إدارة الوحدة النمطية SFR عبر نفق VPN بدون مودم لشبكة LAN

المحتويات

المقدمة
المتطلبات الأساسية
المكونات المستخدمة
عمارة
المتطلبات
نظرة عامة على المخطط
تصميم منخفض المستوى
الحل
توصيل كبلات
عنوان IP
الشبكة الخاصة الظاهرية (VPN) وشبكة NAT
مثال التكوين
مناقشات مجتمع دعم Cisco ذات الصلة

المقدمة

يقدم موفرو الخدمة خدمة WAN المدارة في حافظتهم. يوفر النظام الأساسي Cisco ASA FirePOWER مجموعة ميزات إدارة التهديدات الموحدة لتوفير خدمات متميزة. يحتوي جهاز أمان ASA Firepower على واجهات منفصلة للإدارة تتصل بجهاز شبكة LAN، ومع ذلك، يؤدي توصيل واجهة إدارة بجهاز شبكة LAN إلى إنشاء تبعية على جهاز شبكة LAN.

يقدم هذا المستند حلا يسمح لك بإدارة وحدة Cisco ASA FirePOWER (SFR) النمطية دون الاتصال بجهاز شبكة LAN أو إستخدام واجهة ثانية من جهاز حافة مزود الخدمة.

المتطلبات الأساسية

المكونات المستخدمة

- النظام الأساسي فئة ASA 5500-X مع خدمات FirePOWER (SFR).
- واجهة الإدارة التي تتم مشاركتها بين الوحدة النمطية ASA و FirePOWER.

