Configure the ASA for Dual Internal Networks

TAC **Document ID: 119195**

Contributed by Dinkar Sharma, Bratin Saha, and Prashant Joshi, Cisco
TAC Engineers.

Aug 05, 2015

Contents

Introduction

This document describes how to configure a Cisco Adaptive Security Appliance (ASA) that runs software Version 9.x for the use of two internal networks.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco ASA that runs software Version 9.x.

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.

Conventions

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

Background Information

When you add a second internal network behind an ASA firewall, consider this important information:

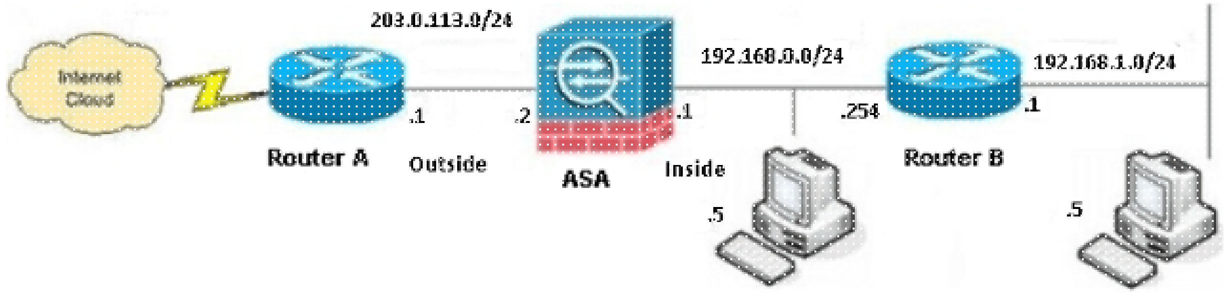
- The ASA does not support secondary addressing.
- A router must be used behind the ASA in order to achieve routing between the current network and the newly added network.
- The default gateway for all of the hosts must point to the inside router.
- You must add a default route on the inside router that points to the ASA.
- You must clear the Address Resolution Protocol (ARP) cache on the inside router.

Configure

Use the information that is described in this section in order to configure the ASA.

Network Diagram

Here is the topology that is used for the examples throughout this document:



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

ASA 9.x Configuration

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

Here is the configuration for the ASA that runs software Version 9.x:

```
ASA Version 9.3(2)
!
hostname ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
```

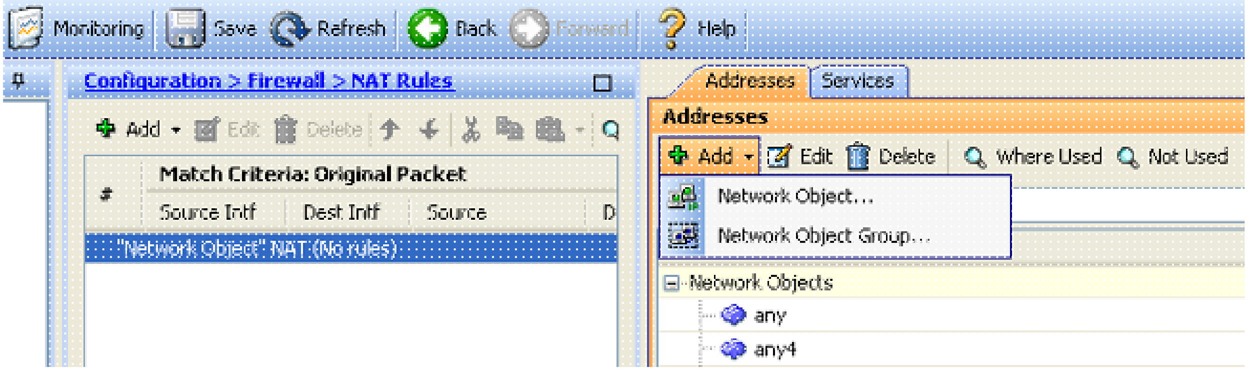
```
!--- This is the configuration for the outside interface.

!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0

!--- This is the configuration for the inside interface.

!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.0.1 255.255.255.0
!

boot system disk0:/asa932-smp-k8.bin

!--- This creates an object called OBJ_GENERIC_ALL.
!--- Any host IP address that does not already match another configured
!--- object will get PAT to the outside interface IP address
!--- on the ASA (or 10.1.5.1), for Internet-bound traffic.


object network OBJ_GENERIC_ALL
subnet 0.0.0.0 0.0.0.0
nat (inside,outside) dynamic interface
!
route inside 192.168.1.0 255.255.255.0 192.168.0.254 1
route outside 0.0.0.0 0.0.0.0 203.0.113.1
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
```

