Enabling Multiple Context Mode

This chapter describes how to use security contexts and enable multiple context mode. This chapter includes the following sections:

Security Context Overview

You can partition a single security appliance into multiple virtual devices, known as security contexts. Each context is an independent device, with its own security policy, interfaces, and administrators. Multiple contexts are similar to having multiple standalone devices. Many features are supported in multiple context mode, including routing tables, firewall features, IPS, and management. Some features are not supported, including VPN and dynamic routing protocols.

In multiple context mode, the security appliance includes a configuration for each context that identifies the security policy, interfaces, and almost all the options you can configure on a standalone device. The system administrator adds and manages contexts by configuring them in the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the security appliance. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the admin context.

The admin context is just like any other context, except that when a user logs in to the admin context, then that user has system administrator rights and can access the system and all other contexts.

This section provides an overview of security contexts, and includes the following topics:

Common Uses for Security Contexts

You might want to use multiple security contexts in the following situations:

- You are a service provider and want to sell security services to many customers. By enabling multiple security contexts on the security appliance, you can implement a cost-effective, space-saving solution that keeps all customer traffic separate and secure, and also eases configuration.
- You are a large enterprise or a college campus and want to keep departments completely separate.
- You are an enterprise that wants to provide distinct security policies to different departments.
- You have any network that requires more than one security appliance.

Unsupported Features

Multiple context mode does not support the following features:

- Dynamic routing protocols

  Security contexts support only static routes. You cannot enable OSPF or RIP in multiple context mode.
- VPN
- Multicast

Context Configuration Files

Each context has its own configuration file that identifies the security policy, interfaces, and, for supported features, all the options you can configure on a standalone device. You can store context configurations on the internal Flash memory or the external Flash memory card, or you can download them from a TFTP, FTP, or HTTP(S) server.

In addition to individual security contexts, the security appliance also includes a system configuration that identifies basic settings for the security appliance, including a list of contexts. Like the single mode configuration, this configuration resides as the startup configuration.

The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from a server), it uses one of the contexts that is designated as the admin context. The system configuration does include a specialized failover interface for failover traffic only. If your system is already in multiple context mode, or if you convert from single mode, the admin context is created automatically as a file on the internal Flash memory called admin.cfg. This context is named “admin.” If you do not want to use admin.cfg as the admin context, you can change the admin context.

How the Security Appliance Classifies Packets

Each packet that enters the security appliance must be classified, so that the security appliance can determine to which context to send a packet. The classifier uses the following rules to assign the packet to a context:

1. If only one context is associated with the ingress interface, the security appliance classifies the packet into that context.

   In transparent firewall mode, unique interfaces for contexts are required, so this method is used to classify packets at all times.

2. If multiple contexts are associated with the ingress interface, then the security appliance classifies the packet into a context by matching the destination address to one of the following context configurations:

   a. Interface IP address (the **ip address** command)

      The classifier looks at the interface IP address for traffic destined to an interface, such as management traffic.

   b. Global address in a static NAT statement (the **static** command)

      The classifier only looks at **static** commands where the global interface matches the ingress interface of the packet.

   c. Global NAT pool address (the **global** command)

      The classifier looks at IP addresses identified by a global pool for the ingress interface.

Note The classifier does not use a NAT exemption configuration for classification purposes because NAT exemption does not identify a global interface.

