Configurar um túnel do IPSec local a local IKEv1 entre um ASA e um roteador do Cisco IOS

Índice

Introdução

Este documento descreve como configurar um túnel de site para site da versão 1 do intercâmbio de chave de Internet do IPsec (do LAN para LAN) (IKEv1) através do CLI entre uma ferramenta de segurança adaptável de Cisco (ASA) e um roteador que execute o software do ® do Cisco IOS.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco IOS
- Cisco ASA
- Conceitos gerais do IPsec

Componentes Utilizados

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

- Cisco 5512-X Series ASA que executa a versão de software 9.4(1)
- Roteador dos Serviços integrados do Cisco 1941 Series (ISR) essa versão 15.4(3)M2 do Cisco IOS Software das corridas

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

Esta seção descreve como terminar as configurações de CLI ASA e de IOS Router.

Diagrama de Rede

A informação neste documento usa esta instalação de rede:

Configuração ASA

Configurar as relações ASA

Se as relações ASA não são configuradas, assegure-se de que você configure pelo menos os endereços IP de Um ou Mais Servidores Cisco ICM NT, conecte-se nomes, e níveis de segurança:

```
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
```

> Nota: Assegure-se de que haja uma Conectividade ao interno e às redes externas, e especialmente ao peer remoto que será usado a fim estabelecer um túnel do VPN de Site-para-Site. Você pode usar um sibilo a fim verificar a conectividade básica.

Configurar a política IKEv1 e permita IKEv1 na interface externa

A fim configurar as políticas do Internet Security Association and Key Management Protocol (ISAKMP) para as conexões IKEv1, incorpore o comando **cripto do <priority> da política ikev1**:

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

> **Nota:** Um fósforo da política IKEv1 existe quando ambas as políticas dos dois pares contêm a mesmos autenticação, criptografia, mistura, e valores de parâmetro de Diffie-Hellman. Para IKEv1, a política do peer remoto deve igualmente especificar uma vida inferior ou igual à vida na política que o iniciador envia. Se as vidas não são idênticas, a seguir o ASA usa a vida mais curto.

> **Nota:** Se você não especifica um valor para um parâmetro dado da política, o valor padrão é aplicado.

Você deve permitir IKEv1 na relação que termina o túnel VPN. Tipicamente, esta é a relação exterior (ou *público*). A fim permitir IKEv1, incorpore o **ikev1 cripto permitem o** comando do **<interface-name> no** modo de configuração global:

```
crypto ikev1 enable outside
```

Configurar o grupo de túneis (o perfil da conexão de LAN para LAN)

Para um túnel de LAN para LAN, o tipo do perfil de conexão é **ipsec-l2l**. A fim configurar a chave IKEv1 preshared, incorpore o modo de configuração dos IPsec-*atributos do grupo de túneis*:

```
crypto ikev1 enable outside
```

Configurar o ACL para o tráfego VPN do interesse

O ASA usa o Access Control Lists (ACLs) a fim diferenciar o tráfego que deve ser protegido com criptografia IPSec do tráfego que não exige a proteção. Protege os pacotes externos que combinam um motor do controle de aplicativo da licença (ACE) e assegura-se de que os pacotes de entrada que combinam uma licença ACE tenha a proteção.

```
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
```

> **Nota:** Um ACL para o tráfego VPN usa os endereços IP de origem e de destino após o Network Address Translation (NAT).

> **Nota:** Um ACL para o tráfego VPN deve ser espelhado em ambos os pares VPN.

> **Nota:** Se há uma necessidade de adicionar uma sub-rede nova ao tráfego protegido, adicionar simplesmente uma sub-rede/host ao objeto-grupo respectivo e termine uma mudança do espelho no par remoto VPN.

Configurar uma isenção de NAT

> Nota: A configuração que é descrita nesta seção é opcional.

Tipicamente, não deve haver nenhum NAT executado no tráfego VPN. A fim isentar esse tráfego, você deve criar uma regra da identidade NAT. A regra da identidade NAT traduz simplesmente um endereço ao mesmo endereço.

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

Configurar o IKEv1 transformam o grupo

Um IKEv1 transforma o grupo é uma combinação de protocolos de segurança e os algoritmos que defina a maneira que o ASA protege dados. Durante negociações da associação de segurança IPSec (SA), os pares devem identificar uma transformação ajustada ou a proposta que sejam as mesmas para ambos os pares. O ASA aplica então combinado transforma o grupo ou a proposta a fim criar um SA que proteja fluxos de dados na lista de acessos para esse crypto map.

