SUPPORTED ON AR720 ONLY

Chapter 31

# Firewall

# Introduction

This chapter describes the router's built-in firewall facility, and how to configure and monitor the firewall.

The Internet is a network which allows access to vast amounts of information and potential customers. However, the Internet is not controlled and certain individuals use it destructively. These individuals attack other user's computer systems for entertainment and/or profit.

A firewall is a security device designed to allow safe access to the Internet by enforcing a set of access rules between the various interfaces of the product. Typically a firewall has two interfaces—one interface is attached to the public network (e.g. the Internet), and the other interface is attached to an internal private network (intranet) which requires protection. The firewall prevents unrestricted access to the private network and protects the computer systems behind the firewall from attack.

Because a firewall provides a single link between the private network and the public network, a firewall is also uniquely positioned to provide a single point where all traffic in to and out of the private network can be logged and monitored. This information is useful for providing a security audit trail.

Currently two main firewall technologies are recognised:

- Application Gateway
  This is the traditional approach used to build a firewall, where every connection between two networks is made via an application program (called a *proxy*) specific for that protocol. A session from the private network is terminated by the proxy, which then creates another separate session to the end destination. Typically, a proxy is designed with a detailed knowledge of how the protocol works and what is and is not allowed. This approach is very CPU intensive and very restrictive. Only protocols that have specific proxies configured are allowed through the firewall; all other traffic is rejected. In practice most third-party proxies are transparent proxies which pass all traffic between the two sessions without regard to the data.
- Stateful Inspection
  A more recent approach to firewall design uses a method called "*stateful inspection*". Stateful inspection is also referred to as *dynamic packet filtering* or *context-based access control* (CBAC). In this technology, an inspection module understands data in packets from the network layer (IP headers) up to the application layer. The inspection module checks every packet passing through the firewall and makes access decisions based on the source, destination and service requested. The term *stateful* refers to the firewall's ability to remember the status of a flow, for example, whether a packet from the public Internet is returning traffic for a flow originated from the private intranet. The TCP state of TCP flows is also monitored, allowing inappropriate traffic to be discarded. The benefit of this approach is that stateful inspection firewalls are generally faster, less demanding on hardware and more adaptive to new Internet applications.

The router's firewall implementation has the following features:

- Dynamic packet filtering (stateful inspection) technology.
- Application of dynamic filtering to traffic flows, using the base rule that all access from the outside (i.e. public interfaces) is denied unless specifically permitted and all access from the inside (i.e. private interfaces) is allowed unless specifically denied.

- The firewall will open only the required ports for the duration of a user session. Configuration commands are required to allow access to internal hosts from a public interface.
- The firewall intercepts all TCP connections and completes the connection. This feature better tracks and defends against denial of service attacks by depletion of TCP slots. Any further out-of-sequence TCP frames are dropped.
- The firewall can be configured to limit internal access to the public network based on a policy setting.
- The generation of unreachable ICMP messages can be enabled or disabled.
- All firewall events can be selectively logged to the Logging Facility.
- Significant firewall events generate notifications to designated destinations including SNMP traps, triggers which can be configured to activate scripts, an email address or an asynchronous port.
- The firewall supports protocols such as FTP, Progressive Networks' RealAudio, Xing Technologies' Streamworks, White Pines' CuSeeMe, VDOnet's VDOLine, Microsoft's NetShow, NETBIOS, GRE, OSPF, PPTP and RSVP.
- The firewall detects and logs a range of denial of service attacks including SYN and FIN flooding, Ping of death (illegal ping packet sizes, or an excessive number of ICMP messages), Smurf attacks (packets with an IP address of the private network and typically a broadcast address) and port scans.
- An accounting facility records, via the Logging Facility, the traffic flow for an individual session.

*The firewall affects only IP-based protocols. It does not affect IPX, DECnet and AppleTalk network protocols.*

## Policies

The first step in deploying a firewall is to determine exactly what traffic should be allowed and what traffic should be denied. This is called the *security policy.* The security policy will contain rules that specify the particular types of traffic that are or are not allowed to pass through the firewall.

The configuration of the firewall is based around this concept of a security policy.

The firewall is enabled or disabled using the commands:

```
ENABLE FIREWALL
DISABLE FIREWALL
```

The current status and configuration summary can be displayed using the command:

```
SHOW FIREWALL
```

A policy is created or destroyed using the commands:

```
CREATE FIREWALL POLICY=name
DESTROY FIREWALL POLICY=name
```

The firewall will not become active until at least one public and one private interface have been assigned to the policy. A public interface is an interface attached to a public network such as the Internet. A private interface is an interface attached to a private network, such as a company intranet, behind the firewall. The basic function of a firewall is to control the forwarding of traffic between the public interface and the private interface. Interfaces are added to or removed from a policy using the commands:

```
ADD FIREWALL POLICY=name INTERFACE=interface TYPE={PUBLIC|
    PRIVATE} [METHOD={DYNAMIC|PASSALL}]
DELETE FIREWALL POLICY=name INTERFACE=interface
```

An interface can only be defined as private in one security policy. An interface can only be defined as public in up to two security policies. Once at least one private interface and one public interface have been added, the firewall will be functional and will automatically implement the default policy rules:

- All flows originating from inside (i.e. private interfaces) are allowed. When a sessions is initiated from a private interface to an outside IP host and has been allowed by the firewall, traffic for that session can flow in both directions. When the session completes no further traffic is accepted to that private IP host on that port.
- All flows originating from the outside (i.e. public interfaces) are blocked.
- All traffic from an interface not specifically covered by policy, to an interface specified in a policy as private will be dropped.
- All traffic between interfaces not specifically covered by a policy will be passed as normal.

The current status and configuration of a policy or all policies can be displayed using the command:

```
SHOW FIREWALL POLICY=name [SUMMARY] [COUNTERS]
```

To further refine the control over flows to and from the public network, rules are added to the policy to allow or deny specific types of traffic.

## Rules

Policy rules are used to refine the default security policy, which denies all access from hosts on the public network to hosts on the private network but allows all access from hosts on the private network to hosts on the public network.

Policy rules define precisely when and how traffic can flow through the firewall, based on IP addresses, port numbers, day of the week, or time of day. For example, if a mail server is running on the private network, a rule could be added to allow TCP traffic to port 25 (the SMTP port) on the mail server host.

A rule is added to or deleted from a policy using the commands:

```
ADD FIREWALL POLICY=name RULE=rule-id ACTION={ALLOW|DENY}
    INTERFACE=interface PROTOCOL={protocol|ALL|EGP|GRE|ICMP|
    OSPF|SA|TCP|UDP} [AFTER=hh:mm] [BEFORE=hh:mm] [DAYS={MON|
    TUE|WED|THU|FRI|SAT|SUN|WEEKDAY|WEEKEND}[,...]]
    [GBLIP=ipadd] [GBLPORT={ALL|port[-port]}]
    [IP=ipadd[-ipadd]] [LIST={list-name|RADIUS}] [PORT={ALL|
    port[-port]|service-name}] [REMOTEIP=ipadd[-ipadd]]
    [SOURCEPORT={ALL|port[-port]}]
```

```
DELETE FIREWALL POLICY=name RULE=rule-id
```

An existing rule can be modified using the command:

```
SET FIREWALL POLICY=name RULE=rule-id [PROTOCOL={protocol|
   ALL|EGP|GRE|ICMP|OSPF|SA|TCP|UDP}] [AFTER=hh:mm]
   [BEFORE=hh:mm] [DAYS={MON|TUE|WED|THU|FRI|SAT|SUN|
   WEEKDAY|WEEKEND}[,...]] [GBLIP=ipadd] [GBLPORT={ALL|
   port[-port]}] [IP=ipadd[-ipadd]] [PORT={ALL|port[-port]|
   service-name] [REMOTEIP=ipadd[-ipadd]] [SOURCEPORT={ALL|
   port[-port]}]
```

In addition to rules based on IP address, port, protocol, date and time, the processing of ICMP packets, IP packets with options set and ping packets can be enabled or disabled on a per-policy basis using the commands:

```
ENABLE FIREWALL POLICY=name [ICMP_FORWARDING={ALL|PARAMETER|
   PING|REDIRECT|SOURCEQUENCH|TIMEEXCEEDED|TIMESTAMP|
   UNREACHABLE}] [OPTIONS={ALL|RECORD_ROUTE|SECURITY|
   SOURCEROUTE|TIMESTAMP}] [PING]

DISABLE FIREWALL POLICY=name [ICMP_FORWARDING={ALL|PARAMETER|
   PING|REDIRECT|SOURCEQUENCH|TIMEEXCEEDED|TIMESTAMP|
   UNREACHABLE}] [OPTIONS={ALL|RECORD_ROUTE|SECURITY|
   SOURCEROUTE|TIMESTAMP}] [PING]
```

The currently configured rules for a policy can be displayed using the command:

```
SHOW FIREWALL POLICY=name
```

Rules are processed in order from the lowest number to the highest number. If rules both deny and allow an activity, the rule with the lowest number takes precedence. Typically, rules specify the access to or from a particular IP address and port. Controlling access to many destinations could require a large number of commands. The firewall solves this problem by providing support for lists of addresses stored in files in the routers file subsystem or on a RADIUS server. A rule can be configured to allow or deny access to addresses in up to four lists or RADIUS servers. See “*Access Lists*” on page 31-7 for more information about configuring access lists.

Rules are processed as follows:

1. Based on the direction of the new flow or session, the default access result is set to the case of no matching rules. For new sessions or flows originating from a private network, access is set to *allowed*. For sessions and flows originating from a public network, access is set to *denied*. Each rule is then matched to the new flow or session until either a match is found or all rules have been rejected as not applicable, in which case the default access is used.
2. The protocol of the new flow is checked against the protocol field of the rule. If there is no match then the rule is rejected as not applicable.
3. The destination port is then matched to the rule port range. If there is no match then the rule is rejected as not applicable.
4. The source port is then matched to the rule’s source port range if it is set. The source port used is dependent on the direction of the flow. For flows from a private network the source port of the flow is used. For flows from the public network, the destination port is used. If there is no match then the rule is rejected as not applicable.
5. The new flow’s remote IP address is then matched to the rule’s remote IP address or range if it is set. The remote IP address used is dependent on the

direction of the flow. For flows from a private network the remote IP address used is the destination IP address of the flow. For flows from the public network, the source IP address if the flow is matched to the remote IP address of the rule. If there is no match then the rule is rejected as not applicable.

6. The new flow's IP address is matched to the rule's IP range or global IP address. If there is no match then the rule is rejected as not applicable. The IP address used is dependent on the direction of the flow. For flows from a private network the IP address used is the source IP address of the flow. For flows from the public network, the destination IP address is matched either to the IP address of the rule or to the global IP address set for the rule, depending on whether or not NAT is being applied to the interface.

7. If the IP address matches the rule then the time period is checked against allowed times for the rule. If the current time is not within the specified time range for the rule then the rule is rejected as not applicable.

8. If a hardware list or lists have been specified for the rule and the rule has been applied to an Ethernet interface, then the hardware lists are checked for a match to the source MAC address of the new flow. If there is no match then the rule is rejected as not applicable.

9. If an IP list or lists have been specified for the rule, then the lists are checked for a match to either the destination IP address for new flows started from the private network, or the source address for new flows started from the public network.

   If there are no IP lists or RADIUS servers set, and the rule action is ALLOW, then the new flow is allowed. If the rule action is to DENY then the flow is denied. Similarly, if there are IP lists and a match is found, and the rule action is ALLOW the new flow is ALLOWED. If the rule action is DENY then the flow is denied.

10. If there are IP lists and there is no match, and RADIUS is not set, then if the rule action is ALLOW the new flow is denied. If the rule action is DENY then the flow is allowed.

