

# Securing and Encrypting Network Traffic with z/OS Communications Server and Policy Agent

## Security Workshop

### IP Filtering



IBM Washington System Center  
IBM Technical Sales Support

# Trademarks

---

- **The following are Registered Trademarks of the International Business Machines Corporation in the United States and/or other countries.**
    - IBM
    - z/OS
  - **The following are trademarks or registered trademarks of other companies.**
    - Microsoft is a registered trademark of Microsoft Corporation in the United States and other countries.
  - All other products may be trademarks or registered trademarks of their respective companies.
  - Refer to [www.ibm.com/legal](http://www.ibm.com/legal) for further legal information.
- 
- OSA-Express Features
  - There are many different types of OSA-Express features. In this document where OSA is mentioned it refers to an OSA port on any of the OSA-Express features unless a specific OSA-Express feature is mentioned.

# Agenda

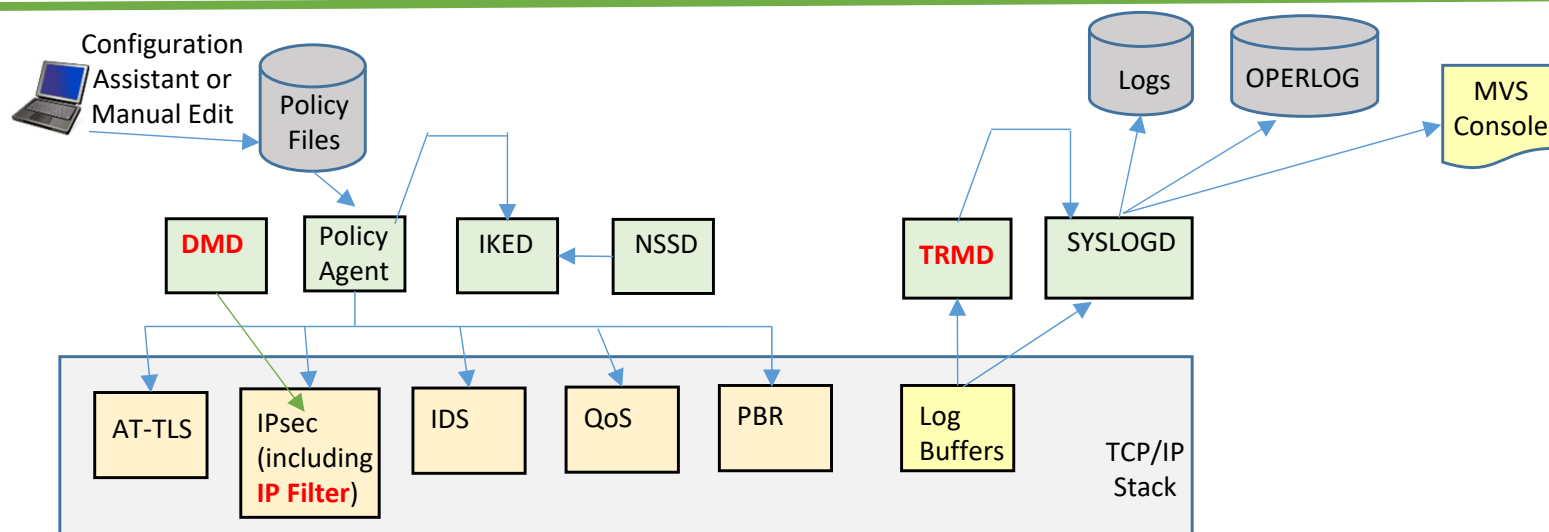
---

- Overview of IP Filtering
- Enabling IP Filtering on z/OS
- Defense Manager Daemon (DMD)

