z/OS Firewall Technologies Filter Rules

Filter Rules Defintions

Mary B. Sweat
sweatm@us.ibm.com

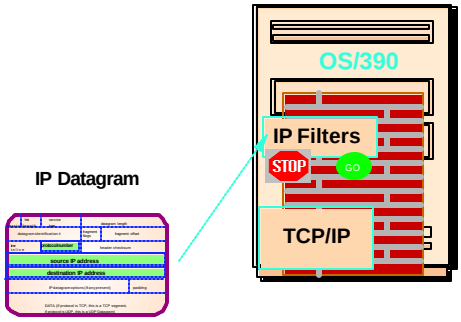
IBM S/390 Security
Advanced Technical Support
Washington Systems Center
Gaithersburg, MD

Unit Expectations

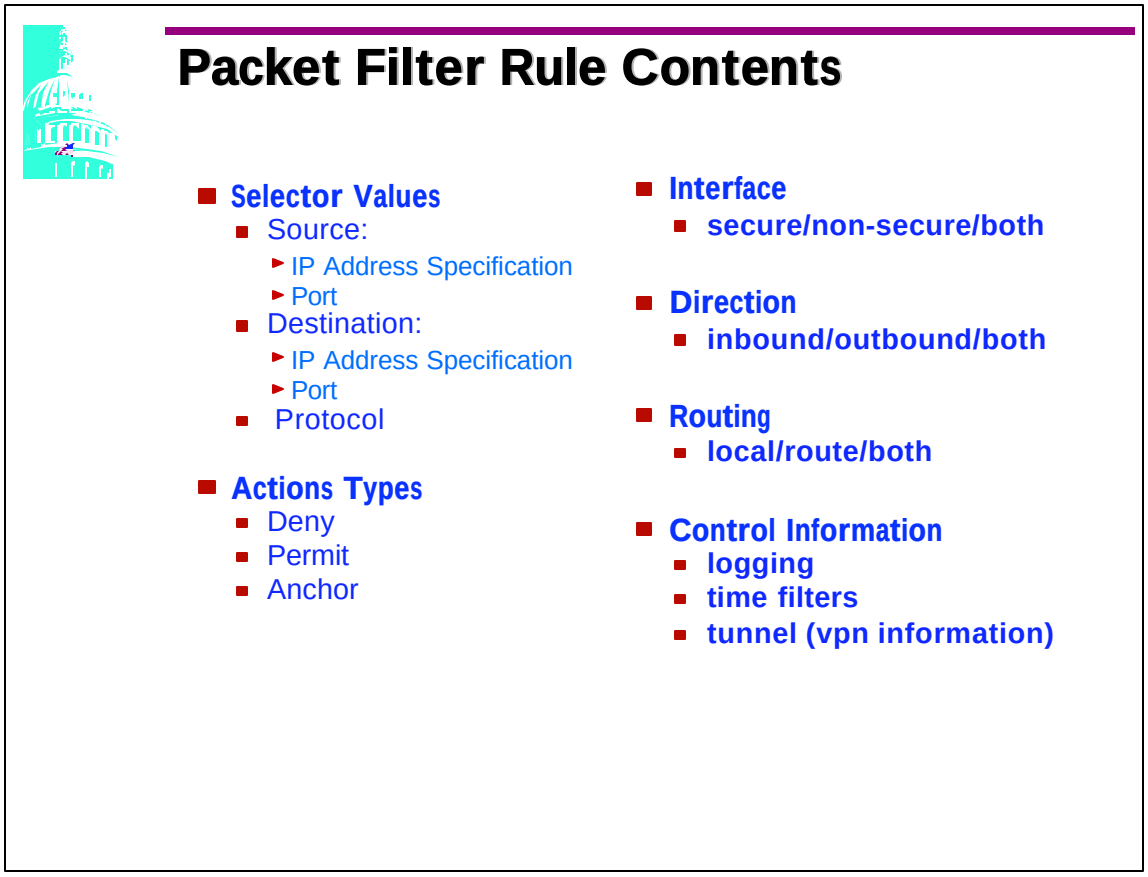
- **Purpose**
  - **To instruct how to configure rules for the OS/390 Firewall Technology**

IP Packet Filtering

- **IP level technology for controlling access through a firewall**
  - set of encoded directives
- **Allows or stops packets based on information in IP header and TCP/UDP headers**
- **Each packet is filtered separately**



- If the IP information in the packet header matches the IP information in the filter, the packet is allowed or denied based on the rule.
- Packets are compared against filters from the top down. When a match is found the packet is permitted or denied. The first match is used and the packet is not compared to any other rule. Therefore, the rules should be listed from most specific down to general. The firewall administrator can do this through firewall commands.
- If no match is made the "default" is to deny.



