action of "reset connection" may be configured
  - Resets all stalled connections when a global TCP stall condition is detected
## Comparing TCP queue size and TCP global stall attack types

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

Existing IDS checks

- IP header
- UDP header
- Local SAP
- Remote SAP
- LDLC command
- SNA data

EE-specific IDS checks

<table>
<thead>
<tr>
<th>EE Port</th>
<th>SNA Trans Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>12000</td>
<td>Signaling</td>
</tr>
<tr>
<td>12001</td>
<td>Network</td>
</tr>
<tr>
<td>12002</td>
<td>High</td>
</tr>
<tr>
<td>12003</td>
<td>Medium</td>
</tr>
<tr>
<td>12004</td>
<td>Low</td>
</tr>
</tbody>
</table>

EE is based on UDP

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

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

In-use connections $\Rightarrow$ Available connections: $A$

Connections from a given source IP address: IP@x: $X$

Configured controlling percentage: $CP$

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 $X+1 < CP \times A$ 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

<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>

Source IP address X attempts its fifth connection

- **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
IDS Actions

- Recording actions
- Defensive actions
Recording Options

- 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
Intrusion Detection Reports for Analysis
IDS Log Reports

trmdstat command produces reports based on IDS data recorded in syslog

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

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

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

- NetView provides ability to trap IDS messages from the system console or syslog and take predefined actions based on IDS event type such as:
  - Route IDS messages to designated NetView consoles
  - email notifications to security administrator
  - Run trmdstat and attach output to email
  - Issue pre-defined commands
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
- 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
IDS Policy Configuration Steps with the Configuration Assistant

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

2. Create system image and TCP/IP stack image

3. Associate new requirements map with TCP/IP stack

4. Perform policy infrastructure and application setup tasks

5. Transfer IDS policy to z/OS
Start a new IDS configuration

Main Perspective

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>DRP</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 navigation tree.
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)

**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>Default Report Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Hiding Attack</td>
<td>DataHiding</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>IPv6 Outbound Raw Attack</td>
<td>IPv6OutboundRaw</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>IPv6 Destination Options Attack</td>
<td>IPv6DestinationOptions</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>IPv6 Hop-by-Hop Options Attack</td>
<td>IPv6HopByHop</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>IPv6 Next Header Attack</td>
<td>IPv6NextHeader</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>TCP Queue Size Attack</td>
<td>TcpQueueSize</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Global TCP Stall Attack</td>
<td>GlobalTCPStall</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Flood Attack</td>
<td>Flood</td>
<td>Both Drop and Report</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td></td>
</tr>
<tr>
<td>Perpetual Echo Attack</td>
<td>Echo</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td></td>
</tr>
</tbody>
</table>

**Console Parameters:**
- No

**SYSLOG Parameters:**
- SYSLOG: Yes
- SYSLOG Level: 4 - Warning
# Details view of IDS_Default requirements map (2 of 4)

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Sub-Attack</th>
<th>Event Type</th>
<th>Report Setting</th>
<th>Statistics Parameters</th>
<th>Trace Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 Options Attack</td>
<td>IPv4 Option</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>Statistics Interval: 60 Minutes</td>
<td>No</td>
</tr>
<tr>
<td>ICMP Redirect Attack</td>
<td>ICMP Redirect</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>Report Stat if no events: Yes</td>
<td>None</td>
</tr>
<tr>
<td>Malformed Packet Attack</td>
<td>MalformedPacket</td>
<td>Both Drop and Report</td>
<td>Use Default Report Settings</td>
<td>Statistics: Yes</td>
<td>No</td>
</tr>
<tr>
<td>IPv4 Fragment Attack</td>
<td>IPv4Fragmentation</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>Statistics Interval: 60 Minutes</td>
<td>No</td>
</tr>
<tr>
<td>EE Malformed Packet Attack</td>
<td>EEMalformedPacket</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>Statistics: Yes</td>
<td>No</td>
</tr>
<tr>
<td>EE LDLC Check Attack</td>
<td>EELDLCCheck</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>Statistics: Yes</td>
<td>No</td>
</tr>
<tr>
<td>EE Port Check Attack</td>
<td>EEPortCheck</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>Statistics: Yes</td>
<td>No</td>
</tr>
<tr>
<td>EE XID Flood Attack</td>
<td>EEXIDFlood</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>Statistics: Yes</td>
<td>None</td>
</tr>
</tbody>
</table>