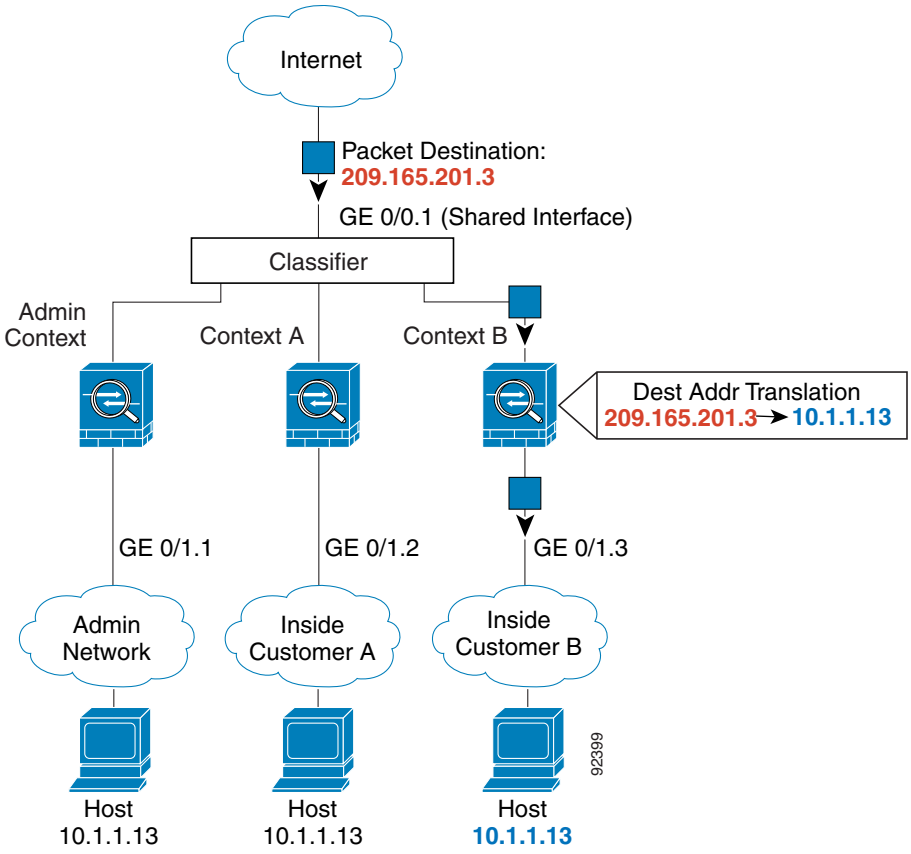
A packet must be classified in to a context based on one of the above methods. For example, if a context includes a static route that points to an external router as the next-hop to a subnet, and a different context includes a **static** command for the same subnet, then the classifier uses the **static** command to classify packets destined for that subnet and ignores the static route.

For example, if each context has unique interfaces, then the classifier associates the packet with the context based on the ingress interface. If you share an interface across contexts, however, then the classifier uses the destination address.

Because the destination address classification requires NAT (for through traffic), be sure to use unique interfaces for each context if you do not use NAT. Alternatively, you can add a **global** command to the ingress interface that specifies the real addresses in a context; a matching **nat** command is not required for classification purposes.

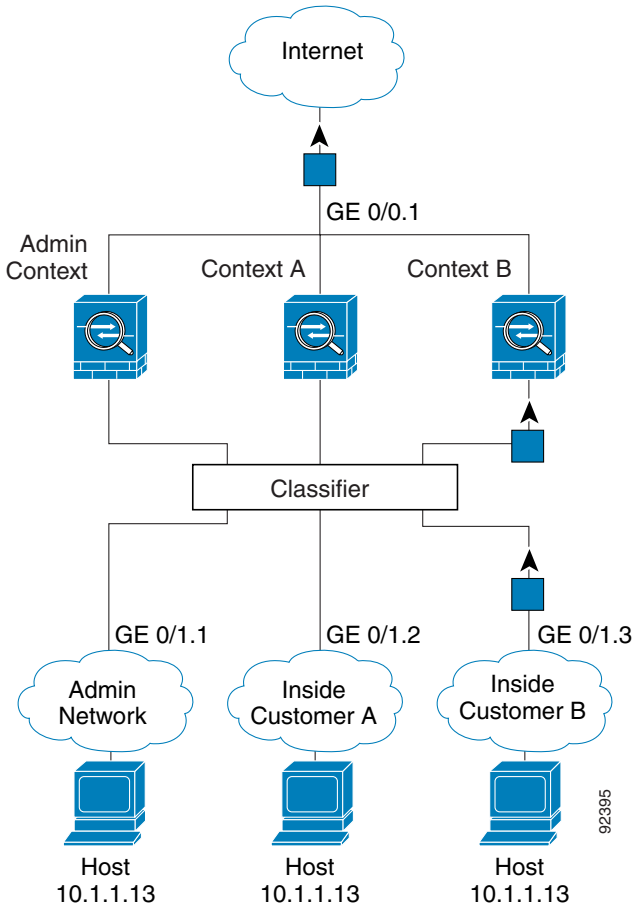
Figure 3-1 shows multiple contexts sharing an outside interface, while the inside interfaces are unique, allowing overlapping IP addresses. The classifier assigns the packet to Context B because Context B includes the address translation that matches the destination address.

