Configurando um túnel de IPsec - Roteador Cisco ao firewall de ponto de controle 4.1

Índice

Introdução

Esse documento demonstra como formar um túnel de IPsec com chaves pré-compartilhadas para unir duas redes privadas: a rede privada 192.168.1.x dentro do roteador Cisco e a rede privada 10.32.50.x dentro do Checkpoint Firewall.

Pré-requisitos

Requisitos

Esta configuração de exemplo supõe que o tráfego do interior do roteador e do interior o ponto de verificação ao Internet (representado aqui pelas redes 172.18.124.x) flui antes que você comece a configuração.

Componentes Utilizados

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

- Cisco 3600 Router
- Software de Cisco IOS® (C3640-JO3S56I-M), liberação 12.1(5)T, SOFTWARE DE VERSÃO

(fc1)
- Firewall de ponto de controle 4.1

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.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a ferramenta Command Lookup Tool (apenas para clientes registrados) para obter mais informações sobre os comandos usados neste documento.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Configurações

Este documento utiliza estas configurações.

- Configuração do roteador
- Configuração do firewall de ponto de controle

Configuração do roteador

Configuração do Cisco 3600 Router

```
Current configuration : 1608 bytes
!
version 12.1
no service single-slot-reload-enable
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname cisco_endpoint
!
logging rate-limit console 10 except errors
!
ip subnet-zero
!
no ip finger
!
ip audit notify log
ip audit po max-events 100
```

```
!
!--- Internet Key Exchange (IKE) configuration crypto
isakmp policy 1 authentication pre-share crypto isakmp
key ciscorules address 172.18.124.157 ! !--- IPsec
configuration crypto ipsec transform-set rtpset esp-des
esp-sha-hmac ! crypto map rtp 1 ipsec-isakmp set peer
172.18.124.157 set transform-set rtpset match address
115 ! call rsvp-sync cns event-service server !
controller T1 1/0 ! controller T1 1/1 ! interface
Ethernet0/0 ip address 172.18.124.35 255.255.255.240 ip
nat outside no ip mroute-cache half-duplex crypto map
rtp ! interface Ethernet0/1 ip address 192.168.1.1
255.255.255.0 ip nat inside half-duplex ! interface
FastEthernet1/0 no ip address shutdown duplex auto speed
auto ! ip kerberos source-interface any ip nat pool
INTERNET 172.18.124.36 172.18.124.36 netmask
255.255.255.240 ip nat inside source route-map nonat
pool INTERNET ip classless ip route 0.0.0.0 0.0.0.0
172.18.124.34 no ip http server ! access-list 101 deny
ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255 access-
list 101 permit ip 192.168.1.0 0.0.0.255 any access-list
115 permit ip 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255
access-list 115 deny ip 192.168.1.0 0.0.0.255 any route-
map nonat permit 10 match ip address 101 ! dial-peer cor
custom ! line con 0 transport input none line aux 0 line
vty 0 4 login ! end
```

Configuração do firewall de ponto de controle

Termine estas etapas para configurar o firewall de ponto de controle.

