Configurar uma sessão de eBGP segura com um IPsec VTI

Índice

Introdução

Este documento descreve como fixar um relacionamento vizinho do Protocolo de Gateway Limite externo (eBGP) (eBGP) com o uso de uma interface de túnel virtual do IPsec (VTI) junto com as interfaces física (NON-túnel) para o tráfego plano dos dados. Os benefícios desta configuração incluem:

- Termine a privacidade da sessão do vizinho de BGP com confidencialidade de dados, anti-repetição, autenticidade, e integridade.
- O tráfego plano dos dados não é forçado às despesas gerais da unidade de transmissão máxima (MTU) da interface de túnel. Os clientes podem enviar pacotes padrão MTU (1500 bytes) sem implicações de desempenho ou fragmentação.
- Menos despesas gerais no Roteadores do ponto final desde que a criptografia do deslocamento predeterminado da política de segurança (SPI)/que decifra é limitada ao tráfego plano do controle BGP.

O benefício desta configuração é que o plano dos dados não está forçado à limitação da relação em túnel. Pelo projeto, o tráfego plano dos dados não é IPsec fixado.

Charles contribuído Stizza, engenheiro de TAC da Cisco.

Pré-requisitos

Requisitos

A Cisco recomenda que você conheça estes tópicos:

- fundamentos da configuração de eBGP e da verificação
- Manipulação da contabilidade da política do BGP (PA) usando um mapa de rotas
- Características básicas do Internet Security Association and Key Management Protocol (ISAKMP) e da política de IPsec

Componentes Utilizados

A informação neste documento é baseada no Cisco IOS? Software Release 15.3(1.3)T mas o outro trabalho das versões suportadas. Desde que a configuração IPSec é uma característica criptograficamente, assegure-se de que sua versão de código contenha este conjunto de recursos.

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.

> Cuidado: O exemplo de configuração neste documento usa os algoritmos modestos da cifra que puderam ou não puderam ser seridos para seu ambiente. Veja o White Paper da criptografia da próxima geração para um exame da Segurança relativa de várias séries e de tamanhos chaves da cifra.

Configurar

> Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Configurações

Conclua estes passos:

1. Configurar parâmetros da fase de intercâmbio de chave de Internet (IKE) 1 no r1 e no R2 com a chave pré-compartilhada no r1:Nota: Nunca use os números do grupo 1, 2 ou 5 DH desde que são considerados inferiores. Se possível use um grupo DH com curva elíptico Cryptopgraphy (ECC) como os grupos 19, 20 ou 24. O Advanced Encryption Standard (AES) e o algoritmo de mistura segura 256 (SHA256) devem ser considerados superior à criptografia padrão de dados (DES)/3DES e message digest 5 (MD5)/SHA1 respectivamente. Nunca use a senha “Cisco” em um ambiente de produção.**Configuração do r1**

```
R1(config)#crypto isakmp policy 1
R1(config-isakmp)#encr aes
R1(config-isakmp)#hash sha256
R1(config-isakmp)#authentication pre-share
R1(config-isakmp)#group 19
```

```
R1(config-isakmp)exit

R1(config)#crypto isakmp key CISCO address 12.0.0.2
```
Configuração R2
```
R2(config)#crypto isakmp policy 1
R2(config-isakmp)#encr aes
R2(config-isakmp)#hash sha256
R2(config-isakmp)#authentication pre-share
R2(config-isakmp)#group 19


R2(config-isakmp)exit

R2(config)#crypto isakmp key CISCO address 12.0.0.1
```
2. Configurar a criptografia de senha do nível 6 para a chave pré-compartilhada no NVRAM no r1 e no R2. Isto reduz a probabilidade da chave pré-compartilhada armazenada no texto simples da leitura se um roteador é comprometido: `R1(config)#key config-key password-encrypt CISCOCISCO`

```
R1(config)#password encryption aes

R2(config)#key config-key password-encrypt CISCOCISCO

R2(config)#password encryption aes
```
Nota: Uma vez que a criptografia de senha do nível 6 é permitida, a configuração ativa já não mostra a versão de texto simples da chave pré-compartilhada:
```
!
R1#show run | include key
crypto isakmp key 6 \Nd`]dcCW\E`^WEObUKRGKIGadiAAB address 12.0.0.2

!
```
3. Configurar os parâmetros da fase 2 IKE no r1 e no R2:
Configuração do r1
`R1(config)#crypto ipsec transform-set TRANSFORM-SET esp-aes 256 esp-sha256 ah-sha256-hmac`

```
R1(config)#crypto ipsec profile PROFILE

R1(ipsec-profile)#set transform-set TRANSFORM-SET
```
`R1(ipsec-profile)#set pfs group19`
Configuração R2
`R2(config)#crypto ipsec transform-set TRANSFORM-SET esp-aes 256 esp-sha256 ah-sha256-hmac`

```
R2(config)#crypto ipsec profile PROFILE

R2(ipsec-profile)#set transform-set TRANSFORM-SET
```
`R2(ipsec-profile)#set pfs group19`
Nota: Ajustar o discrição perfeita adiante (PFS) é opcional mas melhora a força VPN desde que força uma geração de chave simétrica nova no estabelecimento da fase 2 SA IKE.
4. Configurar as interfaces de túnel no r1 e no R2 e fixe-as com o perfil IPSec:
Configuração do r1
`R1(config)#interface tunnel 12`

```
R1(config-if)#ip address 1.1.1.1 255.255.255.0

R1(config-if)#tunnel source Ethernet0/0

R1(config-if)#tunnel mode ipsec ipv4

R1(config-if)#tunnel destination 12.0.0.2

R1(config-if)#tunnel protection ipsec profile PROFILE
```
Configuração R2
`R2(config)#interface tunnel 12`

```
R2(config-if)#ip address 1.1.1.2 255.255.255.0

R2(config-if)#tunnel source Ethernet0/0

R2(config-if)#tunnel mode ipsec ipv4

R2(config-if)#tunnel destination 12.0.0.1

R2(config-if)#tunnel protection ipsec profile PROFILE
```

