Chapter 2

Configuring Firewall

This chapter describes how to configure the Juniper Networks stateful firewall on your ERX router; it contains the following sections:

Overview

Firewalls control access to your network to protect it from costly misuse and malicious intent from other users (for example, denial-of-service [DoS] attacks). You position firewalls at all of your network entrance points to provide effective network access control.

You typically place firewalls between an internal network (or your computer, the "trusted" network) and the external network (like the Internet, an "untrusted" network). This placement forces all incoming traffic from the external network to pass through your firewall before it enters your network. In order to safely communicate outside your own network, you must set up rules of communication and provide failsafes between your network and the outside world.

Depending on your needs, you may require a simple or an elaborate firewall. The following sections discuss some of the typical methods of access control, the sorts of issues they protect against, and how you can configure them within your network.

Denial-of-Service Attacks

Denial-of-service (DoS) attacks attempt to deny valid users access to network or server resources by using up all the resources of the network element or server. By using up all the resources, a malicious user can deny access by valid users.

There are many kinds of DoS attacks. Some can be thwarted by using stateless filtering, while others may require state (flow) information. The following list describes some common DoS attacks:

- Synchronization (SYN) flood—Attempting to create a large number of Transmission Control Protocol (TCP) connections by sending synchronization packets but not completing the connections. Known as half-open connections, these incomplete SYN packets take some time to be removed. Because servers often have a limit on the number of connections allowed, this type of attack denies service to valid users.

- Internet Control Message Protocol (ICMP) or User Datagram Protocol (UDP) flood—Preventing access to a network or host with a flood of either UDP or ICMP packets above that which the network elements can handle.

- Ping of death—Sending very large and fragmented ICMP packets that may cause some IP stacks to crash.

- Land attack—Sending TCP SYN packets with the source and destination address set to the address of the machine being attacked.

- Teardrop—Sending the first and second part of a TCP packet in different IP fragments with overlapping offsets, causing the target host to crash.

- IP source route attack—Using the source route option, an attacker can masquerade as a trusted host.

- IP multicast source—Using a multicast source to cause a response that consumes network resources.

- TCP state machine attacks—Setting both the SYN and finish (FIN) bits or the FIN bit with no acknowledgment (ACK) bit within TCP packets.

- Other UDP issues—Sending a UDP echo to IP broadcast destination addresses (called a *fraggle attack*) consumes network resources (because all hosts on the subnetwork respond). Sending a UDP packet in which the UDP length is less than the IP length can cause some systems to crash.

About Stateless Access Control

You can address certain firewall issues (for example, address spoofing) by using stateless access control. In stateless access control, you can use the E-series policy manager to provide solutions. (See *Chapter 1, Configuring Routing Policy*.)

The E-series routers automatically provide some stateless checks as part of their normal forwarding feature set:

- IP datagram length check
- IP fragment offset
- IP checksum check
- IP address spoofing check
- Land attack check
- Broadcast or multicast source address check
- Illegal or reserved source or destination address check

Of these checks, some occur by default in the forwarding path (like checking the IP checksum) and you can explicitly configure others (like checking for illegal or reserved addresses using source address validation).

You can use policies to deny access to various packets (for example, ICMP packets or packets with certain options). Some policy examples include:

- Allowing or disallowing certain applications based on transport address (port)
- Disallowing packets with well-known IP, TCP, or UDP signatures
- Allowing or disallowing certain IP protocols (TCP, UDP, ICMP, and so on)

Understanding Stateful Access Control

After you configure a firewall for a protocol, all packets that belong to those applications which, in turn, use that protocol are subject to stateful monitoring. Stateful access control guards a network by allowing traffic only in the trusted direction. By inspecting the traffic, the firewall allows access to a restricted set of traffic. This process is called *poking a hole in the firewall*.

You can configure stateful access control on a per-interface basis. In addition, you can configure the firewall to inspect traffic on either the ingress or egress side of the interface. This configuration allows you to create a firewall at any interface and also choose which side of that interface is considered *trusted* or *untrusted*.

With state-based access, you can filter basic TCP, UDP, and ICMP flows, as well as handle certain applications that use in-band signaling to establish new flows (that is, they use a *control* connection to set up and tear down secondary connections to your network).

