

PIX/ASA 7.x and Above: Multiple Context Configuration Example

Document ID: 99131

Introduction

Prerequisites

- Requirements
- Components Used
- Related Products
- Conventions

Background Information

- Context Configuration Files
- Management Access to Security Contexts

Configure

- Network Diagram
- Enable or Disable Multiple Context Mode
- Configure a Security Context
- ASA 8.x – System Execution Space Configuration
- Change Between Contexts and the System Execution Space
- ASA – Context1 Configuration
- ASA – Context2 Configuration
- Save Configuration Changes in Multiple Context Mode

Verify

Troubleshoot

- Restore Single Context Mode
- Assign the Same IP Address to the Shared Interfaces in the Multiple Context Mode
- Rename the Context
- Delete Context

NetPro Discussion Forums – Featured Conversations

Related Information

Introduction

This document describes the steps used to configure multiple context in security appliances.

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

You can use multiple security contexts in these situations:

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

Note: In Multi–context mode, you can upgrade or downgrade the PIX/ASA software only in the System EXEC mode, not in the other context modes.

For more information about the steps used to configure multiple context in the Firewall Service Module (FWSM), refer to FWSM: Multiple Context Configuration Example.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on these software and hardware versions:

- Cisco 5500 Series Adaptive Security Appliance runs with Software Version 7.x and later.

Note: The multiple context feature is not supported on the ASA 5505 Series Adaptive Security Appliance.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This configuration can also be used with Cisco PIX 500 Series Security Appliance Version 7.x and later.

Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Background Information

Context Configuration Files

Context Configurations

The security appliance includes a configuration for each context that identifies the security policy, interfaces, and almost all the options you can configure on a standalone device. You can store context configurations on the internal Flash memory or the external Flash memory card, or you can download them from a TFTP, FTP, or HTTP(S) server.

System Configuration

The system administrator adds and manages contexts by the configuration of each context configuration location, allocated interfaces, and other context operational parameters in the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the security appliance. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as context downloads from the server), it uses one of the contexts that is designated as the admin context. The system

configuration does include a specialized failover interface for failover traffic only.

Admin Context Configuration

The admin context is just like any other context, except that when a user logs in to the admin context, that user has system administrator rights and can access the system and all other contexts. The admin context is not restricted in any way, and can be used as a regular context, but, because logging into the admin context grants you administrator privileges over all contexts, you need to restrict access to the admin context to appropriate users. The admin context must reside on Flash memory, and not remotely.

If your system is already in multiple context mode, or if you convert from single mode, the admin context is created automatically as a file on the internal Flash memory called `admin.cfg`. This context is named "admin." If you do not want to use `admin.cfg` as the admin context, you can change the admin context.

Note: Admin context is not counted in the context license. For example, if you get the license for two contexts, you are allowed to have the admin context and two other contexts.

Management Access to Security Contexts

The security appliance provides system administrator access in multiple context mode, as well as access for individual context administrators. These sections describe logging in as a system administrator or as a context administrator:

System Administrator Access

You can access the security appliance as a system administrator in two ways:

- Access the security appliance console.

From the console, you access the system execution space.

- Access the admin context with Telnet, SSH, or ASDM.

See "Managing System Access," to enable Telnet, SSH, and SDM access.

As the system administrator, you can access all contexts.

When you change to a context from admin or the system, your username changes to the default "enable_15" username. If you configured command authorization in that context, you need to either configure authorization privileges for the "enable_15" user, or you can log in as a different name for which you provide sufficient privileges in the command authorization configuration for the context. In order to log in with a username, enter the login command. For example, you log in to the admin context with the username "admin." The admin context does not have any command authorization configuration, but all other contexts include command authorization. For convenience, each context configuration includes a user "admin" with maximum privileges. When you change from the admin context to context A, your username is altered, so you must log in again as "admin" with the login command. When you change to context B, you must again enter the login command to log in as "admin."

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

Context Administrator Access

You can access a context with Telnet, SSH, or ASDM. If you log in to a non-admin context, you can only access the configuration for that context. You can provide individual logins to the context.