A fim configurar o IKEv1 transforme o grupo, incorporam o comando **cripto do conjunto de transformação do IPsec ikev1**:

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

Configurar um crypto map e aplique-o a uma relação

Um crypto map define uma política de IPsec a ser negociada IPsec SA e inclui-a:

- Uma lista de acessos a fim identificar os pacotes que a conexão IPSec permite e protege
- Identificação do par
- Um endereço local para o tráfego de IPSec
- Os IKEv1 transformam grupos

Aqui está um exemplo:

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

Você pode então aplicar o crypto map à relação:

```
crypto map outside_map interface outside
```

Configuração final ASA

Está aqui a configuração final no ASA:

```
crypto map outside_map interface outside
```

Configuração de CLI do IOS Router

Configurar as relações

Se as relações do IOS Router não são configuradas ainda, a seguir pelo menos o LAN e as interfaces WAN devem ser configurados. Aqui está um exemplo:

```
crypto map outside_map interface outside
```

Assegure-se de que haja uma Conectividade ao interno e às redes externas, e especialmente ao peer remoto que será usado a fim estabelecer um túnel do VPN de Site-para-Site. Você pode usar um sibilo a fim verificar a conectividade básica.

Configurar a política ISAKMP (IKEv1)

A fim configurar as políticas de ISAKMP para as conexões IKEv1, incorpore o comando **cripto do <priority> da política do isakmp ao** modo de configuração global. Aqui está um exemplo:

```
crypto isakmp policy 10
 encr aes
 authentication pre-share
 group 2
```

> **Nota:** Você pode configurar políticas de IKE múltiplas em cada par que participa no IPsec. Quando a negociação de IKE começa, tenta encontrar uma política comum que seja configurada em ambos os pares, e começa com as políticas as mais prioritárias que são especificadas no peer remoto.

Configurar uma chave cripto ISAKMP

A fim configurar uma chave de autenticação *preshared*, inscreva o **comando crypto isakmp key no** modo de configuração global:

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

Configurar um ACL para o tráfego VPN do interesse

Use o prolongado ou a lista de acesso nomeada a fim especificar o tráfego que deve ser protegido pela criptografia. Aqui está um exemplo:

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

> **Nota:** Um ACL para o tráfego VPN usa os endereços IP de origem e de destino após o NAT.

> **Nota:** Um ACL para o tráfego VPN deve ser espelhado em ambos os pares VPN.

Configurar uma isenção de NAT

> Nota: A configuração que é descrita nesta seção é opcional.

Tipicamente, não deve haver nenhum NAT executado no tráfego VPN. Se a sobrecarga NAT é usada, a seguir um mapa de rotas deve ser usado a fim isentar o tráfego VPN do interesse da tradução. Observe que na lista de acesso que é usada no mapa de rotas, o tráfego VPN do interesse deve ser negado.

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

Configurar um grupo da transformação

A fim definir um IPsec transforme o grupo (uma combinação aceitável de protocolos de segurança e de algoritmos), inscrevem o **comando crypto ipsec transform-set no** modo de configuração global. Aqui está um exemplo:

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

Configurar um crypto map e aplique-o a uma relação

A fim criar ou alterar uma entrada do crypto map e incorporar o modo de configuração do crypto map, inscreva o comando global configuration do **crypto map**. Para que a entrada do crypto map esteja completa, lá são alguns aspectos que devem ser definidos em um mínimo:

- Os ipsec peer a que o tráfego protegido pode ser enviado devem ser definidos. Estes são os pares com que um SA pode ser estabelecido. A fim especificar um ipsec peer em uma entrada do crypto map, inscreva o **comando set peer**.
- Os grupos da transformação que são aceitáveis para o uso com o tráfego protegido devem ser definidos. A fim especificar os grupos da transformação que podem ser usados com a

entrada do crypto map, inscreva o **comando set transform-set**.

- O tráfego que deve ser protegido deve ser definido. A fim especificar uma lista de acesso extendida para uma entrada do crypto map, inscreva o **comando address do fósforo**.

Aqui está um exemplo:

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

A etapa final é aplicar o crypto map previamente definido ajustado a uma relação. A fim aplicar isto, inscreva o comando interface configuration do **crypto map**:

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

Configuração final IO

Está aqui a configuração de CLI final do IOS Router:

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

Verificar

Antes que você o verifique se o túnel é ascendente e aquele passar o tráfego, você deve assegurar-se de que o tráfego do interesse esteja enviado para o ASA ou o IOS Router.

