Configuración y resolución de problemas del cifrado de la capa de red de Cisco: Antecedentes - Parte 1

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Convenciones
Información general y configuración del cifrado de la capa de red
Fondo de criptografía
Definiciones
Información preliminar
Advertencias
Configuración de Cifrado de Capa de Red de Cisco IOS
Paso 1: Generar manualmente pares de claves DSS
Paso 2: Intercambio manual de las claves públicas de DSS con pares (fuera de banda)
Ejemplo 1: Configuración de Cisco IOS para el link dedicado
Ejemplo 2: Configuración de Cisco IOS para Frame Relay Multipunto
Ejemplo 3: Cifrado de y hasta un router
Ejemplo 4: Crypto con DDR
Ejemplo 5: Cifrado del tráfico IPX en un túnel IP
Ejemplo 6: Cifrado de túneles L2F
Resolución de problemas
Resolución de problemas de Cisco 7200 con ESA
Resolución de problemas de VIP2 con ESA
Información Relacionada

Introducción

Este documento describe cómo configurar y resolver problemas de la Encripción de Capa de Red de Cisco con IPSec y el Protocolo de Administración de Claves y Asociación de Seguridad Internet (ISAKMP) y contiene información sobre la Encripción de Capa de Red y la configuración básica junto con IPSec e ISAKMP.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las versiones de software y hardware.

- Versión 11.2 y posteriores de Cisco IOS® Software

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.

Información general y configuración del cifrado de la capa de red

La función Network-Layer Encryption se introdujo en la versión 11.2 del software Cisco IOS®. Proporciona un mecanismo para la transmisión segura de datos y consta de dos componentes:

- **Autenticación del router:** Antes de pasar el tráfico cifrado, dos routers realizan una autenticación bidireccional y única mediante claves públicas estándar de firma digital (DSS) para firmar desafíos aleatorios.
- **Cifrado de capa de red:** Para el cifrado de carga útil IP, los routers utilizan intercambio de claves Diffie-Hellman para generar de forma segura una clave de sesión DES(40 o 56 bits), Triple DES - 3DES(168 bits) o el estándar de cifrado avanzado más reciente - AES(128 bits(predeterminado), o 192 bits o clave de 256 bits), introducido en 1 2.2(13)T. Las nuevas claves de sesión se generan sobre una base configurable. La política de cifrado se establece mediante mapas criptográficos que utilizan listas de acceso IP extendidas para definir qué pares de red, subred, host o protocolo se cifrarán entre routers.

Fondo de criptografía

El campo de la criptografía se ocupa de mantener las comunicaciones privadas. La protección de las comunicaciones confidenciales ha sido el énfasis de la criptografía a lo largo de gran parte de su historia. El cifrado es la transformación de los datos en una forma ilegible. Su propósito es asegurar la privacidad manteniendo la información oculta a cualquier persona para la que no está destinada, incluso si pueden ver los datos cifrados. El descifrado es el reverso del cifrado: se trata de la transformación de los datos cifrados en una forma inteligible.

El cifrado y el descifrado requieren el uso de cierta información secreta, normalmente denominada "clave". Dependiendo del mecanismo de cifrado utilizado, se podría utilizar la misma clave para el cifrado y el descifrado; mientras que para otros mecanismos, las claves utilizadas para el cifrado y el descifrado pueden ser diferentes.

Una firma digital enlaza un documento al poseedor de una clave determinada, mientras que una marca de tiempo digital enlaza un documento a su creación en un momento determinado. Estos mecanismos criptográficos se pueden utilizar para controlar el acceso a una unidad de disco

compartido, una instalación de alta seguridad o a un canal de televisión de pago por visión.

Si bien la criptografía moderna es cada vez más diversa, la criptografía se basa fundamentalmente en problemas difíciles de resolver. Un problema puede ser difícil porque su solución requiere conocer la clave, como descifrar un mensaje cifrado o firmar algún documento digital. El problema también puede ser difícil porque es intrínsecamente difícil de completar, como encontrar un mensaje que produzca un valor hash determinado.

A medida que el campo de la criptografía ha avanzado, las líneas divisorias de lo que es y lo que no es criptografía se han difuminado. La criptografía actual podría resumirse como el estudio de técnicas y aplicaciones que dependen de la existencia de problemas matemáticos difíciles de resolver. Un criptográfico intenta comprometer los mecanismos criptográficos, y la criptología es la disciplina de la criptografía y la criptoanálisis combinados.

Definiciones

Esta sección define los términos relacionados utilizados en este documento.

- **Autenticación:** Propiedad de saber que los datos recibidos son efectivamente enviados por el remitente reclamado.
- **Confidencialidad:** Propiedad de la comunicación de modo que los destinatarios previstos sepan lo que se está enviando, pero las partes no deseadas no pueden determinar qué se envía.
- **Estándar de cifrado de datos (DES):** El DES utiliza un método de clave simétrica, también conocido como método de clave secreta. Esto significa que si un bloque de datos se cifra con la clave, el bloque cifrado se debe descifrar con la misma clave, por lo que tanto el cifrado como el descifrado deben utilizar la misma clave. Aunque el método de encriptación es conocido y bien publicado, el método de ataque más conocido públicamente es a través de la fuerza bruta. Las claves se deben probar con los bloques cifrados para ver si pueden resolverlos correctamente. A medida que los procesadores se vuelven más potentes, la vida natural de DES se acerca a su fin. Por ejemplo, un esfuerzo coordinado que utiliza la potencia de procesamiento de repuesto de miles de ordenadores de Internet puede encontrar la clave de 56 bits en un mensaje codificado DES en 21 días.La Agencia de Seguridad Nacional (NSA) de los Estados Unidos valida el DES cada cinco años para cumplir los objetivos del Gobierno de los Estados Unidos. La aprobación actual vence en 1998 y la NSA ha indicado que no volverá a certificar DES. Al ir más allá de DES, hay otros algoritmos de cifrado que tampoco tienen ninguna debilidad conocida que no sean los ataques de fuerza bruta. Para más información, véase DES FIPS 46-2 del Instituto Nacional de Normas y Tecnología (NIST) .
- **Descifrado:** Aplicación inversa de un algoritmo de cifrado a los datos cifrados, restaurando así esos datos a su estado original sin cifrar.
- **DSS y algoritmo de firma digital (DSA):** La DSA fue publicada por el NIST en el Estándar de Firma Digital (DSS), que es parte del proyecto Capstone del gobierno de Estados Unidos. El NIST seleccionó a DSS, en cooperación con la NSA, como el estándar de autenticación digital del gobierno de Estados Unidos. La norma se emitió el 19 de mayo de 1994.
- **Cifrado:** La aplicación de un algoritmo específico a los datos para alterar el aspecto de los datos, haciendo incomprensible para aquellos que no están autorizados a ver la información.
- **Integridad:** Propiedad de garantizar que los datos se transmiten de origen a destino sin que se detecten alteraciones.