- A anchor rule is a place holder for another type of filter rule called a dynamic filter rule. These rules are similar to permit and deny except that the action parameter is set to anchor.

IP Filter Rule Elements

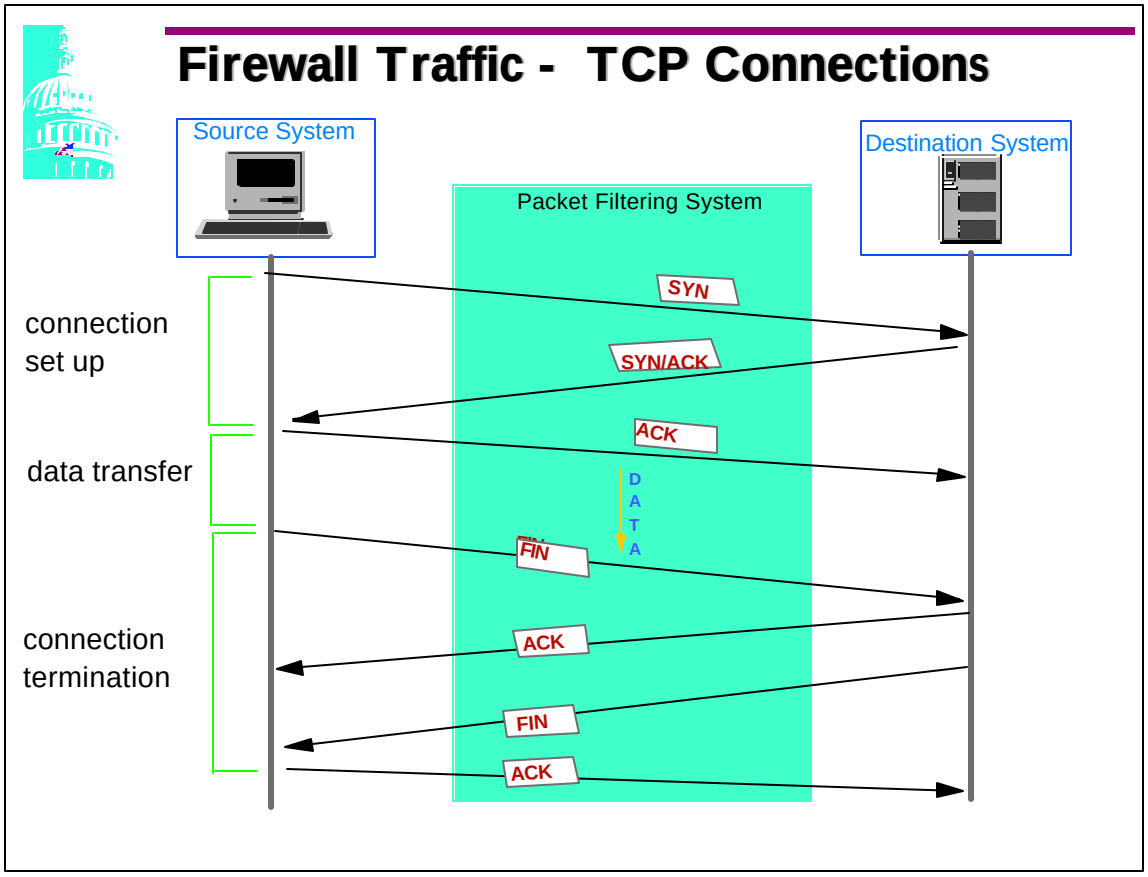
type	=	permit
source address	=	9.12.14.128
source masking	=	255.255.255.255
destination address	=	10.12.14.247
destination mask	=	255.255.255.255
protocol	=	tcp
source operation code	=	gt
source port	=	1023
destination operation code	=	eq
destination port	=	23
interface	=	nonsecure
routing	=	local
direction	=	both
logging	=	y

Type	permit or deny traffic
Protocol	specifies the type of traffic
Source op	logic operator to apply to source port
Dest op	logic operator to apply to destination port