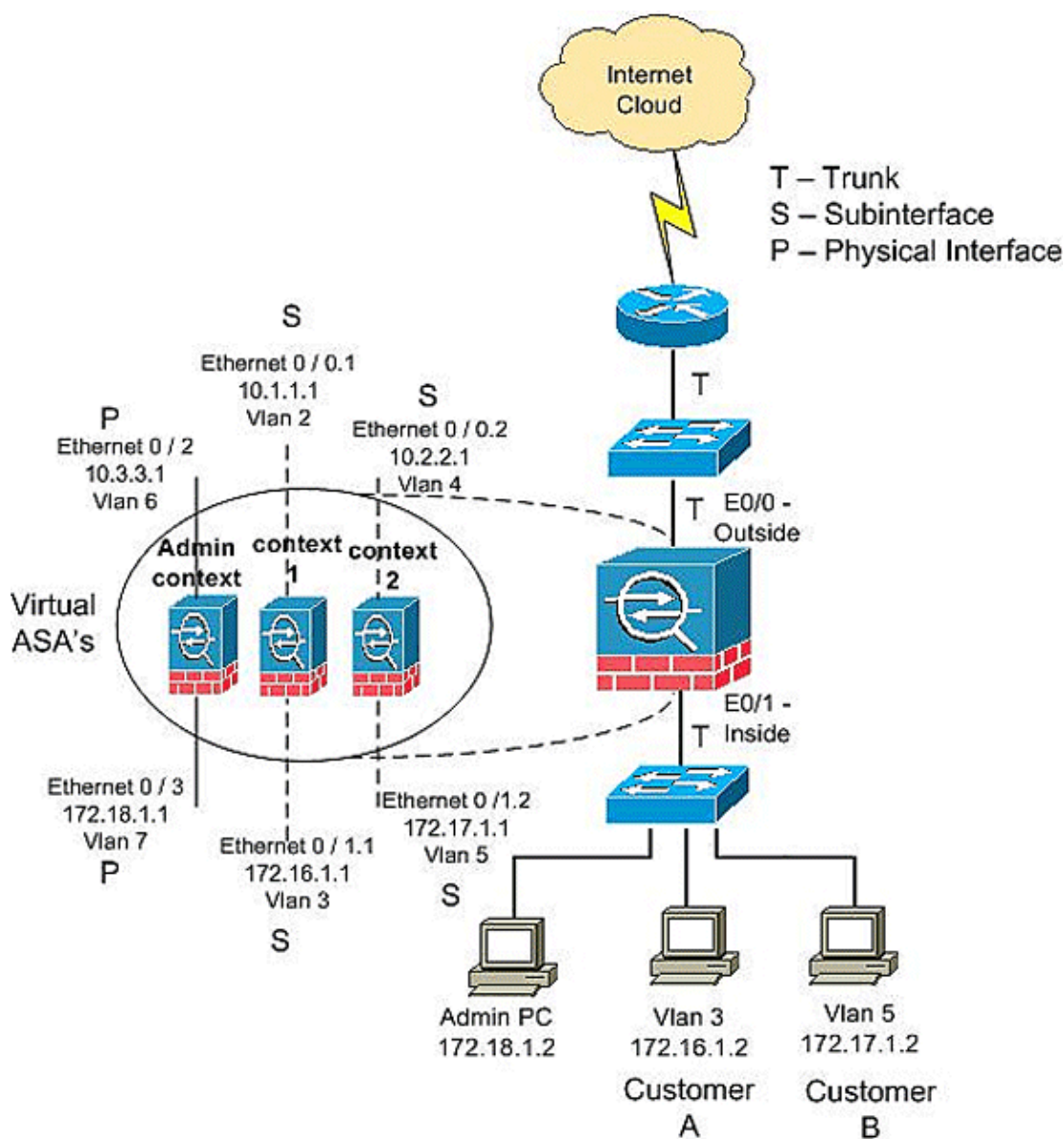
Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Network Diagram

This document uses this network setup:



Note: The ports on the switch that are connected to ASA must be in trunk mode since multiple VLAN traffic has to travel through it once the ASA interfaces are broken into sub-interfaces.

Enable or Disable Multiple Context Mode

Your security appliance is possibly already configured for multiple security contexts dependent upon how you ordered it from Cisco, but if you upgrade, you might need to convert from single mode to multiple mode. This

section explains the procedures to upgrade. ASDM does not support changing modes, so you need to change modes with the CLI.