- **No rechazo:** La propiedad de un receptor al poder probar que el remitente de algunos datos envió efectivamente los datos, aunque el remitente podría negar haber enviado esos datos más tarde.
- **Criptografía de clave pública:** La criptografía tradicional se basa en el remitente y el receptor de un mensaje que conoce y utiliza la misma clave secreta. El remitente utiliza la clave secreta para cifrar el mensaje y el receptor utiliza la misma clave secreta para descifrar el mensaje. Este método se conoce como "clave secreta" o "criptografía simétrica". El problema principal es lograr que el remitente y el receptor se pongan de acuerdo sobre la clave secreta sin que nadie más se entere. Si se encuentran en ubicaciones físicas separadas, deben confiar en un mensajero, en un sistema telefónico o en algún otro medio de transmisión para evitar que se divulgue la clave secreta. Cualquiera que oiga o intercepte la clave en tránsito puede leer, modificar y falsificar posteriormente todos los mensajes cifrados o autenticados mediante esa clave. La generación, transmisión y almacenamiento de claves se denomina administración de claves; todos los criptosistemas deben lidiar con problemas de administración de claves. Dado que todas las claves de un criptosistema de claves secretas deben permanecer en secreto, la criptografía de claves secretas a menudo tiene dificultades para proporcionar una administración de claves segura, especialmente en sistemas abiertos con un gran número de usuarios.El concepto de criptografía de clave pública fue introducido en 1976 por Whitfield Diffie y Martin Hellman para resolver el problema de gestión de claves. En su concepto, cada persona recibe un par de llaves, una llamada clave pública y la otra llamada clave privada. La clave pública de cada persona se publica mientras que la clave privada se mantiene en secreto. Se elimina la necesidad de que el remitente y el receptor compartan información secreta y todas las comunicaciones solo incluyen claves públicas, y ninguna clave privada se transmite o comparte nunca. Ya no es necesario confiar en algunos canales de comunicación para que estén seguros frente a las interceptaciones o las traiciones. El único requisito es que las claves públicas se asocien a sus usuarios de una forma (autenticada) de confianza (por ejemplo, en un directorio de confianza). Cualquiera puede enviar un mensaje confidencial simplemente usando información pública, pero el mensaje sólo puede ser descifrado con una clave privada, que está en posesión del destinatario deseado. Además, la criptografía de clave pública se puede utilizar no sólo para la privacidad (cifrado), sino también para la autenticación (firmas digitales).
- **Firmas digitales de clave pública:** Para firmar un mensaje, una persona realiza un cálculo que involucra tanto su clave privada como el propio mensaje. La salida se denomina firma digital y se adjunta al mensaje, que se envía. Una segunda persona verifica la firma realizando un cálculo que involucra el mensaje, la firma supuestamente y la clave pública de la primera persona. Si el resultado se mantiene correctamente en una relación matemática simple, se verifica que la firma es genuina. De lo contrario, la firma podría ser fraudulenta o el mensaje podría haber sido alterado.
- **Cifrado de clave pública:** Cuando una persona desea enviar un mensaje secreto a otra, la primera persona busca la clave pública de la segunda persona en un directorio, la utiliza para cifrar el mensaje y lo envía. A continuación, la segunda persona utiliza su clave privada para descifrar el mensaje y leerlo. Nadie que escuche en puede descifrar el mensaje. Cualquiera puede enviar un mensaje cifrado a la segunda persona, pero sólo la segunda persona puede leerlo. Claramente, un requisito es que nadie pueda descifrar la clave privada de la clave pública correspondiente.
- **Análisis del tráfico:** El análisis del flujo de tráfico de red con el fin de deducir información que es útil para un adversario. Ejemplos de dicha información son la frecuencia de transmisión, las identidades de las partes que hacen la conversión, los tamaños de los paquetes, los

identificadores de flujo utilizados, etc.

Información preliminar

Esta sección trata algunos conceptos básicos de Network-Layer Encryption . Contiene los aspectos de cifrado que debe tener en cuenta. Inicialmente, estos problemas pueden no tener sentido para usted, pero es una buena idea leerlos de nuevo y estar al tanto de ellos porque tendrán más sentido después de haber trabajado con el cifrado durante varios meses.

- Es importante tener en cuenta que el cifrado ocurre solamente en la salida de una interfaz y el descifrado ocurre solamente cuando se ingresa a la interfaz. Esta distinción es importante a la hora de planificar su política. La política de cifrado y descifrado es simétrica. Esto significa que al definir uno se obtiene el otro automáticamente. Con los mapas criptográficos y sus listas de acceso ampliadas asociadas, sólo se define explícitamente la política de cifrado.La política de descifrado utiliza la información idéntica, pero al hacer coincidir los paquetes, revierte las direcciones de origen y destino y los puertos. De esta manera, los datos están protegidos en ambas direcciones de una conexión dúplex. La *sentencia match address x* en el comando **crypto map** se utiliza para describir los paquetes que salen de una interfaz. En otras palabras, describe el cifrado de los paquetes. Sin embargo, los paquetes también deben coincidir para el descifrado a medida que ingresan a la interfaz. Esto se realiza automáticamente atravesando la lista de acceso con las direcciones de origen y destino y los puertos invertidos. Esto proporciona simetría para la conexión. La lista de acceso señalada por el **mapa criptográfico** debería describir el tráfico solamente en una dirección (saliente). Los paquetes IP que no coincidan con la lista de acceso que defina se transmitirán pero no se cifrarán. Una "denegación" en la lista de acceso indica que esos hosts no deben coincidir, lo que significa que no se cifrarán. En este contexto, "deny" no significa que el paquete se descarte.
- Tenga mucho cuidado al usar la palabra "any" en las listas de acceso extendidas. El uso de "any" hace que el tráfico se descarte a menos que se dirija a la interfaz "descifrado" coincidente. Además, con IPSec en la versión 11.3(3)T del software del IOS de Cisco, "any" no está permitido.
- Se desaconseja el uso de la palabra clave "any" al especificar las direcciones de origen o de destino. La especificación de "any" puede causar problemas con los protocolos de routing, el protocolo de tiempo de red (NTP), el eco, la respuesta de eco y el tráfico de multidifusión, ya que el router receptor descarta este tráfico de forma silenciosa. Si se va a utilizar "any", debe ir precedida de sentencias "deny" para el tráfico que no se va a cifrar, como "ntp".
- Para ahorrar tiempo, asegúrese de que puede **hacer ping** al router de peer con el que intenta tener una asociación de cifrado. Además, haga que los dispositivos finales (que dependen de que su tráfico se cifre) hagan ping entre sí antes de dedicar demasiado tiempo a solucionar el problema incorrecto. En otras palabras, asegúrese de que el ruteo funcione antes de intentar hacer **crypto**. Es posible que el par remoto no tenga una ruta para la interfaz de egreso, en cuyo caso no puede tener una sesión de cifrado con ese par (es posible que pueda utilizar **ip unnumbered** en esa interfaz serial).
- Muchos enlaces punto a punto WAN utilizan direcciones IP no enrutables, y el cifrado de la versión 11.2 del software Cisco IOS se basa en el protocolo de mensajes de control de Internet (ICMP) (lo que significa que utiliza la dirección IP de la interfaz serial de salida para ICMP). Esto puede obligarle a utilizar **ip unnumbered** en la interfaz WAN. Realice siempre un comando **ping** y **traceroute** para asegurarse de que el ruteo esté en su lugar para los dos

