Transfert rapide d'IKEv1 à la configuration de tunnel IKEv2 L2L sur le code ASA 8.4

Contenu

Introduction

Ce document fournit des informations sur le protocole IKEv2 et sur le procédé de migration à partir du protocole IKEv1.

Conditions préalables

Conditions requises

Assurez-vous que vous avez des dispositifs de sécurité de Cisco ASA qui exécutent IPsec avec IKEv1 la méthode d'authentification (PSK) principale pré-partagée, et vous assurez que le tunnel d'IPsec est dans l'état opérationnel.

Pour un exemple de configuration des dispositifs de sécurité de Cisco ASA qui exécutent IPsec avec la méthode d'authentification IKEv1 PSK, référez-vous à PIX/ASA 7.x et en haut : PIX--PIX À l'exemple de configuration de tunnel VPN.

Composants utilisés

Les informations dans ce document sont basées sur des ces matériel et versions de logiciel.

- Appliance de Sécurité de gamme de Cisco ASA 5510 qui fonctionne avec la version 8.4.x et ultérieures.

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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Pourquoi migrez vers IKEv2 ?

- IKEv2 fournit une meilleure résilience d'attaque réseau. IKEv2 peut atténuer une attaque DoS sur le réseau quand il valide le demandeur d'IPsec. Afin de rendre la vulnérabilité DOS difficile à exploiter, le responder peut demander un Témoin au demandeur qui doit assurer le responder que c'est une connexion normale. Dans IKEv2, les Témoins de responder atténuent l'attaque DoS de sorte que le responder ne garde pas un état du demandeur d'IKE ou n'exécute pas une exécution de D-H à moins que le demandeur retourne le Témoin envoyé par le responder. Le responder utilise la CPU minimale et n'investit aucun état dans une association de sécurité (SA) jusqu'à ce qu'il puisse complètement valider le demandeur.
- IKEv2 réduit la complexité dans l'établissement d'IPsec entre différents Produits VPN. Il augmente l'Interopérabilité et permet également une méthode standard pour des méthodes d'authentification existantes. IKEv2 fournit une Interopérabilité sans couture d'IPsec parmi des constructeurs puisqu'il offre des Technologies intégrées telles que Dead Peer Detection (DPD), le NAT Traversal (NAT-T), ou le contact initial.
- IKEv2 a moins de temps système. Avec moins de temps système, il offre la latence améliorée d'installation SA. On permet en transit de plusieurs demandes (par exemple, quand un multiple d'enfant-SAS sont installés en parallèle).
- IKEv2 a un retard réduit SA. Dans IKEv1 le retard de la création SA amplifie pendant que le volume de paquet amplifie. IKEv2 garde le même délai moyen quand le volume de paquet amplifie. Quand le volume de paquet amplifie, l'heure de chiffrer et traiter l'en-tête de paquet amplifie. Quand un nouvel établissement SA doit être créé, plus de temps est exigé. SA générée par IKEv2 est moins que celle générée par IKEv1. Pour une longueur de paquet amplifiée, le temps pris pour créer SA est presque constant.
- IKEv2 a un temps plus rapide de rekey. L'IKE v1 prend plus de temps de réintroduire SAS qu'IKEv2. Le rekey IKEv2 pour SA offre la représentation de sécurité renforcée et diminue le nombre de paquets perdus dans la transition. En raison de la redéfinition de certains mécanismes d'IKEv1 (tels que la charge utile de tos, le choix de la vie SA, et de l'unicité SPI) dans IKEv2, moins paquets sont perdus et reproduits dans IKEv2. Par conséquent, il y a moins de besoin de réintroduire SAS.

Remarque: Puisque la sécurité des réseaux peut seulement être aussi forte que le lien le plus faible, IKEv2 n'interopère pas avec IKEv1.

Aperçu de transfert

Si votre IKEv1, ou même SSL, configuration existe déjà, l'ASA rend le procédé de transfert simple. Sur la ligne de commande, sélectionnez la commande de **migrer** :

```
migrate {l2l | remote-access {ikev2 | ssl} | overwrite}
```

Choses de note :

