Acesso ASA ao ASDM de uma interface interna sobre um exemplo da configuração de túnel VPN

Índice

Introdução

Este documento descreve como configurar um Túnel VPN de Lan para Lan com o uso de dois Firewall adaptáveis da ferramenta de segurança de Cisco (ASA). O Cisco Adaptive Security Device Manager (ASDM) é executado no ASA remoto através da interface externa no lado público, e nele cifra a rede regular e o tráfego ASDM. O ASDM é uma ferramenta de configuração com base em navegador que seja projetada a fim o ajudar a estabelecer, configurar, e monitorar seu Firewall ASA com um GUI. Você não precisa o conhecimento profundo do Firewall CLI ASA.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Criptografia IPSec
- Cisco ASDM

Nota: Assegure-se de que todos os dispositivos que são usados em sua topologia cumpram as exigências que são descritas no guia de instalação de hardware do 5500 Series de Cisco ASA.

Dica: Refira um artigo de Cisco da introdução à criptografia do protocolo de segurança IP (IPSEC) a fim ganhar a familiaridade com a criptografia IPSec básica.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Liberação de software de firewall 9.x de Cisco ASA.
- ASA-1 e ASA-2 são o Firewall 5520 de Cisco ASA
- Versão 7.2(1) dos usos ASDM ASA 2

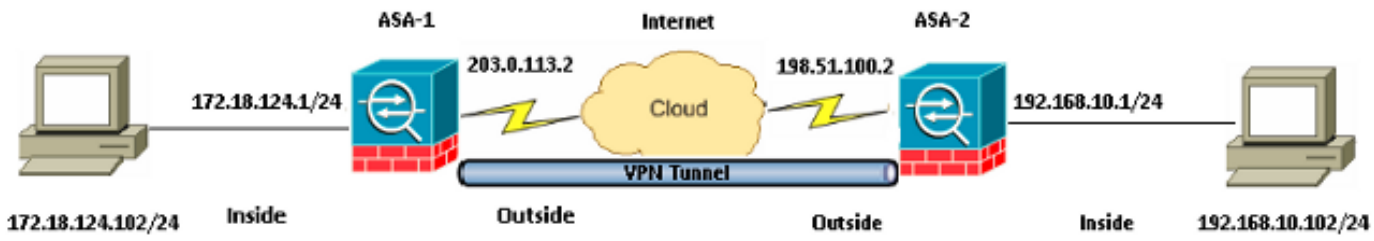
  Nota: Quando você é alertado para um nome de usuário e senha para o ASDM, as configurações padrão não exigem um username. Se uma senha da possibilidade foi configurada previamente, incorpore essa senha como a senha ASDM. Se há nenhum permite a senha, sae de amba a placa de entradas do nome de usuário e senha e clique a **APROVAÇÃO** a fim continuar.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Use a informação que é descrita nesta seção a fim configurar as características que são descritas neste documento.

Diagrama de Rede



Configurações

Esta é a configuração que é usada em 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
```

Esta é a configuração que é usada em 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
```

Alcance ASDM/SSH através de um túnel VPN

A fim alcançar o ASDM através da interface interna de ASA-2 da rede interna ASA-1, você deve usar o comando que é descrito aqui. Este comando pode somente ser usado para uma relação. Em ASA-2, configurar o *acesso de gerenciamento* com o **acesso de gerenciamento dentro do** comando:

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

Verificar

Esta seção fornece a informação que você pode usar a fim verificar que sua configuração trabalha corretamente.

> Nota: O analisador do CLI Cisco (clientes registrados somente) apoia determinados comandos de exibição. Use o analisador do CLI Cisco a fim ver uma análise do emissor de comando de execução.

Use estes comandos a fim verificar sua configuração:

- Incorpore o comando **cripto isakmp sa do isakmp sa/show da mostra** a fim verificar que a fase 1 estabelece corretamente.

- Entre **IPsec cripto sa da mostra** a fim verificar que a fase 2 estabelece corretamente.

Resumo de comandos

Uma vez que os comandos VPN são incorporados nos ASA, um túnel VPN está estabelecido quando o tráfego passa entre o ASDM PC (172.18.124.102) e a interface interna de ASA-2 (192.168.10.1). Neste momento, o ASDM PC pode alcançar https://192.168.10.1 e comunicar-se com a relação ASDM de ASA-2 sobre o túnel VPN.

Troubleshooting

Esta seção fornece a informação que você pode usar a fim pesquisar defeitos sua configuração.

> Nota: Refira os problemas de conexão ASA ao artigo de Cisco do Cisco Adaptive Security Device Manager a fim pesquisar defeitos edições ASDM-relacionadas.

Exemplo de debug

Inscreva o **comando show crypto isakmp sa** a fim ver o túnel que é formado entre 198.51.100.2 e 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
```

Inscreva o **comando show crypto ipsec sa** a fim ver o túnel que passa o tráfego entre 192.168.10.0 255.255.255.0 e 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
```

Informações Relacionadas

- Referência de comandos de Cisco ASA
- Suporte Técnico e Documentação - Cisco Systems