Allow Inside Hosts Access to Outside Networks with PAT

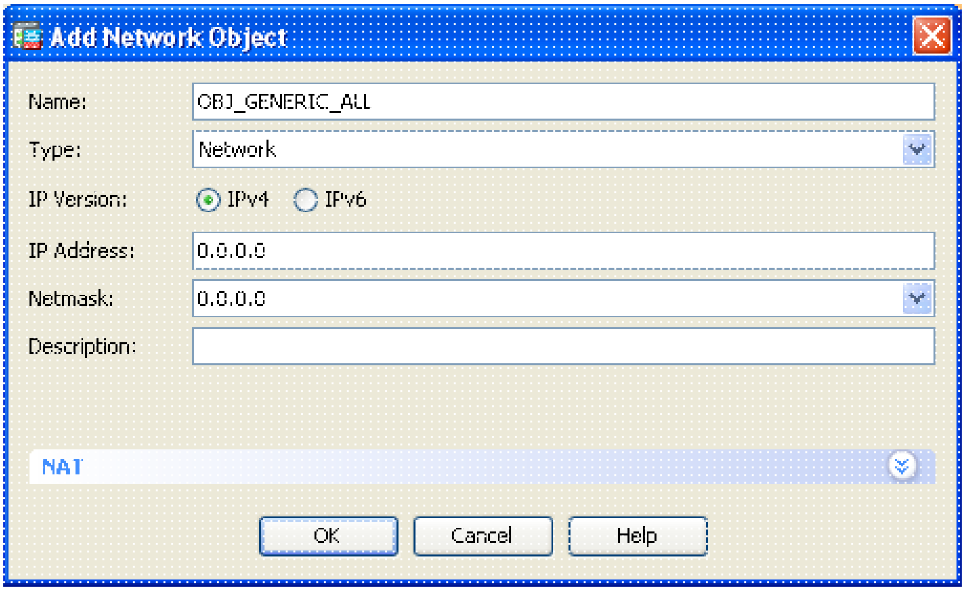
If you intend to have the inside hosts share a single public address for translation, use Port Address Translation (PAT). One of the simplest PAT configurations involves the translation of all internal hosts so that they appear to be the outside interface IP. This is the typical PAT configuration that is used when the number of routable IP addresses that are available from the ISP is limited to only a few, or just one.

Complete these steps in order to allow the inside hosts access to the outside networks with PAT:

1. Navigate to **Configuration > Firewall > NAT Rules**, click **Add**, and choose **Network Object** in order to configure a dynamic NAT rule:



2. Configure the network/Host/Range for which the Dynamic PAT is required. In this example, all inside subnets have been selected. This process should be repeated for the specific subnets that you wish to translate in this manner:



Add Network Object

Name: OBJ_GENERIC_ALL

Type: Network

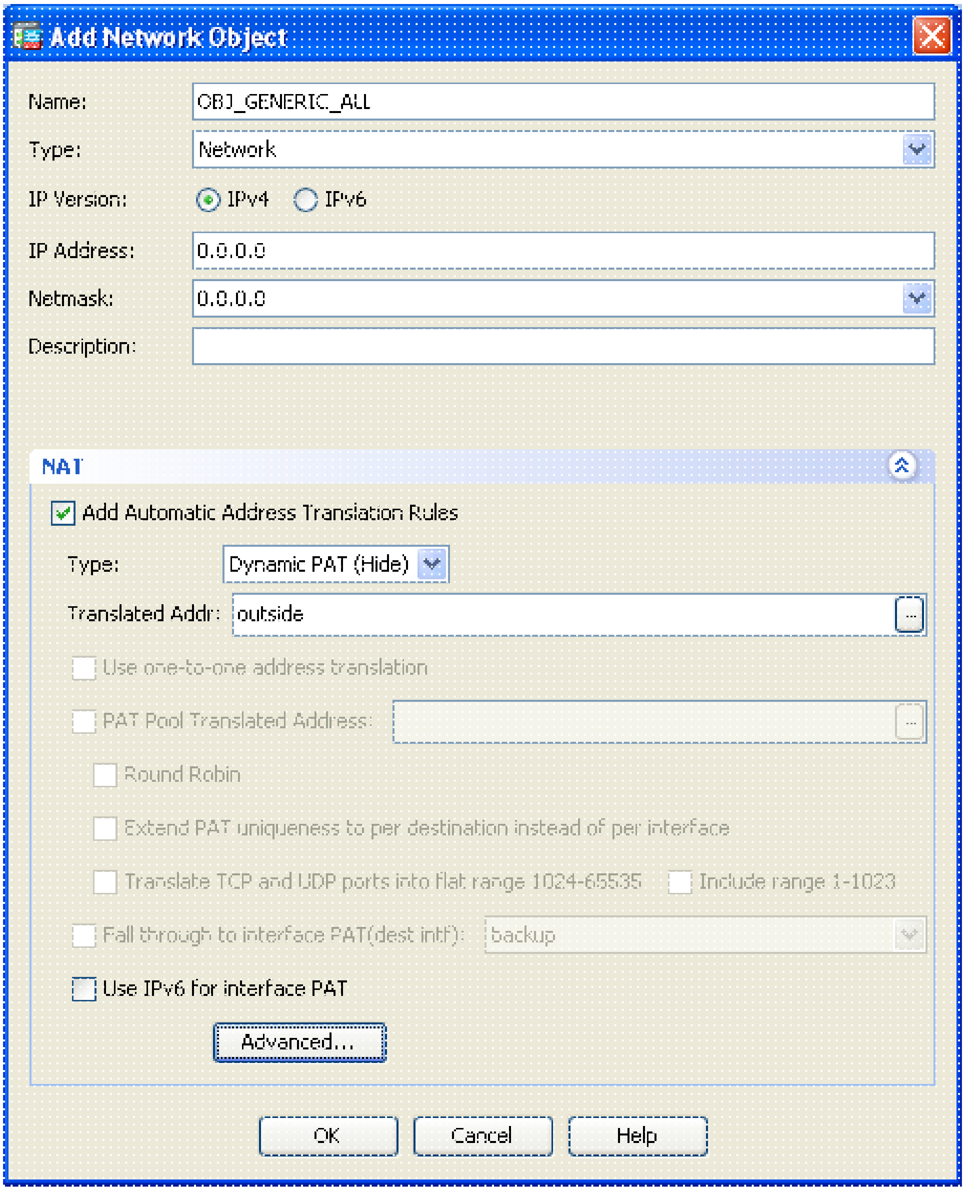
IP Version: ● IPv4 ○ IPv6

IP Address: 0.0.0.0

Netmask: 0.0.0.0

Description:

3. Click **NAT**, check the **Add Automatic Address Translation Rule** check box, enter **Dynamic,** and set the **Translated Addr** option so that it reflects the outside interface. If you click the ellipsis button, it assists you to pick a pre-configured object, such as the outside interface:



Add Network Object

Name: OBJ_GENERIC_ALL

Type: Network

IP Version: ● IPv4 ○ IPv6

IP Address: 0.0.0.0

Netmask: 0.0.0.0

Description:

NAT

☑ Add Automatic Address Translation Rules

Type: Dynamic PAT (Hide)

Translated Addr: outside

□ Use one-to-one address translation

□ PAT Pool Translated Address:

□ Round Robin

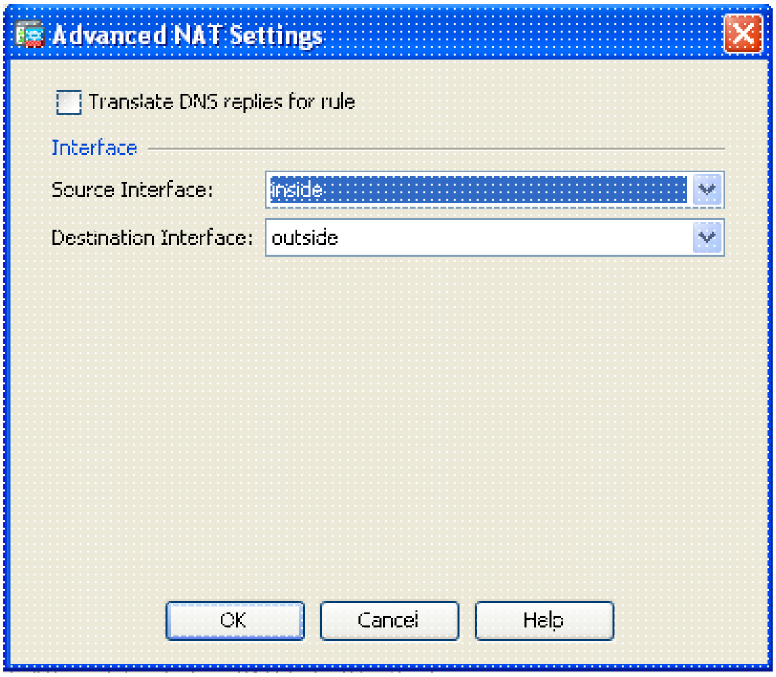
□ Extend PAT uniqueness to per destination instead of per interface

□ Translate TCP and UDP ports into flat range 1024-65535 □ Include range 1-1023

□ Fall through to interface PAT(dest intf): backup

□ Use IPv6 for interface PAT

4. Click **Advanced** in order to select a source and destination interface:



Advanced NAT Settings

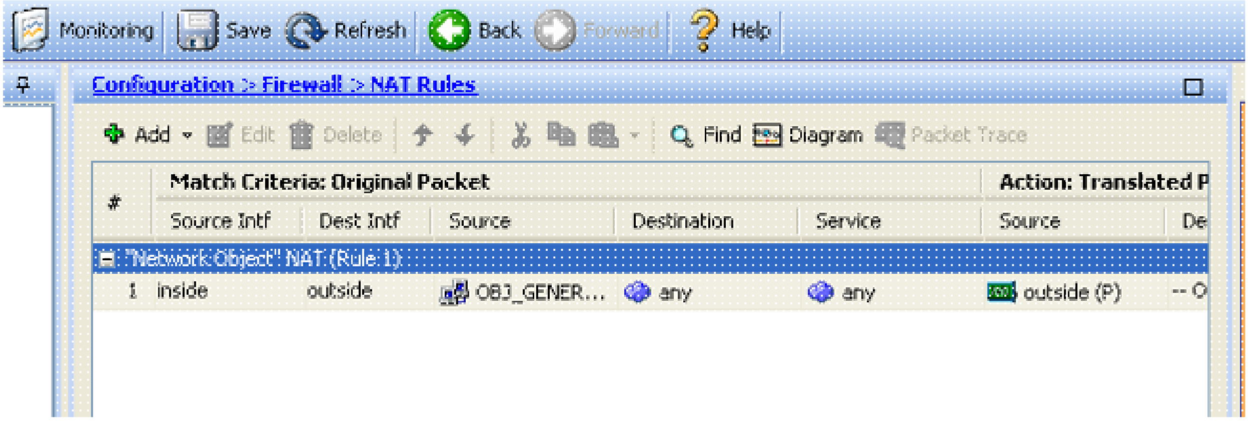
☐ Translate DNS replies for rule

Interface

Source Interface: inside

Destination Interface: outside

5. Click **OK**, and then click **Apply** in order to apply the changes. Once complete, the Adaptive Security Device Manager (ASDM) shows the NAT rule:



Configuration > Firewall > NAT Rules

#	Match Criteria: Original Packet					Action: Translated P	
	Source Intf	Dest Intf	Source	Destination	Service	Source	De
"Network Object" NAT (Rule 1)							
1	inside	outside	OBJ_GENER...	any	any	outside (P)	-- O

Router B Configuration

Here is the configuration for Router B:

```
Building configuration...

Current configuration:
!
version 12.4
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Router B
!
!
username cisco password 0 cisco
!
!
!
!
```

```
ip subnet-zero
ip domain-name cisco.com
!
isdn voice-call-failure 0
!

!
interface Ethernet0/0
ip address 192.168.1.1 255.255.255.0
no ip directed-broadcast
!
interface Ethernet0/1

!--- This assigns an IP address to the ASA-facing Ethernet interface.

ip address 192.168.0.254 255.255.255.0
no ip directed-broadcast

ip classless

!--- This route instructs the inside router to forward all of the
!--- non-local packets to the ASA.

ip route 0.0.0.0 0.0.0.0 192.168.0.1
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
```

Verify

Access a web site via HTTP through a web browser in order to verify that your configuration works properly.