Basic support for the stateful firewall includes TCP, UDP, and ICMP flows. Application-specific support, which takes precedence over basic support, is available for some simple connection applications (for example, DNS, HTTP, HTTPS, POP-2, POP-3, RTSP, SMTP, SSH, TCP, TELNET, UDP, and ICMP) and for FTP (a more complex connection application). This support provides the ability to permit only specific applications while denying others.

NOTE: Application-specific support also allows for application-specific idle timeouts.

TCP Support

To support TCP connections, the JUNOSe stateful firewall supports the following:

- Ability to recognize the start of a new connection using a new 5-tuple on the trusted side of a firewall.
- Ability to add the new connection to the flow table and recognize the return flow.
- Timing out of a connection if the three-way SYN handshake is not completed, or if the connection idle time exceeds the specified timeout value.
- Monitoring the number of half-open TCP connections from a host for SYN floods, and blocking the offending host if the number of half-open TCP connections exceeds the configured threshold.

NOTE: This kind of support is equivalent to passive SYN flood protection; the router does not actively reset the connection.

- Removal of connections that have been idle for a configured length of time.
- Verification of TCP flags on a packet-by-packet basis.
- Monitoring of TCP sequence and ACK numbers for out-of-range packets.

UDP Support

To support UDP flows, the JUNOSe stateful firewall supports the following:

- Ability to recognize the start of a new flow using a new 5-tuple on the trusted side of a firewall.
- Ability to add the new flow to the flow table and recognize the return flow.
- Monitoring the flow for the last access time (for timeout purposes).
- Monitoring the number of unidirectional flows from a host and blocking the offending host if the flows exceed the configured threshold.
- Removal of flows that have been idle for a configured length of time.
- Verification of the UDP length with respect to the IP length.

ICMP Support

When ICMP flows are enabled, the JUNOSe stateful firewall supports flows from trusted networks for echo request and timestamp request messages. Responses to these flows are allowed when the outgoing request is matched based on the source, destination, protocol, and session ID. Also, when related to an established connection, the ICMP firewall support allows ICMP error messages (that is, ICMP destination-unreachable and time-exceeded messages) to pass through. All other ICMP request types are blocked.

Inspection List and Half-Open Connection Support

Firewalls must apply rules to determine whether or not a connection is allowed. You determine these rules by configuring inspection lists and half-open table parameters. When a user configures an interface to have an inspection list, that list (or lists, when you configure both an ingress and egress list) controls the types of traffic (for example, protocols or ports) that are allowed to traverse the firewall.

Attaching an inspection list to the ingress channel of an interface establishes traffic received on that interface as trusted. That is, the interface allows traffic flows that receives on the interface to pass through the firewall. Attaching an inspection list to the egress channel of an interface establishes traffic routed to the interface as trusted. That is, the interface allows internally routed traffic flows to pass through the firewall.

In addition, the firewall also uses the half-open table to monitor connections. The half-open table allows for DoS mitigation, by limiting the number of half-open connections at any given time.

Application-Level Inspection Support

Firewalls may need application-level gateway (ALG) support for the following reasons:

- When using Network Address Translation (NAT) in conjunction with a firewall, the application may include information in the data stream that includes IP addresses or TCP/UDP ports. Because NAT changes the addressing information in the header of a packet, for the application to function properly, the data stream must be adjusted accordingly. For firewall configurations that do not include NAT, this adjustment is not an issue.

- The application may consider multiple TCP/UDP connections to be part of a single *session*. In this instance, a host outside the trusted network may initiate one or more of the connections based on signaling data from the host on the trusted network and, as a result, would be denied passage by the firewall. A classic example of this is the use of FTP, in which the server actually creates the data connection. The firewall must inspect the control connection to allow the incoming data connection.

- The application may suffer from some application-level attacks that may trigger the firewall to protect the network. In this case, the firewall must inspect the data stream, and modify it, to avert the attack. An example of this is an FTP *man-in-the-middle* attack, in which a third host (not part of the initial client server connection) is specified as the recipient of the data stream. The JUNOSe firewall prevents third-party transfers.

NOTE: This release supports only ALGs for FTP.

The stateful firewall allows the ALGs to install new flows as needed for the application to function correctly.

Audit Trails

Because firewalls typically reside at the edge of a network, they can provide useful information about the use of network resources. As a result, firewalls can provide audit information.

NOTE: JUNOSe software can provide audit information, when configured, by using the flowServicesFirewallAudit log.

