Solución de problemas comunes de GETVPN

Contenido

Introducción

Este documento describe las depuraciones que se deben recopilar para la mayoría de los problemas comunes de GETVPN (Group Encrypted Transport VPN).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- GETVPN
- Uso del servidor Syslog

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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.

Información general - Herramientas de resolución de problemas de GETVPN

GETVPN proporciona un amplio conjunto de herramientas de resolución de problemas para facilitar el proceso de resolución de problemas. Es importante comprender cuáles de estas herramientas están disponibles y cuándo son adecuadas para cada tarea de resolución de problemas. Al solucionar problemas, siempre es una buena idea comenzar con los métodos menos intrusivos, de modo que el entorno de producción no se vea afectado negativamente. Para ayudar a ese proceso, esta sección describe algunas de las herramientas más utilizadas disponibles:

Herramientas de depuración del plano de control

Comandos show

Los comandos show se utilizan comúnmente para mostrar las operaciones en tiempo de ejecución en un entorno GETVPN.

Registros del sistema

GETVPN tiene un conjunto mejorado de mensajes syslog para eventos de protocolo significativos y condiciones de error. Este debe ser siempre el primer lugar en el que buscar antes de ejecutar cualquier depuración.

Seguimiento de eventos de dominio de interpretación de grupo (GDOI)

Esta función se agregó en la versión 15.1(3)T. El seguimiento de eventos ofrece un seguimiento ligero y siempre activo para eventos y errores GDOI significativos. También hay un seguimiento de trayectoria de salida con seguimiento habilitado para las condiciones de excepción.

Depuraciones condicionales GDOI

Esta función se agregó en la versión 15.1(3)T. Permite depuraciones filtradas para un dispositivo determinado en función de la dirección de peer y siempre se deben utilizar cuando sea posible, especialmente en el servidor de claves.

Depuraciones globales de cifrado y GDOI

Estos son los diversos debugs de GETVPM. Los administradores deben tener precaución al depurar en entornos a gran escala. Con las depuraciones GDOI, se proporcionan cinco niveles de depuración para mayor granularidad de depuración:

```
GM1#debug crypto gdoi gm rekey ?
all-levels All levels
detail Detail level
error Error level
event Event level
packet Packet level
terse Terse level
```

Nivel de	Lo que obtendrá

depuración	
Error	Condiciones de error
Terse	Mensajes importantes para el usuario y problemas de protocolo
Evento	Transiciones de estado y eventos como enviar y recibir claves
Detalle	Información más detallada del mensaje de depuración
Paquete	Incluye volcado de información detallada del paquete
Todos	Todo lo anterior

Herramientas de depuración del plano de datos

Estas son algunas de las herramientas de depuración del plano de datos:

- Listas de acceso
- Contabilización de Precedencia de IP
- Netflow
- Contadores de interfaz
- Contadores criptográficos
- Contadores de caídas globales y por función de IP Cisco Express Forwarding (CEF)
- Captura de paquetes integrada (EPC)
- Depuraciones del plano de datos (depuraciones de CEF y paquetes IP)

Troubleshoot

Preparación de la instalación de registro y otras prácticas recomendadas

Antes de comenzar a solucionar problemas, asegúrese de haber preparado la función de registro como se describe aquí. A continuación se enumeran algunas prácticas recomendadas:

- Verifique la cantidad de memoria libre del router y configure el **debugging almacenado en buffer** a un valor grande (10 MB o más si es posible).
- Inhabilite el registro en los servidores de consola, monitor y syslog.
- Recupere el contenido del buffer de registro con el comando **show log** a intervalos regulares, cada 20 minutos a una hora, para evitar la pérdida de registros debido a la reutilización del buffer.

- Independientemente de lo que suceda, introduzca el comando **show tech** de los miembros del grupo afectados (GM) y los servidores clave (KS), y examine el resultado del comando **show ip route** en global y cada Virtual Routing and Forwarding (VRF) involucrado, si es necesario.

- Utilice el protocolo de tiempo de red (NTP) para sincronizar el reloj entre todos los dispositivos que se depuran. Habilite las marcas de tiempo en milisegundos (msec) para los mensajes de depuración y registro:

```
service timestamps debug datetime msec
service timestamps log datetime msec
```

- Asegúrese de que los resultados del comando show estén marcados con el tiempo.

```
Router#terminal exec prompt timestamp
```

- Cuando recopila los resultados del comando show para los eventos del plano de control o los contadores del plano de datos, recopila siempre varias iteraciones del mismo resultado.

Solución de problemas de establecimiento IKE

Cuando comienza el proceso de registro, los GM y KS negocian sesiones de intercambio de claves de Internet (IKE) para proteger el tráfico GDOI.

