e-business

Integrated Intrusion Detection Services for z/OS Communications Server

SHARE Session 3920

March 5, 2002

Lin Overby
WebSphere and eServer Networking Solutions
Strategy and Design
Internet: overbylh @ us.ibm.com

Integrated Intrusion Detection Services

z/OS Communications Server provides integrated Intrusion Detection Services (IDS) for TCP/IP in z/OS V1R2. 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
  - Defensive Actions
  - Recording Actions
- IDS Reports
- Automation for IDS
- Working with IDS policy

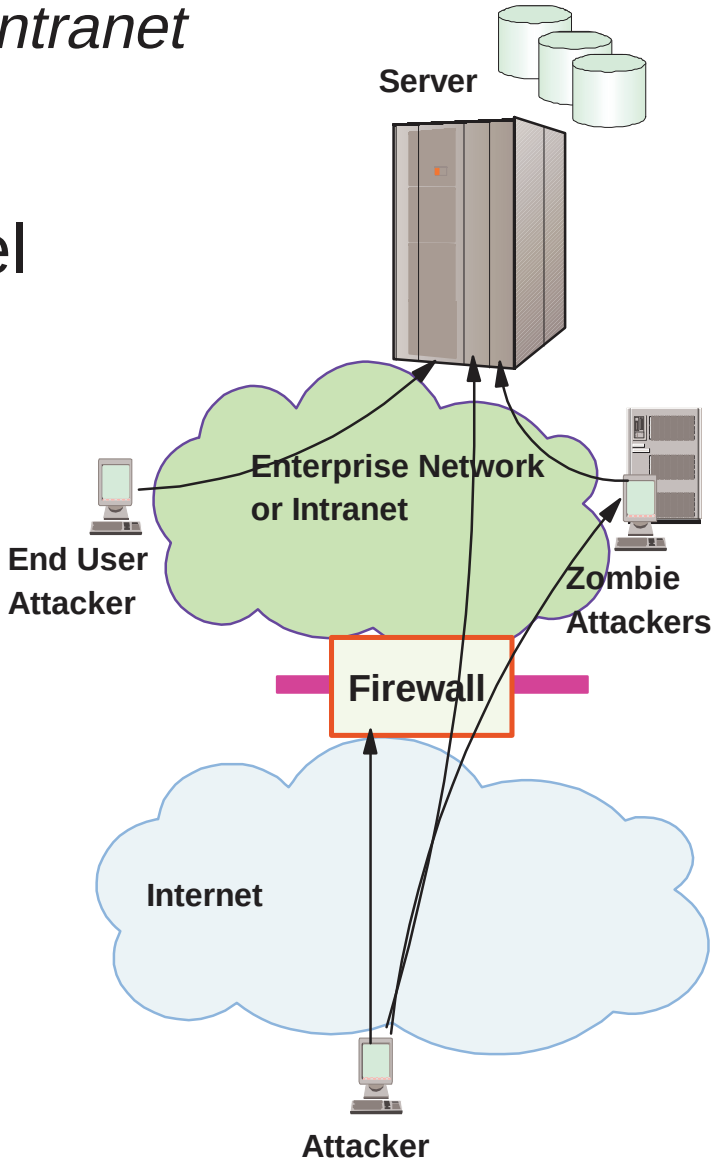
What is an Intrusion?

- Information Gathering
  - Network and system topology
  - Data location and contents
- Unauthorized Usage
  - Eavesdropping/Impersonation/Theft
    - On the network/on the host
  - Base for further attacks on others
    - Amplifier
    - 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

Sources of Intrusions

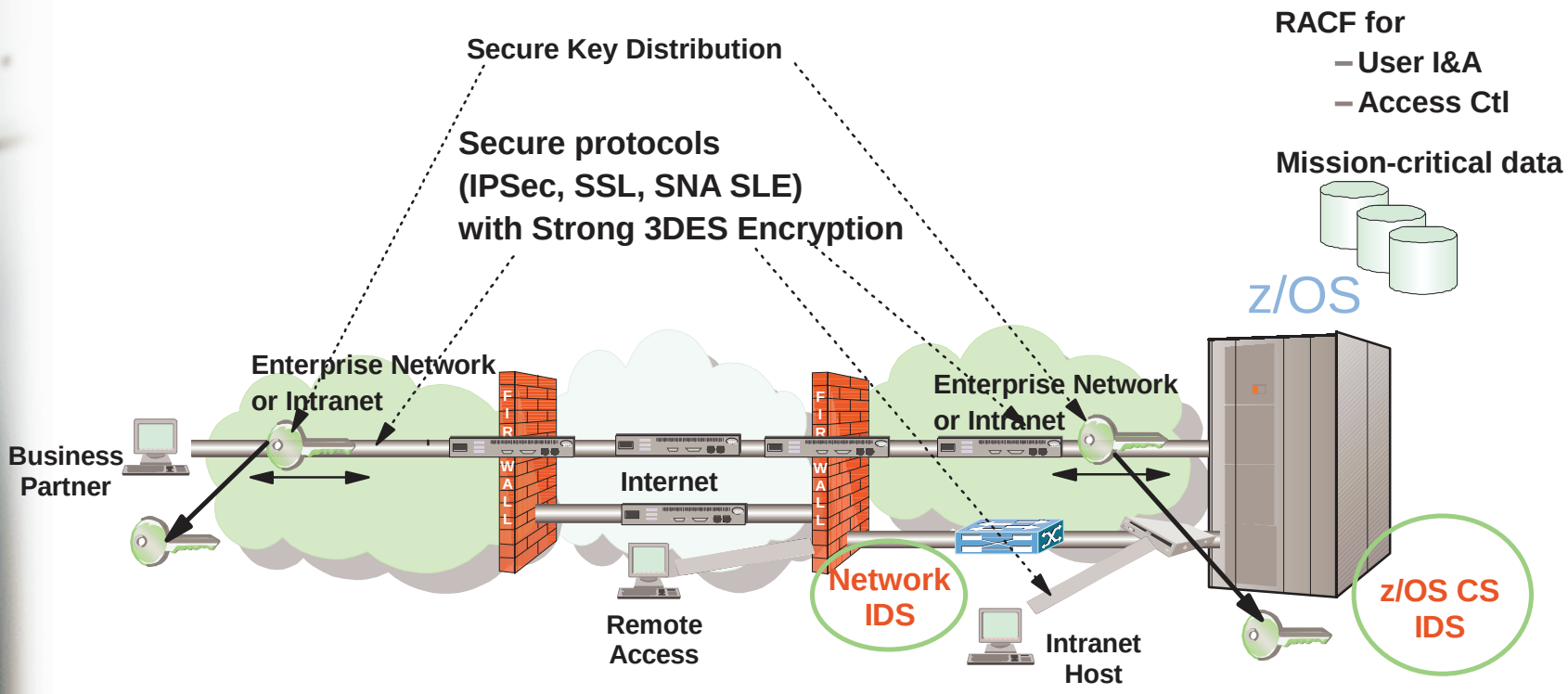
Intrusions can occur from Internet or intranet

- Firewall can provide some level of protection from Internet
- Perimeter Security Strategy *alone* may not be sufficient. Consider:
  - Access permitted from Internet
  - Trust of intranet
    - Users
    - Ability of servers to withstand being taken over
      - ✓ Amplifiers, Robots, zombies



Intrusion Detection Key Element of Secure Infrastructure

- Enterprise Servers must be resistant against security breach
  - Secure platform is prerequisite
- Secure network and application infrastructure should be built on this base
  - Intrusion detection is key element of providing secure infrastructure. Add to:
    - Existing security plans and procedures
    - Firewalls, network, application, and system security