routers de iguales (cifrado/descifrado).

- Sólo dos routers pueden compartir una clave de sesión Diffie-Hellman. Es decir, un router no puede intercambiar paquetes cifrados a dos peers usando la misma clave de sesión; cada par de routers debe tener una clave de sesión que sea el resultado de un intercambio Diffie-Hellman entre ellos.
- El motor criptográfico se encuentra en Cisco IOS, VIP2 Cisco IOS o en hardware en el adaptador de servicios de cifrado (ESA) en un VIP2. Sin un VIP2, el motor de criptografía de Cisco IOS gobierna la política de encripción en todos los puertos. En las plataformas que utilizan VIP2, hay varios motores criptográficos: uno en Cisco IOS y uno en cada VIP2. El motor de criptografía en un VIP2 rige el cifrado en los puertos que residen en la placa.
- Asegúrese de que el tráfico esté configurado para llegar a una interfaz preparada para cifrarlo. Si el tráfico puede llegar de alguna manera a una interfaz diferente a la que tiene aplicado **mapa criptográfico**, se descarta silenciosamente.
- Ayuda a tener acceso de consola (o alternativo) a ambos routers al realizar el intercambio de claves; es posible que el lado pasivo se cuelgue mientras se espera una llave.
- El **cfb-64** es más eficiente para procesar que el **cfb-8** en términos de carga de CPU.
- El router debe ejecutar el algoritmo que desea utilizar con el modo de retroalimentación cifrada (CFB) que desea utilizar; los valores predeterminados para cada imagen son el nombre de la imagen (como "56") con **cfb-64**.
- Considere cambiar el tiempo de espera de la clave. El valor predeterminado de 30 minutos es muy corto. Intente aumentarlo a un día (1440 minutos).
- El tráfico IP se descarta durante la renegociación de clave cada vez que caduca la clave.
- Seleccione sólo el tráfico que realmente desea cifrar (esto ahorra ciclos de CPU).
- Con el routing de marcado a petición (DDR), haga que el ICMP sea interesante o nunca marcará el número.
- Si desea cifrar el tráfico que no sea IP, utilice un túnel. Con los túneles, aplique los mapas criptográficos a las interfaces física y de túnel. Véase la muestra 5: Cifrado del tráfico IPX en un túnel IP para obtener más información.
- Los dos routers de par de cifrado no necesitan estar conectados directamente.
- Un router de gama baja puede darle un mensaje de "bloqueo de CPU". Esto se puede ignorar porque indica que el cifrado utiliza muchos recursos de CPU.
- No coloque routers cifrados de forma redundante para descifrar y volver a cifrar el tráfico y desperdiciar CPU. Basta con cifrar en los dos terminales. Véase Ejemplo 3: Encriptación a y a través de un router para obtener más información.
- Actualmente, no se admite el cifrado de paquetes de difusión y multidifusión. Si las actualizaciones de routing "seguras" son importantes para un diseño de red, se debe utilizar un protocolo con autenticación integrada, como el protocolo de routing de gateway interior mejorado (EIGRP), Open Shortest Path First (OSPF) o Routing Information Protocol Version 2 (RIPv2) para garantizar la integridad de la actualización.

Advertencias

Nota: Se han resuelto todas las advertencias que se mencionan a continuación.

- Un router Cisco 7200 que utiliza un ESA para el cifrado no puede descifrar un paquete bajo una clave de sesión y luego volver a cifrarlo bajo una clave de sesión diferente. Consulte Cisco bug ID CSCdj82613 (sólo clientes registrados) .
- Cuando dos routers están conectados por una línea arrendada cifrada y una línea de

respaldo ISDN, si la línea arrendada cae, el link ISDN funciona correctamente. Sin embargo, cuando la línea arrendada vuelve a activarse, el router que colocó la llamada ISDN falla. Consulte Cisco bug ID CSCdj00310 (sólo clientes registrados) .
- Para los Cisco 7500 Series Routers con varios VIP, si se aplica un **mapa criptográfico** a una sola interfaz de cualquier VIP, uno o más VIP caen. Consulte Cisco bug ID CSCdi88459 (sólo clientes registrados) .
- Para los Cisco 7500 Series Routers con un VIP2 y ESA, el comando **show crypto card** no muestra la salida a menos que el usuario esté en el puerto de la consola. Consulte Cisco bug ID CSCdj89070 (sólo clientes registrados) .

Configuración de Cifrado de Capa de Red de Cisco IOS

La muestra de trabajo de las configuraciones de Cisco IOS en este documento proviene directamente de los routers de laboratorio. La única alteración que se les hizo fue la eliminación de configuraciones de interfaz no relacionadas. Todo el material aquí proviene de recursos disponibles libremente en Internet o en la sección Información Relacionada al final de este documento.

Todas las configuraciones de ejemplo de este documento son de Cisco IOS Software Release 11.3. Hubo varios cambios en los comandos de la versión 11.2 del software del IOS de Cisco, como la adición de las siguientes palabras:

- dss en algunos de los comandos de configuración de claves.
- cisco en algunos de los comandos **show** y **crypto map** para distinguir entre el cifrado propietario de Cisco (como se encuentra en Cisco IOS Software Release 11.2 y posteriores) e IPSec que se encuentra en Cisco IOS Software Release 11.3(2)T.

