z/OS Communications Server
Intrusion Detection Services

SHARE Session 17986

Lin Overby - overbylh@us.ibm.com
### Trademarks and notices

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States or other countries or both:

- Advanced Peer-to-Peer Networking®
- AIX®
- alphaWorks®
- AnyNet®
- AS/400®
- BladeCenter®
- Candle®
- CICS®
- DataPower®
- DB2 Connect
- DB2®
- DRDA®
- e-business on demand®
- e-business (logo)
- e-business(logo)®
- ESCON®
- FICON®
- GDDM®
- GDPS®
- Geographically Dispersed Parallel Sysplex
- HiperSockets
- HPR Channel Connectivity
- HyperSwap
- i5/OS (logo)
- i5/OS®
- IBM eServer
- IBM (logo)®
- IBM®
- IBM zEnterprise™ System
- IMS
- InfiniBand ®
- IP PrintWay
- IPDS
- iSeries
- LANDP®
- Language Environment®
- MQSeries®
- MVS
- NetView®
- OMEGAMON®
- Open Power
- OpenPower
- Operating System/2®
- Operating System/400®
- OS/2®
- OS/390®
- OS/400®
- Parallel Sysplex®
- POWER®
- POWER7®
- PowerVM
- PR/SM
- pSeries®
- RACF®
- Rational Suite®
- Rational®
- Redbooks
- Redbooks (logo)
- Sysplex Timer®
- System i5
- System p5
- System x®
- System z®
- System 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.

### 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.
z/OS Communications Server provides an integrated Intrusion Detection Services (IDS) for TCP/IP. This session will describe the Communications Server IDS and how it can be used to detect intrusion attempts against z/OS.

This session will cover the following topics:

- IDS Overview
- Intrusion events detected by z/OS IDS
- IDS Actions
  - Recording Actions
  - Defensive Actions
- IDS Reports
- Automation for IDS
- Working with IDS policy
The Intrusion Threat

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

- Attacks can be deliberate or unintentional
  - Deliberate: malicious intent from outside or internal bots
  - Unintentional: various forms of errors on network nodes

- Attacks can occur from Internet or intranet
  - Firewalls can provide some level of protection from Internet
  - Perimeter Security Strategy alone may not be sufficient.
    - Considerations:
      ✓ Access permitted from Internet
      ✓ Trust of intranet
Intrusion Detection Services Overview

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

Defensive methods
- Packet discard
- Limit connections
- Reset connections

Reporting
- Logging,
- Event messages to local console,
- IDS packet trace
- Notifications to Tivoli NetView

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

z/OS in-context IDS broadens overall intrusion detection coverage:
- Ability to evaluate inbound encrypted data - IDS applied after IPSec decryption on the target system
- Avoids overhead of per packet evaluation against table of known attacks - IDS policy checked after attack detected
- Detects statistical anomalies real-time - target system has stateful data / internal thresholds that are generally unavailable to external IDSs
- Policy can control prevention methods on the target, such as connection limiting and packet discard
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
Scan Policy Overview

Scan policy provides the ability to:

- Obtain notification and documentation of scanning activity
  - Notify the installation of a detected scan via console message or syslogd message
  - Trace potential scan packets

- Control the parameters that define a scan:
  - The time interval
  - The threshold number of scan events

- Reduce level of false positives
  - Exclude well known "legitimate scanners" via exclusion list
    - e.g. network management
  - Specify a scan sensitivity level
    - by port for UDP and TCP
    - highest priority rule for ICMP, ICMPv6
Scan Event Counting and Scan Sensitivity

- Each scan event is internally classified as normal, suspicious or very suspicious
  - Socket state, ICMP, ICMPv6 type affect this classification
    - Scan instance event classification by event type included in IP Configuration Guide.
- Scan sensitivity determines whether a scan event is "countable"

<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
Attacks Against The TCP/IP Stack

- The system already silently defends itself from many attacks against the TCP/IP stack.

- IDS adds capability to control recording of intrusion events and to provide supporting documentation.