- This is an example of an IP Filter rule.
- Supported Protocol Type:

all	protocols
tcp	TCP without ACK bit
tcp/ack	normal TCP segments
udp	UDP segments
icmp	ICMP datagrams
ospf	OSPF protocol data units
ipip	Encapsulated IP
esp	Encapsulated secure payload
ah	Authentication Header

- Source op - any,eq,neq,lt,gt,le,ge
- Source port - source port number
- Dest op - any,eq,neq,lt,gt,le,ge
- Dest port - destination port number



- The TCP connection setup process consists of three steps::
  1. The source system sets the SYN segment specifying the port number on the destination system the source wants to connect to. It also contains the source's initial sequence number (SN)
  2. The destination system responds with its own SYN segment. And the destination acknowledges the client's SYN.
  3. The source must acknowledge this SYN from the destination by ACKing the destination sequence number (SYN).

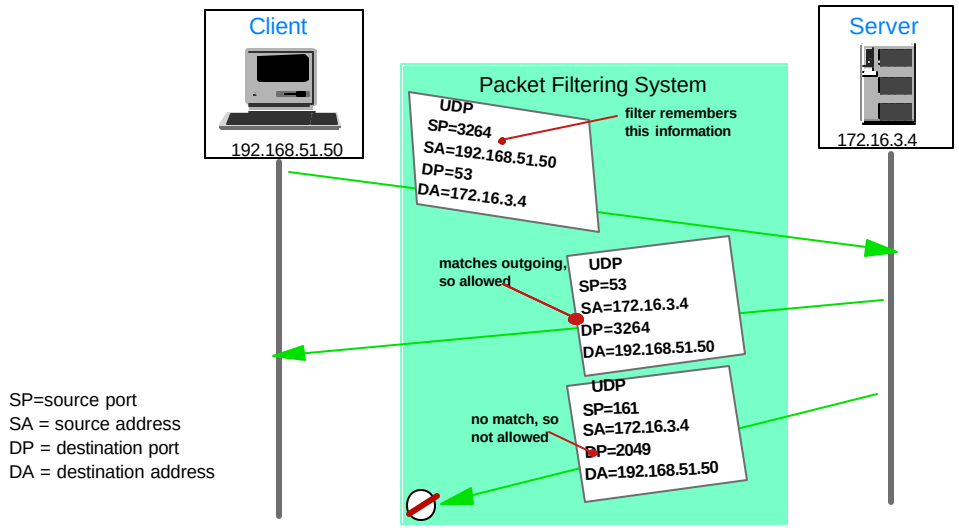
- Since three messages are exchanged between the source and destination system to establish a TCP connection, it is referred to as a threee-way handshaking process

- Only the first segment has no ACK bit The ACK bit. This can be used to determine which system can initiate a TCP connection. For instance, you may want your clients to initiate a FTP session, however, you may not want someone on your firewall system to initiate a FTP session.

- TCP protocol is number 6.

Firewall Traffic - UDP Connection

- Firewall filters UDP based on source and destination ports
- Ports identify which processes are sending/receiving a UDP datagram

