Een site-to-site IPsec IKEv1-tunnel configureren tussen een ASA en een Cisco IOS-router

Inhoud

Inleiding

Dit document beschrijft hoe u een site-to-site (LAN-to-LAN) IKEv1-tunnel via de CLI kunt configureren tussen een Cisco ASA en een router waarop Cisco IOS®-software wordt uitgevoerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco IOS
- Cisco adaptieve security applicatie (ASA)
- Algemene IPSec-concepten

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 5512-X Series ASA waarop software versie 9.4(1) wordt uitgevoerd
- Cisco 1941 Series geïntegreerde services router (ISR) die Cisco IOS-softwareversie 15.4(3)M2 uitvoert

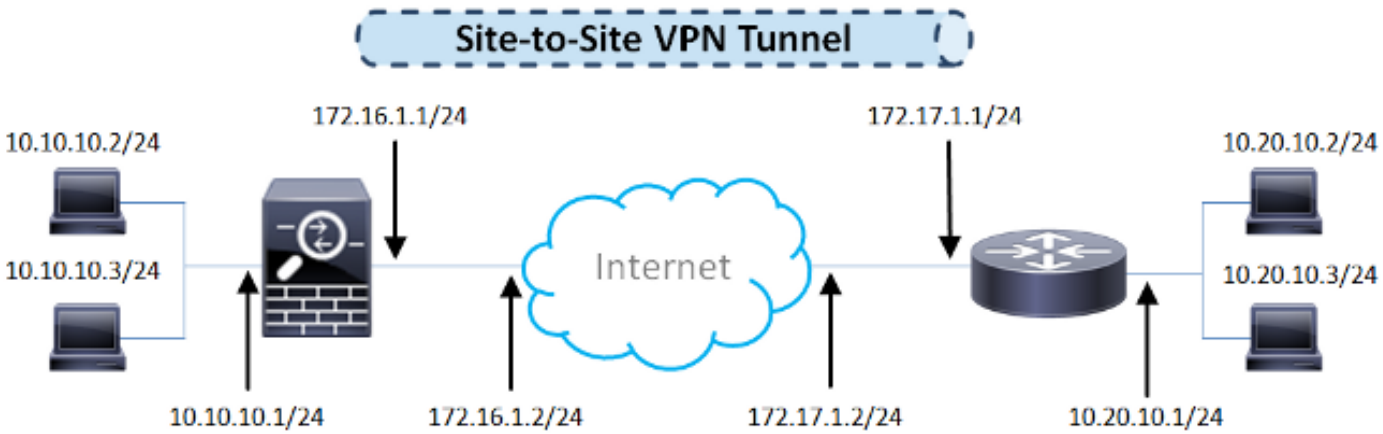
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

In deze sectie wordt beschreven hoe de ASA en Cisco IOS router CLI-configuraties moeten worden voltooid.

Netwerkdiagram

Voor de informatie in dit document wordt gebruik gemaakt van deze netwerkinstelling:



ASA-configuratie

De ASA-interfaces configureren

Als de ASA interfaces niet geconfigureerd zijn, zorg er dan voor dat u ten minste de IP-adressen, interfacenamen en de beveiligingsniveaus configureert:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
```

> **Opmerking**: Zorg ervoor dat er connectiviteit is met zowel de interne als externe netwerken, met name met de externe peer die wordt gebruikt om een site-to-site VPN-tunnel te maken. U kunt gebruiken pingelt om basisconnectiviteit te verifiëren.

Het IKEv1-beleid configureren en IKEv1 aan de buiteninterface inschakelen

Om het beleid van Internet Security Association en Key Management Protocol (ISAKMP) voor de verbindingen met IPSec Internet Key Exchange versie 1 (IKEv1) te configureren, voert u het volgende in: `crypto ikev1 policy` opdracht:

```
crypto ikev1 policy 10
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
```

> **Opmerking:** er bestaat een IKEv1-beleidsovereenkomst wanneer beide beleidsregels van de twee peers dezelfde authenticatie-, encryptie-, hash- en Diffie-Hellman-parameterwaarden bevatten. Voor IKEv1 moet het beleid van de externe peer ook een levensduur specificeren die kleiner is dan of gelijk is aan de levensduur in het beleid dat de initiator verzendt. Als de levensduur niet identiek is, gebruikt de ASA de kortere levensduur.

> **N.B.:** Als u geen waarde opgeeft voor een bepaalde beleidsparameter, wordt de standaardwaarde toegepast.

U moet IKEv1 inschakelen op de interface die de VPN-tunnel beëindigt. Meestal is dit de externe (of openbare) interface. Als u IKEv1 wilt inschakelen, voert u de `crypto ikev1 enable` opdracht in globale configuratiemodus:

```
crypto ikev1 enable outside
```

De tunnelgroep configureren (LAN-naar-LAN-verbindingsprofiel)

Voor een LAN-to-LAN-tunnel is het type verbindingsprofiel `ipsec-l2l` . Om de IKEv1 preshared sleutel te configureren, voert u de `tunnel-group ipsec-attributes` configuratiemodus:

```
tunnel-group 172.17.1.1 type ipsec-l2l
tunnel-group 172.17.1.1 ipsec-attributes
 ikev1 pre-shared-key cisco123
```

Configureer de ACL voor het VPN-verkeer van belang

ASA gebruikt ACL's (Access Control Lists) om het verkeer dat met IPSec-encryptie moet worden beveiligd, te onderscheiden van het verkeer dat geen bescherming nodig heeft. Het beschermt de uitgaande pakketten die overeenkomen met een licentie Application Control Engine (ACE) en zorgt ervoor dat de inkomende pakketten die overeenkomen met een licentie ACE bescherming hebben.

```
object-group network local-network
 network-object 10.10.10.0 255.255.255.0
object-group network remote-network
 network-object 10.20.10.0 255.255.255.0

access-list asa-router-vpn extended permit ip object-group local-network
object-group remote-network
```

> **N.B.:** Een ACL voor VPN-verkeer gebruikt de IP-adressen van bron en bestemming na netwerkadresomzetting (NAT).

> **Opmerking:** er moet een ACL voor VPN-verkeer op beide VPN-peers worden gespiegeld.

> **Opmerking:** Als er een noodzaak is om een nieuw subnetnummer toe te voegen aan het beveiligde verkeer, voeg dan gewoon een subnetnummer/host toe aan de betreffende objectgroep en voltooi een spiegelwijziging op de externe VPN-peer.

Een NAT-vrijstelling configureren

> **Opmerking**: de configuratie die in deze sectie wordt beschreven, is optioneel.

Typisch, moet er geen NAT zijn die op het VPN-verkeer wordt uitgevoerd. Om dat verkeer vrij te stellen, moet u een NAT-regel voor identiteit maken. De identiteitsNAT-regel vertaalt eenvoudig een adres naar hetzelfde adres.

```
nat (inside,outside) source static local-network local-network destination static
remote-network remote-network no-proxy-arp route-lookup
```

De IKEv1-transformatieset configureren

Een IKEv1-transformatieset is een combinatie van beveiligingsprotocollen en algoritmen die definiëren hoe de ASA gegevens beschermt. Tijdens onderhandelingen met IPSec Security Association (SA) moeten de peers een transformatieset of voorstel identificeren die voor beide peers hetzelfde is. ASA past dan de aangepaste transformatieset of het voorstel toe om een SA te creëren die gegevensstromen in de toegangslijst voor die cryptokaart beschermt.

Typ de volgende informatie om de IKEv1-transformatieset te configureren: `crypto ipsec ikev1 transform-set` opdracht:

```
crypto ipsec ikev1 transform-set ESP-AES-SHA esp-aes esp-sha-hmac
```

Configureer een Crypto-kaart en pas deze toe op een interface

Een crypto-kaart definieert een IPSec-beleid waarover in IPSec SA moet worden onderhandeld, en omvat:

- Een toegangslijst om de pakketten te identificeren die door de IPSec-verbinding worden toegestaan en beschermd
- Identificatie van peers
- Een lokaal adres voor het IPSec-verkeer
- De IKEv1-transformatiesets

Hierna volgt een voorbeeld:

```
crypto map outside_map 10 match address asa-router-vpn
crypto map outside_map 10 set peer 172.17.1.1
crypto map outside_map 10 set ikev1 transform-set ESP-AES-SHA
```

U kunt dan de crypto kaart op de interface toepassen:

```
crypto map outside_map interface outside
```

ASA definitieve configuratie

Hier is de definitieve configuratie van de ASA:

```
interface GigabitEthernet0/0
 nameif outside
 security-level 0
```

```
 ip address 172.16.1.1 255.255.255.0
!
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 10.10.10.1 255.255.255.0
!
object-group network local-network
 network-object 10.10.10.0 255.255.255.0
object-group network remote-network
 network-object 10.20.10.0 255.255.255.0
!
access-list asa-router-vpn extended permit ip object-group local-network
object-group remote-network
!
nat (inside,outside) source static local-network local-network destination
static remote-network remote-network no-proxy-arp route-lookup
!
crypto ipsec ikev1 transform-set ESP-AES-SHA esp-aes esp-sha-hmac
!
crypto map outside_map 10 match address asa-router-vpn
crypto map outside_map 10 set peer 172.17.1.1
crypto map outside_map 10 set ikev1 transform-set ESP-AES-SHA
crypto map outside_map interface outside
```

Cisco IOS-router CLI-configuratie

De interfaces configureren

Als de Cisco IOS-routerinterfaces nog niet zijn geconfigureerd, moeten ten minste de LAN- en WAN-interfaces worden geconfigureerd. Hierna volgt een voorbeeld:

```
interface GigabitEthernet0/0
 ip address 172.17.1.1 255.255.255.0
no shutdown
!
interface GigabitEthernet0/1
 ip address 10.20.10.1 255.255.255.0
no shutdown
```

Zorg ervoor dat er connectiviteit is met zowel de interne als externe netwerken, vooral met de externe peer die wordt gebruikt om een site-to-site VPN-tunnel te maken. U kunt gebruiken pingelt om basisconnectiviteit te verifiëren.

Het ISAKMP-beleid (IKEv1) configureren

Om het ISAKMP-beleid voor de IKEv1-verbindingen te configureren, voert u het volgende in: crypto isakmp policy opdracht in globale configuratiemodus. Hierna volgt een voorbeeld:

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
```

```
 group 2
```

Opmerking: u kunt meerdere IKE-beleidsregels configureren op elke peer die deelneemt aan IPSec. Wanneer de IKE-onderhandeling begint, probeert deze een gemeenschappelijk beleid te vinden dat op beide peers is geconfigureerd, en begint de onderhandeling met de hoogste prioriteit die op de externe peer is gespecificeerd.

Een Crypto ISAKMP-toets configureren

Om een vooraf gedeelde verificatiesleutel te configureren, voert u de crypto isakmp key opdracht in globale configuratiemodus:

```
crypto isakmp key cisco123 address 172.16.1.1
```

Configureer een ACL voor VPN-verkeer van belang

Gebruik de uitgebreide of benoemde toegangslijst om het verkeer op te geven dat door codering moet worden beveiligd. Hierna volgt een voorbeeld:

```
access-list 110 remark Interesting traffic access-list
access-list 110 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
```

N.B.: Een ACL voor VPN-verkeer gebruikt de IP-adressen van bron en bestemming na NAT.

Opmerking: er moet een ACL voor VPN-verkeer op beide VPN-peers worden gespiegeld.

Een NAT-vrijstelling configureren

Opmerking: de configuratie die in deze sectie wordt beschreven, is optioneel.

Typisch, moet er geen NAT zijn die op het VPN-verkeer wordt uitgevoerd. Als de NAT-overbelasting wordt gebruikt, moet een routekaart worden gebruikt om het VPN-verkeer dat van belang is, van vertaling vrij te stellen. Bericht dat in de toegang-lijst die in de route-kaart wordt gebruikt, het verkeer van VPN van belang moet worden ontkend.

```
access-list 111 remark NAT exemption access-list
access-list 111 deny   ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 permit ip 10.20.10.0 0.0.0.255 any

route-map nonat permit 10
 match ip address 111

ip nat inside source route-map nonat interface GigabitEthernet0/0 overload
```

Een transformatieset configureren

Voer de volgende handelingen in om een IPSec-transformatieset (een aanvaardbare combinatie van beveiligingsprotocollen en -algoritmen) te definiëren: crypto ipsec transform-set opdracht in globale configuratiemodus. Hierna volgt een voorbeeld:

```
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
```

Configureer een Crypto-kaart en pas deze toe op een interface

Om een crypto kaartingang te creëren of te wijzigen en de crypto kaartconfiguratiewijze in te gaan, ga het globale configuratiebevel van de **kaart crypto in**. Om de crypto-kaartvermelding volledig te maken, zijn er bepaalde aspecten die op zijn minst moeten worden gedefinieerd:

- De IPsec-peers waarnaar het beveiligde verkeer kan worden doorgestuurd, moeten worden gedefinieerd. Dit zijn de peers waarmee een SA kan worden opgericht. Als u een IPSec-peer in een cryptografische kaartregel wilt opgeven, voert u de volgende gegevens in: set peer uit.
- De transformatiesets die acceptabel zijn voor gebruik met het beschermde verkeer moeten worden gedefinieerd. Om de transformatiereeksen te specificeren die met de crypto kaartingang kunnen worden gebruikt, ga in set transform-set uit.
- Het verkeer dat beschermd moet worden, moet gedefinieerd worden. Om een uitgebreide toegangslijst voor een crypto kaartingang te specificeren, ga in match address uit.