Nota: Las direcciones IP utilizadas en estos ejemplos de configuración se eligieron aleatoriamente en el laboratorio de Cisco y se pretende que sean completamente genéricas.

Paso 1: Generar manualmente pares de claves DSS

Se debe generar manualmente un par de claves DSS (una clave pública y privada) en cada router que participa en la sesión de cifrado. En otras palabras, cada router debe tener sus propias claves DSS para participar. Un motor de cifrado sólo puede tener una clave DSS que la identifique de forma única. La palabra clave "dss" se agregó en la versión 11.3 del software del IOS de Cisco para distinguir DSS de las claves RSA. Puede especificar cualquier nombre para las propias claves DSS del router (aunque se recomienda utilizar el nombre de host del router). En una CPU menos potente (como la serie 2500 de Cisco), la generación de pares de claves tarda aproximadamente 5 segundos o menos.

El router genera un par de claves:

- Clave pública (que se envía posteriormente a los routers que participan en sesiones de cifrado).
- Una clave privada (que no se ve ni se intercambia con nadie más; de hecho, se almacena en una sección independiente de la NVRAM que no se puede ver).

Una vez que se ha generado el par de claves DSS del router, se asocia de forma exclusiva con el motor de criptografía en ese router. La generación del par de claves se muestra en el siguiente ejemplo de resultado del comando.

```
dial-5(config)#crypto key generate dss dial5
Generating DSS keys ....
 [OK]

dial-5#show crypto key mypubkey dss
crypto public-key dial5 05679919
 160AA490 5B9B1824 24769FCD EE5E0F46 1ABBD343 4C0C4A03 4B279D6B 0EE5F65F
 F64665D4 1036875A 8CF93691 BDF81722 064B51C9 58D72E12 3E1894B6 64B1D145
quit


dial-5#show crypto engine configuration
slot:               0
engine name:        dial5
engine type:        software
serial number:      05679919
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    43
input queue bot:    43
input queue count:  0

dial-5#
```

Dado que sólo puede generar un par de claves que identifique el router, es posible que sobrescriba la clave original y tenga que volver a enviar la clave pública con cada router de la asociación de cifrado. Esto se muestra en el siguiente ejemplo de resultado del comando:

```
StHelen(config)#crypto key generate dss barney
% Generating new DSS keys will require re-exchanging
   public keys with peers who already have the public key
   named barney!
Generate new DSS keys? [yes/no]: yes
Generating DSS keys ....
 [OK]


StHelen(config)#
Mar 16 12:13:12.851: Crypto engine 0: create key pairs.
```

Paso 2: Intercambio manual de las claves públicas de DSS con pares (fuera de banda)

La generación del par de claves DSS del router es el primer paso para establecer una asociación de sesión de cifrado. El siguiente paso es intercambiar claves públicas con cada otro router. Puede ingresar estas claves públicas manualmente ingresando primero el comando **show crypto mypubkey** para mostrar la clave pública DSS del router. A continuación, intercambia estas claves públicas (por ejemplo, por correo electrónico) y, con el comando **crypto key pubkey-chain dss**, corta y pega la clave pública del router de peer en el router.

También puede utilizar el comando **crypto key exchange dss** para que los routers intercambien claves públicas automáticamente. Si utiliza el método automatizado, asegúrese de que no haya instrucciones **crypto map** en las interfaces utilizadas para el intercambio de claves. Una **clave crypto debug** es útil aquí.

Nota: Es una buena idea **hacer ping** a su par antes de intentar intercambiar claves.

```
Loser#ping 19.19.19.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.19.20, timeout is 2 seconds:
!!!!!

Loser(config)#crypto key exchange dss passive
Enter escape character to abort if connection does not complete.
Wait for connection from peer[confirm]
Waiting ....


  StHelen(config)#crypto key exchange dss 19.19.19.19 barney
  Public key for barney:
  Serial Number 05694352
  Fingerprint   309E D1DE B6DA 5145 D034

  Wait for peer to send a key[confirm]


Public key for barney:
   Serial Number 05694352
   Fingerprint   309E D1DE B6DA 5145 D034

Add this public key to the configuration? [yes/no]:yes


         Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes.
         Mar 16 12:16:55.343: CRYPTO-KE: Sent 4 bytes.
         Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes.
         Mar 16 12:16:55.347: CRYPTO-KE: Sent 64 bytes.


Mar 16 12:16:45.099: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:45.099: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:45.103: CRYPTO-KE: Received 6 bytes.
Mar 16 12:16:45.103: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:45.107: CRYPTO-KE: Received 50 bytes.
Mar 16 12:16:45.111: CRYPTO-KE: Received 14 bytes.

Send peer a key in return[confirm]
Which one?

fred? [yes]:
Public key for fred:
   Serial Number 02802219
   Fingerprint   2963 05F9 ED55 576D CF9D


         Waiting ....
         Public key for fred:
           Serial Number 02802219
         Fingerprint   2963 05F9 ED55 576D CF9D

         Add this public key to the configuration? [yes/no]:

Loser(config)#
Mar 16 12:16:55.339: CRYPTO-KE: Sent 4 bytes.
Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:55.343: CRYPTO-KE: Sent 4 bytes.
Mar 16 12:16:55.343: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:55.347: CRYPTO-KE: Sent 64 bytes.
```

```
Loser(config)#

Mar 16 12:16:56.083: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 52 bytes.
Mar 16 12:16:56.095: CRYPTO-KE: Received 12 bytes.
Add this public key to the configuration? [yes/no]: yes
StHelen(config)#^Z
StHelen#
```

Ahora que se han intercambiado las claves DSS públicas, asegúrese de que ambos routers tengan las claves públicas del otro y que coincidan, como se muestra en el resultado del comando siguiente.

```
Loser#show crypto key mypubkey dss
crypto public-key fred 02802219
 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
quit

Loser#show crypto key pubkey-chain dss
crypto public-key barney 05694352
 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
quit

--------

StHelen#show crypto key mypubkey dss
crypto public-key barney 05694352
 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
quit

StHelen#show crypto key pubkey-chain dss
crypto public-key fred 02802219
 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
quit
```