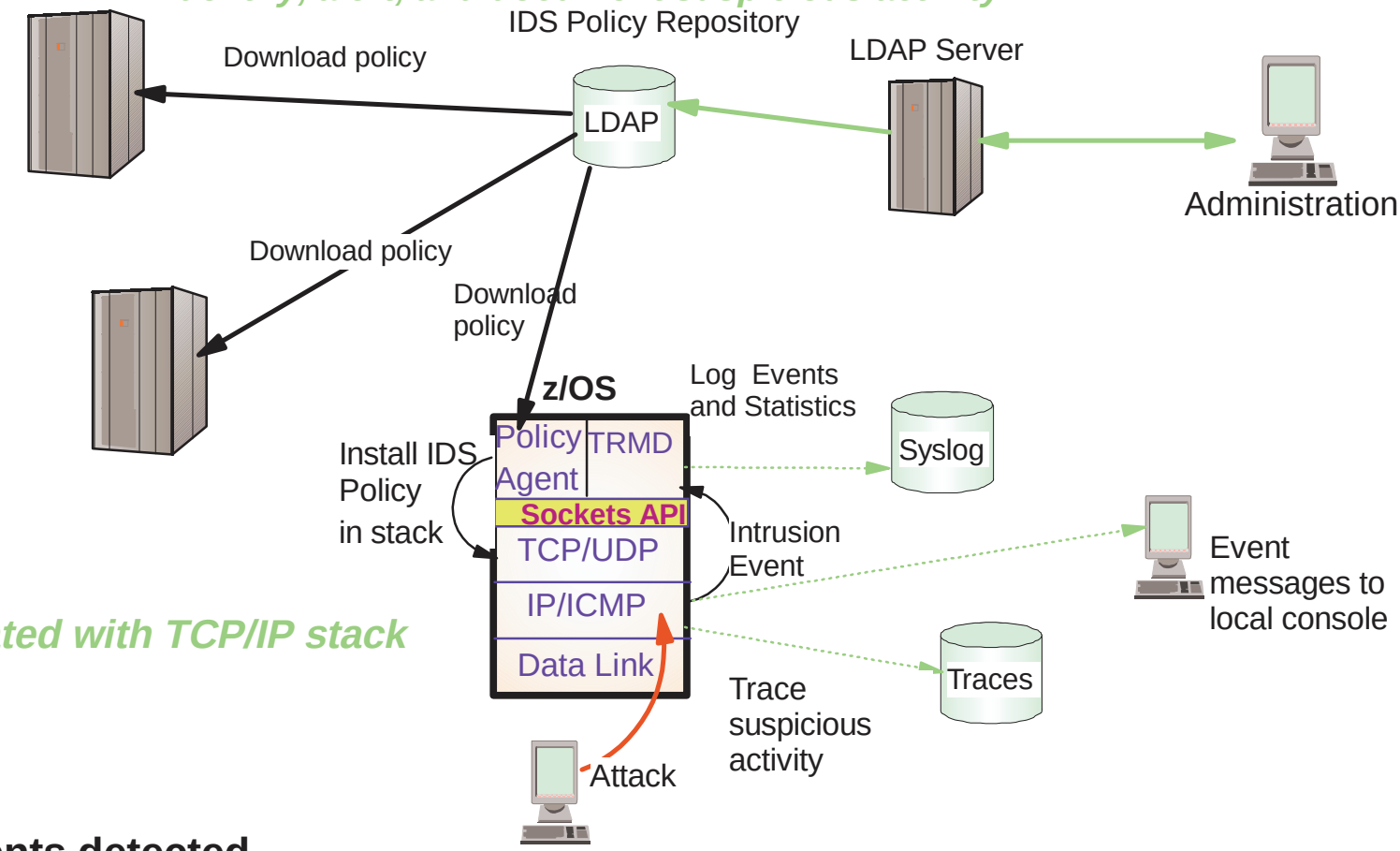


Integrated Intrusion Detection Services

- **z/OS IDS focus is self detection and protection**
  - **Identifies, alerts, and documents suspicious activity**
  - **Inline Real Time detection**
    - Detection logic part of target server system
- **Complements network-based intrusion detection system**
  - **Sniffers or Sensors evaluate packets Near Real Time**
    - Placement can be near firewalls or dedicated to specific host
    - Single *Known* packet attack oriented
    - Use signature file of known attacks for pattern matching
    - Cannot evaluate data encrypted end-to-end
  - **Vulnerability Scanners Not Real Time**
    - Examine system looking for vulnerabilities or evidence of intrusion
    - Analyze historical data, identify behavioral anomalies or intrusion patterns
- **z/OS IDS enables broader intrusion detection coverage**
  - **Ability to evaluate inbound IPSec data**
    - After decryption on the target system
  - **Avoids overhead of per packet evaluation against table of known attacks**
    - IDS policy checked after attack detected
  - **Detects statistical anomalies**
    - Target system has stateful data / internal threshholds unavailable to external IDSs
  - **Policy can control prevention methods on the target**
    - Connection limiting, packet discard

z/OS Intrusion Detection Services Overview

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



Integrated with TCP/IP stack

Events detected

- Scans, Attacks Against Stack, Flooding

Defensive methods

- Packet discard, limit connections

IDS Recording

- Event and statistics logging, event messages to local console, IDS packet trace

IDS Reporting

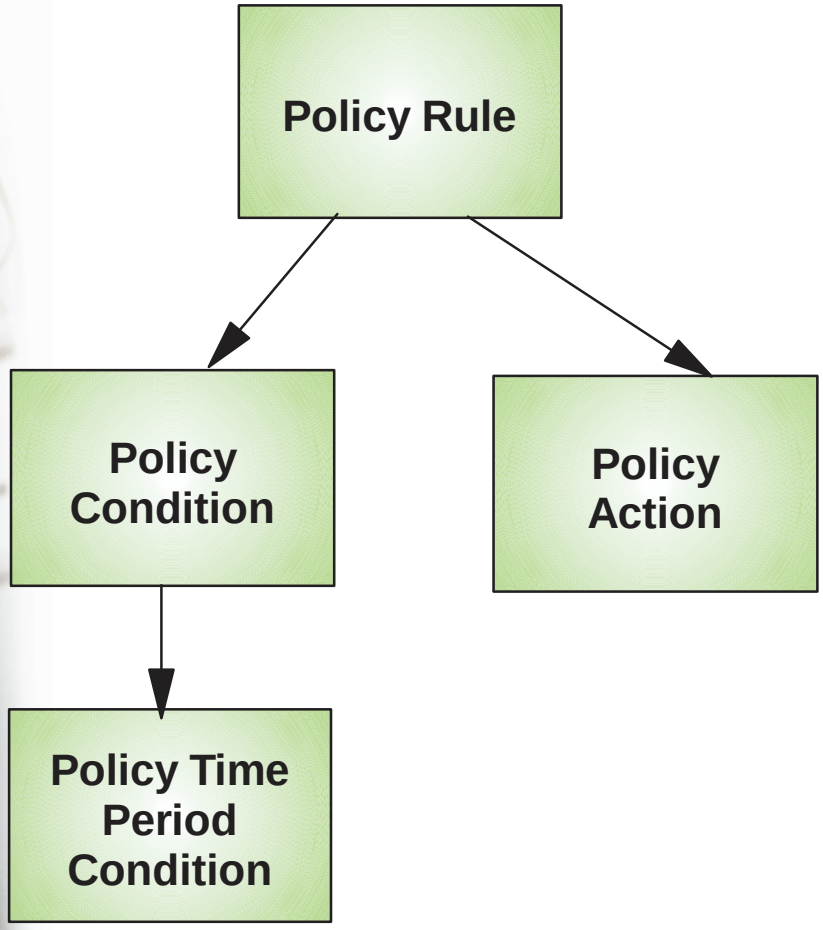
- trmdstat program for IDS reports

IDS Configuration

- IDS is configured with IDS policy
  - IDS policy defines intrusion events to monitor and actions to take
- Policy is stored in LDAP
  - Definition of elements of policy are known as schema
  - IDS schema used to define IDS policy
- Policy Agent read policy definitions from LDAP
  - Policy definitions are processed by Policy Agent and installed in the TCP/IP stack

Policy Model Overview

Basic Policy Objects



Policies consist of several related objects

- Policy Rule is main object and refers to one or more objects:
  - 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 Time Period Condition
    - Determines when a policy rule is active

Policy objects relationship:

IF condition THEN action

Intrusion Events Types Detected

- **SCAN**
- **ATTACK**
- **TRAFFIC REGULATION**
  - TCP
  - UDP

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 events types supported
  - ICMP scans
  - TCP port scans
  - UDP port scans

Scan Policy Overview

Scan policy provides the ability to:

- Obtain notification and documentation of scanning activity
  - Notify the installation of a detected scan via console message or syslogd message
  - Trace potential scan packets
- Control the parameters that define a scan:
  - The time interval
  - The threshold
- Reduce level of false positives
  - Exclude well known "legitimate scanners" via exclusion list
    - e.g. network management
  - Specify a scan sensitivity level
    - by port for UDP and TCP
    - highest priority rule for ICMP

Scan Event Counting and Scan Sensitivity

- Scan sensitivity determines whether a scan event is "countable"

Sensitivity (from policy)	Normal Event	Possibly Suspicious Event	Very Suspicious Event
Low			Count
Medium		Count	Count
High	Count	Count	Count

- Countable scan events count against an origin source IP address
  - Total number of countable events for all scan event types is compared to policy thresholds
    - If threshold exceeded for a single IP address, policy-directed notification and documentation is triggered
- Balance between detecting every scan and limit overhead
  - Reserve low ports not explicitly in use to allow configuration of low sensitivity on low ports for both UDP and TCP
- Scan instance event classification by event type included in appendix

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 intrusion events and supporting documentation.
- IDS adds controls to detect and disable uncommon or unused features which could be used in an attack.

Attack Categories

- Malformed packet events
  - Detects packets with incorrect or partial header information
- Inbound fragment restrictions
  - Detects fragmentation in first 256 bytes of a datagram
- IP protocol restrictions
  - Detects use of IP protocols you are not using that could be misused
- IP option restrictions
  - Detects use of IP options you are not using that could be misused
- UDP perpetual echo
  - Detects traffic between UDP applications that unconditionally respond to every datagram received
- ICMP redirect restrictions
  - Detects receipt of ICMP redirect to modify routing tables.
- Outbound RAW socket restrictions
  - Detects z/OS RAW socket application crafting invalid outbound packets
- TCP SYNflood Flood Events
  - Detects flood of SYN packets from "spoofed" sources

Attack Policy Overview

Attack policy provides the ability to:

- Control attack detection for one or more attack categories independently
- Obtain notification and documentation of attacks
  - Notify the installation of a detected attack via console message or syslogd message
  - Trace potential attack packets
- Allows request for attack statistics on time interval basis
  - Normal or Exception
- Control defensive action when attack is detected

Traffic Regulation

- Traffic Regulation for TCP available in OS/390 V2R10
- Extended and made part of IDS for z/OS V1R2
  - Added additional controls for TCP
  - New function for UDP
- Policy should be defined in LDAP for new z/OS V1R2 functionality
  - OS/390 V2R10 TR definitions for TCP configured in flat file
  - Existing flat file definintions still supported for compatability

Traffic Regulation for TCP

- Allows control over number of inbound connections from a single host
  - Can be specified for specific application ports
    - Especially for forking applications
  - Independent policies for multiple applications on the same port
    - e.g. telnetd and TN3270
      - ✓ New for z/OS V1R2
- Connection limit expressed as
  - Port limit for all connecting hosts
  - Individual limit for a single 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)

Traffic Regulation for UDP

- Allows control over length of inbound receive queues for UDP applications
  - Can be specified for specific application ports
- 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 consistently receive data at higher rates than can be processed
  - LONG
  - VERY LONG
    - Useful for fast applications with bursty arrival rates

IDS Actions

- **Defensive actions**
- **Recording actions**

Defensive Actions

Defensive actions available by event type:

- Scan Events
  - No defensive action defined
- Attack Events
  - Packet discard
    - Certain attack events always result in packet discard and are <u>not</u> controlled by IDS policy action
      - ✓ malformed packets
      - ✓ synflood
    - Some attack types controlled by IDS policy action
      - ✓ ICMP option restrictions
      - ✓ ICMP redirect restrictions
      - ✓ IP protocol restrictions
      - ✓ IP fragment
      - ✓ outbound raw restrictions
      - ✓ perpetual echo
- Traffic Regulation Events
  - Controlled by IDS policy action
    - TCP - Connection limiting
    - UDP - Packet discard

Recording Actions

- Recording options controlled by IDS policy action specification
  - Recording suppression provided if quantity of IDS console messages reach policy-specified thresholds
- Options
  - Event logging
    - Syslogd
      - ✓ Number of events per attack subtype recorded in a five minute interval is limited
    - Local Console
  - Statistics
    - Syslogd
      - ✓ Normal, Exception
  - IDS packet trace
    - Activated after attack detected
      - ✓ Number of packets traced for multi-packet events are limited
      - ✓ Amount of data trace is configurable (header, full, byte count)
- All IDS events recorded in syslog and console messages, and packet trace records have probeid and correlator
  - Probeid identifies the specific event detected
  - Correlator allows events to be matched with corresponding packet trace records

z/OS Communications Server Security

Intrusion Detection Reports for Analysis

IDS Log Reports

trmdstat program produces reports based on IDS data recorded to syslog

- Types of reports generated for logged events
  - Overall summary reports
    - Connection and IDS
  - Event type summary reports
    - For Connection, Attack, Flood, Scan, TCP and UDP information
  - Event type detail reports
    - For Connection, Attack, Flood, Scan, TCP and UDP information
- Types of reports generated for statistics events
  - Details reports
    - Attack, TCP, and UDP reports
- Report examples in appendix

Using IDS Console Messages for Automation

- Console message can drive message automation
  - MPF message suppression can suppress message output to system console
- Example automation actions:
  - Route message to NetView console(s)
  - email notification to security administrator
  - Run trmdstat and attach output to email
- Selectors
  - Automate based on message number, other message content
    - e.g. event type, probeid

Message is multi-line WTO:

- **Always written**
  - **EZZ8761I IDS EVENT DETECTED** *nnn*
  - **EZZ8762I EVENT TYPE:** *eventtype*
  - **EZZ8763I CORRELATOR** *cccccc* **- PROBEID** *iiiiiiii*
- **Written if source IP address or port is present**
  - **EZZ8764I SOURCE IP ADDRESS** *sss.sss.sss.sss* **- PORT** *ppppp*
- **Written if destination IP address or port is present**
  - **EZZ8765I DESTINATION IP ADDRESS** *ddd.ddd.ddd.ddd* **- PORT** *ppppp*
- **Always written**
  - **EZZ8766I IDS RULE** *rulename*
  - **EZZ8767I IDS ACTION** *actionname*

