APPENDIX B

Sample Configurations

This appendix illustrates and describes a number of common ways to implement the security appliance, and includes the following topics:

Example 1: Multiple Mode Firewall With Outside Access

This configuration creates three security contexts plus the admin context, each with an inside and an outside interface. The Customer C context includes a DMZ interface where a Websense server for HTTP filtering resides on the service provider premises (see Figure B-1).

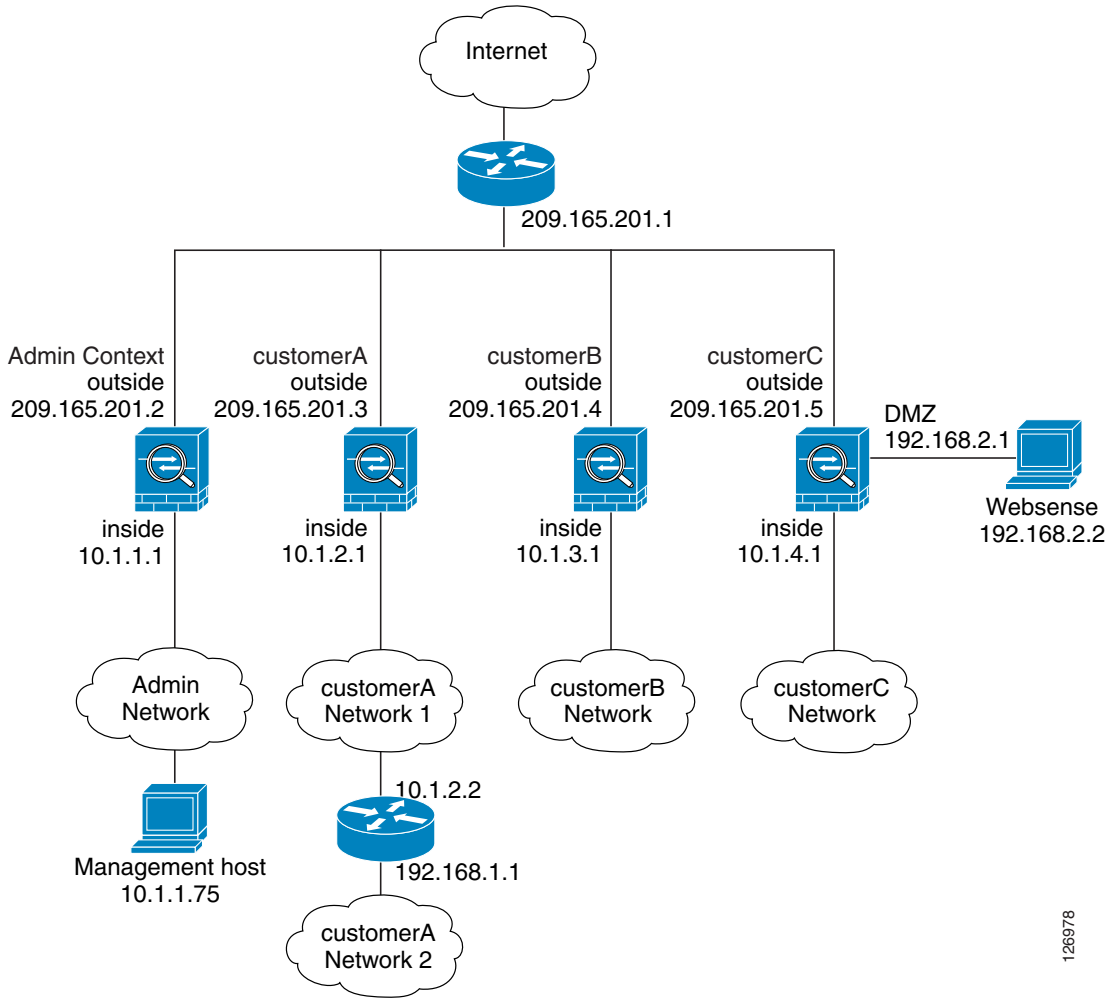
Inside hosts can access the Internet through the outside using dynamic NAT or PAT, but no outside hosts can access the inside.

The Customer A context has a second network behind an inside router.

The admin context allows SSH sessions to the security appliance from one host.

Although inside IP addresses can be the same across contexts when the interfaces are unique, keeping them unique is easier to manage.

Figure B-1 Example 1



See the following sections for the configurations for this scenario:

- Example 1: System Configuration, page B-2
- Example 1: Admin Context Configuration, page B-4
- Example 1: Customer A Context Configuration, page B-4
- Example 1: Customer B Context Configuration, page B-4
- Example 1: Customer C Context Configuration, page B-5

Example 1: System Configuration

You must first enable multiple context mode using the **mode multiple** command. The mode is not stored in the configuration file, even though it endures reboots. Enter the **show mode** command to view the current mode.

```
hostname Farscape
password passw0rd
enable password chr1cht0n
mac-address auto
asdm image disk0:/asdm.bin
boot system disk0:/image.bin
admin-context admin
interface gigabitethernet 0/0
   shutdown
interface gigabitethernet 0/0.3
   vlan 3
   no shutdown
interface gigabitethernet 0/1
   no shutdown
interface gigabitethernet 0/1.4
   vlan 4
   no shutdown
interface gigabitethernet 0/1.5
   vlan 5
   no shutdown
interface gigabitethernet 0/1.6
   vlan 6
   no shutdown
interface gigabitethernet 0/1.7
   vlan 7
   no shutdown
interface gigabitethernet 0/1.8
   vlan 8
   no shutdown
class gold
   limit-resource rate conns 2000
   limit-resource conns 20000
class silver
   limit-resource rate conns 1000
   limit-resource conns 10000
class bronze
   limit-resource rate conns 500
   limit-resource conns 5000
context admin
   allocate-interface gigabitethernet 0/0.3
   allocate-interface gigabitethernet 0/1.4
   config-url disk0://admin.cfg
   member default
context customerA
   description This is the context for customer A
   allocate-interface gigabitethernet 0/0.3
   allocate-interface gigabitethernet 0/1.5
   config-url disk0://contexta.cfg
   member gold
context customerB
   description This is the context for customer B
   allocate-interface gigabitethernet 0/0.3
   allocate-interface gigabitethernet 0/1.6
   config-url disk0://contextb.cfg
   member silver
context customerC
   description This is the context for customer C
   allocate-interface gigabitethernet 0/0.3
   allocate-interface gigabitethernet 0/1.7-gigabitethernet 0/1.8
   config-url disk0://contextc.cfg
   member bronze
```

Example 1: Admin Context Configuration

The host at 10.1.1.75 can access the context using SSH, which requires a key to be generated using the **crypto key generate** command.

```
hostname Admin
domain isp
interface gigabitethernet 0/0.3
   nameif outside
   security-level 0
   ip address 209.165.201.2 255.255.255.224
   no shutdown
interface gigabitethernet 0/1.4
   nameif inside
   security-level 100
   ip address 10.1.1.1 255.255.255.0
   no shutdown
passwd secret1969
enable password h1andl0
route outside 0 0 209.165.201.1 1
ssh 10.1.1.75 255.255.255.255 inside
nat (inside) 1 10.1.1.0 255.255.255.0
! This context uses dynamic NAT for inside users that access the outside
global (outside) 1 209.165.201.10-209.165.201.29
! The host at 10.1.1.75 has access to the Websense server in Customer C, so
! it needs a static translation for use in Customer C's access list
static (inside,outside) 209.165.201.30 10.1.1.75 netmask 255.255.255.255
```

Example 1: Customer A Context Configuration

```
interface gigabitethernet 0/0.3
   nameif outside
   security-level 0
   ip address 209.165.201.3 255.255.255.224
   no shutdown
interface gigabitethernet 0/1.5
   nameif inside
   security-level 100
   ip address 10.1.2.1 255.255.255.0
   no shutdown
passwd hell0!
enable password enter55
route outside 0 0 209.165.201.1 1
! The Customer A context has a second network behind an inside router that requires a
! static route. All other traffic is handled by the default route pointing to the router.
route inside 192.168.1.0 255.255.255.0 10.1.2.2 1
nat (inside) 1 10.1.2.0 255.255.255.0
! This context uses dynamic PAT for inside users that access that outside. The outside
! interface address is used for the PAT address
global (outside) 1 interface
```

Example 1: Customer B Context Configuration

```
interface gigabitethernet 0/0.3
   nameif outside
   security-level 0
   ip address 209.165.201.4 255.255.255.224
```

```
   no shutdown
interface gigabitethernet 0/1.6
   nameif inside
   security-level 100
   ip address 10.1.3.1 255.255.255.0
   no shutdown
passwd tenac10us
enable password defen$e
route outside 0 0 209.165.201.1 1
nat (inside) 1 10.1.3.0 255.255.255.0
! This context uses dynamic PAT for inside users that access the outside
global (outside) 1 209.165.201.9 netmask 255.255.255.255
access-list INTERNET remark Inside users only access HTTP and HTTPS servers on the outside
access-list INTERNET extended permit tcp any any eq http
access-list INTERNET extended permit tcp any any eq https
access-group INTERNET in interface inside
```

Example 1: Customer C Context Configuration

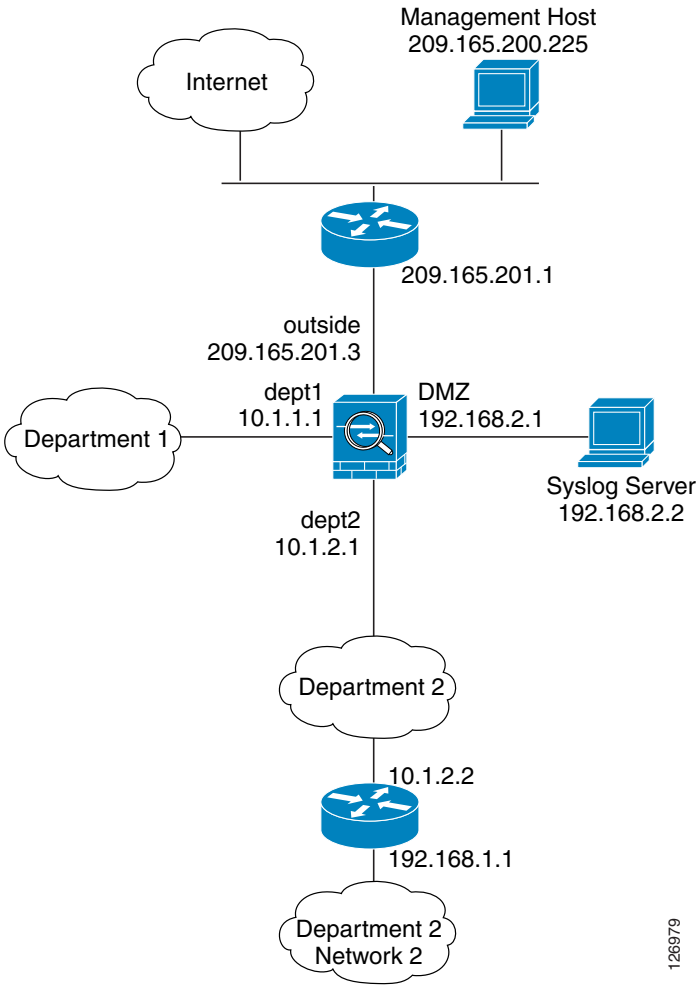
```
interface gigabitethernet 0/0.3
   nameif outside
   security-level 0
   ip address 209.165.201.5 255.255.255.224
   no shutdown
interface gigabitethernet 0/1.7
   nameif inside
   security-level 100
   ip address 10.1.4.1 255.255.255.0
   no shutdown
interface gigabitethernet 0/1.8
   nameif dmz
   security-level 50
   ip address 192.168.2.1 255.255.255.0
   no shutdown
passwd fl0wer
enable password treeh0u$e
route outside 0 0 209.165.201.1 1
url-server (dmz) vendor websense host 192.168.2.2 url-block block 50
url-cache dst 128
filter url http 10.1.4.0 255.255.255.0 0 0
! When inside users access an HTTP server, the security appliance consults with a
! Websense server to determine if the traffic is allowed
nat (inside) 1 10.1.4.0 255.255.255.0
! This context uses dynamic NAT for inside users that access the outside
global (outside) 1 209.165.201.9 netmask 255.255.255.255
! A host on the admin context requires access to the Websense server for management using
! pcAnywhere, so the Websense server uses a static translation for its private address
static (dmz,outside) 209.165.201.6 192.168.2.2 netmask 255.255.255.255
access-list MANAGE remark Allows the management host to use pcAnywhere on the Websense
server
access-list MANAGE extended permit tcp host 209.165.201.30 host 209.165.201.6 eq
pcanywhere-data
access-list MANAGE extended permit udp host 209.165.201.30 host 209.165.201.6 eq
pcanywhere-status
access-group MANAGE in interface outside
```

Example 2: Single Mode Firewall Using Same Security Level

This configuration creates three internal interfaces. Two of the interfaces connect to departments that are on the same security level, which allows all hosts to communicate without using access lists. The DMZ interface hosts a Syslog server. The management host on the outside needs access to the Syslog server and the security appliance. To connect to the security appliance, the host uses a VPN connection. The security appliance uses RIP on the inside interfaces to learn routes. The security appliance does not advertise routes with RIP; the upstream router needs to use static routes for security appliance traffic (see Figure B-2).

The Department networks are allowed to access the Internet, and use PAT.

