حل استجابات UDP DNS الكبيرة التي تفشل من خلال FTD مع تمكين فحص DNS

المحتويات

مسألة

يفشل حزم DNS ذات أحجام الحزم الكبيرة (حوالي 1800-4000 بايت) عندما تنتقل حركة مرور Cisco Firepower البيانات بين شبكات VM في شبكات VLAN مختلفة من خلال جدار حماية Threat Defense (FTD). ال نفسه DNS ينجح حركة مرور عندما يقع إتصال بين VMs في ال نفسه VLAN دون يمر من خلال جدار الحماية. أثناء أستكشاف الأخطاء وإصلاحها، تم اكتشاف أن يتم إعادة تجميع حزم الرد على DNS المزأة بالكامل بواسطة جدار حماية FTD عند تسجيل الخروج وإرسالها كحزم كبيرة واحدة تتجاوز قدرة MTU للعميل، مما يتسبب في قيام العميل بإسقاط الحزم.

البيئة

- مجموعة المنتج: أول مرة يرى فيها على سلسلة Cisco Secure Firewall 4200، يمكن أن تتأثر الأنظمة الأساسية الأخرى أيضا.
- إصدار البرامج: شوهد لأول مرة على إصدار برنامج FTD 7.6.2.1، كما يمكن أن تتأثر إصدارات البرامج الأخرى.
- وحدة الحد الأقصى للنقل (MTU) لواجهة جدار الحماية تبلغ 9000 بايت
- تم تمكين فحص DNS.
- أجهزة عميلة تأثرت تم تكوينها باستخدام وحدة الحد الأقصى للنقل (MTU) القياسية سعة 1500 بايت.
- تقوم خوادم DNS بإنشاء استجابات مجزأة لاستعلامات سجلات SRV كبيرة.

قرار

تم حل المشكلة من خلال ضبط تكوين وحدة الحد الأقصى للنقل (MTU) لواجهة جدار الحماية.
ويمكن إستخدام هذه النهج لمعالجة هذه المشكلة:

الخيار 1: ضبط وحدة الحد الأقصى للنقل (MTU) للواجهة إلى 1500 إذا كانت أجهزة الشبكة الأخرى تسمح بذلك (مستحسن)

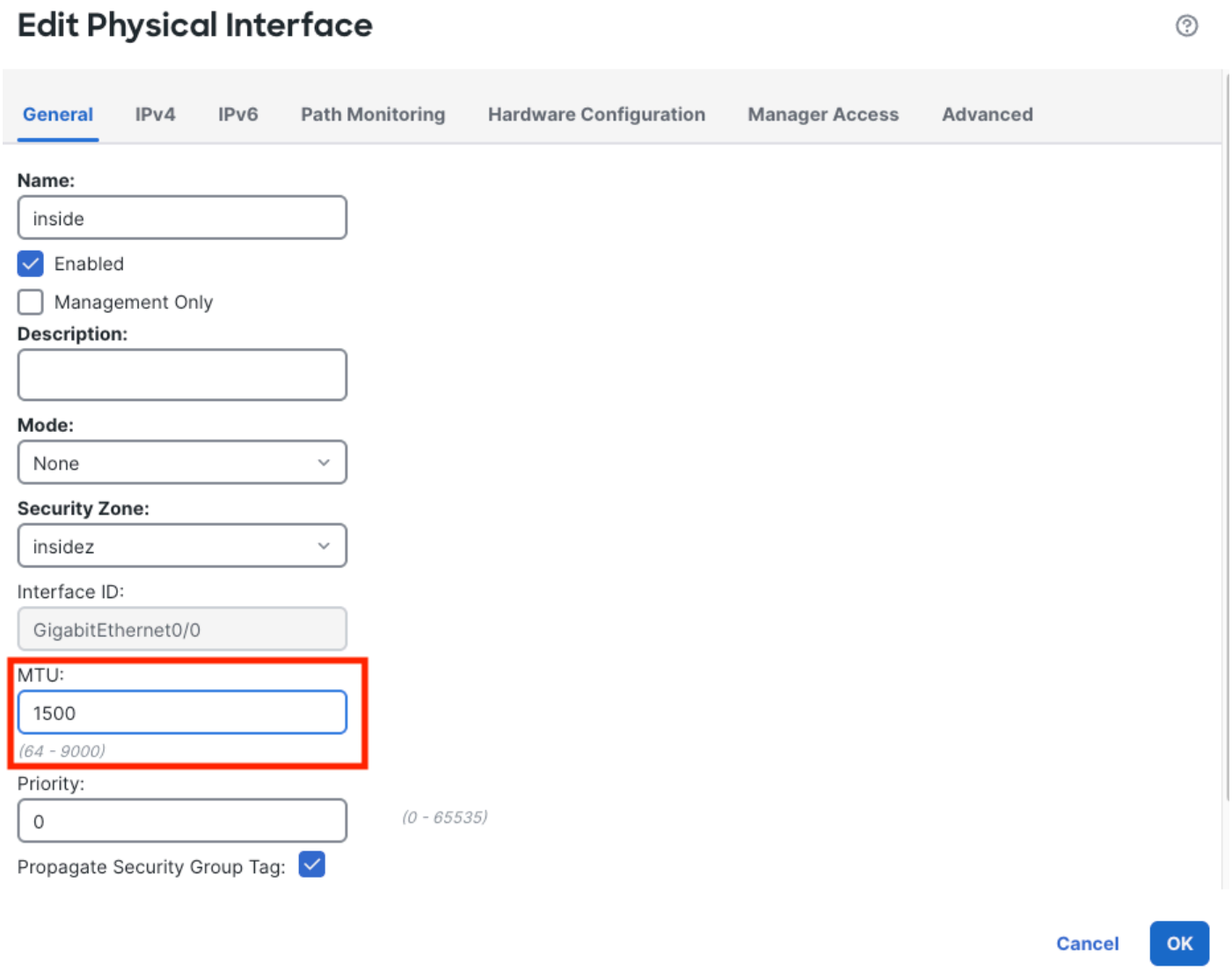
قم بتغيير وحدة الحد الأقصى للنقل (MTU) لواجهة مخرج جدار الحماية من 9000 إلى 1500 بشكل صحيح:
إعادة تجزئة الحزم المعاد تجميعها بايت لضمان