# Overview of IP Filtering

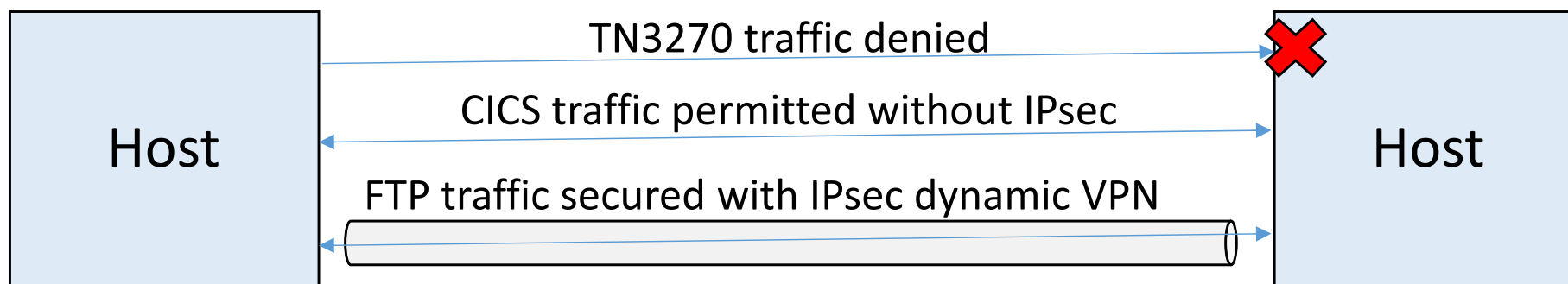


# Lots of Different Policy Types and Started Tasks



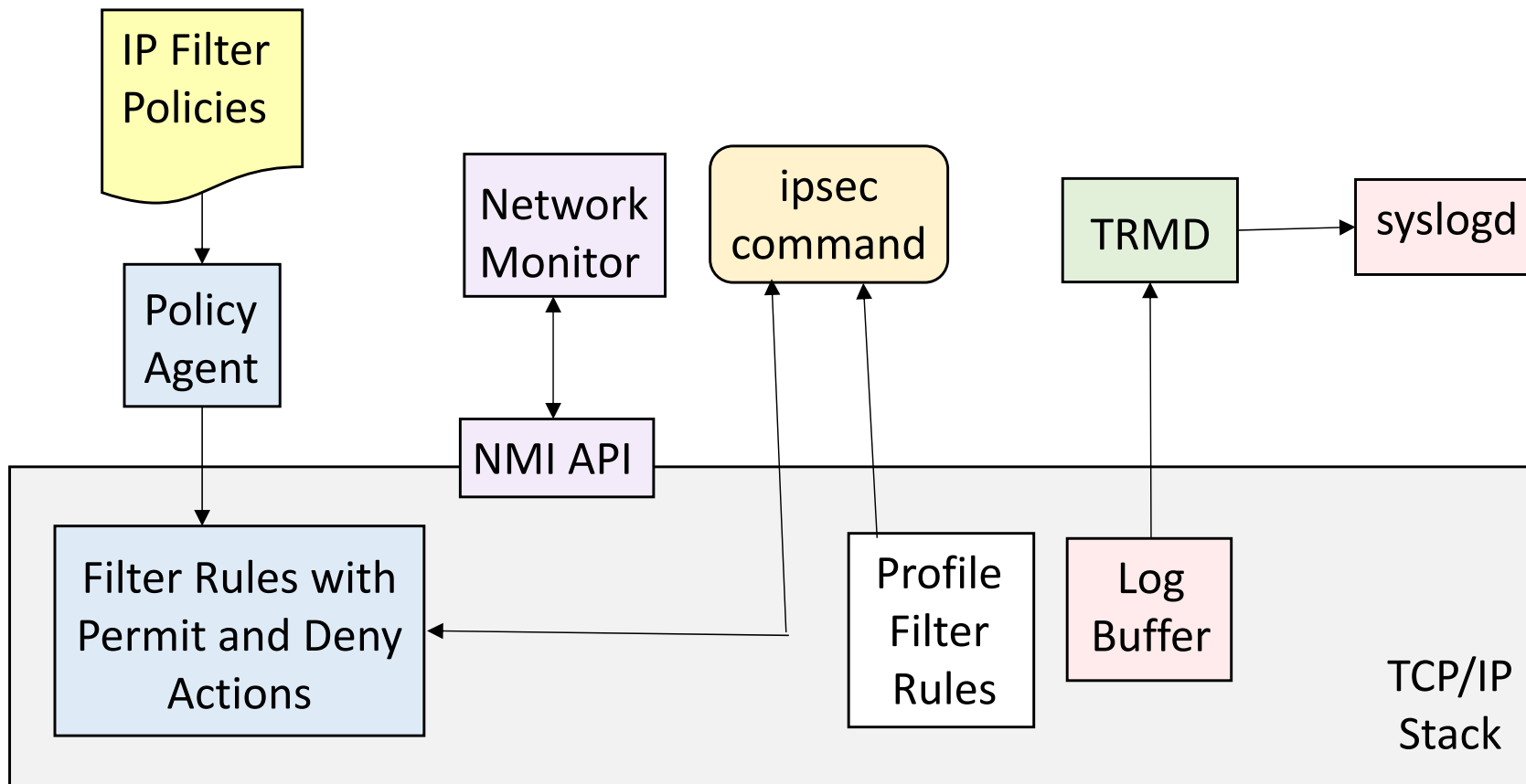
- Policy Agent
  - Installs Policies into the TCP/IP stack
- TCP/IP Stack
  - Enforces the Policies
- **DMD (Defense Manager Daemon)**
  - **ipsec command can be used to install temporary IP Filter rules.**
- IKED (Internet Key Exchange Daemon)
  - Required for IPsec Dynamic VPN (Virtual Private Network) Tunnels
- NSSD (Network Security Server Daemon)
  - Required for IKEv2
  - Provides central RACF certificate repository for remote IKED applications
  - Provides DataPower access to RACF
- TRMD (Traffic Regulation Management Daemon)
  - Required for log messages to syslogd for IP Filter, IPsec, and IDS
- SyslogD
  - Recommended for logging