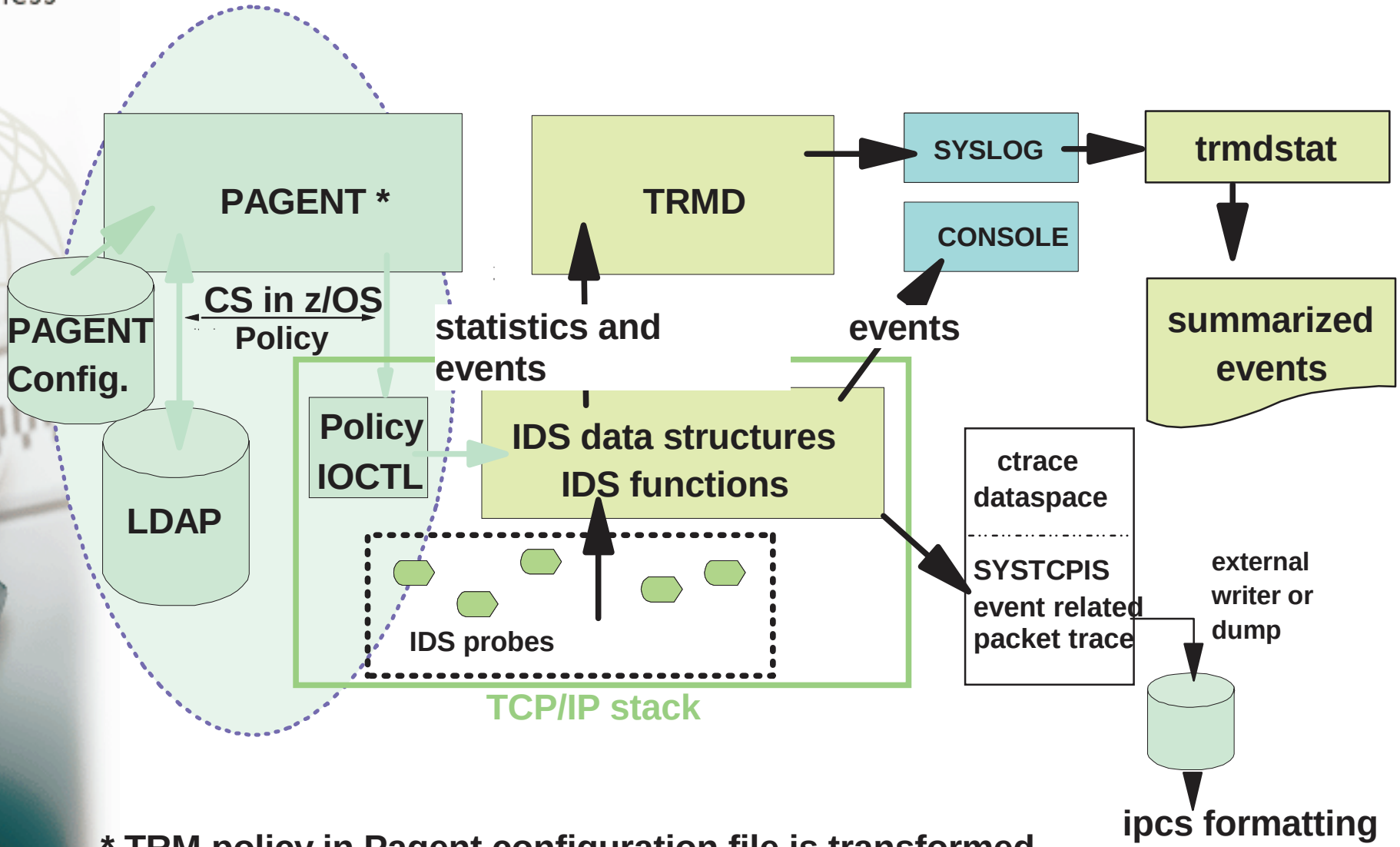
NetView clists: http://www.tivoli.com/support/downloads/netview_390/tools/idsauto.html

z/OS Communications Server Security

Working with IDS Policy

- **Defining IDS Policy**
- **IDS Policy Scenarios**
- **Controlling, Displaying, and Validating Policy**

Intrusion Detection Services Structure



* TRM policy in Pagent configuration file is transformed into IDS TR TCP policy by Pagent.

Defining IDS Policy

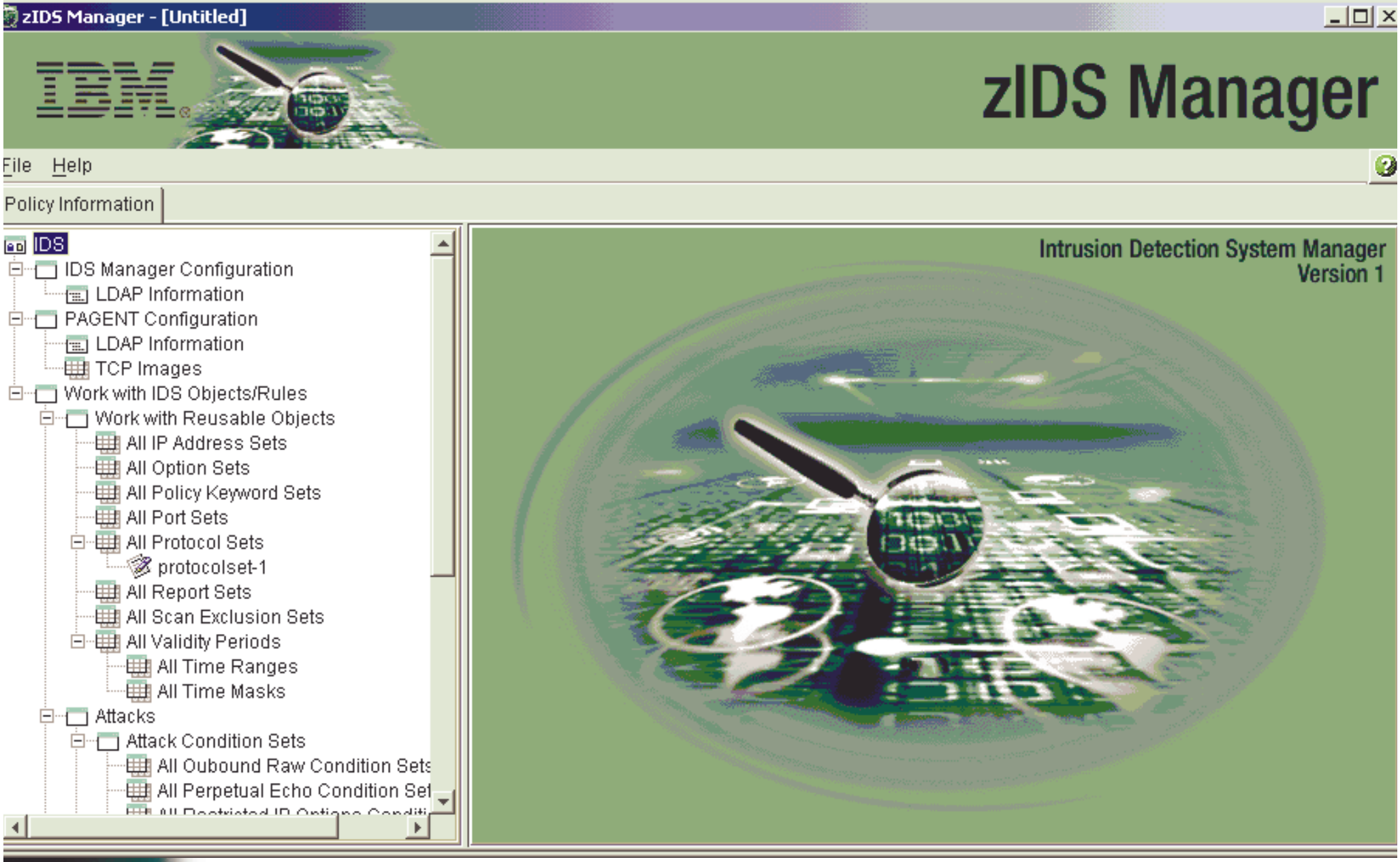
Policy Object examples with
beie.a.aace.
eiitios.
slpptcpipsamples.

- pagent_starter_IDS.ldif
- pagent_advanced_IDS.ldif

1. Start with the samples
2. Consult the associated INFO APARS (II12498, II12499) to understand how to change the samples to fit your LDAP environment.
3. Consult the IP Configuration Guide and the IP Configuration Reference to understand and evaluate additional capabilities
4. Learn LDAP V3 Policy Schema syntax as needed

zIDSManager "as is" Web Tool: Coming Soon! to implement LDAP policies.
Will be available at:
http://www-3.ibm.com/software/network/commserver/downloads

zIDS Manager



Scan Global Policy Example

```
Condition
  ibm-idsConditionType:SCAN_GLOBAL

Action
  ibm-idsActionType:SCAN_GLOBAL
  ibm-idsFSInterval:2
  ibm-idsFSThreshold:5
  ibm-idsSSInterval:480
  ibm-idsSSThreshold:10
  ibm-idsNotification:SYSLOGDETAIL
  ibm-idsTraceData:RECORDSIZE
  ibm-idsTraceRecordSize:200
```

Scan Event Policy Example

rule 1

- **Condition**
  - ibm-conditionType:*SCAN_EVENT*
  - ibm-idsProtocolRange:*6*
  - ibm-idsLocalPortRange:*1-1023*
- **OR**
- **Condition**
  - ibm-conditionType:*SCAN_EVENT*
  - ibm-idsProtocolRange:17
  - ibm-idsLocalPortRange:*1-1023*