Figure B-2 Example 2




```
passwd g00fba11
enable password gen1u$
hostname Buster
asdm image disk0:/asdm.bin
boot system disk0:/image.bin
interface gigabitethernet 0/0
   nameif outside
   security-level 0
```

```
   ip address 209.165.201.3 255.255.255.224
   no shutdown
interface gigabitethernet 0/1
   nameif dept2
   security-level 100
   ip address 10.1.2.1 255.255.255.0
   mac-address 000C.F142.4CDE standby 000C.F142.4CDF
   no shutdown
   rip authentication mode md5
   rip authentication key scorpius key_id 1
interface gigabitethernet 0/2
   nameif dept1
   security-level 100
   ip address 10.1.1.1 255.255.255.0
   no shutdown
interface gigabitethernet 0/3
   nameif dmz
   security-level 50
   ip address 192.168.2.1 255.255.255.0
   no shutdown
same-security-traffic permit inter-interface
route outside 0 0 209.165.201.1 1
nat (dept1) 1 10.1.1.0 255.255.255.0
nat (dept2) 1 10.1.2.0 255.255.255.0
! The dept1 and dept2 networks use PAT when accessing the outside
global (outside) 1 209.165.201.9 netmask 255.255.255.255
! Because we perform dynamic NAT on these addresses for outside access, we need to perform
! NAT on them for all other interface access. This identity static statement just
! translates the local address to the same address.
static (dept1,dept2) 10.1.1.0 10.1.1.0 netmask 255.255.255.0
static (dept2,dept1) 10.1.2.0 10.1.2.0 netmask 255.255.255.0
! The syslog server uses a static translation so the outside management host can access
! the server
static (dmz,outside) 209.165.201.5 192.168.2.2 netmask 255.255.255.255
access-list MANAGE remark Allows the management host to access the syslog server
access-list MANAGE extended permit tcp host 209.165.200.225 host 209.165.201.5 eq telnet
access-group MANAGE in interface outside
! Advertises the security appliance IP address as the default gateway for the downstream
! router. The security appliance does not advertise a default route to the upstream
! router. Listens for RIP updates from the downstream router. The security appliance does
! not listen for RIP updates from the upstream router because a default route to the
! upstream router is all that is required.
router rip
   network 10.0.0.0
   default information originate
   version 2
! The client uses a pre-shared key to connect to the security appliance over IPSec. The
! key is the password in the username command following.
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 group 2
isakmp policy 1 hash sha
isakmp enable outside
crypto ipsec transform-set vpn_client esp-3des esp-sha-hmac
username admin password passw0rd
crypto ipsec transform-set vpn esp-3des esp-sha-hmac
crypto dynamic-map vpn_client 1 set transform-set vpn
crypto map telnet_tunnel 1 ipsec-isakmp dynamic vpn_client
crypto map telnet_tunnel interface outside
ip local pool client_pool 10.1.1.2
access-list VPN_SPLIT extended permit ip host 209.165.201.3 host 10.1.1.2
telnet 10.1.1.2 255.255.255.255 outside
telnet timeout 30
logging trap 5
```

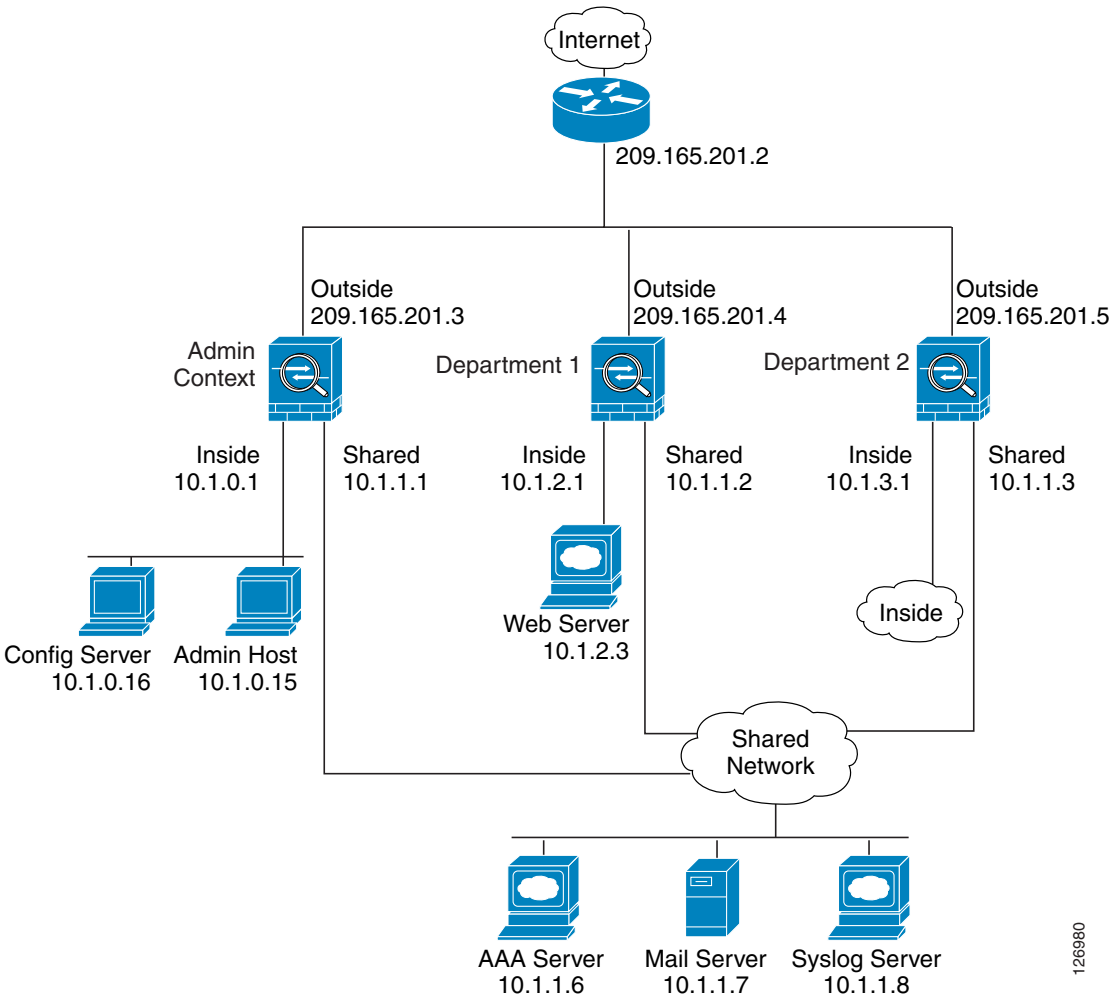
```
! System messages are sent to the syslog server on the DMZ network
logging host dmz 192.168.2.2
logging enable
```

Example 3: Shared Resources for Multiple Contexts

This configuration includes multiple contexts for multiple departments within a company. Each department has its own security context so that each department can have its own security policy. However, the syslog, mail, and AAA servers are shared across all departments. These servers are placed on a shared interface (see Figure B-3).

Department 1 has a web server that outside users who are authenticated by the AAA server can access.

Figure B-3 Example 3



See the following sections for the configurations for this scenario:

- Example 3: System Configuration, page B-9
- Example 3: Admin Context Configuration, page B-9

Example 3: System Configuration

You must first enable multiple context mode using the **mode multiple** command. The mode is not stored in the configuration file, even though it endures reboots. Enter the **show mode** command to view the current mode.

```
hostname Ubik
password pkd55
enable password deckard69
asdm image disk0:/asdm.bin
boot system disk0:/image.bin
mac-address auto
admin-context admin
interface gigabitethernet 0/0
   no shutdown
interface gigabitethernet 0/0.200
   vlan 200
   no shutdown
interface gigabitethernet 0/1
   shutdown
interface gigabitethernet 0/1.201
   vlan 201
   no shutdown
interface gigabitethernet 0/1.202
   vlan 202
   no shutdown
interface gigabitethernet 0/1.300
   vlan 300
   no shutdown
context admin
   allocate-interface gigabitethernet 0/0.200
   allocate-interface gigabitethernet 0/1.201
   allocate-interface gigabitethernet 0/1.300
   config-url disk0://admin.cfg
context department1
   allocate-interface gigabitethernet 0/0.200
   allocate-interface gigabitethernet 0/1.202
   allocate-interface gigabitethernet 0/1.300
   config-url ftp://admin:passw0rd@10.1.0.16/dept1.cfg
context department2
   allocate-interface gigabitethernet 0/0.200
   allocate-interface gigabitethernet 0/1.203
   allocate-interface gigabitethernet 0/1.300
   config-url ftp://admin:passw0rd@10.1.0.16/dept2.cfg
```

Example 3: Admin Context Configuration

```
hostname Admin
interface gigabitethernet 0/0.200
   nameif outside
   security-level 0
   ip address 209.165.201.3 255.255.255.224
   no shutdown
interface gigabitethernet 0/0.201
   nameif inside
```

```
   security-level 100
   ip address 10.1.0.1 255.255.255.0
   no shutdown
interface gigabitethernet 0/0.300
   nameif shared
   security-level 50
   ip address 10.1.1.1 255.255.255.0
   no shutdown
passwd v00d00
enable password d011
route outside 0 0 209.165.201.2 1
nat (inside) 1 10.1.0.0 255.255.255.0
! This context uses PAT for inside users that access the outside
global (outside) 1 209.165.201.6 netmask 255.255.255.255
! This context uses PAT for inside users that access the shared network
global (shared) 1 10.1.1.30
! Because this host can access the web server in the Department 1 context, it requires a
! static translation
static (inside,outside) 209.165.201.7 10.1.0.15 netmask 255.255.255.255
! Because this host has management access to the servers on the Shared interface, it
! requires a static translation to be used in an access list
static (inside,shared) 10.1.1.78 10.1.0.15 netmask 255.255.255.255
access-list SHARED remark -Allows only mail traffic from inside to exit shared interface
access-list SHARED remark -but allows the admin host to access any server.
access-list SHARED extended permit ip host 10.1.1.78 any
access-list SHARED extended permit tcp host 10.1.1.30 host 10.1.1.7 eq smtp
! Note that the translated addresses are used.
access-group SHARED out interface shared
! Allows 10.1.0.15 to access the admin context using Telnet. From the admin context, you
! can access all other contexts.
telnet 10.1.0.15 255.255.255.255 inside
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (shared) host 10.1.1.6
   key TheUauthKey
   server-port 16
! The host at 10.1.0.15 must authenticate with the AAA server to log in
aaa authentication telnet console AAA-SERVER
aaa authorization command AAA-SERVER LOCAL
aaa accounting command AAA-SERVER
logging trap 6
! System messages are sent to the syslog server on the Shared network
logging host shared 10.1.1.8
logging enable
```

Example 3: Department 1 Context Configuration

```
interface gigabitethernet 0/0.200
   nameif outside
   security-level 0
   ip address 209.165.201.4 255.255.255.224
   no shutdown
interface gigabitethernet 0/0.202
   nameif inside
   security-level 100
   ip address 10.1.2.1 255.255.255.0
   no shutdown
interface gigabitethernet 0/0.300
   nameif shared
   security-level 50
   ip address 10.1.1.2 255.255.255.0
   no shutdown
```

```
passwd cugel
enable password rhialto
nat (inside) 1 10.1.2.0 255.255.255.0
! The inside network uses PAT when accessing the outside
global (outside) 1 209.165.201.8 netmask 255.255.255.255
! The inside network uses dynamic NAT when accessing the shared network
global (shared) 1 10.1.1.31-10.1.1.37
! The web server can be accessed from outside and requires a static translation
static (inside,outside) 209.165.201.9 10.1.2.3 netmask 255.255.255.255
access-list WEBSERVER remark -Allows the management host (its translated address) on the
access-list WEBSERVER remark -admin context to access the web server for management
access-list WEBSERVER remark -it can use any IP protocol
access-list WEBSERVER extended permit ip host 209.165.201.7 host 209.165.201.9
access-list WEBSERVER remark -Allows any outside address to access the web server
access-list WEBSERVER extended permit tcp any eq http host 209.165.201.9 eq http
access-group WEBSERVER in interface outside
access-list MAIL remark -Allows only mail traffic from inside to exit out the shared int
! Note that the translated addresses are used.
access-list MAIL extended permit tcp host 10.1.1.31 eq smtp host 10.1.1.7 eq smtp
access-list MAIL extended permit tcp host 10.1.1.32 eq smtp host 10.1.1.7 eq smtp
access-list MAIL extended permit tcp host 10.1.1.33 eq smtp host 10.1.1.7 eq smtp
access-list MAIL extended permit tcp host 10.1.1.34 eq smtp host 10.1.1.7 eq smtp
access-list MAIL extended permit tcp host 10.1.1.35 eq smtp host 10.1.1.7 eq smtp
access-list MAIL extended permit tcp host 10.1.1.36 eq smtp host 10.1.1.7 eq smtp
access-list MAIL extended permit tcp host 10.1.1.37 eq smtp host 10.1.1.7 eq smtp
access-group MAIL out interface shared
aaa-server AAA-SERVER protocol tacacs+
aaa-server AAA-SERVER (shared) host 10.1.1.6
   key TheUauthKey
   server-port 16
! All traffic matching the WEBSERVER access list must authenticate with the AAA server
aaa authentication match WEBSERVER outside AAA-SERVER
logging trap 4
! System messages are sent to the syslog server on the Shared network
logging host shared 10.1.1.8
logging enable
```

Example 3: Department 2 Context Configuration

```
interface gigabitethernet 0/0.200
   nameif outside
   security-level 0
   ip address 209.165.201.5 255.255.255.224
   no shutdown
interface gigabitethernet 0/0.203
   nameif inside
   security-level 100
   ip address 10.1.3.1 255.255.255.0
   no shutdown
interface gigabitethernet 0/0.300
   nameif shared
   security-level 50
   ip address 10.1.1.3 255.255.255.0
   no shutdown
passwd maz1r1an
enable password ly0ne$$e
route outside 0 0 209.165.201.2 1
nat (inside) 1 10.1.3.0 255.255.255.0
! The inside network uses PAT when accessing the outside
global (outside) 1 209.165.201.10 netmask 255.255.255.255
! The inside network uses PAT when accessing the shared network
```

```
global (shared) 1 10.1.1.38
access-list MAIL remark -Allows only mail traffic from inside to exit out the shared int
access-list MAIL extended permit tcp host 10.1.1.38 host 10.1.1.7 eq smtp
! Note that the translated PAT address is used.
access-group MAIL out interface shared
logging trap 3
! System messages are sent to the syslog server on the Shared network
logging host shared 10.1.1.8
logging enable
```

Example 4: Multiple Mode, Transparent Firewall with Outside Access

This configuration creates three security contexts plus the admin context. Each context allows OSPF traffic to pass between the inside and outside routers (see Figure B-4).

