وصول ASA إلى ASDM من واجهة داخلية عبر VPN نفق تكوين مثال

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين نفق VPN من شبكة LAN إلى شبكة LAN باستخدام إثنين من جدران الحماية الخاصة بجهاز الأمان القابل للتكيف (ASA) من Cisco. يعمل مدير أجهزة الأمان المعدلة (ASDM) من Cisco على ASA البعيد من خلال الواجهة الخارجية على الجانب العام، ويقوم بتشفير كل من الشبكة العادية وحركة مرور ASDM. ASDM هي أداة تكوين قائمة على المستعرض تم تصميمها لمساعدتك في إعداد جدار حماية ASA وتكوينه ومراقبته باستخدام واجهة المستخدم الرسومية (GUI). لا تحتاج إلى معرفة شاملة بواجهة سطر الأوامر (CLI) الخاصة بجدار حماية ASA.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تشفير IPsec
- ASDM من Cisco

ملاحظة: تأكد من أن جميع الأجهزة المستخدمة في طبقتك تفي بالمتطلبات الموضحة في دليل تثبت الأجهزة من السلسلة Cisco ASA 5500.

تلميح: ارجع إلى مقال Cisco مقدمة لتشفير أمان IP (IPSec) للحصول على معرفة بتشفير IPsec الأساسي.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- برنامج جدار حماية Cisco ASA الإصدار x.9.
- ASA-1 و ASA-2 هما جدار حماية Cisco ASA 5520
- ASA 2 يستخدم الإصدار 7.2(1) من ASDM

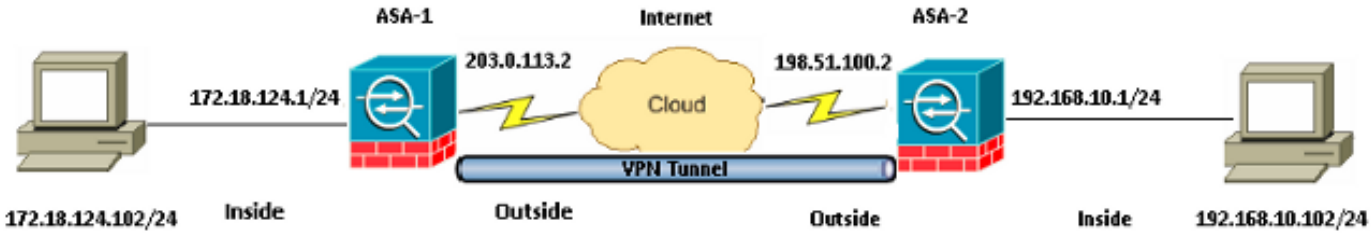
ملاحظة: عندما يطلب منك اسم مستخدم وكلمة مرور ل ASDM، فإن الإعدادات الافتراضية لا تتطلب اسم مستخدم. إن شكلت يمكن كلمة كان سابقا، دخلت أن كلمة بما أن ال ASDM كلمة. إن ليس هناك يمكن كلمة، تركت على حد سواء ال username وكلمة مدخل فارغ وطقطقة **ok** in order to باشرت.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

أستخدم المعلومات الموضحة في هذا القسم لتكوين الميزات الموضحة في هذا المستند.

الرسم التخطيطي للشبكة



التكوينات

هذا هو التكوين الذي يتم إستخدامه على ASA-1:

ASA-1

```
(ASA Version 9.1(5
!
hostname ASA-1
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 203.0.113.2 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 172.18.124.1 255.255.255.0
!
```

```
                                        Traffic matching ACL 101 is punted to VPN ---!
                                        Encrypt/Decrypt traffic matching ACL 101 ---!

access-list 101 extended permit ip 172.18.124.0 255.255.255.0 192.168.10.0
                                                                255.255.255.0

                                                        Do not use NAT ---!
                                                on traffic matching below Identity NAT ---!

                                                  object network obj_192.168.10.0
                                                 subnet 192.168.10.0 255.255.255.0

                                                  object network obj_172.18.124.0
                                                 subnet 172.18.124.0 255.255.255.0

nat (inside,outside) source static obj_172.18.124.0 obj_172.18.124.0 destination
             static obj_192.168.10.0 obj_192.168.10.0 no-proxy-arp route-lookup

                                    .Configures a default route towards the gateway router ---!

                                    route outside 0.0.0.0 0.0.0.0 203.0.113.252 1

                            Point the configuration to the appropriate version of ASDM in flash ---!

                                                    asdm image asdm-722.bin

                                                .Enable the HTTP server required to run ASDM ---!

                                                      http server enable

                                        This is the interface name and IP address of the host or ---!
                                                .network that initiates the HTTP connection ---!

                                    http 172.18.124.102 255.255.255.255 inside

                                        Implicitly permit any packet that came from an IPsec ---!
                                tunnel and bypass the checking of an associated access-group ---!
                                        .command statement for IPsec connections ---!

                                                  sysopt connection permit-vpn

                                        .Specify IPsec (phase 2) transform set ---!
                                          .Specify IPsec (phase 2) attributes ---!

                                crypto ipsec ikev1 transform-set vpn esp-3des esp-md5-hmac
                                     crypto ipsec security-association pmtu-aging infinite
                                                  crypto map vpn 10 match address 101
                                                crypto map vpn 10 set peer 198.51.100.2
                                              crypto map vpn 10 set ikev1 transform-set vpn
                                                  crypto map vpn interface outside

                                                .Specify ISAKMP (phase 1) attributes ---!

                                                    crypto ikev1 enable outside
                                                         crypto ikev1 policy 10
                                                      authentication pre-share
                                                              encryption 3des
                                                                     hash sha
                                                                      group 2
                                                               lifetime 86400

                                                .Specify tunnel-group ipsec attributes ---!

                                                tunnel-group 198.51.100.2 type ipsec-l2l
```

```
tunnel-group 198.51.100.2 ipsec-attributes
ikev1 pre-shared-key cisco
```

هذا التشكيل أن يكون استعملت على ASA-2:

ASA-2

```
(ASA Version 9.1(5
!
hostname ASA-2
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 198.51.100.2 255.255.255.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.10.1 255.255.255.0
!

***Traffic matching ACL 101 is punted to VPN ---!***
***Encrypt/Decrypt traffic matching ACL 101 ---!***

access-list 101 extended permit ip 192.168.10.0 255.255.255.0 172.18.124.0
255.255.255.0

***Do not use NAT ---!***
***on traffic matching below Identity NAT ---!***

object network obj_192.168.10.0
subnet 192.168.10.0 255.255.255.0

object network obj_172.18.124.0
subnet 172.18.124.0 255.255.255.0

nat (inside,outside) source static obj_192.168.10.0 obj_192.168.10.0 destination
static obj_172.18.124.0 obj_172.18.124.0 no-proxy-arp route-lookup

***.Configures a default route towards the gateway router ---!***

route outside 0.0.0.0 0.0.0.0 198.51.100.252 1

***Point the configuration to the appropriate version of ASDM in flash ---!***

asdm image asdm-722.bin

***.Enable the HTTP server required to run ASDM ---!***

http server enable

***This is the interface name and IP address of the host or ---!***
***.network that initiates the HTTP connection ---!***

http 192.168.10.102 255.255.255.255 inside

***Add an aditional 'http' configuration to allow the remote subnet ---!***
**to access ASDM over the VPN tunnel ---!**

http 172.18.124.0 255.255.255.0 outside

***Implicitly permit any packet that came from an IPsec ---!***
```

```
!--- tunnel and bypass the checking of an associated access-group
!--- command statement for IPsec connections.

sysopt connection permit-vpn

!--- Specify IPsec (phase 2) transform set.
!--- Specify IPsec (phase 2) attributes.

crypto ipsec ikev1 transform-set vpn esp-3des esp-md5-hmac
crypto ipsec security-association pmtu-aging infinite
crypto map vpn 10 match address 101
crypto map vpn 10 set peer 203.0.113.2
crypto map vpn 10 set ikev1 transform-set vpn
crypto map vpn interface outside

!--- Specify ISAKMP (phase 1) attributes.

crypto ikev1 enable outside
crypto ikev1 policy 10
authentication pre-share
encryption 3des
hash sha
group 2
lifetime 86400

!--- Specify tunnel-group ipsec attributes.

tunnel-group 203.0.113.2 type ipsec-l2l
tunnel-group 203.0.113.2 ipsec-attributes
ikev1 pre-shared-key cisco
```

الوصول إلى ASDM/SSH عبر نفق VPN

للوصول إلى ASDM عبر الواجهة الداخلية ل ASA-2 من الشبكة الداخلية ASA-1، يجب عليك إستخدام الأمر الموضح هنا. يمكن إستخدام هذا الأمر لواجهة واحدة فقط. في ASA-2، قم بتكوين *management-access* باستخدام الأمر **management-access inside**:

```
management-access
```

التحقق من الصحة

يوفر هذا القسم معلومات يمكنك إستخدامها للتحقق من أن التكوين يعمل بشكل صحيح.