# z/OS IP Filter and IPsec



- IP Filtering
  - Permit or Deny (Block) Traffic
- IPsec
  - Virtual Private Network (VPN) for Authentication, Data Integrity, and Encryption
- On z/OS IP Filtering and IPsec are defined together.
  - IP Filtering may be implemented without IPsec, but IP Filtering is required for IPsec implementation.
  - IP Filtering is not part of the IPsec standard protocol.

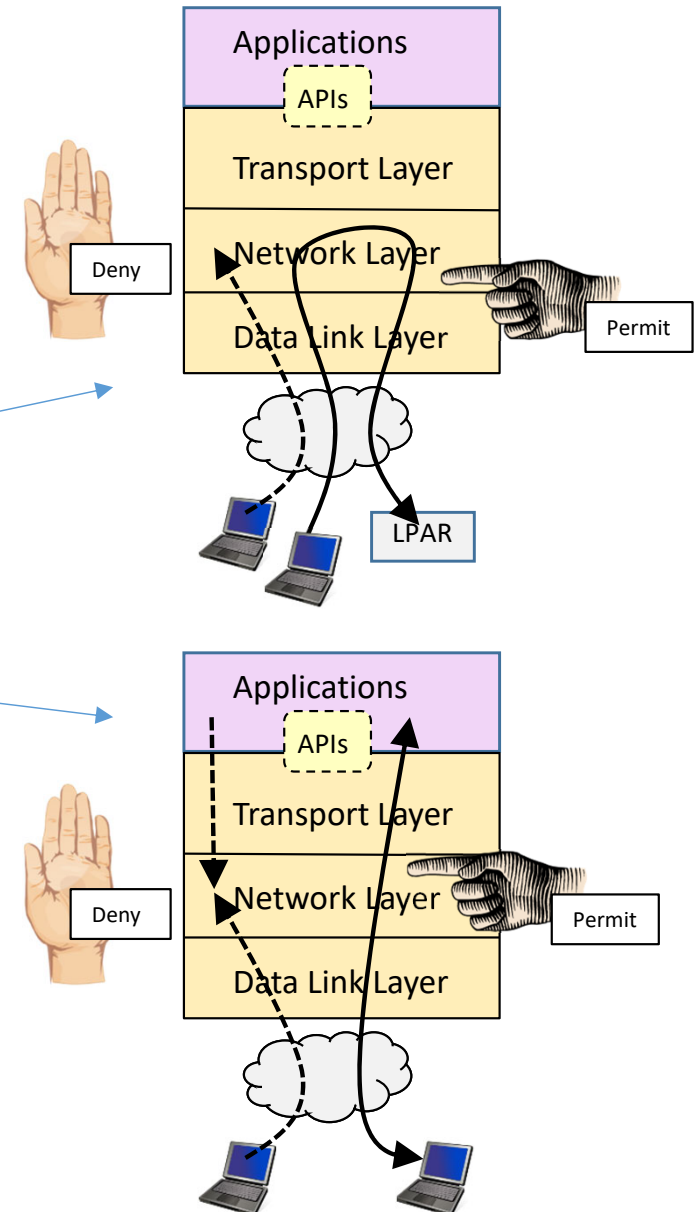
# IP Filtering Implementation



- **TCP/IP Stack**
  - Maintains a list of currently active IP filters (Permit / Deny).
  - Default Filters (Implicit and Explicit Profile Filters)
  - Actively filters network traffic.
- **UNIX System Services (USS) shell command “ipsec”**
  - Provides real-time network management data.
- **Policy Agent**
  - Installs IP Filter policies into the TCP/IP stack.
- **Traffic Regulation Manager Daemon (TRMD)**
  - Responsible for logging IP Filtering events that are detected by the stack (events, updates)
- **System logging daemon (syslogd)**
  - Manages the logging of all messages and events
- **NMI API**
  - Provides network management interface to the same information as the ipsec command.

# IP Packet Filtering Basics

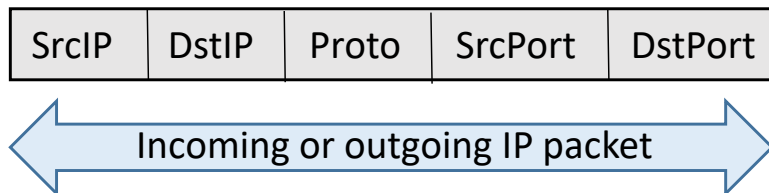
- Packet filtering at IP Layer
- Filter rules defined to match on inbound and outbound packets based on:
  - IP address, port, protocol
  - Direction, link security
  - Time
- Used to control
  - Traffic being routed
  - Local traffic
    - "Personal firewall"
- Possible actions
  - Permit
    - Without IPsec (in the clear)
    - With Manual IPsec
    - With Dynamic IPsec
  - Deny
  - Log (in combination with any other action)





# IP Filter Matching

- Filters are searched in the order they were configured
- Each rule is inspected, from top to bottom, for a match
- If a match is found, the search ends and the action is performed