- En el GM, verifique que el IKE se haya establecido correctamente:

```
gm1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
172.16.1.9 172.16.1.1 GDOI_REKEY 1068 ACTIVE
172.16.1.1 172.16.1.9 GDOI_IDLE 1067 ACTIVE
```

  Nota: El estado GDOI_IDLE, que es la base del registro, se agota rápidamente y desaparece, porque ya no se necesita después del registro inicial.

- En el KS, debe ver:

```
ks1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst src state conn-id status
172.16.1.1 172.16.1.9 GDOI_IDLE 1001 ACTIVE
```

  Nota: La sesión de nueva clave sólo aparece cuando se necesita en el KS.

Complete estos pasos si no alcanza ese estado:

- Para obtener información sobre la causa de la falla, verifique el resultado de este comando:

```
router# show crypto isakmp statistics
```

- Si el paso anterior no es útil, puede obtener información de nivel de protocolo si habilita las depuraciones IKE habituales:
  ```
  router# debug crypto isakmp
  ```
  Notas:
  * Aunque se utiliza IKE, no se utiliza en el puerto UDP/500 habitual, sino en UDP/848.
  * Si encuentra un problema en este nivel, proporcione las depuraciones tanto para el KS como para el GM afectado.

- Debido a la dependencia de los registros de Rivest-Shamir-Adleman (RSA) para las llaves del grupo, el KS **debe tener** una clave RSA configurada y debe tener el mismo nombre que el especificado en la configuración del grupo.

  Para verificar esto, ingrese este comando:

  ```
  ks1# show crypto key mypubkey rsa
  ```

Solución de problemas del registro inicial

En el GM, para verificar el estado del registro, examine el resultado de este comando:

```
gm1# show crypto gdoi | i Registration status
Registration status  : Registered
gm1#
```

Si el resultado indica algo que no sea **Registered**, ingrese estos comandos:

Sobre los MM:

- Cierre las interfaces activadas por criptografía.
  Precaución: Se espera que se habilite la administración fuera de banda.

- Habilitar estos debugs:

  ```
  gm1# debug crypto gdoi infra packet
  gm1# debug crypto gdoi gm packet
  ```

- Habilite las depuraciones en el lado de KS (consulte la siguiente sección).

- Cuando los debugs de KS estén listos, descierre las interfaces con cifrado habilitado y espere al registro (para acelerar el proceso, ejecute el comando **clear crypto gdoi** en el GM).

En los KS:

- Verifique la presencia de la clave RSA en el KS:

  ```
  ks1# show crypto key mypubkey rsa
  ```

- Habilitar estos debugs:

```
ks1# debug crypto gdoi infra packet
ks1# debug crypto gdoi ks packet
```

Solución de problemas relacionados con políticas

El problema de la política se produce antes del registro (relacionado con la política de cierre de fallos)

Esta cuestión sólo afecta a los MM, por lo que debe recopilarse este resultado del MM:

```
gm1# show crypto ruleset
```

> **Nota:** En Cisco IOS-XE?, esta salida siempre está vacía ya que la clasificación de paquetes no se realiza en el software.

La salida del comando **show tech** del dispositivo afectado proporciona el resto de la información requerida.

El problema de la política se produce tras el registro y pertenece a la política global que se envía

Por lo general, hay dos maneras en que este problema se manifiesta:

- El SK no puede imponer las políticas al MM.
- Entre los MM se aplica parcialmente la política.

Para ayudar a resolver cualquier problema, complete estos pasos:

1. En el MM afectado, recopile este resultado:

```
gm1# show crypto gdoi acl
gm1# show crypto ruleset
```

2. Habilitar estos debugs en GM:

```
gm1# debug crypto gdoi infra packet
gm1# debug crypto gdoi gm acls packet
```

3. En el SK al que se registra el MM afectado, recopile este resultado:

```
ks1# show crypto gdoi ks members
ks1# show crypto gdoi ks policy
```

Nota: Para identificar a qué KS se conecta el GM, ingrese el comando **show crypto gdoi group**.

4. En el mismo KS, habilite estos debugs:

```
ks1# debug crypto gdoi infra packet
ks1# debug crypto gdoi ks acls packet
```

5. Obligar al MM a registrarse con este comando en el MM:

```
clear crypto gdoi
```

El problema de política se produce tras el registro y se relaciona con la combinación de políticas globales y anulaciones locales

Este problema generalmente se manifiesta en la forma de mensajes que indican que se recibió un paquete cifrado para el cual las políticas locales indican que no se supone que se debe cifrar y viceversa. Todos los datos solicitados en la sección anterior y el resultado del comando **show tech** son necesarios en este caso.

