VPN トンネルを通って内部インターフェイスから ASA による ASDM へのアクセスの設定例

目次

概要

このドキュメントでは、2 つの Cisco 適応型セキュリティ アプライアンス（ASA）ファイアウォールを使用して、LAN 間 VPN トンネルを設定する方法について説明します。 Cisco Adaptive Security Device Manager（ASDM）は、パブリック側の外部インターフェイスを介してリモート ASA で実行され、通常のネットワーク トラフィックと ASDM トラフィックの両方を暗号化します。 ASDM は、GUI を使用した ASA ファイアウォールのセットアップ、設定、およびモニタするために設計されているブラウザベースの設定ツールです。 ASA ファイアウォール CLI の広範な知識は必要ありません。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- IPSec 暗号化
- Cisco ASDM

注: トポロジで使用されているすべてのデバイスが、「Cisco ASA 5500 シリーズ ハードウェア インストレーション ガイド」で説明されている要件を満たすようにしてください。

ヒント： IPsec 暗号化の基本を理解するには、Cisco の記事「IP Security（IPSec）暗号化の概要」を参照してください。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco ASA ファイアウォール ソフトウェア リリース 9.x。
- ASA-1 および ASA-2 は Cisco ASA ファイアウォール 5520 です。
- ASA 2 では ASDM バージョン 7.2(1) を使用しています。

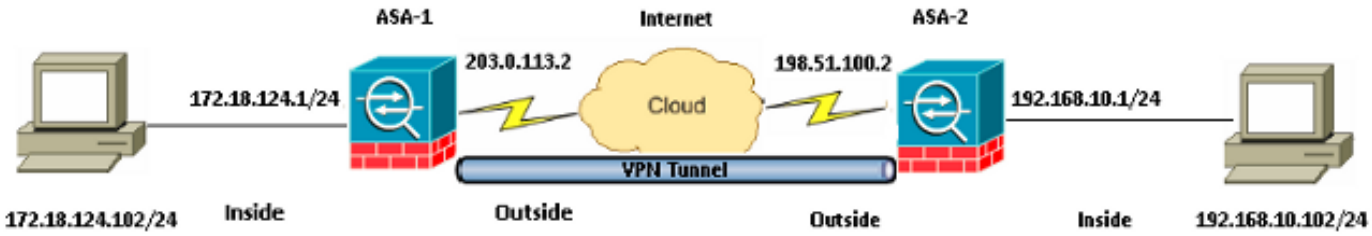
  注: ASDM のユーザ名とパスワードの入力を求められた場合、デフォルト設定ではユーザ名は必要ありません。 イネーブル パスワードを以前に設定していた場合は、そのパスワードを ASDM パスワードとして入力します。 イネーブル パスワードがない場合は、ユーザ名とパスワードの両方とも空白のままにして、[OK] をクリックして続行します。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

設定

このドキュメントで説明している機能を設定するには、この項で説明している情報を使用します。

ネットワーク図



設定

ASA-1 で使用されている構成を次に示します。

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
```

ASA-2 で使用されている構成を次に示します。

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
```

VPN トンネルを通じた ASDM/SSH へのアクセス

ASA 1 の内部ネットワークから ASA 2 の内部インターフェイスを介して ASDM にアクセスするには、ここで説明しているコマンドを使用する必要があります。 このコマンドを使用できるのは、1 つのインターフェイスに対してだけです。 ASA-2 上で、次のように **management-access inside** コマンドを使用して、*management-access* を設定します。

```
management-access <interface-name>
```

確認

この項では、設定が正しく機能していることを検証するために使用できる情報を提供します。

> **注:** Cisco CLI アナライザ（登録ユーザ専用）は、特定の **show** コマンドをサポートしています。 **show** コマンド出力の分析を表示するには、Cisco CLI アナライザを使用します。

以下のコマンドを使用して、設定を検証します。

- フェーズ 1 が正しく確立されていることを検証するには、**show crypto isakmp sa/show isakmp sa** コマンドを入力します。
- フェーズ 2 が正しく確立されていることを検証するには、**show crypto ipsec sa** を入力します。

コマンドの概要

VPN コマンドを各 ASA に入力すると、ASDM PC (172.18.124.102) と ASA-2 の内部インターフェイス (192.168.10.1) との間をトラフィックが通過するときに、VPN トンネルが確立されます。 この時点で、ASDM PC は VPN トンネルを介して https://192.168.10.1 に到達して、ASA-2 の ASDM インターフェイスと通信できるようになります。

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

> **注:** ASDM 関連の問題をトラブルシューティングするには、シスコの記事「Cisco Adaptive Security Device Manager への ASA の接続の問題」を参照してください。

debug 出力例

198.51.100.2 と 203.0.113.2 の間で形成されたトンネルを表示するには、次に示すように **show crypto isakmp sa** コマンドを入力します。

```
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

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

トンネルを表示するために 192.168.10.0 255.255.255.0 および 172 の間でトラフィックを通過させる **show crypto ipsec sa コマンドを**入力して下さい。 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
172.18.124.0 255.255.255.0
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
```

関連情報

- Cisco ASA コマンド リファレンス
- テクニカルサポートとドキュメント - Cisco Systems