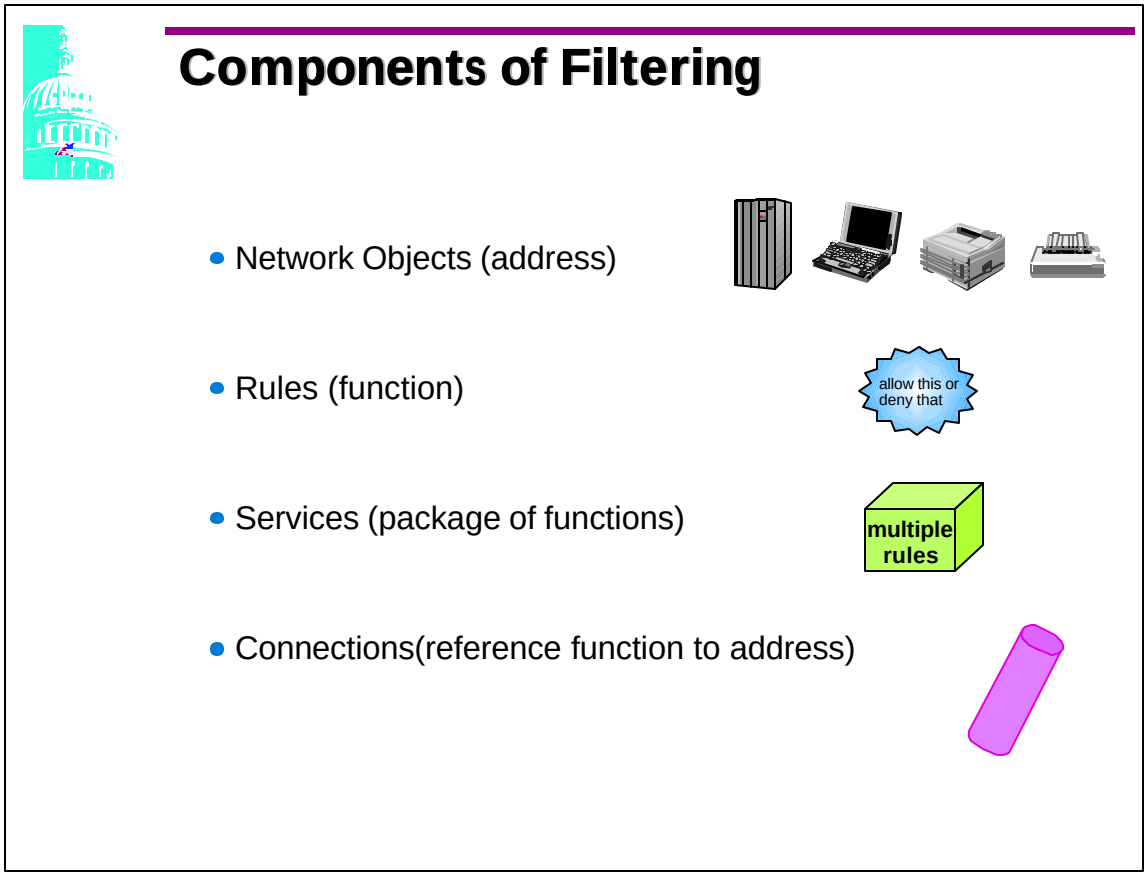


- Primary users of UDP are Domain Name Server (DNS) which will use port 53 and SNMP which uses port 161 and 162.
- This example show s inbound request generated from192.158.51.50 to 172.16.3.4. The request is using the UDP protocol, from a port greater then 1023 and destined for a port 53.
- The second rule shows UDP traffic coming from port 53, back to a port greater then 1023.
- UDP protocol number is 17.

Firewall Traffic - Internet Communication Message Protocol (ICMP)

- **ICMP communicates errors and information between hosts that are processing IP datagrams**
- **ICMP message consists of a type plus a code**
- **There is no source port or destination port used**
  - **source port = ICMP type**
  - **destination port = ICMP code**
  - **the logical operator specified is applied to the type and code**
    - **any**, means that any type or code value will match the rule
- **ICMP type and codes**
  - **Types** **Code Description**
    - 0 — 0 - response to a ping (echo response)
    - 3 — 1 - destination unreachable
    - 3 — 3 - port unreachable
    - 5 — 1 - redirect message
    - 8 — 0 - ping request (echo request)

- The ICMP protocol number is 1.



- A firewall rule is made up of these four components
- When each item is defined the firewall automatically assigns an ID number.
- Network Objects define how the network is laid out in relation to the firewall.
- Rules are used to manage network traffic flowing through the firewall
- Services are groups of rules
- Connections merge objects and rules together

Network Objects

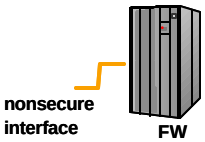
- Represent various hosts and entities
  - single IP address
  - IP address and mask
  - Range of IP addresses
- Defined with "fwnwobj" command
- The Firewall supplies one default object call "The World";

type = network
name = The World
desc =
addr = 0.0.0.0
mask = 0.0.0.0

"Outside World"
0.0.0.0

Example:

type = Host
name ='nonsecure interface'
desc = IBM firewall
addr = 9.82.94.10
mask = 255.255.255.255