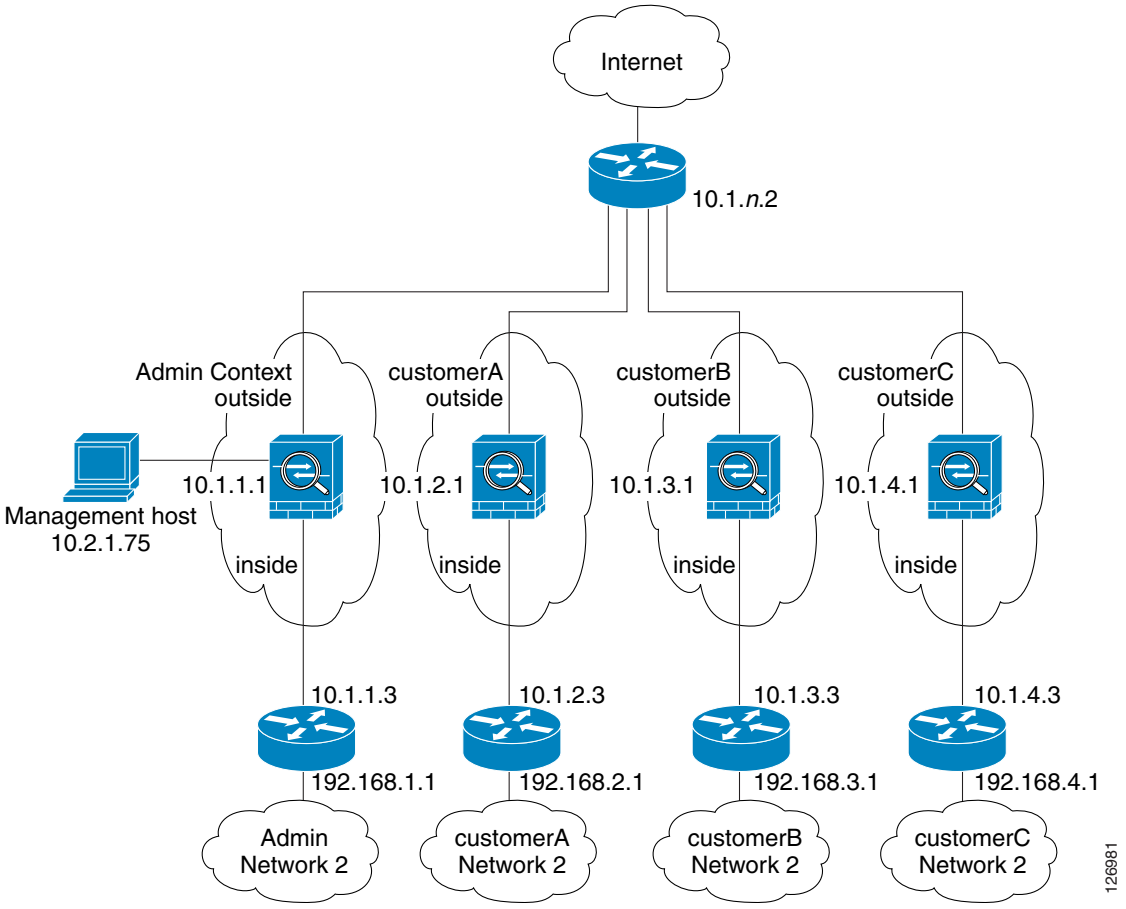
Inside hosts can access the Internet through the outside, but no outside hosts can access the inside.

An out-of-band management host is connected to the Management 0/0 interface.

The admin context allows SSH sessions to the security appliance from one host.

Although inside IP addresses can be the same across contexts, keeping them unique is easier to manage.

Figure B-4 Example 4



See the following sections for the configurations for this scenario:

- Example 4: System Configuration, page B-13
- Example 4: Admin Context Configuration, page B-14
- Example 4: Customer A Context Configuration, page B-15
- Example 4: Customer B Context Configuration, page B-15
- Example 4: Customer C Context Configuration, page B-16

Example 4: System Configuration

You must first enable multiple context mode using the **mode multiple** command. The mode is not stored in the configuration file, even though it endures reboots. Enter the **show mode** command to view the current mode.

```
firewall transparent
hostname Farscape
password passw0rd
enable password chr1cht0n
asdm image disk0:/asdm.bin
boot system disk0:/image.bin
admin-context admin
interface gigabitethernet 0/0
```

```
   no shutdown
interface gigabitethernet 0/0.150
   vlan 150
   no shutdown
interface gigabitethernet 0/0.151
   vlan 151
   no shutdown
interface gigabitethernet 0/0.152
   vlan 152
   no shutdown
interface gigabitethernet 0/0.153
   vlan 153
   no shutdown
interface gigabitethernet 0/1
   shutdown
interface gigabitethernet 0/1.4
   vlan 4
   no shutdown
interface gigabitethernet 0/1.5
   vlan 5
   no shutdown
interface gigabitethernet 0/1.6
   vlan 6
   no shutdown
interface gigabitethernet 0/1.7
   vlan 7
   no shutdown
interface management 0/0
   no shutdown
context admin
   allocate-interface gigabitethernet 0/0.150
   allocate-interface gigabitethernet 0/1.4
   allocate-interface management 0/0
   config-url disk0://admin.cfg
context customerA
   description This is the context for customer A
   allocate-interface gigabitethernet 0/0.151
   allocate-interface gigabitethernet 0/1.5
   config-url disk0://contexta.cfg
context customerB
   description This is the context for customer B
   allocate-interface gigabitethernet 0/0.152
   allocate-interface gigabitethernet 0/1.6
   config-url disk0://contextb.cfg
context customerC
   description This is the context for customer C
   allocate-interface gigabitethernet 0/0.153
   allocate-interface gigabitethernet 0/1.7
   config-url disk0://contextc.cfg
```

Example 4: Admin Context Configuration

The host at 10.1.1.75 can access the context using SSH, which requires a key pair to be generated using the **crypto key generate** command.

```
hostname Admin
domain isp
interface gigabitethernet 0/0.150
   nameif outside
   security-level 0
   no shutdown
```

```
interface gigabitethernet 0/1.4
   nameif inside
   security-level 100
   no shutdown
interface management 0/0
   nameif manage
   security-level 50
   ip address 10.2.1.1 255.255.255.0
   no shutdown
passwd secret1969
enable password h1and10
ip address 10.1.1.1 255.255.255.0
route outside 0 0 10.1.1.2 1
ssh 10.1.1.75 255.255.255.255 inside
access-list OSPF remark -Allows OSPF
access-list OSPF extended permit 89 any any
access-group OSPF in interface outside
```

Example 4: Customer A Context Configuration

```
interface gigabitethernet 0/0.151
   nameif outside
   security-level 0
   no shutdown
interface gigabitethernet 0/1.5
   nameif inside
   security-level 100
   no shutdown
passwd hell0!
enable password enter55
ip address 10.1.2.1 255.255.255.0
route outside 0 0 10.1.2.2 1
access-list OSPF remark -Allows OSPF
access-list OSPF extended permit 89 any any
access-group OSPF in interface outside
```

Example 4: Customer B Context Configuration

```
interface gigabitethernet 0/0.152
   nameif outside
   security-level 0
   no shutdown
interface gigabitethernet 0/1.6
   nameif inside
   security-level 100
   no shutdown
passwd tenac10us
enable password defen$e
ip address 10.1.3.1 255.255.255.0
route outside 0 0 10.1.3.2 1
access-list OSPF remark -Allows OSPF
access-list OSPF extended permit 89 any any
access-group OSPF in interface outside
```

Example 4: Customer C Context Configuration

```
interface gigabitethernet 0/0.153
   nameif outside
   security-level 0
   no shutdown
interface gigabitethernet 0/1.7
   nameif inside
   security-level 100
   no shutdown
passwd fl0wer
enable password treeh0u$e
ip address 10.1.4.1 255.255.255.0
route outside 0 0 10.1.4.2 1
access-list OSPF remark -Allows OSPF
access-list OSPF extended permit 89 any any
access-group OSPF in interface outside
```

Example 5: WebVPN Configuration

This configuration shows the commands needed to create WebVPN connections to the security appliance.

WebVPN lets users establish a secure, remote-access VPN tunnel to the security appliance using a web browser. There is no need for either a software or hardware client. WebVPN provides easy access to a broad range of web resources and web-enabled applications from almost any computer that can reach HTTP(S) Internet sites. WebVPN uses Secure Socket Layer Protocol and its successor, Transport Layer Security (SSL/TLS1) to provide a secure connection between remote users and specific, supported internal resources that you configure at a central site. The security appliance recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate users.

Step 1 Configure the security appliance for WebVPN.

```
webvpn
! WebVPN sessions are allowed on the outside and dmz1 interfaces, ASDM is not allowed.
 enable outside
 enable dmz161
 title-color green
 secondary-color 200,160,0
 text-color black
 default-idle-timeout 3600
! The NetBios Name server used for CIFS resolution.
 nbns-server 172.31.122.10 master timeout 2 retry 2
 accounting-server-group RadiusACS1
! WebVPN sessions are authenticated to a RADIUS aaa server.
 authentication-server-group RadiusACS2
```

Step 2 You must enable WebVPN access lists to be enforced on a group-policy or user policy. The access lists are defined with the **filter value** and **functions** commands in the group or user configuration.

```
access-list maia2 remark -deny access to url and send a syslog every 300 seconds
access-list maia2 remark -containing the hit-count (how many times the url was accessed)
access-list maia2 webtype deny url https://sales.example.com log informational interval
300
access-list maia2 remark -Permits access to the URL.
access-list maia2 webtype permit url http://employee-connection.example.com
```

```
access-list maia2 remark -Permits access to the site using ssh.
access-list maia2 remark -To be enforced via Port-Forwarding application.
access-list maia2 webtype permit tcp asa-35.example.com 255.255.255.255 eq ssh
access-list maia2 remark -Denies access to the application on port 1533.
access-list maia2 webtype deny tcp im.example.com 255.255.255.255 eq 1533
access-list maia2 remark -Permits access to files on this file share via
access-list maia2 remark -WebVPN Common Internet File System (CIFS).
access-list maia2 webtype permit url cifs://server-bos/people/mkting log informational
3600
```

Step 3 You can configure a list of pre-configured URLs presented on the WebVPN user's home page after login, which are defined per user or per group.

```
url-list HomeURL "Sales" https://sales.example.com
url-list HomeURL "VPN3000-1" http://vpn3k-1.example.com
url-list HomeURL "OWA-2000" http://10.160.105.2/exchange
url-list HomeURL "Exchange5.5" http://10.86.195.113/exchange
url-list HomeURL " Employee Benefits" http://benefits.example.com
url-list HomeURL "Calendar" http://http://eng.example.com/cal.html
```

Step 4 Configure a list of non-web TCP applications that will be port-forwarded over WebVPN and enforced per user or per group-policy. These are defined globally but can be enforced per user or per group-policy.

```
port-forward Apps1 4001 10.148.1.81 telnet term-servr
port-forward Apps1 4008 router1-example.com ssh
port-forward Apps1 10143 flask.example.com imap4
port-forward Apps1 10110 flask.example.com pop3
port-forward Apps1 10025 flask.example.com smtp
port-forward Apps1 11533 sametime-im.example.com 1533
port-forward Apps1 10022 secure-term.example.com ssh
port-forward Apps1 21666 tuscan.example.com 1666 perforce-f1
port-forward Apps1 1030 sales.example.com https
```

Step 5 Configure the policy attributes enforced for users of the SSLVPNusers group-policy.

```
group-policy SSLVPNusers internal
group-policy SSLVPNusers attributes
   banner value Welcome to Web Services !!!
   vpn-idle-timeout 2
   vpn-tunnel-protocol IPSec webvpn
   webvpn
      functions url-entry file-access file-entry file-browsing port-forward filter
      url-list value HomeURL
      port-forward value Apps1
```

Step 6 Next, configure the interface(s) where ASDM and WebVPN HTTPS sessions will terminate. Note that The security appliance can support both WebVPN and an ASDM administrative session simultaneously on the same interface. To do so, you must assign different port numbers to these functions.

```
! Enables the HTTP server to allow ASDM and WebVPN HTTPS sessions.
http server enable
! Allows ASDM session(s) from host 10.20.30.47 on the inside interface ; WebVPN sessions
! are not allowed on this interface.
http 10.10.10.45 255.255.255.255 inside
! Allows WebVPN sessions on outside interfce using HTTP to be re-directed to HTTPS.
! ASDM session is not allowed on this interface.
http redirect outside 80
! Allows WebVPN sessions on dmz1 interfce using HTTP to be re-directed to HTTPS.
http redirect dmz161 80
```

Step 7 Next, allow HTTPS ASDM and WebVPN sessions to terminate on the security appliance using the 3DES-sha1 cipher. Requires that a proper 3DES activation-key be previously installed.

```
ssl encryption 3des-sha1
```

```
ssl trust-point CA-MS inside
```

Step 8 Finally, configure the email proxy settings.