1. Desde que o IKE e as durações padrão IPSec diferem entre vendedores, selecione o **Propriedades > Criptografia** para ajustar as durações do ponto de controle para concordar com os padrões Cisco.A duração de IKE do padrão Cisco é 86400 segundos (= 1440 minutos), e pode ser alterada por estes comandos:**política cripto do isakmp #vida #**A duração de IKE configurável de Cisco é de 60-86400 segundos. A duração de IPSec do padrão Cisco é 3600 segundos, e pode ser alterada pelo **comando crypto ipsec security-association lifetime seconds -**.A duração configurável de Cisco IPSec é de 120-86400 segundos.
2. Selecione **Manage > Network Objects o > New (Or Edit) > Network** para configurar o objeto para a rede interna (chamada “cpinside”) atrás do ponto de verificação.Isto deve concordar com a rede (secundária) de destino no comando da **licença IP 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255 da lista de acesso 115 de** Cisco.Selecione o lugar inferior **interno**.
3. Selecione **Manage > Network Objects > Edit** para editar o objeto para o valor-limite do Ponto de controle RTPCPVPN (gateway) esse os pontos do roteador Cisco no comando de **172.18.124.157 do par do grupo**.Selecione o lugar inferior **interno**. Para Tipo, selecione Gateway. Sob os módulos instalados, selecione a **caixa de verificação VPN-1 & firewall-1**, e igualmente selecione a **caixa de verificação da estação de gerenciamento**:
4. Selecione **Manage > Network Objects > New > Network** para configurar o objeto para a rede externa (chamada “inside_cisco”) atrás do roteador Cisco.Isto deve concordar com a primeira) rede da fonte (no comando da **licença IP 192.168.1.0 0.0.0.255 10.32.50.0 0.0.0.255 da lista de acesso 115 de** Cisco.Selecione o lugar inferior **externo**.
5. Selecione **Manage > Network Objects > New > Workstation** para adicionar um objeto para o gateway externo do roteador Cisco (chamado “cisco_endpoint”). Esta é a interface Cisco a

que o **comando crypto map name** é aplicado.Selecione o lugar inferior **externo**. Para Tipo, selecione Gateway.**Nota:** Não selecione a caixa de seleção VPN-1/FireWall-1.

6. Selecionar Manage > Network objetct > Edit para editar o ponto final do gateway do ponto de controle (chamado "RTPCPVPN") na guia VPN. Em Domain, selecione Other e, em seguida, selecione o lado interno da rede de ponto de controle (chamado “cpinside”) a partir da lista suspensa. Sob esquemas de criptografia definidos, selecione IKE e clique em Editar.
7. Mude as propriedades IKE para a criptografia DES para concordar com estes comandos:**política cripto do isakmp #DES da criptografiaNota:** A criptografia DES é o padrão assim que não é visível na configuração Cisco.
8. Mude as propriedades IKE ao hashing SHA1 para concordar com estes comandos:**política cripto do isakmp #sha da misturaNota:** O algoritmo de hashing SHA é o padrão assim que não é visível na configuração Cisco.Mude estes ajustes:Desative o Modo assertivo.A verificação **apoia sub-redes**.Verifique o **segredo pré-compartilhado** sob o método de autenticação. Isto concorda com estes comandos:**política cripto do isakmp #Pré-compartilhamento de autenticação**
9. O clique **edita segredos** para ajustar a chave pré-compartilhada para concordar com o **comando crypto isakmp key key address address de** Cisco:
10. Selecione Gerenciar > Objetos de rede > Editar para editar a guia VPN “cisco_endpoint”. Em Domain, selecione Other e, em seguida, selecione o interior da rede Cisco (chamado "inside_cisco"). Sob esquemas de criptografia definidos, selecione IKE e clique em Editar.
11. Mude a criptografia DES das propriedades IKE para concordar com estes comandos:**política cripto do isakmp #DES da criptografiaNota:** A criptografia DES é o padrão assim que não é visível na configuração Cisco.
12. Mude as propriedades IKE ao hashing SHA1 para concordar com estes comandos:**política cripto do isakmp #sha da misturaNota:** O algoritmo de hashing SHA é o padrão assim que não é visível na configuração Cisco.Mude estes ajustes:Desative o Modo assertivo.A verificação **apoia sub-redes**.Verifique o **segredo pré-compartilhado** sob o método de autenticação. Isto concorda com estes comandos:**política cripto do isakmp #Pré-compartilhamento de autenticação**
13. O clique **edita segredos** para ajustar a chave pré-compartilhada para concordar com o comando cisco **cripto do endereço endereço da** *chave da* **chave do isakmp**.
14. Na janela Policy Editor, insira uma regra com Source e Destination como "inside_cisco" e "cpinside" (bidirecional). Ajustar Serviço=Qualquer, Ação=Criptografar e Rastreio=Longo.
15. Clique o ícone verde de criptografia e selecione-o **Edit Properties** para configurar políticas de criptografia sob o título da ação.
16. Selecione IKE e, em seguida, clique em Editar.
17. No indicador das propriedades IKE, mude estas propriedades para concordar com o Cisco IPSEC transforma no **comando crypto ipsec transform-set rtpset esp-des esp-sha-hmac**:Em Transform, selecione Encryption + Data Integrity (ESP). O algoritmo de criptografia deve ser **DES**, integridade de dados deve ser **SHA1**, e o gateway de peer permitido deve ser o gateway do roteador externo (chamado “cisco_endpoint”). Clique em **OK**.
18. Depois que você configura o ponto de verificação, a **política** seleta **> instala no** menu do ponto de controle para mandar as mudanças tomar o efeito.