> **Nota:** No ASA, a ferramenta do pacote-projétil luminoso que combina o tráfego do interesse pode ser usada a fim iniciar o túnel de IPsec (tal como o pacote-**projétil luminoso entrado dentro de tcp 10.10.10.10 12345 10.20.10.10 80 detalhado** por exemplo).

Verificação da fase 1

A fim verificar se IKEv1 a fase 1 está acima no ASA, inscreva o **comando show crypto isakmp sa**. O rendimento esperado é considerar o estado **MM_ACTIVE**:

```
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#
```

A fim verificar se IKEv1 a fase 1 está acima nos IO, inscreva o **comando show crypto isakmp sa**.

O rendimento esperado é considerar o estado **ATIVO**:

```
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#
```

Verificação da fase 2

A fim verificar se IKEv1 a fase 2 está acima no ASA, inscreva o **comando show crypto ipsec sa**. O rendimento esperado é considerar o Security Parameter Index de entrada e de partida (SPI). Se o tráfego passa através do túnel, você deve ver os encaps/o incremento contadores dos decaps.

> **Nota:** Para cada entrada ACL há SA de entrada/de partida separado criado, que possa conduzir a uma saída longa do **comando show crypto ipsec sa** (dependente do número de entradas ACE no ACL cripto).

Aqui está um exemplo:

```
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#
```

A fim verificar se IKEv1 a fase 2 está acima nos IO, inscreva o **comando show crypto ipsec sa**. O rendimento esperado é considerar o SPI de entrada e de partida. Se o tráfego passa através do túnel, você deve ver os encaps/o incremento contadores dos decaps.

Aqui está um exemplo:

```
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#
```

Fase 1 e verificação 2

Esta seção descreve os comandos que você pode usar no ASA ou nos IO a fim verificar os detalhes por ambas as fases 1 e 2.

Incorpore o comando da **mostra VPN-sessiondb no** ASA para a verificação:

```
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#
```

Incorpore o comando de **sessão de criptografia da mostra nos** IO para a verificação:

```
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#
```

Troubleshooting

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

> **Nota:** Refira a informação importante em comandos Debug e em Troubleshooting de Segurança IP - compreendendo e usando documentos Cisco dos comandos debug antes que você use **comandos debug**.

Ferramenta do verificador do LAN para LAN do IPsec

A fim verificar automaticamente se a configuração de LAN para LAN do IPsec entre o ASA e os IO é válida, você pode usar a ferramenta do verificador do LAN para LAN do IPsec. A ferramenta é projetada de modo que aceite uma **tecnologia** ou um **comando show running-config da mostra de um** ASA ou do IOS Router. Examina a configuração e tenta detectar se um túnel IPSec de LAN para LAN baseado em mapas cripto está configurado. Se configurada, executa uma verificação do multi-ponto da configuração e destaca quaisquer erros de configuração e ajustes para o túnel que seria negociado.

O ASA debuga

A fim pesquisar defeitos a negociação do túnel do IPsec IKEv1 em um Firewall ASA, você pode usar estes **comandos debug**:

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

> **Nota:** Se o número de VPN escava um túnel no ASA é significativo, o **par que da condição do debug crypto o comando a.b.c.d** deve está usado antes que você permitir debuga a fim

limitar os resultados do debug para incluir somente o par especificado.

O IOS Router debuga

A fim pesquisar defeitos a negociação do túnel do IPsec IKEv1 em um IOS Router, você pode usar estes comandos debug:

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

> **Nota:** Se o número de VPN escava um túnel nos IO é significativo, o **par que da condição do debug crypto o IPv4 A.B.C.D deve** está usado antes que você permitir debuga a fim limitar os resultados do debug para incluir somente o par especificado.

> Dica: Refira o L2L o mais comum e o IPSec VPN do Acesso remoto que pesquisa defeitos o documento Cisco das soluções para obter mais informações sobre de como pesquisar defeitos um VPN de Site-para-Site.

Referências

- Informações Importantes sobre Comandos de Depuração
- Troubleshooting de Segurança de IP - Entendendo e Utilizando Comandos debug
- Soluções de Troubleshooting Mais Comuns de VPN IPsec L2L e de Acesso Remoto
- Verificador do LAN para LAN do IPsec
- Suporte Técnico e Documentação - Cisco Systems