Ejemplo 1: Configuración de Cisco IOS para el link dedicado

Después de que se hayan generado las claves DSS en cada router y de que se hayan intercambiado las claves públicas DSS, el comando **crypto map** se puede aplicar a la interfaz. La sesión de criptografía comienza generando tráfico que coincide con la lista de acceso utilizada por los mapas criptográficos.

```
Loser#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 13:01:18 UTC Mon Mar 16 1998
! NVRAM config last updated at 13:03:02 UTC Mon Mar 16 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
```

```
!
hostname Loser
!
enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0
!
ip subnet-zero
no ip domain-lookup
crypto map oldstyle 10
 set peer barney
 match address 133
!
crypto key pubkey-chain dss
 named-key barney
  serial-number 05694352
  key-string
   B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
   732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
  quit
!
interface Ethernet0
 ip address 40.40.40.41 255.255.255.0
 no ip mroute-cache
!
interface Serial0
 ip address 18.18.18.18 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 shutdown
!
interface Serial1
 ip address 19.19.19.19 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 clockrate 2400
 no cdp enable
 crypto map oldstyle
!
ip default-gateway 10.11.19.254
ip classless
ip route 0.0.0.0 0.0.0.0 19.19.19.20
access-list 133 permit ip 40.40.40.0 0.0.0.255 30.30.30.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 no exec
 transport input all
line vty 0 4
 password ww
 login
!
end

Loser#
--------------------------

StHelen#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 13:03:05 UTC Mon Mar 16 1998
! NVRAM config last updated at 13:03:07 UTC Mon Mar 16 1998
!
```

```
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname StHelen
!
boot system flash c2500-is56-l
enable password ww
!
partition flash 2 8 8
!
no ip domain-lookup
crypto map oldstyle 10
 set peer fred
 match address 144
!
crypto key pubkey-chain dss
 named-key fred
  serial-number 02802219
  key-string
   79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
   C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
  quit
 !
 !
interface Ethernet0
 ip address 30.30.30.31 255.255.255.0
!
interface Ethernet1
 no ip address
 shutdown
!
interface Serial0
 no ip address
 encapsulation x25
 no ip mroute-cache
 shutdown
!
interface Serial1
 ip address 19.19.19.20 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 load-interval 30
 compress stac
 no cdp enable
 crypto map oldstyle
!
ip default-gateway 10.11.19.254
ip classless
ip route 0.0.0.0 0.0.0.0 19.19.19.19
access-list 144 permit ip 30.30.30.0 0.0.0.255 40.40.40.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 transport input all
line vty 0 4
 password ww
 login
!
end

StHelen#
```

Ejemplo 2: Configuración de Cisco IOS para Frame Relay Multipunto

El siguiente ejemplo de resultado del comando se tomó del router HUB.

```
Loser#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 10:45:20 UTC Wed Mar 11 1998
! NVRAM config last updated at 18:28:27 UTC Tue Mar 10 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname Loser
!
enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0
!
ip subnet-zero
no ip domain-lookup
!
crypto map oldstuff 10
 set peer barney
 match address 133
crypto map oldstuff 20
 set peer wilma
 match address 144
!
crypto key pubkey-chain dss
 named-key barney
  serial-number 05694352
  key-string
   1D460DC3 BDC73312 93B7E220 1861D55C E00DA5D8 DB2B04CD FABD297C 899D40E7
   D284F07D 6EEC83B8 E3676EC2 D813F7C8 F532DC7F 0A9913E7 8A6CB7E9 BE18790D
  quit
 named-key wilma
  serial-number 01496536
  key-string
   C26CB3DD 2A56DD50 CC2116C9 2697CE93 6DBFD824 1889F791 9BF36E70 7B29279C
   E343C56F 32266443 989B4528 1CF32C2D 9E3F2447 A5DBE054 879487F6 26A55939
  quit
!
crypto cisco pregen-dh-pairs 5
!
crypto cisco key-timeout 1440
!
interface Ethernet0
 ip address 190.190.190.190 255.255.255.0
 no ip mroute-cache
!
interface Serial1
 ip address 19.19.19.19 255.255.255.0
 encapsulation frame-relay
 no ip mroute-cache
 clockrate 500000
 crypto map oldstuff
!
!
ip default-gateway 10.11.19.254
```

```
ip classless
ip route 200.200.200.0 255.255.255.0 19.19.19.20
ip route 210.210.210.0 255.255.255.0 19.19.19.21
access-list 133 permit ip 190.190.190.0 0.0.0.255 200.200.200.0 0.0.0.255
access-list 144 permit ip 190.190.190.0 0.0.0.255 210.210.210.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 no exec
 transport input all
line vty 0 4
 password ww
 login
!
end

Loser#
```

El siguiente ejemplo de resultado del comando se tomó del sitio remoto A.

```
WAN-2511a#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service password-encryption
!
hostname WAN-2511a
!
enable password ww
!
no ip domain-lookup
!
crypto map mymap 10
 set peer fred
 match address 133
!
crypto key pubkey-chain dss
 named-key fred
  serial-number 02802219
  key-string
   56841777 4F27A574 5005E0F0 CF3C33F5 C6AAD000 5518A8FF 7422C592 021B295D
   D95AAB73 01235FD8 40D70284 3A63A38E 216582E8 EC1F8B0D 0256EFF5 0EE89436
  quit
!
interface Ethernet0
 ip address 210.210.210.210 255.255.255.0
 shutdown
!
interface Serial0
 ip address 19.19.19.21 255.255.255.0
 encapsulation frame-relay
 no fair-queue
 crypto map mymap
!
ip default-gateway 10.11.19.254
ip classless
ip route 190.190.190.0 255.255.255.0 19.19.19.19
access-list 133 permit ip 210.210.210.0 0.0.0.255 190.190.190.0 0.0.0.255
!
line con 0
```

```
 exec-timeout 0 0
line 1
 no exec
 transport input all
line 2 16
 no exec
line aux 0
line vty 0 4
 password ww
 login
!
end

WAN-2511a#
```

El siguiente ejemplo de resultado del comando se tomó del Sitio remoto B.

```
StHelen#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 19:00:34 UTC Tue Mar 10 1998
! NVRAM config last updated at 18:48:39 UTC Tue Mar 10 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname StHelen
!
boot system flash c2500-is56-l
enable password ww
!
partition flash 2 8 8
!
no ip domain-lookup
!
crypto map wabba 10
 set peer fred
 match address 144
!
crypto key pubkey-chain dss
 named-key fred
  serial-number 02802219
  key-string
   56841777 4F27A574 5005E0F0 CF3C33F5 C6AAD000 5518A8FF 7422C592 021B295D
   D95AAB73 01235FD8 40D70284 3A63A38E 216582E8 EC1F8B0D 0256EFF5 0EE89436
  quit
!
interface Ethernet0
 ip address 200.200.200.200 255.255.255.0
!
interface Serial1
 ip address 19.19.19.20 255.255.255.0
 encapsulation frame-relay
 no ip mroute-cache
 crypto map wabba
!
ip default-gateway 10.11.19.254
ip classless
ip route 190.190.190.0 255.255.255.0 19.19.19.19
access-list 144 permit ip 200.200.200.0 0.0.0.255 190.190.190.0 0.0.0.255
```

```
!
line con 0
 exec-timeout 0 0
line aux 0
 transport input all
line vty 0 4
 password ww
 login
!
end

StHelen#
```

El siguiente ejemplo de resultado del comando se tomó del switch Frame Relay.

