Migration rapide de la configuration du tunnel L2L IKEv1 vers IKEv2 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 disposez d'un dispositif de sécurité Cisco ASA qui exécute IPsec avec la méthode d'authentification de clé prépartagée (PSK) IKEv1 et assurez-vous que le tunnel IPsec est opérationnel.

Pour un exemple de configuration d'un dispositif de sécurité Cisco ASA qui exécute IPsec avec la méthode d'authentification PSK IKEv1, référez-vous à PIX/ASA 7.x et versions ultérieures : Exemple de configuration d'un tunnel VPN PIX à PIX.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes .

- Appliance de sécurité de la gamme Cisco ASA 5510 qui fonctionne avec les versions 8.4.x et ultérieures.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Pourquoi migrer vers IKEv2 ?

- IKEv2 améliore la résilience des attaques réseau. IKEv2 peut limiter une attaque DoS sur le réseau lorsqu'il valide l'initiateur IPsec. Afin de rendre la vulnérabilité DoS difficile à exploiter, le répondeur peut demander un cookie à l'initiateur qui doit assurer le répondeur qu'il s'agit d'une connexion normale. Dans IKEv2, les cookies du répondeur atténuent l'attaque DoS de sorte que le répondeur ne garde pas l'état de l'initiateur IKE ou n'effectue pas une opération D-H à moins que l'initiateur ne retourne le cookie envoyé par le répondeur. Le répondeur utilise un processeur minimal et n'engage aucun état à une association de sécurité (SA) jusqu'à ce qu'il puisse valider complètement l'initiateur.
- IKEv2 réduit la complexité de l'établissement IPsec entre différents produits VPN. Elle augmente l'interopérabilité et permet également une méthode standard pour les méthodes d'authentification héritées. IKEv2 offre une interopérabilité IPsec transparente entre les fournisseurs puisqu'il offre des technologies intégrées telles que la détection DPD (Dead Peer Detection), NAT Traversal (NAT-T) ou le contact initial.
- IKEv2 a moins de surcharge. Avec moins de surcharge, il offre une meilleure latence de configuration de SA. Plusieurs demandes sont autorisées en transit (par exemple, lorsqu'un multiple de SA enfant est configuré en parallèle).
- IKEv2 a un délai de SA réduit. Dans IKEv1, le délai de création de SA s'amplifie à mesure que le volume de paquets s'amplifie. IKEv2 conserve le même délai moyen lorsque le volume de paquets est amplifié. Lorsque le volume de paquet est amplifié, le temps de cryptage et de traitement de l’en-tête de paquet est amplifié. Lorsqu'un nouvel établissement de SA doit être créé, plus de temps est nécessaire. La SA générée par IKEv2 est inférieure à celle générée par IKEv1. Pour une taille de paquet amplifiée, le temps nécessaire à la création d’une SA est presque constant.
- IKEv2 dispose d'un temps de retouche plus rapide. IKE v1 met plus de temps à reculer les SA qu'IKEv2. IKEv2 rekey for SA offre des performances de sécurité améliorées et réduit le nombre de paquets perdus en transition. En raison de la redéfinition de certains mécanismes d'IKEv1 (comme la charge utile ToS, le choix de la durée de vie de l'association de sécurité et l'unicité SPI) dans IKEv2, moins de paquets sont perdus et dupliqués dans IKEv2. Par conséquent, il est moins nécessaire de reculer des SA.

Remarque : Étant donné que la sécurité du réseau ne peut être que la liaison la plus faible, IKEv2 ne fonctionne pas avec IKEv1.

Présentation de la migration

Si votre configuration IKEv1, ou même SSL, existe déjà, l'ASA simplifie le processus de migration. Sur la ligne de commande, entrez la commande **migrate** :

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

A noter :