Figure 3-1 Packet Classification with a Shared Interface



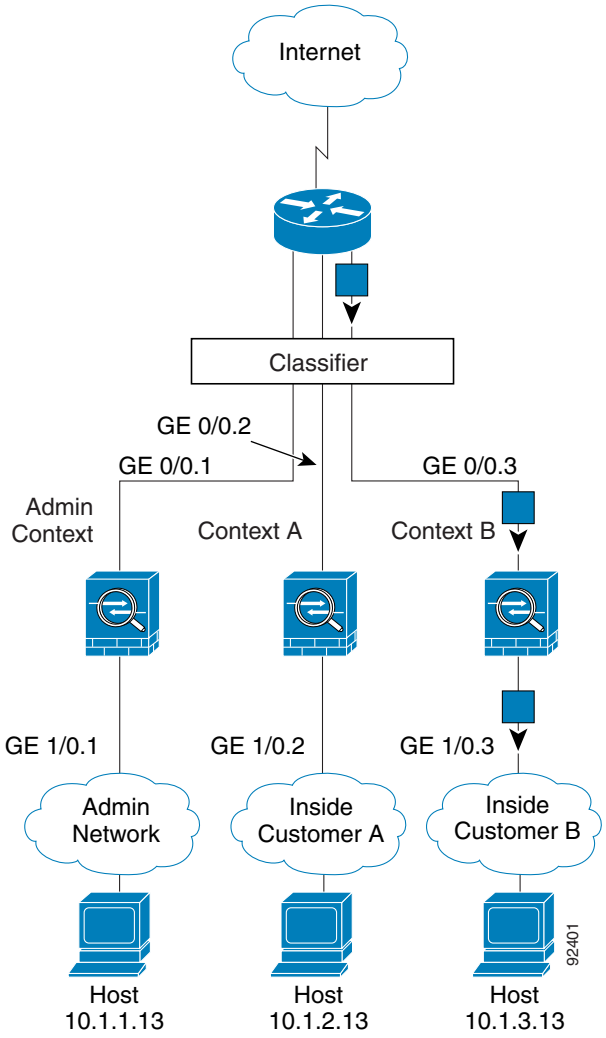
Note that all new incoming traffic must be classified, even from inside networks. Figure 3-2 shows a host on the Context B inside network accessing the Internet. The classifier assigns the packet to Context B because the ingress interface is Gigabit Ethernet 0/1.3, which is assigned to Context B.

Figure 3-2 Incoming Traffic from Inside Networks



For transparent firewalls, you must use unique interfaces. For the classifier, the lack of NAT support in transparent mode leaves unique interfaces as the only means of classification. Figure 3-3 shows a host on the Context B inside network accessing the Internet. The classifier assigns the packet to Context B because the ingress interface is Gigabit Ethernet 1/0.3, which is assigned to Context B.

Figure 3-3 Transparent Firewall Contexts



Sharing Interfaces Between Contexts

Routed Mode Only

The security appliance lets you share an interface between contexts. For example, you might share the outside interface to conserve interfaces. You can also share inside interfaces to share resources between contexts.

This section includes the following topics:

Shared Interface Guidelines

If you want to allow traffic from a shared interface through the security appliance, then you must translate the *destination* addresses of the traffic; the classifier relies on the address translation configuration to classify the packet within a context. If you do not want to perform NAT, you can still ensure classification into a context by specifying a **global** command for the shared interface: the **global** command specifies the real destination addresses, and a matching **nat** command is not required. (If you share an interface, and you allow only management traffic to and from the interface, then the classifier uses the interface IP address configuration to classify the packets. NAT configuration does not enter into the process.)