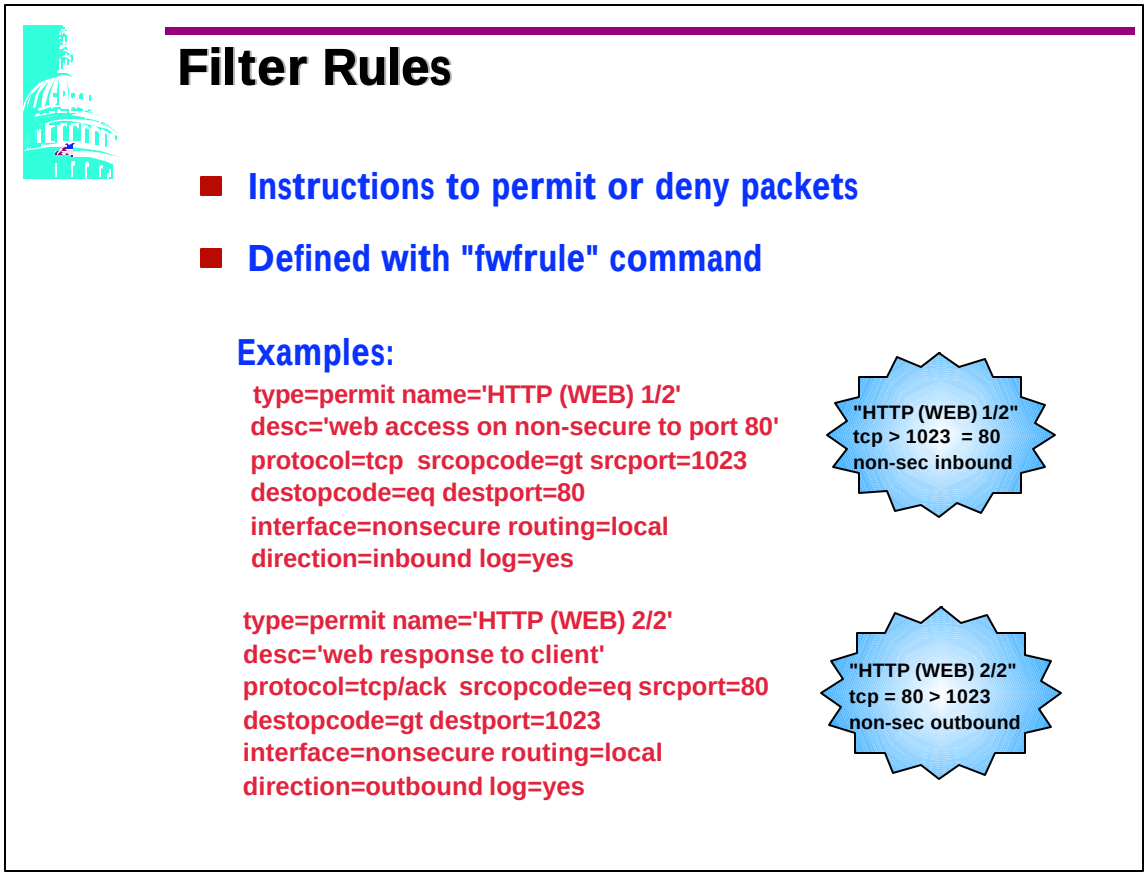


nonsecure interface
9.82.94.10

FW

- FWNWOBJ is used to give an object a name and associate the object with an IP address. Use meaningful names and descriptions.

- name = object name
  type = host, a particular node on the network
  network, a collective range of network addresses
  firewall, a single machine with a firewall installed on it
  router, a host that routes traffic between two or more networks
  interface, a network adapter on a machine
  VPN, Virtual Private Network is the network on the other side of the tunnel
  desc = description of object
  addr = IP address of object
  mask = subnet mask



- When a user issues a request their request will use a port greater then 1023.
- In this example 2 rules have been created, they allow web traffic (HTTP) to flow inbound (HTTP request) and outbound (being the reply to the request). Since HTTP traffic uses the TCP protocol that is what is specified in the rule. All all requests that a user initiates comes from a port greater then 1023, so the source operation code (srcopcode) must be greater then (gt) and the source port (srcport) must be 1023.

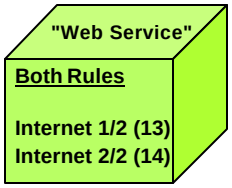
  This is a rule for a web request and it is destined for the web server which listens for it's traffic on port 80. The interface specified is the nonsecure interface, routing is local (meaning that either this request must be initiated from the firewall or it's final destination will be the firewall (web server could be running on the firewall). If the firewall address was neither the initiator nor the destination the "routing" would equal route instead of local.

