Migración rápida de la configuración del túnel IKEv1 a IKEv2 L2L en el código ASA 8.4

Contenido

Introducción

Este documento proporciona información sobre IKEv2 y el proceso de migración de IKEv1.

Prerequisites

Requirements

Asegúrese de tener un dispositivo de seguridad Cisco ASA que ejecute IPsec con el método de autenticación de clave previamente compartida (PSK) IKEv1 y asegúrese de que el túnel IPsec se encuentre en estado operativo.

Para ver un ejemplo de configuración de un Cisco ASA Security Appliance que ejecuta IPsec con el método de autenticación PSK IKEv1, refiérase a PIX/ASA 7.x y superiores: Ejemplo de Configuración de Túnel VPN PIX-to-PIX.

Componentes Utilizados

La información de este documento se basa en estas versiones de hardware y software.

- Dispositivo de seguridad Cisco ASA serie 5510 que se ejecuta con la versión 8.4.x y posteriores.

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.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

¿Por qué migrar a IKEv2?

- IKEv2 proporciona una mejor resistencia a los ataques de red. IKEv2 puede mitigar un ataque de DoS en la red cuando valida el iniciador de IPSec. Para hacer que la vulnerabilidad de DoS sea difícil de explotar, el respondedor puede pedir una cookie al iniciador que debe asegurarse al respondedor de que se trata de una conexión normal. En IKEv2, las cookies de respuesta mitigan el ataque de DoS de modo que el respondedor no mantenga un estado del iniciador IKE o no realice una operación D-H a menos que el iniciador devuelva la cookie enviada por el respondedor. El respondedor utiliza una CPU mínima y no envía ningún estado a una asociación de seguridad (SA) hasta que pueda validar completamente el iniciador.
- IKEv2 reduce la complejidad en el establecimiento de IPSec entre diferentes productos VPN. Aumenta la interoperabilidad y también permite una forma estándar de métodos de autenticación heredados. IKEv2 proporciona una interoperabilidad IPSec perfecta entre los proveedores, ya que ofrece tecnologías integradas como la detección de puntos inactivos (DPD), NAT transversal (NAT-T) o contacto inicial.
- IKEv2 tiene menos sobrecarga. Con menos sobrecarga, ofrece una latencia de configuración de SA mejorada. Se permiten varias solicitudes en tránsito (por ejemplo, cuando se configuran varias SA secundarias en paralelo).
- IKEv2 tiene un retraso de SA reducido. En IKEv1, el retraso de la creación de SA se amplifica a medida que el volumen del paquete se amplía. IKEv2 mantiene el mismo retraso medio cuando el volumen del paquete se amplía. Cuando el volumen del paquete se amplifica, se amplía el tiempo para cifrar y procesar el encabezado del paquete. Cuando se va a crear un nuevo establecimiento de SA, se necesita más tiempo. La SA generada por IKEv2 es menor que la generada por IKEv1. Para un tamaño de paquete amplificado, el tiempo que se tarda en crear una SA es casi constante.
- IKEv2 tiene un tiempo de reinicio más rápido. IKE v1 tarda más tiempo en volver a introducir las SA que IKEv2. La reclave IKEv2 para SA ofrece un rendimiento de seguridad mejorado y reduce el número de paquetes perdidos en la transición. Debido a la redefinición de ciertos mecanismos de IKEv1 (como la carga de ToS, la elección de duración de SA y la unicidad de SPI) en IKEv2, se pierden menos paquetes y se duplican en IKEv2. Por lo tanto, hay menos necesidad de volver a llaves de SA.

Nota: Debido a que la seguridad de la red sólo puede ser tan fuerte como el link más débil, IKEv2 no interactúa con IKEv1.

Descripción general de la migración

Si su configuración IKEv1, o incluso SSL, ya existe, ASA simplifica el proceso de migración. En la línea de comandos, ingrese el comando **migrar**:

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

Aspectos destacados:

- Definiciones de palabras clave:**l2l** - Esto convierte los túneles IKEv1 l2l actuales en IKEv2.**acceso remoto**: esto convierte la configuración de acceso remoto. Puede convertir los grupos de túnel IKEv1 o SSL en IKEv2.**sobrescribir**: si tiene una configuración IKEv2 que desea sobrescribir, esta palabra clave convierte la configuración IKEv1 actual y elimina la superflua configuración IKEv2.
- Es importante tener en cuenta que IKEv2 tiene la capacidad de utilizar tanto claves simétricas como asimétricas para la autenticación PSK. Cuando el comando **migration** se ingresa en el ASA, el ASA crea automáticamente una VPN IKEv2 con un PSK simétrico.
- Después de ingresar el comando, las configuraciones actuales de IKEv1 no se eliminan. En su lugar, las configuraciones IKEv1 e IKEv2 se ejecutan en paralelo y en el mismo mapa criptográfico. También puede hacerlo manualmente. Cuando IKEv1 e IKEv2 se ejecutan en paralelo, esto permite que un iniciador VPN IPsec realice una reserva de IKEv2 a IKEv1 cuando existe un problema de protocolo o configuración con IKEv2 que puede conducir a un error en el intento de conexión. Cuando IKEv1 e IKEv2 se ejecutan en paralelo, también proporciona un mecanismo de reversión y facilita la migración.
- Cuando IKEv1 e IKEv2 se ejecutan en paralelo, ASA utiliza un módulo denominado administrador de túnel/IKE común en el iniciador para determinar la versión del mapa criptográfico y del protocolo IKE que se utilizará para una conexión. El ASA siempre prefiere iniciar IKEv2, pero si no puede, vuelve a ser IKEv1.
- IKEv2 en ASA no admite varios peers utilizados para la redundancia. En IKEv1, para fines de redundancia, se puede tener más de un par bajo el mismo mapa crypto cuando se ingresa el comando **set peer**. El primer par será el primario y si falla, el segundo par se iniciará. Consulte Cisco bug ID CSCud2276 (sólo clientes registrados) , ENH: Compatibilidad con varios pares para IKEv2.

Proceso de migración

Configuración

En este ejemplo, existe una VPN IKEv1 que utiliza autenticación de clave precompartida (PSK) en el ASA.

Nota: La configuración que se muestra aquí sólo es relevante para el túnel VPN.

Configuración de ASA con una VPN IKEv1 actual (antes de la migración)

```
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
```

Configuración de ASA IKEv2 (después de la migración)

Nota: Cambios marcados en cursiva en negrita.

```
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 *****
```

Verificación de establecimiento de túnel 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
```

Verificación de PSK después de la migración

Para verificar su PSK, puede ejecutar este comando en el modo de configuración global:

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

Proceso IKEv2 y Tunnel Manager

Como se mencionó anteriormente, el ASA utiliza un módulo llamado tunnel manager/IKE común en el iniciador para determinar la versión de mapa criptográfico y protocolo IKE que se utilizará para una conexión. Ingrese este comando para monitorear el módulo:

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

Los comandos **debug**, **logging** y **show** se recopilaron cuando se pasa el tráfico para iniciar el túnel IKEv2. Para mayor claridad, se ha omitido parte del resultado.

```
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.
```

Mecanismo de reserva de IKEv2 a IKEv1

Con IKEv1 e IKEv2 en paralelo, ASA siempre prefiere iniciar IKEv2. Si el ASA no puede, vuelve a ser IKEv1. El módulo común Tunnel Manager/IKE administra este proceso. En este ejemplo en el iniciador, se borró la SA IKEv2 y ahora IKEv2 está mal configurado a propósito (se elimina la propuesta IKEv2) para demostrar el mecanismo de recuperación de fallos.

```
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
```

Reforzar IKEv2

Para proporcionar seguridad adicional cuando se utiliza IKEv2, se recomiendan estos comandos opcionales:

- **Desafío de cookie Crypto IKEv2**: Habilita el ASA para enviar desafíos de cookies a los dispositivos de peer en respuesta a los paquetes iniciados por SA semirabiertos.
- **Crypto IKEv2 limit max-sa**: Limita el número de conexiones IKEv2 en el ASA. De forma predeterminada, la conexión IKEv2 máxima permitida es igual al número máximo de conexiones especificado por la licencia ASA.
- **Crypto IKEv2 limit max-in-negotiation-sa**: Limita el número de SA IKEv2 en negociación (abiertas) en ASA. Cuando se utiliza junto con el comando **crypto IKEv2 cookie-desafío**, asegúrese de que el umbral de desafío de cookies sea inferior a este límite.
- Utilice claves asimétricas. Después de la migración, la configuración se puede modificar para utilizar claves asimétricas como se muestra aquí:

```
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
```

Es importante darse cuenta de que la configuración debe reflejarse en el otro par para la clave previamente compartida IKEv2. No funcionará si selecciona y pega la configuración de un lado al otro.

Nota: Estos comandos están inhabilitados de forma predeterminada.

Información Relacionada

- Asistencia técnica y documentación