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

**Enabled Attack Protection: Data Hiding Attack - DataHiding**

<table>
<thead>
<tr>
<th>Enabled Options</th>
<th>Reports</th>
<th>Time Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checking of IP option pad fields: Enabled</td>
<td>Use Default Report</td>
<td>None</td>
<td>Report Events</td>
</tr>
<tr>
<td>Checking of embedded packets within ICMP error</td>
<td>Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>messages: Enabled</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>Starting Protocol</th>
<th>Ending Protocol</th>
<th>Reports</th>
<th>Time Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>16</td>
<td>Use Default Report</td>
<td>None</td>
<td>Report Events</td>
</tr>
<tr>
<td>18</td>
<td>57</td>
<td>Settings</td>
<td></td>
<td></td>
</tr>
<tr>
<td>59</td>
<td>88</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>90</td>
<td>255</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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*

<table>
<thead>
<tr>
<th>Reports</th>
<th>Time Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Default Report Settings</td>
<td>None</td>
<td>Report Events</td>
</tr>
</tbody>
</table>

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**

<table>
<thead>
<tr>
<th>EE XID TimeOut</th>
<th>Reports</th>
<th>Time Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>Report Events</td>
</tr>
</tbody>
</table>

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

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

Copy 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

OK Cancel Help
Modify copied default requirements map
**Attack protection enabled by default**

![Modify Requirement Map](image)

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

<table>
<thead>
<tr>
<th>Attack Type</th>
<th>Rule Name</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Hiding Attack</td>
<td>DataHiding</td>
<td>Report Events</td>
</tr>
<tr>
<td>IPv6 Outbound Raw Attack</td>
<td>IPv6OutboundRaw</td>
<td>Report Events</td>
</tr>
<tr>
<td>IPv6 Destination Options Attack</td>
<td>IPv6DestinationOptions</td>
<td>Report Events</td>
</tr>
<tr>
<td>IPv6 Hop-by-Hop Options Attack</td>
<td>IPv6HopByHop</td>
<td>Report Events</td>
</tr>
<tr>
<td>IPv6 Next Header Attack</td>
<td>IPv6NextHeader</td>
<td>Report Events</td>
</tr>
<tr>
<td>TCP Queue Size Attack</td>
<td>TcpQueueSize</td>
<td>Report Events</td>
</tr>
<tr>
<td>Global TCP Stall Attack</td>
<td>GlobalTCPStall</td>
<td>Report Events</td>
</tr>
<tr>
<td>Flood Attack</td>
<td>Flood</td>
<td>Both Drop and Report</td>
</tr>
<tr>
<td>Perpetual Echo Attack</td>
<td>Echo</td>
<td>Report Events</td>
</tr>
</tbody>
</table>

**Default Report Settings for Attacks...**
Customize report settings

[Image of a dialog box for 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

Buttons: OK, Cancel, Help
Enable scan policy

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

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

<table>
<thead>
<tr>
<th>Traffic Descriptors</th>
<th>Enabled Traffic Descriptor</th>
<th>Rule Name</th>
<th>Sensitivity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized_Policy_Server</td>
<td>All_Well-Known_TCP</td>
<td>All_Well-Known_TCP</td>
<td>Medium</td>
</tr>
<tr>
<td>CICS</td>
<td>All_Well-Known_TCP</td>
<td>All_Well-Known_TCP</td>
<td>Medium</td>
</tr>
<tr>
<td>DNS</td>
<td>ICMP</td>
<td>ICMP</td>
<td>High</td>
</tr>
<tr>
<td>EE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP-Server</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP-Server-SSL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICMP-IPv6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IKE</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IKE-NAT</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Kerberos</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LBA-Advisor</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LBA-Agent</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LDAP-Server</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPN</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Modify Requirement Map

[Image of the Modify Requirement Map window with highlighted instructions and options]
Modify Global Scan Settings

Fast scan settings

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

Slow scan settings

- Enable slow scans
- Slow scan interval: 120 minutes (1-1440)
- How many accesses within scan interval indicate an attack: 10 (1-64)
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).