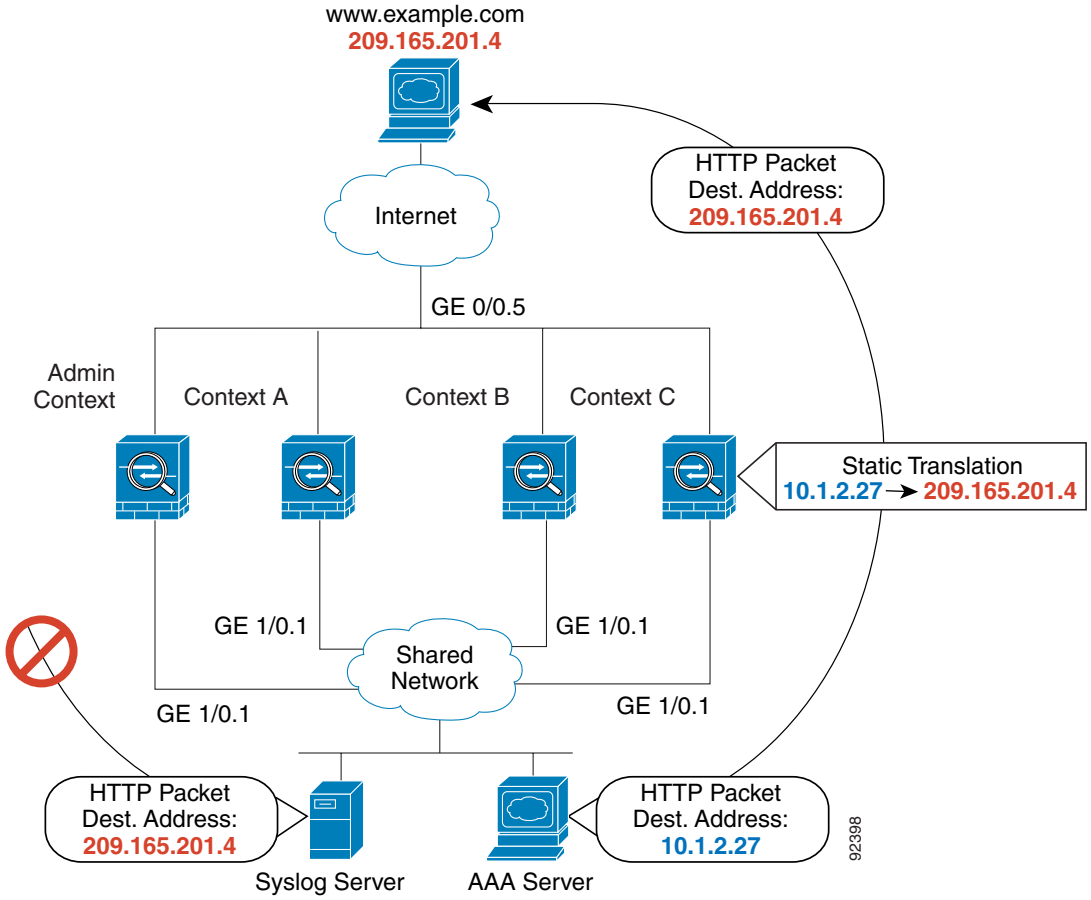
The type of NAT configured for the destination address determines whether the traffic can originate on the shared interface or if it can only respond to an existing connection. When you use dynamic NAT for the destination addresses, you cannot initiate a connection to those addresses. Therefore, traffic from the shared interface must be in response to an existing connection. Static NAT, however, lets you initiate connections, so if you use static NAT for the destination addreses, you can initiate connections on the shared interface.

When you have an outside shared interface (connected to the Internet, for example), the destination addresses on the inside are limited, and are known by the system administrator, so configuring NAT for those addresses is easy, even if you want to configure static NAT.

Configuring an inside shared interface poses a problem, however, if you want to allow communication between the shared interface and the Internet, where the destination addresses are unlimited. For example, if you want to allow inside hosts on the shared interface to initiate traffic to the Internet, then you need to configure static NAT statements for each Internet address. This requirement necessarily limits the kind of Internet access you can provide for users on an inside shared interface. (If you intend to statically translate addresses for Internet servers, then you also need to consider DNS entry addresses and how NAT affects them. For example, if a server sends a packet to www.example.com, then the DNS server needs to return the translated address. Your NAT configuration determines DNS entry management.)

Figure 3-4 shows two servers on an inside shared interface. One server sends a packet to the translated address of a web server, and the security appliance classifies the packet to go through Context C because it includes a static translation for the address. The other server sends the packet to the real untranslated address, and the packet is dropped because the security appliance cannot classify it.