Solución de problemas de reclave

Sobre los MM:

- Recopile estas depuraciones:

```
gm1# debug crypto gdoi infra packet
gm1# debug crypto gdoi gm packet
gm1# debug crypto gdoi gm rekey packet
```

- Ingrese este comando para verificar que el GM todavía tenga una Asociación de Seguridad IKE (SA) del tipo GDOI_REKEY:

```
gm1# show crypto isakmp sa
```

En los KS:

- Recopile el resultado del comando **show crypto key mypubkey rsa** de **CADA** KS. Se espera que las claves sean **idénticas**.

- Ingrese estos debugs para ver lo que ocurre en el KS:

```
ks1# debug crypto gdoi infra packet
ks1# debug crypto gdoi ks packet
ks1# debug crypto gdoi ks rekey packet
```

Resolución de problemas de Anti-Replay basado en tiempo (TBAR)

La función TBAR requiere tiempo en los grupos y, por lo tanto, se deben resincronizar constantemente los relojes pseudo-horarios GMs. Esto se realiza durante el reinicio o cada dos horas, lo que ocurra primero.

> **Nota:** Todos los resultados y las depuraciones deben recopilarse al mismo tiempo tanto de GM como de KS para que puedan correlacionarse adecuadamente.

Para investigar los problemas que se producen en este nivel, recopile este resultado.

- Sobre los MM:

```
gm1# show crypto gdoi
gm1# show crypto gdoi replay
```

- En el KS:

```
ks1# show crypto gdoi ks members
ks1# show crypto gdoi ks replay
```

Para investigar el tiempo de TBAR de una manera más dinámica, habilite estas depuraciones:

- Sobre el MM:

```
gm1# debug crypto gdoi gm rekey packet
gm1# debug crypto gdoi replay packet (verbosity might need to be lowered)
```

- En el KS:

```
ks1# debug crypto gdoi ks rekey packet
ks1# debug crypto gdoi replay packet (verbosity might need to be lowered)
```

A partir de la versión 15.2(3)T del IOS de Cisco, se ha agregado la capacidad de registrar errores TBAR, lo que facilita la detección de estos errores. En el GM, utilice este comando para verificar si hay errores TBAR:

```
R103-GM#show crypto gdoi gm replay
Anti-replay Information For Group GETVPN:
```

```
 Timebased Replay:
   Replay Value             : 512.11 secs
   Input Packets            : 0        Output Packets           : 0
   Input Error Packets    : 0        Output Error Packets   : 0
   Time Sync Error          : 0        Max time delta           : 0.00secs

TBAR Error History (sampled at 10pak/min):
   No TBAR errors detected
```

Para obtener más información sobre cómo resolver problemas de TBAR, refiérase a Error Anti-Replay Basado en Tiempo.

Solución de problemas de redundancia de KS

La cooperativa (COOP) establece una sesión IKE para proteger la comunicación entre los KS, de modo que la técnica de resolución de problemas previamente descrita para el establecimiento de IKE también es aplicable aquí.

La solución de problemas específica de COOP incluye verificaciones de salida de este comando en todos los KS involucrados:

```
ks# show crypto gdoi ks coop
```

> **Nota:** El error más común que se comete con la implementación de COOP KS es olvidar importar la misma clave RSA (privada y pública) para el grupo en todos los KS. Esto causa problemas durante los rekeys. Para verificar y comparar las claves públicas entre los KS, compare el resultado del comando **show crypto key mypubkey rsa** de cada KS.

Si se requiere la resolución de problemas a nivel de protocolo, habilite este debug en todos los KS involucrados:

```
ks# debug crypto gdoi ks coop packet
```

Preguntas frecuentes

¿Por qué aparece este mensaje de error "% Setting rekey authentication reject"?

Aparece este mensaje de error cuando configura el KS después de agregar esta línea:

```
KS(gdoi-local-server)#rekey authentication mypubkey rsa GETVPN_KEYS
% Setting rekey authentication rejected.
```

La razón de este mensaje de error es generalmente porque la clave etiquetada GETVPN_KEYS no existe. Para corregir esto, cree una clave con la etiqueta correcta usando el comando:

```
crypto key generate rsa mod <modulus> label <label_name>
```

> **Nota:** Agregue la palabra clave exportable al final si se trata de una implementación COOP y, a continuación, importe la misma clave en el otro KS

¿Puede un router configurado como KS para un grupo GETVPN funcionar también como GM para el mismo grupo?

No. Todas las implementaciones de GETVPN requieren un KS dedicado que no puede participar como GM para los mismos grupos. Esta función no se admite, porque agregar funcionalidad GM a KS con todas las interacciones posibles como cifrado, routing, QoS, etc., no es óptimo para el estado de este dispositivo de red crucial. Debe estar disponible en todo momento para que funcione toda la implementación de GETVPN.

Información Relacionada

- VPN de transporte cifrado de grupo (GET VPN) - Cisco Systems
- Soporte Técnico y Documentación - Cisco Systems