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está

funcionando adequadamente.

A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

- show crypto isakmp sa - Ver todas as associações de segurança (SAs) IKE atuais no correspondente.
- **mostre IPsec cripto sa** — Veja os ajustes usados por SA atuais.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

Nota: Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos **debug**.

- **motor do debug crypto** — Os indicadores debugam mensagens sobre as crypto-engines, que executam a criptografia e a descriptografia.
- debug crypto isakmp - Exibe mensagens sobre eventos IKE.
- **debug crypto ipsec** — Exibe eventos de IPSec.
- **cancele o isakmp cripto** — Cancela todas as conexões do IKE ativo.
- **cancele o sa cripto** — Cancela todo o sas de IPSec.

Sumarização da rede

Quando as redes internas adjacentes do múltiplo são configuradas no domínio da criptografia no ponto de verificação, o dispositivo pôde automaticamente resumi-las no que diz respeito ao tráfego interessante. Se o roteador não é configurado para combinar, o túnel é provável falhar. Por exemplo, se as redes internas de 10.0.0.0 /24 e de 10.0.1.0 /24 são configuradas para ser incluídas no túnel, puderam ser resumidas a 10.0.0.0 /23.

Ponto de verificação

Como o rastreamento foi definido para Long na janela Policy Editor, o tráfego negado deve aparecer em vermelho em Log Viewer. Mais verboso debugar pode ser obtido com:

```
C:\WINNT\FW1\4.1\fwstop
C:\WINNT\FW1\4.1\fw d -d
```

e em outra janela:

```
C:\WINNT\FW1\4.1\fwstart
```

Nota: Esta era uma instalação de Microsoft Windows NT.

Emita estes comandos cancelar SA no ponto de verificação:

```
fw tab -t IKE_SA_table -x
fw tab -t ISAKMP_ESP_table -x
```

```
fw tab -t inbound_SPI -x
fw tab -t ISAKMP_AH_table -x
```

A resposta **sim no** é você certo? prompt.