Safe IP Fragmentation

IP fragments can be used to perpetrate several types of attacks on a network (for example, the *teardrop attack*). Unfortunately, turning off IP fragmentation is not always an option. To ward against attacks that use fragmentation, the JUNOSe stateful firewall supports virtual reassembly for TCP and UDP packets, as well as reassembly and forwarding of ICMP packets.

With virtual reassembly, the router keeps a state entry for each set of fragments (datagram; initial fragments create an entry in the state table). The router verifies other fragments to be correct (based on state table information) and forwards them. In addition, the initial fragment must include the complete TCP or UDP header to mitigate the tiny fragment attack. The router times out any remaining state entries that exist for any incomplete fragments (datagram).

Because some networks may cause reordering of fragments (initial fragments may not be received first), and result in the virtual reassembly feature dropping fragments, this solution may not be ideal for all networks.

For ICMP reassembly and forwarding, the router buffers all fragments, reassembles them, and forwards only complete and correct packets.

DMZ Support

The DMZ (demilitarized zone), sometimes referred to as the service network, is a firewall concept in which a small, physically separated section of the trusted network is used to host connections from the untrusted network. An example is a Web server for a company on which incoming connections are allowed.

The need to provide access means that the network may be subject to external DoS attacks. The JUNOSe stateful firewall can provide protection against these attacks.

You can protect the DMZ in several ways, including the following:

- Using a normal policy list that you configure to allow access to only certain services.
- Defining rate limits at the physical interface.
- Configuring the JUNOSe stateful firewall to provide DoS protections (for example, against SYN flood).

Using a DMZ does not exclude the ability to use firewall functionality elsewhere in your network. By using a combination of ingress and egress firewall configurations, you can create a DMZ and have specific servers, containing specific applications, behind the firewall.

Platform Considerations

For information about modules that support Firewall on ERX-14xx models, ERX-7xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support Firewall.

NOTE: The E120 router and the E320 router do not support configuration of Firewall.

Module Requirements

To configure a firewall, you must install a Service Module (SM). For information about installing modules in the ERX router, see the *ERX Hardware Guide*.

Unlike other line modules, SMs do not pair with corresponding I/O modules that contain ingress and egress ports. Instead, they receive data from and transmit data to other line modules with access to ingress and egress ports on their own associated I/O modules.

For a list of the modules that support firewall, see *ERX Module Guide, Appendix A, Module Protocol Support*.

Configuring a Firewall License

You must configure a firewall license before you can use any firewall commands on the ERX router.

license firewall maximum-virtual-routers

- Use to specify a firewall license.
- Purchase a firewall license to allow firewall configuration on the ERX router.

NOTE: Firewall licensing is enforced according to a tiered structure based on the number of VR/VRF instances in which you can configure stateful firewall. Acquire the license from Juniper Networks Customer Service or your Juniper Networks sales representative.

- Example

  host1(config)#**license firewall maximum-virtual-routers** *license-value*

- Use the **no** version to disable the license.

Configuring Stateless Firewall

You can use Juniper Networks policy management to configure stateless access control. For example, to stop all ICMP packets from entering the network (192.168.10.0/24), except for echo request and reply messages, you use the following command sequence:

host1(config)#**ip classifier-list 111 icmp any 192.168.10.0 0.0.0.255 8**
host1(config)#**ip classifier-list 111 icmp any 192.168.10.0 0.0.0.255 0**
host1(config)#**ip policy-list 111**
host1(config-policy-list)#**classifier-group 111**
host1(config-policy-list-classifier-group)#**forward**
host1(config-policy-list-classifier-group)#**exit**
host1(config-policy-list)#**classifier-group 112**
host1(config-policy-list-classifier-group)#**forward**
host1(config-policy-list-classifier-group)#**exit**
host1(config-policy-list)#**exit**
host1(config)#**interface fastEthernet 8/0**
host1(config-if)#**ip policy input 111**

For additional information about using Juniper Networks policy management, classifier lists, and policy lists, see *JUNOSe Policy Management Configuration Guide, Chapter 1, Managing Policies on the E-series Router*.

Configuring Stateful Access Control

To configure stateful access control, you can define certain timeout values, limit the number of half-open connections, and change the default alert, as well as enable an audit trail and define inspection lists.