- Définitions de mots clés :**l2l** - Convertit les tunnels IKEv1 l2l actuels en IKEv2.**accès distant** - Convertit la configuration de l'accès distant. Vous pouvez convertir les groupes de tunnels IKEv1 ou SSL en IKEv2.**overwrite** - Si vous souhaitez remplacer une configuration IKEv2, ce mot clé convertit la configuration IKEv1 actuelle et supprime la configuration IKEv2 superflue.
- Il est important de noter que IKEv2 peut utiliser des clés symétriques et asymétriques pour l'authentification PSK. Lorsque la commande **de migration** est entrée sur l'ASA, l'ASA crée automatiquement un VPN IKEv2 avec un PSK symétrique.
- Une fois la commande entrée, les configurations IKEv1 actuelles ne sont pas supprimées. À la place, les configurations IKEv1 et IKEv2 s'exécutent en parallèle et sur la même carte de chiffrement. Vous pouvez aussi le faire manuellement. Lorsque IKEv1 et IKEv2 fonctionnent en parallèle, cela permet à un initiateur VPN IPsec de basculer d'IKEv2 à IKEv1 lorsqu'un problème de protocole ou de configuration avec IKEv2 peut entraîner une défaillance de tentative de connexion. Lorsque IKEv1 et IKEv2 fonctionnent en parallèle, il fournit également un mécanisme de restauration et facilite la migration.
- Lorsque IKEv1 et IKEv2 fonctionnent en parallèle, ASA utilise un module appelé gestionnaire de tunnel/IKE commun sur l'initiateur pour déterminer la carte de chiffrement et la version du protocole IKE à utiliser pour une connexion. L'ASA préfère toujours lancer IKEv2, mais s'il ne le peut pas, il revient à IKEv1.
- Plusieurs homologues utilisés pour la redondance n'est pas pris en charge avec IKEv2 sur l'ASA. Dans IKEv1, à des fins de redondance, il est possible d'avoir plusieurs homologues sous la même crypto-carte lorsque vous entrez la commande **set peer**. Le premier homologue sera le principal et s'il échoue, le second homologue s'y connectera. Reportez-vous à l'ID de bogue Cisco CSCud2276 (clients enregistrés uniquement) , ENH : Plusieurs homologues prennent en charge IKEv2.

Processus de migration

Configuration

Dans cet exemple, le VPN IKEv1 qui utilise l'authentification par clé prépartagée (PSK) existe sur l'ASA.

Remarque : La configuration présentée ici ne concerne que le tunnel VPN.

Configuration ASA avec un VPN IKEv1 actuel (avant la migration)

```
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 la migration)

Note : Modifications marquées en gras en italique.

```
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 de l'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 la migration

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

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

Processus IKEv2 et Tunnel Manager

Comme mentionné précédemment, l'ASA utilise un module appelé gestionnaire de tunnel/IKE commun à l'initiateur pour déterminer la carte de chiffrement et la version du protocole IKE à utiliser pour une connexion. Entrez cette commande pour surveiller le module :

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

Les commandes **debug**, **logging** et **show** ont été collectées lorsque le trafic est passé pour initier le tunnel IKEv2. Par souci de clarté, une partie du résultat 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.
```

Mécanisme de secours IKEv2 vers IKEv1

Avec IKEv1 et IKEv2 en parallèle, l'ASA préfère toujours lancer IKEv2. Si l'ASA ne le peut pas, il revient à IKEv1. Le gestionnaire de tunnel/module commun IKE gère ce processus. Dans cet exemple sur l'initiateur, la SA IKEv2 a été effacée et IKEv2 est maintenant délibérément mal configuré (la proposition IKEv2 est supprimée) pour démontrer le mécanisme de retour arrière.

```
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
```

Sécuriser IKEv2

Afin de fournir une sécurité supplémentaire lorsque IKEv2 est utilisé, les commandes facultatives suivantes sont fortement recommandées :

- **Crypto IKEv2 cookie-challenge** : Permet à l'ASA d'envoyer des problèmes de cookie aux périphériques homologues en réponse à des paquets initiés par l'association de sécurité semi-ouverts.
- **Crypto IKEv2 limit max-sa** : Limite le nombre de connexions IKEv2 sur l'ASA. Par défaut, la connexion IKEv2 maximale autorisée équivaut au nombre maximal de connexions spécifié par la licence ASA.
- **Crypto IKEv2 limit max-in-negotiation-sa** : Limite le nombre de SA en négociation (ouvertes) IKEv2 sur l'ASA. Lorsqu'il est utilisé conjointement avec la commande **crypto IKEv2 cookie-challenge**, assurez-vous que le seuil cookie-challenge est inférieur à cette limite.
- Utilisez des clés asymétriques. Après la migration, la configuration peut être modifiée pour utiliser des clés asymétriques comme indiqué 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 réaliser que la configuration doit être mise en miroir sur l'autre homologue pour la clé pré-partagée 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

- Documentation et assistance techniques