

Testing the PIX Firewall Mailguard Feature

Document ID: 4733

Contents

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Test Mailguard

- Part 1 – No Mailguard

- Part 2 – Mailguard

How Mailguard Works

Related Information

Introduction

The PIX Software Mailguard feature sanitizes SMTP traffic. For PIX Software versions 4.0 and 4.1, the **mailhost** command is used to configure Mailguard. In PIX Software versions 4.2 and later, the command has been changed to **fixup protocol smtp 25**. The **static** and **conduit** statements are also required for your mail server.

When configured, Mailguard allows only the seven SMTP minimum–required commands as described in Section 4.5.1 of RFC 821 . These seven minimum–required commands are HELO, MAIL, RCPT, DATA, RSET, NOOP, and QUIT. Other commands, such as KILL, WIZ, and so forth, are intercepted by the PIX and they are never sent to the mail server on the inside of your network. The PIX responds with an OK even to denied commands, so attackers do not know that their attempts are being thwarted.

This can make it seem difficult to test the Mailhost feature. How do you know it is "working as advertised," when everything comes back OK?

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on PIX Software versions 4.0 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 Cisco Technical Tips Conventions for more information on document conventions.

Test Mailguard

This section describes how to test and make sure Mailguard works properly. This test was performed with PIX Software versions 4.0 and 4.1 using the **mailhost** command. In order to test versions 4.2 and later, use the **fixup protocol smtp 25** command in Part 2, along with the appropriate **static** and **conduit** statements for your mail server.

Part 1 – No Mailguard

Complete these steps:

1. Use a PIX to create a normal static and conduit for TCP 25 (SMTP) and allow all hosts in:

```
static 111.222.111.1 10.2.1.1
conduit 111.222.111.1 25 tcp 0.0.0.0 0.0.0.0
```

2. From outside the PIX, Telnet on port 25 to 111.222.111.1.

```
yourusername@generic-host% telnet 111.222.111.1 25

Trying 111.222.121.1 ?
Connected to 111.222.111.1.
Escape character is ^]?
220-mail.foobar.com Sendmail (thermonuclear mailer) 8.6.11
ready for meltdown at Tue, 17 Jun 1997 1:23:23
20 ESMTTP spoken here
```

3. If you enter **Some-fake-command**, you should receive a type-500 message from the server in return.

```
Some-fake-command

500 Command unrecognized
```

Part 2 – Mailguard

Complete these steps in order to further configure your Mailguard:

1. Configure the PIX with the **mailhost** command.

```
mailhost 111.222.111.1 10.2.1.1
```

2. Try your Telnet and fake command again.

```
yourusername@generic-host% telnet 111.222.111.1 25

Trying 111.222.121.1 ?
Connected to 111.222.111.1.
Escape character is ^]?
220-mail.foobar.com Sendmail (thermonuclear mailer) 8.6.11
ready for meltdown at Tue, 17 Jun 1997 1:25:42
220 ESMTTP spoken here

some-fake-command

OK
```

The PIX intercepts the fake command and returns OK.

How Mailguard Works

In Part 1, when the mailserv receives an invalid or unacceptable command, it generates a 500 Command unrecognized message. In Part 2, when Mailguard is configured, the PIX then intercepts the entered command, and passes only valid commands (that is, one of the seven minimum-required SMTP commands) on to the mail server behind the PIX Firewall. It then returns an OK to the user regardless of whether the command entered was passed on or denied. In this way, PIX confuses anyone that attempts an attack on the mail system. The Mailguard feature also works in versions 4.2 and later. It is activated using the **fixup protocol smtp 25** command instead of the **mailhost** command.

Note: If you have an ESMTP server behind the PIX, such as a Microsoft Exchange Server, you might need to turn off the Mailguard feature to allow mail to flow properly. Also, doing Telnet to port 25 might not work with the **fixup protocol smtp** command, especially with a Telnet client that does character mode.

Related Information

- [Documentation for PIX Firewall](#)
- [PIX Command Reference](#)
- [Cisco PIX 500 Series Security Appliances Support](#)
- [Requests for Comments \(RFCs\)](#)
- [Technical Support & Documentation – Cisco](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Sep 26, 2008

Document ID: 4733
