Configuring Security Policies on Firewall Devices

You can configure general security settings for the device using the General page and the Timeouts page under Platform > Security. You can enable anti-spoofing on interfaces, configure IP fragment settings, and configure a variety of timeout values for the device.

This chapter contains the following topics:

General Page

Use the General page to configure security settings that help protect against malformed packets, spoofed packets, fragmented packets, and denial of service attacks. See Configuring Floodguard, Anti-Spoofing and Fragment Settings, page 57-2 for more information about the settings on this page.

Navigation Path

- (Device view) Select **Platform > Security > General** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Security > General** from the Policy Type selector. Select an existing policy from the Shared Policy selector, or create a new one.

Related Topics

- Chapter 57, "Configuring Security Policies on Firewall Devices"
- Add/Edit General Security Configuration Dialog Box, page 57-3
- Configuring Timeouts, page 57-4

Field Reference

Table 57-1 General Page

Element	Description
Disable Floodguard (PIX 6.3 and FWSM 2.x only)	Check this box to disable Floodguard on the firewall device. This option is available only on PIX 6.3 and FWSM 2.x devices. See Configuring Floodguard, Anti-Spoofing and Fragment Settings, page 57-2 for more information about the Floodguard feature.

Table 57-1 General Page (continued)

Element	Description
Global Fragment Settings	
Use these options to configure global fragment settings for the device. You can override these settings for individual interfaces; see Add/Edit General Security Configuration Dialog Box, page 57-3 for more information.	
Enable Default Settings	Check this box to enable the default fragment settings fields.
Size	Specify the maximum number of fragments that can be in the IP re-assembly database waiting for re-assembly. The default is 200.
Chain	Specify the maximum number of fragments into which a full IP packet can be fragmented. The default is 24 packets.
Timeout	Specify the maximum number of seconds to wait for an entire fragmented packet to arrive. The timer starts after the first fragment of a packet arrives. If all fragments of the packet do not arrive by the number of seconds specified, all fragments of the packet that were already received will be discarded. The default is 5 seconds.
Interface Configuration Table	
This table lists all interfaces on which individual anti-spoofing and fragment settings have been defined. Refer to Configuring Floodguard, Anti-Spoofing and Fragment Settings, page 57-2 for more information about these settings. Refer to Add/Edit General Security Configuration Dialog Box, page 57-3 for more information about configuring these settings on individual interfaces.	

Configuring Floodguard, Anti-Spoofing and Fragment Settings

Use the General page under Platform > Security to enable or disable Floodguard (on a PIX 6.3 or FWSM 2.x device), to enable Unicast Reverse Path Forwarding (anti-spoofing) on individual interfaces, and to configure IP fragment settings for the device, and for each interface of the device.

Floodguard

Floodguard lets you reclaim firewall resources if the user authentication subsystem runs out of resources. If an inbound or outbound `uauth` connection is being attacked or overused, the firewall will actively reclaim TCP user resources.

If the user authentication subsystem is depleted, TCP user resources in different states are reclaimed in the following order, depending on urgency:

1. Timewait
2. LastAck
3. FinWait
4. Embryonic
5. Idle

Floodguard is enabled by default. This option applies only to PIX 6.3 or FWSM 2.x devices.

Anti-spoofing

Unicast Reverse Path Forwarding (RPF) guards against IP spoofing—a packet using an incorrect source IP address to obscure its true source—by ensuring that all packets have a source IP address that matches the correct source interface according to the routing table.

Normally, the security appliance looks only at the destination address when determining where to forward the packet. Unicast RPF instructs the security appliance to also look at the source address; this is why it is called Reverse Path Forwarding. For any traffic that you want to allow through the security appliance, the security appliance routing table must include a route back to the source address. See RFC 2267 for more information.

With outside traffic, for example, the security appliance can use the default route to satisfy the Unicast RPF protection. If traffic enters from an outside interface, and the source address is not known to the routing table, the security appliance uses the default route to correctly identify the outside interface as the source interface.

If traffic enters the outside interface from an address that is known to the routing table, but is associated with the inside interface, the security appliance drops the packet. Similarly, if traffic enters the inside interface from an unknown source address, the security appliance drops the packet because the matching route (the default route) indicates the outside interface.

