ESA Experiences a Bounce (NDR) Storm

Contents

Introduction

This document describes a problem encountered where your Email Security Appliance (ESA) experiences a bounce storm and offers a solution to the problem.

Background Information

A bounce storm is a side effect of a joe job or a backscatter of email spam.

Joe Job

A joe job is a spam attack that uses spoofed sender data and aims to tarnish the reputation of the apparent sender and/or induce the recipients to take action against the apparent sender.

Backscatter

A backscatter is a side effect of email spam, viruses, and worms where email servers that receive spam and other mail send bounce messages to an innocent party. This occurs because the original message envelope sender is forged in order to contain the email address of the victim. Since these messages were not solicited by the recipients, are substantially similar to each other, and are delivered in bulk quantities, they qualify as unsolicited bulk email or spam. As such, systems that generate email backscatter can become listed on various Domain Name System Blacklists (DNSBLs) and be in violation of the Internet service providers Terms of Service.

Problem

Your ESA experiences a bounce storm where there is a deluge of messages injected into the ESA. The incoming connection count spikes during such an attack. The appliance might develop a workqueue backup. In order to verify if the appliance is subject to such an attack, grep the mail logs for the mail **From** address. Bounces (Non-Delivery Reports - NDRs) have an empty envelope mail **From** address.

```
ironport.com> grep -e "From:" mail_logs
Mon Oct 20 14:40:55 2008 Info: MID 10 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 11 ICID 19 From: <>
Mon Oct 20 14:40:55 2008 Info: MID 12 ICID 19 From: <>
```

An appliance that is subject to a bounce storm will have the majority of the messages with the envelope mail **From** address of '<>'.

Solution

There are a number of options to manage a bounce storm.

Bounce Verification

In order to combat these misdirected bounce attacks, AsyncOS includes Cisco Bounce Verification. When enabled, this feature tags the Envelope Sender address for messages sent via the ESA. The Envelope Recipient for any bounce message received by the ESA is then checked for the presence of this tag. When legitimate bounce messages are received, the tag that was added to Envelope Sender address is removed and the bounce is delivered to the recipient. Bounce messages that do not contain the tag can be handled separately.

AsyncOS considers bounces as mail with a null mail **From** address (<>). Messages that are from addresses such as mailer-daemon@example.com or postmaster@example.com are not considered bounces by the system and are not subject to Bounce Verification.

Configure Bounce Verification Address Tagging Keys

The Bounce Verification Address Tagging Keys listing shows your current key and any unpurged keys you used in the past. In order to add a new key, complete these steps:

1. On the **Mail Policies** > **Bounce Verification** page, click **New Key**.
2. Enter a text string and click **Submit**.
3. Commit your changes.

Purging Keys

You can purge your old address tagging keys if you select a rule for purging from the pull-down menu and click **Purge.**

Configure Cisco Bounce Verification Settings

The bounce verification settings determine which action to take when an invalid bounce is

received.

- Choose **Mail Policies** > **Bounce Verification**.
- Click **Edit Settings**.
- Select whether to reject invalid bounces or to add a custom header to the message. If you want to add a header, enter the header name and value.
- Optionally, enable smart exceptions. This setting allows incoming mail messages and bounce messages generated by internal mail servers to be automatically exempted from bounce verification processing (even when a single listener is used for both incoming and outgoing mail).
- Submit and commit your changes.

Configure Cisco Bounce Verification with the CLI

You can use the **bvconfig** and **destconfig** commands in the CLI in order to configure bounce verification. These commands are discussed in the Cisco AsyncOS CLI Reference Guide.

Cisco Bounce Verification and Cluster Configuration

Bounce verification works in a cluster configuration as long as both Cisco appliances use the same "bounce key." When you use the same key, either system should be able to accept a legitimate bounceback. The modified header tag/key is not specific to each Cisco appliance.

Mail Filter

If you cannot use Bounce Verification because you use separate appliances for receipt and delivery, you can set up a message filter in order to block messages that have an empty mail **From** address.

Mail Block

Since these bounce messages will most likely have a nonexistent envelope recipient address, you can block invalid addresses via conversation Lightweight Directory Access Protocol (LDAP) recipient validation in order to help lower the impact of such messages.