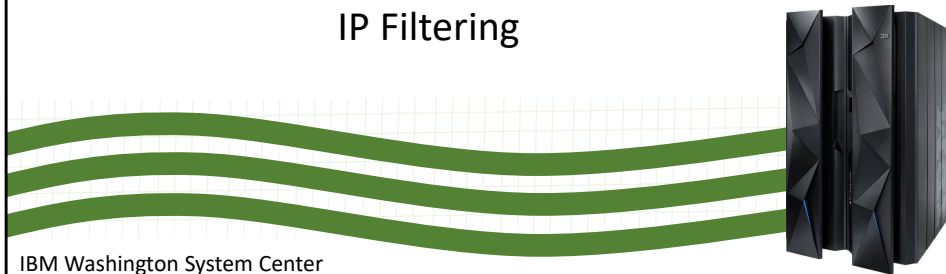


Securing and Encrypting Network Traffic with z/OS Communications Server and Policy Agent

Security Workshop

IP Filtering



IBM Washington System Center
IBM Technical Sales Support

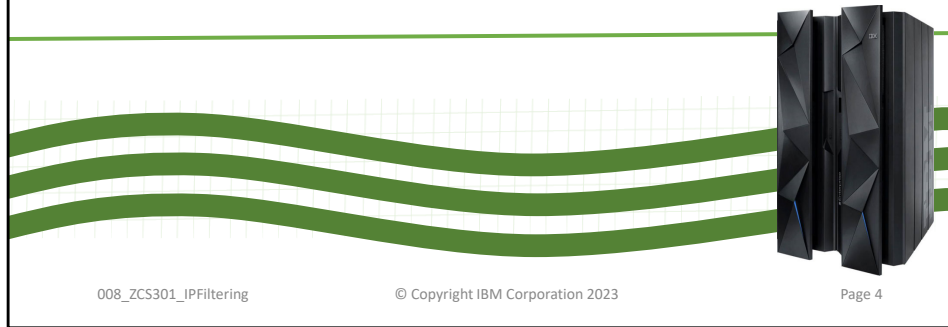
Trademarks

- **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 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

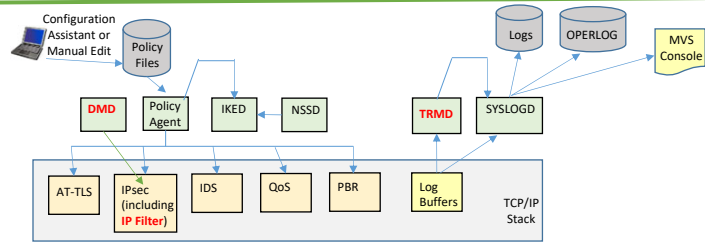


008_ZCS301_IPFiltering

© Copyright IBM Corporation 2023

Page 4

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

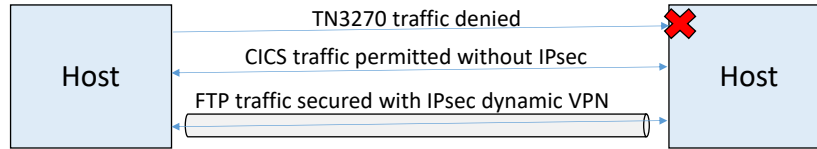
008_ZCS301_IPFiltering

© Copyright IBM Corporation 2023

Page 5

Configuration Assistant can really help getting the whole environment setup.

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.

008_ZCS301_IPFiltering

© Copyright IBM Corporation 2023

Page 6

Configuration support

- Optimized for z/OS host-to-host and z/OS host-to-gateway (z/OS gateway still supported)
- IPsec NAT Traversal support
- IP address translation
- Port translation (V1R8)
- IPv4 and IPv6 support (IPv6 in V1R8)