11. Finally, if there are IP lists and there is no match, and RADIUS is set, then the new flow is placed in a queried state and a request is passed to a RADIUS server to determine if the new flow is to be allowed or denied. RADIUS server responses are interpreted as follows:

    - If the rule action is ALLOW and the RADIUS server either rejects the request or returns an IP address of 0.0.0.0, then the flow will be denied.
    - If the rule action is ALLOW and the RADIUS server accepts the request and returns a valid IP address then the flow will be allowed.
    - If the rule action is DENY and the RADIUS server either rejects the request or returns a valid IP address, then the flow will be allowed.
    - If the rule action is DENY and the RADIUS server accepts the request and returns an IP address of 0.0.0.0 then the flow will be denied.

    See "*RADIUS Servers*" on page 31-8 for a detailed description of the format of RADIUS requests and RADIUS database entries.

# Access Lists

Access lists are lists of addresses to which access is controlled by one or more policy rules. The firewall supports two mechanisms for storing and managing access lists—list files stored in the router's file subsystem and RADIUS servers.

## List Files

A list file is an ASCII text file with a `.TXT` stored on the router's file subsystem and containing a list of addresses. List files are more suited to small lists of addresses that remain relatively static. Two types of list files can be used—IP address lists and hardware address lists.

An IP list file contains a list of IP host and network addresses. Lines in an IP address file have the following format:

- A single IP address in dotted decimal notation; *or*
- A single IP address in dotted decimal notation, followed a space or tab and the name of the host; *or*
- A comment character "#" followed by comment text; *or*
- A range of IP addresses in dotted decimal notation separated by a hyphen, optionally followed by a text name.

For example, the file LISTIP.TXT might contain the following:

```
202.36.163.6
202.49.72.92 aslan.somewhere.com # FTP host
# access for an entire network
202.36.163.0 - 202.36.163.255 dummy network
```

A hardware address list file contains a list of hardware addresses. Lines in a hardware address file have the following format:

- A single MAC address in standard notation.
- A single MAC address in standard notation, followed by a space or tab and the name of the host.
- The comment character "#" followed by arbitrary text.

For example, the file LISTMAC.TXT might contain the following:

```
00-00-f4-02-03-01
00-00-f4-02-03-01 pc1.somewhere.com # FTP host
# a comment line
```

A list file is added to or deleted from a policy using the commands:

```
ADD FIREWALL POLICY=name LIST=list-name FILE=filename
    TYPE={IP|ADDRESS}
```

where *name* is the name of the policy, *list-name* is a user-defined name for the list and *filename* is the name of the file on the router's file subsystem. A rule is created to provide access control for the addresses in a list using the command:

```
ADD FIREWALL POLICY=name RULE=rule-id ACTION={ALLOW|DENY}
    INTERFACE=interface PROTOCOL={protocol|ALL|EGP|GRE|ICMP|
    OSPF|SA|TCP|UDP} LIST=list-name [other-options...]
DELETE FIREWALL POLICY=name LIST=list-name
```

Up to four lists can be added to a single rule using multiple invocations of the command:

```
ADD FIREWALL POLICY=name RULE=rule-id LIST=list-name
```

## RADIUS Servers

There are situations where it is necessary or desirable to control access to a large number of addresses, but impractical to store these addresses in a list file on the router. A typical example would be an organisation wanting to allow general access to the web but restrict access to specific web sites. Several entities have complied lists of web sites that individuals or groups may find objectionable. These can be very large and are often updated regularly. A RADIUS server is an ideal place to store such lists.

The firewall can be configured to use one or more RADIUS servers to perform checks on user access rights. If a LIST of type RADIUS is specified for a rule, and a RADIUS server has been configured, the router makes RADIUS requests of the form:

```
User-Name [ipadd]
```

```
User-Password allowdeny
```

where *ipadd* is the source or destination IP address of the new flow, depending on the direction of the flow.

The RADIUS server entry to specifically deny access looks like:

```
[ipadd] Password = “allowdeny”, Framed-Address = 0.0.0.0
```

The RADIUS server entry to specifically allow access looks like:

```
[ipadd] Password = “allowdeny”, Framed-Address = ipadd
```

Once the RADIUS server has been configured and the address added to the server’s database, the router must be configured to generate RADIUS requests. A RADIUS server is added or deleted using the commands:

```
ADD RADIUS SERVER=ipadd SECRET=secret
DELETE RADIUS SERVER=ipadd
```

The list of known RADIUS servers is displayed using the command:

```
SHOW RADIUS
```

See *Chapter 1, Operation* for a detailed description of the ADD RADIUS SERVER, DELETE RADIUS SERVER and SHOW RADIUS SERVER commands.

A rule is created to provide access control for the addresses in the RADIUS server using the command:

```
ADD FIREWALL POLICY=name RULE=rule-id ACTION={ALLOW|DENY}
    INTERFACE=interface PROTOCOL={protocol|ALL|EGP|GRE|ICMP|
    OSPF|SA|TCP|UDP} LIST=RADIUS [other-options...]
```

# NAT

ENAT (*Enhanced NAT*) actually implements a form of dynamic packet filtering as a side effect of its implementation. To reduce the overhead of performing packet filtering twice (once by the firewall and once by NAT), the firewall has a built in NAT service that allows the IP addresses (and ports) of hosts on the private network to be translated using NAT or ENAT as they pass through the firewall.

Because the firewall has its own NAT service, when the firewall is enabled the router's standard NAT service (see "*Network Address Translation*" on page 8-32 of *Chapter 8, Internet Protocol (IP)*) is automatically disabled. The configuration is saved and can be restored if the firewall is disabled.

A NAT translation is added to or removed from a policy using the commands:

```
ADD FIREWALL POLICY=name NAT={STANDARD|ENHANCED}
   INTERFACE=interface [IP=ipadd] GBLINTERFACE=interface
   [GBLIP=ipadd[-ipadd]]
DELETE FIREWALL POLICY=name NAT INTERFACE=interface
   GBLINTERFACE=interface [IP=ipadd]
```

# Monitoring Firewall Activity

The firewall provides a range of options for monitoring the configuration of the firewall itself, as well as firewall events, access control and attacks.

## Notifications

The firewall can be configured to send notifications about significant firewall events to one or more of the following destinations:

- An email address. See "*Mail Subsystem*" on page 1-26 of *Chapter 1, Operation* for information about configuring the mail subsystem.
- All terminal and Telnet sessions logged in with MANAGER privilege.
- An asynchronous port
- An SNMP trap host. See *Chapter 28, Simple Network Management Protocol (SNMP)* for information about configuring SNMP trap hosts.

Notification destinations can be enabled or disabled using the commands:

```
ENABLE FIREWALL NOTIFY={ALL|MAIL|MANAGER|PORT|SNMP}
DISABLE FIREWALL NOTIFY={ALL|MAIL|MANAGER|PORT|SNMP}
```

A history of recent events can be displayed using the command:

```
SHOW FIREWALL EVENT
```

## Debugging

Debugging can be enabled or disabled on a per-policy basis using the commands:

```
ENABLE FIREWALL POLICY=name DEBUG={ALL|PACKET|PKT|PROCESS}
DISABLE FIREWALL POLICY=name DEBUG={ALL|PACKET|PKT|PROCESS}
```

## Event Triggers

The firewall forwards the following events to the Trigger Facility:

- DOSATTACK—A denial of service attack in which a remote user continually sends unwanted traffic.
- FRAGATTACK—An attack using TCP fragments that are either too large or can never be reassembled.
- HOSTSCAN—A scan of the hosts of the private network.
- PORTSCAN—A portscan of the firewall or private network.
- SMURFATTACK—A directed attack on the hosts on the private network hidden by NAT.
- SYNATTACK—An attack on a host using multiple opening TCP SYN packets to exhaust a host's available sessions or memory.
- TCPATTACK—An attack on a host using TCP tiny fragments.

The Trigger Facility can be configured to respond to these events by running management-defined scripts.Triggers can be activated by the start or end of an event. See *Chapter 20, Trigger Facility* for more information about creating triggers to respond to firewall events.

## Logging

The firewall can be configured to log an extensive range of events to the router's Logging Facility (Table 31-1 on page 31-10).

Table 31-1: Log types and subtypes for firewall events.

| Option | Meaning |
|---|---|
| INATCP | Logs the start of TCP sessions initiated from the public Internet. |
| INAUDP | Logs the start of a UDP flow initiated from the public Internet. |
| INAICMP | Logs a ICMP request initiated from the public Internet. |
| INAOTHER | Logs the start of an IP protocol flow (other than TCP, UDP or ICMP) initiated from the public Internet. |
| INALLOW | Logs the start of all incoming allowed sessions and flows, and is the sum of the previous four values. |
| OUTATCP | Logs the start of TCP sessions initiated from the private Intranet. |
| OUTAUDP | Logs the start of a UDP flow initiated from the private Intranet. |
| OUTAICMP | Logs a ICMP request initiated from the private Intranet. |
| OUTAOTHER | Logs the start of an IP protocol flow (other than TCP, UDP or ICMP) initiated from the private Intranet. |
| OUTALLOW | Logs the start of all allowed outgoing sessions and flows, and is the sum of the previous four values. |
| ALLOW | Logs the start of all allowed flows and sessions both in and out of the firewall. |
| INDTCP | Logs the failed start of TCP sessions initiated from the public Internet. |
| INDUDP | Logs the failed start of a UDP flow initiated from the public Internet. |
| INDICMP | Logs a failed ICMP request initiated from the public Internet. |
| INDOTHER | Logs the failed start of an IP protocol flow (other than TCP, UDP or ICMP) initiated from the public Internet. |

Table 31-1: Log types and subtypes for firewall events. (Continued)

| Option | Meaning |
|---|---|
| INDENY | Logs the failed start of all denied incoming sessions and flows, and is the sum of the previous four values. |
| OUTDTCP | Logs the failed start of TCP sessions initiated from the private Intranet. |
| OUTDUDP | Logs the failed start of a UDP flow initiated from the private Intranet. |
| OUTDICMP | Logs a failed ICMP request initiated from the private Intranet. |
| OUTDOTHER | Logs the failed start of an IP protocol flow (other than TCP, UDP or ICMP) initiated from the private Intranet. |
| OUTDENY | Logs the failed start of all denied outgoing sessions and flows, and is the sum of the previous four values. |
| DENY | Logs the failed start of all flows and sessions both in and out of the firewall. |
| INDDTCP | Logs the failed start of TCP sessions initiated from the public Internet. Up to 192 bytes of the IP packet are also logged. |
| INDDUDP | Logs the failed start of a UDP flow initiated from the public Internet. Up to 192 bytes of the IP packet are also logged. |
| INDDICMP | Logs a failed ICMP request initiated from the public Internet. Up to 192 bytes of the IP packet are also logged. |
| INDDOTHER | Logs the failed start of an IP protocol flow (other than TCP, UDP or ICMP) initiated from the public Internet. Up to 192 bytes of the IP packet are also logged. |
| INDDUMP | Logs the failed start of all denied incoming sessions and flows, and is the sum of the previous four values. Up to 192 bytes of the IP packet are also logged. |
| OUTDDTCP | Logs the failed start of TCP sessions initiated from the private Intranet. Up to 192 bytes of the IP packet are also logged. |
| OUTDDUDP | Logs the failed start of a UDP flow initiated from the private Intranet. Up to 192 bytes of the IP packet are also logged. |
| OUTDDICMP | Logs a failed ICMP request initiated from the private Intranet. Up to 192 bytes of the IP packet are also logged. |
| OUTDDOTHER | Logs the failed start of an IP protocol flow (other than TCP, UDP and ICMP) initiated from the private Intranet. Up to 192 bytes of the IP packet are also logged. |
| OUTDDUMP | Logs the failed start of all denied OUT sessions and flows, and is the sum of the previous four values. Up to 192 bytes of the IP packet are also logged. |
| DENYDUMP | Logs the failed start of all flows and sessions both in and out of the firewall. Up to 192 bytes of the IP packet are also logged. |

The logging of specific firewall events can be enabled or disabled on a per-policy basis using the commands:

```
ENABLE FIREWALL POLICY=name LOG={ALLOW|DENY|DENYDUMP|INAICMP|
    INALLOW|INAOTHER|INATCP|INAUDP|INDDICMP|INDDOTHER|
    INDDTCP|INDDUDP|INDDUMP|INDENY|INDICMP|INDOTHER|INDTCP|
    INDUDP|OUTAICMP|OUTALLOW|OUTAOTHER|OUTATCP|OUTAUDP|
    OUTDDICMP|OUTDDOTHER|OUTDDTCP|OUTDDUDP|OUTDDUMP|OUTDENY|
    OUTDICMP|OUTDOTHER|OUTDTCP|OUTDUDP}
```

```
DISABLE FIREWALL POLICY=name LOG={ALLOW|DENY|DENYDUMP|
    INAICMP|INALLOW|INAOTHER|INATCP|INAUDP|INDDICMP|
    INDDOTHER|INDDTCP|INDDUDP|INDDUMP|INDENY|INDICMP|
    INDOTHER|INDTCP|INDUDP|OUTAICMP|OUTALLOW|OUTAOTHER|
    OUTATCP|OUTAUDP|OUTDDICMP|OUTDDOTHER|OUTDDTCP|OUTDDUDP|
    OUTDDUMP|OUTDENY|OUTDICMP|OUTDOTHER|OUTDTCP|OUTDUDP}
```

Several options can be enabled or disable in a single invocation by specifying the options as a comma separated list, for example:

```
ENABLE FIREWALL POLICY=office LOG=INDENY,OUTDENY
```

To minimise the number of log messages generated by the firewall, for some events the first four packets will be logged, then the first packet will be repeated with the text "(x *number*)" appended to indicate the number of repeat messages.

