Sample Configurations

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

For failover examples, see Chapter 11, "Failover Configuration Examples,"

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).

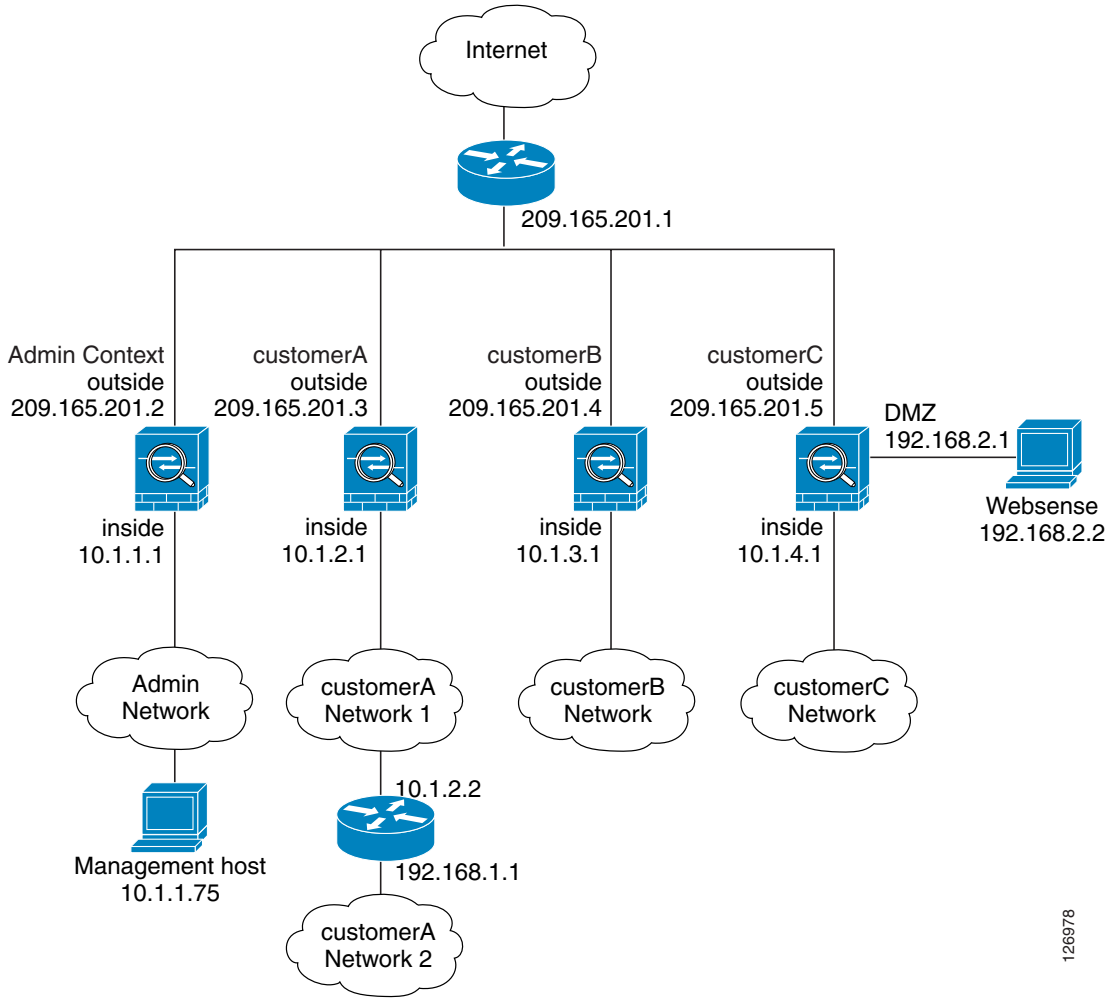
Inside hosts can access the Internet through the outside using dynamic NAT or PAT, but no outside hosts can access the inside.

