ASA Access à l'ASDM d'une interface interne au-dessus d'un exemple de configuration de tunnel VPN

Contenu

Introduction

Ce document décrit comment configurer un tunnel VPN d'entre réseaux locaux avec l'utilisation de deux Pare-feu de l'appliance de sécurité adaptable Cisco (ASA). Le Cisco Adaptive Security Device Manager (ASDM) s'exécute là-dessus le distant ASA par l'interface extérieure du côté public, et chiffre le réseau régulier et le trafic ASDM. L'ASDM est un outil de configuration basé sur navigateur qui est conçu afin de vous aider à installer, configurer, et surveiller votre Pare-feu ASA avec un GUI. Vous n'avez pas besoin de la connaissance étendue du Pare-feu CLI ASA.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cryptage d'IPsec
- Cisco ASDM

Remarque: Assurez-vous que tous les périphériques qui sont utilisés dans votre topologie répondent aux exigences qui sont décrites dans le guide d'installation du matériel de gamme de Cisco ASA 5500.

Conseil : Référez-vous à une introduction à l'article de Cisco de cryptage de sécurité IP (IPSec) afin de gagner la connaissance du cryptage de base d'IPsec.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Pare-feu, version 9.x de Cisco ASA.
- ASA-1 et ASA-2 sont le Pare-feu 5520 de Cisco ASA
- Version 7.2(1) des utilisations ASDM ASA 2

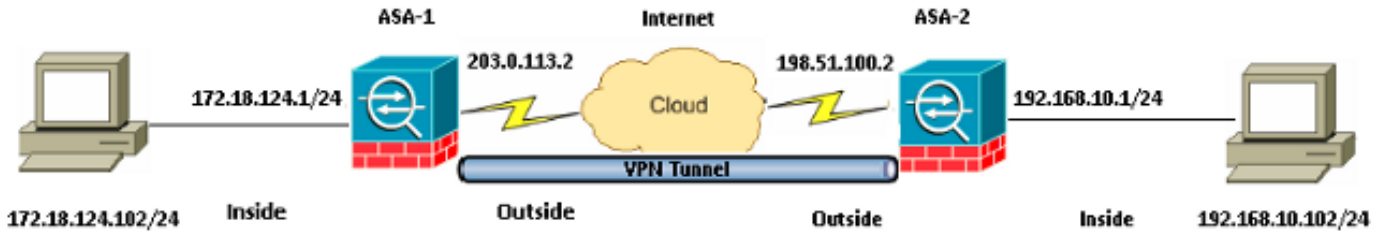
  Remarque: Quand vous êtes incité pour un nom d'utilisateur et mot de passe pour l'ASDM, les valeurs par défaut n'exigent pas un nom d'utilisateur. Si un mot de passe d'enable était précédemment configuré, entrez ce mot de passe comme mot de passe ASDM. S'il n'y a aucun mot de passe d'enable, laissez le les deux le blanc d'entrées de nom d'utilisateur et mot de passe et cliquez sur OK afin de continuer.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Utilisez les informations qui sont décrites dans cette section afin de configurer les caractéristiques qui sont décrites dans ce document.

Diagramme du réseau



Configurations

C'est la configuration qui est utilisée sur 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
```

C'est la configuration qui est utilisée sur 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
```

Access ASDM/SSH à travers un tunnel VPN

Afin d'accéder à l'ASDM par l'intermédiaire de l'interface interne d'ASA-2 de l'ASA-1 à l'intérieur du réseau, vous devez utiliser la commande qui est décrite ici. Cette commande peut seulement être utilisée pour une interface. Sur ASA-2, configurez Gestion-*Access* avec Gestion-**Access à l'intérieur de** commande :

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

Vérifiez

Cette section fournit les informations que vous pouvez employer afin de vérifier que votre configuration fonctionne correctement.

> Remarque: L'analyseur de Cisco CLI (clients enregistrés seulement) prend en charge certaines **commandes show**. Employez l'analyseur de Cisco CLI afin de visualiser une analyse de sortie de commande show.

Employez ces commandes afin de vérifier votre configuration :

- Sélectionnez la commande d'**ISAKMP SA du crypto isakmp sa/show d'exposition** afin de vérifier que le Phase 1 établit correctement.
- Entrez dans le **show crypto ipsec sa** afin de vérifier que le Phase 2 établit correctement.

Résumé des commandes

Une fois que les commandes VPN sont sélectionnées dans les ASA, un tunnel VPN est établi quand le trafic passe entre le PC ASDM (172.18.124.102) et l'interface interne d'ASA-2 (192.168.10.1). En ce moment, le PC ASDM peut atteindre https://192.168.10.1 et communiquer avec l'interface ASDM d'ASA-2 au-dessus du tunnel VPN.

Dépannez

Cette section fournit les informations que vous pouvez employer afin de dépanner votre configuration.

> Remarque: Référez-vous aux problèmes de connexion ASA à l'article de Cisco de Cisco Adaptive Security Device Manager afin de dépanner les questions liées à l'ASDM.

Exemple de sortie de débogage

Sélectionnez la commande de **show crypto isakmp sa** afin de visualiser le tunnel qui est formé entre 198.51.100.2 et 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

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

Sélectionnez la commande de **show crypto ipsec sa** afin de visualiser le tunnel qui passe le trafic entre 192.168.10.0 255.255.255.0 et 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
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
```

Informations connexes

- Référence des commandes Cisco ASA
- Support et documentation techniques - Cisco Systems