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.
Set details for TR

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

Modify Requirement Map

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

Enabled traffic regulations
- **FTP-Server-SSL**
  - Rule Name: FTP-Server-SSL
  - Action: Limit and Report
- **FTP-Server**
  - Rule Name: FTP-Server
  - Action: Limit and Report

Buttons:
- Modify...
- Copy...
- Advanced...
- Move Up
- Move Down
- View Details...
- OK
- Cancel
- Help

Default Report Settings for Traffic Regulation...
IDS_Policy_Demo
requirements map now created
Create System Image

IDS Perspective

Work with settings for z/OS images

Add a New z/OS Image...

New z/OS Image: Information

z/OS image name: *SYSTEMA

Description: z/OS System A

z/OS release: V1R13

OK Cancel Help
Create TCP/IP stack

IDS Perspective

Image Information
- z/OS image name: *SYSTEMA
- Description: z/OS System A
- z/OS release: V1R13

Add New TCP/IP Stack...

New TCP/IP Stack: Information
- TCP/IP stack name: *TCPIPA
- Description: TCP/IP stack TCPIPA

OK Cancel Help
Associate TCP/IP Stack with Requirements Map

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

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

- Name: IDS_policy_demo
  - Description: Show how to configure IDS policy
Perform application setup tasks
Install configuration files

- Add New TCP/IP Stack
- Application Setup Tasks
- Install Configuration Files

IDS Perspective

Navigation tree

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

Image Information

- z/OS image name: SYSTEMA
- Description: z/OS System A
- z/OS release: V1R13

- Perform initial setup tasks including RACF directives and start procedures.
- View the produced configuration files, install the files to the z/OS system, and view a configuration summary.
Show the configuration file to be installed

```
##
## IDS Policy Agent Configuration file for:
##   Image: SYSTEMA
##   Stack: TCP/IPA
##
## 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
  }
  IDSAActionRef DataHiding
}

IDSRule IPv6OutboundRaw
{
  ConditionType Attack
  IDSAttackCondition
  {
    AttackType OUTBOUND_RAW_IPV6
    ProtocolGroupRef IpProtGroup-1
  }
  IDSAActionRef IPv6OutboundRaw
```
Set up to transfer policy file to z/OS

List of Configuration Files for Image SYSTEMA

Tip: Not all application setup tasks are marked complete. These tasks provide instructions for setting up your environment, including RACF directives and start procedures. Click Help for more information.

List of Configuration Files for Image SYSTEMA

<table>
<thead>
<tr>
<th>Stack</th>
<th>Configuration</th>
<th>File Name (may be modified)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCPIPA</td>
<td>IDS Policy</td>
<td>/etc/cfgasst/v1r13/SYSTEMA/TCPIPA/idsPol</td>
</tr>
</tbody>
</table>

Show Configuration File | Install | Configuration Summary

- Permanently save backing store after install

Install Files to Remote Host

Install file:

/etc/cfgasst/v1r13/SYSTEMA/TCPIPA/idsPol

FTP login information

Host name: *hostname.com
Port number: *21
User ID: *idsking
Password: *password

- Use SSL

Data transfer mode

- Default
- Passive
- Active

Comment for the configuration file prologue (optional)

Comment:

Go | Close | View FTP Log | Help
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)
Please fill out your session evaluation

- z/OS Communications Server Intrusion Detection Services
- Session #12847
- QR Code:
For more information ...

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