- IDS adds controls to detect and disable uncommon or unused features which could be used in an attack.
Attack Categories

- **Malformed packet events**
  - Detects IPv4 and IPv6 packets with incorrect or partial header information

- **Inbound fragment restrictions**
  - Detects fragmentation in first 88 bytes of an IPv4 datagram
    - z/OS V2R1 changes the fragmentation attack probe to no longer consider fragment length as a criteria. Checks will be based purely on whether overlays occur and whether they change the packet content.

- **IPv4 and IPv6 protocol restrictions**
  - Detects use of IP protocols you are not using that could be misused
  - Called "next header restrictions" for IPv6

- **IPv4 and IPv6 option restrictions**
  - Detects use of IP options you are not using that could be misused
  - Can restrict both destination and hop-by-hop options for IPv6

- **ICMP, ICMPv6 redirect restrictions**
  - Detects receipt of ICMP redirect to modify routing tables.

- **UDP perpetual echo**
  - Detects traffic between IPv4 and IPv6 UDP applications that unconditionally respond to every datagram received

- **Outbound RAW socket restrictions**
  - Detects z/OS IPv4 or IPv6 RAW socket application crafting invalid outbound packets

- **Flood Events**
  - Detects flood of SYN packets from "spoofed" IPv4 or IPv6 sources
  - Detects high percentage of packet discards on a physical IPv4 or IPv6 interface

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

- **TCP queue size**
  - Detects queue size constraints for individual connections

- **Global TCP stall**
  - Detects cases where large number and percentage of TCP connections are stalled

- **Enterprise Extender-specific attacks**
  - Malformed Packet
  - LDLC Check
  - Port Check
  - EE XID Flood
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
    - Flood minimum discard (default 1000)
    - Flood percentage (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 (flood minimum discard) 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 flood percentage 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
  - Discard rate for the interval is less than or equal to 1/2 of the specified flood percentage threshold
# Interface Flooding Example

- Assume the IDS flood policy specifies:
  - Flood minimum discard: 2000
  - Flood percentage: 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>
</tbody>
</table>
| < 1 min       | 20,000      | 2000        | 10%          | **interface flood start detected.**
  
  Run 1 minute timer until flood end detected. |

| +1 min        | 40,000      | 3000        | 7.5%         | flood condition still exists, reset 1 minute timer. |

| +1 min        | 50,000      | 2500        | 5%           | **Interface flood end detected.**

Discard rate <= half of policy specified rate.
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

Available connections: \( A \)

Configured controlling percentage: \( CP \)

Connections from a given source IP address: IP@x: \( X \)

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 \( X+1 < CP \cdot A \) 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 have 40 connections available (A=40) and a controlling percentage (CP) of 20%, when source IP address X tries to establish its fifth connection, it will be allowed (40 * 20% = 8, so 5 connections is within the acceptable range).

B If we have 20 connections available (A) and CP is again 20%, when source IP address X tries to establish its fifth connection, it will be rejected (20 * 20% = 4, so 5 would exceed the allowable number of connections).
Traffic Regulation for UDP

- Allows control over length of inbound receive queues for UDP applications
  - Specified on a per-port basis
  - Can be applied to ports of your choosing

- Before TR for UDP, UDP queue limit control was requested globally for all queues
  - UDPQueueLimit ON | OFF in TCP/IP Profile

- If neither TR UDP or UDPQueueLimit is used, a stalled application or a flood against a single UDP port could consume all available buffer storage
  - TR UDP supercedes UDPQueueLimit specification

- TR UDP queue limit expressed as abstract queue length
  - SHORT or VERY SHORT
    - For applications that tend to receive data faster than they can process it
  - LONG or VERY LONG
    - Useful for fast or high priority applications with bursty arrival rates
IDS Actions

- Recording actions
- Defensive actions
Recording Actions

- Recording options controlled by IDS policy action specification

- Possible options
  - Event logging
    - Syslogd
      - Number of events per attack subtype recorded in a five minute interval can be limited (for most attack subtypes)
  - Local Console
    - Recording suppression provided if quantity of IDS console messages reach policy-specified thresholds
  - Statistics
    - Syslogd
      - Normal and Exception conditions
  - IDS packet trace
    - Activated after attack detected
      - Number of packets traced for multipacket events are limited
      - Amount of data trace is configurable (header, full, byte count)
    - Not available for all attack types