Active filters in TCP/IP stack



SrcIP	DstIP	Proto	SrcPort	DstPort
-------	-------	-------	---------	---------



SrcIP	DstIP	Proto	SrcPort	DstPort
-------	-------	-------	---------	---------



SrcIP	DstIP	Proto	SrcPort	DstPort
-------	-------	-------	---------	---------

Associated action is performed



SrcIP	DstIP	Proto	SrcPort	DstPort
-------	-------	-------	---------	---------

SrcIP	DstIP	Proto	SrcPort	DstPort
-------	-------	-------	---------	---------

# Policy Definition

Criteria	Description
<b>From Packet</b>	
Source address	Source IP address in IP header of packet
Remote address	Destination IP address in IP header of packet
Protocol	Protocol in the IP header of the packet (TCP, UDP, OSPF, etc.)
Source port	For TCP and UDP, the source port in the transport header of the packet
Destination port	For TCP and UDP, the destination port in the transport header of the packet
ICMP type and code	ICMP type and code in the header of the packet
OSPF type	OSPF type in the header of the packet
<b>Network Attributes</b>	
Direction	Inbound, Outbound, or Both
Routing	Packet is local if source or destination IP address exists on local host, otherwise it is routed
Link Security Class	Virtual class that allows you to group interfaces with similar security requirements.
<b>Time Condition</b>	
Time, Day, Week, Month	When filter rule is active.
<b>Action to Apply</b>	
Permit, Deny, or apply IPsec	Permit, Deny, or use IPsec

# Enabling IP Filtering on z/OS



# Default Rules and Policy Rules

## 1 PROFILE.TCPIP IPCONFIG IPSECURITY

- Implicit Default Rules
  - Deny All
  - After all other rules
  - Cannot be removed
- Not loadable by Obeyfile

## 2 PROFILE.TCPIP IPSECRULE

- Explicit Default Rules
- Permit Rules Only

## 3 Policy Agent IP Filter Rules

- After policy rules are loaded Profile IPSECRULEs are no longer used.

