أستكشاف المشكلات المتقطعة والاتصالات التي تم إجهاضها أثناء إستلام البريد وتسليمه وإصلاحها

المحتويات

المقدمة

يوضح هذا المستند كيفية أستكشاف المشكلات المتقطعة والاتصالات التي تم إيقافها قبل اكتمالها أثناء إستلام البريد وتسليمه.

المتطلبات الأساسية

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Cisco Private Internet Xchange (PIX) أو جهاز الأمان القابل للتكيف (ASA)، الإصدار x.7 والإصدارات الأعلى
- أجهزة أمان البريد الإلكتروني Cisco Email Security Appliance (ESA)

معلومات أساسية

تكون بوابات البريد الإلكتروني ل Cisco ESA عبارة عن جدران أمان بريد إلكتروني بطبيعتها. وهذا ينفي الحاجة إلى جدار حماية للتحميل، مثل PIX أو ASA من Cisco، لفحص حركة مرور البريد من وإلى ESA. يقترح تعطيل ميزات فحص تطبيق بروتوكول نقل البريد البسيط الموسع (ESMTP) على جدار الحماية لأي عناوين مضيف من أجهزة الأمان. بشكل افتراضي، يتم تمكين فحص بروتوكول ESMTP لجميع الاتصالات التي تمر عبر جدران الحماية من Cisco. هذا يعني أن كل الأوامر الصادرة بين بوابات البريد عبر منفذ TCP 25، بالإضافة إلى رؤوس الرسائل الفردية، يتم تحليلها بحيث تلتزم بدقة بمواصفات طلب التعليقات (RFC) التي تتضمن مواصفة 821 و 1123 و 1870 الخاصة ب RFC. هناك قيم افتراضية معرفة للحد الأقصى من عدد المستلمين وأحجام الرسائل التي قد تتسبب في مشاكل مع التسليم إلى ESA ومنه. يتم توضيح إعدادات التكوين الافتراضية المحددة هذه هنا (مأخوذة من أداة بحث أوامر Cisco).

يتضمن الأمر **inspection esmtp** الوظائف التي تم توفيرها مسبقا من خلال الأمر **fix smtp**، كما يوفر دعما إضافيا لبعض أوامر ESMTP. يضيف فحص تطبيق ESMTP دعما لثمانية أوامر ESMTP، بما في ذلك AUTH، EHLO، SOML، SEND، SAML، HELP، ETRN و VRFY. إلى جانب دعم سبعة أوامر (DATA، HELO، RFC 821 RSET، **RCPT**، QUIT، NOOP، MAIL)، يدعم جهاز الأمان إجمالي 15 أمر SMTP. أوامر ESMTP الأخرى، مثل ATRN، و**STARTLS**، و**OneEx**، و**VERB**، و**Chunking**، والامتدادات الخاصة وغير مدعومة. تتم ترجمة الأوامر غير المدعومة إلى XS، والتي يتم رفضها بواسطة الخادم الداخلي. وينتج عن ذلك رسالة مثل **الأمر 500 غير معروف: xxx**. يتم تجاهل الأوامر غير المكتملة.

يقوم الأمر **فحص esmtp** بتغيير الأحرف الموجودة في شعار SMTP للخادم إلى علامات نجمية باستثناء الأحرف "2" و"0" و"0". يتم تجاهل أحرف إرجاع النقل (CR) وأداة تعريف الخط (LF). مع تمكين فحص SMTP، تنتظر جلسة العمل المستخدمة ل SMTP التفاعلي الأمر الصالح ويحتفظ جهاز حالة جدار الحماية بالحالات الصحيحة للجلسة إذا لم يتم مراعاة هذه القواعد:

- يجب أن يكون طول أوامر SMTP أربعة أحرف على الأقل.
- يجب إنهاء أوامر SMTP باستخدام إعادة النقل وموجز السطر.
- يجب أن تنتظر أوامر SMTP الاستجابة قبل إصدار الرد التالي.

يستجيب خادم SMTP لطلبات العملاء من خلال رموز الرد الرقمية والسلاسل الاختيارية القابلة للقراءة من قبل الإنسان. يتحكم فحص تطبيق SMTP في الأوامر التي يمكن للمستخدم إستخدامها، بالإضافة إلى الرسائل التي يرجعها الخادم، ويعمل على تقليل هذه الأوامر. ينجز فحص SMTP ثلاث مهام أساسية:

- قصر طلبات SMTP على سبعة أوامر SMTP أساسية وثمانية أوامر موسعة.
- يراقب تسلسل أمر-إستجابة SMTP.
- إنشاء سجل تدقيق. يتم إنشاء سجل التدقيق 108002 عند إستبدال حرف غير صالح مضمن في عنوان البريد. لمزيد من المعلومات، راجع RFC 821.