Defining Flow Timeout Values

The JUNOSe stateful firewall enables you to define timeout values for specific states of a Domain Name System (DNS), ICMP, TCP, and UDP flow.

ip inspect dns-timeout

- Use to define the DNS timeout value, in seconds, for DNS flows.
- Example

  host1(config)#**ip inspect dns-timeout 300**

- Use the **no** version to restore the default value of 5 seconds.

ip inspect icmp idle-time

- Use to define the idle-time value, in seconds, for ICMP flows.
- Example

  host1(config)#**ip inspect icmp idle-time 5000**

- Use the **no** version to restore the default value of 10 seconds.

ip inspect tcp

- Use to define one of the following TCP timeout values:
  - synwait-time—Length of time, in seconds, the software waits for a TCP session
  - finwait-time—Length of time, in seconds, a TCP session is managed after the firewall detects a FIN-exchange
  - idle-time—Length of time, in seconds, a TCP session is managed following no activity
- Example 1

  host1(config)#**ip inspect tcp synwait-time 55**

- Example 2

  host1(config)#**ip inspect tcp finwait-time 20**

- Example 3

  host1(config)#**ip inspect tcp idle-time 6000**

- Use the **no** version to restore the default value of the timer.

ip inspect udp idle-time

- Use to define the idle-time value, in seconds, for UDP flows.
- Example

  host1(config)#**ip inspect udp idle-time 100**

- Use the **no** version to restore the default value of 30 seconds.

Limiting the Number of Half-Open Sessions

You can specify limits for the number of concurrent half-open sessions and the session establishment rate for those sessions. For TCP connections, you can also specify a limit for any destination host, as well as block connections to a targeted host after reaching that limit.

ip inspect max-incomplete

- Use to define the number of half-open (incomplete) sessions that cause the router to start deleting half-complete sessions (the high value) and stop deleting half-complete sessions (the low value).
- When the high value is reached, the router drops the oldest half-open session before it allows a new one.
- When the low value is reached, the router no longer drops half-open sessions before it allows new sessions.
- Example 1

  host1(config)#**ip inspect max-incomplete high 800**

- Example 2

  host1(config)#**ip inspect max-incomplete low 200**

- Use the **no** version to restore the high default value (500) or low default value (400).

ip inspect one-minute

- Use to define the connection establishment rate at which the router starts deleting half-complete sessions (the high value) and stops deleting half-complete sessions (the low value).
- When the high value is reached, the router drops the oldest half-open session before it allows a new one.
- When the low value is reached, the router no longer drops half-open sessions before it allows new sessions.
- Example 1

  host1(config)#**ip inspect one-minute high 800**

- Example 2

  host1(config)#**ip inspect one-minute low 200**

- Use the **no** version to restore the high default value (500) or low default value (400).

ip inspect tcp max-incomplete host

- Use to define the maximum number of half-open TCP connections that the router allows to the same destination before it begins removing sessions, and an amount of time that the router disallows all connections to an affected host after removing sessions to that host.
- A block-time value of zero (the default) begins removing the oldest incomplete sessions as the router meets the specified limit for half-open TCP connections to a specific host.
- A positive block-time value removes all half-open TCP connections when the specified limit is reached, and disallows connections to that host for the specified amount of time.
- Example

  host1(config)#**ip inspect tcp max-incomplete host 3000 block-time 3**

- Use the **no** version to restore the session number default value (250) or the block-time default value (0).

Defining Alert Status and Audit Trails

Stateful firewall functionality allows you to enable or disable alert and audit trail logging.

The router generates alerts when a problem appears in either a connection attempt or with some internal resource. The alerts appear in a system event log and provide various messages.

The router generates audit trail log information when you enable the audit trail functionality. When you enable the audit trail, the router places flow-specific information into the system event log. This information includes timestamp, source and destination addresses, and port and protocol information for each connection.

For additional information about monitoring system logs, see the *JUNOSe System Event Logging Reference Guide*.

ip inspect alert-off

- Use to disable the inspect alert control behavior for the virtual router.
- Example

  host1(config)#**ip inspect alert-off**

- Use the **no** version to reenable the alert control.

ip inspect audit-trail

- Use to enable the inspect audit trail control behavior for the virtual router.
- Example

  host1(config)#**ip inspect audit-trail**

- Use the **no** version to disable the audit trail control.