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

Enable Multiple Context Mode

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

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

In order to enable multiple mode, enter this command:

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

You are prompted to reboot the security appliance.

```
CiscoASA(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]
!
The old running configuration file will be written to flash

The admin context configuration will be written to flash

The new running configuration file was written to flash
Security context mode: multiple

***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode

Rebooting...

Booting system, please wait...
*
*
!--- output suppressed

*
*
INFO: Admin context is required to get the interfaces
*** Output from config line 20, "arp timeout 14400"
Creating context 'admin'... Done. (1)
*** Output from config line 23, "admin-context admin"

Cryptochecksum (changed): a219baf3 037b31b4 09289829 1ab9790a
```

*** Output from config line 25, " config-url flash:/admi..."

```
Cryptochecksum (changed): d4f0451b 405720e1 bbccf404 86be061c
Type help or '?' for a list of available commands.
CiscoASA>
```

After reboot, this is the default configuration of the ASA:

ASA 8.x Default Configuration
<pre>CiscoASA# show running-config : Saved : ASA Version 8.0(2) <system> ! hostname CiscoASA enable password 8Ry2YjIyt7RRXU24 encrypted no mac-address auto ! interface Ethernet0/0 shutdown ! interface Ethernet0/1 shutdown ! interface Ethernet0/2 shutdown ! interface Ethernet0/3 shutdown ! interface Management0/0 shutdown ! class default limit-resource All 0 limit-resource ASDM 5 limit-resource SSH 5 limit-resource Telnet 5 ! ftp mode passive pager lines 24 no failover asdm image disk0:/asdm-602.bin no asdm history enable arp timeout 14400 console timeout 0 admin-context admin context admin config-url disk0:/admin.cfg ! !--- admin context is created !--- by default once you enable !--- multiple mode prompt hostname context Cryptochecksum:410be16e875b7302990a831a5d91aefd : end</pre>

Configure a Security Context

The security context definition in the system configuration identifies the context name, configuration file URL, and interfaces that a context can use.

Note: If you do not have an admin context (for example, if you clear the configuration), you must first specify the admin context name when you enter this command:

```
hostname(config)# admin-context <name>
```

Note: Although this context name does not exist yet in your configuration, you can subsequently enter the context name command to match the specified name to continue the admin context configuration.

In order to add or change a context in the system configuration, perform these steps:

1. In order to add or modify a context, enter this command in the **system execution space**:

```
hostname(config)# context <name>
```

The name is a string up to 32 characters long. This name is case sensitive, so you can have two contexts named "customerA" and "CustomerA," for example. You can use letters, digits, or hyphens, but you cannot start or end the name with a hyphen.

"System" or "Null" (in upper or lower case letters) are reserved names, and cannot be used.

2. (Optional) In order to add a description for this context, enter this command:

```
hostname(config-ctx)# description text
```

3. In order to specify the interfaces that you can use in the context, enter the command appropriate for a physical interface or for one or more subinterfaces.

- ◆ In order to allocate a physical interface, enter this command:

```
hostname(config-ctx)# allocate-interface  
<physical_interface> [mapped_name]  
[visible | invisible]
```

- ◆ In order to allocate one or more subinterfaces, enter this command:

```
hostname(config-ctx)# allocate-interface  
<physical_interface.subinterface[-physical_interface.subinterface]>  
[mapped_name[-mapped_name]] [visible | invisible]
```

You can enter these commands multiple times to specify different ranges. If you remove an allocation with the no form of this command, any context commands that include this interface are removed from the running configuration.

4. In order to identify the URL from which the system downloads the context configuration, enter this command:

```
hostname(config-ctx)# config-url url
```

Note: Enter the **allocate-interface** command(s) before you enter the **config-url** command. The security appliance must assign interfaces to the context before it loads the context configuration; the context configuration can include commands that refer to interfaces (interface, nat, global...). If you enter the **config-url** command first, the security appliance loads the context configuration immediately. If the context contains any commands that refer to interfaces, those commands fail.

In this scenario, follow the steps in the table to configure the multiple context.

There are two customers, Customer A and Customer B. Create three multiple contexts (virtually three ASAs) in a single ASA box such as Context1 for Customer A , Context2 for Customer B, and Admin Context to administrate the ASA contexts.

Create two subinterfaces for each context for inside and outside connection. Assign the different VLANs for each subinterface.

Create the two subinterfaces in ethernet 0/0 as ethernet 0/0.1, ethernet 0/0.2 for outside connection of context1 and context2, respectively. Similarly, create two subinterfaces in ethernet 0/1 as ethernet 0/1.1, ethernet 0/1.2 for inside connection of context1 and context2, respectively.

Assign vlan for each subinterface such as vlan 2 for ethernet 0/0.1, vlan3 for ethernet 0/1.1,vlan 4 for ethernet 0/0.2, vlan5 for ethernet 0/1.2.