  This rule is for traffic coming inbound to the firewall and any requests that use this rule will have a log record cut.
- The second rule allows the web server to reply to the initial request. Therefore, the protocol is a tcp/ack rather then tcp and the source port and destination ports are reversed from the first rule. The interface and routing remain the same but the direction now specifies outbound.

Services

- **Groups of rules which instruct firewall to permit or deny access**
- **Defined with "fwservice" command**

  name='Web Service'
  desc='Service for Web Server access'
  rulelist=13/f,14/b



name = name you assign to this service
desc = description that you give this service rule
rulelist = list of rules and direction to add to this service (f or b)

- A Service is a set of filter rules.
- This service definition associates the previous rules that were defined on the previous page.
- F = forward and B=backward, effects how the rule is used. Coding a B with the rule in the Service definition caused the source and destination address to switch places, but that is the only change that occurs. Neither Ports, nor Direction are changed.
- A time parameter can be specified on the services command so it is only active for a specified time period (hours, day, month or weekday) and a timefilter parameter that specifies whether this rule should be active or deactivate during the specified time period.
- Each rule receives an ID number, so the rule for inbound traffic was assigned 13 and the rule from outbound traffic was assigned 14.

  Example:
  fwservice cmd=create name=ping desc=xxxxxx rulelist=13/f,12/b month=Jun-Aug day=15-31 timefilter=activate

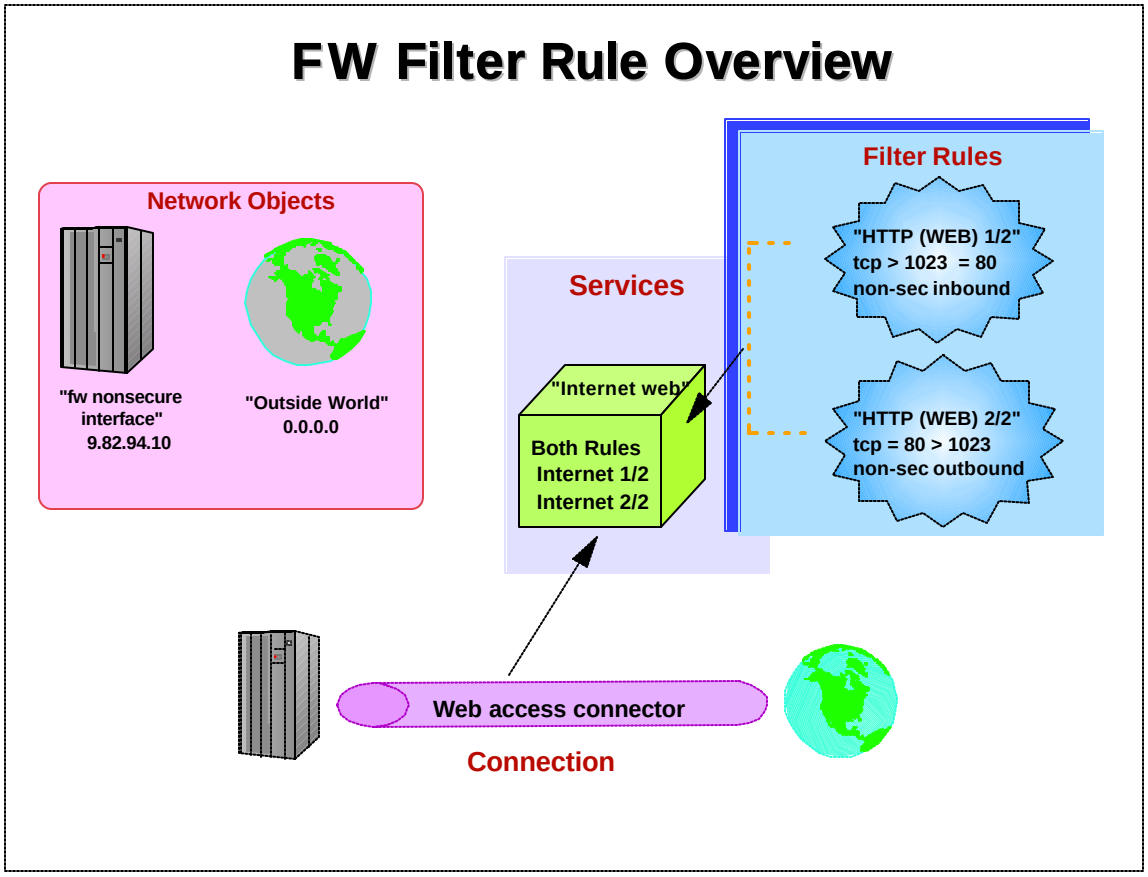
Connections

- **Associate network objects with services to define types of communications allowed between endpoints**
- **Defined with "fwconns" command**