ملاحظة: يدعم Cisco CLI Analyzer (محلل واجهة سطر الأوامر من Cisco) (للعملاء المسجلين فقط) أوامر **show** معينة. استخدم Cisco CLI Analyzer (محلل واجهة سطر الأوامر من Cisco) لعرض تحليل لمُخرَج الأمر **show**.

استعملت هذا أمر in order to دققت تشكيلك:

- أدخل الأمر **show crypto isakmp sa/show isakmp sa** للتحقق من إنشاء المرحلة 1 بشكل صحيح.
- أدخل **show crypto ipSec** للتحقق من قيام المرحلة 2 بشكل صحيح.

ملخص الأوامر

ما إن دخلت ال VPN أمر داخل ال VPN، ASAs خلقت نفق عندما حركة مرور بين ال ASDM pc (172.18.124.102) وال داخلي من ASA-2 (192.168.10.1). عند هذه النقطة، يمكن لجهاز ASDM PC الوصول إلى https://192.168.10.1 والاتصال بواجهة ASDM من ASA-2 عبر نفق VPN.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

ملاحظة: ارجع إلى مشاكل اتصال ASA إلى مقالة مدير أجهزة الأمان المعدلة من Cisco لاستكشاف أخطاء المشكلات المتعلقة ب ASDM وإصلاحها.

إخراج تصحيح الأخطاء للعينة

أدخل الأمر **show crypto isakmp sa** لعرض النفق الذي تم تكوينه بين 198.51.100.2 و 203.0.113.2:

```
ASA-2(config)# show crypto isakmp sa

IKEv1 SAs:

   Active SA: 1
(Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey
   Total IKE SA: 1

IKE Peer: 203.0.113.2   1
Type    : L2L             Role    : initiator
Rekey   : no              State   : MM_ACTIVE
```

أدخل الأمر **show crypto ipSec** لعرض النفق الذي يعبر حركة المرور بين 192.168.10.0 255.255.255.0 و 172. 18.124.0 255.255.255.0:

```
ASA-2(config)# show crypto ipsec sa
                                interface: outside
            Crypto map tag: vpn, seq num: 10, local addr: 198.51.100.2

          access-list 101 extended permit ip 192.168.10.0 255.255.255.0
                                        255.255.255.0 172.18.124.0
       (local ident (addr/mask/prot/port): (192.168.10.0/255.255.255.0/0/0
      (remote ident (addr/mask/prot/port): (172.18.124.0/255.255.255.0/0/0
                                        current_peer: 203.0.113.2

                      pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5#
                      pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5#
                          pkts compressed: 0, #pkts decompressed: 0#
    pkts not compressed: 5, #pkts comp failed: 0, #pkts decomp failed: 0#
     pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0#
PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0#
                                        TFC rcvd: 0, #TFC sent: 0#
            Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0#
                                    send errors: 0, #recv errors: 0#

local crypto endpt.: 198.51.100.2/0, remote crypto endpt.: 203.0.113.2/0
                path mtu 1500, ipsec overhead 58(36), media mtu 1500
                    PMTU time remaining (sec): 0, DF policy: copy-df
```

```
ICMP error validation: disabled, TFC packets: disabled
                                current outbound spi: DDE6AD22
                                current inbound spi : 92425FE5

                                                    :inbound esp sas
                                        (spi: 0x92425FE5 (2453823461
                    transform: esp-3des esp-md5-hmac no compression
                            { ,in use settings ={L2L, Tunnel, IKEv1
                           slot: 0, conn_id: 28672, crypto-map: vpn
    (sa timing: remaining key lifetime (kB/sec): (4373999/28658
                                                    IV size: 8 bytes
                                    replay detection support: Y
                                            :Anti replay bitmap
                                    0x00000000 0x0000003F
                                                :outbound esp sas
                                        (spi: 0xDDE6AD22 (3722882338
                    transform: esp-3des esp-md5-hmac no compression
                            { ,in use settings ={L2L, Tunnel, IKEv1
                           slot: 0, conn_id: 28672, crypto-map: vpn
    (sa timing: remaining key lifetime (kB/sec): (4373999/28658
                                                    IV size: 8 bytes
                                    replay detection support: Y
                                            :Anti replay bitmap
                                    0x00000000 0x00000001
```

معلومات ذات صلة

- مرجع أمر ASA من Cisco
- الدعم التقني والمستندات - Cisco Systems

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).