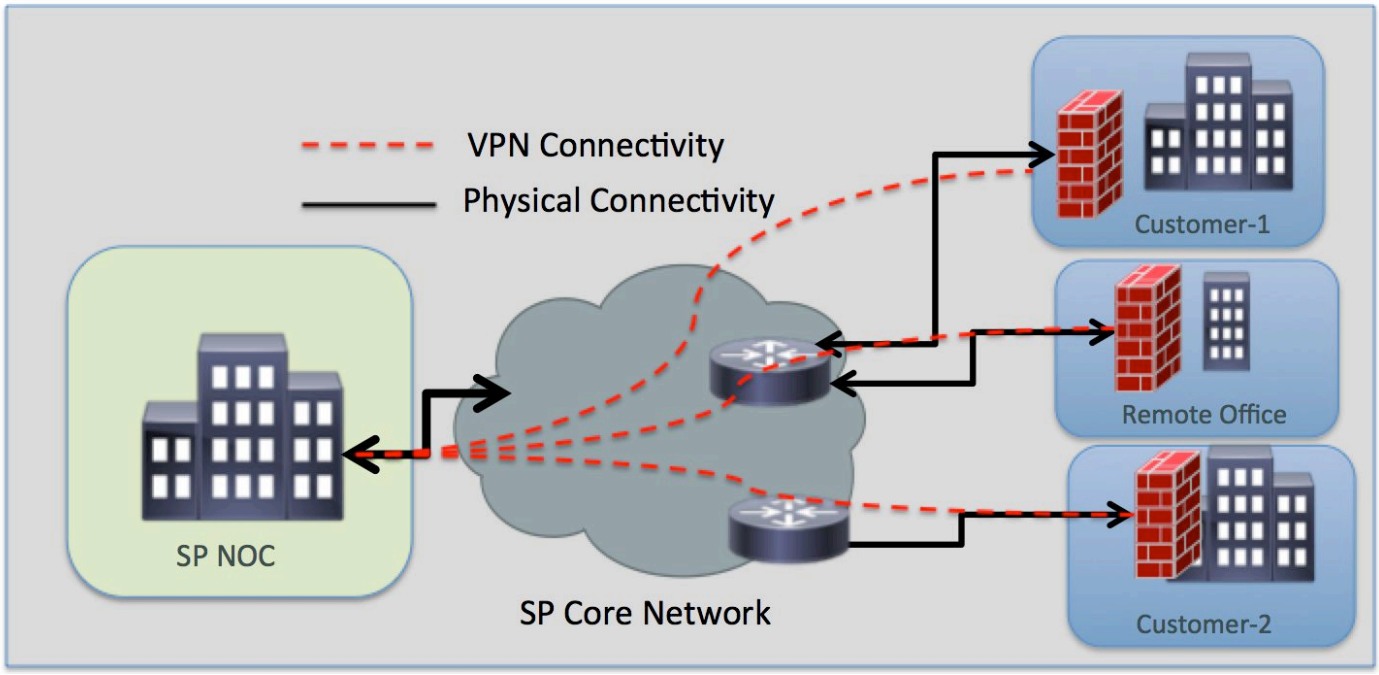
عمارة

المتطلبات

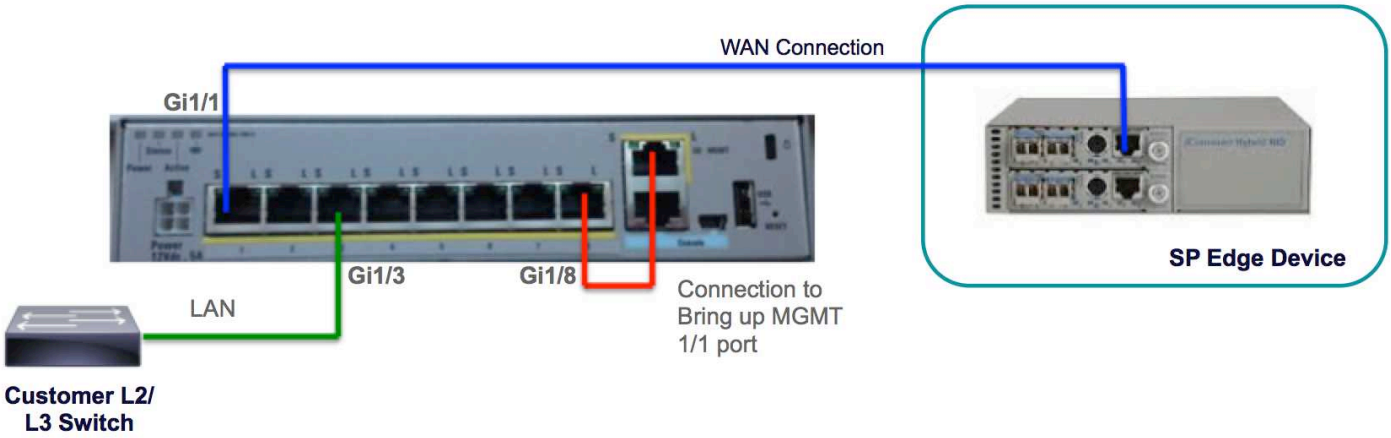
- نقل وصول مخصص واحد للإنترنت من جهاز حافة مزود الخدمة إلى ASA FirePOWER.
- الوصول إلى واجهة الإدارة ضروري لتغيير حالة الواجهة إلى up.
- يجب أن تظل واجهة إدارة ASA عالية حتى تتمكن من إدارة الوحدة النمطية FirePOWER.
- لا يجب فقد اتصال الإدارة إذا قام العميل بقطع اتصال جهاز الشبكة المحلية (LAN).

• يجب أن تدعم بنية الإدارة ميزة التغلب على أعطال شبكة الاتصال واسعة النطاق (WAN) النشطة/الاحتياطية.

نظرة عامة على المخطط



تصميم منخفض المستوى



الحل

تتيح لك التكوينات التالية إدارة وحدة SFR عبر الشبكة الخاصة الظاهرية (VPN) عن بعد، دون أي اتصال بشبكة LAN كشرط مسبق.

توصيل كبلات

• قم بتوصيل واجهة الإدارة 1/1 بواجهة GigabitEthernet1/8 باستخدام كبل إيثرنت.

ملاحظة: يجب أن تستخدم الوحدة النمطية FirePOWER الخاصة ب ASA واجهة Management 1/x (1/0 أو 1/1) لإرسال حركة مرور الإدارة واستقبالها. بما أن الإدارة x/1 قارن ليس على مستوى البيانات، أنت تحتاج أن يحيل طبيعي الإدارة قارن إلى آخر lan أداة to order in مررت حركة مرور عبر ال ASA عبر التحكم مستوى.

كجزء من حل المربع الواحد، ستقوم بتوصيل واجهة الإدارة 1/1 بواجهة GigabitEthernet1/8 باستخدام كبل إيثرنت.

عنوان IP

- **واجهة GigabitEthernet 1/8**: 192.168.10.1/24
- **واجهة إدارة SFR**: 192.168.10.2/24
- **بوابة SFR**: 192.168.10.1
- **واجهة الإدارة 1/1**: لا تحتوي واجهة الإدارة على أي عنوان IP تم تكوينه. يجب تكوين الأمر management-access بغرض الإدارة (MGMT).

ستكون حركة المرور المحلية والبعيدة على الشبكات الفرعية التالية:

- حركة المرور المحلية موجودة على الشبكة الفرعية للإدارة 24/192.168.10.0.
- توجد حركة المرور عن بعد على الشبكة الفرعية 24/192.168.11.0.

الشبكة الخاصة الظاهرية (VPN) وشبكة NAT

- قم بتحديد سياسات شبكات VPN.
- يجب تكوين الأمر nat باستخدام بادئة route-lookup لتحديد واجهة الخروج باستخدام بحث المسار بدلا من إستخدام الواجهة المحددة في الأمر nat.

مثال التكوين

```
!
management-access MGMT
!
interface GigabitEthernet1/1
 nameif outside
 security-level 0
 ip address 10.106.223.1 255.255.255.0
!

interface GigabitEthernet1/8
 nameif MGMT
 security-level 90
 ip address 192.168.10.1 255.255.255.252
!

interface Management1/1
 management-only
 no nameif
 no security-level
 no ip address
!

object network obj_any
 subnet 0.0.0.0 0.0.0.0
object-group network LOCAL-LAN
 network-object 192.168.10.0 255.255.255.0
object-group network REMOTE-LAN
 network-object 192.168.11.0 255.255.255.0
access-list INTREST-TRAFFIC extended permit ip 192.168.10.0 255.255.255.0 192.168.11.0
 255.255.255.0
access-list TEST extended permit tcp any any eq www
```

```
access-list TEST extended permit tcp any any eq https

nat (MGMT,outside) source static LOCAL-LAN LOCAL-LAN destination static REMOTE-LAN REMOTE-LAN
route-lookup

object network obj_any
 nat (any,outside) dynamic interface

route outside 0.0.0.0 0.0.0.0 10.106.223.2 1

crypto ipsec ikev1 transform-set TRANS-SET esp-3des esp-md5-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map CMAP 10 match address INTREST-TRAFFIC
crypto map CMAP 10 set peer 10.106.223.2
crypto map CMAP 10 set ikev1 transform-set TRANS-SET
crypto map CMAP interface outside

crypto ikev1 enable outside
crypto ikev1 policy 10
 authentication pre-share
 encryption 3des
 hash md5
 group 2
 lifetime 86400
!
tunnel-group 10.106.223.1 type ipsec-l2l
tunnel-group 10.106.223.1 ipsec-attributes
***** ikev1 pre-shared-key
!

class-map TEST
 match access-list TEST

policy-map global_policy
 class TEST
 sfr fail-close
!
```

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).