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 2
- Example 1: Admin Context Configuration, page 3
- Example 1: Customer A Context Configuration, page 4
- Example 1: Customer B Context Configuration, page 4
- Example 1: Customer C Context Configuration, page 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. If you view the configuration on the security appliance using the **write terminal**, **show startup-config**, or **show running-config** commands, the mode displays after the security appliance Version (blank means single mode, "<system>" means you are in multiple mode in the system configuration, and <context> means you are in multiple mode in a context).

```
hostname Farscape
password passw0rd
enable password chr1cht0n
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
context admin
    allocate-interface gigabitethernet 0/0.3
    allocate-interface gigabitethernet 0/1.4
    config-url disk0://admin.cfg
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
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
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
```

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

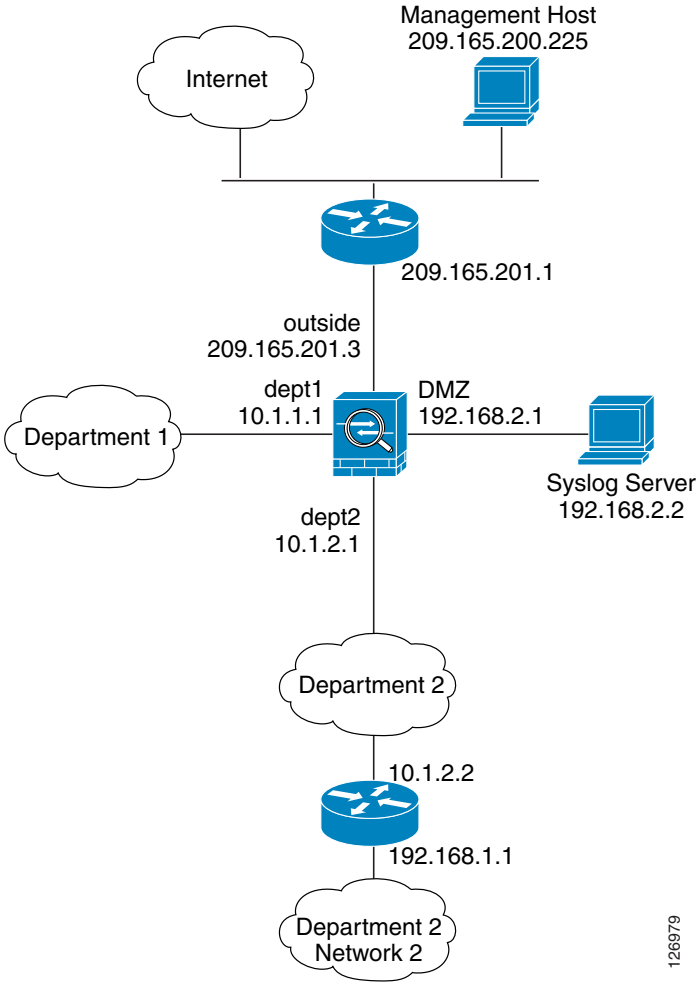
```
interface gigabitethernet 0/0.3
    nameif outside
    security-level 0
    ip address 209.165.201.5 255.255.255.224
    no shutdown
interface gigabitethernet 0/1.7
    nameif inside
    security-level 100
    ip address 10.1.4.1 255.255.255.0
    no shutdown
interface gigabitethernet 0/1.8
    nameif 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. Because 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




