تحديد موقع معلومات تنبيه DHP على ESA

المحتويات

المقدمة
تحديد موقع حالات حدوث حدوث حدوث حدوث نشاط نشاط نشاط نشاط نشاط كهربي في الفضاء الخارجي من الإيسا
عرض تكوين DHP أو تحديثه من واجهة المستخدم الرسومية
عرض تكوين DHP أو تحديثه من واجهة سطر الأوامر
معلومات ذات صلة

المقدمة

يصف هذا المستند كيفية تحديد موقع المعلومات فيما يتعلق بتنبيهات منع هجمات الدليل (DHAP) على جهاز أمان البريد الإلكتروني (ESA) من Cisco لديك.

تحديد موقع حالات حدوث حدوث حدوث حدوث نشاط نشاط نشاط نشاط نشاط كهربي في الفضاء الخارجي من الإيسا

توجد الإدخالات التي تصف حدث DHP في سجلات البريد. فيما يلي مثال لإدخال سجل البريد عند حدوث DHP:

```
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
```

ملاحظة: بشكل افتراضي، يتم البحث عن قناع الشبكة **24/** في البحث.

أدخل هذا الاستعلام في CLI لعرض سجلات البريد:

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

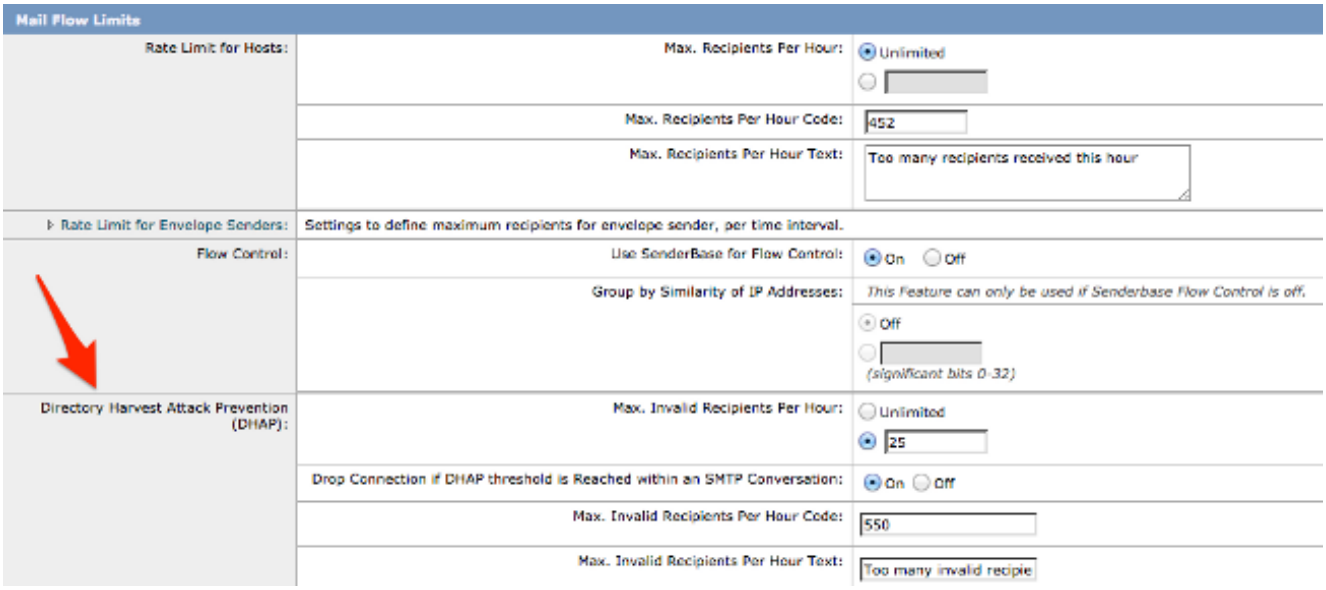
تتضمن عدادات DHP كل من عمليات رفض جدول وصول المستلم (RAT) وعمليات رفض استعلام قبول بروتوكول الوصول إلى الدليل الخفيف (LDAP). تم تكوين إعدادات DHP في نهج تدفق البريد.

عرض تكوين DHP أو تحديثه من واجهة المستخدم الرسومية

أتمت هذا steps in order to شاهدت أو حررت ك DHP تشكيل معلم من ال gui:

1. انتقل إلى **نهج البريد > نهج تدفق البريد**.
2. انقر فوق اسم النهج لإجراء التحريرات، أو انقر فوق **معلمات النهج الافتراضية** لعرض تكوين DHP الحالي.

3. قم بإجراء تغييرات على قسم **منع هجوم حصاد الدليل (DHAP)** حسب الحاجة:



4. انقر فوق **إرسال**، ثم انقر فوق **التزام** لحفظ التغييرات التي قمت بها.

عرض تكوين DHP أو تحديثه من واجهة سطر الأوامر

لعرض معلمات تكوين DHP الخاصة بك أو تحريرها من واجهة سطر الأوامر، أدخل **الأمر** listEnergyConfig **< تحرير < [مستمع رقم] < hostaccess < افتراضي**:

```
                                  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
Drop .1
Code .2
<[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
No .1
Preferred .2
Required .3
Preferred - Verify .4
Required - Verify .5
<[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
```

إذا أخترت إجراء تحديثات، فتأكد من الرجوع إلى موجه أوامر واجهة سطر الأوامر الرئيسي **وقم** بتنفيذ كافة التغييرات.

معلومات ذات صلة

- جهاز أمان البريد الإلكتروني من Cisco - أدلة المستخدم النهائي
- الدعم التقني والمستندات - سيسكو سيستمز

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).