- Définitions de mot clé :**l2l** - Ceci convertit des tunnels du courant IKEv1 l2l en IKEv2.**Accès à distance** - Ceci convertit la configuration d'Accès à distance. Vous pouvez convertir l'IKEv1 ou les groupes de tunnel SSL en IKEv2.**remplacez** - Si vous avez une configuration IKEv2 que vous souhaitez remplacer, alors ce mot clé convertit la configuration du courant IKEv1 et retire la configuration IKEv2 superflue.
- Il est important de noter qu'IKEv2 a la capacité d'utiliser des clés symétriques aussi bien qu'asymétriques pour l'authentification PSK. Quand la commande de **transfert** est sélectionnée sur l'ASA, l'ASA crée automatiquement un IKEv2 VPN avec un PSK symétrique.
- Après que la commande soit sélectionnée, les configurations du courant IKEv1 ne sont pas supprimées. Au lieu de cela IKEv1 et les configurations IKEv2 fonctionnent en parallèle et sur le même crypto map. Vous pouvez faire ceci manuellement aussi bien. Quand IKEv1 et IKEv2 exécuté en parallèle, ceci permet un demandeur d'IPsec VPN au retour d'IKEv2 à IKEv1 quand une question de protocole ou de configuration existe avec IKEv2 qui peut mener à la panne de tentative de connexion. Quand IKEv1 et IKEv2 exécuté en parallèle, il également fournit un mécanisme de repositionnement et facilite le transfert.
- Quand IKEv1 et IKEv2 exécuté en parallèle, ASA utilise un module appelé le tunnel manager/IKE commun sur le demandeur pour déterminer la version de crypto map et de protocole d'IKE pour l'utiliser pour une connexion. L'ASA préfère toujours initier IKEv2, mais s'il ne peut pas, elle retombe à IKEv1.
- Des plusieurs homologues utilisés pour la Redondance ne sont pas pris en charge avec IKEv2 sur l'ASA. Dans IKEv1, pour des raisons de redondance, on peut avoir plus d'un pair sous le même crypto map quand vous sélectionnez la commande de **pair de positionnement**. Le premier pair sera le primaire et s'il échoue, le deuxième pair donnera un coup de pied dedans. Référez-vous à l'ID de bogue Cisco CSCud22276 (clients enregistrés seulement), ENH : Les plusieurs homologues les prennent en charge pour IKEv2.

Procédé de transfert

Configuration

Dans cet exemple, IKEv1 VPN qui utilise principal pré-partagé l'authentification (PSK) existe sur l'ASA.

Remarque: La configuration illustrée ici est seulement appropriée au tunnel VPN.

Configuration ASA avec un courant IKEv1 VPN (avant transfert)

```
ASA-2(config)# sh run
ASA Version 8.4(2)
!
hostname ASA-2
!
crypto ipsec IKEv1 transform-set goset esp-3des esp-sha-hmac
crypto map vpn 12 match address NEWARK
```

```
crypto map vpn 12 set pfs group5
crypto map vpn 12 set peer <peer_ip-address>
crypto map vpn 12 set IKEv1 transform-set goset
crypto map vpn interface outside
crypto isakmp disconnect-notify
crypto IKEv1 enable outside
crypto IKEv1 policy 1
 authentication pre-share
 encryption 3des
 hash sha
 group 5
 lifetime 86400
!
tunnel-group <peer_ip-address> type ipsec-l2l
tunnel-group <peer_ip-address> ipsec-attributes
 IKEv1 pre-shared-key *****
 isakmp keepalive threshold 10 retry 3
```

Configuration ASA IKEv2 (après transfert)

Remarque: Changements marqués des italiques gras.

```
ASA-2(config)# migrate l2l
ASA-2(config)# sh run
ASA Version 8.4(2)
!
hostname ASA-2
!
crypto ipsec IKEv1 transform-set goset esp-3des esp-sha-hmac
crypto ipsec IKEv2 ipsec-proposal goset protocol esp encryption 3des protocol esp integrity sha-
1 crypto map vpn 12 match address NEWARK crypto map vpn 12 set pfs group5 crypto map vpn 12 set
peer <peer_ip-address> crypto map vpn 12 set IKEv1 transform-set goset crypto map vpn 12 set
IKEv2 ipsec-proposal goset crypto map vpn interface outside crypto isakmp disconnect-notify
crypto IKEv2 policy 1 encryption 3des integrity sha group 5 prf sha lifetime seconds 86400
crypto IKEv2 enable outside crypto IKEv1 enable outside crypto IKEv1 policy 1 authentication
pre-share encryption 3des hash sha group 5 lifetime 86400 ! tunnel-group <peer_ip-address> type
ipsec-l2l tunnel-group <peer_ip-address> ipsec-attributes IKEv1 pre-shared-key ***** isakmp
keepalive threshold 10 retry 3 IKEv2 remote-authentication pre-shared-key ***** IKEv2 local-
authentication pre-shared-key *****
```

