

Understanding the alias Command for the Cisco Secure PIX Firewall

Document ID: 6353

Note: This command functionality has been replaced by NAT, including the `nat` and `static` commands with the `dns` keyword. In order to configure DNS Doctoring with NAT, refer to [PIX/ASA: Perform DNS Doctoring with the static Command and Two NAT Interfaces Configuration Example](#) or [PIX/ASA: Perform DNS Doctoring with the static Command and Three NAT Interfaces Configuration Example](#). For additional information about NAT, refer to [nat](#) and [Using nat, global, static, conduit, and access-list Commands and Port Redirection on PIX](#).

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Translate an Internal Address with DNS Doctoring

- Network Diagram

Translate a DMZ Address with Destination NAT

- Network Diagram
- Other Configuration Notes

Related Information

Introduction

This document explains the use of the **alias** command on the Cisco Secure PIX Firewall.

The **alias** command has two functions:

- You can use the **alias** command to perform DNS Doctoring of DNS replies from an external DNS server.
 - ◆ In DNS Doctoring, the PIX changes the DNS response from a DNS server to be a different IP address than the DNS server actually answered for a given name.
 - ◆ This process is used when you want the actual application call from the internal client to connect to an internal server by its internal IP address.
- You can use this command to perform Destination NAT (dnat) of one destination IP address to another IP address.
 - ◆ In dnat, the PIX changes the destination IP of an application call from one IP address to another IP address.
 - ◆ This process is used when you want the actual application call from the internal client to the server in a perimeter (dmz) network by its external IP address. This does not "doctor" the DNS replies.

For example, if a host sends a packet to 99.99.99.99, you can use the **alias** command to redirect traffic to another address, such as 10.10.10.10. You can also use this command to prevent conflicts when

you have IP addresses on a network that are the same as those on the Internet or another intranet. Consult the PIX documentation for more information.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco Secure PIX Firewall Software Releases 5.0.x and later.

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.

Translate an Internal Address with DNS Doctoring

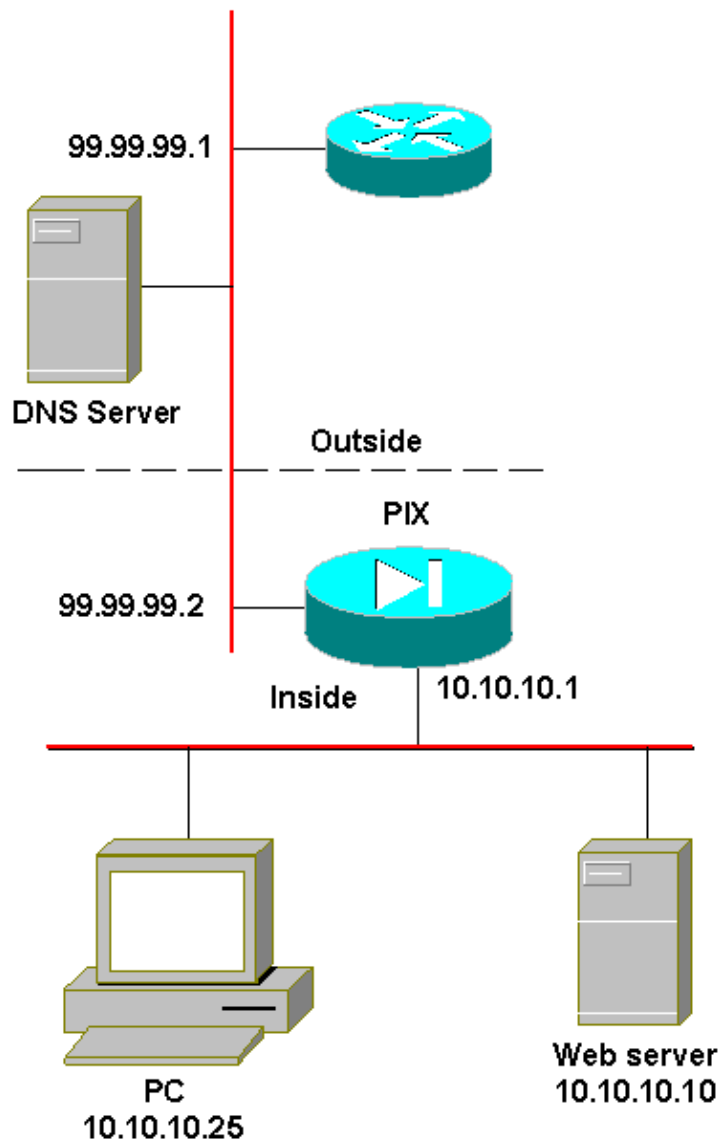
In the first example, the web server has an IP address of 10.10.10.10. The global IP address of this web server is 99.99.99.99.