Hierna volgt een voorbeeld:

```
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set ESP-AES-SHA
 match address 110
```

De laatste stap is om de eerder gedefinieerde crypto map toe te passen die is ingesteld op een interface. Om dit toe te passen, voert u de crypto map opdracht voor interfaceconfiguratie:

```
interface GigabitEthernet0/0
crypto map outside_map
```

Cisco IOS definitieve configuratie

Hier is de definitieve CLI-configuratie van Cisco IOS-router:

```
crypto isakmp policy 10
 encr aes
```

```
 authentication pre-share
 group 2
crypto isakmp key cisco123 address 172.16.1.1
!
crypto ipsec transform-set ESP-AES-SHA esp-aes esp-sha-hmac
 mode tunnel
!
crypto map outside_map 10 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set ESP-AES-SHA
 match address 110
!
interface GigabitEthernet0/0
 ip address 172.17.1.1 255.255.255.0
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
 crypto map outside_map
!
interface GigabitEthernet0/1
 ip address 10.20.10.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
ip nat inside source route-map nonat interface GigabitEthernet0/0 overload
!
route-map nonat permit 10
 match ip address 111
!
access-list 110 remark Interesting traffic access-list
access-list 110 permit ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 remark NAT exemption access-list
access-list 111 deny   ip 10.20.10.0 0.0.0.255 10.10.10.0 0.0.0.255
access-list 111 permit ip 10.20.10.0 0.0.0.255 any
```

Verifiëren

Alvorens u verifieert of de tunnel omhoog is en dat het het verkeer overgaat, moet u ervoor zorgen dat het verkeer van belang naar of ASA of de Cisco IOS router wordt verzonden.

> **Opmerking:** op de ASA kan het pakkettracer-gereedschap dat overeenkomt met het verkeer van belang worden gebruikt om de IPSec-tunnel te openen (zoals `packet-tracer input inside tcp 10.10.10.10 12345 10.20.10.10 80 detailed` bijvoorbeeld).

Verificatie in fase 1

Om te verifiëren of IKEv1 Fase 1 op ASA is, ga de **show crypto isakmp als** bevel in. De verwachte output ziet de MM_ACTIVE toestand:

```
ciscoasa# 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: 172.17.1.1
   Type    : L2L             Role    : responder
   Rekey   : no              State   : MM_ACTIVE

There are no IKEv2 SAs
ciscoasa#
```

Om te controleren of IKEv1 fase 1 op Cisco IOS is, voert u de show crypto isakmp sa uit. De verwachte output ziet de ACTIVE toestand:

```
Router#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
172.16.1.1      172.17.1.1      QM_IDLE           1005 ACTIVE

IPv6 Crypto ISAKMP SA

Router#
```

Verificatie in fase 2

Om te verifiëren of IKEv1 fase 2 op de ASA is gestart, voert u de show crypto ipsec sa uit. De verwachte output moet zowel de inkomende als uitgaande Security Parameter Index (SPI) zien. Als het verkeer door de tunnel gaat, moet u de toename van de tellers van encaps/decaps zien.

> **Opmerking:** voor elke ACL-ingang wordt een afzonderlijke inkomende/uitgaande SA gemaakt, wat kan resulteren in een lange show crypto ipsec sa opdrachtoutput (afhankelijk van het aantal ACE-vermeldingen in de crypto ACL).