Creating and Adding to an Inspection List

Use the **ip inspect name** command to create and add context-based access control rules to an inspection list.

ip inspect name

- Use to create and add to an inspection list.
- Example

  host1(config)#**ip inspect name list1 alert on audit-trail on timeout 500**

- Use the **no** version to delete the inspection list or remove a specific value from the inspection list.

Associating an Inspection List with an Interface

Use the **ip inspection** command to associate an inspection list with an IP interface. For ingress inspection lists, the router applies the rules of the associated inspection list to all of the packets it receives on this interface. For egress inspection lists, the router applies the rules of the associated inspection list to all packets to be transmitted on the interface.

ip inspection

- Use to associate an inspection list with the ingress (in) or egress (out) side of the IP interface.
- Example

  host1(config-if)#**ip inspection list1 in**

- Use the **no** version to remove the inspection list association with this interface.

Monitoring Stateful Firewall

This section shows how to set a stateful firewall statistics baseline, lists the system event logs associated with the stateful firewall feature, and describes the **show** commands you can use to view inspection lists, inspection parameters, current sessions, firewall configuration, license information, and firewall-related statistics.

System Event Logs

To troubleshoot and monitor your firewall, use the following system event logs:

- flowInspection
- flowServicesFirewallAudit
- flowServicesFirewallAlert

For more information about using event logs, see the *JUNOSe System Event Logging Reference Guide*.

Establishing a Baseline for Firewall Statistics

You can establish a baseline for firewall statistics by setting a group of reference counters to zero. The router implements the baseline by reading and storing the statistics at the time the baseline is set, and then subtracting this baseline whenever you retrieve baseline-relative statistics.

baseline ip inspection global

- Use to set a statistics baseline for global firewall statistics.
- Use the **delta** keyword with IP **show** commands to specify that baselined statistics are to be shown.
- Example

  host1#**baseline ip inspection global**

- There is no **no** version.

baseline ip inspection name

- Use to set a statistics baseline for the specified inspection list.
- Use the **delta** keyword with IP **show** commands to specify that baselined statistics are to be shown.
- Example

  host1#**baseline ip inspection name list1**

- There is no **no** version.

Viewing Firewall Information

You can monitor the following aspects of IP by using **show ip** commands:

To Display	Command
Firewall inspection lists	**show ip inspect**
All inspection parameters	**show ip inspect config**
Information for a specified inspection list	**show ip inspect name**
Current sessions being tracked by the stateful firewall	**show ip inspect session**
All firewall-related statistics	**show ip inspect statistics**
Firewall license information	**show license firewall**

To set a statistics baseline for stateful firewall, use the **baseline ip inspection global** and **baseline ip inspection name** commands. Use the **delta** keyword with firewall **show** commands to specify that baselined statistics are to be shown.

You can use the output filtering feature of the **show** command to include or exclude lines of output based on a text string that you specify. See *JUNOSe System Basics Configuration Guide, Chapter 2, Command-Line Interface*, for details.

show ip inspect

- Use to display firewall configuration and sessions.
- Field descriptions
  - Inspection List—Name of the inspection list
  - Time since counters last reset—Length of time since the statistical counters were last reset
  - Number of connections permitted—Number of sessions allowed for any interface with which this inspection list is associated
  - Number of current connections—Number of current sessions
  - Number of interfaces using—Number of interfaces using this inspection list
  - Application [*application*]—Audit trail control state, alert control state, and idle timeout value for each application configured in the inspection list
  - Referenced by Profile(s)—Name of any profile that references this inspection list and the interface direction (ingress or egress) for which the inspection list applies
- Example

```
host1#show ip inspect
Inspection Lists:
    (Inspection List Information Spans all virtual routers)
    Inspection List     listin
            Time since counters last reset: 04:44:07
            Number of connections permitted 1

            Number of current connections 1
            Number of interfaces using 1
        Application TCP
            Auditing follows router state
            Alerting follows router state
            Timeout set to: 3000
        Application UDP
            Auditing follows router state
            Alerting follows router state
            Timeout set to: 30
        Application ICMP
            Auditing follows router state
            Alerting follows router state
            Timeout set to: 10
        Application Ftp
            Auditing follows router state
            Alerting follows router state
            Timeout set to: 3600

        Referenced by Profile(s):
            foo (ingress)

    Inspection List     listout
            Time since counters last reset: 00:01:33
            Number of connections permitted 0
            Number of current connections 0
            Number of interfaces using 0
        Application TCP
            Auditing follows router state
            Alerting follows router state
            Timeout set to: 3000
```

```
Application Http
    Auditing follows router state
    Alerting follows router state
    Timeout set to: 3600

Referenced by Profile(s):
    foo (egress)
```