ASA Multiple Context Configuration Steps

```
:  
  
!--- Outside interface for context1 and context2.  
!--- Create the sub interface in  
!--- outside interface for context1 and context2.  
  
ciscoasa(config)# interface Ethernet0/0  
ciscoasa(config-if)# no shutdown  
  
!--- Inside interface for context1 and context2.  
!--- Create the sub interface in  
!--- inside interface for context1 and context2.  
  
ciscoasa(config)# interface Ethernet0/1  
ciscoasa(config-if)# no shutdown  
  
!--- Outside interface for admin context  
!--- to access the ASA from outside network  
!--- using telnet or SSH.  
  
ciscoasa(config-if)# interface Ethernet0/2  
ciscoasa(config-if)# no shutdown  
ciscoasa(config-if)# vlan 6  
  
!--- Inside interface for admin context  
!--- to access the ASA from inside network  
!--- using telnet or SSH.  
  
ciscoasa(config-if)# interface Ethernet0/3  
ciscoasa(config-if)# no shutdown  
ciscoasa(config-if)# vlan 7  
  
!--- Context1 outside subinterface  
  
ciscoasa(config-subif)# interface Ethernet0/0.1  
ciscoasa(config-subif)# vlan 2
```

```

!--- !--- Context1 inside subinterface

ciscoasa(config-subif)# interface ethernet 0/1.1
ciscoasa(config-subif)# vlan 3

!--- !--- Context2 outside subinterface

ciscoasa(config-subif)# interface ethernet 0/0.2
ciscoasa(config-subif)# vlan 4

!--- !--- Context2 inside subinterface

ciscoasa(config-subif)# interface ethernet 0/1.2
ciscoasa(config-subif)# vlan 5

!--- Customer A Context as Context1

ciscoasa(config)# context context1
Creating context 'context1'... Done. (3)
ciscoasa(config-ctx)# allocate-interface
    Ethernet0/0.1 outside-context1
ciscoasa(config-ctx)# allocate-interface
    Ethernet0/1.1 inside-context1

!--- To specify the interfaces
!--- used for the context1

ciscoasa(config-ctx)# config-url disk0:/context1.cfg

!--- To identify the URL from which the
!--- system downloads the context configuration.

ciscoasa(config-ctx)# exit

!--- Customer B Context as Context2

ciscoasa(config)# context context2
Creating context 'context2'... Done. (3)
ciscoasa(config-ctx)# allocate-interface
    Ethernet0/0.2 outside-context2
ciscoasa(config-ctx)# allocate-interface
    Ethernet0/1.2 inside-context2
ciscoasa(config-ctx)# config-url
    disk0:/context2.cfg

ciscoasa(config)# context admin
ciscoasa(config-ctx)# allocate-interface Ethernet0/2 outside
ciscoasa(config-ctx)# allocate-interface Ethernet0/3 inside

```

ASA 8.x – System Execution Space Configuration

ASA 8.x – System Execution Space Configuration

```

ciscoasa# sh run

ASA Version 8.0(2) <system>
!
hostname ciscoasa

```

```
enable password 8Ry2YjIyt7RRXU24 encrypted
mac-address auto
!
interface Ethernet0/0
!
interface Ethernet0/0.1
  vlan 2
!
interface Ethernet0/0.2
  vlan 4
!
interface Ethernet0/1
!
interface Ethernet0/1.1
  vlan 3
!
interface Ethernet0/1.2
  vlan 5
!
interface Ethernet0/2
!
interface Ethernet0/3
!
interface Management0/0
  shutdown
!
class default
  limit-resource All 0
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
!

ftp mode passive
pager lines 24
no failover
no asdm history enable
arp timeout 14400
console timeout 0

admin-context admin
context admin
  allocate-interface Ethernet0/2 outside
  allocate-interface Ethernet0/3 inside
  config-url disk0:/admin.cfg
!

context context1
  allocate-interface Ethernet0/0.1 outside-context1
  allocate-interface Ethernet0/1.1 inside-context1
  config-url disk0:/context1.cfg
!

context context2
  allocate-interface Ethernet0/0.2 outside-context2
  allocate-interface Ethernet0/1.2 inside-context2
  config-url disk0:/context2.cfg
!

prompt hostname context
Cryptochecksum:9e8bc648b240917631fa5716a007458f
: end
```

Change Between Contexts and the System Execution Space

If you log in to the system execution space (or the admin context with Telnet or SSH), you can change between contexts, as well as perform configuration and monitoring tasks within each context. The running configuration that you edit in a configuration mode, or that is used in the copy or write commands, depends on your location. When you are in the system execution space, the running configuration consists only of the system configuration; when you are in a context, the running configuration consists only of that context. For example, you cannot view all running configurations (system plus all contexts) when you enter the **show running-config** command. Only the current configuration displays.