Policy agent reads and manages IPsec and IKE policy

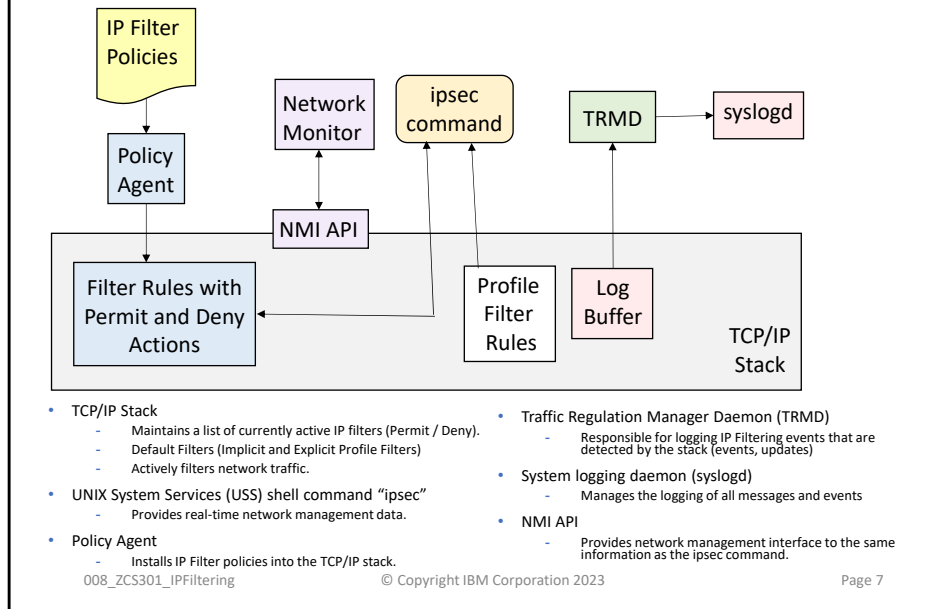
Default filters part of TCP profile

Administrative controls

- pasearch
- ipsec command

Cryptographic algorithms (uses cryptographic hardware if available)

IP Filtering Implementation



TCP/IP Stack

- Maintains a list of currently active IP filters.
- Actively filters network traffic.

UNIX System Services (USS) shell command "ipsec"

- Provides real-time network management data.

NMI API

- Provides network management interface to the same information as the ipsec command.

Policy Agent

- Installs IP Filter policies into the TCP/IP stack.

Traffic Regulation Manager Daemon (TRMD)

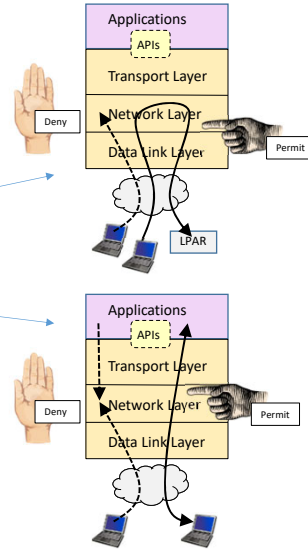
- Responsible for logging IP Filter events that are detected by the stack

System logging daemon (syslogd)

- Manages the logging of all messages and events

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)



008_ZCS301_IPFiltering

© Copyright IBM Corporation 2023

Page 8

IP Filtering may be defined for Local traffic, Routed traffic, or both.

Packet filtering at IP Layer

Filter rules defined to match on inbound and outbound packets based on:

- packet information
- IP address, port, protocol
- network attributes
- direction, link security
- time

Used to control

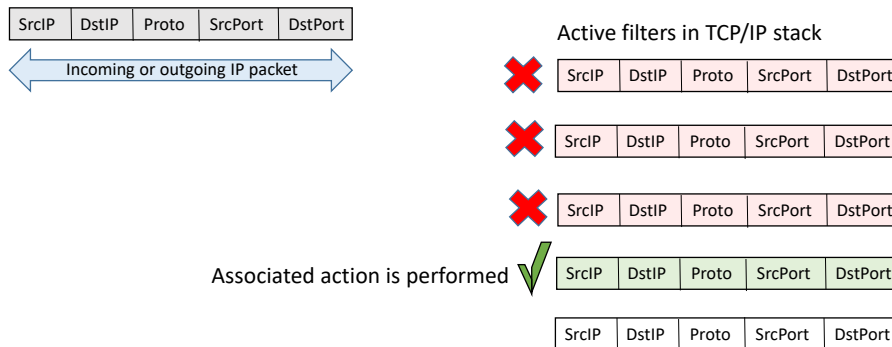
- traffic being routed
- access at server

"Personal firewall" on z/OS

Payment Card Industry demands "Stateful Firewall Filtering." IP Filtering does not keep track of session state. As a result, it is not considered stateful, although this is a known requirement.

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



The order of the configured filters matters. The most granular should be first and the least granular should be last.

