Configurez une session sécurisée d'eBGP avec un IPsec VTI

Contenu

Introduction

Ce document décrit comment sécuriser des relations voisines d'External Border Gateway Protocol (eBGP) avec l'utilisation d'une interface de tunnel virtuelle d'IPsec (VTI) avec les interfaces physiques (non-tunnel) pour le trafic de plan de données. Les avantages de cette configuration incluent :

- Intimité complète de la session voisine BGP avec la confidentialité des données, l'anti-relecture, l'authenticité, et l'intégrité.
- Le trafic de plan de données n'est pas contraint au temps système de Maximum Transmission Unit (MTU) de l'interface de tunnel. Les clients peuvent envoyer les paquets standard de MTU (1500 octets) sans implications ou fragmentation de représentation.
- Moins de temps système sur les Routeurs de point final puisque chiffrer de l'index de stratégie de sécurité (SPI)/déchiffrant est limité au trafic d'avion de contrôle BGP.

L'avantage de cette configuration est que le plan de données n'est pas contraint à la limite de l'interface percée un tunnel. Par conception, le trafic de plan de données n'est pas IPsec a sécurisé.

Charles contribué Stizza, ingénieur TAC Cisco.

Conditions préalables

Conditions requises

Cisco recommande de posséder des connaissances sur ces sujets :

- principes fondamentaux de configuration et de vérification d'eBGP
- Manipulation du BGP Policy Accounting (PA) utilisant un route-map
- Fonctionnalités de stratégie de base de Protocole ISAKMP (Internet Security Association and Key Management Protocol) et d'IPsec

Composants utilisés

Les informations dans ce document sont basées sur le Cisco IOS? Version de logiciel 15.3(1.3)T mais tout autre travail de versions prises en charge. Puisque la configuration d'IPsec est une caractéristique cryptographique, assurez que votre version de code contient cet ensemble de caractéristiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

> **Attention** : L'exemple de configuration dans ce document utilise les algorithmes modestes de chiffrement qui pourraient ou ne pourraient pas approprié à votre environnement. Voyez Livre Blanc de cryptage de nouvelle génération pour un examen de la Sécurité relative de diverses suites et de tailles de clé de chiffrement.

Configurez

> **Note**: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Configurations

Procédez comme suit :

1. Configurez les paramètres de la phase 1 d'Échange de clés Internet (IKE) sur R1 et R2 avec la clé pré-partagée sur R1 :**Note**: N'utilisez jamais les numéros de groupe CAD 1, 2 ou 5 puisqu'ils sont considérés inférieurs. Si possible utilisez un groupe CAD avec la curve elliptique Cryptopgraphy (ECC) comme les groupes 19, 20 ou 24. Le Norme AES (Advanced Encryption Standard) et le Secure Hash Algorithm 256 (SHA256) devraient être considérés supérieur à la norme de chiffrement de données (DES)/3DES et Message Digest 5 (MD5)/SHA1 respectivement. N'utilisez jamais le mot de passe « Cisco » dans un environnement de production.**Configuration 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
```

Configuration 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. Configurez le cryptage de mot de passe du niveau 6 pour la clé pré-partagée dans NVRAM sur R1 et R2. Ceci réduit la probabilité de la clé pré-partagée enregistrée en texte brut de l'lecture si un routeur est compromis :

```
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
```

Note: Une fois que le cryptage de mot de passe du niveau 6 est activé, la configuration active n'affiche plus la version de texte brut de la clé pré-partagée :

```
!
R1#show run | include key
crypto isakmp key 6 \Nd`]dcCW\E`^WEObUKRGKIGadiAAB address 12.0.0.2

!
```

3. Configurez les paramètres de la phase 2 d'IKE sur R1 et R2 :Configuration 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
```

Configuration 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
```

Note: L'établissement du perfect forward secrecy (PFS) est facultatif mais améliore le point fort VPN puisqu'il force une nouvelle génération de clés symétrique dans l'établissement SA de la phase 2 d'IKE.

4. Configurez les interfaces de tunnel sur R1 et R2 et les sécurisez avec le profil IPSec :Configuration 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
```

Configuration 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. Configurez le BGP sur R1 et R2 et annoncez les réseaux loopback0 dans le BGP :

Configuration 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
```

Configuration 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. Configurez un route-map sur R1 et R2 afin de changer manuellement la prochaine adresse IP de saut de sorte qu'elle indique l'interface physique et pas le tunnel. Vous devez appliquer ce route-map sur la direction d'arrivée.

Configuration 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
```

Configuration 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
```

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Vérifiez que la phase 1 d'IKE et la phase 2 d'IKE se sont terminées. La ligne protocole sur l'interface de tunnel virtuelle (VTI) ne change pas à « vers le haut de » jusqu'à ce que la phase 2 d'IKE se soit terminée :

```
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
```

Notez qu'avant l'application du route-map, la prochaine adresse IP de saut indique l'adresse IP voisine BGP qui est l'interface de tunnel :

```
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
```

Quand le trafic utilise le tunnel, le MTU est contraint au MTU de tunnel :

```
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
```

Après application du route-map, l'adresse IP n'est changée à l'interface physique de R2, pas le tunnel :

```
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
```

Changez de plan de données afin d'utiliser le prochain saut physique par opposition au MTU de taille standard d'autorisations de tunnel :

```
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
```

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.