- ipsec command switches between Profile IPSECRULEs and Policy Agent Rules.

### 4 ipsec -f default

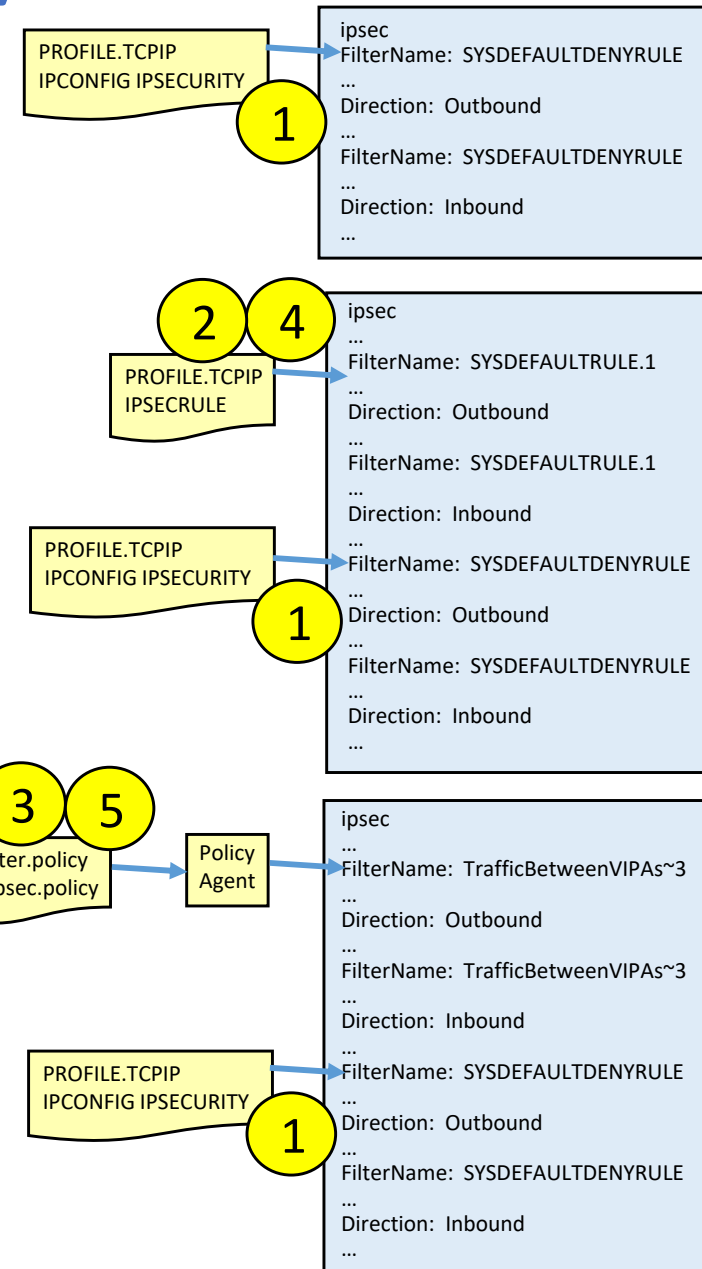
- Causes Profile IPSECRULEs to be used.

### 5 ipsec -f reload

- Causes Policy Rules to be used.

### - ipsec -f display

- Displays the current setting.



# IPSECRULE and IPSEC6RULE

```
IPSEC LOGENable LOGIMPLICIT DVIPSEC
; Rule SrcAddr DstAddr Logging Protocol SrcPort DestPort Routing Secclass
; OSPF protocol used by Omproute
IPSECRule * * NOLOG PROTO OSPF
; IGMP protocol used by Omproute
IPSECRule * * NOLOG PROTO 2
; DNS queries to UDP port 53
IPSECRule * * NOLOG PROTO UDP SRCPort * DESTport 53
; Administrative access
IPSECRule * 9.1.1.2 LOG ROUTING LOCAL
; ICMPv6 protocol
IPSEC6Rule * * NOLOG PROTO ICMPv6
ENDIPSEC
```