Policy Definition

Criteria	Description
From Packet	
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
Network Attributes	
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.
Time Condition	
Time, Day, Week, Month	When filter rule is active.
Action to Apply	
Permit, Deny, or apply IPsec	Permit, Deny, or use IPsec

Enabling IP Filtering on z/OS



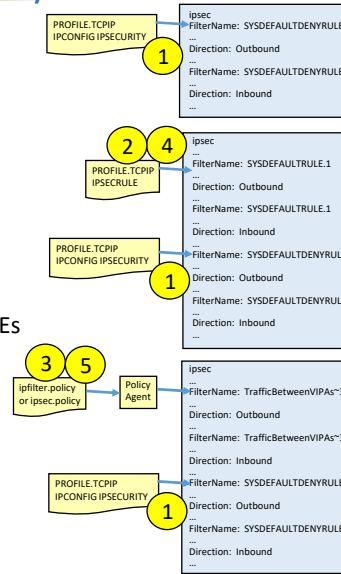
008_ZCS301_IPFiltering

© Copyright IBM Corporation 2023

Page 11

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.



008_ZCS301_IPFiltering

© Copyright IBM Corporation 2023

Page 12

The IPSECURITY option is activated only at the TCP/IP startup. If you want to remove the IP filtering function, you must restart the stack without it.

The default policy is always loaded by the stack when the configuration profile is first processed with IPCONFIG IPSECURITY. If the initial profile does not have any IP filter rules, only the implicit rules will be loaded. Any rule defined for the log options can be changed by the vary tcpip obeyfile console command.

Important: The implicit rules are always created using either the default or the filter policy. Just by using the IPSECURITY option in the IPCONFIG statement, the implicit rules are created and deny all the inbound and outbound TCP/IP traffic in that z/OS image. This means that if you code IPSECURITY without either some IPSEC statements or filter policies, you will have a completely inaccessible stack.

Therefore, consider defining a default policy that has an IPSECRULE to allow one administrative IP address to connect to the TCP/IP stack. In this way, if PAGENT fails to start, you will still have a way to access the stack using TN3270.

The major differences between the default policy and the filter policy are:

- In the default policy, there are only permit rules. The implicit rules implement the deny all functions. In the pagent policy, you have the option to create deny rules.
- The default policy only permits local packets; all routed traffic is denied. If you want to apply filter policies to messages that are being routed between a z/OS image and other z/OS images, then the filter policy must be used.
- There is no option to group similar resources in the default policy. That capability is only available in the filter policy.

The default policy is always used in the absence of a filter policy. If a filter policy is defined, both are loaded into the TCP/IP stack and the filter policy is used unless you specify with the ipsec command that the default policy should be used. Using the ipsec command, you can switch between the default and the filter policy whenever necessary.

The ipsec command is used to manage and monitor the IP security filtering.

- ipsec -f reload: reloads your own policy rules for filtering and IPSEC.
- ipsec -f default:loads the default rules defined in the TCP/IP Profile.
- Ipsec -f display

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.

008_ZCS301_IPFiltering

© Copyright IBM Corporation 2023

Page 13

Use IPSECRULE and IPSEC6RULE for EXPLICITLY DEFINED Default permit rules that denote exceptions to the IMPLICIT Default "deny" policy (also known as the "SYSDEFAULTDENYRULE").

When the IMPLICIT default IP filter policy is active, these permit rules appear in the default IP filter table before the SYSDEFAULTDENYRULE entries.

Typically, these exceptions are few in number and are used for administrative access to the system in the event that IP security policy is unavailable.

For instance, a sample default set of permit rules might include entries to provide the following:

- Administrative access
- Basic network services, such as DNS and OSPF routing advertisements
- Use of ping to test for server availability

IPSECRULE and IPSEC6RULE entries are coded in the IPSEC block of the TCP/IP profile. They describe the attributes of the IP traffic that is allowed when the default IP filter policy is active.

These rules can specify source address, destination address, protocol, source port, destination port, routing, and security class.

Unlike IP filter rules that are defined in Policy Agent, which allow direction to be specified, an IPSECRULE or IPSEC6RULE is always bidirectional. This means that for any IPSECRULE or IPSEC6RULE entry that specifies a source and destination address or port, an outbound rule is created with that source and destination address and port, along with an inbound rule with the source and destination addresses and ports reversed. (This equates to the use of the bidirectional keyword in an IpFilterRule statement.)