In order to change between the system execution space and a context, or between contexts, see these commands:

- In order to change to a context, enter this command:

```
hostname# changeto context <context name>
```

The prompt changes to this:

```
hostname/name#
```

- In order to change to the system execution space, enter this command

```
hostname/admin# changeto system
```

The prompt changes to this:

```
hostname#
```

ASA – Context1 Configuration

In order to configure the context1, change to the context1 and follow the procedure:

```
!--- From the system execution space,  
!--- enter the command  
!--- "changeto context context1  
!--- to configure the context1 configuration"  
  
ciscoasa(config)# changeto context context1  
ciscoasa/context1(config)#
```

ASA 8.x – Context1 Default Configuration

```
ciscoasa/context1(config)# show run  
  
!--- Default configuration of the context1  
  
ASA Version 8.0(2) <context>  
!  
hostname context1  
enable password 8Ry2YjIyt7RRXU24 encrypted  
names  
!  
interface outside-context1  
no nameif  
no security-level
```

```

no ip address
!
interface inside-context1
no nameif
no security-level
no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
pager lines 24
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400
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
no crypto isakmp nat-traversal
telnet timeout 5
ssh timeout 5
!
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
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
Cryptochecksum:000000000000000000000000000000000000
: end

```

Customer A Configuration for Internet connectivity.

ASA 8.x – Configuration of Context1

!--- Configuring Context1 for customer A

```

ciscoasa/context1# conf t
ciscoasa/context1(config)# int outside-context1
ciscoasa/context1(config-if)# ip add 10.1.1.1 255.255.255.0

```

```

ciscoasa/context1(config-if)# no shutdown
ciscoasa/context1(config-if)# nameif outside
INFO: Security level for "outside" set to 0 by default.

ciscoasa/context1(config-if)# int inside-context1
ciscoasa/context1(config-if)# ip add 172.16.1.1 255.255.255.0
ciscoasa/context1(config-if)# no shutdown
ciscoasa/context1(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ciscoasa/context1(config-if)# exit

ciscoasa/context1(config)# access-list outbound permit ip any any
ciscoasa/context1(config)# nat (inside-context1) 1 access-list outbound
ciscoasa/context1(config)# global (outside-context1) 1 interface
INFO: outside interface address added to PAT pool
ciscoasa/context1(config)# route outside-context1 0.0.0.0 0.0.0.0 10.1.1.2
ciscoasa/context1(config)# exit

```

ASA 8.x – Context1 Configuration

```

ciscoasa/context1(config)# show run

ciscoasa/context1# sh run
: Saved
:
ASA Version 8.0(2) <context>
!
hostname context1
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface outside-context1
 nameif outside
 security-level 0
 ip address 10.1.1.1 255.255.255.0
!
interface inside-context1
 nameif inside
 security-level 100
 ip address 172.16.1.1 255.255.255.0
!
passwd 2KFQnbNIdI.2KYOU encrypted
access-list outbound extended permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400

global (outside-context1) 1 interface
nat (inside-context1) 1 access-list outbound
route outside-context1 0.0.0.0 0.0.0.0 10.1.1.2 1

!--- Output Suppressed

!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
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
Cryptochecksum:00000000000000000000000000000000
: end
ciscoasa/context1#

```

ASA – Context2 Configuration

Customer B Configuration for Internet connectivity.

In order to configure the context2, change to context2 from context1:

```

!--- From the system execution space, enter the command
!--- "changeto context context2
--to configure the context2 configuration"

ciscoasa/context1(config)# changeto context context2
ciscoasa/context2(config)#

```

ASA 8.x – Context2 Configuration

```

ciscoasa/context2(config)# show run
ASA Version 8.0(2) <context>
!
hostname context2
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface inside-context2
 nameif inside
 security-level 100
 ip address 172.17.1.1 255.255.255.0
!
interface outside-context2
 nameif outside
 security-level 0
 ip address 10.2.2.1 255.255.255.0
!
!--- Output Suppressed

!
access-list outbound extended permit ip any any
pager lines 24
mtu outside 1500
mtu inside 1500
icmp unreachable rate-limit 1 burst-size 1
no asdm history enable
arp timeout 14400

```

```

global (outside-context2) 1 interface
nat (inside-context2) 1 access-list outbound
route outside-context2 0.0.0.0 0.0.0.0 10.2.2.2 1

!--- Output Suppressed

!
!
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum 512
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
Cryptochecksum:000000000000000000000000000000000000
: end

```

Similarly configure the admin context to administrate the ASA and its contexts from the inside and outside interface.