Vérification d'établissement du tunnel IKEv2

```
ASA1# sh cry IKEv2 sa detail

IKEv2 SAs:
Session-id:12, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id   Local                Remote     Status        Role
102061223 192.168.1.1/500  192.168.2.2/500  READY    INITIATOR
     Encr: 3DES, Hash: SHA96, DH Grp:5, Auth sign: PSK,Auth verify: PSK
     Life/Active Time: 86400/100 sec
     Status Description: Negotiation done
     Local spi: 297EF9CA996102A6       Remote spi: 47088C8FB9F039AD
     Local id: 192.168.1.1
     Remote id: 192.168.2.2
      DPD configured for 10 seconds, retry 3
     NAT-T is not detected
Child sa: local selector  10.10.10.0/0 - 10.10.10.255/65535
         remote selector 10.20.20.0/0 - 10.20.20.255/65535
         ESP spi in/out: 0x637df131/0xb7224866

ASA1# sh crypto ipsec sa
interface: outside
   Crypto map tag: vpn, seq num: 12, local addr: 192.168.1.1
     access-list NEWARK extended permit ip 10.10.10.0 255.255.255.0
```

```
     10.20.20.0 255.255.255.0
     local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
     remote ident (addr/mask/prot/port): (10.20.20.0/255.255.255.0/0/0)
     current_peer: 192.168.2.2
     #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
```

Vérification PSK après transfert

Afin de vérifier votre PSK, vous pouvez exécuter cette commande en mode de configuration globale :

```
more system: running-config | beg tunnel-group
```

IKEv2 et processus maître de tunnel

Comme indiqué précédemment, l'ASA utilise un module appelé le tunnel manager/IKE commun sur le demandeur pour déterminer la version de crypto map et de protocole d'IKE pour l'utiliser pour une connexion. Sélectionnez cette commande de surveiller le module :

```
debug crypto ike-common <level>
```

Le débogage, **se connecter**, et les **commandes show** ont été collectés quand le trafic est passé pour initier le tunnel IKEv2. Pour la clarté, une partie de la sortie a été omise.

```
ASA1(config)# logging enable
ASA1(config)# logging list IKEv2 message 750000-752999
ASA1(config)# logging console IKEv2
ASA1(config)# exit
ASA1# debug crypto IKEv2 platform 4
ASA1# debug crypto IKEv2 protocol  4
ASA1# debug crypto ike-common 5

%ASA-5-752003: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv2.
Map Tag = vpn.  Map Sequence Number = 12.
%ASA-5-750001: Local:192.168.1.1:500 Remote:192.168.2.2:500 Username:Unknown
Received request to establish an IPsec tunnel; local traffic selector = Address Range:
10.10.10.11-10.10.10.11 Protocol: 0
Port Range: 0-65535; remote traffic selector = Address Range:
10.20.20.21-10.20.20.21 Protocol: 0 Port Range: 0-65535
Mar 22 15:03:52 [IKE COMMON DEBUG]Tunnel Manager dispatching a KEY_ACQUIRE
message to IKEv2.  Map Tag = vpn.  Map Sequence Number = 12.
IKEv2-PLAT-3: attempting to find tunnel group for IP: 192.168.2.2
IKEv2-PLAT-3: mapped to tunnel group 192.168.2.2 using peer IP
    26%ASA-5-750006: Local:192.168.1.1:500 Remote:192.168.2.2:500
Username:192.168.2.2 SA UP. Reason: New Connection Established
43%ASA-5-752016: IKEv2 was successful at setting up a tunnel.
Map Tag = vpn. Map Sequence Number = 12.
%ASA-7-752002: Tunnel Manager Removed entry.  Map Tag = vpn.
Map Sequence Number = 12.
IKEv2-PLAT-4: SENT PKT [IKE_SA_INIT] [192.168.1.1]:500->[192.168.2.2]:500
InitSPI=0x297ef9ca996102a6 RespSPI=0x0000000000000000 MID=00000000
IKEv2-PROTO-3: (12): Insert SA
IKEv2-PLAT-4: RECV PKT [IKE_SA_INIT] [192.168.2.2]:500->[192.168.1.1]:500
InitSPI=0x297ef9ca996102a6 RespSPI=0x47088c8fb9f039ad MID=00000000
IKEv2-PLAT-4: SENT PKT [IKE_AUTH] [192.168.1.1]:500->[192.168.2.2]:500
InitSPI=0x297ef9ca996102a6 RespSPI=0x47088c8fb9f039ad MID=00000001
IKEv2-PLAT-4: RECV PKT [IKE_AUTH] [192.168.2.2]:500->[192.168.1.1]:500
InitSPI=0x297ef9ca996102a6 RespSPI=0x47088c8fb9f039ad MID=00000001
IKEv2-PROTO-3: (12): Verify peer's policy
IKEv2-PROTO-3: (12): Get peer authentication method
IKEv2-PROTO-3: (12): Get peer's preshared key for 192.168.2.2
IKEv2-PROTO-3: (12): Verify authentication data
```

```
IKEv2-PROTO-3: (12): Use preshared key for id 192.168.2.2, key len 5
IKEv2-PROTO-2: (12): SA created; inserting SA into database
IKEv2-PLAT-3:
CONNECTION STATUS: UP... peer: 192.168.2.2:500, phase1_id: 192.168.2.2
IKEv2-PROTO-3: (12): Initializing DPD, configured for 10 seconds
IKEv2-PLAT-3: (12) DPD Max Time will be: 10
IKEv2-PROTO-3: (12): Checking for duplicate SA
Mar 22 15:03:52 [IKE COMMON DEBUG]IKEv2 was successful at setting up a tunnel.
Map Tag = vpn. Map Sequence Number = 12.
Mar 22 15:03:52 [IKE COMMON DEBUG]Tunnel Manager Removed entry.
Map Tag = vpn.  Map Sequence Number = 12.
```