# Accounting

The firewall maintains accounting information that enables the firewall manager to determine the effect that various firewall policies are having on traffic flow. Accounting can be enabled or disabled on a per-policy basis using the commands:

```
ENABLE FIREWALL POLICY=name ACCOUNTING

DISABLE FIREWALL POLICY=name ACCOUNTING
```

The currently stored accounting records can be displayed using the command:

```
SHOW FIREWALL ACCOUNTING [POLICY=name] [REVERSE=number]
    [TAIL=number]
```

# Configuration Examples

The following examples illustrate the steps required to configure the firewall for a range of applications. The configurations will provide very good firewall protection for a number of common router configurations. In particular, when a host on a network connected to a private interface initiates a session (TCP) or flow(UDP) to a host reachable by a public interface, then only context sensitive traffic relating to that session or flow is allowed back through the firewall. All other traffic initiated from hosts reachable by a public interface will be dropped by the firewall. The exception to this is when special filter rules have been added (see the fourth example below). Further, most common denial of service attacks will be logged and combated by the firewall.

## Minimum Configuration for a Small Office

This example illustrates how to configure the most basic firewall for a small office wanting to be as secure as possible without restricting access to the public Internet. The office computers are connected to the router via Ethernet port 0, and there is a connection to the Internet via ISDN over PPP interface 0. The Ethernet interface has been assigned the global IP addresses 202.49.74.0 to 202.49.74.255. The PPP interface has been assigned a single global Internet address 202.49.72.2.

To configure a firewall without restricting access to the public Internet:

1. Create the security policy.

   Create a policy named “office”, using the command:

   ```
   CREATE FIREWALL POLICY=office
   ```

2. Add the interfaces to the security policy.

   Add the Ethernet and PPP interfaces to the policy, using the commands:

   ```
   ADD FIREWALL POLICY=office INTERFACE=eth0 TYPE=PRIVATE
   ADD FIREWALL POLICY=office INTERFACE=ppp0 TYPE=PUBLIC
      METHOD=DYNAMIC
   ```

   Since externally initiated access to hosts on the private network is not required, no further configuration is required. When at least one private and one public interface are added to a policy, the policy is operational.

## A Firewall with an ISP-assigned Internet Address

This example illustrates how to configure a firewall for a small office which is dynamically assigned a single global Internet address by their ISP when the router connects to the ISP and negotiates an IP option for the PPP link. For this reason NAT must be used on the private network. The office computers are connected to the router via Ethernet port 0, and there is a connection to the Internet via ISDN over PPP interface 0. The Ethernet interface will use the private IP network addresses 192.168.10.0 to 192.168.10.255. The PPP interface is dynamically assigned a single global Internet address by the ISP.

To configure Firewall with a single global Internet address from an ISP:

1. Create the security policy.

   Create a policy named “office”, using the command:

   ```
   CREATE FIREWALL POLICY=office
   ```

2. Add the interfaces to the security policy.

   Add the Ethernet and PPP interfaces to the policy, using the commands:

   ```
   ADD FIREWALL POLICY=office INTERFACE=eth0 TYPE=PRIVATE
   ADD FIREWALL POLICY=office INTERFACE=ppp0 TYPE=PUBLIC
      METHOD=DYNAMIC
   ```

3. Add the NAT mapping to the private interface.

   Add a NAT mapping to the Ethernet interface to translate private IP addresses to the dynamically assigned global IP address, using the command:

   ```
   ADD FIREWALL POLICY=office NAT=ENHANCED INTERFACE=eth0
      GBLINTERFACE=ppp0
   ```

## A Firewall with a Single Global Internet Address

This example is similar to the previous example, except that the ISP has assigned a single static global Internet address to the office. NAT must be used on the private network to translate private IP addresses to the global IP address. The office computers are connected to the router via Ethernet port 0, and there is a connection to the Internet via ISDN over PPP interface 0. The Ethernet interface will use the private IP network addresses 192.168.10.0 to

192.168.10.255. The PPP interface has been assigned the global Internet address 202.49.72.2.

To configure Firewall with a single global Internet address:

1. Create the security policy.

   Create a policy named “office”, using the command:

   ```
   CREATE FIREWALL POLICY=office
   ```

2. Add the interfaces to the security policy.

   Add the Ethernet and PPP interfaces to the policy, using the commands:

   ```
   ADD FIREWALL POLICY=office INTERFACE=eth0 TYPE=PRIVATE
   ADD FIREWALL POLICY=office INTERFACE=ppp0 TYPE=PUBLIC
      METHOD=DYNAMIC
   ```

3. Add the NAT mapping to the private interface.

   Add a NAT mapping to the Ethernet interface to translate private IP addresses to the statically assigned global IP address, using the command:

   ```
   ADD FIREWALL POLICY=office NAT=ENHANCED INTERFACE=eth0
      GBLINTERFACE=PPP0 GBLIP=202.49.72.2
   ```

## Allowing Access to a WWW Server

This example builds on the previous example by allowing access from the public Internet to a WWW server on the private network. The office has been assigned a single global Internet address by their ISP. For this reason NAT must be used on the private network. The office computers are connected to the router via Ethernet port 0, and there is a connection to the Internet via ISDN over PPP interface 0. The Ethernet interface will use the private IP network addresses 192.168.10.0 to 192.168.10.255. The PPP interface has been assigned the single global Internet address 202.49.72.2. The office wants to provide access to a WWW server on the private network to advertise its products.

To configure Firewall to allow access to a WWW server:

1. Create the security policy.

   Create a policy named “office”, using the command:

   ```
   CREATE FIREWALL POLICY=office
   ```

2. Add the interfaces to the security policy.

   Add the Ethernet and PPP interfaces to the policy, using the commands:

   ```
   ADD FIREWALL POLICY=office INTERFACE=eth0 TYPE=PRIVATE
   ADD FIREWALL POLICY=office INTERFACE=ppp0 TYPE=PUBLIC
      METHOD=DYNAMIC
   ```

3. Add the NAT mapping to the private interface.

   Add a NAT mapping to the Ethernet interface to translate private IP addresses to the statically assigned global IP address, using the command:

   ```
   ADD FIREWALL POLICY=office NAT=ENHANCED INTERFACE=eth0
      GBLINTERFACE=PPP0 GBLIP=202.49.72.2
   ```

4. Add a rule to allow access to the WWW server.

   The basic firewall configuration will not allow hosts on the private network to be accessed from the public network. To allow access to the office

WWW server behind the firewall, add a rule to allow access to the WWW server at IP address 192.168.10.12 from the public Internet. Web browsers and web servers interact using the HTTP protocol, which is a TCP/IP-based protocol using a well-known port, so the rule must allow TCP traffic to the HTTP port to pass from the public interface to the private interface:

```
ADD FIREWALL POLICY=office FILTER=1 ACTION=ALLOW
   INTERFACE=ppp0 IP=192.168.10.12 PROTOCOL=TCP PORT=HTTP
   GBLIP=202.49.72.2 GBLPORT=HTTP
```

## Command Reference

This section describes the commands available on the router to enable, configure, control and monitor the firewall. The firewall requires IP to be enabled and configured correctly. See *Chapter 8, Internet Protocol (IP)* for the commands required to enable and configure IP.

See “*Conventions*” on page xlv of *Preface* in the front of this manual for details of the conventions used to describe command syntax. See *Appendix A, Messages* for a complete list of messages and their meanings.

## ADD FIREWALL POLICY INTERFACE

Syntax

```
ADD FIREWALL POLICY=name INTERFACE=interface TYPE={PUBLIC|
   PRIVATE} [METHOD={DYNAMIC|PASSALL}]
```

where:

- *name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character (“_”).
- *interface* is an interface name formed by concatenating a layer 2 interface type, an interface instance, and optionally a hyphen followed by a logical interface number in the range 0 to 3 (e.g. eth0, ppp1-1). If a logical interface is not specified, 0 is assumed (i.e. ‘eth0’ is equivalent to ‘eth0-0’).

Description

This command adds an interface to the specified policy. The completed policy must contain at least one private interface and one public interface. An interface can only be specified as “private” in one policy. An interface can be specified as “public” in multiple policies. Multiple interfaces specified in a policy as “private” exchange packets without intervention from the firewall.

The POLICY parameter specifies the policy to which the interface will be added. The specified policy must already exist.

The INTERFACE parameter specifies an existing IP interface to be added to the policy.

The TYPE parameter specifies whether the interface is to be treated as a private interface (inside the firewall) or a public interface (outside the firewall).

The METHOD parameter specifies the method to be used by the firewall to pass packets between private and public interfaces, and is only valid if TYPE is set to PUBLIC. If PASSALL is specified, the firewall does not interfere with packet flow. This option should only be selected to allow an interface to run 1:1 NAT translation as defined in RFC 1631. If DYNAMIC is specified, dynamic packet filtering is used. The default is DYNAMIC.

Examples To add an interface to an existing policy named "zone1", use the command:

```
ADD FIREWALL POLICY=zone1 INTERFACE=eth0 TYPE=PRIVATE
```

To add a WAN interface operating over PPP0 to the policy named "zone1", use the command:

```
ADD FIREWALL POLICY=zone1 INTERFACE=PPP0 TYPE=PUBLIC
    METHOD=PASSALL
```

See Also CREATE FIREWALL POLICY
DELETE FIREWALL POLICY INTERFACE
SHOW FIREWALL POLICY

# ADD FIREWALL POLICY LIST

Syntax

```
ADD FIREWALL POLICY=name LIST=list-name FILE=filename
    TYPE={IP|ADDRESS}
```

where:

- *name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character ("_").
- *list-name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character ("_").
- *filename* is the name of a file on the router.

Description This command adds a list of either IP addresses and networks or Ethernet MAC addresses to the specified policy. These lists are used in policy rules.

The POLICY parameter specifies the policy to which the list will be added. The specified policy must already exist.

The LIST parameter specifies a name for the list. The name is used in other commands to refer to the list.

The TYPE parameter specifies the type of information in the file. If IP is specified, the file contains IP host and network address information. If ADDRESS is specified, the file contains Ethernet MAC addresses.

The FILE parameter specifies the name of a file on the router's file subsystem containing the list. The filename must have an extension of `.TXT` and be a text file. See "*List Files*" on page 31-7 for a detailed description of the format of list files.