show ip inspect config

- Use to display all inspection parameters.
- Field descriptions
  - Global Firewall Parameters
    - Alert—Status of alert logging at the router level
    - Audit trail—Status of audit trail logging at the router level
    - Syn-Wait Time—Amount of time the software waits for a TCP session
    - Fin-Wait Time—Amount of time a TCP session is managed after the firewall detects a FIN-exchange
    - Tcp Idle Time—TCP idle timer value
    - Udp Idle Time—UDP idle timer value
    - Icmp Idle Time—ICMP idle timer value
    - Dns Time—DNS timer value
    - Max Incomplete High—Max-incomplete high value
    - Max Incomplete Low—Max-incomplete low value
    - One Minute High—One-minute high value
    - One Minute Low—One-minute low value
    - Max Host Number—Maximum number of half-complete TCP sessions that the router allows to the same destination before it begins removing sessions
    - Max Host Block Time—Amount of time that the router disallows connection to affected hosts after removing sessions to those hosts
  - Inspection List—Name of the inspection list
  - Application [*application*]—Audit trail control state, alert control state, and idle timeout value for each application configured in the inspection list
  - Referenced by Profile(s)—Name of any profile that references this inspection list and the interface direction (ingress or egress) to which the inspection list applies
  - Interface Attachments—Interfaces with which the inspection lists are associated

- Example

```
host1#show ip inspect config
Global Firewall Parameters

Alert is on
Audit trail is off
Syn-Wait Time:          30
Fin-Wait Time:          5
Tcp Idle Time:          3000
Udp Idle Time:          30
Icmp Idle Time:         10
Dns Time:               5
Max Incomplete High:    500
Max Incomplete Low:     400
One Minute High:        500
One Minute Low:         400
Max Host Number:        250
Max Host Block Time:    0

Inspection Lists:
    (Inspection List Information Spans all virtual routers)
    Inspection List     listin
        Application TCP
            Auditing follows router state
            Alerting follows router state
            Timeout set to: 3000
        Application UDP
            Auditing follows router state
            Alerting follows router state
            Timeout set to: 30
        Application ICMP
            Auditing follows router state
            Alerting follows router state
            Timeout set to: 10
        Application Ftp
            Auditing follows router state
            Alerting follows router state
            Timeout set to: 3600

        Referenced by Profile(s):
            foo (ingress)

    Inspection List     listout
        Application TCP
            Auditing follows router state
            Alerting follows router state
            Timeout set to: 3000
        Application Http
            Auditing follows router state
            Alerting follows router state
            Timeout set to: 3600

        Referenced by Profile(s):
            foo (egress)

Interface Attachments

Interface: ATM10/0.1  (ingress) listin
```

show ip inspect name

- Use to display information about a specified inspection list.
- Field descriptions
  - Inspection List—Name of the inspection list
  - Time since counters last reset—Length of time since the statistical counters were last reset
  - Number of connections permitted—Number of sessions allowed for any interface with which this inspection list is associated
  - Number of current connections—Number of current sessions
  - Number of interfaces using—Number of interfaces using this inspection list
  - Application [*application*]—Audit trail control state, alert control state, and idle timeout value for each application configured in the inspection list
  - Referenced by Profile(s)—Name of any profile that references this inspection list and the interface direction (ingress or egress) to which the inspection list applies
- Example

```
host1#show ip inspect name listin
    Inspection List     list1
        (Information spans all virtual routers)

            Time since counters last reset: 04:44:04
            Number of connections permitted 1

            Number of current connections 1
            Number of interfaces using 1
        Application TCP
            Auditing follows router state
            Alerting follows router state
            Timeout set to: 3000
        Application UDP
            Auditing follows router state
            Alerting follows router state
            Timeout set to: 30
        Application ICMP
            Auditing follows router state
            Alerting follows router state
            Timeout set to: 10
        Application Ftp
            Auditing follows router state
            Alerting follows router state
            Timeout set to: 3600
        Application RTSP
            Auditing follows router state
            Alerting follows router state
            Timeout set to: 3600

        Referenced by Profile(s):
            foo (ingress)
```

