Individuazione delle informazioni di allarme DHAP sull'ESA

Sommario

[Introduzione](#)
[Individuazione delle occorrenze DHCP dall'ESA](#)
[Visualizzazione o aggiornamento della configurazione DHCP dalla GUI](#)
[Visualizza o aggiorna la configurazione DHCP dalla CLI](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come individuare le informazioni relative agli avvisi DHCP (Directory Harvest Attack Prevention) su Cisco Email Security Appliance (ESA).

Individuazione delle occorrenze DHCP dall'ESA

Le voci che descrivono l'evento DHCP si trovano nei log di posta. Di seguito è riportato un esempio di voce del log di posta quando si verifica il protocollo DHCP:

```
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
```

Nota: per impostazione predefinita, nella ricerca viene cercata la maschera di rete **/24**.

Immettere questa query nella CLI per visualizzare i log di posta:

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

I contatori DHCP includono sia i rifiuti della tabella Accesso destinatari (RAT, Recipient Access Table) che i rifiuti delle query di accettazione LDAP (Lightweight Directory Access Protocol). Le impostazioni DHCP sono configurate nel criterio Flusso di posta.

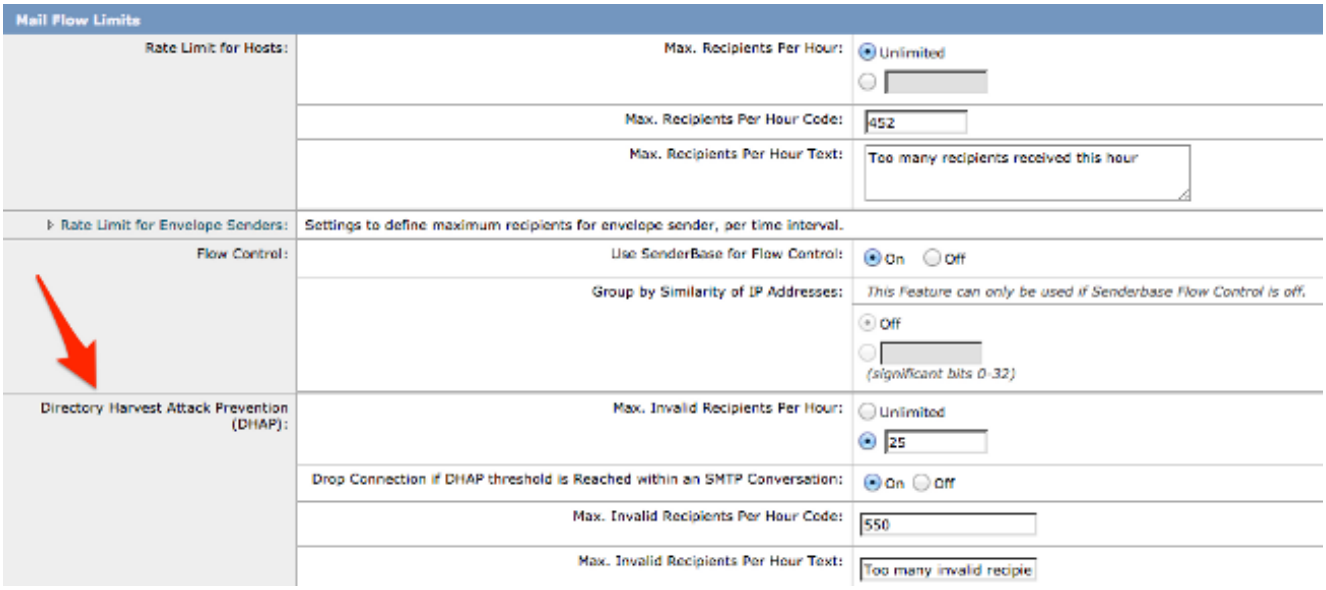
Visualizzazione o aggiornamento della configurazione DHCP dalla GUI

Completare questa procedura per visualizzare o modificare i parametri di configurazione DHCP dalla GUI:

1. Selezionare **Mail Policies > Mail Flow Policies** (Policy di posta > Criteri flusso di posta).

2. Per apportare modifiche, fare clic sul nome del criterio oppure su **Parametri criteri predefiniti** per visualizzare la configurazione DHCP corrente.

3. Apportare le modifiche necessarie alla sezione **Directory Harvest Attack Prevention (DHAP)**:



4. Per salvare le modifiche, fare clic su **Invia** e quindi su **Conferma**.

Visualizza o aggiorna la configurazione DHCP dalla CLI

Per visualizzare o modificare i parametri di configurazione DHCP dalla CLI, immettere il comando **listener config > edit [*listener number*] > hostaccess > default**:

```
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]>
```

Se si sceglie di eseguire gli aggiornamenti, accertarsi di tornare al prompt della CLI principale e **confermare** tutte le modifiche.

Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Documentazione e supporto tecnico - Cisco Systems