Locate DHAP Alert Information on the ESA

Document ID: 118936

Contributed by John Yu and Robert Sherwin, Cisco TAC Engineers.
Apr 23, 2015

Contents

Introduction

This document describes how to locate information in regards to Directory Harvest Attack Prevention (DHAP) alerts on your Cisco Email Security Appliance (ESA).

Locate DHAP Occurrences from the ESA

The entries that describe the DHAP event reside in the mail logs. Here is an example mail log entry when DHAP occurs:

```
Tue Oct 18 00:25:35 2005 Warning: LDAP: Dropping connection due to potential Directory
 Harvest Attack from host=(192.168.10.1', None), dhap_limit=4, sender_group=SUSPECTLIST
```

Note: By default, the ***/24*** netmask is looked for in the search.

Enter this query into the CLI in order to view the mail logs:

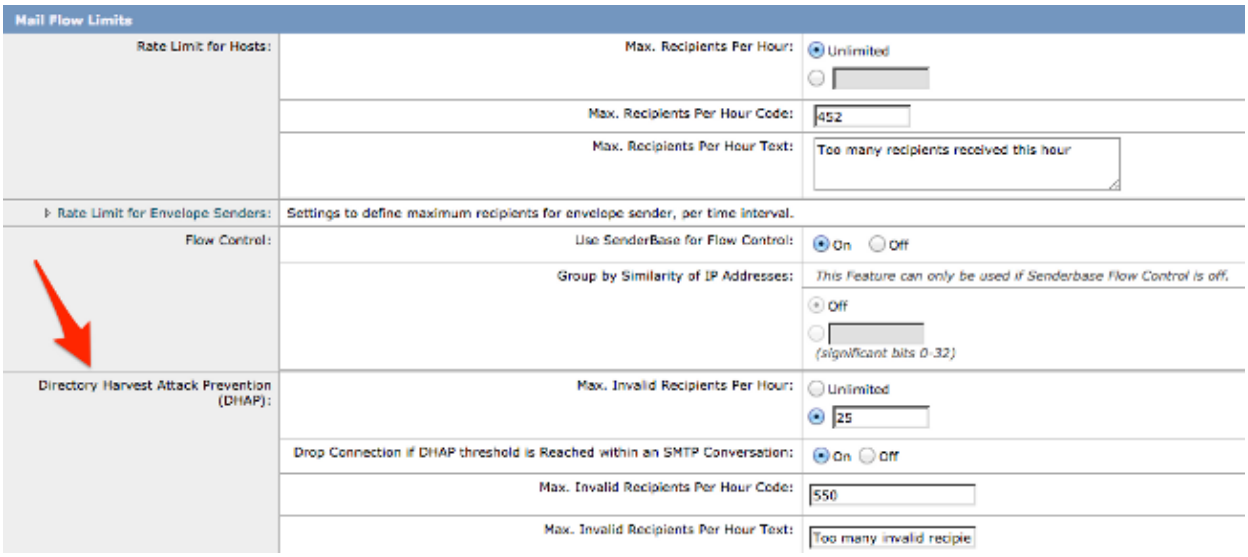
```
myesa.local> grep "dhap_limit=" mail_logs
```

The DHAP counters include both Recipient Access Table (RAT) rejections and Lightweight Directory Access Protocol (LDAP) acceptance query rejections. The DHAP settings are configured in the Mail Flow policy.

View or Update DHAP Configuration from the GUI

Complete these steps in order to view or edit your DHAP configuration parameters from the GUI:

1. Navigate to ***Mail Policies > Mail Flow Policies***.
2. Click the policy name in order to make edits, or click ***Default Policy Parameters*** in order to view the current DHAP configuration.
3. Make changes to the ***Directory Harvest Attack Prevention (DHAP)*** section as needed:



4. Click ***Submit***, and then click ***Commit*** in order to save your changes.

View or Update DHAP Configuration from the CLI

In order to view or edit your DHAP configuration parameters from the CLI, enter the ***listenerconfig*** > ***edit [listener number]*** > ***hostaccess*** > ***default*** command:

```
Default Policy Parameters
==========================
Maximum Message Size: 10M
Maximum Number Of Concurrent Connections From A Single IP: 10
Maximum Number Of Messages Per Connection: 10
Maximum Number Of Recipients Per Message: 50
Directory Harvest Attack Prevention: Enabled
Maximum Number Of Invalid Recipients Per Hour: 25
Maximum Number Of Recipients Per Hour: Disabled
Maximum Number of Recipients per Envelope Sender: Disabled
Use SenderBase for Flow Control: Yes
Spam Detection Enabled: Yes
Virus Detection Enabled: Yes
Allow TLS Connections: No
Allow SMTP Authentication: No
Require TLS To Offer SMTP authentication: No
DKIM/DomainKeys Signing Enabled: No
DKIM Verification Enabled: No
SPF/SIDF Verification Enabled: No
DMARC Verification Enabled: No
Envelope Sender DNS Verification Enabled: No
Domain Exception Table Enabled: No
Accept untagged bounces: No

There are currently 5 policies defined.
There are currently 8 sender groups.

Choose the operation you want to perform:
- NEW - Create a new entry.
- EDIT - Modify an entry.
- DELETE - Remove an entry.
- MOVE - Move an entry.
- DEFAULT - Set the defaults.
- PRINT - Display the table.
- IMPORT - Import a table from a file.
- EXPORT - Export the table to a file.
- RESET - Remove senders and set policies to system default.
```

```
[]> default

Enter the default maximum message size. Add a trailing k for kilobytes, M for
 megabytes, or no letter for bytes.
[10M]>

Enter the maximum number of concurrent connections allowed from a single IP address.
[10]>

Enter the maximum number of messages per connection.
[10]>

Enter the maximum number of recipients per message.
[50]>

Do you want to override the hostname in the SMTP banner? [N]>

Would you like to specify a custom SMTP acceptance response? [N]>

Would you like to specify a custom SMTP rejection response? [N]>

Do you want to enable rate limiting per host? [N]>

Do you want to enable rate limiting per envelope sender? [N]>

Do you want to enable Directory Harvest Attack Prevention per host? [Y]>

Enter the maximum number of invalid recipients per hour from a remote host.
[25]>

Select an action to apply when a recipient is rejected due to DHAP:
1. Drop
2. Code
[1]>

Would you like to specify a custom SMTP DHAP response? [Y]>

Enter the SMTP code to use in the response. 550 is the standard code.
[550]>

Enter your custom SMTP response. Press Enter on a blank line to finish.

Would you like to use SenderBase for flow control by default? [Y]>

Would you like to enable anti-spam scanning? [Y]>

Would you like to enable anti-virus scanning? [Y]>

Do you want to allow encrypted TLS connections?
1. No
2. Preferred
3. Required
4. Preferred - Verify
5. Required - Verify
[1]>

Would you like to enable DKIM/DomainKeys signing? [N]>

Would you like to enable DKIM verification? [N]>

Would you like to change SPF/SIDF settings? [N]>

Would you like to enable DMARC verification? [N]>

Would you like to enable envelope sender verification? [N]>
```

```
Would you like to enable use of the domain exception table? [N]>

Do you wish to accept untagged bounces? [N]>
```

If you choose to make updates, ensure that you return to the main CLI prompt and ***commit*** all changes.

Related Information

- ***Cisco Email Security Appliance End−User Guides***
- ***Technical Support & Documentation Cisco Systems***

Updated: Apr 23, 2015 Document ID: 118936