IKEv2 au mécanisme de repli IKEv1

Avec IKEv1 et IKEv2 en parallèle, l'ASA préfère toujours initier IKEv2. Si l'ASA ne peut pas, elle retombe à IKEv1. Le module commun du tunnel manager/IKE gère ce processus. Dans cet exemple sur le demandeur, IKEv2 SA a été effacé et IKEv2 SIG-est maintenant exprès configuré (la proposition IKEv2 est retirée) pour expliquer le mécanisme de chute de retour.

```
ASA1# clear  crypto  IKEv2 sa%ASA-5-750007: Local:192.168.1.1:500 Remote:192.168.2.2:500
Username:192.168.2.2 SA DOWN. Reason: operator request
ASA1(config)# no crypto map vpn 12 set IKEv2 ipsec-proposal GOSET
ASA1# (config ) logging enable
ASA1# (config ) logging list IKEv2 message 750000-752999
ASA1# (config ) logging console IKEv2
ASA1# (config ) exit
ASA1# debug crypto IKEv2 platform 4
ASA1# debug crypto IKEv2 protocol  4
ASA1# debug crypto ike-common 5
%ASA-5-752004: Tunnel Manager dispatching a KEY_ACQUIRE message to IKEv1.
Map Tag = vpn.  Map Sequence Number = 12.
%ASA-4-752010: IKEv2 Doesn't have a proposal specified
Mar 22 15:11:44 [IKE COMMON DEBUG]Tunnel Manager dispatching a KEY_ACQUIRE
message to IKEv1.  Map Tag = vpn.  Map Sequence Number = 12.
Mar 22 15:11:44 [IKE COMMON DEBUG]IKEv2 Doesn't have a proposal specified
%ASA-5-752016: IKEv1 was successful at setting up a tunnel.  Map Tag = vpn.
Map Sequence Number = 12.
%ASA-7-752002: Tunnel Manager Removed entry.  Map Tag = vpn.
Map Sequence Number = 12.
Mar 22 15:11:44 [IKE COMMON DEBUG]IKEv1 was successful at setting up a tunnel.
Map Tag = vpn. Map Sequence Number = 12.
Mar 22 15:11:44 [IKE COMMON DEBUG]Tunnel Manager Removed entry.  Map Tag = vpn.
Map Sequence Number = 12.

ASA1(config)# sh cry IKEv2 sa
There are no IKEv2 SAs
ASA1(config)# sh cry IKEv1 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: 192.168.2.2
   Type    : L2L             Role    : initiator
   Rekey   : no              State   : MM_ACTIVE
```

Durcissez IKEv2

Afin de fournir la Sécurité supplémentaire quand IKEv2 est utilisé, ces commandes facultatives sont fortement recommandées :

- **Crypto Témoin-défi IKEv2** : Permet à l'ASA d'envoyer des défis de Témoin pour scruter des

périphériques en réponse aux paquets initiés par SA entrouverts.
- **Crypto maximum-SA de la limite IKEv2** : Limite le nombre de connexions IKEv2 sur l'ASA. Par défaut, la connexion du maximum autorisé IKEv2 égale le nombre maximal de connexions spécifié par le permis ASA.
- **Crypto maximum-dans-négociation-SA de la limite IKEv2** : Limite le nombre de dans-négociation IKEv2 (ouvrez-vous) SAS sur l'ASA. Une fois utilisé en même temps que la **crypto** commande du Témoin-**défi IKEv2**, assurez que le seuil de Témoin-défi est inférieur à cette limite.
- Clés asymétriques d'utilisation. Après transfert, la configuration peut être modifiée pour utiliser des clés asymétriques comme affiché ici :`ASA-2(config)# more system:running-config`
```
tunnel-group <peer_ip-address> type ipsec-l2l
tunnel-group <peer_ip-address> ipsec-attributes
 IKEv1 pre-shared-key cisco1234
 IKEv2 remote-authentication pre-shared-key cisco1234
 IKEv2 local-authentication pre-shared-key cisco123
```

Il est important de se rendre compte que la configuration doit être reflétée sur l'autre pair pour le pre-shared-key IKEv2. Cela ne fonctionnera pas si vous sélectionnez et collez la configuration d'un côté à l'autre.

Remarque: Ces commandes sont désactivées par défaut.

Informations connexes

- Soutien technique et documentation