IMPORTANT: The IPSECRule that you see here uses the parameters SRCADDR and SRCPORT. In reality, the IPSECRules are always written from the perspective of the LOCAL node in which they appear. Therefore, SRCADDR actually means "IP Address of the LOCAL System" and SRCPORT means "PORT on the LOCAL System." Likewise, DstAddr and DestPort reference the "REMOTE" system.

IPSECRULE and IPSEC6RULE entries always have an action of permit; there is no action specification for deny or permit with IPsec protection.

For LOGGING you must have enabled TRMD:

- The "master switch" are the LOG parameters on the IPSEC statement:
 - LOGENABLE or LOGDISABLE for the DEFAULT IPSECRules (SYSDEFAULTRULE)
 - LOGIMPLICIT or NOLOGINPLICIT for the SYSDEFAULTDENY rule
- The individual switch is on the IPSECRule statement:
 - LOG or NOLOG

IPSEC DVIPSEC:

- Indicates that IPsec tunnels associated with IPv4 dynamic VIPA addresses are eligible to be distributed if the dynamic VIPA address is being distributed. The IPsec tunnels are also eligible to be moved during dynamic VIPA takeover or giveback.

The ROUTING parameter defaults to LOCAL, but you may specify ROUTED. When using the default filter policy statements in the PROFILE.TCPIP, you can choose to permit local and routed traffic using the parameter ROUTING on the IPSECRULE and IPSEC6RULE statements. The options can be LOCAL, indicating that this rule applies to packets destined for this stack, ROUTED, indicating the rule applies only to packets being forwarded by this stack, or EITHER, indicating the rule applies to forwarded and non-forwarded packets.

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

008_ZCS301_IPFiltering

© Copyright IBM Corporation 2023

Page 14

Once you code IPCONFIG IPSECURITY in a stack, you still want to ensure that you can telnet into that stack for maintenance. This means that you will want to ensure that your Policy Agent rules are working the way you want them to. If PAGENT does not initialize, you will not be able to access the TCP/IP stack unless you have IPSECRULEs inside the TCP/IP Profile that allow at least the administrator to telnet into the stack.

- Of course, you should always have a backup plan to be able to modify non-working TCP/IP profiles.
 - Example: an alternate TCP/IP profile without IPCONFIG IPSECURITY. (Note that the OBEYFILE technique will not work for removing IPCONFIG IPSECURITY from a TCP/IP Profile.)
 - Example: an SNA path into the VTAM of the MVS image.
 - Example: an alternate path to the DASD that holds the non-functioning TCP/IP profile so that you may edit the necessary definitions to provide access.

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
 - -?

008_ZCS301_IPFiltering

© Copyright IBM Corporation 2023

Page 15

You must have IPSEC command authorization in the SERVAUTH class to be able to execute the IPSEC command:

- On our systems, the USER and the SYS1 groups have access to the SERVAUTH class named EZB.IPSECCMD.*.*

The ipsec command is an APF-authorized application. Users of the ipsec command must also be authorized through the security access facility (SAF). This information assumes that the SAF is RACF. Authorization is managed with the SERVAUTH profile. For the ipsec -f default and ipsec -f reload command, file system access is also required. You do not need root authority to use the ipsec command, but for filter rule set control on a local stack, the administrator must provide you with some file access capability

Defense Manager Daemon (DMD)



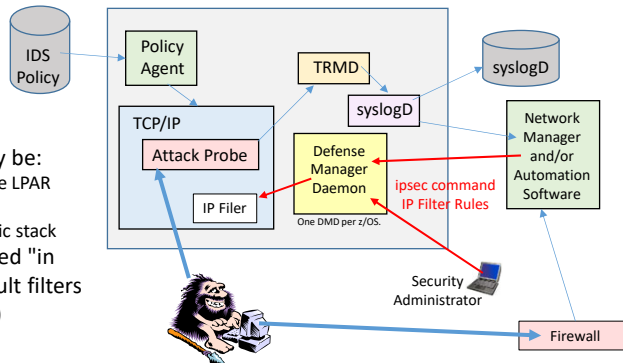
008_ZCS301_IPFiltering

© Copyright IBM Corporation 2023

Page 16

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)



008_ZCS301_IPFiltering

© Copyright IBM Corporation 2023

Page 17

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 SourceIp DestIp 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

008_ZCS301_IPFiltering

© Copyright IBM Corporation 2023

Page 18

See the IP Configuration Guide and the IP Configuration Reference.

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



008_ZCS301_IPFiltering

© Copyright IBM Corporation 2023

Page 20