```
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
    no shutdown
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
passwd g00fba11
enable password gen1u$
hostname Buster
```

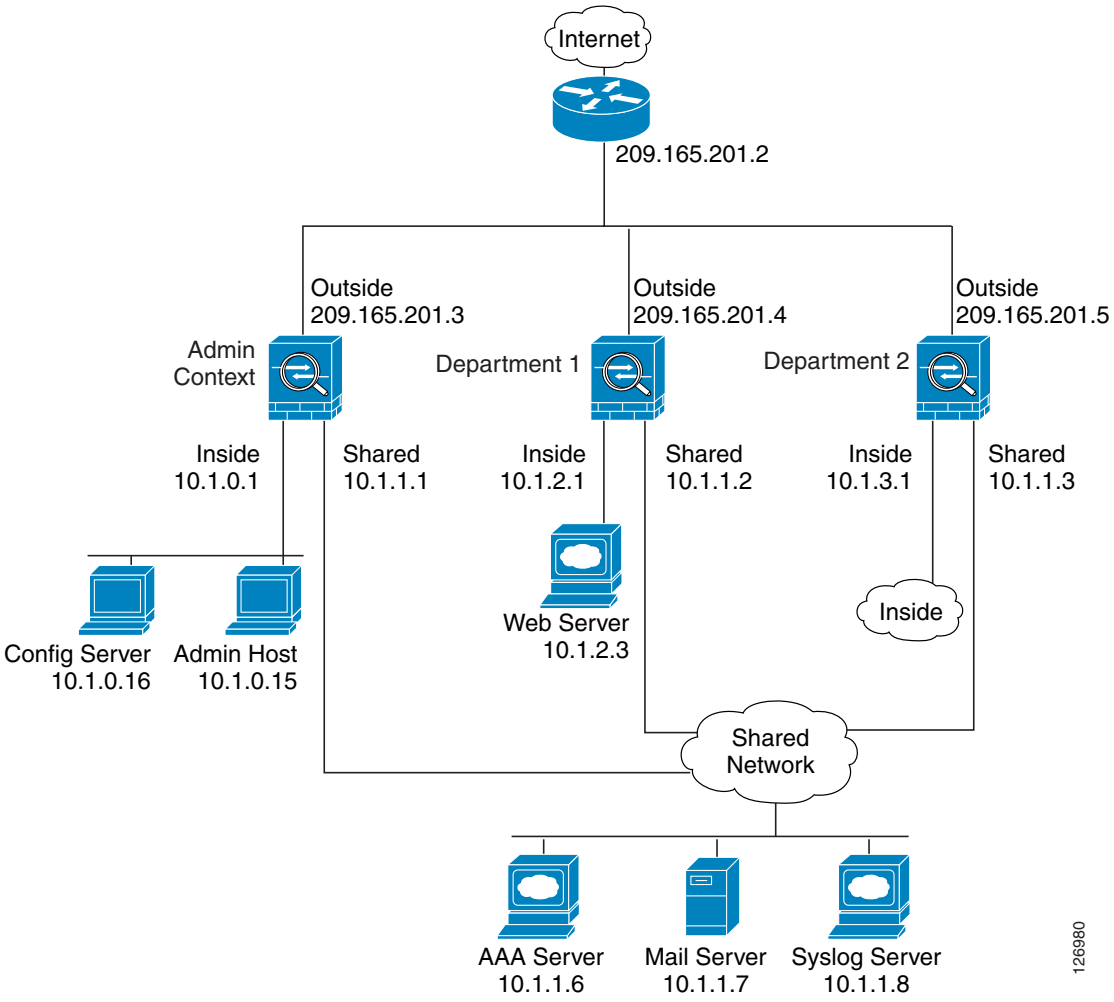
```
same-security-traffic permit inter-interface
route outside 0 0 209.165.201.1 1
nat (dept1) 1 10.1.1.0 255.255.255.0
nat (dept2) 1 10.1.2.0 255.255.255.0
! The dept1 and dept2 networks use PAT when accessing the outside
global (outside) 1 209.165.201.9 netmask 255.255.255.255
! Because we perform 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 router.
rip dept2 default version 2 authentication md5 scorpius 1
! Listens for RIP updates from the downstream router. The security appliance does not
! listen for RIP updates from the router because a default route to the router is all that
! is required.
rip dept2 passive version 2 authentication md5 scorpius 1
! 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 on
```

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 8
- Example 3: Admin Context Configuration, page 9
- Example 3: Department 1 Context Configuration, page 10
- Example 3: Department 2 Context Configuration, page 11

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. If you view the configuration on the security appliance using the **write terminal**, **show startup-config**, or **show running-config** commands, the mode displays after the security appliance Version (blank means single mode, "<system>" means you are in multiple mode in the system configuration, and <context> means you are in multiple mode in a context).