Hierna volgt een voorbeeld:

```
ciscoasa# show crypto ipsec sa peer 172.17.1.1
peer address: 172.17.1.1
   Crypto map tag: outside_map, seq num: 10, local addr: 172.16.1.1

access-list asa-router-vpn extended permit ip 10.10.10.0 255.255.255.0
 10.20.10.0 255.255.255.0
     local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
     remote ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
     current_peer: 172.17.1.1


#pkts encaps: 1005, #pkts encrypt: 1005, #pkts digest: 1005
     #pkts decaps: 1014, #pkts decrypt: 1014, #pkts verify: 1014
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 1005, #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.: 172.16.1.1/0, remote crypto endpt.: 172.17.1.1/0
     path mtu 1500, ipsec overhead 74(44), media mtu 1500
     PMTU time remaining (sec): 0, DF policy: copy-df
     ICMP error validation: disabled, TFC packets: disabled
     current outbound spi: 8A9FE619
     current inbound spi : D8639BD0

inbound esp sas:
     spi: 0xD8639BD0 (3630406608)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (3914900/3519)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0xFFFFFFFF 0xFFFFFFFF
outbound esp sas:
     spi: 0x8A9FE619 (2325734937)
        transform: esp-aes esp-sha-hmac no compression
        in use settings ={L2L, Tunnel, IKEv1, }
        slot: 0, conn_id: 8192, crypto-map: outside_map
        sa timing: remaining key lifetime (kB/sec): (3914901/3519)
        IV size: 16 bytes
        replay detection support: Y
        Anti replay bitmap:
         0x00000000 0x00000001

ciscoasa#
```

Om te verifiëren of IKEv1 Phase 2 op Cisco IOS actief is, voert u de show crypto ipsec sa uit. De verwachte output moet zowel de inkomende als uitgaande SPI zien. Als het verkeer door de tunnel gaat, moet u de toename van de tellers van encaps/decaps zien.

Hierna volgt een voorbeeld:

```
Router#show crypto ipsec sa peer 172.16.1.1

interface: GigabitEthernet0/0
   Crypto map tag: outside_map, local addr 172.17.1.1

  protected vrf: (none)
local  ident (addr/mask/prot/port): (10.20.10.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
  current_peer 172.16.1.1 port 500
    PERMIT, flags={origin_is_acl,}
#pkts encaps: 2024, #pkts encrypt: 2024, #pkts digest: 2024
   #pkts decaps: 2015, #pkts decrypt: 2015, #pkts verify: 2015
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
   #send errors 26, #recv errors 0

    local crypto endpt.: 172.17.1.1, remote crypto endpt.: 172.16.1.1
```

```
    path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
    current outbound spi: 0xD8639BD0(3630406608)
    PFS (Y/N): N, DH group: none

inbound esp sas:
     spi: 0x8A9FE619(2325734937)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000046,
crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4449870/3455)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    inbound ah sas:

    inbound pcp sas:

outbound esp sas:
     spi: 0xD8639BD0(3630406608)
       transform: esp-aes esp-sha-hmac ,
       in use settings ={Tunnel, }
       conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000046,
crypto map: outside_map
       sa timing: remaining key lifetime (k/sec): (4449868/3455)
       IV size: 16 bytes
       replay detection support: Y
       Status: ACTIVE

    outbound ah sas:

    outbound pcp sas:
Router#
```

Verificatie fase 1 en 2

In deze sectie worden de opdrachten beschreven die u op de ASA of Cisco IOS kunt gebruiken om de details voor zowel fase 1 als 2 te verifiëren.

Voer het show vpn-sessiondb opdracht op de ASA ter verificatie:

```
ciscoasa# show vpn-sessiondb detail l2l filter ipaddress 172.17.1.1

Session Type: LAN-to-LAN Detailed

Connection   : 172.17.1.1
Index        : 2                     IP Addr      : 172.17.1.1
Protocol     : IKEv1 IPsec
Encryption   : IKEv1: (1)AES128  IPsec: (1)AES128
Hashing      : IKEv1: (1)SHA1  IPsec: (1)SHA1
Bytes Tx     : 100500                Bytes Rx     : 101400
Login Time   : 18:06:02 UTC Wed Jul 22 2015
Duration     : 0h:05m:07s
IKEv1 Tunnels: 1
IPsec Tunnels: 1

IKEv1:
```

```
 Tunnel ID    : 2.1
 UDP Src Port : 500                    UDP Dst Port : 500
 IKE Neg Mode : Main                   Auth Mode    : preSharedKeys
 Encryption   : AES128                 Hashing      : SHA1
 Rekey Int (T): 86400 Seconds          Rekey Left(T): 86093 Seconds
 D/H Group    : 2
 Filter Name  :

IPsec:
 Tunnel ID    : 2.2
 Local Addr   : 10.10.10.0/255.255.255.0/0/0
 Remote Addr  : 10.20.10.0/255.255.255.0/0/0
 Encryption   : AES128                 Hashing      : SHA1
 Encapsulation: Tunnel
 Rekey Int (T): 3600 Seconds           Rekey Left(T): 3293 Seconds
 Rekey Int (D): 4608000 K-Bytes        Rekey Left(D): 4607901 K-Bytes
 Idle Time Out: 30 Minutes             Idle TO Left : 26 Minutes
 Bytes Tx     : 100500                 Bytes Rx     : 101400
 Pkts Tx      : 1005                   Pkts Rx      : 1014

NAC:
 Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
 SQ Int (T)   : 0 Seconds              EoU Age(T)   : 309 Seconds
 Hold Left (T): 0 Seconds              Posture Token:
 Redirect URL :

ciscoasa#
```