يراقب فحص SMTP الأمر وتسلسل الاستجابة للتواقيع الشاذة التالية:

- الأوامر المقطوعة.
- إنهاء أمر غير صحيح (لم يتم إنهاؤه باستخدام <CR><LR>).
- إذا تم العثور على واجهة PHY لتوقيع PCI Express (PIPE) كمعلمة لأمر **بريد** من أو **RCPT** إلى، يتم إغلاق الجلسة. غير قابل للتكوين بواسطة المستخدم.
- انتقال غير متوقع بواسطة خادم SMTP.
- بالنسبة للأوامر غير المعروفة، يقوم جهاز الأمان بتغيير كافة الأحرف الموجودة في الحزمة إلى **X**. في هذه الحالة، سيقوم الخادم بإنشاء رمز خطأ للعميل. بسبب التغيير في الحزمة، يجب إعادة حساب المجموع الاختباري ل TCP أو ضبطه.
- تحرير تدفق TCP.

يوفر إخراج **show service-policy inspection ESMTP** قيم الفحص الافتراضية والإجراءات المقابلة لها.

```
:Global policy
Service-policy: global_policy
Class-map: inspection_default
Inspect: esmtp _default_esmtp_map, packet 104468, drop 0, reset-drop 0
mask-banner, count 639 obfuscate the SMTP banner greeting
(match cmd line length gt 512 deny all SMTP commands (and close connection
drop-connection log, packet 0
match cmd RCPT count gt 100 drop all messages (and connection) with more
than 100 recipients
drop-connection log, packet 0
match body line length gt 998 log all messages with lines > 998 chars
log, packet 0
(match header line length gt 998 drop all messages (and connection
with headers > 998 chars
drop-connection log, packet 41
```

```
match sender-address length gt 320 drop all messages (and connection) with
                                                envelope sender > 320 bytes
                                                drop-connection log, packet 0
match MIME filename length gt 255 drop all messages (and connection) with
                                                MIME attachment filenames > 255 bytes
                                                drop-connection log, packet 0
match ehlo-reply-parameter others obfuscate extended commands not explicitly
                                                (noted in the RFCs (such as STARTTLS
                                                mask, packet 2555
```

المشكلة

وفي بعض الأحيان، لن يتم تسليم الرسائل بشكل صحيح أو تلقيها بواسطة Cisco ESA. رأيت رسالة أو أكثر من هذا رسالة في ال cisco ESA أداة mail_log:

- تم إجهاض الرسالة في منتصف xxx
- فقد تلقي ICID 21916 الذي تم إجهاضه
- إغلاق ICID 21916
- خطأ اتصال: DCID: XXX domain:example.com ip: منفذ 10.1.2.3: 25 تفصيلا: [خطأ 60] واجهة انتهاء مهلة العملية: 10.10.10.1 سبب: خطأ الشبكة

الحل

قد تؤثر بعض هذه الإعدادات الافتراضية على أشياء مثل تسليم الرسائل المشفرة لأمان طبقة النقل (TLS) وحملات القائمة البريدية واستكشاف الأخطاء وإصلاحها. قد تجعلك سياسة أفضل تستخدم جدار الحماية لتفحص جميع حركة مرور البريد الإلكتروني المتبقية التي لا تمر أولا عبر جهاز الأمان، مع إعفاء جميع حركة المرور التي تحتوي على. يوضح هذا المثال كيفية ضبط التكوين الافتراضي (المشار إليه سابقا) لإعفاء فحص تطبيق ESMTP لعنوان مضيف أمان واحد.

يمكنك تحديد حركة مرور البيانات بالكامل من العنوان الداخلي ل Cisco ESAs وإليه كمرجع في خريطة فئة إطار عمل السياسة النمطية (MPF):

```
access-list ironport_esa_internal extended permit ip any 192.168.1.1
access-list ironport_esa_internal extended permit ip 192.168.1.1 any
```

يؤدي هذا إلى إنشاء خريطة فئة جديدة لمطابقة حركة المرور أو تحديدها بشكل محدد لكي يتم معالجتها بشكل مختلف:

```
class-map ironport_esa
match address ironport_esa_internal
```

يربط هذا القسم خريطة فئة Cisco الجديدة ويعطل ميزات فحص بروتوكول ESMTP:

```
policy-map global_policy
      class ironport_esa
        no inspect esmtp
```

لاحظ أيضا بيان ترجمة العنوان الذي يمكن أن يساعد في التحكم في عدد الاتصالات (الجنينية) الواردة ونصف المفتوحة للعنوان. ويعد هذا مفيدا لمكافحة هجمات رفض الخدمة (DoS)، ولكنه قد يتعارض مع معدلات تقديم الخدمة.

تنسيق لتتبع معلمات أوامر **NAT** وmax_ryonic] [(max_conns) TCP] ..**STATIC**].
يحدد هذا المثال حدود إجمالي 50 اتصال TCP و 100 محاولة اتصال نصف مفتوحة أو جنينية:

```
static (inside,outside) 1.1.1.1 192.168.1.1 netmask 255.255.255.255 tcp 50 100
```

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).