Exemplo de debug

```
Configuration register is 0x2102

cisco_endpoint#debug crypto isakmp Crypto ISAKMP debugging is on cisco_endpoint#debug crypto
isakmp Crypto IPSEC debugging is on cisco_endpoint#debug crypto engine Crypto Engine debugging
is on cisco_endpoint# 20:54:06: IPSEC(sa_request): , (key eng. msg.) src= 172.18.124.35, dest=
172.18.124.157, src_proxy= 192.168.1.0/255.255.255.0/0/0 (type=4), dest_proxy=
10.32.50.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac , lifedur=
3600s and 4608000kb, spi= 0xA29984CA(2727969994), conn_id= 0, keysize= 0, flags= 0x4004
20:54:06: ISAKMP: received ke message (1/1) 20:54:06: ISAKMP: local port 500, remote port 500
20:54:06: ISAKMP (0:1): beginning Main Mode exchange 20:54:06: ISAKMP (0:1): sending packet to
172.18.124.157 (I) MM_NO_STATE 20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I)
MM_NO_STATE 20:54:06: ISAKMP (0:1): processing SA payload. message ID = 0 20:54:06: ISAKMP
(0:1): found peer pre-shared key matching 172.18.124.157 20:54:06: ISAKMP (0:1): Checking ISAKMP
transform 1 against priority 1 policy 20:54:06: ISAKMP: encryption DES-CBC 20:54:06: ISAKMP:
hash SHA 20:54:06: ISAKMP: default group 1 20:54:06: ISAKMP: auth pre-share 20:54:06: ISAKMP
(0:1): atts are acceptable. Next payload is 0 20:54:06: CryptoEngine0: generate alg parameter
20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0 20:54:06: CRYPTO_ENGINE: Dh phase 1 status: 0
20:54:06: ISAKMP (0:1): SA is doing pre-shared key authentication using id type ID_IPV4_ADDR
20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I) MM_SA_SETUP 20:54:06: ISAKMP (0:1):
received packet from 172.18.124.157 (I) MM_SA_SETUP 20:54:06: ISAKMP (0:1): processing KE
payload. message ID = 0 20:54:06: CryptoEngine0: generate alg parameter 20:54:06: ISAKMP (0:1):
processing NONCE payload. message ID = 0 20:54:06: ISAKMP (0:1): found peer pre-shared key
matching 172.18.124.157 20:54:06: CryptoEngine0: create ISAKMP SKEYID for conn id 1 20:54:06:
ISAKMP (0:1): SKEYID state generated 20:54:06: ISAKMP (1): ID payload next-payload : 8 type : 1
protocol : 17 port : 500 length : 8 20:54:06: ISAKMP (1): Total payload length: 12 20:54:06:
CryptoEngine0: generate hmac context for conn id 1 20:54:06: ISAKMP (0:1): sending packet to
172.18.124.157 (I) MM_KEY_EXCH 20:54:06: ISAKMP (0:1): received packet from 172.18.124.157 (I)
MM_KEY_EXCH 20:54:06: ISAKMP (0:1): processing ID payload. message ID = 0 20:54:06: ISAKMP
(0:1): processing HASH payload. message ID = 0 20:54:06: CryptoEngine0: generate hmac context
for conn id 1 20:54:06: ISAKMP (0:1): SA has been authenticated with 172.18.124.157 20:54:06:
ISAKMP (0:1): beginning Quick Mode exchange, M-ID of 1855173267 20:54:06: CryptoEngine0:
generate hmac context for conn id 1 20:54:06: ISAKMP (0:1): sending packet to 172.18.124.157 (I)
QM_IDLE 20:54:06: CryptoEngine0: clear dh number for conn id 1 20:54:06: ISAKMP (0:1): received
packet from 172.18.124.157 (I) QM_IDLE 20:54:06: CryptoEngine0: generate hmac context for conn
id 1 20:54:06: ISAKMP (0:1): processing HASH payload. message ID = 1855173267 20:54:06: ISAKMP
(0:1): processing SA payload. message ID = 1855173267 20:54:06: ISAKMP (0:1): Checking IPSec
proposal 1 20:54:06: ISAKMP: transform 1, ESP_DES 20:54:06: ISAKMP: attributes in transform:
20:54:06: ISAKMP: encaps is 1 20:54:06: ISAKMP: SA life type in seconds 20:54:06: ISAKMP: SA
life duration (basic) of 3600 20:54:06: ISAKMP: SA life type in kilobytes 20:54:06: ISAKMP: SA
life duration (VPI) of 0x0 0x46 0x50 0x0 20:54:06: ISAKMP: authenticator is HMAC-SHA 20:54:06:
validate proposal 0 20:54:06: ISAKMP (0:1): atts are acceptable. 20:54:06:
IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 172.18.124.157, src=
172.18.124.35, dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4), src_proxy=