- **Action**
  - ibm-idsActionType:*SCAN_EVENT*
  - ibm-idsSensitivity:***LOW***
  - ibm-idsScanExclusion:*scan_exclusion*

rule 2

Condition

ibm-conditionType:*SCAN_EVENT*
ibm-idsProtocolRange:1

- **Action**
  - ibm-idsActionType:*SCAN_EVENT*
  - ibm-idsSensitivity:***MEDIUM***
  - ibm-idsScanExclusion:*scan_exclusion*

Attack Policy Example Conditions

ibm-ids<u>ConditionType</u>:*ATTACK*

ibm-ids<u>AttackType</u>:*MALFORMED*

ibm-ids<u>AttackType</u>:*IP_FRAGMENT*

ibm-ids<u>AttackType</u>:*RESTRICTED_IP_PROTOCOL*
ibm-idsIPProtocolRange:*xx*

ibm-ids<u>AttackType</u>:*RESTRICTED_IP_OPTIONS*
ibm-idsIPOptionRange:yy

Attack Policy Scenarios (cont'd.) Conditions

ibm-ids<u>AttackType</u>:*OUTBOUND_RAW*
ibm-idsProtocolRange:*xx*

ibm-ids<u>AttackType</u>:*PERPETUAL_ECHO*
ibm-idsLocalPortRange:*aa*
ibm-idsRemotePortRange:*bb*

ibm-ids<u>AttackType</u>:*ICMP_REDIRECT*

ibm-ids<u>AttackType</u>:*FLOOD*

Attack Policy Example
Actions

One or more "ibm-idsTypeActions" may be specified....

ibm-idsActionType:*ATTACK*

To request statistics about attacks :

ibm-idsTypeActions:*EXCEPTSTATS*
ibm-idsTypeActions:*STATISTICS*
ibm-idsStatInterval*:n*

To request that a packet be discarded when it is detected as an attack :
ibm-idsTypeActions:*LIMIT*

Attack Policy Example (cont'd.)
Actions

To request that a message be logged when an attack is detected:

ibm-idsTypeActions:*LOG*

ibm-idsNotification:*CONSOLE*

ibm-idsNotification:*SYSLOG*

ibm-idsLoggingLevel:*n*

ibm-idsMaxEventMessage:*n*

To request that a packet be traced when an attack is detected :

ibm-idsTraceData:*HEADER*

ibm-idsTraceData:*RECORDSIZE*

ibm-idsTraceRecordSize:*xx*

ibm-idsTraceData:*FULL*

ibm-idsTraceData:*NONE*

TR TCP Policy Example

Condition

ibm-idsConditionType:*condition_type*
ibm-idsProtocolRange:*protocol_range*
ibm-idsLocalPortRange:*local_port_range*

Action

ibm-idsActionType:*action_type*
ibm-idsNotification:*notification*
ibm-idsLoggingLevel:*logging_level*
ibm-idsTypeActions:*type_actions*
ibm-idsStatInterval:*stat_interval*
ibm-idsTRtcpTotalConnections:*total_connections*
ibm-idsTRtcpPercentage:*percentage*
ibm-idsTRtcpLimitScope:*limit_scope*

TR UDP Policy Example

Condition

ibm-idsConditionType:*condition_type*
ibm-idsProtocolRange:*protocol_range*
ibm-idsLocalPortRange:*local_port_range*

Action

ibm-idsActionType:*action_type*
ibm-idsNotification:*notification*
ibm-idsLoggingLevel:*logging_level*
ibm-idsTypeActions:*type_actions*
ibm-idsStatInterval:*stat_interval*
ibm-idsTRudpQueueSize:*queue_size*

Controlling Active IDS Policy

Delete & Reload Policy

- TcpImage .. FLUSH | NOFLUSH {PURGE | NOPURGE} 1800
- FLUSH and NOFLUSH take effect at Policy Agent initialization and will delete or not delete the policies already installed in the stack.
- PURGE and NOPURGE indicate whether the policies should or should not be purged/deleted from the stack at PAGENT termination.
  - PURGE specifies that policies should be deleted from this stack when the Policy Agent shuts down
  - NOPURGE specifies that policies should not be deleted from this stack when the Policy Agent shuts down (default)

Refresh Policy

- At Interval (1800-second default)
- With MODIFY PAGENT command (REFRESH option)
- With SIGHUP UNIX command
- When Policy Agent configuration file (HFS only) is updated (refresh is automatic)

Display Netstat IDS

- NETSTAT IDS command supported from operator console, TSO and OE (-k).

```
netstat ids summary   (from tso)
netstat -k summary    (from OE)
```

Options: `Summary`

`Protocol (TCP or UDP)`

- RACF resource (EZB.NETSTAT.mvsname.tcpprocname.IDS) can be used to restrict access to command.

Netstat IDS Summary Example

```
onetstat -k SUM
MVS TCP/IP onetstat CS V1R2        TCPIP Name: TCPCS
Intrusion Detection Services Summary:
Scan Detection:
  GlobRuleName: ScanGlobal-rule
  IcmpRuleName: ScanEventMedium-rule
  TotDetected:  0            DetCurrPlc: 0
  DetCurrInt:   0            Interval:   60
  SrcIPsTrkd:   1            StrgLev:    00000M
Attack Detection:
  Malformed Packets
    PlcRuleName: AttackMalformed-rule
    TotDetected: 0            DetCurrPlc: 0
    DetCurrInt:  0            Interval:   60
  OutBound RAW Restrictions
    PlcRuleName: AttackOutboundRaw-rule
    TotDetected: 1200         DetCurrPlc: 1200
    DetCurrInt:  1200         Interval:   60
    ...
Traffic Regulation:
  TCP
    ConnRejected: 0            PlcActive: N
  UDP
    PckDiscarded: 0            PlcActive: N
```

Validating IDS Policy

1. Inspect the IDS policy for correctness
2. Verify LDAP accepts the IDS policy
3. Invoke PAGENT and TRMD
4. Issue PASEARCH
   a. Verify the correct policy is installed
5. Keep policy in force for a trial period
6. Issue IDS netstat to view active IDS policy and statistics
7. Verify syslog messages document intrusions
   a. Display syslog
   b. Run TRMDSTAT reports
8. Adjust the policy as required
   a. Remember V1R2 MODIFY command to reload altered policies or PAGENT 'tcpimage ... PURGE' option to delete policies from TCP stack.

z/OS Communications Server Security

Features Summary

IDS Features Summary

IDS events detected include:

- Scan detection
  - TCP port scans
  - UDP port scans
  - ICMP scans
    - ✓ Sensitivity levels for all scans can be adjusted to control number of false positives recorded.
- Attack detection
  - Malformed packet events
  - Outbound raw restrictions
  - Inbound fragment restrictions
  - IP option restrictions
  - IP protocol restrictions
  - ICMP restrictions
  - SYNflood events
  - UDP perpetual echo
- Traffic Regulation (Flood detection and prevention)
  - UDP backlog management by port
    - ✓ Packets discard
  - TCP total connection and source percentage management by port (R10)
    - ✓ Connection limiting

IDS Recording Options

- Event logging
  - syslogd, local console
- Statistics
  - syslogd
    - ✓ normal, exception
- IDS packet trace after attack detected for offline analysis
  - Number of packets traced for multi-packet events are limited

Reports

- trmdstat produces reports from IDS syslogd records
  - Summary and detailed

z/OS Communications Server Security

Appendix A

- **Scan Probe Instance Event Classifications**

ICMP Scan Probe Instance Classification

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

UDP Scan Probe Instance Classification

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

TCP Scan Probe Instance Classification

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

z/OS Communications Server Security

Appendix B

- **Report Summary Examples**

Summary Report: trmdstat

```
trmdstat /tmp/dablog.log
trmdstat for z/OS CS V1R2          Wed Jan 31 15:43:59 2001

Log Time Interval     : Jan  9 12:16:26  - Jan  9 12:20:54
Stack Time Interval   : Jan  9 16:10:40  - Jan  9 17:20:36
TRM Records Scanned   : 3307
Port Range            : ALL


Traffic Regulation - TCP
-----------------------------------------------
Connections would have been refused :          0
Connections refused                 :          0

Constrained entry logged            :          0
Constrained exit logged             :          0
Constrained entry                   :          1
Constrained exit                    :          1

QOS exceptions logged               :          0
QOS exceptions made                 :          0

TRMD Started                  : Jan  9 10:53:42
TRMD Ended                    : Jan  9 11:05:14
TRMD Started                  : Jan  9 12:16:22
```