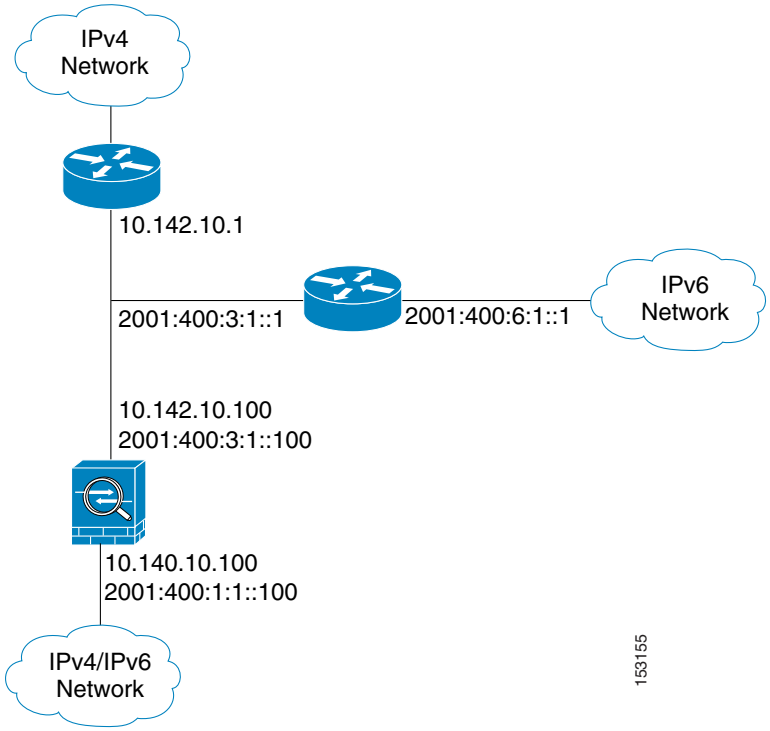
```
imap4s
   enable outside
   enable inside
   enable dmz161
   default-group-policy DfltGrpPolicy
pop3s
   enable outside
   enable inside
   enable dmz161
   default-group-policy DfltGrpPolicy
smtps
   enable outside
   enable inside
   enable dmz161
   default-group-policy DfltGrpPolicy
```

Example 6: IPv6 Configuration

This sample configuration shows several features of IPv6 support on the security appliance:

- Each interface is configured with both IPv6 and IPv4 addresses.
- The IPv6 default route is set with the **ipv6 route** command.
- An IPv6 access list is applied to the outside interface.
- The enforcement of Modified-EUI64 format interface identifiers in the IPv6 addresses of hosts on the inside interface.
- The outside interface suppresses router advertisement messages.
- An IPv6 static route.

Figure B-5 IPv6 Dual Stack Configuration



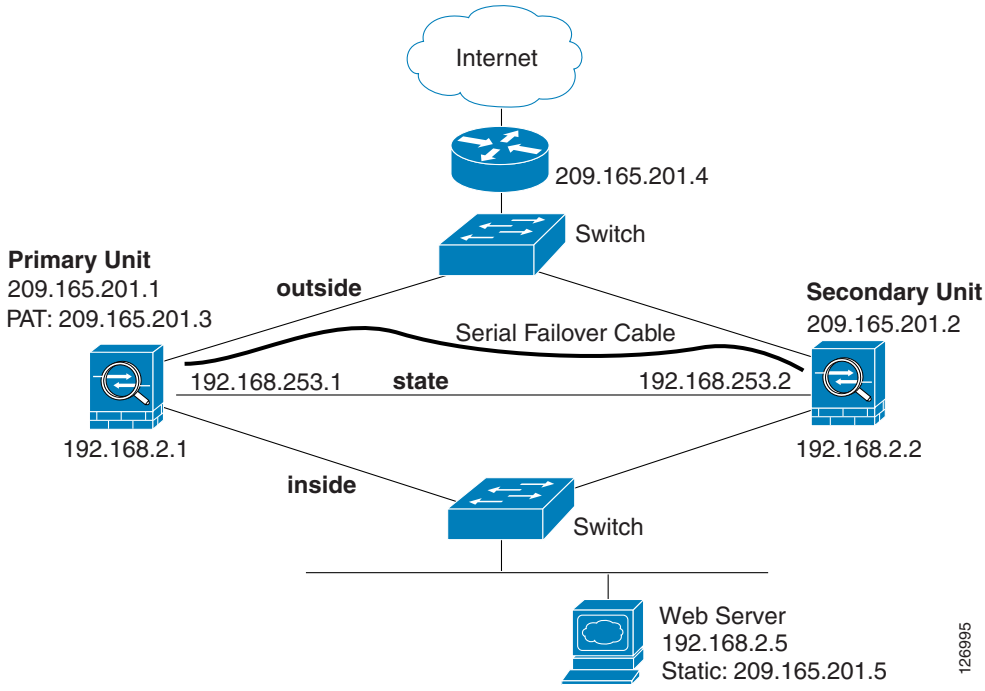

```
enable password myenablepassword
passwd mypassword
hostname coyupix
asdm image flash:/asdm.bin
boot system flash:/image.bin
interface Ethernet0
   nameif outside
   security-level 0
   ip address 10.142.10.100 255.255.255.0
   ipv6 address 2001:400:3:1::100/64
   ipv6 nd suppress-ra
   ospf mtu-ignore auto
   no shutdown
interface Ethernet1
   nameif inside
   security-level 100
   ip address 10.140.10.100 255.255.255.0
   ipv6 address 2001:400:1:1::100/64
   ospf mtu-ignore auto
   no shutdown
access-list allow extended permit icmp any any
ssh 10.140.10.75 255.255.255.255 inside
logging enable
logging buffered debugging
ipv6 enforce-eui64 inside
ipv6 route outside 2001:400:6:1::/64 2001:400:3:1::1
ipv6 route outside ::/0 2001:400:3:1::1
ipv6 access-list outacl permit icmp6 2001:400:2:1::/64 2001:400:1:1::/64
ipv6 access-list outacl permit tcp 2001:400:2:1::/64 2001:400:1:1::/64 eq telnet
ipv6 access-list outacl permit tcp 2001:400:2:1::/64 2001:400:1:1::/64 eq ftp
ipv6 access-list outacl permit tcp 2001:400:2:1::/64 2001:400:1:1::/64 eq www
access-group allow in interface outside
```

```
access-group outacl in interface outside
route outside 0.0.0.0 0.0.0.0 16.142.10.1 1
```

Example 7: Cable-Based Active/Standby Failover (Routed Mode)

Figure B-6 shows the network diagram for a failover configuration using a serial Failover cable. This configuration is only available on the PIX security appliance.

Figure B-6 Cable-Based Failover Configuration



The following are the typical commands in a cable-based failover configuration.

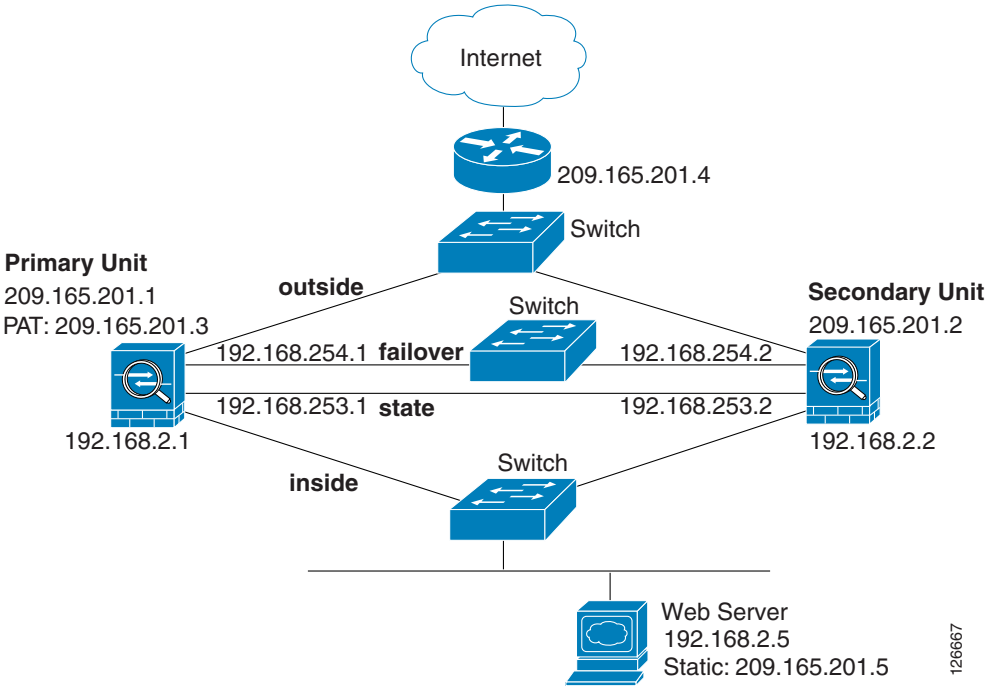
```
enable password myenablepassword
passwd mypassword
hostname pixfirewall
asdm image flash:/asdm.bin
boot system flash:/image.bin
interface Ethernet0
   nameif outside
   security-level 0
   speed 100
   duplex full
   ip address 209.165.201.1 255.255.255.224 standby 209.165.201.2
   no shutdown
interface Ethernet1
   nameif inside
   security-level 100
   speed 100
   duplex full
   ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2
   no shutdown
```

```
interface Ethernet3
   description STATE Failover Interface
telnet 192.168.2.45 255.255.255.255 inside
access-list acl_in permit tcp any host 209.165.201.5 eq 80
access-group acl_in in interface outside
failover
failover link state Ethernet3
failover interface ip state 192.168.253.1 255.255.255.252 standby 192.168.253.2
global (outside) 1 209.165.201.3 netmask 255.255.255.224
nat (inside) 1 0.0.0.0 0.0.0.0
static (inside,outside) 209.165.201.5 192.168.2.5 netmask 255.255.255.255 0 0
route outside 0.0.0.0 0.0.0.0 209.165.201.4 1
```

Example 8: LAN-Based Active/Standby Failover (Routed Mode)

Figure B-7 shows the network diagram for a failover configuration using an Ethernet failover link. The units are configured to detect unit failures and to fail over in under a second (see the **failover polltime unit** command in the primary unit configuration).

Figure B-7 LAN-Based Failover Configuration



See the following sections for the configurations for this scenario:

- Example 8: Primary Unit Configuration, page B-21
- Example 8: Secondary Unit Configuration, page B-22

Example 8: Primary Unit Configuration

```
hostname pixfirewall
enable password myenablepassword
```

```
password mypassword
interface Ethernet0
   nameif outside
   ip address 209.165.201.1 255.255.255.224 standby 209.165.201.2
   no shutdown
interface Ethernet1
   nameif inside
   ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2
   no shutdown
interface Ethernet2
   description LAN Failover Interface
   no shutdown
interface ethernet3
   description STATE Failover Interface
telnet 192.168.2.45 255.255.255.255 inside
access-list acl_out permit tcp any host 209.165.201.5 eq 80
failover
failover lan unit primary
failover lan interface failover Ethernet2
failover lan enable
! The failover lan enable command is required on the PIX security appliance only.
failover polltime unit msec 200 holdtime msec 800
failover key key1
failover link state Ethernet3
failover interface ip failover 192.168.254.1 255.255.255.0 standby 192.168.254.2
failover interface ip state 192.168.253.1 255.255.255.0 standby 192.168.253.2
global (outside) 1 209.165.201.3 netmask 255.255.255.224
nat (inside) 1 0.0.0.0 0.0.0.0
static (inside,outside) 209.165.201.5 192.168.2.5 netmask 255.255.255.255 0 0
access-group acl_out in interface outside
route outside 0.0.0.0 0.0.0.0 209.165.201.4 1
```