Voer het show crypto session opdracht op Cisco IOS ter verificatie:

```
Router#show crypto session remote 172.16.1.1 detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation

Interface: GigabitEthernet0/0
Uptime: 00:03:36
Session status: UP-ACTIVE
Peer: 172.16.1.1 port 500 fvrf: (none) ivrf: (none)
     Phase1_id: 172.16.1.1
     Desc: (none)
 IKE SA: local 172.17.1.1/500 remote 172.16.1.1/500 Active
         Capabilities:(none) connid:1005 lifetime:23:56:23
 IPSEC FLOW: permit ip 10.20.10.0/255.255.255.0 10.10.10.0/255.255.255.0
       Active SAs: 2, origin: crypto map
       Inbound:  #pkts dec'ed 2015 drop 0 life (KB/Sec) 4449870/3383
       Outbound: #pkts enc'ed 2024 drop 26 life (KB/Sec) 4449868/3383

Router#
```

Problemen oplossen

Deze sectie verschaft informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

N.B.: Raadpleeg de belangrijke informatie over debug-opdrachten en probleemoplossing voor IP-beveiliging - Begrip en gebruik van debug-opdrachten voor Cisco-documenten voordat u deze gebruikt debug opdrachten.

IPsec LAN-to-LAN controletool

U kunt het IPSec LAN-to-LAN-gereedschap gebruiken om automatisch te controleren of de IPSec LAN-to-LAN-configuratie tussen de ASA en Cisco IOS geldig is. Het gereedschap is zo ontworpen dat het een show tech of show running-config opdracht van een ASA- of Cisco IOS-router. Het onderzoekt de configuratie en probeert te detecteren of een op crypto map gebaseerde LAN-to-LAN IPSec-tunnel is geconfigureerd. Indien geconfigureerd voert het een multi-point controle van de configuratie uit en markeert alle configuratiefouten en instellingen voor de tunnel die worden besproken.

ASA debugs

Om problemen op te lossen met IPSec IKEv1-tunnelonderhandeling op een ASA-firewall, kunt u deze gebruiken debug opdrachten:

```
debug crypto ipsec 127
debug crypto isakmp 127
debug ike-common 10
```

Opmerking: als het aantal VPN-tunnels op de ASA significant is, wordt de debug crypto condition peer A.B.C.D Het bevel moet worden gebruikt alvorens u de debugs toelaat om te beperken zuivert output om slechts de gespecificeerde peer te omvatten.

Cisco IOS-routerfouten

Om problemen op te lossen met IPSec IKEv1-tunnelonderhandeling op een Cisco IOS-router, kunt u deze debug-opdrachten gebruiken:

```
debug crypto ipsec
debug crypto isakmp
```

N.B.: Als het aantal VPN-tunnels op Cisco IOS significant is, wordt het debug crypto condition peer ipv4 A.B.C.D moet worden gebruikt voordat u de debugs activeert om de debug-uitgangen te beperken zodat alleen de gespecificeerde peer wordt opgenomen.

Tip: Raadpleeg het meest gebruikelijke Cisco-document voor L2L en externe toegang tot IPSec VPN-oplossingen voor probleemoplossing voor een site-to-site VPN.

Referenties

- Important Information on Debug Commands (Belangrijke informatie over debug-opdrachten)
- IP-beveiligingsprobleemoplossing - Begrijpen en gebruiken van debug-opdrachten

- Meest gebruikelijke oplossingen voor probleemoplossing in L2L en IPSec VPN met externe toegang
- IPsec LAN-to-LAN controleur
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.