IDS Summary Report: trmdstat - I

```
trmdstat -I /tmp/dablog.log
trmdstat for z/OS CS V1R2          Wed Jan 31 15:51:45 2001

Log Time Interval     : Jan  9 12:16:24  - Jan  9 12:20:54
Stack Time Interval   : Jan  9 16:09:06  - Jan  9 17:20:36
TRM Records Scanned   : 3307
Port Range            : ALL


Traffic Regulation - TCP
------------------------------------------------
Connections would have been refused :          0
Connections refused                 :          0

Constrained entry logged            :          0
Constrained exit logged             :          0
Constrained entry                   :          1
Constrained exit                    :          1

QOS exceptions logged               :          0
QOS exceptions made                 :          0

Traffic Regulation - UDP
------------------------------------------------
Constrained entry logged            :          0
Constrained exit logged             :          0
Constrained entry                   :          0
Constrained exit                    :          0
```

IDS Summary Report: trmdstat - I (*continued*)

```
SCAN Detection
-----------------------------------------------
Threshold exceeded                    :          0
Detection delayed                     :          0
Storage constrained entry             :          0
Storage constrained exit              :          0

ATTACK Detection
-----------------------------------------------
Packet would have been discarded      :          0
Packet discarded                      :        593
Accept queue expanded                 :          0

FLOOD Detection
-----------------------------------------------
SYN flood start                       :          0
SYN flood end                         :          0

440 ATTACK messages lost at 01/09/2001
16:08:26.49

TRMD Started                     : Jan  9 10:53:42
TRMD Ended                       : Jan  9 11:05:14
TRMD Started                     : Jan  9 12:16:22
```

Scan Summary Report: trmdstat - N

Displays the summary of scan events.

```
trmdstat -N /tmp/tstlog.log
trmdstat for Z/OS CS V1R2          Wed Nov  8 09:06:56 2000

Log Time Interval     : Aug 21 08:32:09  - Aug 21 10:32:09
Stack Time Interval   : Aug 21 14:32:09  - Aug 21 14:32:09
TRM Records Scanned   : 71
Port Range            : ALL

                         SCAN TR Summary

     IP Address            Scans                  Suspicion Level
                     Fast       Slow       Very     Possibly    Normal
   --------------- ---------- ---------- ---------- ---------- ----------
   11.12.13.14            2          2         20         20         20
   22.33.44.55            2          0        200        400        600


TRMD Started                  : Aug 21 10:32:09
```

Scan Detail Report: trmdstat - N - D

Display the contents of individual scan event records.

```
trmdstat -N -D /tmp/tstlog.log
trmdstat for Z/OS CS V1R2          Wed Nov  8 09:08:54 2000

Log Time Interval     : Aug 21 08:32:09  - Aug 21 10:32:09
Stack Time Interval   : Aug 21 14:32:09  - Aug 21 14:32:09
TRM Records Scanned   : 71
Port Range            : ALL

                                SCAN TR Events

    Date and Time        IP Address            Suspicion Level          Type Correlator
                                          Very     Possibly   Normal
---------------------- --------------- ---------- ---------- ---------- --- ----------
8/21/2000 14:32:9.53   11.12.13.14             5          5          5  S       47113
8/21/2000 14:32:9.53   11.12.13.14             5          5          5  S       47212
8/21/2000 14:32:9.53   11.12.13.14             5          5          5  F       57287
8/21/2000 14:32:9.53   11.12.13.14             5          5          5  F       67333
8/21/2000 14:32:9.54   22.33.44.55           100        200        300  F       87433
8/21/2000 14:32:9.54   22.33.44.55           100        200        300  F       97500

TRMD Started                  : Aug 21 10:32:09
```

Attack Summary Report: trmdstat -A

Displays the summary of all attack events.

```
trmdstat -A /tmp/tstlog.log
trmdstat for Z/OS CS V1R2          Wed Nov  8 10:14:11 2000

Log Time Interval     : Aug 21 08:32:09  - Aug 21 10:32:09
Stack Time Interval   : Aug 21 14:32:09  - Aug 21 14:32:09
TRM Records Scanned   : 71
Port Range            : ALL

                                          ATTACK Summary
                                        Datagrams Discarded
Source: 31.32.33.34      Destination: 51.52.53.54
                                         Attacks
  Dst Port   Malf       ORaw       IPFr       ICMP       IPop       Prto       Perp       NoId
   ------ ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
    13001          1          0          0          0          0          0          0          0
    14001          0          0          0          0          0          0          1          0

                                        Datagrams would have been Discarded
Source: 61.62.63.64      Destination: 31.32.33.34
                                         Attacks
  Dst Port   Malf       ORaw       IPFr       ICMP       IPop       Prto       Perp       NoId
   ------ ---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
    12001          0          2          0          0          0          0          0          0

TRMD Started                  : Aug 21 10:32:09
```

Attack Detail Report: trmdstat -A -D

Displays the contents of attack event records.

```
trmdstat -A -D /tmp/trmlog.log
trmdstat for Z/OS CS V1R2          Wed Nov  8 09:55:36 2000

Log Time Interval     : Aug 21 08:32:09  - Aug 21 10:32:09
Stack Time Interval   : Aug 21 14:32:09  - Aug 21 14:32:09
TRM Records Scanned   : 71
Port Range            : ALL

                                ATTACK Events


Pckets Discarded
Attack      Date and Time       Dst IpAddr      Src IpAddr      Dst Port Src Port Correlator ProbeID
------ ---------------------- --------------- --------------- -------- -------- ---------- --------
 Malf  8/21/2000 14:32:9.53   51.52.53.54     41.42.43.44          0        0       82334 04010009
 IPFr  8/21/2000 14:32:9.53   51.52.53.54     41.42.43.44          0        0       82336 04030001
 IPOP  8/21/2000 14:32:9.53   51.52.53.54     41.42.43.44          0        0       82338 04050001
 PRTO  8/21/2000 14:32:9.53   51.52.53.54     41.42.43.44          0        0       82339 04060001
 Perp  8/21/2000 14:32:9.53   51.52.53.54     41.42.43.44      13001    10001       82342 04080001
 ICMP  8/21/2000 14:32:9.53   51.52.53.54     41.42.43.44      12001    10001       82337 04040009
                            Packets would have been Discarded
Attack      Date and Time       Dst IpAddr      Src IpAddr      Dst Port Src Port Correlator ProbeID
------ ---------------------- --------------- --------------- -------- -------- ---------- --------
 ORAW  8/21/2000 14:32:9.54   41.42.43.44     71.72.73.74          0        0       87999 04020001
 TRMD Started                 : Aug 21 10:32:09
```

Attack Statistics Report: trmdstat -A -S

Displays the contents of attack statistics records (including Flood statistics).

```
trmdstat -A -S /tmp/statlog.log
trmdstat for Z/OS CS V1R2          Tue Jan 16 13:13:30 2001

Log Time Interval     : Jan  9 10:54:15  - Jan  9 10:54:16
Stack Time Interval   : Jan  9 15:42:53  - Jan  9 15:45:58
TRM Records Scanned   : 27
Port Range            : ALL

                        ATTACK Statistics

Attack            Date and Time                Attacks          Action
------          ----------------------        ----------        -------
 Malf           01/09/2001 15:42:53.20            11111          LIMIT
 IPFr           01/09/2001 15:42:53.20            22222          LIMIT
 ORAW           01/09/2001 15:43:54.84            33333          LIMIT
 PRTO           01/09/2001 15:43:54.84            44444          LIMIT
 ICMP           01/09/2001 15:44:56.52            55555          LIMIT
 IPOP           01/09/2001 15:44:56.52            66666          NOLIMIT
 Perp           01/09/2001 15:45:58.17            77777          NOLIMIT
 Flod           01/09/2001 15:45:58.18            88888          LIMIT


TRMD Started                  : Jan  9 10:53:42
```