- All IDS events recorded in syslog and console messages, and packet trace records have probeid and correlator
  - Probeid identifies the point at which the event detected
  - Correlator allows association of corresponding syslog and packet trace records
Defensive Actions by Event Type

- **Attack Events**
  - Packet discard
    - Certain attack events always result in packet discard and are not controlled by IDS policy action
      - malformed packets
      - flood (synflood discard)
    - Most attack types controlled by IDS policy action
      - ICMP redirect restrictions
      - IPv4 and IPv6 option restrictions
      - IPv4 and IPv6 protocol restrictions
      - IP fragment
      - outbound raw restrictions
      - perpetual echo
      - data hiding
      - EE malformed, LDLC and port checks
  - Reset connection
    - TCP queue size
    - Global TCP stall
  - No defensive action defined
    - flood (interface flood detection)

- **Scan Events**
  - No defensive action defined

- **Traffic Regulation Events**
  - Controlled by IDS policy action
    - TCP - Connection limiting
    - UDP - Packet discard
IDS and Defensive Filtering

- The Defense Manager component allows authorized users to dynamically install time-limited, defensive filters:
  - A local security administrator can install filters based on information received about a pending threat
  - Enables filter installation through automation based on analysis of current attack conditions

- Defensive filtering is an extension to IDS capabilities
  - Adds additional defensive actions to protect against attacks

- Requires minimal IP Security configuration to enable IP packet filtering function
  - Uses ipsec command to control and display defensive filters

- Defense Manager
  - Manages installed defensive filters in the TCP/IP stack
  - Maintains record of defensive filters on DASD for availability in case of DM restart or stack start/restart

- Defensive filter scope may be:
  - Global - all stacks on the LPAR where DM runs
  - Local - apply to a specific stack

- Defensive filter are installed "in-front" of configured/default filters
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. Initially configure policy for reporting actions only (no defensive actions)
2. Invoke PAGENT and TRMD
3. Issue PASEARCH and verify that the correct policy is installed
4. Keep policy in force for a trial period
5. Issue IDS netstat to view active IDS policy and statistics
6. Run TRMDSTAT reports to verify syslog messages for intrusion events
7. Adjust the policy as required
8. Add defensive actions
Configuration Assistant for z/OS Communications Server

- GUI-based approach to configuring:
  - IDS
  - AT-TLS
  - IPSec and IP filtering
  - QoS
  - Policy-based Routing
- Focus on high level concepts vs. low level file syntax
- Available through z/OSMF-based web interface
  - Standalone Windows application
    - Not supported after z/OS V1R13
- Builds and maintains
  - Policy files
  - Related configuration files
  - JCL procedures and RACF directives
- Supports import of existing policy files
IDS Policy Configuration Steps
with the Configuration Assistant

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

2. Create system image and TCP/IP stack image

3. Associate new requirements map with TCP/IP stack

4. Transfer IDS policy to z/OS

5. Perform policy infrastructure and application setup tasks
Configuration Assistant for z/OS Communications Server

Welcome to V2R1 Configuration Assistant for z/OS Communications Server
Use this task to create and manage configuration for z/OS Communications Server policy-based networking functions.

Select a backing store for configuration:
- saveData
- Open

Learn more about Configuration Assistant:
- What’s New
- Getting Started
- Migrating to z/OSMF
- Application Setup Tasks
- Tutorials
- FAQs
Start a new IDS configuration - create a new backing store
Create IDS policy objects - select the IDS policy perspective
### Traffic Descriptors