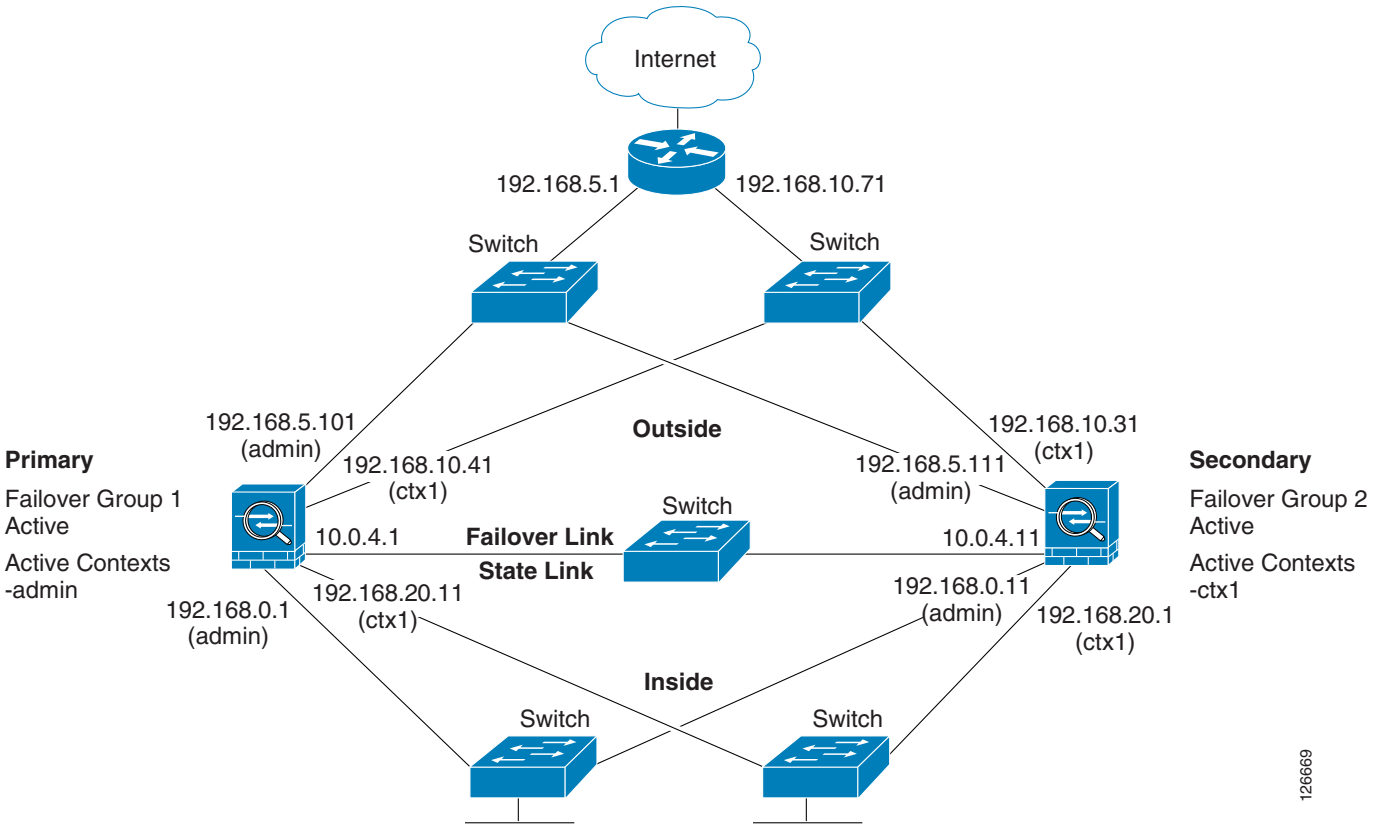
Example 8: Secondary Unit Configuration

```
failover
failover lan unit secondary
failover lan interface failover ethernet2
failover lan enable
failover key key1
failover interface ip failover 192.168.254.1 255.255.255.0 standby 192.168.254.2
```

Example 9: LAN-Based Active/Active Failover (Routed Mode)

The following example shows how to configure Active/Active failover. In this example there are 2 user contexts, named admin and ctx1. Figure B-8 shows the network diagram for the example.

Figure B-8 Active/Active Failover Configuration



See the following sections for the configurations for this scenario:

- Example 9: Primary Unit Configuration
- Example 9: Secondary Unit Configuration

Example 9: Primary Unit Configuration

See the following sections for the primary unit configuration:

- Example 9: Primary System Configuration, page B-23
- Example 9: Primary admin Context Configuration, page B-24
- Example 9: Primary ctx1 Context Configuration, page B-25

Example 9: Primary System Configuration

You must first enable multiple context mode using the **mode multiple** command. The mode is not stored in the configuration file, even though it endures reboots. Enter the **show mode** command to view the current mode.

```
hostname ciscopix
enable password farscape
password crichton
asdm image flash:/asdm.bin
```

```
boot system flash:/cdisk.bin
mac-address auto
interface Ethernet0
   description LAN/STATE Failover Interface
interface Ethernet1
   no shutdown
interface Ethernet2
   no shutdown
interface Ethernet3
   no shutdown
interface Ethernet4
   no shutdown
interface Ethernet5
   no shutdown
interface Ethernet6
   no shutdown
interface Ethernet7
   no shutdown
interface Ethernet8
   no shutdown
interface Ethernet9
   no shutdown
failover
failover lan unit primary
failover lan interface folink Ethernet0
failover link folink Ethernet0
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
failover group 1
   primary
   preempt
failover group 2
   secondary
   preempt
admin-context admin
context admin
   description admin
   allocate-interface Ethernet1
   allocate-interface Ethernet2
   config-url flash:/admin.cfg
   join-failover-group 1
context ctx1
   description context 1
   allocate-interface Ethernet3
   allocate-interface Ethernet4
   config-url flash:/ctx1.cfg
   join-failover-group 2
```

Example 9: Primary admin Context Configuration

```
enable password frek
password elixir
hostname admin
interface Ethernet1
   nameif outside
   security-level 0
   ip address 192.168.5.101 255.255.255.0 standby 192.168.5.111
interface Ethernet2
   nameif inside
   security-level 100
   ip address 192.168.0.1 255.255.255.0 standby 192.168.0.11
monitor-interface outside
monitor-interface inside
```

```
route outside 0.0.0.0 0.0.0.0 192.168.5.1 1
ssh 192.168.0.2 255.255.255.255 inside
```

Example 9: Primary ctx1 Context Configuration

```
enable password quadrophenia
password tommy
hostname ctx1
interface Ethernet3
   nameif inside
   security-level 100
   ip address 192.168.20.1 255.255.255.0 standby 192.168.20.11
interface Ethernet4
   nameif outside
   security-level 0
   ip address 192.168.10.31 255.255.255.0 standby 192.168.10.41
   asr-group 1
access-list 201 extended permit ip any any
access-group 201 in interface outside
logging enable
logging console informational
monitor-interface inside
monitor-interface outside
route outside 0.0.0.0 0.0.0.0 192.168.10.71 1
```

Example 9: Secondary Unit Configuration

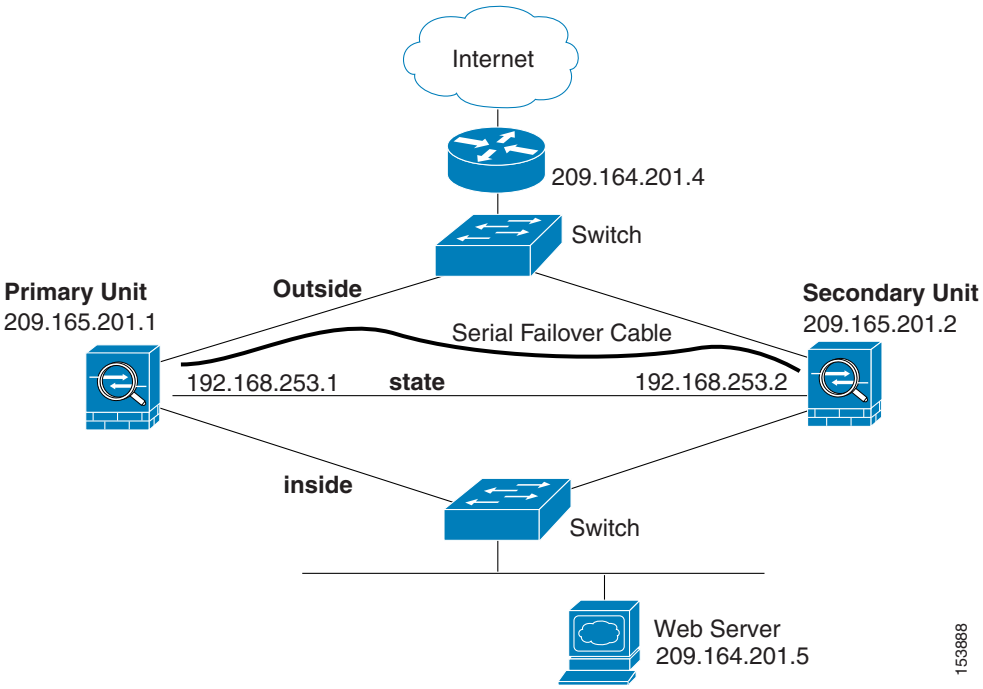
You only need to configure the secondary security appliance to recognize the failover link. The secondary security appliance obtains the context configurations from the primary security appliance upon booting or when failover is first enabled. The **preempt** commands in the failover group configurations cause the failover groups to become active on their designated unit after the configurations have been synchronized and the preempt delay has passed.

```
failover
failover lan unit secondary
failover lan interface folink Ethernet0
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
```

Example 10: Cable-Based Active/Standby Failover (Transparent Mode)

Figure B-6 shows the network diagram for a transparent mode failover configuration using a serial Failover cable. This configuration is only available on the PIX 500 series security appliance.

Figure B-9 Transparent Mode Cable-Based Failover Configuration



The following are the typical commands in a cable-based, transparent firewall failover configuration.

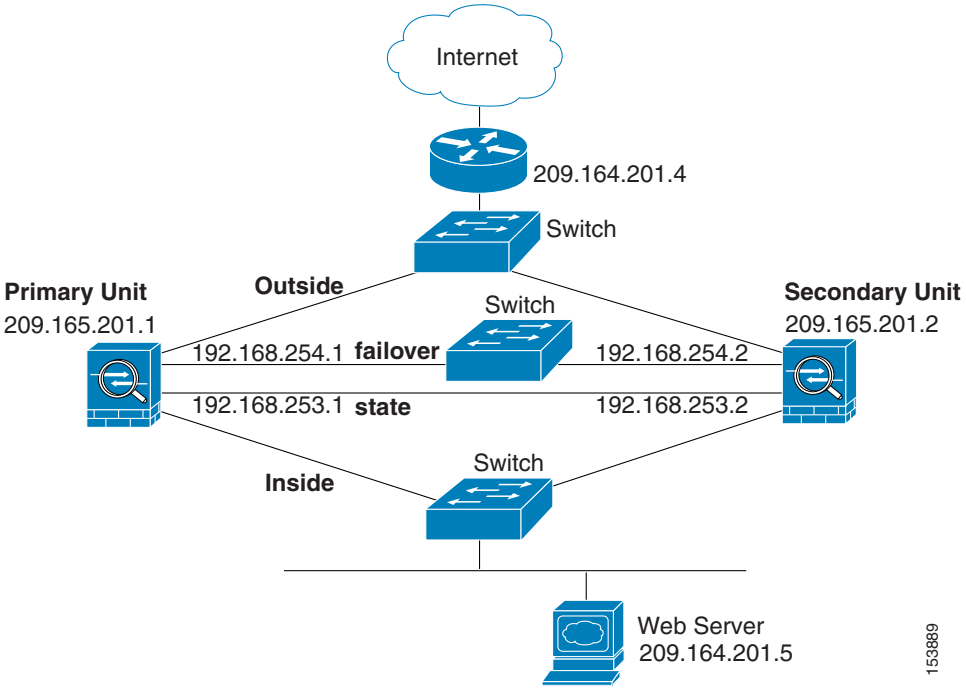
```
enable password myenablepassword
passwd mypassword
hostname pixfirewall
asdm image flash:/asdm.bin
boot system flash:/image.bin
firewall transparent
interface Ethernet0
   speed 100
   duplex full
   nameif outside
   security-level 0
   no shutdown
interface Ethernet1
   speed 100
   duplex full
   nameif inside
   security-level 100
   no shutdown
interface Ethernet3
   description STATE Failover Interface
telnet 192.168.2.45 255.255.255.255 mgmt
access-list acl_in permit tcp any host 209.165.201.5 eq 80
access-group acl_in in interface outside
```

```
ip address 209.165.201.1 255.255.255.0 standby 209.165.201.2
failover
failover link state Ethernet3
failover interface ip state 192.168.253.1 255.255.255.0 standby 192.168.253.2
route outside 0.0.0.0 0.0.0.0 209.165.201.4 1
```

Example 11: LAN-Based Active/Standby Failover (Transparent Mode)

Figure B-7 shows the network diagram for a transparent mode failover configuration using an Ethernet failover link. The units are configured to detect unit failures and to fail over in under a second (see the **failover polltime unit** command in the primary unit configuration).

