

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

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[¿Por qué emigre a IKEv2?](#)

[Descripción de la migración](#)

[Proceso de migración](#)

[Configuración](#)

[Verificación del establecimiento del túnel IKEv2](#)

[Verificación del PSK después de la migración](#)

[IKEv2 y proceso de administrador del túnel](#)

[IKEv2 al mecanismo de repliegue IKEv1](#)

[Endurezca IKEv2](#)

[Información Relacionada](#)

[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 autenticación 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 autenticación 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 autenticación 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.**sobregrebe** - Si usted tiene una configuración IKEv2 que usted desee sobregrebar, 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

```
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 PSK después de la migración

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

```
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 *****

```

[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:

```

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 *****
```

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

```
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 *****
```

[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.

```
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 *****
```

```
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 ******

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)# 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 *****
```

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](#)