ESA에서 DHAP 알림 정보 찾기

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance)에서 DHAP(Directory Harvest Attack Prevention) 경고와 관련된 정보를 찾는 방법에 대해 설명합니다.

ESA에서 DHAP 발생 찾기

DHAP 이벤트를 설명하는 항목은 메일 로그에 있습니다.다음은 DHAP가 발생할 경우 메일 로그 항목의 예입니다.

```
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
```

참고: 기본적으로 **/24** 넷마스크는 검색에서 찾습니다.

메일 로그를 보려면 CLI에 이 쿼리를 입력합니다.

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

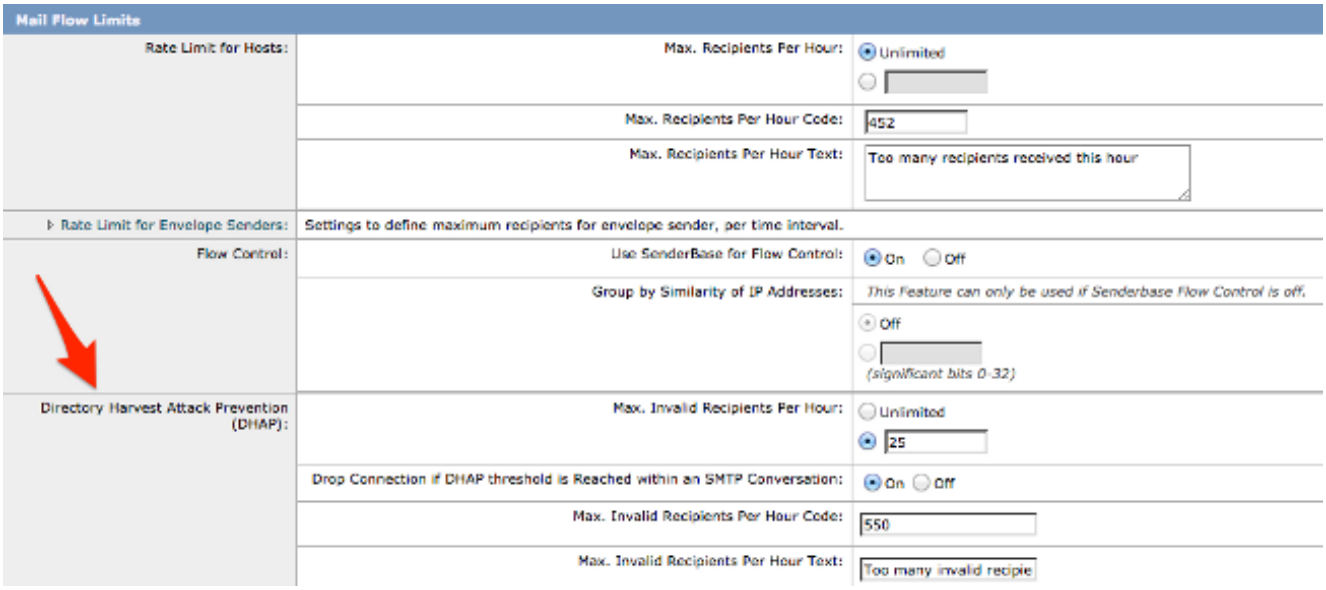
DHAP 카운터는 RAT(Recipient Access Table) 거부 및 LDAP(Lightweight Directory Access Protocol) 수락 쿼리 거부를 모두 포함합니다.DHAP 설정은 메일 플로우 정책에서 구성됩니다.

GUI에서 DHAP 컨피그레이션 보기 또는 업데이트

GUI에서 DHAP 컨피그레이션 매개변수를 보거나 편집하려면 다음 단계를 완료하십시오.

1. Mail Policies(**메일 정책) > Mail Flow Policies(메일 플로우 정책)로 이동합니다**.
2. 수정하려면 정책 이름을 클릭하고 현재 DHAP 컨피그레이션을 보려면 **Default Policy Parameters**를 클릭합니다.

3. 필요에 따라 DHAP(**Directory Harvest Attack Prevention**) 섹션을 변경합니다.



4. Submit(**제출**)을 클릭한 다음 **Commit**(커밋)을 클릭하여 변경 사항을 저장합니다.

CLI에서 DHAP 컨피그레이션 보기 또는 업데이트

CLI에서 DHAP 컨피그레이션 매개변수를 보거나 편집하려면 listenerconfig **> edit [*listener number*] > hostaccess > default** 명령을 입력합니다.

```
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]>
```

업데이트를 수행하도록 선택한 경우 기본 CLI 프롬프트로 돌아가 모든 변경 사항을 **커밋해야 합니다**.

관련 정보

- Cisco Email Security Appliance - 최종 사용자 가이드
- 기술 지원 및 문서 - Cisco 시스템