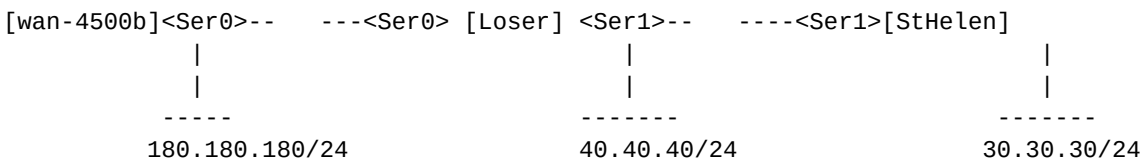
```
Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname wan-4700a
!
enable password ww
!
no ip domain-lookup
frame-relay switching
!
interface Serial0
 no ip address
 encapsulation frame-relay
 clockrate 500000
 frame-relay intf-type dce
 frame-relay route 200 interface Serial1 100
!
interface Serial1
 no ip address
 encapsulation frame-relay
 frame-relay intf-type dce
 frame-relay route 100 interface Serial0 200
 frame-relay route 300 interface Serial2 200
!
interface Serial2
 no ip address
 encapsulation frame-relay
 clockrate 500000
 frame-relay intf-type dce
 frame-relay route 200 interface Serial1 300
!
```

Ejemplo 3: Cifrado de y hasta un router

Los routers de par no tienen que estar a un salto de distancia. Puede crear una sesión de peering con un router remoto. En el siguiente ejemplo, el objetivo es cifrar todo el tráfico de red entre 180.180.180.0/24 y 40.40.40.0/24 y entre 180.180.180.0/24 y 30.30.30.0/24. No hay problema con el cifrado del tráfico entre 40.40.40.0/24 y 30.30.30.0/24.

El router wan-4500b tiene una asociación de sesión de cifrado con Loser y también con StHelen. Al cifrar el tráfico del segmento Ethernet de wan-4500b al segmento Ethernet de StHelen, se evita el paso de descifrado innecesario en Loser. El perdedor simplemente pasa el tráfico cifrado a la