ASA:

```
device# configure terminal
device(config)# interface gigabitethernet0/0
device(config-if)# mtu 1500
device(config-if)# exit
```

FTD:

Change MTU from FMC GUI



تحقق من تكوين وحدة الحد الأقصى للنقل (MTU):

```
device# show interface gigabitethernet0/0
GigabitEthernet0/0 is up, line protocol is up
Hardware is i82580 rev03, BW 1000000 Kbit, DLY 10 usec
Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)
Available but not configured via nameif
MAC address 0050.56bb.09c8, MTU 1500
```

الخيار 2: تعطيل فحص DNS (حل بديل غير مستحسن)

ملاحظة: إذا كان تعطيل فحص DNS مقبولا وقواعد لمتطلبات الأمان وإذا لم يكن جدار الحماية جدار حماية محيط، يمكنك إعتبار تعطيل فحص DNS من خريطة السياسة.

(يمكن أن يزيد هذه أيضا عدد الاتصالات الإجمالية إذا كانت حركة مرور DNS مرتفعة):

```
ASA:
device# configure terminal
device(config)# policy-map global_policy
device(config-pmap)# class inspection_default
device(config-pmap-c)# no inspect dns
device(config-pmap-c)# exit

FTD:
> configure inspection dns disable
```

خطوات التحقق

بعد تنفيذ الحل، تحقق من وظيفة DNS:

إختبار دقة DNS باستخدام استجابات كبيرة:

```
dig @dns_server_ip _ldap._tcp.domain.com SRV
```

معالجة حزمة جدار الحماية للشاشة:

```
Collect packet packets on ingress and egress interface to analyse in WireShark
```

السبب

عند تمكين فحص DNS على FTD، يقوم جدار الحماية بتنفيذ إعادة تجميع كاملة لحزم DNS قبل إعادة توجيه الحزمة إلى محرك الفحص (SNORT) بفحص حمولة DNS الكاملة. بعد الفحص، إذا كانت حزمة DNS أكبر من حجم الحزمة المعاد تجميعها، يقوم جدار الحماية بإعادة تجزئة الحزمة إلى أجزاء للسماح لمحرك الفحص بفحص حمولة DNS الكاملة. بعد الفحص، إذا كانت حزمة DNS أكبر من حجم الحزمة المعاد تجميعها، يقوم جدار الحماية بإعادة توجيه الحزمة كإطار واحد دون إعادة تفتيت ذلك.

واجهة جدار الحماية التي تم تكوينها باستخدام وحدة الحد الأقصى للنقل (MTU) بمقدار 9000 بايت، مما يسمح بإعادة تجميع استجابات DNS (حوالي 1884 بايت) ليتم إرسالها كحزمة واحدة. ومع ذلك، فإن أجهزة العميل التي تم تكوينها باستخدام وحدة الحد الأقصى للنقل (MTU)

طاقسإ ىلإ يدأ مما ،ةريبكلا مزحلا هذه لوبق هيلع رذعت تايب 1500 غلبت تيلا ةيسايقلا
.رورملا ةكرح

ةيلمع MTU عراق lina ىلع ناكمإ DNS صحف نوكي نأ عقوتملا نم نوكي لوكسلا عندما
.همجيعاا ةعادملا مزحلا مجح نم رباكأ دادعإ

- فحص Lina DNS: يجري إعادة تجميع كاملة للتفتيش العميق على الحزم. (راجع هذا المستند خلل CSCwv66007 للحصول على مزيد من التفاصيل.)
- Snort 3: يجري إعادة تجميع منطقي (ظاهري) للتفتيش بدون إعادة تجميع مادي.

المحتوى ذي الصلة

- الدعم الفني والتنزيلات من Cisco
- CSCwv66007 (DOC:Clear ASA/FTD سلوك إعادة تجميع التجزئة مع ميزة خريطة السياسة الممكنة التي تتطلب إعادة التجميع بالكامل)

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).