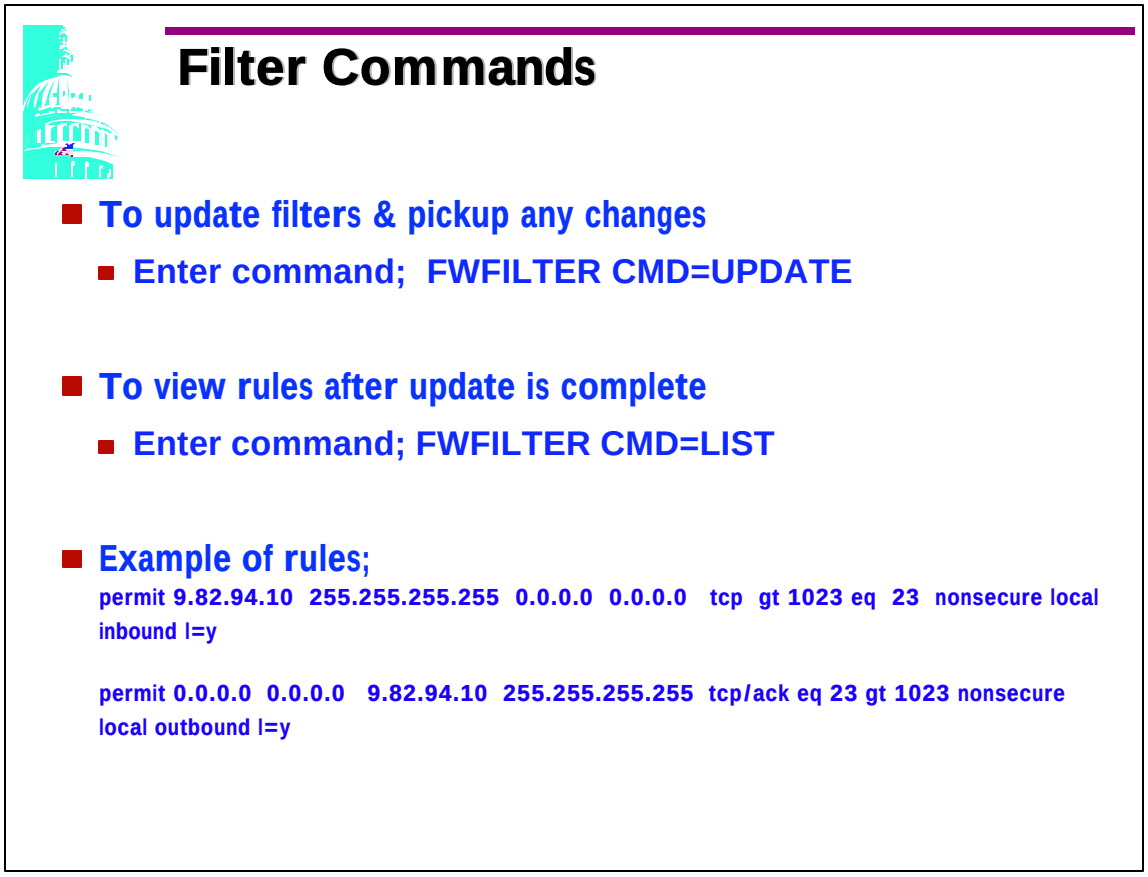
```
name='Web access connector'
desc='allow "World" to access web server'
source='outside-world'
destination='nonsecure interface'
servicelist=40
```

name	name you assign to this connection
desc	description that you give to this connection
source	ID of source network object
destination	ID of destination network object
servicelist	ID's of service rules that apply to this connection

- The firewall connection is an association of the network objects/groups to specific services. Taking a service and connecting it to an object forms a connection.
- The service from the previous page was assigned ID 40, and the name for the network objects, previously defined, are used here in the connection.
- You now have a complete filter rule that state;
  TCP traffic from the source address is allowed to flow into the firewalls nonsecure interface and the firewall will send a reply back from the web server to the initiator of the request.