Examples To add a list of IP addresses named "firstfloor" from the file LISTIP.TXT to the firewall policy named "zone1", use the command:

```
ADD FIREWALL POLICY=zone1 LIST=firstfloor TYPE=IP
    FILE=LISTIP.TXT
```

See Also CREATE FIREWALL POLICY
DELETE FIREWALL POLICY LIST
SHOW FIREWALL POLICY

## ADD FIREWALL POLICY NAT

Syntax

```
ADD FIREWALL POLICY=name NAT={STANDARD|ENHANCED}
   INTERFACE=interface [IP=ipadd] GBLINTERFACE=interface
   [GBLIP=ipadd[-ipadd]]
```

where:

- *name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character (“_”).
- *ipadd* is an IP address in dotted decimal notation.
- *interface* is an interface name formed by concatenating a layer 2 interface type, an interface instance, and optionally a hyphen followed by a logical interface number in the range 0 to 3 (e.g. eth0, ppp1-1). If a logical interface is not specified, 0 is assumed (i.e. ‘eth0’ is equivalent to ‘eth0-0’).

Description This command adds a NAT translation to the specified policy. If an interface or global interface is specified then that interface must have already been added to the security policy.

The POLICY parameter specifies the policy to which the NAT translation will be added. The specified policy must already exist.

The NAT parameter specifies the type of NAT translation to perform. If STANDARD is specified, there is either a one-to-one translation between a private IP address and the specified global IP address, or if more than one global IP address is supplied, then the global IP addresses are used dynamically from the supplied pool of addresses as required. When a pool of global addresses is specified and all sessions are complete for a particular global IP mapping, then that global IP address is returned to the pool for reuse. If ENHANCED is specified, Enhanced NAT (ENAT) is used and both the private IP address and protocol dependent port numbers are translated. The benefit of ENAT is that only a single global Internet address is required to map an entire private network.

The INTERFACE parameter specifies the private interface from which all received traffic is translated before being passed to the public interface specified by the GBLINTERFACE parameter. Both interfaces must already be defined and belong to the same policy.

The IP parameter specifies the private IP address used when a single public IP address is mapped to a single private IP address, and is only valid when NAT is set to STANDARD. This parameter is not valid if a range is specified for the GBLIP parameter.

The GBLINTERFACE parameter specifies the public interface from which all received traffic is translated before being passed to the private interface specified by the INTERFACE parameter. Both interfaces must already be defined and belong to the same policy.

The GBLIP parameter specifies a single global IP address or a range of global IP addresses to be used by the NAT translation. If NAT is set to STANDARD and a pool of global IP addresses is required then a range must be specified. In all other cases only a single global IP address is required.

Examples To add an enhanced NAT mapping to the firewall policy named "zone1", use the command:

```
ADD FIREWALL POLICY=zone1 NAT=ENHANCED INTERFACE=eth0
   GBLINTERFACE=PPP0 GBLIP=202.36.163.2
```

See Also CREATE FIREWALL
DELETE FIREWALL POLICY NAT
SHOW FIREWALL POLICY

# ADD FIREWALL POLICY RULE

Syntax

```
ADD FIREWALL POLICY=name RULE=rule-id ACTION={ALLOW|DENY}
   INTERFACE=interface PROTOCOL={protocol|ALL|EGP|GRE|
   ICMP|OSPF|SA|TCP|UDP} [AFTER=hh:mm] [BEFORE=hh:mm]
   [DAYS={MON|TUE|WED|THU|FRI|SAT|SUN|WEEKDAY|
   WEEKEND}[,...]] [GBLIP=ipadd] [GBLPORT={ALL|
   port[-port]}] [IP=ipadd[-ipadd]] [LIST={list-name|
   RADIUS}] [PORT={ALL|port[-port]|service-name]
   [REMOTEIP=ipadd[-ipadd]] [SOURCEPORT={ALL|port[-port]}]
```

where:

- *name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character ("_").
- *rule-id* is a number in the range 1 to 299.
- *interface* is an interface name formed by concatenating a layer 2 interface type, an interface instance, and optionally a hyphen followed by a logical interface number in the range 0 to 3 (e.g. eth0, ppp1-1). If a logical interface is not specified, 0 is assumed (i.e. 'eth0' is equivalent to 'eth0-0').
- *protocol* is an Internet IP protocol number.
- *hh:mm* is a time in hours and minutes.
- *ipadd* is an IP addresses in dotted decimal notation.
- *port* is an Internet service port number or name.
- *list-name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character ("_").
- *service-name* is a predefined name for an IP service (Table 31-2 on page 31-19).

Description This command adds a rule defining the access allowed between private and public interfaces of the specified policy. By default all access from public interfaces (outside the firewall) is denied and all access from private interfaces (inside the firewall) is allowed. To refine the security policy additional rules can be added to allow or deny access based on IP addresses, port numbers, day of the week, or time of day. Each rule for a specific interface in a policy is processed in order, starting with the lowest numbered rule and proceeding to the highest numbered rule, or until a match is found.

The POLICY parameter specifies the policy to which the rule will be added. The specified policy must already exist.

The RULE parameter specifies both an identifier for the rule and the position of the rule in the list of rules for this policy. Rules are processed in order, from the lowest to the highest numbered rule. The identifier is used to refer to this rule in other commands.

The ACTION parameter specifies whether the rule allows or denies a particular activity.

The INTERFACE parameter specifies the interface to which the rule will be applied. The interface must already exist and belong to the policy.

The PROTOCOL parameter specifies the IP protocol number or the name of a predefined protocol type to match. If TCP or UDP is specified, then the PORT parameter must also be specified.

The AFTER and BEFORE parameters specify the time period during which the rule is active.

The DAYS parameter specifies the days on which the rule will apply, as a comma-separated list. This allows rules to be active only on certain days of the week. The value WEEKDAY is a synonym for the list "MON,TUE,WED,THU,FRI". The value WEEKEND is a synonym for the list "SAT,SUN".

The GBLIP parameter specifies a global IP address to be used as the public IP address for the rule if NAT is active on the interface.

The GBLPORT parameter specifies the port number, service name, or range of port numbers that apply to the rule if NAT is active on an interface.

The IP parameter specifies a single IP address or a range of IP addresses to match. If NAT is active on the interface, then the IP address range is that of the untranslated IP addresses.

The LIST parameter specifies a list of addresses to be checked for a match against the source or destination address of the new flow. The value may be the name of a predefined list of IP or MAC addresses, or the keyword RADIUS. If RADIUS is specified and a RADIUS server has been defined, a RADIUS lookup is performed to check the source or destination address of the new flow. Up to four lists can be add to a rule by repeated invocations of this command.

The PORT parameter specifies a port number, a range of port numbers, or a predefined service name (Table 31-2 on page 31-19) to match. If ALL is specified, the rule matches any port number. If dynamic NAT is active on the interface it is possible to re-map a global port number to a different internal port number.

Table 31-2: Predefined IP protocol service names.

| Service Name | Port Number |
|---|---|
| ECHO | 7 |
| DISCARD | 9 |
| FTP | 21 |
| TELNET | 23 |

Table 31-2: Predefined IP protocol service names. (Continued)

| Service Name | Port Number |
|---|---|
| SMTP | 25 |
| TIME | 37 |
| DNS | 53 |
| BOOTPS | 67 |
| BOOTPC | 68 |
| TFTP | 69 |
| GOPHER | 70 |
| FINGER | 79 |
| WWW | 80 |
| HTTP | 80 |
| KERBEROS | 88 |
| RTELNET | 107 |
| POP2 | 109 |
| POP3 | 110 |
| SNMPTRAP | 162 |
| SNMP | 161 |
| BGP | 179 |
| RIP | 520 |
| VDOLIVE | 7000 |
| REALAUDIO | 7070 |
| REALVIDEO | 7070 |

The REMOTEIP parameter specifies a single remote IP address or a range of remote IP addresses to match. This allows rules to be made based on the remote source of an IP flow.

The SOURCEPORT parameter specifies a source port to match for a TCP or UDP flow. This allows rules to be made based on the source port of the IP flow.

### Examples

To allow WWW access to an internal server at IP address 202.36.163.12, attached to a private interface defined in the policy named “zone1” via the public interface PPP0, use the command:

```
ADD FIREWALL POLICY=zone1 RULE=1 ACTION=ALLOW INTERFACE=ppp0
    IP=202.36.163.12 PROTOCOL=TCP PORT=WWW
```

If the company’s business hours are from 8am to 5pm, and no external access is permitted outside these hours, use the command:

```
ADD FIREWALL POLICY=zone1 RULE=2 ACTION=ALLOW INTERFACE=ppp0
    IP=202.36.163.12 PROTOCOL=TCP PORT=WWW AFTER=08:00
    BEFORE=17:00
```

To deny staff WWW access during the company’s business hours from 8am to 5pm, use the command:

```
ADD FIREWALL POLICY=zone1 RULE=3 ACTION=DENY INTERFACE=eth0
    PROTOCOL=TCP PORT=WWW AFTER=08:00 BEFORE=17:00
```

To allow DNS information from a server at 192.168.12.2 to a private DNS server at IP address 192.168.34.1, which uses UDP originating on port 53, use the command:

```
ADD FIREWALL POLICY=zone1 RULE=5 ACTION=ALLOW INTERFACE=ppp0
   PROTOCOL=UDP IP=192.168.34.1 REMOTE=192.168.12.2
   SOURCEPORT=53
```

To allow Telnet access to a UNIX server on a private network with NAT configured to use the public interface PPP0 with the global IP address 202.49.72.1, use the command:

```
ADD FIREWALL POLICY=zone1 RULE=6 ACTION=ALLOW INTERFACE=ppp0
   IP=192.168.1.1 PROTOCOL=TCP PORT=TELNET GBLIP=202.49.72.1
   GBLPORT=TELNET
```

To add a list to limit the destinations that users of the private network can access based on the list file LISTIP.TXT and also a RADIUS lookup, use the commands:

```
ADD FIREWALL POLICY=zone1 LIST=listallow TYPE=IP
   FILE=listip.txt

ADD FIREWALL POLICY=zone1 RULE=7 ACTION=ALLOW INTERFACE=eth0
   LIST=listallow PROTOCOL=ALL

ADD FIREWALL POLICY=zone1 RULE=7 LIST=RADIUS
```

### See Also

CREATE FIREWALL POLICY
DELETE FIREWALL POLICY RULE
SET FIREWALL POLICY RULE
SHOW FIREWALL POLICY

# CREATE FIREWALL POLICY

### Syntax

CREATE FIREWALL POLICY=*name*

where:

- *name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character (“_”).

### Description

This command creates a new firewall policy. The POLICY parameter specifies the name of the policy to be created, and is used in other commands to refer to the policy. The specified policy must not already exist.

A new policy will not become active until at least one private and one public interface have been added. The policy can be customised to handle specific traffic by adding interfaces, address lists, NAT translations and/or rules, using the commands:

```
ADD FIREWALL POLICY INTERFACE
ADD FIREWALL POLICY LIST
ADD FIREWALL POLICY NAT
ADD FIREWALL POLICY RULE
```

### Examples

To create a firewall policy named “area1”, use the command:

```
CREATE FIREWALL POLICY=area1
```

See Also

ADD FIREWALL POLICY INTERFACE
ADD FIREWALL POLICY LIST
ADD FIREWALL POLICY NAT
ADD FIREWALL POLICY RULE
DESTROY FIREWALL POLICY
DISABLE FIREWALL POLICY
ENABLE FIREWALL POLICY
SHOW FIREWALL POLICY

# DELETE FIREWALL POLICY INTERFACE

Syntax

```
DELETE FIREWALL POLICY=name INTERFACE=interface
```

where:

- *name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character (“_”).
- *interface* is an interface name formed by concatenating a layer 2 interface type, an interface instance, and optionally a hyphen followed by a logical interface number in the range 0 to 3 (e.g. eth0, ppp1-1). If a logical interface is not specified, 0 is assumed (i.e. ‘eth0’ is equivalent to ‘eth0-0’).

Description

This command deletes an interface from the specified policy. The resulting policy must contain at least one private interface and one public interface to remain operational.