192.168.1.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-des esp-sha-hmac ,
lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 20:54:06: validate proposal
request 0 20:54:06: ISAKMP (0:1): processing NONCE payload. message ID = 1855173267 20:54:06:
ISAKMP (0:1): processing ID payload. message ID = 1855173267 20:54:06: ISAKMP (0:1): processing
ID payload. message ID = 1855173267 20:54:06: CryptoEngine0: generate hmac context for conn id 1
20:54:06: ipsec allocate flow 0 20:54:06: ipsec allocate flow 0 20:54:06: ISAKMP (0:1): Creating
IPSec SAs 20:54:06: inbound SA from 172.18.124.157 to 172.18.124.35 (proxy 10.32.50.0 to
192.168.1.0) 20:54:06: has spi 0xA29984CA and conn_id 2000 and flags 4 20:54:06: lifetime of
3600 seconds 20:54:06: lifetime of 4608000 kilobytes 20:54:06: outbound SA from 172.18.124.35 to
172.18.124.157 (proxy 192.168.1.0 to 10.32.50.0) 20:54:06: has spi 404516441 and conn_id 2001
and flags 4 20:54:06: lifetime of 3600 seconds 20:54:06: lifetime of 4608000 kilobytes 20:54:06:
ISAKMP (0:1): sending packet to 172.18.124.157 (I) QM_IDLE 20:54:06: ISAKMP (0:1): deleting node
1855173267 error FALSE reason "" 20:54:06: IPSEC(key_engine): got a queue event... 20:54:06:
```

```
IPSEC(initialize_sas): , (key eng. msg.) dest= 172.18.124.35, src= 172.18.124.157, dest_proxy=
192.168.1.0/255.255.255.0/0/0 (type=4), src_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 3600s and 4608000kb, spi=
0xA29984CA(2727969994), conn_id= 2000, keysize= 0, flags= 0x4 20:54:06: IPSEC(initialize_sas): ,
(key eng. msg.) src= 172.18.124.35, dest= 172.18.124.157, src_proxy=
192.168.1.0/255.255.255.0/0/0 (type=4), dest_proxy= 10.32.50.0/255.255.255.0/0/0 (type=4),
protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 3600s and 4608000kb, spi=
0x181C6E59(404516441), conn_id= 2001, keysize= 0, flags= 0x4 20:54:06: IPSEC(create_sa): sa
created, (sa) sa_dest= 172.18.124.35, sa_prot= 50, sa_spi= 0xA29984CA(2727969994), sa_trans=
esp-des esp-sha-hmac , sa_conn_id= 2000 20:54:06: IPSEC(create_sa): sa created, (sa) sa_dest=
172.18.124.157, sa_prot= 50, sa_spi= 0x181C6E59(404516441), sa_trans= esp-des esp-sha-hmac ,
sa_conn_id= 2001 cisco_endpoint#sho cry ips sa interface: Ethernet0/0 Crypto map tag: rtp, local
addr. 172.18.124.35 local ident (addr/mask/prot/port): (192.168.1.0/255.255.255.0/0/0) remote
ident (addr/mask/prot/port): (10.32.50.0/255.255.255.0/0/0) current_peer: 172.18.124.157 PERMIT,
flags={origin_is_acl,} #pkts encaps: 14, #pkts encrypt: 14, #pkts digest 14 #pkts decaps: 14,
#pkts decrypt: 14, #pkts verify 14 #pkts compressed: 0, #pkts decompressed: 0 #pkts not
compressed: 0, #pkts compr. failed: 0, #pkts decompress failed: 0, #send errors 1, #recv errors
0 local crypto endpt.: 172.18.124.35, remote crypto endpt.: 172.18.124.157 path mtu 1500, media
mtu 1500 current outbound spi: 181C6E59 inbound esp sas: spi: 0xA29984CA(2727969994) transform:
esp-des esp-sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 2000, flow_id: 1, crypto
map: rtp --More-- sa timing: remaining key lifetime (k/sec): (4607998/3447) IV size: 8 bytes
replay detection support: Y inbound ah sas: inbound pcp sas: outbound esp sas: spi:
0x181C6E59(404516441) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 2001, flow_id: 2, crypto map: rtp sa timing: remaining key lifetime (k/sec):
(4607997/3447) IV size: 8 bytes replay detection support: Y outbound ah sas: outbound pcp sas:
cisco_endpoint#show crypto isakmp sa dst src state conn-id slot 172.18.124.157 172.18.124.35
QM_IDLE 1 0 cisco_endpoint#exit
```

Informações Relacionadas

- Negociação IPsec/Protocolos IKE
- Configurando a Segurança de rede IPSec
- Configurando o protocolo de segurança do intercâmbio chave de Internet
- Suporte Técnico e Documentação - Cisco Systems