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

Contenido

Introducción

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

prerrequisitos

Requisitos

Asegúrese de que usted tenga un dispositivo de seguridad de Cisco ASA que ejecute el IPSec con el método de autentificación de la clave previamente compartida IKEv1 (PSK), y se asegure que el túnel IPsec está en el estado operacional.

Para un ejemplo de configuración de un dispositivo de seguridad de Cisco ASA que ejecute el IPSec con el método de autentificación del PSK IKEv1, refiera al PIX/ASA 7.x y arriba: Ejemplo de la configuración del túnel PIX-a-PIX VPN.

Componentes Utilizados

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

- Dispositivo de seguridad de las 5510 Series de Cisco ASA que se ejecuta con la versión 8.4.x y posterior.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

¿Por qué emigre a IKEv2?

- IKEv2 proporciona una mejor resistencia del ataque a la red. IKEv2 puede atenuar un ataque DOS en la red cuando valida el iniciador del IPSec. Para hacer la vulnerabilidad DOS difícil explotar, el respondedor puede pedir un Cookie al iniciador que tiene que asegurar al respondedor que esto es una conexión normal. En IKEv2, los Cookie del respondedor atenúan el ataque DOS de modo que el respondedor no guarde un estado del iniciador IKE ni realice una operación del D-H a menos que el iniciador vuelva el Cookie enviado por el respondedor. El respondedor utiliza el CPU mínimo y no confía ningún estado a una asociación de seguridad (SA) hasta que pueda validar totalmente el iniciador.
- IKEv2 reduce la complejidad en el establecimiento del IPSec entre diversos productos VPN. Aumenta la Interoperabilidad y también permite a un modo estándar para los métodos de autentificación de la herencia. IKEv2 proporciona una Interoperabilidad inconsútil del IPSec entre los vendedores puesto que ofrece las Tecnologías incorporadas tales como Dead Peer Detection (DPD), Traversal NAT (NAT-T), o contacto inicial.
- IKEv2 tiene menos gastos indirectos. Con menos gastos indirectos, ofrece el tiempo de espera mejorado de la configuración SA. Las peticiones múltiples se permiten adentro transitan (por ejemplo, cuando un múltiplo de los niño-SA se configura paralelamente).
- IKEv2 tiene un retardo reducido SA. En IKEv1 el retardo de la creación SA amplifica mientras que el volumen del paquete amplifica. IKEv2 guarda el mismo retraso promedio cuando el volumen del paquete amplifica. Cuando el volumen del paquete amplifica, la época de cifrar y de procesar el encabezado de paquete amplifica. Cuando un nuevo establecimiento SA debe ser creado, se requiere más tiempo. El SA generado por IKEv2 es menos que el que está generado por IKEv1. Para un tamaño de paquetes amplificado, el tiempo llevado para crear un SA es casi constante.
- IKEv2 tiene más rápidamente reintroducir el tiempo. El v1 IKE tarda más tiempo para reintroducir los SA que IKEv2. IKEv2 reintroducen para el funcionamiento mejorado las ofertas de la Seguridad SA y disminuyen el número de Packets Lost en la transición. Debido a la redefinición de ciertos mecanismos de IKEv1 (tales como payload TOS, opción del curso de la vida SA, y de la unicidad de SPI) en IKEv2, menos paquetes se pierden y se duplican en IKEv2. Por lo tanto, hay menos necesidad de reintroducir los SA.

Nota: Porque la seguridad de la red puede solamente ser tan fuerte como el link más débil, IKEv2 no interopera con IKEv1.

Descripción de la migración

Si existe su IKEv1, o aún el SSL, configuración ya, el ASA hace el proceso de migración simple. En la línea de comando, ingrese el comando de la **migración**:

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

Cosas de la nota:

- Definiciones de la palabra clave:**l2l** - Esto convierte los túneles actuales IKEv1 l2l a IKEv2.**Acceso Remoto** - Esto convierte la configuración del Acceso Remoto. Usted puede convertir el IKEv1 o los grupos de túnel SSL a IKEv2.**sobregrabe** - Si usted tiene una configuración IKEv2 que usted desee sobregrabar, después esta palabra clave convierte la configuración actual IKEv1 y quita la configuración superflua IKEv2.
- Es importante observar que IKEv2 tiene la capacidad de utilizar las claves simétricas así como asimétricas para la autenticación del PSK. Cuando el comando de la **migración** se ingresa en el ASA, el ASA crea automáticamente un IKEv2 VPN con un PSK simétrico.
- Después de que se ingrese el comando, las configuraciones actuales IKEv1 no se borran. En lugar IKEv1 y configuraciones IKEv2 funcionadas con paralelamente y en la misma correspondencia de criptografía. Usted puede hacer esto manualmente también. Cuando IKEv1 e IKEv2 se ejecutan paralelamente, éste permite un iniciador del IPSec VPN al retraso de IKEv2 a IKEv1 cuando un protocolo o el problema de configuración existe con IKEv2 que pueda llevar al error del intento de conexión. Cuando IKEv1 e IKEv2 ejecutado paralelamente, él también proporciona un mecanismo de la restauración no actualizada y hace la migración más fácil.
- Cuando IKEv1 e IKEv2 ejecutado paralelamente, ASA utiliza un módulo llamado el túnel manager/IKE común en el iniciador para determinar la correspondencia de criptografía y la versión del IKE Protocol para utilizar para una conexión. El ASA prefiere siempre iniciar IKEv2, pero si no puede, recurre a IKEv1.
- No soportan a los peeres múltiples usados para la Redundancia con IKEv2 en el ASA. En IKEv1, para los propósitos de la redundancia, uno puede tener más de un par bajo misma correspondencia de criptografía cuando usted ingresa el **comando set peer**. El primer par será el primario y si falla, el segundo par golpeará con el pie adentro. Refiera al Id. de bug Cisco CSCud22276 (clientes registrados solamente), ENH: Los peeres múltiples soportan para IKEv2.

Proceso de migración

Configuración

En este ejemplo, IKEv1 VPN que utiliza la clave previamente compartida (PSK) autenticación existe en el ASA.

Nota: La configuración mostrada aquí es solamente relevante al túnel VPN.

Configuración ASA con un IKEv1 actual VPN (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 ASA IKEv2 (después de la migración)

Nota: Cambios marcados en las negrita cursivas.

```
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 del establecimiento del 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 del PSK después de la migración

Para verificar su PSK, usted puede funcionar con este comando en el modo de configuración global:

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

IKEv2 y proceso de administrador del túnel

Según lo mencionado antes, el ASA utiliza un módulo llamado el túnel manager/IKE común en el iniciador para determinar la correspondencia de criptografía y la versión del IKE Protocol para utilizar para una conexión. Ingrese este comando de monitorear el módulo:

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

Recogieron el **debug**, el **registro**, y a los **comandos show** cuando el tráfico se pasa para iniciar el túnel IKEv2. Para mayor clareza, algo de la salida se ha omitido.

```
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 al mecanismo de repliegue IKEv1

Con IKEv1 e IKEv2 paralelamente, el ASA prefiere siempre iniciar IKEv2. Si no puede el ASA, recurre a IKEv1. El módulo común del túnel manager/IKE maneja este proceso. En este ejemplo en el iniciador, IKEv2 SA fue borrado e IKEv2 es adrede mis configurado ahora (se quita la oferta IKEv2) demostrar el mecanismo de la caída detrás.

```
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
```

Endurezca IKEv2

Para proporcionar la seguridad complementaria cuando se utiliza IKEv2, recomiendan estos comandos opcionales altamente:

- **Cookie-desafío Crypto IKEv2**: Permite al ASA para enviar los desafíos del Cookie a los dispositivos de peer en respuesta a los paquetes iniciados SA medio abiertos.
- **MAX-sa Crypto del límite IKEv2**: Limita el número de las conexiones IKEv2 en el ASA. Por abandono, el máximo no prohibido la conexión IKEv2 iguala la cantidad máxima de conexiones especificada por la licencia ASA.
- **MAX-en-negociación-sa Crypto del límite IKEv2**: Limita el número de la en-negociación IKEv2 (ábrase) SA en el ASA. Cuando está utilizado conjuntamente con el comando **crypto del Cookie-desafío IKEv2**, asegúrese que el umbral del Cookie-desafío es más bajo que este límite.
- Utilice las claves asimétricas. Después de la migración, la configuración se puede modificar para utilizar las 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 realizar que la configuración necesita ser duplicada en el otro par para la clave previamente compartida IKEv2. No trabajará si usted selecciona y pega la configuración a partir de un lado al otro.

Nota: Estos comandos se inhabilitan por abandono.

Información Relacionada

- Soporte técnico y documentación