#### V2R1 Current Backing Store = idsdemoLHO

Select a perspective: **IDS**

**System** | **Traffic Descriptors** | **Requirement Maps**
--- | --- | ---

**Actions**

<table>
<thead>
<tr>
<th>Name Filter</th>
<th>Description Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>AI_WellKnown_TCP</td>
<td>IBM supplied: AI Well-Known TCP Traffic</td>
</tr>
<tr>
<td>AI_WellKnown_UDP</td>
<td>IBM supplied: AI Well-Known UDP Traffic</td>
</tr>
<tr>
<td>Centralized_Policy_Server</td>
<td>(VERIFY) IBM supplied: Centralized Policy Server</td>
</tr>
<tr>
<td>CCS</td>
<td>(VERIFY) IBM supplied: CCS traffic</td>
</tr>
<tr>
<td>DNS</td>
<td>(VERIFY) IBM supplied: Domain Name Server traffic</td>
</tr>
<tr>
<td>EE</td>
<td>IBM supplied: Enterprise Extender (EE) traffic</td>
</tr>
<tr>
<td>FTP-Server</td>
<td>(VERIFY) IBM supplied: FTP Server traffic</td>
</tr>
<tr>
<td>FTP-Server-SSL</td>
<td>(VERIFY) IBM supplied: FTP Server SSL traffic using port 990</td>
</tr>
<tr>
<td>ICMP</td>
<td>IBM supplied: ICMP IPv4 traffic</td>
</tr>
<tr>
<td>ICMPv6</td>
<td>IBM supplied: ICMP IPv6 traffic</td>
</tr>
<tr>
<td>KE</td>
<td>IBM supplied: Internet Key Exchange daemon traffic</td>
</tr>
<tr>
<td>KE-NAT</td>
<td>IBM supplied: NAT - Internet Key Exchange daemon traffic</td>
</tr>
<tr>
<td>Kerberos</td>
<td>(VERIFY) IBM supplied: Kerberos Server traffic</td>
</tr>
<tr>
<td>LBA-Advisor</td>
<td>(VERIFY) IBM supplied: z/OS Load Balancing Advisor traffic</td>
</tr>
<tr>
<td>LBA-Agent</td>
<td>(VERIFY) IBM supplied: z/OS Load Balancing Advisor - Agent traffic</td>
</tr>
<tr>
<td>LDAP-Server</td>
<td>(VERIFY) IBM supplied: LDAP Server traffic</td>
</tr>
<tr>
<td>LPD</td>
<td>IBM supplied: LPD Server traffic</td>
</tr>
<tr>
<td>NSS_Server</td>
<td>(VERIFY) IBM supplied: Network Security Services server traffic</td>
</tr>
<tr>
<td>Ntpmap-Server</td>
<td>IBM supplied: Ntpmap Server traffic</td>
</tr>
<tr>
<td>REXEC-Server</td>
<td>IBM supplied: REXEC - Remote Execution Server</td>
</tr>
<tr>
<td>RSH-Server</td>
<td>IBM supplied: RSH - Remote Shell Server</td>
</tr>
<tr>
<td>SMTP</td>
<td>IBM supplied: Simple Mail Transfer Protocol (SMTP) Server</td>
</tr>
<tr>
<td>SNMP-Agent</td>
<td>IBM supplied: Simple Network Management Protocol (SNMP) Agent traffic</td>
</tr>
</tbody>
</table>

Total: 26, Selected: 0
Evalute 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 Attack¹</td>
<td>DataHiding</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>IPv6 Outbound Raw Attack¹</td>
<td>IPv6OutboundRaw</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>IPv6 Destination Options Attack¹</td>
<td>IPv6DestinationOptions</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>IPv6 Hop-by-Hop Options Attack¹</td>
<td>IPv6HopByHop</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>IPv6 Next Header Attack¹</td>
<td>IPv6NextHeader</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>TCP Queue Size Attack¹</td>
<td>TcpQueueSize</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>Global TCP Stall Attack¹</td>
<td>GlobalTCPStall</td>
<td>Both Drop and Report</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>0</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>0</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>0</td>
</tr>
<tr>
<td>IPv4 Protocols Attack</td>
<td>IPv4Protocol</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>IPv4 Options Attack</td>
<td>IPv4Option</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>ICMP Redirect Attack</td>
<td>ICMPRedirect</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>Malformed Packet Attack</td>
<td>MalformedPacket</td>
<td>Both Drop and Report</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>IPv4 Outbound Raw Attack¹</td>
<td>IPv4OutboundRaw</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>IP Fragment Attack</td>
<td>Fragmentation</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>Ee Malformed Packet Attack¹</td>
<td>EEMalformedPacket</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>EE L DLC Check Attack¹</td>
<td>EEldlcheck</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>EE Port Check Attack¹</td>
<td>EEPortCheck</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>0</td>
</tr>
<tr>
<td>EE X ID Flood Attack¹</td>
<td>EExFlood</td>
<td>Report Events</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>0</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 Settings</td>
<td>None</td>
<td>Report Events</td>
</tr>
<tr>
<td>Checking of embedded packets within ICMP error messages: Enabled</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>Report Events</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.
Details view of IDS_Default requirements map (2 of 4)