Flood Summary Report: trmdstat -F

Displays the summary of all flood events.

```
trmdstat -F /tmp/tstlog.log
trmdstat for Z/OS CS V1R2          Wed Nov  8 09:59:32 2000

Log Time Interval     : Aug 21 08:32:09  - Aug 21 10:32:09
Stack Time Interval   : Aug 21 14:31:09  - Aug 21 14:32:09
TRM Records Scanned   : 71
Port Range            : ALL

                        FLOOD Summary

     IP Address        Port   SYN Flood   SYN Flood   SYN Flood
                              Start        End        Duration
   ---------------    ------  ----------  ----------  ----------
   11.12.13.14        11000          2           2          80
   61.62.63.64        12000          2           2         120
   61.62.63.64        14000          1           1         120


TRMD Started                  : Aug 21 10:32:09
```

Flood Detail Report: trmdstat -F -D

Display the contents of flood event records.

```
trmdstat -F -D /tmp/tstlog.log
trmdstat for Z/OS CS V1R2          Wed Nov  8 10:00:37 2000

Log Time Interval     : Aug 21 08:32:09  - Aug 21 10:32:09
Stack Time Interval   : Aug 21 14:31:09  - Aug 21 14:32:09
TRM Records Scanned   : 71
Port Range            : ALL

                                FLOOD Events

   Date and Time        IP Address      Port  Type   Duration   Correlator
---------------------- --------------- ------  ---  ----------  ----------
8/21/2000 14:31:9.53   11.12.13.14      11000   E                   87591
8/21/2000 14:31:9.53   11.12.13.14      11000   E                   87704
8/21/2000 14:32:9.53   11.12.13.14      11000   X           40      87893
8/21/2000 14:32:9.53   11.12.13.14      11000   X           40      87997
8/21/2000 14:32:9.53   61.62.63.64      12000   X           60      87999

TRMD Started                  : Aug 21 10:32:09
```

TR TCP Summary Report: trmdstat -T

Displays the summary of TCP constrained state and datagram discard information.

```
trmdstat -T /tmp/tstlog.log
trmdstat for Z/OS CS V1R2          Wed Nov  8 10:42:41 2000

Log Time Interval     : Aug 21 09:32:09  - Aug 21 12:32:09
Stack Time Interval   : Aug 21 09:32:09  - Aug 21 12:32:09
TRM Records Scanned   : 71
Port Range            : ALL

                              TCP TR Summary


Local Host: 00.01.02.03      Host: 10.11.12.13
                Constrained States                      Connections
 Port                Limited                  Excp          Refused
           Enter      Exit     Duration     QOS        Appl       Host
------ ---------- ---------- ---------- ---------- ---------- ----------
  7001          0          0          0          1          0          0

Local Host: 20.21.22.23      Host: 11.12.13.14
                Constrained States                      Connections
 Port                Logged                   Excp   Would have been Refused
           Enter      Exit     Duration     QOS        Appl       Host
------ ---------- ---------- ---------- ---------- ---------- ----------
  2001          1          1        100          0          0          0
  9001          0          0          0          0          1          1

TRMD Started                 : Aug 21 10:32:09
```

TR TCP Extended Summary Report: trmdstat -T -E

Displays the extended summary of TCP constrained state and datagram discard information.

```
trmdstat -T -E /tmp/tstlog.log
trmdstat for Z/OS CS V1R2          Wed Dec 20 17:02:50 2000

Log Time Interval     : Aug 21 08:32:09  - Aug 21 08:32:09
Stack Time Interval   : Aug 21 09:32:09  - Aug 21 12:32:09
TRM Records Scanned   : 70
Port Range            : ALL

                                TCP Extended TR Summary


Local Host: 00.01.02.03      Host: ALL
                             Constrained States                    Connections
 Port       Host                  Limited                  Excp         Refused
                         Enter      Exit     Duration     QOS        Appl       Host
------ --------------- ---------- ---------- ---------- ---------- ---------- ----------
  3001 11.12.13.14             1          1        100          0          0          0
  7001 10.11.12.13             0          0          0          1          0          0
  8001 11.12.13.14             0          0          0          0          1          0

Local Host: 20.21.22.23      Host: ALL
                             Constrained States                    Connections
 Port       Host                  Logged                   Excp  Would have been Refused
                         Enter      Exit     Duration     QOS        Appl       Host
------ --------------- ---------- ---------- ---------- ---------- ---------- ----------
  2001 11.12.13.14             1          1        100          0          0          0
  7001 10.11.12.13             0          0          0          1          0          0
  9001 11.12.13.14             0          0          0          0          1          1

TRMD Ended                   : Aug 21 08:32:09
```

TR TCP Detail Report: trmdstat -T -D

Displays the contents of individual TCP TR records.

```
trmdstat -T -D /tmp/tstlog.log
trmdstat for Z/OS CS V1R2          Wed Nov  8 10:45:08 2000

Log Time Interval     : Aug 21 09:32:09  - Aug 21 12:32:09
Stack Time Interval   : Aug 21 09:32:09  - Aug 21 12:32:09
TRM Records Scanned   : 71
Port Range            : ALL


                                          TCP TR Events

                                          Events Limited
Local Host: 00.01.02.03      Source Host: ALL
    Date and Time        Port    Source Host   Rec Cns     Connections                Policy           Correlator ProbeID
                                               Typ Typ  Current   Available  Total Conn Pct Qos Limit
   ---------------      ------ --------------- --- --- ---------- ---------- ---------- --- ---------- ---------- --------
8/21/2000 10:32:9.53     1001 11.12.13.14      C             411        500       1000  25          0       8333 01004042
8/21/2000 10:32:9.53     2001 21.22.23.24      C             411        500       1000  25          0       8333 01004042
8/21/2000 10:32:9.53     2001 22.23.24.25      C             411        500       1000  25          0       8333 01004042
8/21/2000 10:32:9.53     3001 31.32.33.34      C             411        500       1000  25          0       8333 01004042
8/21/2000 10:32:9.53     3001 31.32.33.34      C             411        500       1000  25          0       8333 01004042

                                            Events  Logged
Local Host: 00.01.02.03      Source Host: ALL
    Date and Time        Port    Source Host   Rec Cns     Connections                Policy           Correlator ProbeID
                                               Typ Typ  Current   Available  Total Conn Pct Qos Limit
   ---------------      ------ --------------- --- --- ---------- ---------- ---------- --- ---------- ---------- --------
8/21/2000 10:32:9.54     1001 11.12.13.14      C             222        500       1000  25          0       9333 01004042

 TRMD Started                 : Aug 21 10:32:09
```

TR TCP Statistics Report: trmdstat -T -S

Display the contents of individual TCP TR statistics records.

```
trmdstat for z/OS CS V1R2          Thu Jan 18 16:28:59 2001

Log Time Interval     : Jan  9 10:54:15  - Jan  9 10:54:15
Stack Time Interval   : Jan  9 15:42:53  - Jan  9 15:42:53
TRM Records Scanned   : 27
Port Range            : ALL

                                        TCP TR Statistics

Local Host: 127.0.0.1        Peak Host: ALL
    Date and Time       Port        Action          Peak     Requests   Warnings  QosExcepts Terminates
                                  Peak Host      HostPeak   Current    Duration   SugLimit  SugPercent
--------------------- ------   --------------- ---------- ---------- ---------- ---------- ----------
01/09/2001 15:42:53.20   8054       NOLIMIT              1          1       1111        111          1
                              112.122.132.142           1        111      11111         10         11

01/09/2001 15:42:53.20   8055       LIMIT                2          2       2222        222          2
                              2.2.2.2                   2        222      22222         20         22

01/09/2001 15:42:53.20   8056       LIMIT                3          3       3333        333          3
                              3.3.3.3                   3        333      33333         30         33
TRMD Started                 : Jan  9 10:53:42
TRMD Ended                   : Jan  9 11:05:14
```