Save Configuration Changes in Multiple Context Mode

You can save each context (and system) configuration separately, or you can save all context configurations at the same time. This section includes these topics:

Save Each Context and System Separately

In order to save the system or context configuration, enter this command within the system or context:

```
hostname# write memory
```

Note: The copy running-config startup-config command is equivalent to the write memory command.

For multiple context mode, context startup configurations can reside on external servers. In this case, the security appliance saves the configuration back to the server that you identified in the context URL, except for an HTTP or HTTPS URL, which does not let you save the configuration to the server.

Save All Context Configurations at the Same Time

In order to save all context configurations at the same time, as well as the system configuration, enter this command in the system execution space:

```
hostname# write memory all [/noconfirm]
```

If you do not enter the /noconfirm keyword, you see this prompt:

```
Are you sure [Y/N]:
```

Verify

Use this section to confirm that your configuration works properly.

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

- **show flash** Verify that the context configuration file is stored in flash.
- **show mode** Verify that the ASA is configured as a single or multiple mode.

```
ciscoasa# sh flash
--#--  --length--  -----date/time-----  path
 71  14524416    Jul 23 2007 23:11:22  asa802-k8.bin
 75  6889764     Jul 23 2007 23:32:16  asdm-602.bin
  2   4096       Jul 23 2007 23:51:36  log
  6   4096       Jul 23 2007 23:51:48  crypto_archive
 76  2635734     Aug 12 2007 22:44:50  anyconnect-win-2.0.0343-k9.pkg
 77   1841      Sep 20 2007 04:21:38  old_running.cfg
 78   1220      Sep 20 2007 04:21:38  admin.cfg
```

```
ciscoasa/context2# sh mode
Security context mode: multiple
```

Troubleshoot

Restore Single Context Mode

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

In order to copy the old running configuration to the startup configuration and to change the mode to single mode, perform these steps in the system execution space:

1. In order to copy the backup version of your original running configuration to the current startup configuration, enter this command in the system execution space:

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

2. In order to set the mode to single mode, enter this command in the system execution space:

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

The security appliance reboots.

Assign the Same IP Address to the Shared Interfaces in the Multiple Context Mode

You can assign the same IP address to shared interfaces in a different context. Although this is possible, a separate MAC address must be assigned for this interface in each context in order to classify the traffic into the context as shown.

Note: If the admin does not wish to assign the MAC address with the manual method, you can use the command `mac-address auto`. This command assigns the MAC address automatically to all interfaces, inclusive of subinterfaces.

```
<system context configuration>
interface Ethernet0
!
interface Ethernet0.1
  vlan 2
!
interface Ethernet0.2
  vlan 3
!

<context1 configuration>
!
interface Ethernet0.1
mac-address 0000.0707.0000

!--- MAC address must be unique

nameif inside
  security-level 100
  ip address 192.168.0.1 255.255.255.0
!

<context2 configuration>
!
interface Ethernet0.2
mac-address 0000.0808.0000

!--- MAC address must be unique

nameif inside
  security-level 100
  ip address 192.168.0.1 255.255.255.0
!
```

Rename the Context

In multiple context mode, to rename a context without changing the configuration is not supported.

You can save the configuration as a firewall configuration, but you need to copy the entire configuration to a new context name and delete the old context configuration.

Delete Context

From the system space, issue this command to delete the context:

```
no context contA
```

Also make sure to remove the correspondent configuration file for the context.

```
dir disk:
```

```
delete disk:/contA.cfg
```

NetPro Discussion Forums – Featured Conversations

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [Cisco ASA 5500 Series Security Appliances](#)
- [Cisco PIX 500 Series Security Appliances](#)
- [PIX/ASA – Adding and Managing Security Contexts](#)
- [PIX/ASA – Classifies Packets in Security Contexts](#)
- [Technical Support & Documentation – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Feb 20, 2009

Document ID: 99131