5. Configurar o BGP no r1 e no R2 e anuncie as redes loopback0 no BGP:**Configuração do r1**
```
R1(config)#router bgp 65510

R1(config-router)#neighbor 1.1.1.2 remote-as 65511

R1(config-router)#network 10.0.0.0 mask 255.255.255.0
```
Configuração R2
```
R2(config)#router bgp 65511

R2(config-router)#neighbor 1.1.1.2 remote-as 65510

R2(config-router)#network 20.0.0.0 mask 255.255.255.0
```
6. Configurar um mapa de rotas no r1 e no R2 a fim mudar manualmente o endereço IP de Um ou Mais Servidores Cisco ICM NT do salto seguinte de modo que aponte à interface física e não ao túnel. Você deve aplicar este mapa de rotas na direção de entrada.**Configuração do r1**
```
R1(config)ip prefix-list R2-NETS seq 5 permit 20.0.0.0/24

R1(config)#route-map CHANGE-NEXT-HOP permit 10

R1(config-route-map)#match ip address prefix-list R2-NETS

R1(config-route-map)#set ip next-hop 12.0.0.2

R1(config-route-map)#end

R1(config)#router bgp 65510

R1(config-router)#neighbor 1.1.1.2 route-map CHANGE-NEXT-HOP in

R1(config-router)#do clear ip bgp *

R1(config-router)#end
```
Configuração R2
```
R2(config)#ip prefix-list R1-NETS seq 5 permit 10.0.0.0/24

R2(config)#route-map CHANGE-NEXT-HOP permit 10

R2(config-route-map)#match ip address prefix-list R1-NETS

R2(config-route-map)#set ip next-hop 12.0.0.1

R2(config-route-map)#end

R2(config)#router bgp 65511

R2(config-router)#neighbor 1.1.1.1 route-map CHANGE-NEXT-HOP in

R2(config-router)#do clear ip bgp *

R2(config-router)#end
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A ferramenta Output Interpreter (clientes registrados somente) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

Verifique que a fase 1 IKE e a fase 2 IKE terminaram. O protocolo de linha na interface de túnel virtual (VTI) não muda a “acima de” até que a fase 2 IKE termine:

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
12.0.0.1 12.0.0.2 QM_IDLE 1002 ACTIVE
12.0.0.2 12.0.0.1 QM_IDLE 1001 ACTIVE

R1#show crypto ipsec sa | inc encaps|decaps
#pkts encaps: 88, #pkts encrypt: 88, #pkts digest: 88
#pkts decaps: 90, #pkts decrypt: 90, #pkts verify: 90
```

Note que antes do aplicativo do mapa de rotas, o endereço IP de Um ou Mais Servidores Cisco ICM NT do salto seguinte aponta ao endereço IP de Um ou Mais Servidores Cisco ICM NT do vizinho de BGP que é a interface de túnel:

```
R1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
*> 20.0.0.0/24 1.1.1.2 0 0 65511 i
```

Quando o tráfego usa o túnel, o MTU está forçado ao túnel MTU:

```
R1#ping 20.0.0.2 size 1500 df-bit
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set

*May 6 08:42:07.311: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:09.312: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:11.316: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:13.319: ICMP: dst (20.0.0.2): frag. needed and DF set.
*May 6 08:42:15.320: ICMP: dst (20.0.0.2): frag. needed and DF set.
Success rate is 0 percent (0/5)

R1#show interfaces tunnel 12 | inc transport|line

Tunnel12 is up, line protocol is up
Tunnel protocol/transport IPSEC/IP
Tunnel transport MTU 1406 bytes <---

R1#ping 20.0.0.2 size 1406 df-bit
Type escape sequence to abort.
Sending 5, 1406-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/5/6 ms
```

Após ter aplicado o mapa de rotas, o endereço IP de Um ou Mais Servidores Cisco ICM NT é mudado à interface física do R2, não o túnel:

```
R1#show ip bgp
BGP table version is 2, local router ID is 10.0.0.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
x best-external, a additional-path, c RIB-compressed,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

Network Next Hop Metric LocPrf Weight Path
*> 20.0.0.0/24 12.0.0.2 0 0 65511 i
```

Mude o plano dos dados a fim usar o salto seguinte físico ao contrário do tamanho padrão MTU das licenças do túnel:

```
R1#ping 20.0.0.2 size 1500 df-bit
Type escape sequence to abort.
Sending 5, 1500-byte ICMP Echos to 20.0.0.2, timeout is 2 seconds:
Packet sent with the DF bit set
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/5 ms
```

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.