Figure B-10 Transparent Mode LAN-Based Failover Configuration



See the following sections for the configurations for this scenario:

- Example 8: Primary Unit Configuration, page B-21
- Example 8: Secondary Unit Configuration, page B-22

Example 11: Primary Unit Configuration

```
firewall transparent
hostname pixfirewall
enable password myenablepassword
password mypassword
interface Ethernet0
   nameif outside
```

```
   no shutdown
interface Ethernet1
   nameif inside
   no shutdown
interface Ethernet2
   description LAN Failover Interface
   no shutdown
interface ethernet3
   description STATE Failover Interface
telnet 192.168.2.45 255.255.255.255 inside
access-list acl_out permit tcp any host 209.165.201.5 eq 80
ip address 209.165.201.1 255.255.255.0 standby 209.165.201.2
failover
failover lan unit primary
failover lan interface failover Ethernet2
failover lan enable
! The failover lan enable command is required on the PIX security appliance only.
failover polltime unit msec 200 holdtime msec 800
failover key key1
failover link state Ethernet3
failover interface ip failover 192.168.254.1 255.255.255.0 standby 192.168.254.2
failover interface ip state 192.168.253.1 255.255.255.0 standby 192.168.253.2
access-group acl_out in interface outside
route outside 0.0.0.0 0.0.0.0 209.165.201.4 1
```

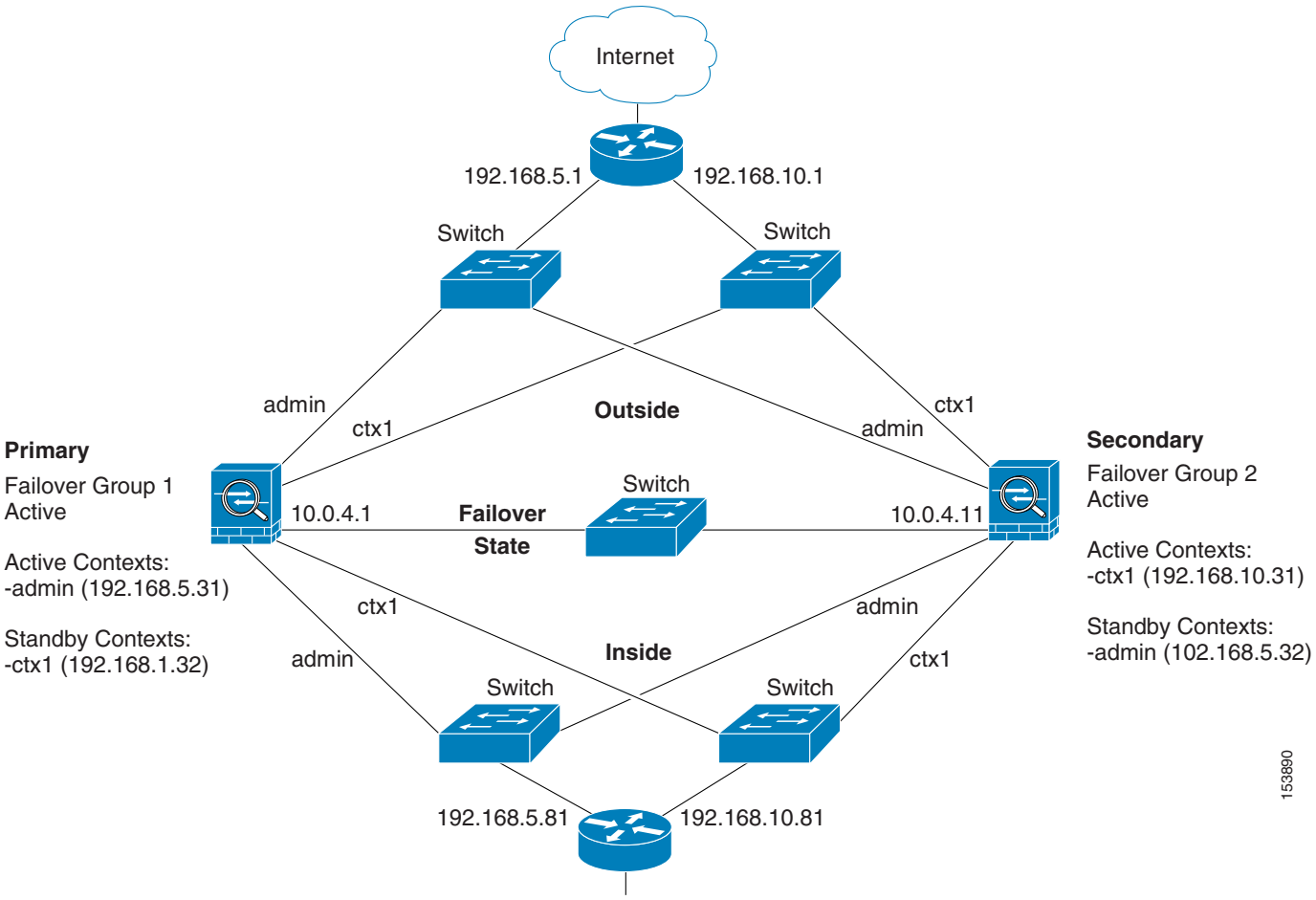
Example 11: Secondary Unit Configuration

```
firewall transparent
failover
failover lan unit secondary
failover lan interface failover ethernet2
failover lan enable
failover key key1
failover interface ip failover 192.168.254.1 255.255.255.0 standby 192.168.254.2
```

Example 12: LAN-Based Active/Active Failover (Transparent Mode)

The following example shows how to configure transparent mode Active/Active failover. In this example there are 2 user contexts, named admin and ctx1. Figure B-8 shows the network diagram for the example.

Figure B-11 Transparent Mode Active/Active Failover Configuration



See the following sections for the configurations for this scenario:

- Example 9: Primary Unit Configuration
- Example 9: Secondary Unit Configuration

Example 12: Primary Unit Configuration

See the following sections for the primary unit configuration:

- Example 9: Primary System Configuration, page B-23
- Example 9: Primary admin Context Configuration, page B-24
- Example 9: Primary ctx1 Context Configuration, page B-25

Example 12: Primary System Configuration

You must first enable multiple context mode using the **mode multiple** command. The mode is not stored in the configuration file, even though it endures reboots. Enter the **show mode** command to view the current mode.

```
firewall transparent
```

```
hostname ciscopix
enable password farscape
password crichton
asdm image flash:/asdm.bin
boot system flash:/cdisk.bin
mac-address auto
interface Ethernet0
   description LAN/STATE Failover Interface
interface Ethernet1
   no shutdown
interface Ethernet2
   no shutdown
interface Ethernet3
   no shutdown
interface Ethernet4
   no shutdown
interface Ethernet5
   no shutdown
interface Ethernet6
   no shutdown
interface Ethernet7
   no shutdown
interface Ethernet8
   no shutdown
interface Ethernet9
   no shutdown
failover
failover lan unit primary
failover lan interface folink Ethernet0
failover link folink Ethernet0
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
failover group 1
   primary
   preempt
failover group 2
   secondary
   preempt
admin-context admin
context admin
   description admin
   allocate-interface Ethernet1
   allocate-interface Ethernet2
   config-url flash:/admin.cfg
   join-failover-group 1
context ctx1
   description context 1
   allocate-interface Ethernet3
   allocate-interface Ethernet4
   config-url flash:/ctx1.cfg
   join-failover-group 2
```

Example 12: Primary admin Context Configuration

```
enable password frek
password elixir
hostname admin
interface Ethernet1
   nameif outside
   security-level 0
interface Ethernet2
   nameif inside
   security-level 100
```

```
ip address 192.168.5.31 255.255.255.0 standby 192.168.5.32
monitor-interface outside
monitor-interface inside
route outside 0.0.0.0 0.0.0.0 192.168.5.1 1
ssh 192.168.5.72 255.255.255.255 inside
```

Example 12: Primary ctx1 Context Configuration

```
enable password quadrophenia
password tommy
hostname ctx1
interface Ethernet3
   nameif inside
   security-level 100
interface Ethernet4
   nameif outside
   security-level 0
access-list 201 extended permit ip any any
access-group 201 in interface outside
logging enable
logging console informational
ip address 192.168.10.31 255.255.255.0 standby 192.168.10.32
monitor-interface inside
monitor-interface outside
route outside 0.0.0.0 0.0.0.0 192.168.10.1 1
```

Example 12: Secondary Unit Configuration

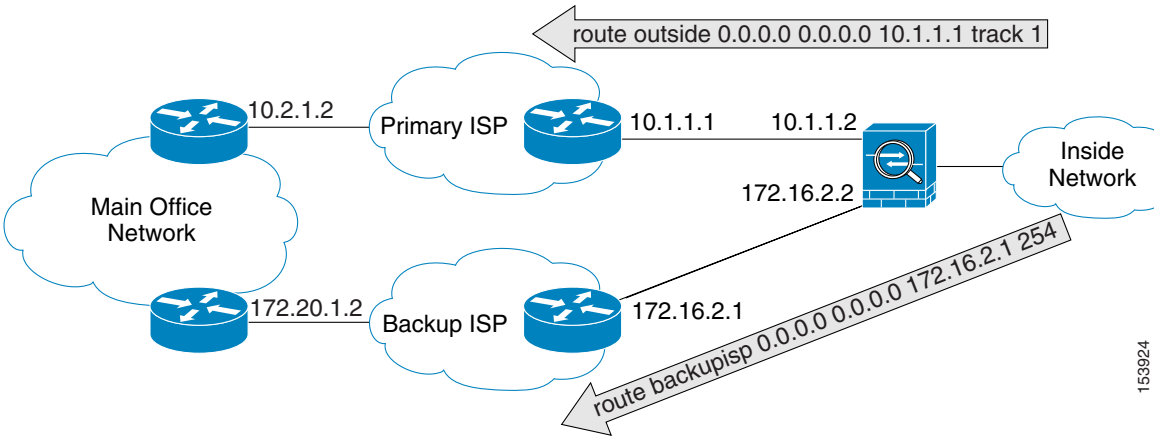
You only need to configure the secondary security appliance to recognize the failover link. The secondary security appliance obtains the context configurations from the primary security appliance upon booting or when failover is first enabled. The **preempt** commands in the failover group configurations cause the failover groups to become active on their designated unit after the configurations have been synchronized and the preempt delay has passed.

```
firewall transparent
failover
failover lan unit secondary
failover lan interface folink Ethernet0
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
```

Example 13: Dual ISP Support Using Static Route Tracking

This configuration shows a remote office using static route tracking to use a backup ISP route if the primary ISP route fails. The security appliance in the remote office uses ICMP echo requests to monitor the availability of the main office gateway. If that gateway becomes unavailable through the default route, the default route is removed from the routing table and the floating route to the backup ISP is used in its place.

Figure B-12 Dual ISP Support

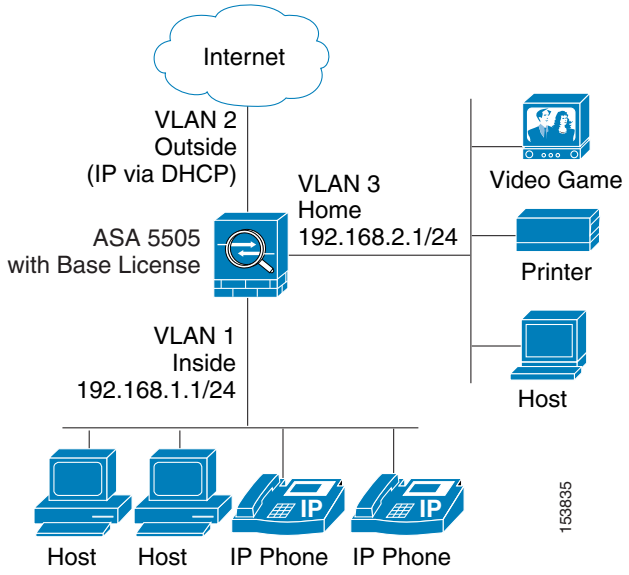



```
passwd password1
enable password password2
hostname myfirewall
asdm image disk0:/asdm.bin
boot system disk0:/image.bin
!
interface gigabitethernet 0/0
   nameif outside
   security-level 0
   ip address 10.1.1.2 255.255.255.0
   no shutdown
!
interface gigabitethernet 0/1
   description backup isp link
   nameif backupisp
   security-level 100
   ip address 172.16.2.2 255.255.255.0
   no shutdown
!
sla monitor 123
   type echo protocol ipIcmpEcho 10.2.1.2 interface outside
   num-packets 3
   timeout 1000
   frequency 3
sla monitor schedule 123 life forever start-time now
!
track 1 rtr 123 reachability
!
route outside 0.0.0.0 0.0.0.0 10.1.1.1 track 1
! The above route is used while the tracked object, router 10.2.1.2
! is available. It is removed when the router becomes unavailable.
!
route backupisp 0.0.0.0 0.0.0.0 172.16.2.1 254
! The above route is a floating static route that is added to the
! routing table when the tracked route is removed.
```

Example 14: ASA 5505 Base License

This configuration creates three VLANs: inside (business), outside (Internet), and home (see Figure B-13). Both the home and inside VLANs can access the outside, but the home VLAN cannot access the inside VLAN. The inside VLAN can access the home VLAN so both VLANs can share a printer. Because the outside IP address is set using DHCP, the inside and home VLANs use interface PAT when accessing the Internet.