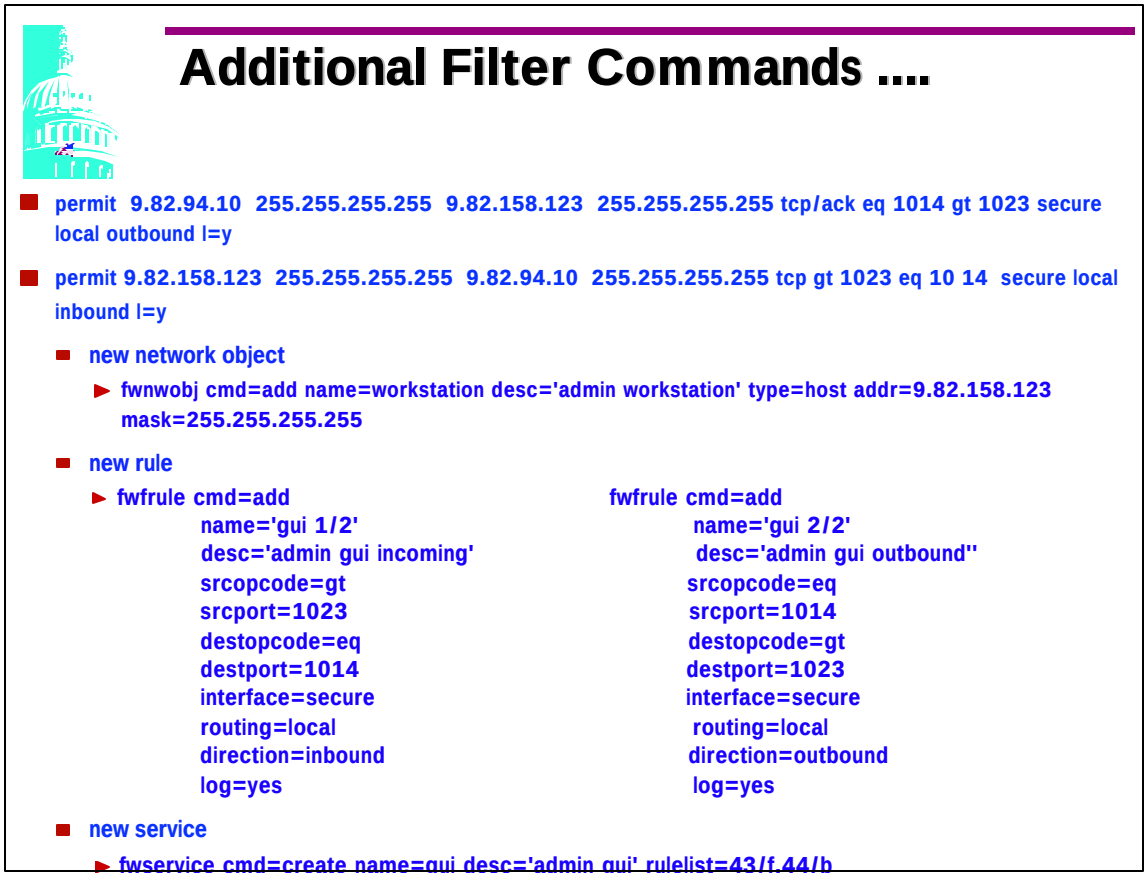


- It is through the connection definition that the network objects are associated with the service, which in turns references the actual rules that will be applied.



- To pick up any changes, additions, deletions, etc. you make to a rule you must enter the FWFILTER CMD=UPDATE command. After that you can list the rules and see the entire rules with the addresses assigned, etc.
- The two rules shown on this page allows telnet traffic to come inbound from and address in the world to the firewall nonsecure adapter (9.82.94.10). The firewall will allow TELNET to responde back to the initiator anywhere in the world.

- This rule would have allowed incoming telnet requests from the internal network (9.82.0.0) through the secure interface. The network object 9.82.94.10 was previous defined.



- These two rules allowed the administrator to use the firewall GUI. The GUI uses SSL to communicate therefore it required port 1014, protocol tcp and a new network object that reflects the administrator's workstation address.

- Using the 'b' option in the service list allowed me to define one service and one connection. Be careful when using this option it can be confusing. It only tells the firewall to switch the source and destination addresses. No other options in the rule is switched.