Welcome | Configuration...

Configuration Assistant (Home) | IDS | View Details

**View Details**

**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 Settings</td>
<td>None</td>
<td>Report Events</td>
</tr>
<tr>
<td>Checking of embedded packets within ICMP error 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 Settings</td>
<td>None</td>
<td>Report Events</td>
</tr>
<tr>
<td>18</td>
<td>87</td>
<td></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.

**Enabled Attack Protection: IPv6 Destination Options Attack - IPv6DestinationOptions**

<table>
<thead>
<tr>
<th>Starting Option</th>
<th>Ending Option</th>
<th>Reports</th>
<th>Time Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>Report Events</td>
</tr>
<tr>
<td>3</td>
<td>137</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>139</td>
<td>193</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>195</td>
<td>200</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>202</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.

**Enabled Attack Protection: IPv6 Hop-by-Hop Options Attack - IPv6HopByHop**

<table>
<thead>
<tr>
<th>Starting Option</th>
<th>Ending Option</th>
<th>Reports</th>
<th>Time Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
<td>Use Default Report Settings</td>
<td>None</td>
<td>Report Events</td>
</tr>
<tr>
<td>3</td>
<td>137</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>139</td>
<td>193</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>195</td>
<td>200</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>202</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 (3 of 4)
Details view of IDS_Default requirements map (4 of 4)

(... several intervening pages)

<table>
<thead>
<tr>
<th>View Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attack - EEMalformedPacket</strong></td>
</tr>
<tr>
<td>Reports</td>
</tr>
<tr>
<td>Use Default Report Settings</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

| Enabled Attack Protection: EELDLC Check Attack - EELDLCCheck |
| Reports | Time Condition | Action |
| Use Default Report Settings | None | Report Events |
| The attack is not available for V1R12 stacks. The requirement map is configured with this attack, but if the stack is mapped to a V1R12 stack, the attack will be ignored. |

| Enabled Attack Protection: EE Port Check Attack - EEPorCkCheck |
| Reports | Time Condition | Action |
| Use Default Report Settings | None | Report Events |
| The attack is not available for V1R12 stacks. The requirement map is configured with this attack, but if the stack is mapped to a V1R12 stack, the attack will be ignored. |

| Enabled Attack Protection: EE XID Flood Attack - EEXIDFlood |
| Reports | Time Condition | Action |
| Use Default Report Settings | None | Report Events |
| The attack is not available for V1R12 stacks. The requirement map is configured with this attack, but if the stack is mapped to a V1R12 stack, the attack will be ignored. |

| Scan Protection Summary |
| No Scan Protection Configured |

| Traffic Regulation Summary |
| No Traffic Regulation Configured |
Use IDS_Default as a starting point

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Attacks</th>
<th>Scans</th>
<th>Traffic Regulation</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Configuration Assistant (Home) › IDS › Requirement Map**

**Copy Requirement Map**

- **Name:**
  - IDS_policy_demo

- **Description:**
  - Show how to configure IDS policy

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

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

[OK]  [Cancel]
Modify copied default requirements map
Attack protection enabled by default

Modify Requirement Map

Enable attack protection

Steps

Default report settings for Attacks...
Customize report settings

Report Types

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

[OK] [Cancel]
Enable scan policy

Modify Requirement Map

- Name
- Attacks
- Scans
- Traffic Regulation

- Enable scan

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

Enable commands:
- All_Well-Known_TCP
- All_Well-Known_UDP
- ICMP

Default report settings for Scans...