This example uses a site that is hosted at IP address *198.51.100.100*. If the connection is successful, the outputs that are provided in the sections that follow can be seen on the ASA CLI.

Connection

Enter the **show connection address** command in order to verify the connection:

```
ASA(config)# show connection address 172.16.11.5
6 in use, 98 most used
TCP outside  198.51.100.100:80 inside  192.168.1.5:58799, idle 0:00:06, bytes 937,
flags UIO
```

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

Note: Refer to the ASA TCP Connection Flags (Connection build-up and teardown) Cisco document for more information about connection flags.

Troubleshoot

Use the information that is described in this section in order to troubleshoot configuration issues.

Syslogs

Enter the **show log** command in order to view the syslogs:

```
ASA(config)# show log | in 192.168.1.5

Apr 27 2014 11:31:23: %ASA-6-305011: Built dynamic TCP translation from inside:
192.168.1.5/58799 to outside:203.0.113.2/58799

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:192.168.1.5/58799 (203.0.113.2/58799)
```

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 the *informational* level.

In this example, there are two syslogs generated. The first is a log message to indicate that the firewall has built a translation; specifically, a dynamic TCP translation (PAT). It indicates the source IP address and port, as well as 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 does not generate a log to indicate that the connection was built. Instead, it logs a reason for the connection to be denied or an indication in regards to the factor that inhibited the connection from being created.

Packet Tracers

Enter this command in order to enable the packet tracer functionality:

```
ASA(config)# packet-tracer input inside tcp 192.168.1.5 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 view all of the various steps, checks, and functions that the firewall completes when it processes the traffic. With this tool, it is helpful to identify an example of the traffic that you believe *should* be allowed to pass through the firewall, and use that 5-tupple in order to simulate the 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 interface.
- The protocol that is used is TCP.
- The simulated client IP address is 192.168.1.5.
- The client sends traffic that is 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 outside interface in the command. This is due to 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.

Tip: For more information about the packet tracer functionality, refer to the Tracing packets with Packet Tracer section of the *Cisco ASA 5500 Series Configuration Guide using the CLI, 8.4 and 8.6*.

Capture

Enter these commands in order to apply a capture:

```
ASA# capture capin interface inside match tcp host 192.168.1.5 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 192.168.1.5.58799 > 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 > 192.168.1.5.58799: S 2123396067:
   2123396067(0) ack 780523449 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
   3: 11:31:23.712884 192.168.1.5.58799 > 198.51.100.100.80: . ack 2123396068
   win 32768

ASA#show capture capout

3 packets captured

   1: 11:31:23.432869 203.0.113.2.58799 > 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 > 203.0.113.2.58799: S 95714629:
   95714629(0) ack 1633080466 win 8192 <mss 1024,nop,nop,sackOK,nop,wscale 8>
   3: 11:31:23.712914 203.0.113.2.58799 > 198.51.100.100.80: . ack 95714630
   win 32768/pre>
```

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

For the *capin* capture example, it is indicated that you want to match the traffic that is seen on the inside interface (ingress or egress) that matches *tcp host 192.168.1.5 host 198.51.100.100*. In other words, you want to capture any TCP traffic that is sent from host *192.168.1.5* 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 that is 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 can then attempt to 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 is able to connect to the server, as evident by the TCP 3-way handshake that is seen in the captures.

Related Information

- **Cisco Adaptive Security Device Manager**
- **Cisco ASA 5500-X Series Next-Generation Firewalls**
- **Requests for Comments (RFC)**
- **Cisco ASA Series CLI Configuration Guide, 9.0 – Configuring Static and Default Routes**
- **Technical Support & Documentation – Cisco Systems**

Updated: Aug 05, 2015 Document ID: 119195