interfaz serial de StHelen, donde se descifra. Esto reduce el retraso del tráfico para los paquetes IP y los ciclos de CPU en el router Loser. Lo que es más importante, aumenta en gran medida la seguridad del sistema, ya que un observador en Loser no puede leer el tráfico. Si el Perdedor descifrara el tráfico, habría la posibilidad de que los datos descifrados se desviaran.




```
wan-4500b#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service password-encryption
!
hostname wan-4500b
!
enable password 7 111E0E
!
username cse password 0 ww
no ip domain-lookup
!
crypto map toworld 10
 set peer loser
 match address 133
crypto map toworld 20
 set peer sthelen
 match address 144
!
crypto key pubkey-chain dss
 named-key loser
  serial-number 02802219
  key-string
   F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4
   6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24
  quit
 named-key sthelen
  serial-number 05694352
  key-string
   5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10
   A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618
  quit
 !
interface Ethernet0
 ip address 180.180.180.180 255.255.255.0
!
interface Serial0
 ip address 18.18.18.19 255.255.255.0
 encapsulation ppp
 crypto map toworld
!
router rip
 network 18.0.0.0
 network 180.180.0.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 30.30.30.31
```

```
ip route 171.68.118.0 255.255.255.0 10.11.19.254
access-list 133 permit ip 180.180.180.0 0.0.0.255 40.40.40.0 0.0.0.255
access-list 144 permit ip 180.180.180.0 0.0.0.255 30.30.30.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 password 7 044C1C
line vty 0 4
 login local
!
end

wan-4500b#

--------------------

Loser#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 11:01:54 UTC Wed Mar 18 1998
! NVRAM config last updated at 11:09:59 UTC Wed Mar 18 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname Loser
!
enable secret 5 $1$AeuFSMx7O/DhpqjLKc2VQVbeC0
!
ip subnet-zero
no ip domain-lookup
ip host StHelen.cisco.com 19.19.19.20
ip domain-name cisco.com
!
crypto map towan 10
 set peer wan
 match address 133
!
crypto key pubkey-chain dss
 named-key wan
  serial-number 07365004
  key-string
   A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
   2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
  quit
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
 no ip mroute-cache
!
interface Serial0
 ip address 18.18.18.18 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 clockrate 64000
 crypto map towan
!
interface Serial1
 ip address 19.19.19.19 255.255.255.0
 encapsulation ppp
```

```
 no ip mroute-cache
 priority-group 1
 clockrate 64000
!
!
router rip
 network 19.0.0.0
 network 18.0.0.0
 network 40.0.0.0
!
ip default-gateway 10.11.19.254
ip classless
access-list 133 permit ip 40.40.40.0 0.0.0.255 180.180.180.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 no exec
 transport input all
line vty 0 4
 password ww
 login
!
end

Loser#

-------------------------

StHelen#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 11:13:18 UTC Wed Mar 18 1998
! NVRAM config last updated at 11:21:30 UTC Wed Mar 18 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname StHelen
!
boot system flash c2500-is56-l
enable password ww
!
partition flash 2 8 8
!
no ip domain-lookup
!
crypto map towan 10
 set peer wan
 match address 144
!
crypto key pubkey-chain dss
 named-key wan
  serial-number 07365004
  key-string
   A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
   2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
  quit
!
interface Ethernet0
 no ip address
```

```
!
interface Ethernet1
 ip address 30.30.30.30 255.255.255.0
!
interface Serial1
 ip address 19.19.19.20 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 load-interval 30
 crypto map towan
!
router rip
 network 30.0.0.0
 network 19.0.0.0
!
ip default-gateway 10.11.19.254
ip classless
access-list 144 permit ip 30.30.30.0 0.0.0.255 180.180.180.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 transport input all
line vty 0 4
 password ww
 login
!
end

StHelen#

--------------------------

wan-4500b#show crypto cisco algorithms
  des cfb-64
  40-bit-des cfb-64

wan-4500b#show crypto cisco key-timeout
Session keys will be re-negotiated every 30 minutes

wan-4500b#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 0

wan-4500b#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 1    Serial0         18.18.18.19 set    DES_56_CFB64    1683     1682
 5    Serial0         18.18.18.19 set    DES_56_CFB64    1693     1693

wan-4500b#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

Serial0              18.18.18.19   52
wan-4500b#show crypto engine configuration
slot:               0
engine name:        wan
engine type:        software
serial number:      07365004
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    303
input queue bot:    303
input queue count:  0
```

```
wan-4500b#show crypto key mypubkey dss
crypto public-key wan 07365004
 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
quit

wan-4500b#show crypto key pubkey-chain dss
crypto public-key loser 02802219
 F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4
 6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24
quit
crypto public-key sthelen 05694352
 5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10
 A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618
quit

wan-4500b#show crypto map interface serial 1
No crypto maps found.

wan-4500b#show crypto map
Crypto Map "toworld" 10 cisco
        Connection Id = 1        (1 established,    0 failed)
        Peer = loser
        PE = 180.180.180.0
        UPE = 40.40.40.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 180.180.180.0/0.0.0.255
                dest:   addr = 40.40.40.0/0.0.0.255

Crypto Map "toworld" 20 cisco
        Connection Id = 5        (1 established,    0 failed)
        Peer = sthelen
        PE = 180.180.180.0
        UPE = 30.30.30.0
        Extended IP access list 144
            access-list 144 permit ip
                source: addr = 180.180.180.0/0.0.0.255
                dest:   addr = 30.30.30.0/0.0.0.255

wan-4500b#

--------------------------

Loser#show crypto cisco algorithms
  des cfb-64
  des cfb-8
  40-bit-des cfb-64
  40-bit-des cfb-8

Loser#show crypto cisco key-timeout
Session keys will be re-negotiated every 30 minutes

Loser#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 10

Loser#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 61   Serial0         18.18.18.18 set    DES_56_CFB64    1683     1682

Loser#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count
```

```
Serial0              18.18.18.18   1
Serial1              19.19.19.19   90
Loser#show crypto engine configuration
slot:               0
engine name:        loser
engine type:        software
serial number:      02802219
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    235
input queue bot:    235
input queue count:  0

Loser#show crypto key mypubkey dss
crypto public-key loser 02802219
 F0BE2128 752D1A24 F394B355 3216BA9B 7C4E8677 29C176F9 A047B7D9 7D03BDA4
 6B7AFDC2 2DAEF3AB 393EE7C7 802C1A95 B40031D1 908004F9 8A33A352 FF19BC24
quit

Loser#show crypto key pubkey-chain dss
crypto public-key wan 07365004
 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
quit

Loser#show crypto map interface serial 1
No crypto maps found.

Loser#show crypto map
Crypto Map "towan" 10 cisco
        Connection Id = 61       (0 established,    0 failed)
        Peer = wan
        PE = 40.40.40.0
        UPE = 180.180.180.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 40.40.40.0/0.0.0.255
                dest:   addr = 180.180.180.0/0.0.0.255

Loser#

----------------------------------------

StHelen#show crypto cisco algorithms
  des cfb-64

StHelen#show crypto cisco key-timeout
Session keys will be re-negotiated every 30 minutes

StHelen#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 10

StHelen#show crypto engine connections active

ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 58   Serial1         19.19.19.20 set    DES_56_CFB64    1694     1693

StHelen#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

Ethernet0            0.0.0.0       1
Serial1              19.19.19.20   80
```

```
StHelen#show crypto engine configuration
slot:               0
engine name:        sthelen
engine type:        software
serial number:      05694352
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    220
input queue bot:    220
input queue count:  0

StHelen#show crypto key mypubkey dss
crypto public-key sthelen 05694352
 5C401002 404DC5A9 EAED2360 D7007E51 4A4BB8F8 6F9B1554 51D8ACBB D3964C10
 A23848CA 46003A94 2FC8C7D6 0B57AE07 9EB5EF3A BD71482B 052CF06B 90C3C618
quit

StHelen#show crypto key pubkey-chain dss
crypto public-key wan 07365004
 A547B701 4312035D 2FC7D0F4 56BC304A 59FA76C3 B9762E4A F86DED86 3830E66F
 2ED5C476 CFF234D3 3842BC98 3CA4A5FB 9089556C 7464D2B4 AF7E6AEB 86269A5B
quit

StHelen#show crypto map interface serial 1
Crypto Map "towan" 10 cisco
        Connection Id = 58       (1 established,    0 failed)
        Peer = wan
        PE = 30.30.30.0
        UPE = 180.180.180.0
        Extended IP access list 144
            access-list 144 permit ip
                source: addr = 30.30.30.0/0.0.0.255
                dest:   addr = 180.180.180.0/0.0.0.255

StHelen#show crypto map
Crypto Map "towan" 10 cisco
        Connection Id = 58       (1 established,    0 failed)
        Peer = wan
        PE = 30.30.30.0
        UPE = 180.180.180.0
        Extended IP access list 144
            access-list 144 permit ip
                source: addr = 30.30.30.0/0.0.0.255
                dest:   addr = 180.180.180.0/0.0.0.255

StHelen#
```

Ejemplo 4: Crypto con DDR

Debido a que Cisco IOS se basa en el ICMP para establecer sesiones de cifrado, el tráfico ICMP debe clasificarse como "interesante" en la lista de marcador cuando se realiza el cifrado a través de un link DDR.

Nota: Compression funciona en Cisco IOS Software Release 11.3, pero no es muy útil para datos cifrados. Puesto que los datos cifrados tienen un aspecto bastante aleatorio, la compresión sólo ralentiza las cosas. Pero puede dejar la función activada para el tráfico no cifrado.

