ASA 8.3(x): Connect Three Internal Networks with Internet Configuration Example

Contents

Introduction

This document provides information on how to set up the Cisco Adaptive Security Appliance (ASA) with version 8.3(1) for use with three internal networks. Static routes are used on the routers for simplicity.

Refer to [PIX/ASA : Connecting Three Internal Networks with Internet Configuration Example](#) for the same configuration on Cisco Adaptive Security Appliance (ASA) with versions 8.2 and earlier.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco Adaptive Security Appliance (ASA) with version 8.3(1).

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact

of any command before using it.

Conventions

Refer to Cisco Technical Tips Conventions for more information about document conventions.
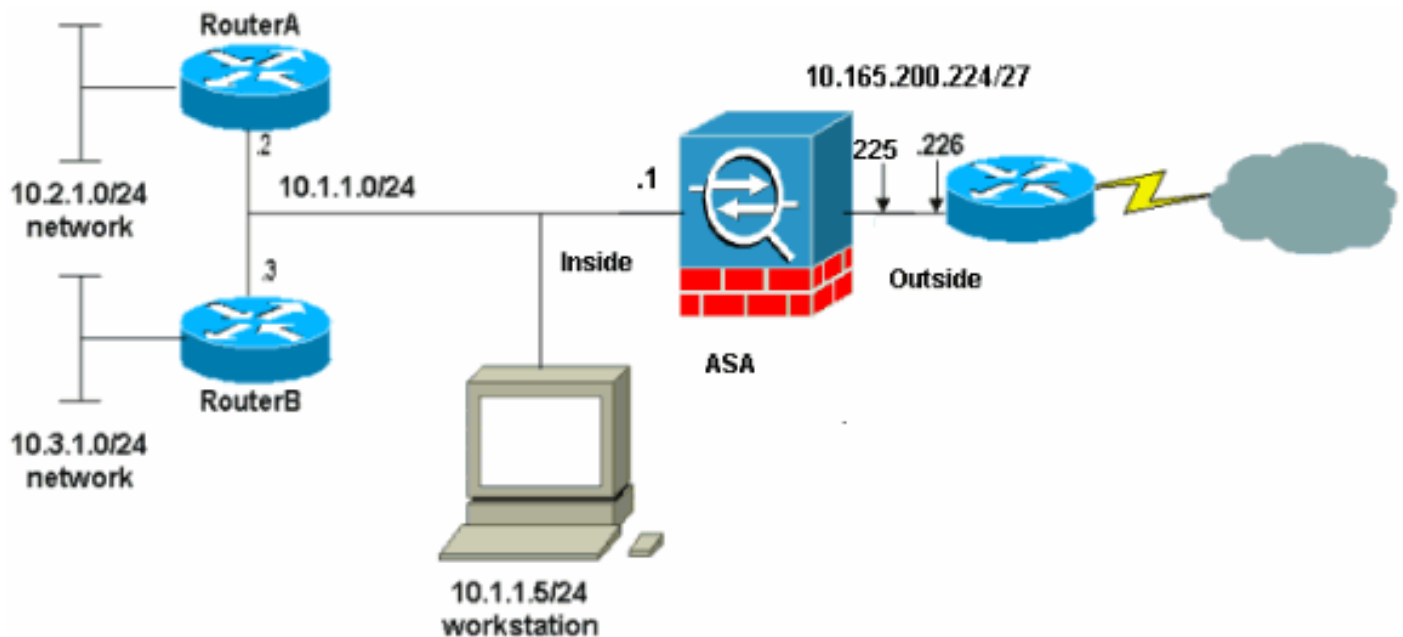
Configure

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

Note: To find additional information on the commands used in this document, use the Command Lookup Tool (registered customers only) .

Network Diagram

This document uses this network setup.

Note: The default gateway of the hosts on the 10.1.1.0 network points to RouterA. A default route on RouterB is added that points to RouterA. RouterA has a default route that points to the ASA inside interface.

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

ASA 8.3 Configuration

This document uses these configurations.

If you have the output of a **write terminal** command from your Cisco device, you can use Output Interpreter (registered customers only) to display potential issues and fixes.