Figure B-13 Example 13



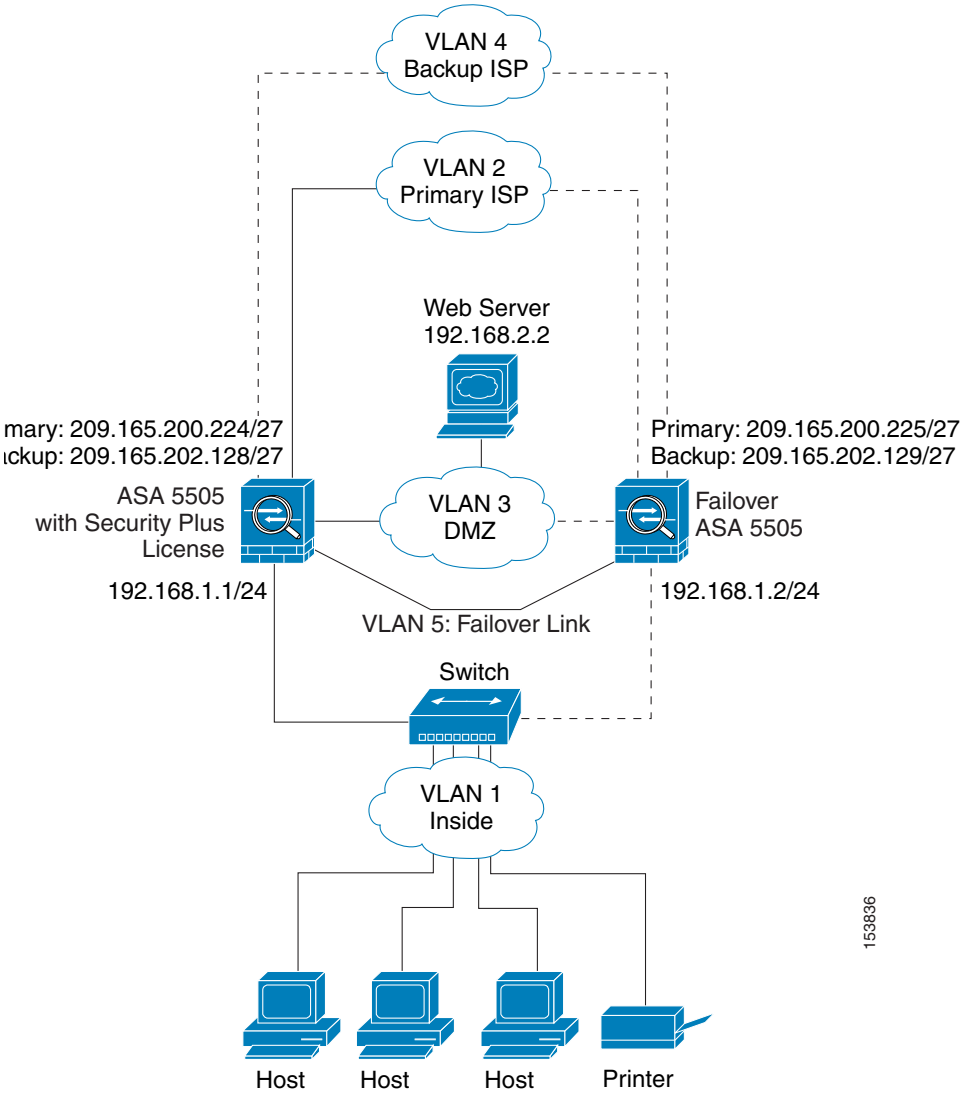

```
passwd g00fba11
enable password gen1u$
hostname Buster
asdm image disk0:/asdm.bin
boot system disk0:/image.bin
interface vlan 2
   nameif outside
   security-level 0
   ip address dhcp setroute
   no shutdown
interface vlan 1
   nameif inside
   security-level 100
   ip address 192.168.1.1 255.255.255.0
   no shutdown
interface vlan 3
! This interface cannot communicate with the inside interface. This is required using
! the Base license
   no forward interface vlan 1
   nameif home
   security-level 50
   ip address 192.168.2.1 255.255.255.0
   no shutdown
interface ethernet 0/0
   switchport access vlan 2
   no shutdown
   interface ethernet 0/1
```

```
   switchport access vlan 1
   no shutdown
interface ethernet 0/2
   switchport access vlan 1
   no shutdown
interface ethernet 0/3
   switchport access vlan 3
   no shutdown
interface ethernet 0/4
   switchport access vlan 3
   no shutdown
interface ethernet 0/5
   switchport access vlan 3
   no shutdown
interface ethernet 0/6
   description PoE for IP phone1
   switchport access vlan 1
   no shutdown
interface ethernet 0/7
   description PoE for IP phone2
   switchport access vlan 1
   no shutdown
nat (inside) 1 0 0
nat (home) 1 0 0
global (outside) 1 interface
! The previous NAT statements match all addresses on inside and home, so you need to
! also perform NAT when hosts access the inside or home networks (as well as the outside).
! Or you can exempt hosts from NAT for inside <--> home traffic, as effected by the
! following:
access-list natexmpt-inside extended permit ip any 192.168.2.0 255.255.255.0
access-list natexmpt-home extended permit ip any 192.168.1.0 255.255.255.0
nat (inside) 0 access-list natexmpt-inside
nat (home) 0 access-list natexmpt-home
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.2-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
ssh 192.168.1.0 255.255.255.0 inside
```

Example 15: ASA 5505 Security Plus License with Failover and Dual-ISP Backup

This configuration creates five VLANs: inside, outside, dmz, backup-isp and faillink (see Figure B-13).

Figure B-14 Example 15



See the following sections for the configurations for this scenario:

- Example 15: Primary Unit Configuration
- Example 16: Network Traffic Diversion

Example 15: Primary Unit Configuration

```
passwd g00fba11
enable password gen1u$
```

```
hostname Buster
asdm image disk0:/asdm.bin
boot system disk0:/image.bin
interface vlan 2
   description Primary ISP interface
   nameif outside
   security-level 0
   ip address 209.165.200.224 standby 209.165.200.225
   backup interface vlan 4
   no shutdown
interface vlan 1
   nameif inside
   security-level 100
   ip address 192.168.1.1 255.255.255.0
   no shutdown
interface vlan 3
   nameif dmz
   security-level 50
   ip address 192.168.2.1 255.255.255.0
   no shutdown
interface vlan 4
   description Backup ISP interface
   nameif backup-isp
   security-level 0
   ip address 209.168.202.128 standby 209.168.202.129
   no shutdown
interface vlan 5
   description LAN Failover Interface
interface ethernet 0/0
   switchport access vlan 2
   no shutdown
interface ethernet 0/1
   switchport access vlan 4
   no shutdown
interface ethernet 0/2
   switchport access vlan 1
   no shutdown
interface ethernet 0/3
   switchport access vlan 3
   no shutdown
interface ethernet 0/4
   switchport access vlan 5
   no shutdown
failover
failover lan unit primary
failover lan interface faillink vlan5
failover lan faillink vlan5
failover polltime unit 3 holdtime 10
failover key key1
failover interface ip faillink 10.1.1.1 255.255.255.0 standby 10.1.1.2
nat (inside) 1 0 0
nat (home) 1 0 0
global (outside) 1 interface
! The previous NAT statements match all addresses on inside and home, so you need to
! also perform NAT when hosts access the inside or home networks (as well as the outside).
! Or you can exempt hosts from NAT for inside <--> home traffic, as effected by the
! following:
access-list natexmpt-inside extended permit ip any 192.168.2.0 255.255.255.0
access-list natexmpt-home extended permit ip any 192.168.1.0 255.255.255.0
nat (inside) 0 access-list natexmpt-inside
nat (home) 0 access-list natexmpt-home
sla monitor 123
 type echo protocol ipIcmpEcho 209.165.200.234 interface outside
 num-packets 2
```

```
 frequency 5
sla monitor schedule 123 life forever start-time now
track 1 rtr 123 reachability
route outside 0 0 209.165.200.234 1 track 1
! This route is for the primary ISP.
route backup-isp 0 0 209.165.202.154 2
! If the link goes down for the primary ISP, either due to a hardware failure
! or unplugged cable, then this route will be used.
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.2-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
ssh 192.168.1.0 255.255.255.0 inside
```

Example 15: Secondary Unit Configuration

You only need to configure the secondary security appliance to recognize the failover link. The secondary security appliance obtains the context configurations from the primary security appliance upon booting or when failover is first enabled.

```
interface ethernet 0/4
   switchport access vlan 5
   no shutdown
failover
failover lan unit secondary
failover lan interface faillink vlan5
failover polltime unit 3 holdtime 10
failover key key1
failover interface ip faillink 10.1.1.1 255.255.255.0 standby 10.1.1.2
```

Example 16: Network Traffic Diversion

The following configuration example shows the ASA 5500 series adaptive security appliance with Version 7.2.1 software and the AIP SSM module with IPS software 5.1.1.

Network traffic that traverses the adaptive security appliance includes internal users who access the Internet, Internet users who access resources protected by an adaptive security appliance in a demilitarized zone (DMZ), or in an inside network. Network traffic sent to and from the adaptive security appliance is not sent to the IPS module for inspection. Examples of traffic not sent to the IPS module include pinging (through ICMP) of the adaptive security appliance interfaces or Telnetting to the adaptive security appliance.

The required configuration components for the ASA 5510 adaptive security appliance include interfaces, access lists, network address translation (NAT), and routing. The required configuration components for the AIP SSM include the network setup, allowed hosts, interface configuration, signature definitions, and event action rules.

To obtain more information about the commands used in this section, use the Command Lookup Tool (for registered customers only).

Note The IP addressing schemes used in this configuration are not legally routable on the Internet. These schemes are RFC 1918 addresses that have been used in a test environment.

Figure B-15 shows the network diagram for this configuration example.

Figure B-15 Network Diagram

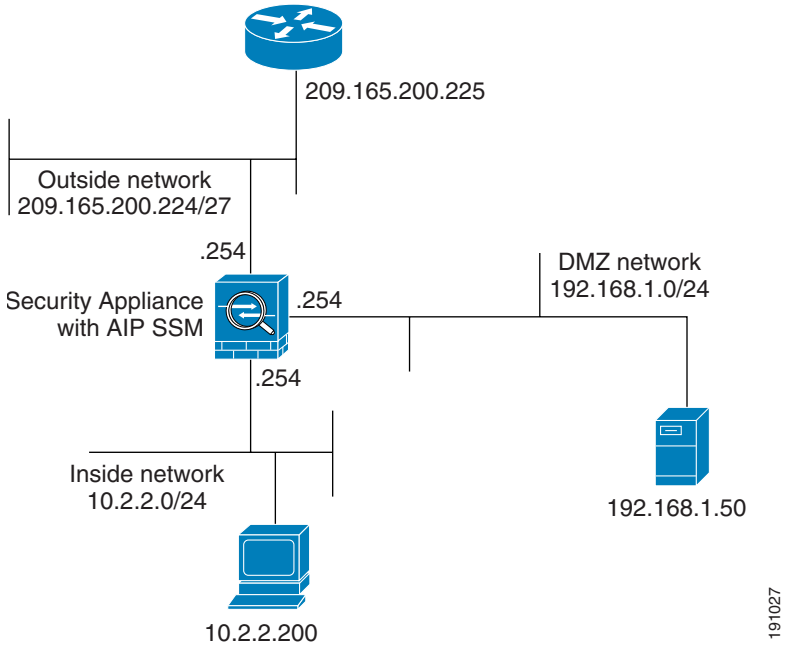


Figure B-16 on page B-39 and Figure B-17 on page B-41 show the initial configurations for the ASA 5510 adaptive security appliance and AIP SSM.

Figure B-16 Configuration for the ASA 5510 Adaptive Security Appliance

```
onionlabaip#show configuration
! ------------------------------
! Version 5.1(1)
! Current configuration last modified Wed Aug 23 09:26:03 2006
! ------------------------------
service interface
exit
! ------------------------------
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/1
exit
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0

!--- The variables are defined.

variables DMZ address 192.168.1.0-192.168.1.255
variables IN address 10.2.2.0-10.2.2.255
exit
! ------------------------------
service host
network-settings

!--- The management IP address is set.

host-ip 172.22.1.169/24,172.22.1.1
host-name onionlabaip
telnet-option disabled
access-list x.x.0.0/16

!--- The access list IP address is removed from the configuration
!--- because the specific IP address is not relevant to this document.

exit
time-zone-settings
offset -360
standard-time-zone-name GMT-06:00
exit
summertime-option recurring
offset 60
summertime-zone-name UTC
start-summertime
month april
week-of-month first
day-of-week sunday
time-of-day 02:00:00
exit
end-summertime
month october
week-of-month last
day-of-week sunday
time-of-day 02:00:00
exit
exit


asdm image disk0:/asdm521.bin
no asdm history enable
arp timeout 14400
```

191240

```
!--- Translation rules are added.

global (outside) 1 172.16.1.100
global (dmz) 1 192.168.1.100
nat (inside) 1 10.2.2.0 255.255.255.0
static (dmz,outside) 172.16.1.50 192.168.1.50 netmask 255.255.255.255
static (inside,dmz) 10.2.2.200 10.2.2.200 netmask 255.255.255.255

!--- Access lists are applied to the interfaces.

access-group acl_outside_in in interface outside
access-group acl_inside_in in interface inside
access-group acl_dmz_in in interface dmz
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
telnet timeout 5
ssh timeout 5
console timeout 0
!
class-map inspection_default

 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
 message-length maximum 512
policy-map global_policy

!--- Out-of-the-box default configuration includes
!--- policy-map global_policy.

class inspection_default
 inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
!
service-policy global_policy global

!--- Out-of-the-box default configuration includes
!--- the service-policy global_policy applied globally.

prompt hostname context
.
: end
```

Figure B-17 Configuration for the AIP SSM

```
ciscoasa#show running-config
: Saved
:
ASA Version 7.2(1)
!
hostname ciscoasa
enable password WwXYvtKrnjXqGbu1 encrypted
names
!

!--- IP addressing is added to the default configuration.

interface Ethernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.254 255.255.255.0
!
interface Ethernet0/1
 nameif inside
 security-level 100
 ip address 10.2.2.254 255.255.255.0
!
interface Ethernet0/2
 nameif dmz
 security-level 50
 ip address 192.168.1.254 255.255.255.0
!
interface Management0/0
 nameif management
 security-level 0
 ip address 172.22.1.160 255.255.255.0
 management-only
!
passwd 2KFQnbNIdI.2KYOU encrypted
ftp mode passive

!--- Access lists are added in order to allow test
!--- traffic (ICMP and Telnet).

access-list acl_outside_in extended permit icmp any host 172.16.1.50
access-list acl_inside_in extended permit ip 10.2.2.0 255.255.255.0 any
access-list acl_dmz_in extended permit icmp 192.168.1.0 255.255.255.0 any
pager lines 24

!--- Logging is enabled.

logging enable
logging buffered debugging
mtu outside 1500
mtu inside 1500
mtu dmz 1500
mtu management 1500

exit
! ------------------------------
service logger
exit
! ------------------------------
```

191241

```
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0

!--- The signature is modified from the default setting for testing purposes.

signatures 2000 0
alert-severity high
engine atomic-ip
event-action produce-alert|produce-verbose-alert
exit
alert-frequency
summary-mode fire-all
summary-key AxBx
exit
exit
status
enabled true
exit
exit

!--- The signature is modified from the default setting for testing purposes.

signatures 2004 0
alert-severity high
engine atomic-ip
event-action produce-alert|produce-verbose-alert
exit
alert-frequency
summary-mode fire-all
summary-key AxBx
exit
exit
status
enabled true
exit
exit

!--- The custom signature is added for testing purposes.

signatures 60000 0
alert-severity high
sig-fidelity-rating 75
sig-description
sig-name Telnet Command Authorization Failure
sig-string-info Command authorization failed
sig-comment signature triggers string command authorization failed
exit
engine atomic-ip
specify-l4-protocol yes
l4-protocol tcp
no tcp-flags
no tcp-mask
exit
specify-payload-inspection yes

regex-string Command authorization failed
exit
exit
exit
```

```
exit
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
enable-tls true
exit
onionlabaip#
```

Inspecting All Traffic with the AIP SSM

This configuration meets the requirement to monitor all traffic. In addition, you must make two decisions about how the ASA 5510 and AIP SSM interact.