- IPSECRULE or IPSEC6RULE may be Inbound, Outbound, or Bidirectional.
- SRCADDR and SRCPORT define the local system while DSTADDR and DESTPORT define the remote system.
  - They do not refer to the source and destination addresses in the IP and Transport headers of the packet.
  - SRCADDR means "IP Address of the LOCAL System"
  - SRCPORT means "PORT on the LOCAL System"
  - DSTADDR means "IP Address of the REMOTE System"
  - DSTPORT means "PORT on the REMOTE System"
- IPSECRULE and IPSEC6RULE entries always have an action of PERMIT.
  - No DENY option.
- Logging requires TRMD.
- IPSEC DVIPSEC indicates that IPsec tunnels associated with IPv4 DVIPA are eligible to be distributed if the DVIPA is being distributed.
- The ROUTING parameter defaults to LOCAL, but may specify ROUTED.

# Steps for Implementing IP Filtering

- Implement PAGENT, SYSLOGD, and TRMD on z/OS
- Enable IPSecurity in the TCP/IP Stack:
  - Set IPCONFIG IPSECURITY in PROFILE.TCPIP.
- Optionally establish IPSECRULEs in the TCP/IP Profile to override the Default Implicit "denyall" rule that is in effect until a set of PAGENT IPsec policy rules is activated.
  - Test Profile Default Rules
- Configure Policy IP Filtering Rules to Permit and Deny Traffic
- Install Policy IP Filter Rules into Stack
- Test Policy Filter Rules

# ipsec Command

- ipsec command SERVAUTH profile
  - EZB.IPSECCMD.sysname.stackname.command\_type
    - SETROPTS GENERIC(SERVAUTH)
    - RDEFINE SERVAUTH EZB.IPSECCMD.sysname.tcpprocname.\* UACC(NONE)
    - PERMIT EZB.IPSECCMD.sysname.tcpprocname.\* CLASS(SERVAUTH) ID(userid) ACCESS(READ)
    - SETROPTS GENERIC(SERVAUTH) REFRESH
- ipsec command options
  - -f for IP Filter
  - -F for Defensive Filter
  - -m for Manual Tunnel
  - -k for IKE Tunnel
  - -y for Dynamic Tunnel
  - -i for Interface
  - -t for IP Traffic Test
  - -o for NATT Port Translation
  - -w for IKED Network Security
  - -x for Network Security Server
  - -?

