Problemas comunes del Troubleshooting GETVPN

Contenido

Introducción

Este documento describe qué debugs publica recoger para la mayor parte del transporte cifrado grupo común VPN (GETVPN).

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- GETVPN
- Uso del servidor de Syslog

Componentes Utilizados

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

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.

Información previa - Herramientas de Troubleshooting GETVPN

GETVPN proporciona un conjunto extenso de las herramientas de Troubleshooting para facilitar el proceso del Troubleshooting. Es importante entender cuáles de estas herramientas están disponibles, y cuando son apropiados para cada tarea de Troubleshooting. Al resolver problemas, es siempre una buena idea comenzar con los menos métodos intrusos, para no afectar el entorno de producción negativamente. Para ayudar a ese proceso, esta sección describe algunas de las herramientas de uso general disponibles:

Controle las herramientas de debugging planas

Comandos show

Los comandos show son de uso general para mostrar las operaciones del tiempo de ejecución en un entorno GETVPN.

Registros del sistema

GETVPN tiene un conjunto aumentado de los mensajes de Syslog para los eventos y las condiciones de error significativos del protocolo. Éste debe siempre ser el primer lugar a mirar antes de que usted ejecute cualquier debug.

Dominio del grupo de la traza del evento de la interpretación (GDOI)

Esta característica fue agregada en la versión 15.1(3)T. El seguimiento de evento ofrece al peso ligero, siempre-en el seguimiento para los eventos significativos y los errores GDOI. Hay también seguimiento de la salida-trayectoria con el traceback habilitado para las condiciones de excepción.

Debugs condicionales GDOI

Esta característica fue agregada en la versión 15.1(3)T. Permite los debugs filtrados para un dispositivo dado basado en la dirección de peer, y debe ser utilizada siempre cuando es posible, especialmente en el servidor dominante.

Debugs Crypto y GDOI globales

Éstos son los todos los diversos debugs GETVPM. Admins debe tener cuidado al hacer el debug de en los entornos en grande. Con los debugs GDOI, cinco niveles de debug se proporcionan para el granularity adicional del debugging:

```
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 debug	Qué usted conseguirá
Error	Condiciones de error

Conciso	Mensajes importantes al usuario y a los problemas del protocolo
Evento	Las transiciones de estado y los eventos por ejemplo envían y reciben reintroducen
Detalle	La mayoría de la información de mensajes detallada del debug
Paquete	Incluye el volcado de la información del paquete detallada
Todos	Todo el arriba

Herramientas de debugging planas de los datos

Aquí están las herramientas de debugging del avión de un ciertos datos:

- Listas de acceso
- Contabilización de Precedencia de IP
- Netflow
- Contadores de la interfaz
- Contadores Crypto
- Cisco Express Forwarding (CEF) IP global y contadores de caídas de la Por-característica
- Captura de paquetes integrada (EPC)
- Debugs del avión de los datos (paquete del IP y debugs CEF)

Troubleshooting

Preparación de la instalación de explotación forestal y otras mejores prácticas

Antes de que usted comience a resolver problemas, asegúrese de que usted haya preparado la instalación de explotación forestal según lo descrito aquí. Algunas mejores prácticas también se enumeran aquí:

- Marque la cantidad de memoria libre del router, y el **debugging guardada en la memoria intermedia del registro de la** configuración a un valor grande (10 MB o más si es posible).
- Inhabilite el registro a la consola, al monitor, y a los servidores de Syslog.
- Extraiga el contenido de memoria intermedia de registro con el **comando show log** a intervalos regulares, cada 20 minutos a una hora, para prevenir la pérdida del registro debida mitigar la reutilización.

- Sea cual sea sucede, ingrese el **comando show tech de los** miembros afectados del grupo (GMs) y de los servidores dominantes (KSs), y examine la salida del **comando show ip route** en global y cada ruteo virtual y expedición (VRF) implicaron, si se requieren ningunos.

- Utilice el Network Time Protocol (NTP) para sincronizar el reloj entre todos los dispositivos se hagan el debug de que. Habilite los grupos fecha/hora del milisegundo (milisegundo) para el debug y los mensajes del registro:

```
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
```

- Aseegurese las salidas del comando show son con impresión horaria.

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

- Cuando usted recoge las salidas del comando show para el control acepillan los eventos o los contadores planos de los datos, recogen siempre las iteraciones múltiples de la misma salida.

Establecimiento de IKE del Troubleshooting

Cuando el proceso de inscripción primero comienza, GMs y KSs negocian las sesiones del Internet Key Exchange (IKE) para proteger el tráfico GDOI.

- En el GM, control que el IKE está establecido con éxito:

```
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
```

Note: El estado GDOI_IDLE, que es la base del registro, mide el tiempo hacia fuera rápidamente y desaparece, porque no se necesita más después del registro inicial.

- En el KS, usted 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
```

Note: La sesión de la reintroducción aparece solamente cuando está necesitada en el KS.

Complete estos pasos si usted no alcanza ese estado:

- Para la penetración sobre la causa del error, marque la salida de este comando:
  ```
  router# show crypto isakmp statistics
  ```
- Si el paso anterior no es útil, usted puede conseguir las penetraciones del nivel del protocolo si usted habilita los debugs usuales IKE:
  ```
  router# debug crypto isakmp
  ```
  Notas:
  * Aunque se utiliza el IKE, no se utiliza en el puerto usual UDP/500, sino bastante en UDP/848.
  * Si usted encuentra un problema a este nivel, proporcione los debugs para KS y el GM afectado.