Modify Fast and Slow Scan Settings...
Modify global scan settings

**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 (minutes, 1-1440)

[OK] [Cancel]
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

Modify Requirement Map

- Enable traffic regulation

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

**Actions**
- Enable...
- Disable
- Modify...
- Copy...
- Move Up
- Move Down
- Advanced...

Default report settings for Traffic Regulation...
Set details for TR

New Traffic Regulation Details

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
* Max number of connections: 100 (0-65535)
* Limit each host to the following percentage of the available connections: 20
Limit scope: All sockets

OK  Cancel
Traffic regulation enabled

Modify Requirement Map

Enable traffic regulation

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

Actions

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

Default report settings for Traffic Regulation...

OK  Cancel
IDS_policy_demo requirements map now created

V2R1 Current Backing Store = idsdemoLHO

Select a perspective: IDS

Actions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDS_Default</td>
<td>IBM Supplied: Intrusion Detection Services Starter Set</td>
</tr>
<tr>
<td>IDS_policy_demo</td>
<td>Show how to configure IDS policy</td>
</tr>
</tbody>
</table>
Create system image

Welcome X Configuratio... X

Configuration Assistant (Home) → IDS

V2R1 Current Backing Store = idsdemoLHO

Select a perspective: IDS

Systems Traffic Descriptors Requirement Maps

Actions
Properties...
Copy...
Delete

Add z/OS Image...

Welcome X Configuratio... X

Configuration Assistant (Home) → IDS → z/OS Image

Add z/OS Image

Name:
IDSDEMO

Description:
IDS Demo System

z/OS Release:
V2R1

OK Cancel

© Copyright International Business Machines Corporation 2015. All rights reserved.
Create TCP/IP stack

V2R1 Current Backing Store = idsdemoLHO

Select a perspective: IDS

Systems | Traffic Descriptors | Requirement Maps

Actions

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Status</th>
<th>Release</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSDMO</td>
<td>Image</td>
<td>Complete</td>
<td>V2R1</td>
<td>IDS Demo System</td>
</tr>
</tbody>
</table>

Proceed to the Next Step?

IDS requirement maps are configured for each TCP/IP stack. To continue with configuration you need to add a TCP/IP stack to the new z/OS image. Do you want to add a TCP/IP stack now?

Cancel  Proceed

Add TCP/IP Stack

* Name:  IDSSTACK

Description:

IDS Demo Stack

OK  Cancel
Associate TCP/IP stack with requirements map

The stack is now configured to use the IDS_Default requirement map protection. To change the level of protection you can select a different requirement map for this stack. Click Proceed if you would like to be directed to the stack requirement map panel.
Install configuration files
Show the configuration file to be installed
Set up to install configuration files on target z/OS system

Install File
* Install file name:
/etc/cfgasst/v2r1/IDSDMO/IDSSTACK/idsPol

Select installation method
- Save to disk
- FTP

FTP information
* Host name: 
* Port number: 21
* User ID: 
* Password: 

Create the directories if they do not exist

Data transfer mode
- Default
- Passive
- Active

Comment for the configuration file prologue (optional)
Perform application setup tasks - All workflows view

IBM z/OS Management Facility

Welcome
Notifications (3)
Workflows
Configuration
Configuration Assistant
Links
z/OSMF Administration
z/OSMF Settings
Refresh

