ASA 8.3(x): Connect a Single Internal Network to the Internet

Document ID: 112998

Contents

Introduction

This document describes how to set up the Cisco Adaptive Security Appliance (ASA) with version 8.3(1) for use on a single internal network.

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

Before You Begin

Prerequisites

There are no specific prerequisites 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.

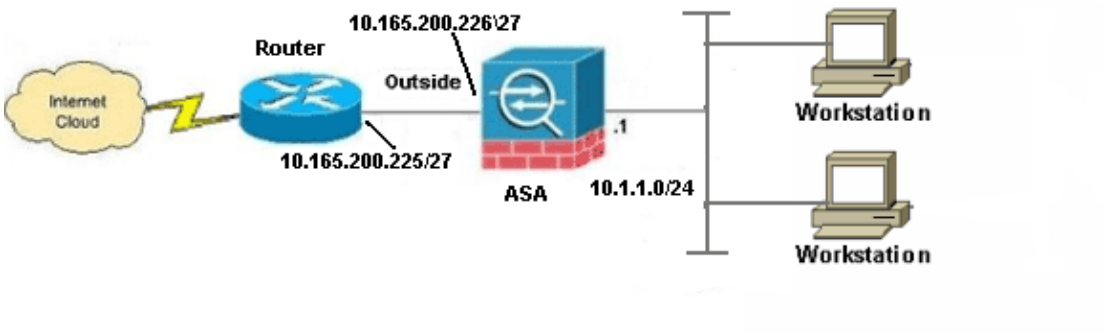
Configure

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

ASA 8.3 Configuration

This document uses these configurations:

- Router Configuration
- ASA 8.3 and Later Configuration

Router Configuration

Router Configuration
Building configuration... Current configuration: ! version 12.4 service timestamps debug uptime service timestamps log uptime no service password-encryption ! hostname R3640_out ! ! username cisco password 0 cisco ! ! ! ! ip subnet-zero ip domain-name cisco.com ! isdn voice-call-failure 0

```
!

!
interface Ethernet0/1
 ip address 10.165.200.225 255.255.255.224
 no ip directed-broadcast

!
ip classless
no ip http server
!
!
line con 0
 exec-timeout 0 0
 length 0
 transport input none
line aux 0
line vty 0 4
 password ww
 login
!
end
```

ASA 8.3 and Later Configuration

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
!

!--- Configure the outside interface.

!
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 10.165.200.226 255.255.255.224

!--- Configure the inside interface.

!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.1.1.1 255.255.255.0
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 no security-level
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 no security-level
```

```
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 no security-level
 no ip address
 management-only
!
boot system disk0:/asa831-k8.bin

ftp mode passive

!--- 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

route outside 0.0.0.0 0.0.0.0 10.165.200.225
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 sip-provisional-media 0:02:00 uauth 0:05:00 absolute
timeout tcp-proxy-reassembly 0:01:00
dynamic-access-policy-record DfltAccessPolicy
http server enable
http 192.168.0.0 255.255.254.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
crypto ipsec security-association lifetime seconds 28800
crypto ipsec security-association lifetime kilobytes 4608000
telnet timeout 5
ssh timeout 5
console timeout 0
threat-detection basic-threat
threat-detection statistics access-list
no threat-detection statistics tcp-intercept
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  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 rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
```

```
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect ip-options
!
service-policy global_policy global
prompt hostname context
Cryptochecksum:6fffbd3dc9cb863fd71c71244a0ecc5f
: end
```

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

For more information about the configuration of access lists on ASA 8.3, refer to Information About Access Lists.

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

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

Updated: May 13, 2011 Document ID: 112998