Figure 3-4 Originating Traffic on a Shared Interface

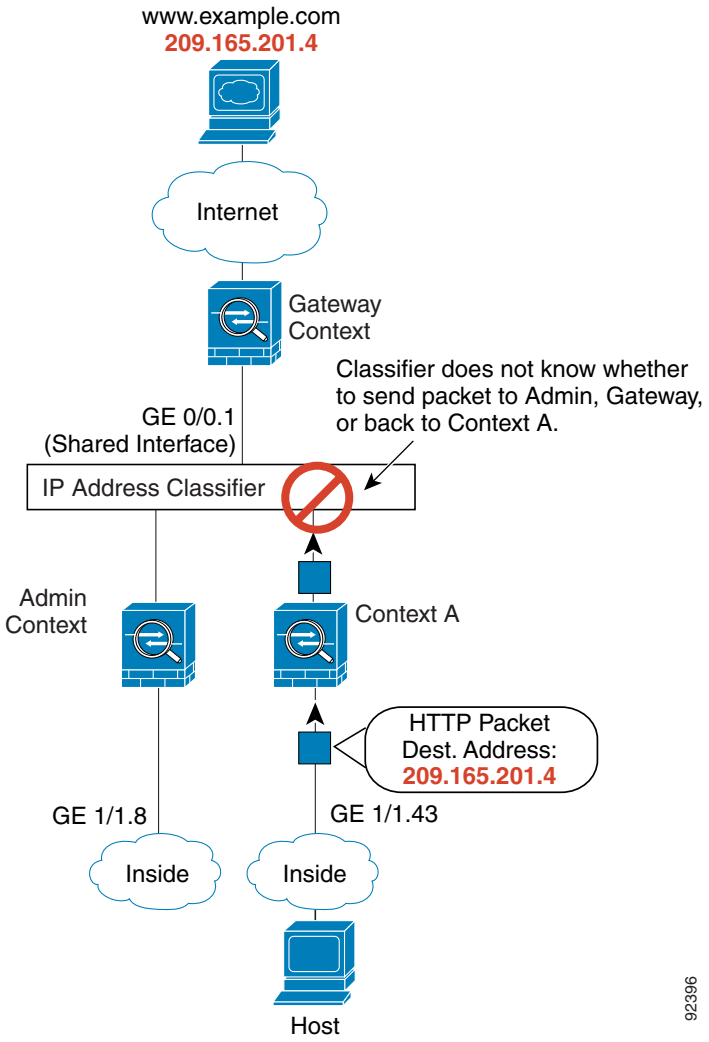


Cascading Security Contexts

Because of the limitation for originating traffic on a shared interface, a scenario where you place one context behind another requires that you configure static statements in the top context for every single outside address that bottom context users want to access.

Figure 3-5 shows a user in the bottom context (Context A) trying to access www.example.com. Because the Gateway Context does not have a static translation for www.example.com, the user cannot access the web server; the classifier does not know which context on the shared interface to assign the packet.

Figure 3-5 Cascading Contexts



Logging into the Security Appliance in Multiple Context Mode

When you access the security appliance console, you access the system execution space. If you later configure Telnet or SSH access to a context, you can log in to a specific context. If you log in to a specific context, you can only access the configuration for that context. However, if you log in to the admin context or the system execution space, you can access all contexts.

When you change to a context from admin, you continue to use the username and command authorization settings set in the admin context.

The system execution space does not support any AAA commands, but you can configure its own enable password, as well as usernames in the local database to provide individual logins.

Enabling or Disabling Multiple Context Mode

Your security appliance might already be configured for multiple security contexts depending on how you ordered it from Cisco. If you are upgrading, however, you might need to convert from single mode to multiple mode by following the procedures in this section. ASDM does not support changing modes, so you need to change modes using the CLI.

This section includes the following topics:

Backing Up the Single Mode Configuration

When you convert from single mode to multiple mode, the security appliance converts the running configuration into two files. The original startup configuration is not saved, so if it differs from the running configuration, you should back it up before proceeding.

Enabling Multiple Context Mode

The context mode (single or multiple) is not stored in the configuration file, even though it does endure reboots. If you need to copy your configuration to another device, set the mode on the new device to match using the **mode** command.

When you convert from single mode to multiple mode, the security appliance converts the running configuration into two files: a new startup configuration that comprises the system configuration, and admin.cfg that comprises the admin context (in the root directory of the internal Flash memory). The original running configuration is saved as old_running.cfg (in the root directory of the internal Flash memory). The original startup configuration is not saved. The security appliance automatically adds an entry for the admin context to the system configuration with the name “admin.”

To enable multiple mode, enter the following command:

```
hostname(config)# mode multiple
```

You are prompted to reboot the security appliance.

Restoring Single Context Mode

If you convert from multiple mode to single mode, you might want to first copy a full startup configuration (if available) to the security appliance; the system configuration inherited from multiple mode is not a complete functioning configuration for a single mode device. Because the system configuration does not have any network interfaces as part of its configuration, you must access the security appliance from the console to perform the copy.

To copy the old running configuration to the startup configuration and to change the mode to single mode, perform the following steps in the system execution space:

Step 1 To copy the backup version of your original running configuration to the current startup configuration, enter the following command in the system execution space:

```
hostname(config)# copy flash:old_running.cfg startup-config
```

Step 2 To set the mode to single mode, enter the following command in the system execution space:

```
hostname(config)# mode single
```

The security appliance reboots.