Waarschuwingsinformatie op DHAP-hoogte instellen op ESA

Inhoud

Inleiding

Dit document beschrijft hoe u informatie kunt lokaliseren in verband met DHAP-waarschuwingen (Directory Harvest Prevention) op uw Cisco Email Security Appliance (ESA).

HEEP-incidenten lokaliseren vanuit de ESA

De ingangen die de gebeurtenis van DHAP beschrijven verblijven in de postlogs. Hier is een voorbeeld post logingang wanneer DHAP zich voordoet:

```
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
```

Opmerking: standaard wordt **24/24** netmask in de zoekfunctie gezocht.

Voer deze zoekopdracht in in de CLI om de maillogs te bekijken:

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

De DHCP-tellers omvatten zowel afwijzingen in de ontvangstentabel (RAT) als afwijzing van de Lichtgewicht Directory Access Protocol (LDAP)-acceptatie. De instellingen van DHAP worden gevormd in het beleid van de Stroom van de Post.

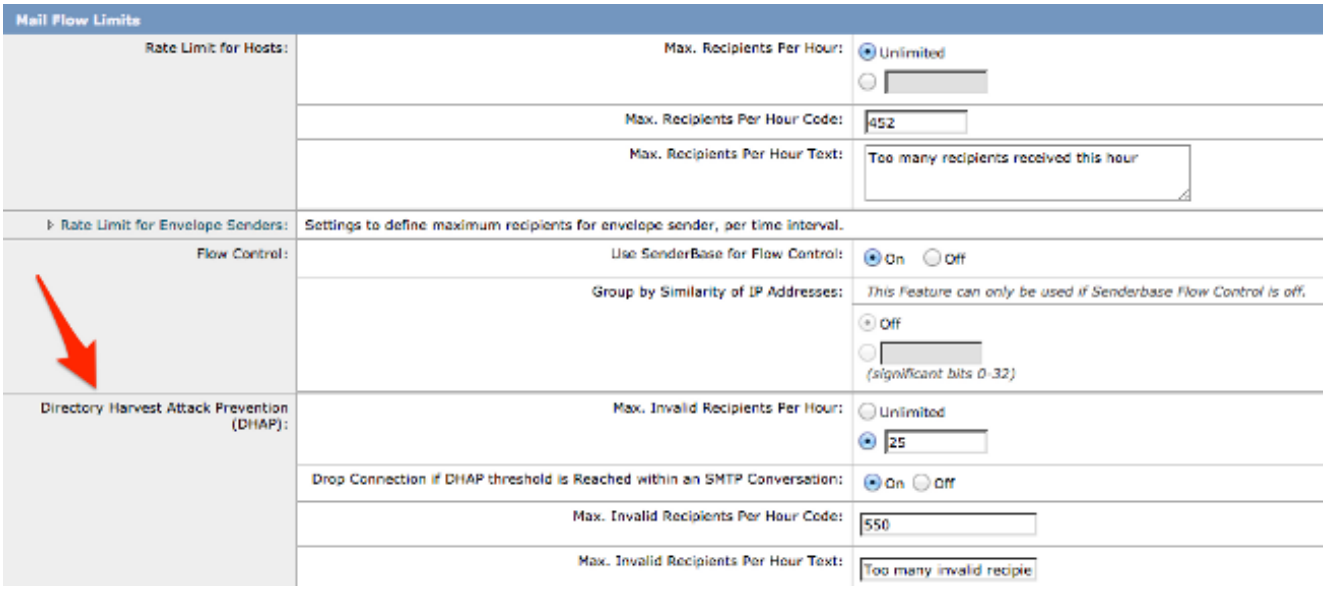
DHCP-configuratie bekijken of bijwerken vanuit de GUI

Voltooi deze stappen om de configuratieparameters van de DHCP-configuratie in de GUI te bekijken of te bewerken:

1. Navigeer naar **Mail-beleid > Mail Flow**.

2. Klik op de beleidsnaam om redits te maken of klik op **Standaardbeleidsparameters** om de huidige configuratie van DHCP te bekijken.

3. Breng indien nodig wijzigingen aan in het gedeelte **Directory Harvest Prevention (DHAP)**:



4. Klik op **Inzenden** en vervolgens op **Aanmelden** om de wijzigingen op te slaan.

DHCP-configuratie bekijken of bijwerken vanuit CLI

Om uw de configuratieparameters van de DHAP van de CLI te bekijken of te bewerken, voer de **listenerfig > bewerk [*luisteraaraantal*] > hostaccess > standaard** opdracht in:

```
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]>
```

Als u ervoor kiest om updates te maken, zorg er dan voor dat u terugkeert naar de belangrijkste CLI prompt en alle veranderingen **toegewijd**.

Gerelateerde informatie

- Cisco e-mail security applicatie - eindgebruikershandleidingen
- Technische ondersteuning en documentatie - Cisco-systemen