Unicast RPF is implemented as follows:

- ICMP packets have no session, so each packet is checked.
- UDP and TCP have sessions, so the initial packet requires a reverse route look-up. Subsequent packets arriving during the session are checked using an existing state maintained as part of the session. Non-initial packets are checked to ensure they arrived on the same interface used by the initial packet.

Fragment Settings

Fragment settings provide management of packet fragmentation and improve compatibility with the Network File System (NFS). By default, the security appliance allows up to 24 fragments per IP packet, and up to 200 fragments awaiting reassembly. You might need to allow fragments on your network if you have an application that routinely fragments packets, such as NFS over UDP. However, if you do not have an application that fragments traffic, we recommend that you do not allow fragments through the security appliance, as fragmented packets are often used as DoS attacks.

Related Topics

- General Page, page 57-1
- Add/Edit General Security Configuration Dialog Box, page 57-3

Add/Edit General Security Configuration Dialog Box

Use the Add/Edit General Security Configuration dialog box to enable or disable anti-spoofing, and to configure override fragment settings, for an interface.

Navigation Path

You can access the Add/Edit General Security Configuration dialog box from the Anti-Spoofing and Fragment Interface Configuration table on the Platform > Security > General Page, page 57-1.

Related Topics

- Chapter 57, “Configuring Security Policies on Firewall Devices”

- Configuring Floodguard, Anti-Spoofing and Fragment Settings, page 57-2

Field Reference

Table 57-2 Add/Edit General Security Configuration Dialog Box

Element	Description
Interface	Enter or Select the name of the interface for which you want to configure anti-spoofing or fragment settings.
Enable Anti-Spoofing	Check this box to enable Unicast RPF (anti-spoofing) on the specified interface.
Override Default Fragment Settings	To override the default fragment settings on the specified interface, check this box to enable the following fields, and then enter the new values. See the General Page, page 57-1 for the default global fragment settings on the device.
Size	Specify the maximum number of fragments that can be in the IP re-assembly database waiting for re-assembly for the specified interface. The default is 200.
Chain	Specify the maximum number of fragments into which a full IP packet can be fragmented for the specified interface. The default is 24 packets.
Timeout	Specify the maximum number of seconds to wait for an entire fragmented packet to arrive on the specified interface. The timer starts after the first fragment of a packet arrives. If all fragments of the packet do not arrive by the number of seconds specified, all fragments of the packet that were already received will be discarded. The default is 5 seconds.

Configuring Timeouts

The Timeouts page lets you set a variety of timeout values on the security appliance. All times are in the format **hh:mm:ss**.

These values represent idle timeouts for the connection and translation slots for various protocols. If a slot has not been used for the idle time specified, the resource is returned to the free pool. TCP connection slots are freed approximately 60 seconds after a normal connection close sequence.

Warning **We recommend that you do not change these values unless advised to do so by Customer Support.**

Navigation Path

- (Device view) Select **Platform > Security > Timeouts** from the Device Policy selector.
- (Policy view) Select **PIX/ASA/FWSM Platform > Security > Timeouts** from the Policy Types selector. Select an existing policy from the Policies selector, or create a new one.

Related Topics

- Chapter 57, "Configuring Security Policies on Firewall Devices"

