Acceso ASA al ASDM de una interfaz interior sobre un ejemplo de la configuración del túnel VPN

Contenido

Introducción

Este documento describe cómo configurar un túnel VPN de LAN a LAN con el uso de dos Firewall adaptantes del dispositivo de seguridad de Cisco (ASA). El Cisco Adaptive Security Device Manager (ASDM) se ejecuta en el telecontrol ASA a través de la interfaz exterior en el lado público, y él cifra la red común y el tráfico del ASDM. El ASDM es una herramienta de configuración basada en buscador que se diseña para ayudarle a configurar, a configurar, y a monitorear su Firewall ASA con un GUI. Usted no necesita el tener demasiado conocimiento del Firewall CLI ASA.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Encripción de IPSec
- ASDM de Cisco

Nota: Asegúrese de que todos los dispositivos que se utilizan en su topología cumplan los requisitos que se describen en el guía de instalación del hardware de las 5500 Series de Cisco ASA.

Consejo: Refiera a un artículo de Cisco de la Introducción al encripción de seguridad IP

(IPSec) para ganar la familiaridad con la encripción de IPSec básica.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión de software de firewall de Cisco ASA 9.x.
- ASA-1 y ASA-2 son el Firewall 5520 de Cisco ASA
- Versión 7.2(1) del ASDM de las aplicaciones ASA 2

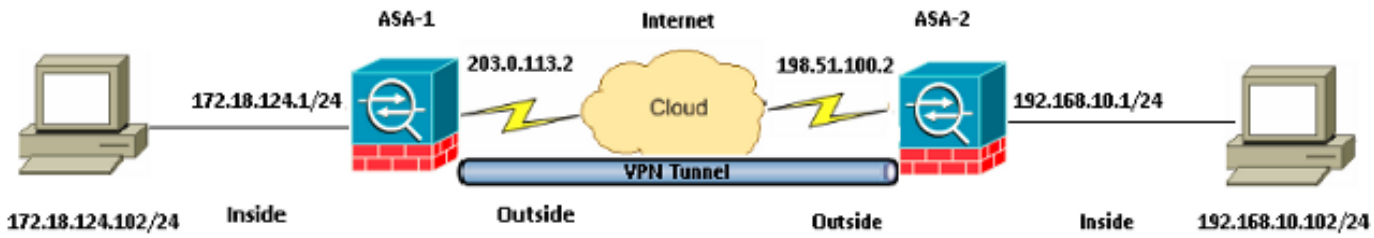
  Nota: Cuando le indican para un nombre de usuario y contraseña para el ASDM, las configuraciones predeterminadas no requieren un nombre de usuario. Si una contraseña habilitada fue configurada previamente, ingrese esa contraseña como la contraseña del ASDM. Si no hay contraseña habilitada, deje ambo el espacio en blanco de entradas del nombre de usuario y contraseña y haga clic la **AUTORIZACIÓN** para continuar.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Utilice la información que se describe en esta sección para configurar las características que se describen en este documento.

Diagrama de la red



Configuraciones

Ésta es la configuración que se utiliza en 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
```

Ésta es la configuración que se utiliza en 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
```

Acceso ASDM/SSH a través de un túnel VPN

Para acceder el ASDM vía la interfaz interior de ASA-2 de la red interna ASA-1, usted debe utilizar el comando que se describe aquí. Este comando se puede utilizar solamente para una interfaz. En ASA-2, *Acceso de administración de la* configuración con el **Acceso de administración dentro del** comando:

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

Verificación

Esta sección proporciona la información que usted puede utilizar para verificar que su configuración trabaja correctamente.

> Nota: El analizador del CLI de Cisco (clientes registrados solamente) apoya los ciertos comandos show. Utilice el analizador del CLI de Cisco para ver una análisis de la salida del comando show.

Utilice estos comandos para verificar su configuración:

- Ingrese el comando **crypto isakmp sa del isakmp sa/show de la demostración** para verificar que la fase 1 establece correctamente.
- Ingrese **IPSec crypto sa de la demostración** para verificar que la fase 2 establece correctamente.

Resumen de Comandos

Una vez que los comandos VPN se ingresan en los ASA, se establece un túnel VPN cuando el tráfico pasa entre el ASDM PC (172.18.124.102) y la interfaz interior de ASA-2 (192.168.10.1). En este momento, el ASDM PC puede alcanzar https://192.168.10.1 y comunicar con la interfaz del ASDM de ASA-2 sobre el túnel VPN.

Troubleshooting

Esta sección proporciona la información que usted puede utilizar para resolver problemas su configuración.

> Nota: Refiera a los Problemas de conexión ASA al artículo de Cisco del Cisco Adaptive Security Device Manager para resolver problemas los problemas ASDM-relacionados.

Ejemplo de resultado del comando debug

Ingrese el **comando show crypto isakmp sa** para ver el túnel que se forma entre 198.51.100.2 y 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
```

Ingrese el **comando show crypto ipsec sa** para ver el túnel que pasa el tráfico entre 192.168.10.0 255.255.255.0 y 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
```

Información Relacionada

- Referencia de comandos de Cisco ASA
- Soporte Técnico y Documentación - Cisco Systems