The POLICY parameter specifies the policy from which the interface will be deleted. The specified policy must already exist.

The INTERFACE parameter specifies the interface to be deleted from the policy.

Examples

To delete interface ETH0 from a policy named “zone1”, use the command:

```
DELETE FIREWALL POLICY=zone1 INTERFACE=eth0
```

See Also

ADD FIREWALL POLICY INTERFACE
SHOW FIREWALL POLICY

# DELETE FIREWALL POLICY LIST

**Syntax**

```
DELETE FIREWALL POLICY=name LIST=list-name
```

where:

- *name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character ("_").
- *list-name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character ("_").

**Description**

This command deletes a predefined list of IP addresses, networks or Ethernet MAC addresses from the specified policy.

The POLICY parameter specifies the policy from which the list will be deleted. The specified policy must already exist.

The LIST parameter specifies the name of the list to be deleted. The specified list must already exist and be assigned to the policy.

**Examples**

To delete the list named "firstfloor" from the policy named "zone1", use the command:

```
DELETE FIREWALL POLICY=zone1 LIST=firstfloor
```

**See Also**

ADD FIREWALL POLICY LIST
SHOW FIREWALL POLICY

# DELETE FIREWALL POLICY NAT

**Syntax**

```
DELETE FIREWALL POLICY=name NAT INTERFACE=interface
   GBLINTERFACE=interface [IP=ipadd]
```

where:

- *name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character ("_").
- *interface* is an interface name formed by concatenating a layer 2 interface type, an interface instance, and optionally a hyphen followed by a logical interface number in the range 0 to 3 (e.g. eth0, ppp1-1). If a logical interface is not specified, 0 is assumed (i.e. 'eth0' is equivalent to 'eth0-0').
- *ipadd* is an IP address in dotted decimal notation.

**Description**

This command deletes a NAT translation from an interface, or IP address associated with an interface.

The POLICY parameter specifies the policy from which the NAT translation or IP address will be deleted. The specified policy must already exist.

The INTERFACE parameter specifies the private interface for which the NAT translation will be deleted.

The GBLINTERFACE parameter specifies the public interface for which the NAT translation will be deleted.

The IP parameter specifies a previously defined private IP address used when a single public IP address is mapped to a single private IP address, for which the NAT translation will be deleted.

Examples To delete a NAT mapping defined in the policy named "zone1", use the command:

```
DELETE FIREWALL POLICY=zone1 NAT INTERFACE=eth0
    GBLINTERFACE=ppp0
```

See Also ADD FIREWALL POLICY NAT
SHOW FIREWALL POLICY

## DELETE FIREWALL POLICY RULE

Syntax `DELETE FIREWALL POLICY=`*`name`* `RULE=`*`rule-id`*

where:

- *name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character ("_").
- *rule-id* is a number in the range 1 to 299.

Description This command deletes a rule from the specified policy. The POLICY parameter specifies the policy from which the rule will be deleted. The specified policy must already exist. The RULE parameter specifies the rule to be deleted from the policy.

Examples To delete rule number 1 from the policy named "zone1", use the command:

```
DELETE FIREWALL POLICY=zone1 RULE=1
```

See Also ADD FIREWALL POLICY RULE
SET FIREWALL POLICY RULE
SHOW FIREWALL POLICY

## DELETE FIREWALL SESSION

Syntax `DELETE FIREWALL SESSION={`*`session-number`*`|ALL}`

where:

- *session-number* is the identifier for a currently active session.

Description This command terminates the specified currently active session or flow, or all currently active sessions and flows.

The SESSION parameter specifies the identifier of the active session or flow to be terminated. If ALL is specified, all active sessions and flows are terminated. The session identifier is read from the output of the SHOW FIREWALL POLICY SESSION command.

Examples To delete session number 1B32, use the command:

```
DELETE FIREWALL SESSION=1B32
```

See Also SHOW FIREWALL SESSION

## DESTROY FIREWALL POLICY

Syntax `DESTROY FIREWALL POLICY=`*`name`*

where:

- *name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character (“_”).

Description This command destroys the specified policy. The POLICY parameter specifies the policy to be destroyed. The specified policy must already exist.

Examples To destroy a policy named “area1”, use the command:

```
DESTROY FIREWALL POLICY=area1
```

See Also CREATE FIREWALL POLICY
DISABLE FIREWALL POLICY
ENABLE FIREWALL POLICY
SHOW FIREWALL POLICY

## DISABLE FIREWALL

Syntax `DISABLE FIREWALL`

Description This command disables the firewall. A warning message, notification message and log message are generated when this command is issued.

Examples To disable the firewall, use the command:

```
DISABLE FIREWALL
```

See Also DISABLE FIREWALL NOTIFY
DISABLE FIREWALL POLICY
ENABLE FIREWALL
ENABLE FIREWALL NOTIFY
ENABLE FIREWALL POLICY
SHOW FIREWALL

## DISABLE FIREWALL NOTIFY

Syntax

```
DISABLE FIREWALL NOTIFY={ALL|MAIL|MANAGER|PORT|SNMP}
```

Description

This command disables the sending of notification messages about firewall events to the specified destinations. The destinations are assumed to belong to the firewall manager. Notifications can be sent to one or more destinations.

The NOTIFY parameter specifies where the notifications are no longer to be sent, and accepts either a single value or a comma-separated list of values. If ALL is specified, notifications are no longer sent to any destinations. If MAIL is specified, notifications are no longer sent to an email address. If MANAGER is specified, notifications are no longer sent to all users currently logged in with MANAGER privilege. If PORT is specified, notifications are no longer sent to an asynchronous port. If SNMP is specified, notifications are no longer sent as SNMP traps to a pre-configured SNMP trap host. The default is MANAGER.

Examples

To disable the sending of notifications via SNMP and email, use the command:

```
DISABLE FIREWALL NOTIFY=MAIL,SNMP
```

See Also

DISABLE FIREWALL
DISABLE FIREWALL POLICY
ENABLE FIREWALL
ENABLE FIREWALL NOTIFY
ENABLE FIREWALL POLICY
SHOW FIREWALL

## DISABLE FIREWALL POLICY

Syntax

```
DISABLE FIREWALL POLICY=name [ACCOUNTING] [DEBUG={ALL|
   PACKET|PKT|PROCESS}] [ICMP_FORWARDING={ALL|PARAMETER|
   PING|REDIRECT|SOURCEQUENCH|TIMEEXCEEDED|TIMESTAMP|
   UNREACHABLE}] [LOG={ALLOW|DENY|DENYDUMP|INAICMP|
   INALLOW|INAOTHER|INATCP|INAUDP|INDDICMP|INDDOTHER|
   INDDTCP|INDDUDP|INDDUMP|INDENY|INDICMP|INDOTHER|INDTCP|
   INDUDP|OUTAICMP|OUTALLOW|OUTAOTHER|OUTATCP|OUTAUDP|
   OUTDDICMP|OUTDDOTHER|OUTDDTCP|OUTDDUDP|OUTDDUMP|
   OUTDENY|OUTDICMP|OUTDOTHER|OUTDTCP|OUTDUDP}]
   [OPTIONS={ALL|RECORD_ROUTE|SECURITY|SOURCEROUTE|
   TIMESTAMP}] [PING]
```

where:

- *name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character (“_”).

Description

This command disables the processing of specific types of IP packets by the specified policy, and/or disables accounting, logging or debugging for the policy.

The POLICY parameter specifies the policy for which packet processing attributes, accounting, logging or debugging are to be disabled. The specified policy must already exist.

The ACCOUNTING parameter disables the recording of accounting information for flows and sessions handled by the policy.

The DEBUG parameter specifies the types of debugging information to be disabled. If ALL is specified, all debugging information is disabled. If PACKET or PKT is specified, the display of the first 56 bytes of each IP packet received is disabled. If PROCESS is specified, the display of information about the processing of a particular IP packet is disabled. The DEBUG parameter is not retained over a reboot.

The ICMP_FORWARDING parameter disables the forwarding of the specified ICMP messages through the router. The value may be a single option or a comma-separated list of options. The default is not to forward any ICMP messages because ICMP packets can be used as a method for denial of service attacks.

The LOG parameter disables the logging of the specified firewall events to the router's Logging Facility. The value may be a single option or a comma-separated list of options. Table 31-1 on page 31-10 lists the options and their meanings.

The OPTIONS parameter disables the forwarding of packets with the specified IP option or options to the next level of firewall checking. The value may be a single option or a comma-separated list of options. The default is not to forward packets with IP options.

The PING parameter disables the handling of ping packets destined for a public interface on the router. The default is to reject such ping packets.

Examples

To disable the forwarding of all ICMP messages to the next level of firewall checking defined in the policy named “zone1”, use the command:

```
DISABLE FIREWALL POLICY=zone1 ICMP_FORWARDING=ALL
```

To disable the logging of all allowed sessions started from the public Internet, in the policy named “zone1”, use the command:

```
DISABLE FIREWALL POLICY=zone1 LOG=INALLOW
```

See Also

DISABLE FIREWALL
DISABLE FIREWALL NOTIFY
ENABLE FIREWALL
ENABLE FIREWALL NOTIFY
ENABLE FIREWALL POLICY
SHOW FIREWALL

## ENABLE FIREWALL

Syntax

```
ENABLE FIREWALL
```

Description

This command enables the firewall. A log message is generated when this command is issued.

Examples

To enable the firewall software, use the command:

```
ENABLE FIREWALL
```

See Also

DISABLE FIREWALL<br>
DISABLE FIREWALL NOTIFY<br>
DISABLE FIREWALL POLICY<br>
ENABLE FIREWALL NOTIFY<br>
ENABLE FIREWALL POLICY<br>
SHOW FIREWALL

# ENABLE FIREWALL NOTIFY

Syntax

```
ENABLE FIREWALL NOTIFY={ALL|MAIL|MANAGER|PORT|SNMP}[,...]
    [PORT=port-number] [TO=address]
```

where:

- *port-number* is the number of an asynchronous port on the router. Ports are number sequentially starting from 0.
- *address* is a character string, 1 to 131 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character (“_”).

Description

This command enables the sending of notification messages about firewall events to the specified destinations. The destinations are assumed to belong to the firewall manager. Notifications can be sent to one or more destinations.

The NOTIFY parameter specifies where the notifications are to be sent, and accepts either a single value or a comma-separated list of values. If ALL is specified, notifications are sent to all destinations. If MAIL is specified, notifications are sent via email to the email address specified by the TO parameter. The MAIL subsystem must also be configured. See *Chapter 1, Operation* for more information about configuring the mail subsystem. If MANAGER is specified, notifications are sent to all users currently logged in with MANAGER privilege. If PORT is specified, notifications are sent to the asynchronous port specified by the PORT parameter. The port must be configured to the correct baud rate and flow control for the terminal. If SNMP is specified, notifications are sent as SNMP traps to the pre-configured SNMP trap host. See *Chapter 28, Simple Network Management Protocol (SNMP)* for more information about configuring an SNMP trap host. The default is MANAGER.

The PORT parameter specifies the asynchronous port to which notifications are sent. This parameter is required, and is only valid when NOTIFY is set to PORT or a list of destinations including PORT.

The TO parameter specifies the email address to which notifications are sent. This parameter is required, and is only valid when NOTIFY is set to MAIL or a list of destinations including MAIL.

