ASA 8.4(x) Connects a Single Internal Network to the Internet Configuration Example

Contents

Introduction

This document describes how to set up the Cisco Adaptive Security Appliance (ASA) with Version 8.4(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 the ASA with Versions 8.2 and earlier.

Prerequisites

Requirements

There are no specific prerequisites for this document.

Components Used

The information in this document is based on the ASA with Version 8.4(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.

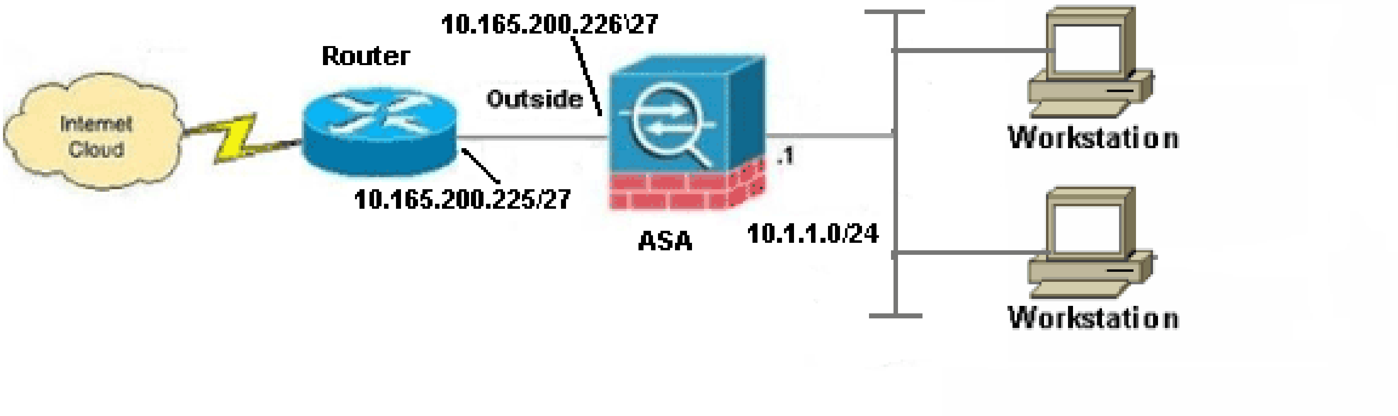
Configure

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

> **Note**: In order 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 8.4 Configuration

This document uses these configurations:

- Router Configuration
- ASA 8.4 and Later 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 8.4 and Later Configuration

```
ASA#show run
: Saved
:
ASA Version 8.4(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:/asa841-k8.bin

ftp mode passive
!
!--- Creates an object called OBJ_GENERIC_ALL.
!--- Any host IP not already matching another configured
!--- NAT rule will Port Address Translate (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 Network Address Translation (NAT) and Port Address Translation (PAT) on ASA Version 8.4, refer to Information About NAT.
>
> For more information about the configuration of access lists on ASA Version 8.4, refer to Information About Access Lists.

Verify

Try to access a web site via HTTP with a web browser. This example uses a site that is hosted at 198.51.100.100. If the connection is successful, this output can be seen on the ASA CLI:

Connection

```
ASA(config)# show connection address 10.1.1.154
6 in use, 98 most used
TCP outside 198.51.100.100:80 inside 10.1.1.154:58799, idle 0:00:06, bytes 937,
flags UIO
```

The ASA is a stateful firewall, and return traffic from the web server is allowed back through the firewall because it matches a ***connection*** in the firewall connection table. Traffic that matches a connection that preexists is allowed through the firewall without being blocked by an interface ACL.

In the previous output, the client on the inside interface has established a connection to the 198.51.100.100 host off of the outside interface. This connection is made with the TCP protocol and has been idle for six seconds. The connection flags indicate the current state of this connection. More information about connection flags can be found in ASA TCP Connection Flags.

Syslog

```
ASA(config)# show log | in 10.1.1.154

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
10.1.1.154/58799 to outside:10.165.200.226/58799

Apr 27 2014 11:31:23: %ASA-6-302013: Built outbound TCP connection 2921 for outside:
198.51.100.100/80 (198.51.100.100/80) to inside:10.1.1.154/58799 (10.165.200.226/58799)
```

The ASA Firewall generates syslogs during normal operation. The syslogs range in verbosity based on the logging configuration. The output shows two syslogs that are seen at level six, or **'informational'** level.

In this example, there are two syslogs generated. The first is a log message that indicates that the firewall has built a **translation**, specifically a dynamic TCP translation (PAT). It indicates the source IP address and port and the translated IP address and port as the traffic traverses from the inside to the outside interfaces.

The second syslog indicates that the firewall has built a **connection** in its connection table for this specific traffic between the client and server. If the firewall was configured in order to block this connection attempt, or some other factor inhibited the creation of this connection (resource constraints or a possible misconfiguration), the firewall would not generate a log that indicates that the connection was built. Instead it would log a reason for the connection to be denied or an indication about what factor inhibited the connection from being created.

NAT Translations (Xlate)