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

<table>
<thead>
<tr>
<th>Workflow Name</th>
<th>Description</th>
<th>Version</th>
<th>Vendor Filter</th>
<th>Owner Filter</th>
<th>System Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>z/OS Communications Server: Setup to run Traffic Regulation Management Daemon (TRMD) - Workflow_0</td>
<td>z/OS Communications Server: Setup to run Traffic Regulation Management Daemon (TRMD)</td>
<td>1.0</td>
<td>IBM</td>
<td>user1</td>
<td>XESDEV/MVS160 (MVS160_00)</td>
</tr>
<tr>
<td>z/OS Communications Server: Setup for Syslogd - Workflow_0</td>
<td>z/OS Communications Server: Setup for Syslogd</td>
<td>1.0</td>
<td>IBM</td>
<td>user1</td>
<td>XESDEV/MVS160 (MVS160_00)</td>
</tr>
<tr>
<td>Setting up to run IP Defensive Filters with Defense Manager Daemon (DMD) - Workflow_0</td>
<td>Setting up to run IP Defensive Filters with Defense Manager Daemon (DMD)</td>
<td>1.0</td>
<td>IBM</td>
<td>user1</td>
<td>XESDEV/MVS160 (MVS160_00)</td>
</tr>
<tr>
<td>Set up to run Network Security Services (NSS) - Workflow_0</td>
<td>Set up to run Network Security Services (NSS)</td>
<td>1.0</td>
<td>IBM</td>
<td>user1</td>
<td>XESDEV/MVS160 (MVS160_00)</td>
</tr>
<tr>
<td>z/OS Communications Server: IP Security with IKE - Workflow_0</td>
<td>z/OS Communications Server: IP Security with IKE</td>
<td>1.0</td>
<td>IBM</td>
<td>user1</td>
<td>XESDEV/MVS160 (MVS160_00)</td>
</tr>
<tr>
<td>z/OS Communications Server: Install Sample Profiles for TCP/IP Components - Workflow_0</td>
<td>z/OS Communications Server: Install Sample Profiles for TCP/IP Components</td>
<td>1.0</td>
<td>IBM</td>
<td>user1</td>
<td>XESDEV/MVS160 (MVS160_00)</td>
</tr>
<tr>
<td>z/OS Communications Server: Setup to run Policy Agent - Workflow_0</td>
<td>z/OS Communications Server: Setup to run Policy Agent</td>
<td>1.0</td>
<td>IBM</td>
<td>user1</td>
<td>XESDEV/MVS160 (MVS160_00)</td>
</tr>
</tbody>
</table>
Perform application setup tasks - Specific workflow view

![Workflow Setup](image)

<table>
<thead>
<tr>
<th>State Filter</th>
<th>No. Filter</th>
<th>Title Filter</th>
<th>Owner Filter</th>
<th>Skill Category Filter</th>
<th>Assignees Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unassigned</td>
<td>1</td>
<td>Define the RACF user ID for Policy Agent</td>
<td></td>
<td>Basic JCL</td>
<td></td>
</tr>
<tr>
<td>Unassigned</td>
<td>2</td>
<td>Setup for Policy Agent to execute operator commands</td>
<td></td>
<td>Basic JCL</td>
<td></td>
</tr>
<tr>
<td>Unassigned</td>
<td>3</td>
<td>Setup for Policy Agent to have access to the BPX.DAEMON RACF profile</td>
<td></td>
<td>Basic JCL</td>
<td></td>
</tr>
<tr>
<td>Unassigned</td>
<td>4</td>
<td>Permit the display of policies, access to policies by Configuration Assistant and policy clients</td>
<td></td>
<td>Basic JCL</td>
<td></td>
</tr>
<tr>
<td>Unassigned</td>
<td>5</td>
<td>Sample Policy Agent Configuration for Image</td>
<td></td>
<td>Basic JCL</td>
<td></td>
</tr>
<tr>
<td>Unassigned</td>
<td>6</td>
<td>Sample Policy Agent Configuration for Stack</td>
<td></td>
<td>Basic JCL</td>
<td></td>
</tr>
<tr>
<td>Unassigned</td>
<td>7</td>
<td>Sample started procedure for the Policy Agent</td>
<td></td>
<td>Basic JCL</td>
<td></td>
</tr>
</tbody>
</table>
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**
  - trmddstat produces reports from IDS syslogd records
    - Summary and detailed
  - IDS event handling by Tivoli NetView

- **Defensive filtering**
  - Installed through ipsec command
  - Manually (by human being) or through automation (via external security event manager)
For more information ...

<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/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/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/atsmastr.nsf/Web/TechDocs">http://www.ibm.com/support/techdocs/atsmastr.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>