تكوين الوصول الداخلي إلى الموارد لمستخدمي VPN على FTD باستخدام حركة مرور بيانات HairPin

المحتويات

مسألة

الهدف هو تمكين الوصول الكامل لمستخدمي VPN إلى موارد الشبكة الداخلية بعد مصادقة VPN الناجحة باستخدام RADIUS (مقابل خادم مرتبط بالمجال لنظام Windows) على Cisco Secure Firewall FTD.

إعداد VPN قيد التشغيل بالفعل؛ يمكن للمستخدمين تنزيل عميل VPN وتثبيته والمصادقة بنجاح. وتركز المشكلة على تكوين التحكم في الوصول اللازم وقواعد NAT للسماح بالوصول المطلوب إلى الموارد الداخلية عبر VPN.

البيئة

- المنتج: Cisco Secure Firewall Firepower (FTD)، الإصدار 7.6.0 (مثل جهاز CSF1220CX)
- الإدارة: مركز إدارة FirePOWER (FMC) أو وحدة تحكم في الإدارة (FMC) يتم تسليمها عبر السحابة (cdFMC) أو مدير أجهزة FirePOWER (FDM)
- VPN: تم تكوينه بمصادقة RADIUS مقابل خادم Windows متصل بالمجال (NPS)
- تجمع عناوين VPN: 192.168.250.1 - 192.168.250.200
- مثال الشبكة الفرعية الداخلية المستهدفة: 192.168.95.0/24
- إصدار البرنامج: 9.22.1 (كما تمت الإشارة إليه في سير العمل)
- الواجهات ذات الصلة: الواجهة 'الخارجية' لمدخل VPN
- يلزم وصول RDP و Active Directory عبر اتصال VPN

قرار

تقوم هذه الخطوات بتفصيل التكوين المطلوب للسماح لمستخدمي الشبكة الخاصة الظاهرية (VPN) بالوصول إلى الموارد الداخلية (مثل RDP و Active Directory) على Cisco FTD. وهذا يتضمن إنشاء قواعد سياسة الوصول، وتكوين إعفاءات NAT و NAT لإعادة توجيه حركة مرور الشبكة الخاصة الظاهرية (VPN)، واستخدام أوامر أستكشاف الأخطاء وإصلاحها للتحقق من التكوين.

الخطوة 1: إضافة إدخال قائمة وصول للسماح لتجمع عناوين VPN بالوصول إلى الموارد الداخلية.

```
access-list CSM_FW_ACL_ advanced permit ip object VPN_Pool any rule-id 268438528
```

```
access-list CSM_FW_ACL_ remark rule-id 268438528: ACCESS POLICY: Default Access Control Policy - Mandat
access-list CSM_FW_ACL_ remark rule-id 268438528: L7 RULE: Permit_VPN_Pool
```

الخطوة 2: إضافة قاعدة قائمة وصول للسماح للمواردالداخلية بإرسال حركة مرور البيانات العائدة إلى تجمع VPN:

```
access-list CSM_FW_ACL_ advanced permit ip any object VPN_Pool
```

ويمكن في وقت لاحق تشديد هذه القواعد لتقييد مصادر وجهات محددة حسب الحاجة.

الخطوة 3: تكوين إستثناء NAT وأ NAT لمعرف فئة المورد (VPN) لحركة مرور البيانات لشبكة VPN

هناك نهجان مشتركان:

- الخيار A: إستثناء NAT لتجمع شبكات VPN إلى الشبكة الفرعية الداخلية

```
nat (outside,inside) source static VPN_Pool VPN_Pool destination static Net_192.168.95.1-24 Net_192.168
```

- الخيار B: NAT لسماكة وم رشر الموارس لتجمع الشبكة الخاصة الظاهرية (VPN) على الواجهة نفسها (بدون وكيل-arp)

```
nat (any,any) source static VPN_Pool VPN_Pool no-proxy-arp
```

- الخيار C: بطاقة واجهة الشبكة (NAT) فائقة الأداء الديناميكية لتجمع الشبكة الخاصة الظاهرية (VPN) على الواجهة الخارجية

```
nat (outside,outside) dynamic VPN_Pool interface
```

يعتمد الأسلوب صحيح على ما إذا كانت الموارد الداخلية على ال نفس قارن طبيعي (يتطلب رقاقة nat) أو قارن مختلف (nat إعفاء).

الخطوة 4: أستخدم الأمر packet-tracer لمحاكاة حركة مرور البيانات من تجمع VPN إلى الموارد الداخلية والتحقق من صحة ما إذا كانت حركة المرور مسموح بها بواسطة القاعدة المقصودة و NAT و route.

```
packet-tracer input outside icmp 192.168.250.1 8 0 192.168.95.1
packet-tracer input outside tcp 192.168.250.1 12345 192.168.95.1 80
packet-tracer input inside icmp 192.168.95.1 8 0 192.168.250.1
packet-tracer input inside tcp 192.168.250.1 54321 192.168.95.1 443
--
Phase 5
ID: 5
Type: ACCESS-LIST
Result: ALLOW
Config: access-group CSM_FW_ACL_ globalaccess-list CSM_FW_ACL_ advanced permit ip object VPN_Pool any r
Additional Information:  This packet will be sent to snort for additional processing where a verdict wi
Elapsed Time: 0 ns
--
Phase 7
ID: 7
Type: NAT
Result: ALLOW
Config: nat (outside,outside) dynamic VPN_Pool interface
Additional Information: Static translate 192.168.250.1/12345 to 192.168.250.1/12345 Forward Flow based
Elapsed Time: 0 ns
```

ملاحظة: يمكن أن يعرض إخراج Packet-tracer لمرحلة WebVPN "drop" لحركة مرور VPN على الواجهة الخارجية. هذا سلوك متوقع لحركة مرور النص العادي على الواجهة الخارجية والتي لا يمكن إستخدامه للتحقق من NAT.

ملاحظات إضافية:

- من المحتمل أن تظهر صور الحزم في واجهة مستخدم الدفاع عن التهديد الطلبات الواردة فقط. إذا لم يتم ملاحظة عمليات إسقاط، لكن لا تصل حركة المرور إلى المورد الداخلي، فتحقق من قواعد NAT وقائمة الوصول.
- عندما لا يكون بروتوكول SSH متاحا، يمكن تنفيذ جميع عمليات أستكشاف الأخطاء وإصلاحها عبر ميزات واجهة مستخدم الدفاع عن التهديد في CDfmc، ولكن إستخدام الأوامر محدود.
- من المحتمل أن تكون هناك حاجة إلى بعض التعديلات على الأجهزة المجاورة للاتصال الشامل.

السبب

كان السبب الجذري سياسة وصول غير كافية وتكوين NAT لحركة مرور تجمع VPN إلى الداخل و داخلي إلى VPN. التقصير تشكيل ال يسمح كامل ثنائي إتجاه اتصال من ال VPN بركة إلى مورد داخلي ورجع، والى يعالج وه شنطة شرط nat لمرور مدخل ومدخل على ال نفس قارن.

المحتوى ذي الصلة

- تكوين إستثناء NAT على FTD
- الدعم الفني والتنزيلات من Cisco

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).