- Is the AIP SSM module to be deployed in promiscuous or inline mode?

  Promiscuous mode means that a copy of the data is sent to the AIP SSM while the ASA 5510 forwards the original data to the destination. The AIP SSM in promiscuous mode can be considered as an intrusion detection system (IDS). In this mode, the trigger packet that causes the alarm can still reach the destination. Shunning can occur and stop additional packets from reaching the destination; however, the trigger packet is not stopped.

  Inline mode means that the ASA 5510 forwards the data to the AIP SSM for inspection. If the data passes AIP SSM inspection, the data returns to the ASA 5510 in order to continue being processed and sent to the destination. The AIP SSM in inline mode can be considered to be an intrusion prevention system (IPS). Unlike promiscuous mode, an inline mode IPS can actually stop the trigger packet from reaching the destination.

- If the ASA 5510 cannot communicate with the AIP SSM, how should the adaptive security appliance handle traffic for inspection?

  Examples of instances when the ASA 5510 cannot communicate with the AIP SSM include AIP SSM reloads or whether the module fails and needs replacement. In this case, the adaptive security appliance can fail-open or fail-closed.

  Fail-open allows the adaptive security appliance to continue to pass traffic for inspection to the final destination if the AIP SSM cannot be reached. Fail-closed blocks traffic for inspection when the adaptive security appliance cannot communicate with the AIP SSM.

Note Define the traffic for inspection with an access list. In the following example, the access list permits all IP traffic from any source to any destination. Therefore, traffic for inspection can be anything that passes through the adaptive security appliance.

```
ciscoasa(config)#access-list traffic_for_ips permit ip any any
ciscoasa(config)#class-map ips_class_map
ciscoasa(config-cmap)#match access-list traffic_for_ips

!--- The match any
!--- command can be used in place of the match access-list [access-list name]
!--- command. In this example, access-list traffic_for_ips permits
!--- all traffic. The match any command also
```

```
!--- permits all traffic. You can use either configuration.
!--- When you define an access-list, it can ease troubleshooting.

ciscoasa(config)#policy-map global_policy

!--- Note that policy-map global_policy is a part of the
!--- default configuration. In addition, policy-map global_policy is applied
!--- globally using the service-policy command.

ciscoasa(config-pmap)#class ips_class_map
ciscoasa(config-pmap-c)#ips inline fail-open

!--- Two decisions need to be made.
    !--- First, does the AIP-SSM function
    !--- in inline or promiscuous mode?
    !--- Second, does the ASA fail-open or fail-closed?
```

Inspecting Specific Traffic with the AIP SSM

If you want the AIP SSM to monitor a subset of all traffic, you can modify two independent variables on the adaptive security appliance:

- You can write the access list to include or exclude the necessary traffic.
- You can apply a service policy to an interface or globally.

The network diagram in Figure B-15 shows the AIP SSM inspecting all traffic between the outside network and the DMZ network, as shown in the following example:

```
ciscoasa#configure terminal
ciscoasa(config)#access-list traffic_for_ips deny ip 10.2.2.0 255.255.255.0 192.168.1.0
255.255.255.0
ciscoasa(config)#access-list traffic_for_ips permit ip any 192.168.1.0 255.255.255.0
ciscoasa(config)#access-list traffic_for_ips deny ip 192.168.1.0 255.255.255.0 10.2.2.0
255.255.255.0
ciscoasa(config)#access-list traffic_for_ips permit ip 192.168.1.0 255.255.255.0 any
ciscoasa(config)#class-map ips_class_map
ciscoasa(config-cmap)#match access-list traffic_for_ips
ciscoasa(config)#policy-map interface_policy
ciscoasa(config-pmap)#class ips_class_map
ciscoasa(config-pmap-c)#ips inline fail-open
ciscoasa(config)#service-policy interface_policy interface dmz

!--- The access-list denies traffic from the inside network to the DMZ network
!--- and traffic to the inside network from the DMZ network.
!--- In addition, the service-policy command is applied to the DMZ interface.
```

The following example shows how to configure the AIP SSM to monitor traffic from the inside network to the outside network, but exclude the inside network to the DMZ network.

Note You must have an intermediate understanding of statefulness, TCP, UDP, ICMP, connection, and connectionless communications to understand the following example.

```
ciscoasa#configure terminal
    ciscoasa(config)#access-list traffic_for_ips deny ip 10.2.2.0 255.255.255.0
192.168.1.0 255.255.255.0
    ciscoasa(config)#access-list traffic_for_ips permit ip 10.2.2.0
255.255.255.0 any
    ciscoasa(config)#class-map ips_class_map
```

```
    ciscoasa(config-cmap)#match access-list traffic_for_ips
    ciscoasa(config)#policy-map interface_policy
    ciscoasa(config-pmap)#class ips_class_map
    ciscoasa(config-pmap-c)#ips inline fail-open
ciscoasa(config)#service-policy interface_policy interface inside
```

The access list denies traffic initiated on the inside network destined for the DMZ network. The second access list line permits or sends traffic initiated on the inside network destined for the outside network to the AIP SSM. At this point the statefulness of the adaptive security appliance comes into play.

For example, an internal user initiates a TCP connection (Telnet) to a device on the outside network (router). The user successfully connects to the router and logs in, then issues a router command that is not authorized. The router responds with the message, "Command authorizaton failed." The data packet that contains the message, "Command authorization failed" has the outside router as the source and the inside user as the destination. The source (outside) and destination (inside) do not match the access lists previously defined. The adaptive security appliance keeps track of stateful connections. As a result, the returning data packet (outside to inside) is sent to the AIP SSM for inspection. Custom signature 60000 0 (configured on the AIP SSM) alarms.

Note By default, the adaptive security appliance does not maintain state for the ICMP traffic. In the previous example, the internal user pings (ICMP echo request) the outside router. The router responds with an ICMP echo-reply. The AIP SSM inspects the echo request packet, but not the echo-reply packet. If ICMP inspection is enabled on the adaptive security appliance, both the echo request and echo-reply packets are inspected by the AIP SSM.

Verifying the Recording of Alert Events

To verify that alert events are recorded in the AIP SSM, perform the following steps:

Step 1 Log into the AIP SSM with the administrator user account.

Note The output varies according to signature settings, the type of traffic sent to the AIP SSM, and network load.

The Output Interpreter Tool (OIT), for registered customers only, supports certain **show** commands. Use the OIT to view an analysis of **show** command output. This tools is one of a set of support tools, available at https://www.cisco.com/pcgi-bin/Support/OutputInterpreter/home.pl.

Step 2 Enter the **show events alert** command.

The following output appears.

```
evIdsAlert: eventId=1156198930427770356 severity=high vendor=Cisco
    originator:
        hostId: onionlabaip
        appName: sensorApp
        appInstanceId: 345
time: 2006/08/24 18:52:57 2006/08/24 13:52:57 UTC
signature: description=Telnet Command Authorization Failure id=60000 version=custom
    subsigId: 0
    sigDetails: Command authorization failed
interfaceGroup:
vlan: 0
participants:
```

```
    attacker:
        addr: locality=OUT 172.16.1.200
        port: 23
    target:
        addr: locality=IN 10.2.2.200
        port: 33189
riskRatingValue: 75
interface: ge0_1
protocol: tcp

evIdsAlert: eventId=1156205750427770078 severity=high vendor=Cisco
    originator:
    hostId: onionlabaip
    appName: sensorApp
    appInstanceId: 345
time: 2006/08/24 19:46:08 2006/08/24 14:46:08 UTC
signature: description=ICMP Echo Request id=2004 version=S1
    subsigId: 0
interfaceGroup:
vlan: 0
participants:
    attacker:
        addr: locality=OUT 172.16.1.200
    target:
        addr: locality=DMZ 192.168.1.50
triggerPacket:
000000 00 16 C7 9F 74 8C 00 15 2B 95 F9 5E 08 00 45 00 ....t...+..^..E.
000010 00 3C 2A 57 00 00 FF 01 21 B7 AC 10 01 C8 C0 A8 .<*W....!.......
000020 01 32 08 00 F5 DA 11 24 00 00 00 01 02 03 04 05 .2.....$........
000030 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 ................
000040 16 17 18 19 1A 1B 1C 1D 1E 1F ..........
riskRatingValue: 100
interface: ge0_1
protocol: icmp

evIdsAlert: eventId=1156205750427770079 severity=high vendor=Cisco originator:
hostId: onionlabaip
appName: sensorApp
appInstanceId: 345
time: 2006/08/24 19:46:08 2006/08/24 14:46:08 UTC
signature: description=ICMP Echo Reply id=2000 version=S1
subsigId: 0
 interfaceGroup:
vlan: 0
 participants:
attacker:
addr: locality=DMZ 192.168.1.50
target:
addr: locality=OUT 172.16.1.200
triggerPacket:
000000 00 16 C7 9F 74 8E 00 03 E3 02 6A 21 08 00 45 00 ....t.....j!..E.
000010 00 3C 2A 57 00 00 FF 01 36 4F AC 10 01 32 AC 10 .<*W....6O...2..
000020 01 C8 00 00 FD DA 11 24 00 00 00 01 02 03 04 05 .......$........
000030 06 07 08 09 0A 0B 0C 0D 0E 0F 10 11 12 13 14 15 ................
000040 16 17 18 19 1A 1B 1C 1D 1E 1F ..........
riskRatingValue: 100
interface: ge0_1
protocol: icmp
```

In these configurations, several IPS signatures are tuned to alarm on test traffic. Signatures 2000 and 2004 are modified. Custom signature 60000 is added. In a network where little data passes through the adaptive security appliance, you may need to modify signatures in order to trigger events. If the adaptive security appliance and AIP SSM are deployed in an environment that passes a large amount of traffic, the default signature settings will probably generate an event.

Troubleshooting the Configuration

To troubleshoot your configuration, perform the following steps:

The OIT (for registered customers only) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Step 1 From the ASA 5510, enter these **show** commands:

a. **show module—**Shows information about the SSM on the adaptive security appliance as well as system information.

```
ciscoasa#show module
Mod Card Type Model Serial No.
--- ------------------------------------------ ------------------ -----------
0 ASA 5510 Adaptive Security Appliance ASA5510 JMX1016K0RN
1 ASA 5500 Series Security Services Module-10 ASA-SSM-10 JAB101502A6

Mod MAC Address Range Hw Version Fw Version Sw Version
--- ------------------------------- ------------ ------------ ---------------
 0 0016.c79f.748c to 0016.c79f.7490 1.1 1.0(10)0 7.2(1)
 1 0016.c79f.7567 to 0016.c79f.7567 1.0 1.0(10)0 5.1(1)S205.0

Mod SSM Application Name Status SSM Application Version
--- ------------------------------ ---------------- --------------------------
1 IPS Up 5.1(1)S205.0

Mod Status Data Plane Status Compatibility
--- ------------------ ---------------------- -------------
0 Up Sys Not Applicable
1 Up Up

!--- Each of the areas highlighted indicate that
!--- the ASA recognizes the AIP-SSM and the AIP-SSM status is up.
```

b. **show run**—Shows the current running configuration on the adaptive security appliance.

```
ciscoasa#show run

!--- Output is suppressed.

access-list traffic_for_ips extended permit ip any any
...
class-map ips_class_map
match access-list traffic_for_ips
...
policy-map global_policy
...
class ips_class_map
ips inline fail-open
...
service-policy global_policy global
```

```
!--- Each of these lines are needed
!--- in order to send data to the AIP-SSM.
```

c. show access-list —Shows the counters for an access list.

```
ciscoasa#show access-list traffic_for_ips
access-list traffic_for_ips; 1 elements
access-list traffic_for_ips line 1 extended permit ip any any (hitcnt=2) 0x9bea7286

!--- Confirms the access-list displays a hit count greater than zero.
```

Step 2 Before you install and use the AIP SSM, if network traffic does not pass through the adaptive security appliance as expected, troubleshoot the network and ASA 5510 access policy rules.