Examples

To send notifications via email to fireman@mycorp.com, use the command:

```
ENABLE FIREWALL NOTIFY=MAIL TO="fireman@mycorp.com"
```

See Also

DISABLE FIREWALL<br>
DISABLE FIREWALL NOTIFY<br>
DISABLE FIREWALL POLICY<br>
ENABLE FIREWALL<br>
ENABLE FIREWALL POLICY<br>
SHOW FIREWALL

# ENABLE FIREWALL POLICY

Syntax

```
ENABLE FIREWALL POLICY=name [ACCOUNTING] [DEBUG={ALL|
   PACKET|PKT|PROCESS}] [ICMP_FORWARDING={ALL|PARAMETER|
   PING|REDIRECT|SOURCEQUENCH|TIMEEXCEEDED|TIMESTAMP|
   UNREACHABLE}] [LOG={ALLOW|DENY|DENYDUMP|INAICMP|
   INALLOW|INAOTHER|INATCP|INAUDP|INDDICMP|INDDOTHER|
   INDDTCP|INDDUDP|INDDUMP|INDENY|INDICMP|INDOTHER|INDTCP|
   INDUDP|OUTAICMP|OUTALLOW|OUTAOTHER|OUTATCP|OUTAUDP|
   OUTDDICMP|OUTDDOTHER|OUTDDTCP|OUTDDUDP|OUTDDUMP|
   OUTDENY|OUTDICMP|OUTDOTHER|OUTDTCP|OUTDUDP}]
   [OPTIONS={ALL|RECORD_ROUTE|SECURITY|SOURCEROUTE|
   TIMESTAMP}] [PING]
```

where:

- *name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character (“_”).

Description

This command enables the processing of specific types of IP packets by the specified policy, and/or enables accounting, logging or debugging for the policy.

The POLICY parameter specifies the policy for which packet processing attributes, accounting, logging or debugging are to be enabled. The specified policy must already exist.

The ACCOUNTING parameter enables the recording of accounting information for flows and sessions handled by the policy.

The DEBUG parameter specifies the types of debugging information to be enabled. If ALL is specified, all debugging information is enabled. If PACKET or PKT is specified, the display of the first 56 bytes of each IP packet received is enabled. If PROCESS is specified, the display of information about the processing of a particular IP packet is enabled. The DEBUG parameter is not retained over a reboot.

The ICMP_FORWARDING parameter enables the forwarding of the specified ICMP messages through the router. The value may be a single option or a comma-separated list of options. The default is not to forward any ICMP messages because ICMP packets can be used as a method for denial of service attacks.

The LOG parameter enables the logging of the specified firewall events to the router’s Logging Facility. The value may be a single option or a comma-separated list of options. Table 31-1 on page 31-10 lists the possible options and their meanings.

The OPTIONS parameter enables the forwarding of packets with the specified IP option or options to the next level of firewall checking. The value may be a single option or a comma-separated list of options. The default is not to forward packets with IP options.

The PING parameter enables the handling of ping packets destined for a public interface on the router. The default is to reject such ping packets.

**Examples** To enable the passing of all ICMP messages to the next level of firewall checking defined in the policy named "zone1", use the command:

```
ENABLE FIREWALL POLICY=zone1 ICMP_FORWARDING=ALL
```

To enable the logging of all allowed sessions started from the public Internet and all denied sessions in both directions, in the policy named "zone1", use the command:

```
ENABLE FIREWALL POLICY=zone1 LOG=INALLOW,DENY
```

**See Also** DISABLE FIREWALL
DISABLE FIREWALL NOTIFY
DISABLE FIREWALL POLICY
ENABLE FIREWALL
ENABLE FIREWALL NOTIFY
SHOW FIREWALL

# SET FIREWALL POLICY RULE

**Syntax**

```
SET FIREWALL POLICY=name RULE=rule-id [PROTOCOL={protocol|
   ALL|EGP|GRE|ICMP|OSPF|SA|TCP|UDP}] [AFTER=hh:mm]
   [BEFORE=hh:mm] [DAYS={MON|TUE|WED|THU|FRI|SAT|SUN|
   WEEKDAY|WEEKEND}[,...]] [GBLIP=ipadd] [GBLPORT={ALL|
   port[-port]}] [IP=ipadd[-ipadd]] [PORT={ALL|
   port[-port]|service-name] [REMOTEIP=ipadd[-ipadd]]
   [SOURCEPORT={ALL|port[-port]}]
```

where:

- *name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character ("_").
- *rule-id* is a number in the range 1 to 299.
- *protocol* is an Internet IP protocol number.
- *hh:mm* is a time in hours and minutes.
- *ipadd* is an IP addresses in dotted decimal notation.
- *port* is an Internet service port number or name.
- *list-name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character ("_").
- *service-name* is a predefined name for an IP service (Table 31-2 on page 31-19).

**Description** This command modifies a rule defining the access allowed between private and public interfaces of the specified policy. By default all access from public interfaces (outside the firewall) is denied and all access from private interfaces (inside the firewall) is allowed. To refine the security policy additional rules can be added to allow or deny access based on IP addresses, port numbers, day of the week, or time of day. Each rule for a specific interface in a policy is processed in order, starting with the lowest numbered rule and proceeding to the highest numbered rule, or until a match is found.

The POLICY parameter specifies the policy containing the rule to be modified. The specified policy must already exist.

The RULE parameter specifies the rule to be modified.

The PROTOCOL parameter specifies the IP protocol number or the name of a predefined protocol type to apply to the rule. If TCP or UDP is specified, then the PORT parameter must also be specified.

The AFTER and BEFORE parameters specify the time period during which the rule is active.

The DAYS parameter specifies the days on which the rule will apply, as a comma-separated list. This allows rules to be active only on certain days of the week. The value WEEKDAY is a synonym for the list "MON,TUE,WED,THU,FRI". The value WEEKEND is a synonym for the list "SAT,SUN".

The GBLIP parameter specifies a global IP address to be used as the public IP address for the rule if NAT is active on the interface.

The GBLPORT parameter specifies the port number, service name, or range of port numbers that apply to the rule if NAT is active on an interface.

The IP parameter specifies a single IP address or a range of IP addresses to be applied by the rule. If NAT is active on the interface, then the IP address range is that of the untranslated IP addresses.

The PORT parameter specifies a port number, a range of port numbers, or a predefined service name (Table 31-2 on page 31-19) to match. If ALL is specified, the rule matches any port number. If dynamic NAT is active on the interface it is possible to re-map a global port number to a different internal port number.

The REMOTEIP parameter specifies a single remote IP address or a range of remote IP addresses to be applied to the rule. This allows rules to be made based on the remote source of an IP flow.

The SOURCEPORT parameter specifies a source port for a TCP or UDP flow. This allows rules to be made based on the source port of the IP flow.

Examples To modify rule number 1 in the policy named "zone1" to match IP address 202.36.163.114, use the command:

```
SET FIREWALL POLICY=zone1 RULE=1 IP=202.36.163.114
```

See Also ADD FIREWALL POLICY RULE
DELETE FIREWALL POLICY RULE
SHOW FIREWALL POLICY

# SHOW FIREWALL

Syntax

```
SHOW FIREWALL
```

Description This command displays a summary of all security policies that have been created and the interfaces assigned to each policy (Figure 31-1 on page 31-32, Table 31-3 on page 31-32).

Figure 31-1: Example output from the SHOW FIREWALL command.

```
Firewall Configuration

Status .................... enabled
Enabled Notify Options .... all
Notify Port ............... 1
Notify Mail To ............ root@netman.company.com

Policy : test
  Private Interface : eth0
  Public Interface  : eth1
    Method .......................... dynamic
    NAT ............................. enhanced
      Method ........................ enhanced dynamic
      Private Interface ............. eth0
      Global IP ..................... 192.168.72.89
```

Table 31-3: Parameters displayed in the output of the SHOW FIREWALL command.

| Parameter | Meaning |
|---|---|
| Status | The status of the firewall; one of "enabled" or "enabled". |
| Enabled Notify Options | A list of the notification destinations currently enabled; one or more of "all", "mail", "manager", "port", "snmp" or "none". |
| Notify Port | The asynchronous port to which notifications will be sent. Only displayed when *Enable Notify Options* includes "port". |
| Notify Mail To | The email address to which notifications will be sent. Only displayed when *Enable Notify Options* includes "mail". |
| Policy | The name of a policy. |
| Private Interface | The name of a private interface assigned to the policy. |
| Public Interface | The name of a public interface assigned to the policy. |
| Method | The method used to packets to or from the public interface; one of "dynamic" or "passall". |
| NAT | The type of NAT translation enabled; one of "standard" or "enhanced". Only displayed when NAT is enabled on the policy. |
| NAT/Method | The method used to perform NAT translation; one of "none", "static", "dynamic", "enhanced static", "enhanced dynamic" or "enhanced interface". This field depends on the combination of options configured in the ADD FIREWALL POLICY NAT command, and is only displayed when NAT is enabled on the policy. |
| NAT/Private Interface | The private interface to which NAT translations will apply. Only displayed when NAT is enabled on the policy. |
| NAT Global IP | The global IP address used by NAT translations. Only displayed when NAT is enabled on the policy. |

**See Also** ADD FIREWALL POLICY INTERFACE
CREATE FIREWALL POLICY
DELETE FIREWALL POLICY INTERFACE
DESTROY FIREWALL POLICY
DISABLE FIREWALL
ENABLE FIREWALL

## SHOW FIREWALL ACCOUNTING

**Syntax**

```
SHOW FIREWALL ACCOUNTING [POLICY=name] [REVERSE=number]
   [TAIL=number]
```

where:

- *name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character (“_”).
- *number* is a decimal number in the range 1 to 60.

**Description** This command displays the currently stored accounting records for the specified or all policies (Figure 31-2 on page 31-33, Table 31-4 on page 31-34).

The POLICY parameter specifies the policy for which accounting records are to be displayed. The specified policy must already exist. If a value is not specified, accounting records for all policies are displayed.

The REVERSE parameter specifies that the accounting records are to be displayed in reverse order. If a value is specified, output is limited to the specified number of records.

The TAIL parameter specifies that the only the most recent accounting records are to be displayed. If a value is specified, output is limited to the specified number of records.

Figure 31-2: Example output from the SHOW FIREWALL ACCOUNTING command.

```
Policy : test
Date/Time   Event  Dir Prot  IP:Port <-> Dest IP:Port /Traffic statistics
--------------------------------------------------------------------------------
20 10:10:00 START  OUT TCP   202.36.163.10:1113 192.168.72.50:80
20 10:10:01 END    OUT TCP   202.36.163.10:1112 192.168.72.50:80
                             Traffic out 5:695 in 5:367
20 10:10:15 START  OUT TCP   202.36.163.6:1025 192.168.72.50:23
20 10:10:15 START  IN  TCP   192.168.72.50:10778 192.168.72.89:113
20 10:11:01 END    OUT TCP   202.36.163.10:1069 192.168.72.50:80
                             Traffic out 5:692 in 5:366
20 10:11:01 END    OUT TCP   202.36.163.10:1070 192.168.72.50:80
                             Traffic out 5:696 in 5:365
20 10:11:02 END    OUT TCP   202.36.163.10:1071 192.168.72.50:80
                             Traffic out 5:696 in 5:365
20 10:12:01 END    OUT TCP   202.36.163.10:1113 192.168.72.50:80
                             Traffic out 5:695 in 5:367
20 10:12:15 END    IN  TCP   192.168.72.50:10778 192.168.72.89:113
                             Traffic out 3:164 in 6:264
--------------------------------------------------------------------------------
```

Table 31-4: Parameters displayed in the output of the SHOW FIREWALL ACCOUNTING command.

| Parameter | Meaning |
|---|---|
| Policy | The name of the policy. |
| Date/Time | The date and time of the entry. |
| Event | The event recorded by the entry; one of "START" or "END". |
| Dir | The direction of the flow; one of "IN" or "OUT". |
| Prot | The protocol for the flow; one of "ICMP", "TCP", "UDP", or the IP protocol number. |
| IP:Port | The source IP address and port for the flow. |
| Dest IP:Port | The destination IP address and port for the flow. |
| Traffic statistics | The number of packets and octets processed for the outgoing or incoming traffic flows, expressed in the format "*direction packets*:*octets*". |

*ICMP pings only display end records to reduce the number of records stored.*

**See Also**

DISABLE FIREWALL POLICY
ENABLE FIREWALL POLICY
SHOW FIREWALL POLICY

# SHOW FIREWALL EVENT

**Syntax**

```
SHOW FIREWALL EVENT={ALLOW|DENY|NOTIFY} [POLICY=name]
   [REVERSE=number] [TAIL=number]
```

where:

- *name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character ("_").
- *number* is a decimal number in the range 1 to 60.

