ASA-Zugriff von einer internen Schnittstelle über ein VPN-Tunnel-Konfigurationsbeispiel

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Konfigurieren](#)
[Netzwerkdiagramm](#)
[Konfigurationen](#)
[Zugriff auf ASDM/SSH über einen VPN-Tunnel](#)
[Überprüfen](#)
[Befehlsübersicht](#)
[Fehlerbehebung](#)
[Beispielausgabe für Debugging](#)
[Zugehörige Informationen](#)

Einführung

Dieses Dokument beschreibt die Konfiguration eines LAN-zu-LAN VPN-Tunnels mithilfe von zwei Cisco Adaptive Security Appliance (ASA)-Firewalls. Der Cisco Adaptive Security Device Manager (ASDM) wird auf der Remote-ASA über die externe Schnittstelle auf der öffentlichen Seite ausgeführt und verschlüsselt sowohl regulären Netzwerk- als auch ASDM-Datenverkehr. Das ASDM ist ein browserbasiertes Konfigurationstool, das Sie beim Einrichten, Konfigurieren und Überwachen Ihrer ASA-Firewall über eine grafische Benutzeroberfläche unterstützen soll. Sie benötigen keine umfassenden Kenntnisse der ASA Firewall CLI.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- IPsec-Verschlüsselung
- Cisco ASDM

Hinweis: Stellen Sie sicher, dass alle in Ihrer Topologie verwendeten Geräte die im Hardware-Installationsleitfaden der Cisco Serie ASA 5500 beschriebenen Anforderungen erfüllen.

Tipp: Lesen Sie den Artikel An Introduction to IP Security (IPSec) Encryption Cisco, um sich mit der grundlegenden IPsec-Verschlüsselung vertraut zu machen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ASA Firewall Software Version 9.x
- ASA-1 und ASA-2 sind Cisco ASA Firewall 5520
- ASA 2 verwendet ASDM Version 7.2(1)

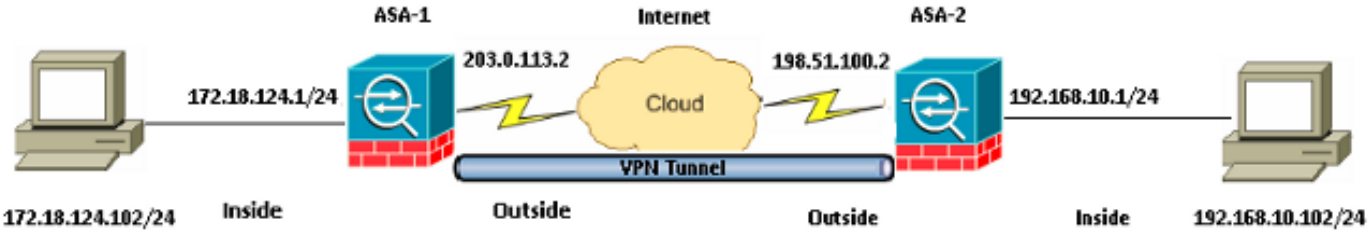
  Hinweis: Wenn Sie zur Eingabe eines Benutzernamens und eines Kennworts für den ASDM aufgefordert werden, ist für die Standardeinstellungen kein Benutzername erforderlich. Wenn zuvor ein Aktivierungskennwort konfiguriert wurde, geben Sie dieses als ASDM-Kennwort ein. Wenn das Kennwort nicht aktiviert ist, lassen Sie die Einträge für den Benutzernamen und das Kennwort leer, und klicken Sie auf **OK**, um fortzufahren.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Mithilfe der in diesem Abschnitt beschriebenen Informationen können Sie die in diesem Dokument beschriebenen Funktionen konfigurieren.

Netzwerkdiagramm



Konfigurationen

Dies ist die Konfiguration, die auf ASA-1 verwendet wird:

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
```

Dies ist die Konfiguration, die auf ASA-2 verwendet wird:

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
```

Zugriff auf ASDM/SSH über einen VPN-Tunnel

Um über die interne Schnittstelle von ASA-2 aus dem ASA-1-internen Netzwerk auf das ASDM zuzugreifen, müssen Sie den hier beschriebenen Befehl verwenden. Dieser Befehl kann nur für eine Schnittstelle verwendet werden. Konfigurieren Sie auf ASA-2 den *Management-Zugriff* mit dem Befehl **management-access inside**:

```
management-access
```

Überprüfen

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Hinweis: Der Cisco CLI Analyzer (nur registrierte Kunden) unterstützt bestimmte **Show-**

Befehle. Verwenden Sie den Cisco CLI Analyzer, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Verwenden Sie die folgenden Befehle, um Ihre Konfiguration zu überprüfen:

- Geben Sie den Befehl **show crypto isakmp sa/show isakmp sa** ein, um zu überprüfen, ob Phase 1 korrekt eingerichtet wurde.
- Geben Sie die **show crypto ipsec sa ein**, um zu überprüfen, ob Phase 2 korrekt eingerichtet wurde.

Befehlsübersicht

Sobald die VPN-Befehle in die ASAs eingegeben wurden, wird ein VPN-Tunnel eingerichtet, wenn der Datenverkehr zwischen dem ASDM-PC (172.18.124.102) und der internen Schnittstelle von ASA-2 (192.168.10.1) verläuft. An diesem Punkt kann der ASDM-PC https://192.168.10.1 erreichen und über den VPN-Tunnel mit der ASDM-Schnittstelle von ASA-2 kommunizieren.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung in Ihrer Konfiguration verwenden können.

> **Hinweis**: Informationen zur Behebung von ASDM-Problemen finden Sie im Cisco Adaptive Security Device Manager-Artikel zur Behebung von ASDM-bezogenen Problemen.

Beispielausgabe für Debugging

Geben Sie den Befehl **show crypto isakmp sa** ein, um den Tunnel anzuzeigen, der zwischen 198.51.100.2 und 203.0.113.2 gebildet wird:

```
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
```

Geben Sie den Befehl **show crypto ipsec sa** ein, um den Tunnel anzuzeigen, der den Datenverkehr zwischen 192.168.10.0 und 255.255.0 und 172 übergibt. 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
```

Zugehörige Informationen

- Cisco ASA-Befehlsreferenz
- Technischer Support und Dokumentation - Cisco Systems