Note: The DNS server is on the outside. Verify that the DNS server resolves your domain name to the global IP address of the web server by issuing an **nslookup** command. The result of the **nslookup** on the client PC is the internal IP address of the server (10.10.10.10). This is because the DNS reply gets doctored as it passes through the PIX.

Also note that in order for DNS **fixup** to work properly, **proxy-arp** has to be disabled. If you use the **alias** command for DNS **fixup**, disable **proxy-arp** with the **sysopt noproxyarp internal_interface** command after the **alias** command is executed.

Note: You cannot use DNS Doctoring while Port Redirection is in use.

Network Diagram



If you want the machine with the IP address 10.10.10.25 to access this web server by its domain name (www.mydomain.com), implement the **alias** command as this output shows:

```
alias (inside) 10.10.10.10 99.99.99.99 255.255.255.255

!--- This command sets up DNS Doctoring. It is initiated from the clients in
!--- the "inside" network. It watches for DNS replies that contain
!--- 99.99.99.99. Then it replaces the 99.99.99.99 address with the 10.10.10.10
!--- address in the "DNS reply" sent to the client PC.
```

Next, a static translation must be created for the web server. You also need to give anyone on the Internet access to the web server on port 80 (http):

```
static(inside,outside) 99.99.99.99 10.10.10.10 netmask 255.255.255.255

!--- This command creates a static translation between the web server
!--- real address of 10.10.10.10 to the global IP address 99.99.99.99.
```

In order to grant permission for access, use **access list** commands, as this output shows.

```
access-list 101 permit tcp any host 99.99.99.99 eq www
```

```
access-group 101 in interface outside
```

!--- These commands permit any outside user to access the web server on port 80.

If you prefer the older syntax, you can use a **conduit** command as this output shows.

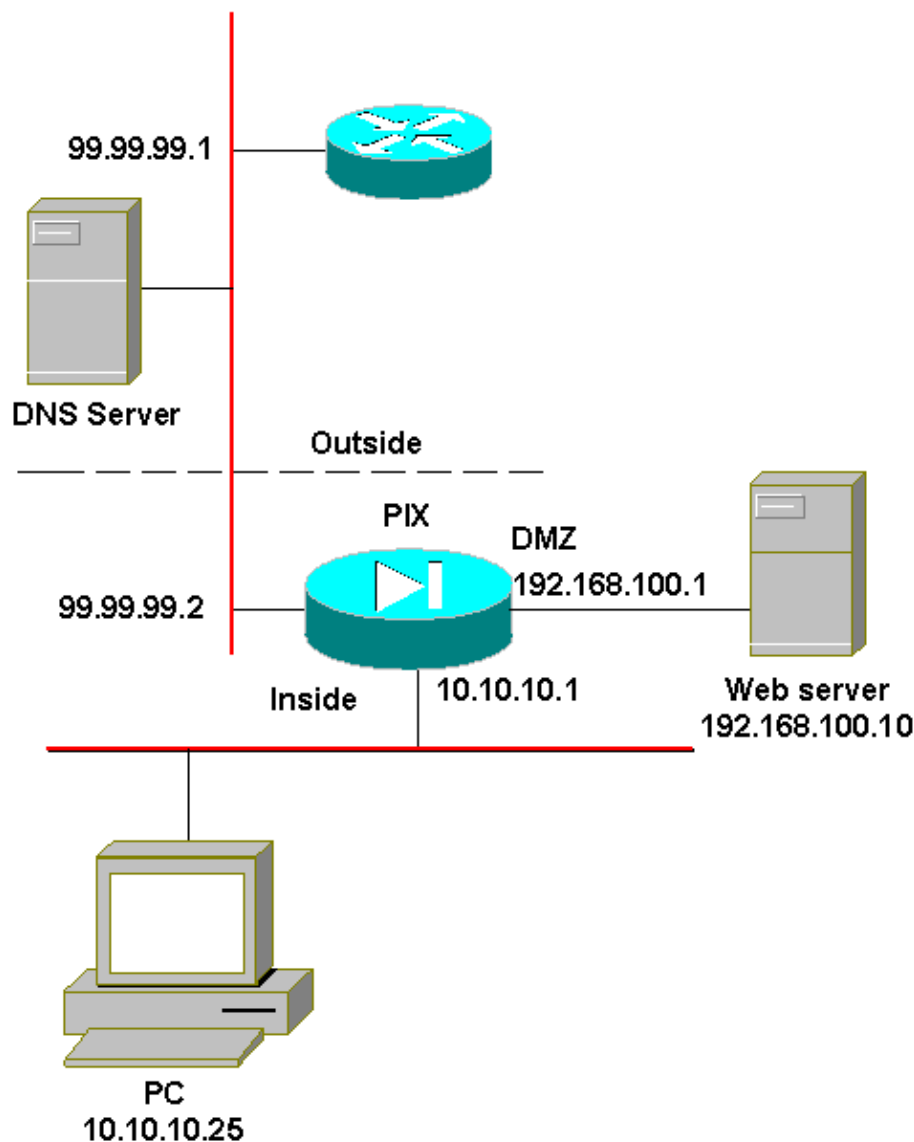
```
conduit permit tcp host 99.99.99.99 eq www any
```