Field Reference

Table 57-3 Timeouts Page

Element	Description
To change the timeout value for a parameter, click the radio button to the left of the parameter entry to activate it, and then enter the new value in the parameter field. To reset any value to its default, click the related Default button. Clicking the Disable button, where provided, disables the timeout by setting its value to 0:00:00. Follow either of the procedures in the previous paragraph to re-enable a disabled value.	
Translation Slot (xlate)	Length of time idle until a translation slot is freed. This value must be at least 1 minute; the default is 3 hours. Enter 0:00:00 to disable this timeout.
Connection (conn)	Length of time idle until a connection slot is freed. This value must be at least 5 minutes; the default is 1 hour. Click Disable or enter 0:00:00 to disable this timeout.
Half-Closed	Length of time idle until a half-closed TCP connection is closed. For ASA 9.1.2 and later devices, the minimum is 30 seconds. For all other devices, the minimum is 5 minutes. The default is 10 minutes. Click Disable or enter 0:00:00 to disable this timeout.
UDP	Length of time idle until a UDP protocol connection is closed. This value must be at least 1 minute; the default is 2 minutes. Click Disable or enter 0:00:00 to disable this timeout.
SCTP	Length of time idle until a SCTP protocol connection is closed. This value must be at least 1 minute; the default is 2 minutes. Click Disable or enter 0:00:00 to disable this timeout.
Connection Holddown	Length of time idle until traffic is forwarded. This is the time for which the ASA waits before forwarding traffic, to avoid route flapping.This value must be at least 1 second; the default is 15 seconds. Click Disable or enter 0:00:00 to disable this timeout.
ICMP (PIX 7.x+, ASA, FWSM 3.x+)	Length of time idle after which general ICMP states are closed.
RPC/Sun RPC	Length of time idle until a SunRPC slot is freed. This value must be at least 1 minute; the default is 10 minutes. Click Disable or enter 0:00:00 to disable this timeout.
H.225	Length of time idle until an H.225 signaling connection is closed. The H.225 default timeout is 1 hour (01:00:00). Setting the value to 00:00:00 means never close the connection. To close a connection immediately after all calls are cleared, enter 1 second (0:00:01).
H.323	Length of time idle until an H.323 media connection is closed. The default is 5 minutes. Click Disable or enter 0:00:00 to disable this timeout.
MGCP	Length of time idle after which MGCP media ports are closed. The default is 5 minutes (0:05:00). Click Disable or enter 0:00:00 to disable this timeout.
MGCP PAT (PIX 7.x+, ASA, FWSM 3.x+)	Length of time idle after which an MGCP PAT translation is removed. The minimum time is 30 seconds; the default is 5 minutes (0:05:00). Click Disable or enter 0:00:00 to disable this timeout.

Table 57-3 Timeouts Page (continued)

Element	Description
SIP	Length of time idle until an SIP signaling port connection is closed. This value must be at least 5 minutes; the default is 30 minutes. Click Disable or enter 0:00:00 to disable this timeout.
SIP Media	Length of time idle until an SIP media port connection is closed. This value must be at least 1 minute; the default is 2 minutes. Click Disable or enter 0:00:00 to disable this timeout.
SIP Disconnect (PIX 6.3(5), PIX/ASA 7.2+, FWSM 3.2+)	Length of time idle after which a SIP session is deleted if the 200 OK is not received for a CANCEL or a BYE message. The minimum value is 0:00:01; the maximum value is 0:10:00. The default value is 0:02:00.
SIP Invite (PIX 6.3(5), PIX/ASA 7.2+, FWSM 3.2+)	Length of time idle after which pinholes for PROVISIONAL responses and media xlates will be closed. The minimum value is 0:01:00; the maximum value is 0:30:00. The default value is 0:03:00.
SIP Provisional Media (PIX/ASA 7.2(3)+)	The timeout value for SIP provisional media connections; must be a value between 0:01:00 and 1193:00:00. The default is 2 minutes.
Auth. (uath) Absolute	Length of time until the authentication cache times out and new connections must be re-authenticated. The system waits until a user starts a new connection to prompt for re-authentication. This time must be shorter than the Translation Slot value. Click Disable or enter 0:00:00 to disable caching and require re-re-authentication on every new connection. **Note** Do not set this value to 0:00:00 if passive FTP is used on the connections. **Note** If you set this value to 0:00:00; HTTPS authentication may not work. If a browser initiates multiple TCP connections to load a Web page after HTTPS authentication, the first connection is permitted through, but subsequent connections trigger authentication. As a result, users are continuously presented with an authentication page, even after successful authentication. To work around this, set the authentication absolute timeout to 1 second. However, this workaround opens a one-second window of opportunity that might allow non-authenticated users through the firewall if they are coming from the same source IP address.
Auth. (uath) Inactivity	Length of time idle until the authentication cache times out and users have to re-authenticate new connections. This duration must be shorter than the Translation Slot value.
IGP	The Cisco ASA supports Non-Stop Forwarding from software Version 9.3.1 and later for dynamic routing protocols— Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF). The length of convergence time of Open Shortest Path First (OSPF) is 70 seconds by default. Using this field, you can change the length of the convergence time. This value must be within the range of 10 seconds to 1 hour and 40 seconds. The default value for IGP is 0:01:10.