# 查找DHAP关于ESA的警报信息

## 目录



## 简介

本文描述如何关于目录收获攻击在您的思科电子邮件安全工具(ESA)的预防(DHAP)警报查找信息。

## 找出从ESA的DHAP出现

描述DHAP事件的条目位于邮件日志。这是示例邮件日志条目，当DHAP发生时：

```
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: 默认情况下，/24网络屏蔽在搜索寻找。

参与此查询到CLI为了查看邮件日志：

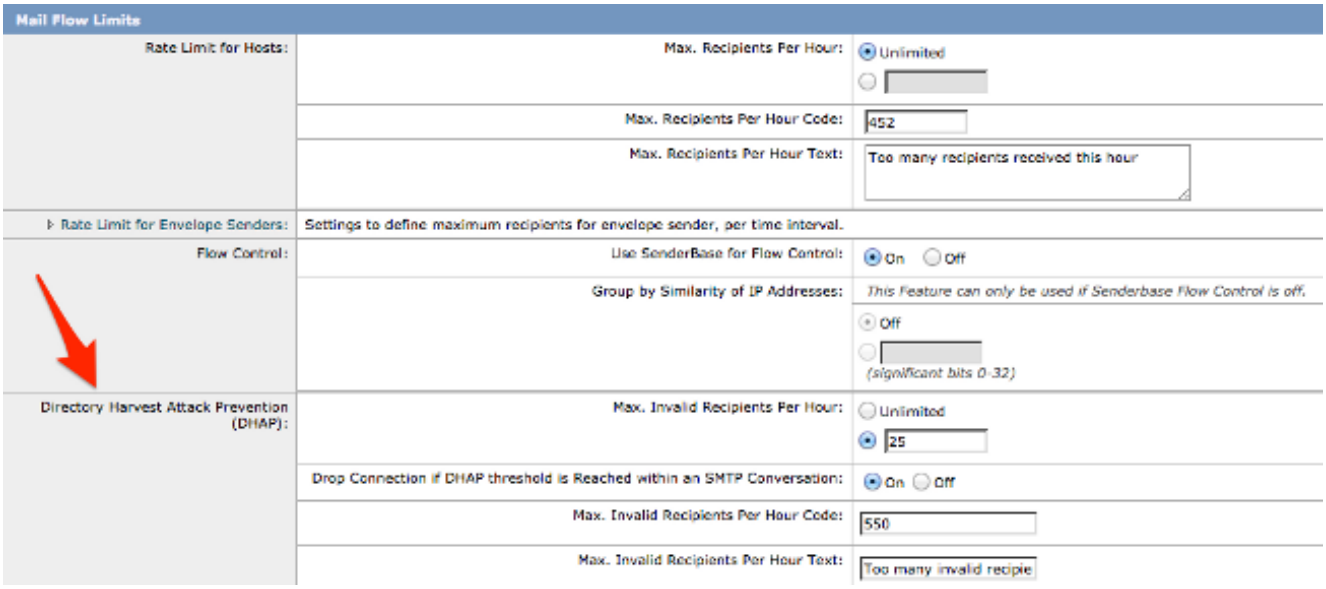
```
myesa.local> grep "dhap_limit=" mail_logs
```

DHAP计数器包括接收访问表(RATS)拒绝和轻量级目录访问协议(LDAP)接受查询拒绝。DHAP设置在邮件流量策略配置。

## 查看或更新从GUI的DHAP配置

完成这些步骤为了查看或编辑您的从GUI的DHAP配置参数：

1. 导航**邮寄策略>邮件流量策略**。
2. 点击策略名称为了做编辑或者点击**默认策略参数**为了查看当前DHAP配置。
3. 做对**目录的**变动**收获攻击预防(DHAP)**部分当必要时：




4. 单击**提交**，然后单击**进行**为了保存您的更改。

# 查看或更新从CLI的DHAP配置

为了查看或编辑您的从CLI的DHAP配置参数，输入**listenerconfig > Edit [listener number] > hostaccess > default命令**：

```
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]>
```

如果选择做更新，请保证您回到主CLI提示符并且**确认**所有更改。

# 相关信息

- 思科电子邮件安全工具–最终用户指南
- 技术支持和文档 - Cisco Systems