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

  Para marcar esto, ingrese este comando:

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

Resuelva problemas el registro inicial

En el GM, para marcar el estado de registro, examine la salida de este comando:

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

Si la salida indica cualquier cosa con excepción de **registrado**, ingrese estos comandos:

En el GMs:

- Interfaces crypto-habilitadas apagadas.
  Caution: Se espera que la administración fuera de banda esté habilitada.

- Habilite estos debugs:

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

- Habilite los debugs en el lado KS (véase la siguiente sección).

- Cuando los debugs KS están listos, el unshut crypto-habilitado interconecta, y espera para el registro (para acelerar el proceso, publique el comando **crypto claro del gdoi** en el GM).

En el KSs:

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

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

- Habilite estos debugs:

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

Resuelva problemas los problemas Directiva-relacionados

El problema de políticas ocurre antes del registro (la directiva relacionada del Fracaso-cierre)

Este problema afecta solamente a GMs, así que recoja esta salida del GM:

```
gm1# show crypto ruleset
```

> **Note**: ¿En el Cisco IOS XE? , esta salida está siempre vacía desde la clasificación de paquetes en no hecho en el software.

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

El problema de políticas ocurre registro del POSTE, y pertenece a la política global se avanza que

Hay generalmente dos maneras que este problema manifiesta:

- El KS no puede avanzar las directivas al GM.
- Hay una aplicación parcial de la directiva entre el GMs.

Para ayudar a resolver problemas cualquier problema, complete estos pasos:

1. En el GM afectado, recoja esta salida:

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

2. Habilite estos debugs en el GM:

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

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

3. En el KS al cual los registros afectados GM, recogen esta salida:

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

Note: Para identificar con las cuales KS el GM conecta, ingrese el **comando group crypto del gdoi de la demostración**.

4. En el mismo KS, habilite estos debugs:

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

5. Fuerce el GM a registrarse con este comando en el GM:

```
clear crypto gdoi
```

El problema de políticas ocurre registro del POSTE, y pertenece a la fusión de la política global y el Local reemplaza

Este problema se manifiesta generalmente bajo la forma de mensajes que indiquen que un paquete encriptado fue recibido para el cual las políticas locales indican que no está supuesto ser cifrado y vice versa. Todos los datos pedidos en la sección anterior y la salida del **comando show tech** se requieren en este caso.

El Troubleshooting reintroduce los problemas

En el GMs:

- Recoja estos debugs:

```
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 tiene una asociación de seguridad IKE (SA) del tipo GDOI_REKEY:

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

En el KSs:

- Recoja el **comando show crypto key mypubkey rsa** hecho salir de **CADA** KS. Se espera que las claves sean **idénticas**.

- Ingrese estos debugs para ver qué ocurre en el KS:

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

Resuelva problemas la Anti-respuesta del time basado (TBAR)

La característica TBAR requiere la tiempo-custodia a través de los grupos, y por lo tanto requiere los relojes del pseudo-tiempo de GMs resynced constantemente. Esto se realiza durante reintroduce o cada dos horas, cualquiera viene primero.

> **Note**: Toda la salida y debugs se deben recoger al mismo tiempo de GMs y de KS para poderlos correlacionar apropiadamente.

Para investigar los problemas que ocurren a este nivel, recoja esta salida.

- En el GMs:

```
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 TBAR tiempo-que guarda en una más forma dinámica, habilite estos debugs:

- En el GM:

```
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 de IOS 15.2(3)T de Cisoc, se ha agregado la capacidad de registrar los errores TBAR, que hace más fácil manchar estos errores. En el GM, utilice este comando para marcar si hay algunos 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 más información sobre cómo resolver problemas los problemas TBAR, refiera al error basado tiempo de la Anti-respuesta.

Resuelva problemas la Redundancia KS

La cooperativa (GALLINERO) establece una sesión IKE para proteger la comunicación de los interKSs, así que las técnicas de Troubleshooting descritas previamente para el establecimiento de IKE es aplicable aquí también.

el troubleshooting Gallinero-específico comprende los controles de la salida de este comando en todo el KSs implicó:

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

> **Note**: La mayoría del error común incurrido en con el despliegue del GALLINERO KSs es olvidar importar la misma clave RSA (soldado y público) para el grupo en todo el KSs. Esto causa los problemas durante reintroduce. Para marcar y comparar las claves públicas entre KSs, compare la salida del **comando show crypto key mypubkey rsa de** cada KS.

Si se requiere el troubleshooting del nivel del protocolo, habilite este debug en todo el KSs implicó:

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

FAQ

¿Por qué usted ve este de la configuración del mensaje de error “% reintroducir la autenticación rechazada”?

Usted ve este mensaje de error cuando usted configura el KS después de que se agregue esta línea:

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

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

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

> **Note**: Agregue la palabra clave exportable en el extremo si esto es un despliegue del GALLINERO y después importe la misma clave en el otro KS

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

No. Todas las implementaciones GETVPN requieren un KS dedicado que no pueda participar como GM para los mismos grupos. Esta característica no se soporta, porque agrega las funciones GM a KS con todas las interacciones posibles como el cifrado, la encaminamiento, QoS, el etc., no es óptima para la salud de este dispositivo de red crucial. Debe estar disponible siempre para que el despliegue entero GETVPN trabaje.

Información Relacionada

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