**Description**

This command displays information about recent firewall events (Figure 31-3 on page 31-35, Table 31-5 on page 31-36).

The EVENT parameter specifies which category of events to display. If a value is not specified, all events are displayed. If ALLOW is specified, events for flows that have been allowed are displayed. If DENY is specified, events for flows that have been denied are displayed. If NOTIFY is specified, notification events are displayed.

The POLICY parameter specifies the policy for which events are to be displayed. The specified policy must already exist. If a value is not specified, events for all policies are displayed.

The REVERSE parameter specifies that the events are to be displayed in reverse order. If a value is specified, output is limited to the specified number of events.

The TAIL parameter specifies that the only the most recent events are to be displayed. If a value is specified, output is limited to the specified number of events.

Figure 31-3: Example output from the SHOW FIREWALL EVENT command.

```
Policy : test - Notify Events:
Date/Time   Dir Prot Number IP:Port <map> Dest IP:Port /Reason /IP header
-------------------------------------------------------------------------------
15 15:21:58 IN  TCP       2 203.97.191.217:1046 192.168.72.33:20
                SYN attack underway
15 15:22:00 IN  TCP       2 203.97.191.217:0 192.168.72.33:0
                Port scan underway
                45000044 8d8f4000 3f061097 cb61bfd9 ca314821 04160014 9610e710
                00000000 c0024000
15 15:25:55 IN  TCP       1 203.97.191.217:0 192.168.72.33:0
                Port scan finished
                45000044 8d8f4000 3f061097 cb61bfd9 ca314821 04160014 9610e710
                00000000 c0024000
15 15:28:55 IN  TCP       1 203.97.191.217:1046 192.168.72.33:20
                SYN attack finished
-------------------------------------------------------------------------------

Policy : test - Deny Events:
Date/Time   Dir Prot Number IP:Port <map> Dest IP:Port /Reason /IP header
-------------------------------------------------------------------------------
19 18:32:43 OUT TCP      10 192.168.72.33:23366 192.12.33.2:113
                Policy rejected
                45000033 c83d4000 40067f26 ca314821 c00c2102 5b460071 a207ca65
                04fb64e5 50187c00
19 20:32:35 OUT TCP       1 192.168.72.33:26973 210.55.162.101:25
                TCP open failed
19 21:34:54 OUT TCP      10 192.168.72.33:28897 12.7.242.94:113
                Policy rejected
                45000034 d9994000 40065072 ca314821 0c07f25e 70e10071 3d6a5027
                05014535 50187c00
20 01:59:51 OUT TCP       1 192.168.72.33:6595 210.55.162.101:25
                TCP open failed
20 09:53:37 OUT TCP       1 192.168.72.33:19610 207.46.131.137:80
                Policy rejected
                45000222 203e4000 4006b38d ca314821 cf2e8389 4c9a0050 644c1cf8
                0520df4d 50187c00
-------------------------------------------------------------------------------

Policy : test - Allow Events:
Date/Time   Dir Prot Number IP:Port <map> Dest IP:Port /Reason /IP header
-------------------------------------------------------------------------------
20 09:51:11 OUT TCP       1 192.168.72.33:17972 207.46.131.137:80
                TCP session started
20 09:51:39 IN  UDP       1 192.168.72.41:53 192.168.72.33:53
                UDP flow started
20 09:51:44 IN  TCP       1 128.230.18.29:2013 192.168.72.33:25
                TCP session started
20 09:51:44 IN  TCP       1 137.103.210.2:1345 192.168.72.33:25
                TCP session started
-------------------------------------------------------------------------------
```

Table 31-5: Parameters displayed in the output of the SHOW FIREWALL EVENT command.

| Parameter | Meaning |
|---|---|
| Policy | The name of the policy to which the following events apply. |
| Date/Time | The date and time of the event. |
| Dir | The direction of the flow; one of "IN" or "OUT". |
| Prot | The protocol for the flow; one of "ICMP", "TCP", "UDP" or the IP protocol number. |
| Number | The number of times the event has occurred. |
| IP:Port | The source IP address and port for the flow. |
| Dest IP:Port | The destination IP address and port for the flow. |
| Reason | The reason for the event record. |
| IP Header | A dump of the first nine octets of the IP header of the packet causing the event. |

**See Also**

DISABLE FIREWALL NOTIFY
ENABLE FIREWALL NOTIFY
SHOW FIREWALL ACCOUNTING
SHOW FIREWALL POLICY
SHOW FIREWALL SESSIONS

# SHOW FIREWALL POLICY

**Syntax**

```
SHOW FIREWALL POLICY=name [COUNTERS] [LIST] [SUMMARY]
```

where:

- *name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character ("_").

**Description**

This command displays detailed information about the specified or all policies (Figure 31-4 on page 31-37, Table 31-6 on page 31-37).

The POLICY parameter specifies the policy to be displayed. The specified policy must already exist. If a value is not specified then information for all policies is displayed.

The COUNTERS parameter displays counters for the specified policy or all policies (Figure 31-5 on page 31-40, Table 31-7 on page 31-41).

The LIST parameter displays information about address lists assigned to the specified policy or all policies (Figure 31-6 on page 31-43, Table 31-8 on page 31-43).

The SUMMARY parameter displays a summary of the information for each policy.

Figure 31-4: Example output from the SHOW FIREWALL POLICY command.

```
Policy : test
  Accounting ........................ enabled
  Enabled Logging Options ........... allow denydump
  Enabled Debug Options ............. checksum
  Enabled IP options ................ none
  Enabled ICMP forwarding ........... ping timeexceeded
  Receive of ICMP PINGS ............. enabled
  Number of Notifications ........... 0
  Number of Deny Events ............. 20
  Number of Allow Events ............ 8987
  Number of Active TCP Opens ........ 0
  Number of Active Sessions ......... 1
  Cache Hits ........................ 429073
  Discarded ICMP Packets ............ 74
  Private Interface : eth0
  Public Interface  : eth1
    Method .......................... dynamic
    NAT ............................. enhanced
      Method ........................ enhanced dynamic
      Private Interface ............. eth0
      Global IP ..................... 192.168.72.89
    Rule ............................ 2
      Action ........................ allow
      IP ............................ 202.36.163.20
      Protocol ...................... TCP
      Port .......................... 23
      Global IP ..................... 192.168.72.89
      Global Port ................... 23
      Days .......................... all
```

Table 31-6: Parameters displayed in the output of the SHOW FIREWALL POLICY command.

| Parameter | Meaning |
|---|---|
| Policy | The name of a policy. |
| Accounting | Whether or not accounting is enabled for the policy; one of “enabled” or “disabled”. |
| Enabled Logging Options | A list of the logging options currently enabled; one or more of “allow”, “deny”, “denydump”, “inaicmp”, “inallow”, “inaother”, “inatcp”, “inaudp”, “inddicmp”, “inddother”, “inddtcp”, “inddudp”, “inddump”, “indeny”, “indicmp”, “indother”, “indtcp”, “indudp”, “outaicmp”, “outallow”, “outaother”, “outatcp”, “outaudp”, “outddicmp”, “outddother”, “outddtcp”, “outddudp”, “outddump”, “outdeny”, “outdicmp”, “outdother”, “outdtcp”, “outdudp” or “none”. |
| Enabled Debug Options | A list of the debug options currently enabled; one or more of “all”, “packet”, “process” or “none”. |
| Enabled IP options | A list of the IP options allowed in IP packets to be forwarded by this policy; one or more of “all”, “record_route”, “security”, “sourceroute”, “timestamp” or “none”. |
| Enabled ICMP forwarding | A list of the ICMP packet types that will be forwarded by this policy; one or more of “all”, “parameter”, “ping”, “redirect”, “sourcequench”, “timeexceeded”, “timestamp”, “unreachable” or “none”. |

Table 31-6: Parameters displayed in the output of the SHOW FIREWALL POLICY command. (Continued)

| Parameter | Meaning |
|---|---|
| Receive of ICMP PINGS | Whether or not the reception of ICMP PING packets is enabled for this policy; one of “enabled” or “disabled”. |
| Number of Notifications | The number of notifications generated. |
| Number of Deny Events | The number of deny events for this policy. |
| Number of Allow Events | The number of allow events for this policy. |
| Number of Active TCP Opens | The number of currently active TCP connections for this policy. |
| Number of Active Sessions | The number of currently active sessions for this policy. |
| Cache Hits | The number of flow lookups found from the cache. |
| Discarded ICMP Packets | The number of ICMP packets discarded by this policy. |
| IP List | The name of an IP list assigned to this policy. |
| Hardware List | The name of a hardware address list assigned to this policy. |
| File name | The name of the file containing the list. |
| Number IP hosts | The number of IP hosts in the list. |
| Number Networks | The number of IP networks in the list. |
| Number MAC addresses | The number of MAC addresses in the list. |
| Private Interface | The name of a private interface assigned to the policy. |
| Public Interface | The name of a public interface assigned to the policy. |
| Method | The method used to packets to or from the public interface; one of “dynamic” or “passall”. |
| NAT | The type of NAT translation enabled; one of “standard” or “enhanced”. Only displayed when NAT is enabled on the policy. |
| NAT/Method | The method used to perform NAT translation; one of “none”, “static”, “dynamic”, “enhanced static”, “enhanced dynamic” or “enhanced interface”. This field depends on the combination of options configured in the ADD FIREWALL POLICY NAT command, and is only displayed when NAT is enabled on the policy. |
| NAT/Private Interface | The private interface to which NAT translations will apply. Only displayed when NAT is enabled on the policy. |
| NAT Global IP | The global IP address used by NAT translations. Only displayed when NAT is enabled on the policy. |
| Rule | The identifier for a rule associated with the private or public interface. |
| Action | The action to perform when a flow matches this rule; one of “allow” or “deny”. |
| IP List | The name (and file) of an IP list referenced by this rule. |
| Hardware List | The name (and file) of a hardware address list referenced by this rule. |
| Protocol | The IP protocol type to apply to this rule. |
| Port | The port number, service name (Table 31-2 on page 31-19) or range of port numbers to apply to this rule. |

Table 31-6: Parameters displayed in the output of the SHOW FIREWALL POLICY command. (Continued)

| Parameter | Meaning |
|---|---|
| Global IP | The IP address to apply to this rule, if NAT is active on the interface. |
| Global Port | The port number, service name (Table 31-2 on page 31-19) or range of port numbers to apply to this rule, if NAT is active on the interface. |
| Remote IP | The remote IP address to match for this rule. |
| Source Port | The source port to match for this rule. |
| Days | The days on which this rule is active; a list of one or more of “mon”, “tue”, “wed”, “thu”, “fri”, “sat”, “sun” or “all”. |
| After | The time of day after which this rule is active. |
| Before | The time of day before which this rule is active. |