TR UDP Summary Report: trmdstat -U

Displays the summary of UDP constrained state and datagram discard information.

```
trmdstat -U /tmp/tstlog.log
trmdstat for Z/OS CS V1R2          Wed Nov  8 09:00:20 2000

Log Time Interval     : Aug 21 08:32:09  - Aug 21 10:32:09
Stack Time Interval   : Aug 21 14:32:09  - Aug 21 16:33:09
TRM Records Scanned   : 71
Port Range            : ALL

                              UDP TR Summary

                                  Constrained State          Datagrams
   IP Address       Port    Entered      Exited    Duration   Discarded
----------------- ------ ---------- ---------- ---------- ----------
 05.16.17.18        2001          1          1        100        155
 05.16.17.18        5001          2          2        200        310


                                  Constrained State          Datagrams
   IP Address       Port    Entered      Exited    Duration     Would
                                                                have been
                                                                Discarded
----------------- ------ ---------- ---------- ---------- ----------
 05.16.17.18        1001          1          1        100        155
 05.16.17.18        2001          2          2        200        310


TRMD Started                   : Aug 21 10:32:09
```

TR UDP Detail Report: trmdstat -U -D

Displays the contents of individual UDP records.

```
trmdstat -U -D /tmp/tstlog.log
trmdstat for Z/OS OS V1R2          Wed Nov  8 09:03:34 2000

Log Time Interval     : Aug 21 08:32:09  - Aug 21 10:32:09
Stack Time Interval   : Aug 21 14:32:09  - Aug 21 16:33:09
TRM Records Scanned   : 71
Port Range            : ALL

                                UDP TR Events

IP Address : 05.16.17.18
    Date and Time       Port   Type   Duration   Discarded  Qsize  Correlator
   ---------------     ------  ---   ----------  ---------- -----  ----------
8/21/2000 14:32:9.53     5001   E                             VS        87011
8/21/2000 14:33:9.53     2001   X           100         155   VS        87232

IP Address : 05.16.17.18
    Date and Time       Port   Type  Duration     Would    Qsize  Correlator
                                                 have been
                                                 Discarded
   ---------------     ------  ---   ----------  ---------- -----  ----------
8/21/2000 16:32:9.54     1001   E                             VS        87887
8/21/2000 16:33:9.54     2001   X           100         155   VL        87995

TRMD Started                  : Aug 21 10:32:09
```

TR UDP Statistics Report: trmdstat -W -S

Displays the contents of individual UDP statistics records.

```
trmdstat -U -S /tmp/statlog.log
trmdstat for Z/OS CS V1R2          Tue Jan 16 13:17:08 2001

Log Time Interval     : Jan  9 10:54:17  - Jan  9 10:55:45
Stack Time Interval   : Jan  9 15:47:00  - Jan  9 15:55:15
TRM Records Scanned   : 27
Port Range            : ALL

                                UDP Statistics

IP Address : 127.0.0.1
    Date and Time        Port    Datagrams Received  Datagrams Discarded  Dgs Peak
---------------------- ------ --------------------- --------------------- ----------
01/09/2001 15:47:00.11   8000              12345670                  1230        111
                                Bytes Received      Bytes Discarded    Bytes Peak
                              --------------------- --------------------- ----------
                                          12345671                  1231       1111
                                     Duration           Constraints    Qsize Action
                                    ----------          ----------    ----- -------
                                            10                  50      VS  NOLIMIT

    Date and Time        Port    Datagrams Received  Datagrams Discarded  Dgs Peak
---------------------- ------ --------------------- --------------------- ----------
01/09/2001 15:49:03.63   8002              33333330                  3330        333
                                Bytes Received      Bytes Discarded    Bytes Peak
                              --------------------- --------------------- ----------
                                          33333333                  3333       3333
TRMD Started                 : Jan  9 10:53:42
TRMD Ended                   : Jan  9 11:05:14
```

z/OS Communications Server Security

Appendix C

- **Automation Examples**

Automation Example
IDS message on NetView Console

Session E - [32 x 80]

File Edit View Communication Actions Window Help

```
Product Introduction      Tivoli NetView   N5173 SECOP    07/10/01 14:42:
| N5173
EZZ8761I IDS EVENT DETECTED 389
EZZ8762I EVENT TYPE: SUSPICIOUS PACKET RECEIVED
EZZ8763I CORRELATOR 4 - PROBEID 04030001
EZZ8764I SOURCE IP ADDRESS 10.10.11.199 - PORT 0
EZZ8765I DESTINATION IP ADDRESS 197.11.106.1 - PORT 0
EZZ8766I IDS RULE prIDS-FRG1
EZZ8767I IDS ACTION paIDS-FRG1
--------------------------------------------------------------------------
```

Automation Example
email of trmdstat Output

e-business

To: gforghetti@tivoli.com, garyf@nmpipl73
cc:
Subject: Intrusion Detection Services Report

```
Report of intrusions detected by probe ID. Reporting Interval: 00:01:00

There were 6 Intrusions with probe ID:'04030001' during this Reporting Interval.

/bin/trmdstat -A -D /u/garyf/trmdstat.log
trmdstat for z/OS CS V1R2          Tue Jul 10 18:47:19 2001

Stack Name            : ALL
Log Time Interval     : Jun  1 18:25:02  - Jun  1 18:25:02
Stack Time Interval   : Jun  1 18:24:54  - Jun  1 18:24:55
TRM Records Scanned   : 108
Port Range            : ALL

                                ATTACK  Events

                              Packets Discarded
Attack      Date and Time       Dst IpAddr      Src IpAddr      Dst Port Src Port Correlator ProbeID
------ --------------------- --------------- --------------- -------- -------- ---------- --------
 IPFr  06/01/2001 18:24:54.96 197.11.106.1    10.10.11.199          0        0         13 04030001
 IPFr  06/01/2001 18:24:54.96 197.11.106.1    10.10.11.199          0        0         14 04030001
 IPFr  06/01/2001 18:24:54.96 197.11.106.1    10.10.11.199          0        0         15 04030001
 IPFr  06/01/2001 18:24:54.96 197.11.106.1    10.10.11.199          0        0         16 04030001
 IPFr  06/01/2001 18:24:54.96 197.11.106.1    10.10.11.199          0        0         17 04030001
 IPFr  06/01/2001 18:24:54.96 197.11.106.1    10.10.11.199          0        0         18 04030001
```

IBM

Automation Example
email containing IDS message

To: Gary Forghetti/Raleigh/IBM@IBMUS
cc:
Subject: Intrusion Detection Services Alert

```
The following message has been sent to you from Intrusion Detection Services:

EZZ8761I IDS EVENT DETECTED 389
EZZ8762I EVENT TYPE: SUSPICIOUS PACKET RECEIVED
EZZ8763I CORRELATOR 4 - PROBEID 04030001
EZZ8764I SOURCE IP ADDRESS 10.10.11.199 - PORT 0
EZZ8765I DESTINATION IP ADDRESS 197.11.106.1 - PORT 0
EZZ8766I IDS RULE prIDS-FRG1
EZZ8767I IDS ACTION paIDS-FRG1
```

For More Information....

URL	Content
http://www.ibm.com/servers/eserver/zseries	IBM Enterprise Servers (z900 & S/390)
http://www.ibm.com/servers/eserver/zseries/networking	z900 Networking
http://www.ibm.com/servers/eserver/zseries/networking/technology.html	Networking White Papers and Information
http://www.ibm.com/software/network	Networking & Communications Software
http://www.ibm.com/software/network/commserver	Communications Server
http://www.ibm.com/software/network/commserver/library	CS White Papers, Product Doc, etc.
http://www.redbooks.ibm.com	ITSO Redbooks
	Security in OS/390-based TCP/IP Networks (SG24-5383)
	A Comprehensive Guide to Virtual Private Networks, Volume 1: IBM Firewall, Server, and Client Solutions (SG24-5201)
	A Comprehensive Guide to Virtual Private Networks, Volume III: Cross-Platform Key and Policy Management (SG24-5309)
http://www.ibm.com/support/techdocs/	Advanced Technical Support (Flashes, Presentations, White Papers, etc.)