```
hostname Ubik
password pkd55
enable password deckard69
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 on
```

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 on
```

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 on
```

Example 4: Multiple Mode, Transparent Firewall with Outside Access

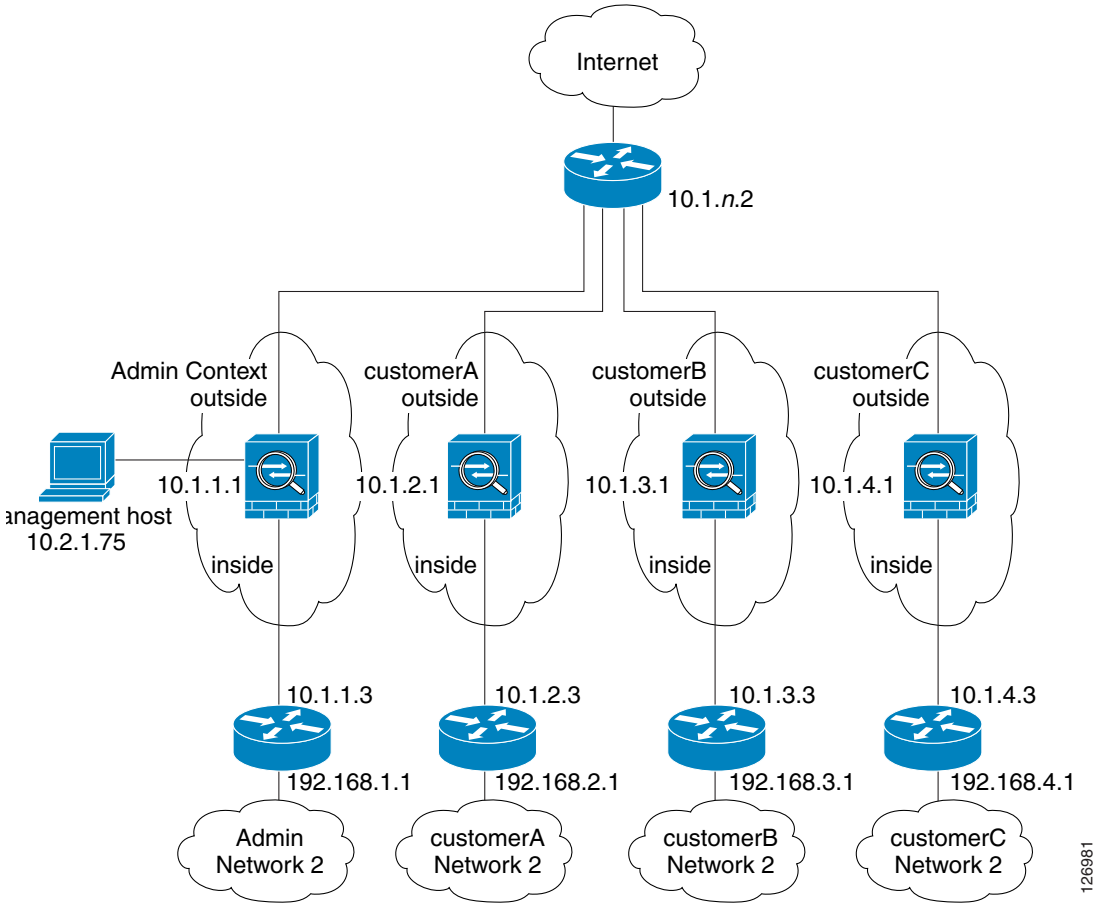
This configuration creates three security contexts plus the admin context. Each context allows OSPF traffic to pass between the inside and outside routers (see Figure B-4).

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

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

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. If you view the configuration on the security appliance using the **write terminal**, **show startup-config**, or **show running-config** commands, the mode displays after the security appliance version (blank means single mode, "<system>" means you are in multiple mode in the system configuration, and <context> means you are in multiple mode in a context).

```
firewall transparent
hostname Farscape
password passw0rd
enable password chr1cht0n
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
context admin
    allocate-interface gigabitethernet 0/0.150
    allocate-interface gigabitethernet 0/1.4
    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
passwd secret1969
enable password h1andl0
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 simultaneous ASDM/WebVPN use on the same interface is not supported.

```
! 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 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.
! ASDM session is not allowed on this interface.
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
```