Figure 31-5: Example output from the SHOW FIREWALL POLICY COUNTERS command.

```
Policy : test
  Accounting ......................... enabled
  Enabled Logging Options ........... allow denydump
  Enabled Debug Options ............. none
  Enabled IP options ................ none
  Enabled ICMP forwarding ........... ping timeexceeded
  Receive of ICMP PINGS ............. enabled
  Number of Notifications ........... 0
  Number of Deny Events ............. 20
  Number of Allow Events ............ 9101
  Number of Active TCP Opens ........ 0
  Number of Active Sessions ......... 1
  Cache Hits ........................ 430160
  Discarded ICMP Packets ............ 74
  Private Interface : eth0
    Total Packets Received .......... 186331
    Number Flows Started ............ 9083
    Number Cache Hits ............... 173174
    Number Dropped Packets .......... 0
    Number Unknown IP Protocols ..... 0
    Number Bad ICMP Packets ......... 0
    Number Dumped ICMP Packets ...... 0
    Number Spoofing Packets ......... 0
    Number Dropped GBLIP is Zero .... 0
    Number No Spare Entries ......... 0
    Number FTP Port Commands ........ 0
    Number Bad FTP Port Commands .... 0
  Public Interface  : eth1
    Method .......................... dynamic
    Total Packets Received .......... 264548
    Number Flows Started ............ 18
    Number Cache Hits ............... 256986
    Number Dropped Packets .......... 3751
    Number Unknown IP Protocols ..... 0
    Number Bad ICMP Packets ......... 0
    Number Dumped ICMP Packets ...... 0
    Number Spoofing Packets ......... 0
    Number Dropped GBLIP is Zero .... 0
    Number No Spare Entries ......... 0
    Number FTP Port Commands ........ 0
    Number Bad FTP Port Commands .... 0
    NAT ............................. enhanced
      Method ........................ enhanced dynamic
      Private Interface ............. eth0
      Global IP ..................... 192.168.72.89
    Rule ............................ 2
      Action ........................ allow
      IP ............................ 202.36.163.20
      Protocol ...................... TCP
      Port .......................... 23
      Global IP ..................... 192.168.72.89
      Global Port ................... 23
      Number Hits ................... 0
      Days .......................... all
```

Table 31-7: Parameters displayed in the output of the SHOW FIREWALL POLICY COUNTERS command.

| Parameter | Meaning |
|---|---|
| Policy | The name of a policy. |
| Accounting | Whether or not accounting is enabled for the policy; one of "enabled" or "disabled". |
| Enabled Logging Options | A list of the logging options currently enabled; one or more of "allow", "deny", "denydump", "inaicmp", "inallow", "inaother", "inatcp", "inaudp", "inddicmp", "inddother", "inddtcp", "inddudp", "inddump", "indeny", "indicmp", "indother", "indtcp", "indudp", "outaicmp", "outallow", "outaother", "outatcp", "outaudp", "outddicmp", "outddother", "outddtcp", "outddudp", "outddump", "outdeny", "outdicmp", "outdother", "outdtcp", "outdudp" or "none". |
| Enabled Debug Options | A list of the debug options currently enabled; one or more of "all", "packet", "process" or "none". |
| Enabled IP options | A list of the IP options allowed in IP packets to be forwarded by this policy; one or more of "all", "record_route", "security", "sourceroute", "timestamp" or "none". |
| Enabled ICMP forwarding | A list of the ICMP packet types that will be forwarded by this policy; one or more of "all", "parameter", "ping", "redirect", "sourcequench", "timeexceeded", "timestamp", "unreachable" or "none". |
| Receive of ICMP PINGS | Whether or not the reception of ICMP PING packets is enabled for this policy; one of "enabled" or "disabled". |
| Number of Notifications | The number of notifications generated. |
| Number of Deny Events | The number of deny events for this policy. |
| Number of Allow Events | The number of allow events for this policy. |
| Number of Active TCP Opens | The number of currently active TCP connections for this policy. |
| Number of Active Sessions | The number of currently active sessions for this policy. |
| Cache Hits | The number of flow lookups found from the cache. |
| Discarded ICMP Packets | The number of ICMP packets discarded by this policy. |
| IP List | The name of an IP list assigned to this policy. |
| Hardware List | The name of a hardware address list assigned to this policy. |
| File name | The name of the file containing the list. |
| Number IP hosts | The number of IP hosts in the list. |
| Number Networks | The number of IP networks in the list. |
| Number MAC addresses | The number of MAC addresses in the list. |
| Private Interface | The name of a private interface assigned to the policy. |
| Public Interface | The name of a public interface assigned to the policy. |
| Total Packets Received | The total number of packets received on the interface. |
| Number Flows Started | The number of flows started on the interface. |
| Number Cache Hits | The number of flow lookups for the interface found from the cache. |
| Number Dropped Packets | The number of packets received on the interface that were dropped. |

Table 31-7: Parameters displayed in the output of the SHOW FIREWALL POLICY COUNTERS command. (Continued)

| Parameter | Meaning |
|---|---|
| Number Unknown IP Protocols | The number of packets received on the interface with an unknown IP protocol. |
| Number Bad ICMP Packets | The number of badly formatted ICMP packets received on the interface. |
| Number Dumped ICMP Packets | The number of ICMP packets received on the interface that were dumped. |
| Number Spoofing Packets | The number of Smurf attack packets received on the interface. |
| Number Dropped GBLIP Zero | The number of packets received on the interface that were dumped because the global IP address was zero. |
| Number No Spare Entries | The number of packets received on the interface that were dumped because the system had insufficient memory. |
| Number FTP Port Commands | The number of valid FTP port commands received on the interface. |
| Number Bad FTP Port Commands | The number of invalid FTP port commands received on the interface. |
| Method | The method used to packets to or from the public interface; one of “dynamic” or “passall”. |
| NAT | The type of NAT translation enabled; one of “standard” or “enhanced”. Only displayed when NAT is enabled on the policy. |
| NAT/Method | The method used to perform NAT translation; one of “none”, “static“, “dynamic“, “enhanced static“, “enhanced dynamic“ or “enhanced interface”. This field depends on the combination of options configured in the ADD FIREWALL POLICY NAT command, and is only displayed when NAT is enabled on the policy. |
| NAT/Private Interface | The private interface to which NAT translations will apply. Only displayed when NAT is enabled on the policy. |
| NAT Global IP | The global IP address used by NAT translations. Only displayed when NAT is enabled on the policy. |
| Rule | The identifier for a rule associated with the private or public interface. |
| Action | The action to perform when a flow matches this rule; one of “allow” or “deny”. |
| IP List | The name (and file) of an IP list referenced by this rule. |
| Hardware List | The name (and file) of a hardware address list referenced by this rule. |
| Protocol | The IP protocol type to apply to this rule. |
| Port | The port number, service name (Table 31-2 on page 31-19) or range of port numbers to apply to this rule. |
| Global IP | The IP address to apply to this rule, if NAT is active on the interface. |
| Global Port | The port number, service name (Table 31-2 on page 31-19) or range of port numbers to apply to this rule, if NAT is active on the interface. |
| Remote IP | The remote IP address to match for this rule. |

Table 31-7: Parameters displayed in the output of the SHOW FIREWALL POLICY COUNTERS command. (Continued)

| Parameter | Meaning |
|---|---|
| Source Port | The source port to match for this rule. |
| Days | The days on which this rule is active; a list of one or more of "mon", "tue", "wed", "thu", "fri", "sat", "sun" or "all". |
| After | The time of day after which this rule is active. |
| Before | The time of day before which this rule is active. |

Figure 31-6: Example output from the SHOW FIREWALL POLICY LIST command.

```
Policy : office

Hardware List : devices ( listmac.txt )
MAC Address        Label
-------------------------------------------------------------------------------
00-00-cd-02-03-01
00-00-cd-02-03-05  John's PC
00-00-ef-39-08-01  access server
-------------------------------------------------------------------------------

IP List : iphosts ( listip.txt )
IP              - IP               Label
-------------------------------------------------------------------------------
192.168.163.6                      FTP host
192.168.16.0      192.168.16.255   Test network
-------------------------------------------------------------------------------
```

Table 31-8: Parameters displayed in the output of the SHOW FIREWALL POLICY LIST command.

| Parameter | Meaning |
|---|---|
| Policy | The name of a policy. |
| Hardware List | The name (and filename) of a hardware address list assigned to this policy. |
| IP List | The name (and filename) of an IP list assigned to this policy. |
| MAC address | A hardware address in the hardware address list. |
| IP | A IP address or network in the IP address list |
| Label | The name of the host associated with the address. |

See Also

ADD FIREWALL POLICY INTERFACE
ADD FIREWALL POLICY LIST
ADD FIREWALL POLICY NAT
ADD FIREWALL POLICY RULE
CREATE FIREWALL POLICY
DELETE FIREWALL POLICY INTERFACE
DELETE FIREWALL POLICY LIST
DELETE FIREWALL POLICY NAT
DELETE FIREWALL POLICY RULE
DESTROY FIREWALL POLICY
DISABLE FIREWALL NOTIFY
DISABLE FIREWALL POLICY
ENABLE FIREWALL NOTIFY
ENABLE FIREWALL POLICY
SET FIREWALL POLICY RULE
SHOW FIREWALL
SHOW FIREWALL EVENTS

# SHOW FIREWALL SESSION

Syntax

```
SHOW FIREWALL SESSION[=session-number] [POLICY=name]
   [COUNTERS] [PORT={port-port|service-name}]
   [PROTOCOL={protocol|ALL|EGP|ICMP|OSPF|TCP|UDP}]
   [SUMMARY]
```

where:

- *session-number* is the identifier for a currently active session.
- *name* is a character string, 1 to 15 characters in length. Valid characters are letters (a–z, A–Z), digits (0–9) and the underscore character (“_”).
- *port* is an Internet service port number or name.
- *service-name* is a predefined name for an IP service (Table 31-2 on page 31-19).
- *protocol* is an Internet IP protocol number.

Description

This command displays information about the sessions and flows currently active for the specified policy (Figure 31-7 on page 31-45). If SESSION is specified, only information about the specified session is displayed. Otherwise, information about all sessions is displayed.

The POLICY parameter specifies the policy for which session information is to be displayed. The specified policy must already exist. If a value is not specified, session information for all policies is displayed.

If COUNTERS is specified, session counters for the specified policy are displayed.

If SUMMARY is specified, only summary information for the specified policy is displayed.

If PROTOCOL is specified, the display is limited to sessions based on the specified IP protocol type.

If PORT is specified, the display is limited to sessions between ports in the specified range of ports or using the specified service (Table 31-2 on page 31-19).

Figure 31-7: Example output from the SHOW FIREWALL SESSION command.

```
Policy : test
Current Sessions
-------------------------------------------------------------------------------
cc2b TCP  202.36.163.10:1383    192.168.72.89:52267    192.168.72.50:21
     TCP state ............................ established
     Start time ........................... 17:58:57 19-Apr-1999
     Minutes to deletion .................. 536
-------------------------------------------------------------------------------
```

Table 31-9: Parameters displayed in the output of the SHOW FIREWALL SESSION command.

| Parameter | Meaning |
|---|---|
| Policy | The name of a policy. |
| *hex-num* | The session identifier |
| TCP/UDP/*number* | The IP protocol (one of "TCP", "UDP" or an IP protocol number), followed by the source address:port, the global IP address:mapped port, and the destination IP address:port |
| Packets from private IP | The number of packets forwarded from the private network to the public network. |
| Octets from private IP | The number of octets forwarded from the private network to the public network. |
| Packets to private IP | The number of packets forwarded from the public network to the private network. |
| Octets to private IP | The number of octets forwarded from the public network to the private network. |
| TCP state | The state of the TCP session; one of "free", "closed", "listen", "synSent", "synReceived", "established", "finWait1", "finWait2", "closeWait", "lastAck", "closing", "timeWait", "deleteTCB", "synSent", "synReceived" or "RADIUS query". |
| Private SEQ number | The current sequence number for the TCP connection to the private IP address. |
| Private ACK number | The current acknowledgement number for the TCP connection to the private IP address. |
| Private max window size | The current maximum window size for the TCP connection to the private IP address. |
| Public SEQ number | The current sequence number for the TCP connection to the public IP address. |
| Public ACK number | The current acknowledgement number for the TCP connection to the public IP address. |
| Public max window size | The current maximum window size for the TCP connection to the public IP address. |
| Sequence Delta | The different between the current sequence numbers for the private and public connections. |

Table 31-9: Parameters displayed in the output of the SHOW FIREWALL SESSION command. (Continued)

| Parameter | Meaning |
|---|---|
| ICMP type | The type of ICMP request, for ICMP sessions; one of "Echo request", "Time request", "Name request" or "Unknown ICMP type". |
| Start time | The date and time that the session was started. |
| Minutes to deletion | The number of minutes remaining before the session is automatically deleted. |

See Also DELETE FIREWALL SESSION
SHOW FIREWALL EVENTS
SHOW FIREWALL POLICY