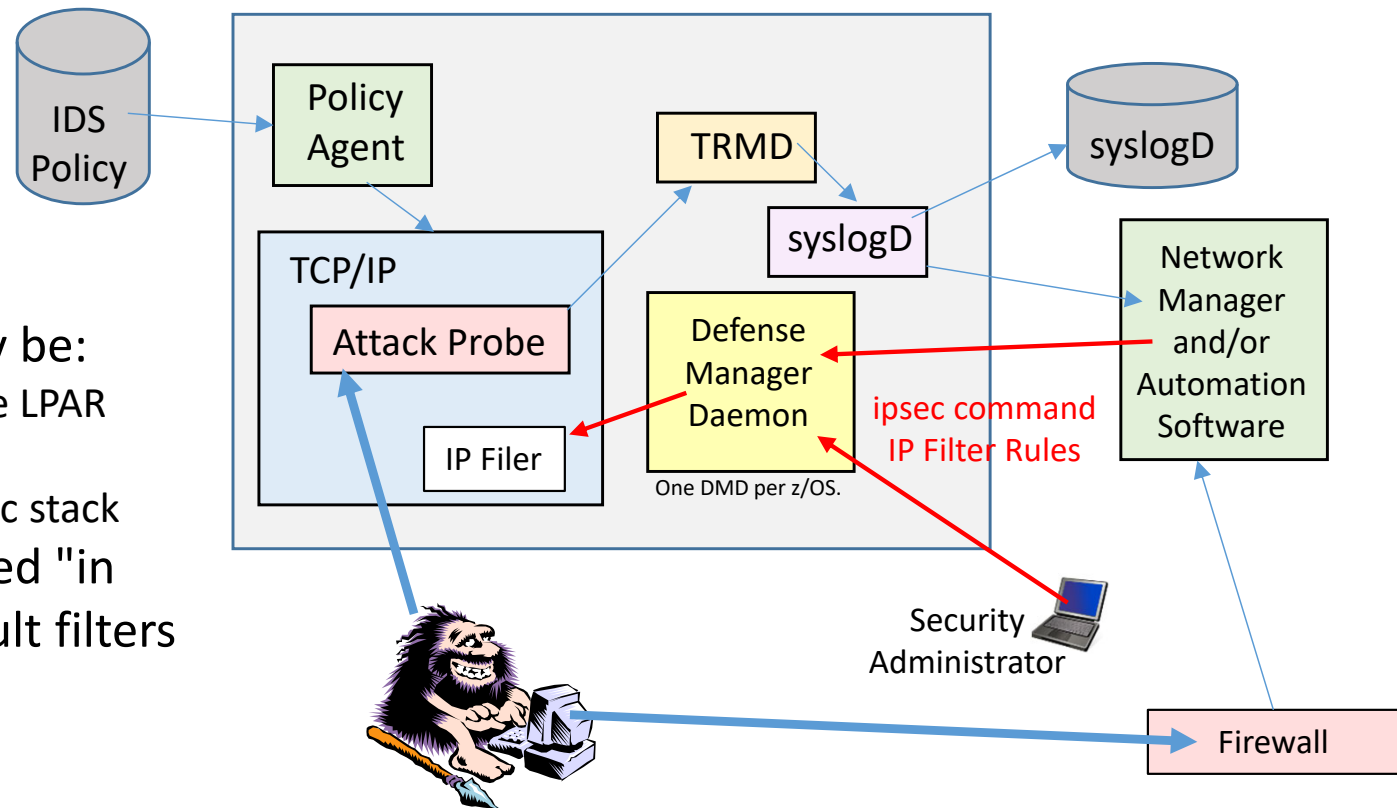
# Defense Manager Daemon (DMD)





# z/OS Defense Manager Daemon

- Allows authorized users to dynamically install time-limited, defensive filters via ipsec command:
  - Security Administrator on z/OS
  - Automation
- Defensive filtering is an extension to IDS capabilities
- Requires minimal IPsec configuration to enable IP packet filtering
- Uses ipsec command to control and display defensive filters
- Maintains record of defensive filters on DASD for availability in case of DMD restart or stack start/restart
- Defensive filter scope may be:
  - Global - all stacks on the LPAR where DMD runs
  - Local - apply to a specific stack
- Defensive filter are installed "in front of" configured/default filters (from policies and profile)



# Customize DMD

- IPCONFIG IPSECURITY in PROFILE.TCPIP.
- Create an IP Filter Policy
  - Either a default filter using the IPSEC statement in the PROFILE.TCPIP and/or policy file.
  - ie.
    - IPSEC
    - ; Rule Sourcelp Destlp Logging Prot SrcPort DestPort Routing Secclass
    - ; Permit all local and routed IPv4 traffic, no logging.
    - IPSECR \* \* NOLOG PROTO \* ROUTING EITHER
    - ENDIPSEC
- SYSLOGD for logging
- DMD Configuration File
  - Use the z/OS Configuration Assistant to create a DMD configuration file.
  - Or create the file using the sample /usr/lpp/tcpip/samples/dmd.conf.
  - Search order:
    - Environment variable DMD\_FILE
    - /etc/security/dmd.conf
- DMD Start
  - Create DMD JCL procedure, sample is SEZAINST(DMD).
  - Or use dmd command in unix to start DMD.
    - Environment variable \_BPX\_JOBNAME

# Modify DMD

---

- **MODIFY procname,REFRESH**
  - Reread DMD configuration file.
  - **MODIFY DMD,REFRESH,FILE='/etc/security/dm.conf2'**
    - Modify may be used to point to a different configuration file than the one used at startup.
- **MODIFY procname,DISPLAY**
  - Display configuration parameters in use by DMD.
- **MODIFY procname,FORCE\_INACTIVE,stackname**
  - Disable defensive filtering for the stack
  - REFRESH command may be used to enable defensive filtering for the stack again.

# End of Topic

