

Encuentre la información de la alerta DHAP en el ESA

Contenido

[Introducción](#)

[Localice los acontecimientos DHAP del ESA](#)

[Vea o ponga al día la configuración DHAP del GUI](#)

[Vea o ponga al día la configuración DHAP del CLI](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo encontrar la información con respecto a las alertas de la prevención del ataque de recopilación de direcciones (DHAP) en su dispositivo de seguridad del correo electrónico de Cisco (ESA).

Localice los acontecimientos DHAP del ESA

Las entradas que describen el evento DHAP residen en los registros del correo. Aquí está una entrada de registro del correo del ejemplo cuando ocurre DHAP:

```
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: Por abandono, el netmask de /24 se busca en la búsqueda.

Ingrese esta interrogación en el CLI para ver los registros del correo:

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

Los contadores DHAP incluyen los rechazos receptores de la interrogación de los rechazos de la tabla del acceso (RAT) y de la aceptación del Lightweight Directory Access Protocol (LDAP). Las configuraciones DHAP se configuran en la directiva del flujo de correo.

Configuración de la visión o de la actualización DHAP del GUI

Complete estos pasos para ver o editar sus parámetros de la configuración DHAP del GUI:

1. Navegue **para enviar las directivas > las directivas del flujo de correo**.

2. Haga clic el nombre de la directiva para hacer edita, o hace clic los **parámetros de la política predeterminada** para ver la configuración actual DHAP.

3. Realice los cambios a la **prevención del ataque de recopilación de direcciones (DHAP)** seccionar según las necesidades:

Mail Flow Limits	
Rate Limit for Hosts:	Max. Recipients Per Hour: <input checked="" type="radio"/> Unlimited <input type="radio"/> <input type="text"/>
	Max. Recipients Per Hour Code: <input type="text" value="452"/>
	Max. Recipients Per Hour Text: <input type="text" value="Too many recipients received this hour"/>
▶ Rate Limit for Envelope Senders: Settings to define maximum recipients for envelope sender, per time interval.	
Flow Control:	Use SenderBase for Flow Control: <input checked="" type="radio"/> On <input type="radio"/> Off
	Group by Similarity of IP Addresses: <i>This Feature can only be used if Senderbase Flow Control is off.</i> <input type="radio"/> Off <input type="radio"/> <input type="text"/> <small>(significant bits 0-32)</small>
Directory Harvest Attack Prevention (DHAP):	Max. Invalid Recipients Per Hour: <input type="radio"/> Unlimited <input checked="" type="radio"/> <input type="text" value="25"/>
	Drop Connection if DHAP threshold is Reached within an SMTP Conversation: <input checked="" type="radio"/> On <input type="radio"/> Off
	Max. Invalid Recipients Per Hour Code: <input type="text" value="550"/>
	Max. Invalid Recipients Per Hour Text: <input type="text" value="Too many invalid recipie"/>

4. El tecleo **somete**, y después hace clic el **cometer** para salvar sus cambios.

Configuración de la visión o de la actualización DHAP del CLI

Para ver o editar sus parámetros de la configuración DHAP del CLI, ingrese el **listenerconfig > editan el [listener number] > los hostaccess > el comando 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]>

Si usted elige hacer las actualizaciones, asegúrese de que usted vuelva al prompt principal CLI y **confíe** todos los cambios.

Información Relacionada

- [Dispositivo de seguridad del correo electrónico de Cisco – Guías del usuario final](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)