!--- This command permits any outside user to access the web server on port 80.

Translate a DMZ Address with Destination NAT

If the web server is on the DMZ network of the PIX, the **alias** command must be used to do Destination NAT (dnat). In this example, the web server on the DMZ has an IP address of 192.168.100.10, and the outside IP address for this web server is 99.99.99.99. Use dnat to translate the IP address 99.99.99.99 to 192.168.100.10 on the actual call to the server. The DNS call and reply remain unchanged. In this example the DNS response seen by the internal client PC is the external 99.99.99.99 IP address, since it is not DNS doctored.

Network Diagram



In this example, the intent is for the machines in the 10.10.10.0 /24 network to access this web server in the DMZ by its external domain name (www.mydomain.com). You do not want the PIX to do DNS Doctoring of the DNS replies. Instead, you want the PIX to dnat the external (global) IP address of the web server to its "real" DMZ address (192.168.100.10).

Use the **alias** command to perform dnat:

```
alias(inside) 99.99.99.99 192.168.100.10 255.255.255.255

!--- This sets up the Destination NAT. In this example the DNS reply is not
!--- doctored by the PIX because the external address (99.99.99.99) does not
!--- match the foreign IP address in the alias command (the second IP).
!--- But the call is "dnat-ed" because the destination address
!--- in the call matches the dnat IP address in the alias command (the first IP).
```

Note: The IP addresses in the **alias** command are in reverse order compared with the example for DNS Doctoring.

Next, a static translation must be created for the web server. You also need to give anyone on the Internet access to the web server on port 80 (http):

```
static(dmz,outside) 99.99.99.99 192.168.100.10 netmask 255.255.255.255

!--- This command creates a static translation between the web server's
!--- real address 192.168.100.10 to the global IP address 99.99.99.99.
```

In order to grant permission for access, use **access list** commands, as this output shows.

```
access-list 101 permit tcp any host 99.99.99.99 eq www
access-group 101 in interface outside

!--- These commands permit any outside user to access the web server on port 80.
```

If you prefer the older syntax, you can use a **conduit** command as this output shows.

```
conduit permit tcp host 99.99.99.99 eq www any

!--- This command permits any outside user to access the web server on port 80.
```

Other Configuration Notes

- The interface in the **alias** command needs to be the "interface" that the clients call from.
- If there are also clients on the DMZ, you can add another **alias** for the DMZ interface (this one is DNS Doctoring).

For instance, assume that from the previous example that you want other clients on the DMZ to use the external DNS but to call the web server by its DMZ address. In order to do this, create an additional **alias** command, tied to the DMZ interface, in order to DNS doctor the DNS reply packets.

```
alias (dmz) 192.168.100.10 99.99.99.99 255.255.255.255

!--- This command sets up DNS Doctoring. It is initiated from the clients in
!--- the "dmz" network. It watches for DNS replies that contain
!--- 99.99.99.99, then replaces the 99.99.99.99 address with the 192.168.100.10
!--- address in the "DNS reply" sent to the client PC.
```

- You can have multiple **alias** commands tied to different interfaces on the same PIX.
-

Related Information

- [Cisco PIX 500 Series Security Appliances Support Page](#)
 - [Documentation for PIX Firewall](#)
 - [PIX Command References](#)
 - [Requests for Comments \(RFCs\)](#)
 - [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: Sep 26, 2008

Document ID: 6353