```
ASA(config)# show xlate local 10.1.1.154
3 in use, 80 most used
Flags: D - DNS, e - extended, I - identity, i - dynamic, r - portmap,
s - static, T - twice, N - net-to-net
TCP PAT from inside:10.1.1.154/58799 to outside:10.165.200.226/58799 flags ri idle
0:02:42 timeout 0:00:30
```

As part of this configuration, PAT is configured in order to translate the internal host IP addresses to addresses that are routable on the Internet. In order to confirm that these translations are created, you can check the xlate (translation) table. The command **show xlate,** when combined with the **local** keyword and the internal host's IP address, shows all of the entries present in the translation table for that host. The previous output shows that there is a translation currently built for this host between the inside and outside interfaces. The inside host IP and port are translated to the 10.165.200.226 address per our configuration. The flags listed, r i , indicate that the translation is **dynamic** and a **portmap**. More information about different NAT configurations can be found here: Information About NAT.

Troubleshoot

The ASA provides multiple tools with which to troubleshoot connectivity. If the issue persists after you verify the configuration and check the output listed previously, these tools and techniques might help determine the cause of your connectivity failure.

Packet-Tracer

```
ASA(config)# packet-tracer input inside tcp 10.1.1.154 1234 198.51.100.100 80


--Omitted--

Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: allow
```

The **packet tracer** functionality on the ASA allows you to specify a *simulated* packet and see all of the various steps, checks, and functions that the firewall goes through when it processes traffic. With this tool, it is helpful to identify an example of traffic you believe *should* be allowed to pass through the firewall, and use that 5-tupple in order to simulate traffic. In the previous example, the packet tracer is used in order to simulate a connection attempt that meets these criteria:

- The simulated packet arrives on the **inside**.
- The protocol used is **TCP**.
- The simulated client IP address is **10.1.1.154**.
- The client sends traffic sourced from port **1234**.
- The traffic is destined to a server at IP address **198.51.100.100**.
- The traffic is destined to port **80**.

Notice that there was no mention of the interface **outside** in the command. This is by packet tracer design. The tool tells you how the firewall processes that type of connection attempt, which includes how it would route it, and out of which interface. More information about packet tracer can be found in Tracing packets with Packet Tracer.

Capture

```
ASA# capture capin interface inside match tcp host 10.1.1.154 host 198.51.100.100
ASA# capture capout interface outside match tcp any host 198.51.100.100

ASA#   show capture capin

3 packets captured

  1: 11:31:23.432655       10.1.1.154.58799 > 198.51.100.100.80: S 780523448:
780523448(0) win 8192 <mss 1460,nop,wscale 2,nop,nop,sackOK>
  2: 11:31:23.712518       198.51.100.100.80 > 10.1.1.154.58799: S 2123396067:
2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712884       10.1.1.154.58799 > 198.51.100.100.80: . ack 2123396068
win 32768



ASA# show capture capout
```

```
3 packets captured

  1: 11:31:23.432869       10.165.200.226.58799 > 198.51.100.100.80: S 1633080465:
1633080465(0) win 8192 <mss 1380,nop,wscale 2,nop,nop,sackOK>
  2: 11:31:23.712472       198.51.100.100.80 > 10.165.200.226.58799: S 95714629:
95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
  3: 11:31:23.712914       10.165.200.226.58799 > 198.51.100.100.80: . ack 95714630
win 32768/pre>
```

The ASA firewall can capture traffic that enters or leaves its interfaces. This capture functionality is fantastic because it can definitively prove if traffic arrives at, or leaves from, a firewall. The previous example showed the configuration of two captures named **capin** and **capout** on the inside and outside interfaces respectively. The capture commands used the **match** keyword, which allows you to be specific about what traffic you want to capture.

For the capture **capin,** you indicated that you wanted to match traffic seen on the inside interface (ingress or egress) that matches **tcp host 10.1.1.154 host 198.51.100.100**. In other words, you want to capture any TCP traffic that is sent from **host 10.1.1.154** to **host 198.51.100.100** or **vice versa**. The use of the **match** keyword allows the firewall to capture that traffic bidirectionally. The capture command defined for the outside interface does not reference the internal client IP address because the firewall conducts PAT on that client IP address. As a result, you cannot **match** with that client IP address. Instead, this example uses **any** in order to indicate that all possible IP addresses would match that condition.

After you configure the captures, you would then attempt the establish a connection again, and proceed to view the captures with the **show capture <*capture_name*>** command. In this example, you can see that the client was able to connect to the server as evident by the TCP 3-Way handshake seen in the captures.

Related Information

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