- RouterA Configuration

RouterA Configuration

```
RouterA#show running-config Building configuration...
Current configuration : 1151 bytes ! version 12.4
service timestamps debug uptime service timestamps log
uptime no service password-encryption ! hostname RouterA
! boot-start-marker boot-end-marker ! enable password
cisco ! memory-size iomem 25 no network-clock-
participate slot 1 no network-clock-participate wic 0 no
network-clock-participate wic 1 no network-clock-
participate wic 2 no network-clock-participate aim 0 no
network-clock-participate aim 1 no aaa new-model ip
subnet-zero ip cef ! ! ! ! ip audit po max-events 100 no
ftp-server write-enable ! ! ! ! ! no crypto isakmp
enable ! ! ! interface FastEthernet0/0 ip address
10.1.1.2 255.255.255.0 duplex auto speed auto !
interface FastEthernet0/1 ip address 10.2.1.1
255.255.255.0 duplex auto speed auto ! interface IDS-
Sensor1/0 no ip address shutdown hold-queue 60 out ! ip
classless ip route 0.0.0.0 0.0.0.0 10.1.1.1 ip route
10.3.1.0 255.255.255.0 10.1.1.3 no ip http server no ip
http secure-server ! ! ! ! ! control-plane ! ! ! line
con 0 line 33 no activation-character no exec transport
preferred none transport input all transport output all
line aux 0 line vty 0 4 password ww login ! ! end
RouterA#
```

RouterB Configuration

```
RouterB#show running-config Building configuration...
Current configuration : 1132 bytes ! version 12.4 no
service pad service timestamps debug uptime service
timestamps log uptime no service password-encryption !
hostname RouterB ! boot-start-marker boot-end-marker ! !
no network-clock-participate slot 1 no network-clock-
participate wic 0 no network-clock-participate wic 1 no
network-clock-participate wic 2 no network-clock-
participate aim 0 no network-clock-participate aim 1 no
aaa new-model ip subnet-zero ip cef ! ! ! ! ip audit po
max-events 100 no ip domain lookup no ftp-server write-
enable ! ! ! ! ! no crypto isakmp enable ! ! ! interface
FastEthernet0/0 ip address 10.1.1.3 255.255.255.0 duplex
auto speed auto no cdp enable ! interface
FastEthernet0/1 ip address 10.3.1.1 255.255.255.0 duplex
auto speed auto ! interface IDS-Sensor1/0 no ip address
shutdown hold-queue 60 out ! ip classless ip route
0.0.0.0 0.0.0.0 10.1.1.2 no ip http server no ip http
secure-server ! ! ! ! ! control-plane ! ! ! line con 0
stopbits 1 line 33 no activation-character no exec
transport preferred none transport input all transport
output all line aux 0 line vty 0 4 password cisco login
! ! end RouterB#
```

ASA 8.3 and Later Configuration

Note: Non-default commands are shown in **bold**.

ASA 8.3(1) Running Config

```
ASA#show run
```

```
: Saved
:
ASA Version 8.3(1)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Ethernet0
 nameif outside
 security-level 0
 ip address 10.165.200.225 255.255.255.224
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
boot system disk0:/asa831-k8.bin

ftp mode passive

!--- Output Suppressed !--- Creates an object called
OBJ_GENERIC_ALL. !--- Any host IP not already matching
another configured !--- object will get PAT to the
outside interface IP !--- on the ASA (or 10.165.200.226)
for internet bound traffic. object network
OBJ_GENERIC_ALL subnet 0.0.0.0 0.0.0.0 nat
(inside,outside) source dynamic OBJ_GENERIC_ALL
interface !--- Output Suppressed !--- Define a default
route to the ISP router. route outside 0.0.0.0 0.0.0.0
10.165.200.226 1 !--- Define a route to the INTERNAL
router with network 10.2.1.0. route inside 10.2.1.0
255.255.255.0 10.1.1.2 1 !--- Define a route to the
INTERNAL router with network 10.3.1.0. route inside
10.3.1.0 255.255.255.0 10.1.1.3 1 : end
```

Note: For more information about the configuration of NAT and PAT on ASA 8.3, refer to Information About NAT.

For more information on how to configure access lists on PIX/ASA, refer to PIX/ASA 7.x : Port Redirection (Forwarding) with nat, global, static and access-list Commands.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Note: For more information on how to troubleshoot PIX/ASA, refer to Troubleshoot Connections through the PIX and ASA.

Troubleshooting Commands

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

Note: Refer to [Important Information on Debug Commands](#) before you use **debug** commands.

- **debug icmp trace**âShows whether ICMP requests from the hosts reach the PIX. You need to add the **access-list** command to permit ICMP in your configuration in order to run this debug.
- **logging buffer debugging**âShows connections being established and denied to hosts that go through the PIX.? The information is stored in the PIX log buffer and the output can be seen using the **show log** command.

Refer to [Setting Up the PIX Syslog](#) for more information on how to set up logging.

Related Information

- **[Cisco Adaptive Security Device Manager](#)**
- **[Cisco ASA 5500 Series Adaptive Security Appliances](#)**
- **[Requests for Comments (RFCs)](#)** ↗
- **[Technical Support & Documentation - Cisco Systems](#)**