show ip inspect session

- Use to display the current sessions being tracked by the stateful firewall.
- Field descriptions
  - Entry—Table entry number
  - Source—Source address
  - Destination—Destination address
  - Prot—Protocol operating over this session (TCP, UDP, or ICMP)
  - Time since Creation—Time elapsed since this session was created
  - Time since last use—Time elapsed since this session was last used
  - Inspection Name—Name of the inspection list used to allow this session
  - Application Used—Configured application in the inspection list that was used to allow this session
- Example

```
host1#show ip inspect session
                                                  Time       Time
                                                 since      since    Inspection
Entry       Source        Destination    Prot  Creation   last use     Name
------ ---------------- ---------------- ---- ---------- ---------- ----------
1      10.1.1.1:1038    13.1.1.1:23      TCP  00:00:49   00:00:07   listin
       Application
Entry     Used
------ -----------
1      TCP
```

show ip inspect statistics

- Use to display the current statistics being tracked by the stateful firewall.
- Field descriptions
  - Current Information
    - Number of blocked destinations—Number of destinations blocked by the firewall
    - Size of the half open table—Number of half-open connections in the half-open table
  - Statistics
    - Time since last reset—Time elapsed since last statistics were reset
    - Evaluations—Total number of evaluations performed
    - Permits—Total number of permits allowed
    - Denies by rule—Total number of denials based on inspection list rules
    - Denies due to blocked destinations—Total number of denials due to blocked destinations
    - Evaluate permitted but no resources—Total number of evaluations permitted but not performed due to resource constraints
    - Denies for other reasons—Total number of denials that occurred for reasons not mentioned above

- Packets forwarded through firewall—Total number of packets forwarded through the firewall
- Bytes forwarded through firewall—Total number of bytes forwarded through the firewall
- Packets discarded (flow control error)—Total number of packets discarded for flow control errors
- Packets discarded (packet error)—Total number of packets discarded for packet errors
- Packets discarded (reassembly)—Total number of packets discarded for reassembly errors
- Packets discarded (other)—Total number of packets discarded for packet errors other than those mentioned above
- Deleted half open connections—Total number of deleted half-open connections
- Total blocked destinations—Total number of blocked destinations
- Transitions into rate flood protection—Total number of times the firewall has entered into rate flood protection because the number of half-open sessions exceeded the configured maximum value
- Transitions out of rate flood protection—Total number of times the firewall has ceased rate flood protection because the number of half-open sessions returned to below the configured maximum value
- Transitions into size flood protection—Total number of times the firewall has entered into SYN flood protection because the number of half-open sessions exceeded the configured maximum value
- Transitions out of size flood protection—Total number of times the firewall has ceased SYN flood protection because the number of half-open sessions returned to below the configured maximum value

  - Dynamic Translation Type—Always reads “fully extended” to indicate a 5-tuple entry
  - Current—Number of current sessions
  - Peak—Number of peak concurrent sessions
  - Accumulated—Total number of sessions
  - Failed—Number of times the router could not create a session

- Example

```
host1#show ip inspect statistics
Virtual Router Statistics
Current Information
        Number of blocked destinations: 0
        Size of the half open table:    0

Statistics
Time since last reset 04:41:27
Evaluations                             : 3
Permits                                 : 3
Denies by rule                          : 0
Denies due to blocked destinations      : 0
Evaluate permitted but no resources     : 0
Denies for other reasons                : 0
```

```
Packets forwarded through firewall      : 28
Bytes forwarded through firewall        : 1770

Packets discarded (flow control error)  : 0
Packets discarded (packet error)        : 0
Packets discarded (reassembly)          : 0
Packets discarded (other)               : 2

Deleted half open connections           : 0
Total blocked destinations              : 0
Transitions into rate flood protection  : 0
Transitions out of rate flood protection: 0
Transitions into size flood protection  : 0
Transitions out of size flood protection: 0


  Dynamic Translation Type     Current       Peak     Accumulated    Failed
----------------------------  ----------  ----------  -----------  ----------
Fully Extended                         1           1            3           0
```

show license firewall

- Use to display the firewall license key configured on the router.
- Example

```
host1#show license firewall
Firewall license is firewall_license
```