En algunas situaciones, querrá realizar una copia de seguridad de marcado al mismo router. Por ejemplo, se utiliza como combustible cuando los usuarios desean protegerse contra el fallo de un

link concreto en sus redes WAN. Si dos interfaces van al mismo par, se puede utilizar el mismo mapa criptográfico en ambas interfaces. Para que esta función funcione correctamente, se debe utilizar la interfaz de respaldo. Si un diseño de respaldo tiene un marcado de router en un cuadro diferente, se deben crear mapas criptográficos diferentes y los pares deben configurarse en consecuencia. Una vez más, se debe utilizar el comando **backup interface**.

```
dial-5#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname dial-5
!
boot system c1600-sy56-l 171.68.118.83
enable secret 5 $1$oNe1wDbhBdcN6x9Y5gfuMjqh10
!
username dial-6 password 0 cisco
isdn switch-type basic-ni1
!
crypto map dial6 10
 set peer dial6
 match address 133
!
crypto key pubkey-chain dss
 named-key dial6
  serial-number 05679987
  key-string
   753F71AB E5305AD4 3FCDFB6D 47AA2BB5 656BFCAA 53DBE37F 07465189 06E91A82
   2BC91236 13DC4AA8 7EC5B48C D276E5FE 0D093014 6D3061C5 03158820 B609CA7C
  quit
!
interface Ethernet0
 ip address 20.20.20.20 255.255.255.0
!
interface BRI0
 ip address 10.10.10.11 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 load-interval 30
 dialer idle-timeout 9000
 dialer map ip 10.10.10.10 name dial-6 4724118
 dialer hold-queue 40
 dialer-group 1
 isdn spid1 919472417100 4724171
 isdn spid2 919472417201 4724172
 compress stac
 ppp authentication chap
 ppp multilink
 crypto map dial6
!
ip classless
ip route 40.40.40.0 255.255.255.0 10.10.10.10
access-list 133 permit ip 20.20.20.0 0.0.0.255 40.40.40.0 0.0.0.255
dialer-list 1 protocol ip permit
!
line con 0
```

```
 exec-timeout 0 0
line vty 0 4
 password ww
 login
!
end

dial-5#

-----------------------

dial-6#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname dial-6
!
boot system c1600-sy56-l 171.68.118.83
enable secret 5 $1$VdPYuA/BIVeEm9UAFEm.PPJFc.
!
username dial-5 password 0 cisco
no ip domain-lookup
isdn switch-type basic-ni1
!
 crypto map dial5 10
 set peer dial5
 match address 144
!
crypto key pubkey-chain dss
 named-key dial5
  serial-number 05679919
  key-string
   160AA490 5B9B1824 24769FCD EE5E0F46 1ABBD343 4C0C4A03 4B279D6B 0EE5F65F
   F64665D4 1036875A 8CF93691 BDF81722 064B51C9 58D72E12 3E1894B6 64B1D145
  quit
 !
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
!
interface BRI0
 ip address 10.10.10.10 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 dialer idle-timeout 9000
 dialer map ip 10.10.10.11 name dial-5 4724171
 dialer hold-queue 40
 dialer load-threshold 5 outbound
 dialer-group 1
 isdn spid1 919472411800 4724118
 isdn spid2 919472411901 4724119
 compress stac
 ppp authentication chap
 ppp multilink
 crypto map dial5
!
ip classless
ip route 20.20.20.0 255.255.255.0 10.10.10.11
```

```
access-list 144 permit ip 40.40.40.0 0.0.0.255 20.20.20.0 0.0.0.255
dialer-list 1 protocol ip permit
!
line con 0
 exec-timeout 0 0
line vty 0 4
 password ww
 login
!
end

dial-6#
```

Ejemplo 5: Cifrado del tráfico IPX en un túnel IP

En este ejemplo, el tráfico IPX en un túnel IP está cifrado.

Nota: Sólo se cifra el tráfico de este túnel (IPX). El resto del tráfico IP se deja solo.

```
WAN-2511a#write terminal
Building configuration...

Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname WAN-2511a
!
enable password ww
!
no ip domain-lookup
ipx routing 0000.0c34.aa6a
!
crypto public-key wan2516 01698232
 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
 B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962
 quit
!
crypto map wan2516 10
 set peer wan2516
 match address 133
!
!
interface Loopback1
 ip address 50.50.50.50 255.255.255.0
!
interface Tunnel1
 no ip address
 ipx network 100
 tunnel source 50.50.50.50
 tunnel destination 60.60.60.60
 crypto map wan2516
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
 ipx network 600
!
interface Serial0
 ip address 20.20.20.21 255.255.255.0
```

```
 encapsulation ppp
 no ip mroute-cache
 crypto map wan2516
!
interface Serial1
 no ip address
 shutdown
!
ip default-gateway 10.11.19.254
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.20
access-list 133 permit ip host 50.50.50.50 host 60.60.60.60
!
line con 0
 exec-timeout 0 0
 password ww
 login
line 1 16
line aux 0
 password ww
 login
line vty 0 4
 password ww
 login
!
end

WAN-2511a#

------------------------

WAN-2516a#write terminal
Building configuration...

Current configuration:
!
version 11.2
no service pad
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname WAN-2516a
!
enable password ww
!
no ip domain-lookup
ipx routing 0000.0c3b.cc1e
!
crypto public-key wan2511 01496536
 C8EA7C21 DF3E48F5 C6C069DB 3A5E1B08 8B830AD4 4F1DABCE D62F5F46 ED08C81D
 5646DC78 DDC77EFC 823F302A F112AF97 668E39A1 E2FCDC05 545E0529 9B3C9553
 quit
!
crypto map wan2511 10
 set peer wan2511
 match address 144
!
!
hub ether 0 1
 link-test
 auto-polarity
!
! <other hub interfaces snipped>
```

```
!
hub ether 0 14
 link-test
 auto-polarity
!
interface Loopback1
 ip address 60.60.60.60 255.255.255.0
!
interface Tunnel1
 no ip address
 ipx network 100
 tunnel source 60.60.60.60
 tunnel destination 50.50.50.50
 crypto map wan2511
!
interface Ethernet0
 ip address 30.30.30.30 255.255.255.0
 ipx network 400
!
interface Serial0
 ip address 20.20.20.20 255.255.255.0
 encapsulation ppp
 clockrate 2000000
 crypto map wan2511
!
interface Serial1
 no ip address
 shutdown
!
interface BRI0
 no ip address
 shutdown
!
ip default-gateway 20.20.20.21
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.21
access-list 144 permit ip host 60.60.60.60 host 50.50.50.50
access-list 188 permit gre any any
!
line con 0
 exec-timeout 0 0
 password ww
 login
line aux 0
 password ww
 login
 modem InOut
 transport input all
 flowcontrol hardware
line vty 0 4
 password ww
 login
!
end

WAN-2516a#
-----------------------

WAN-2511a#show ipx route
Codes: C - Connected primary network,    c - Connected secondary network
       S - Static, F - Floating static, L - Local (internal), W - IPXWAN
       R - RIP, E - EIGRP, N - NLSP, X - External, A - Aggregate
       s - seconds, u - uses
```

```
3 Total IPX routes. Up to 1 parallel paths and 16 hops allowed.

No default route known.

C        100 (TUNNEL),        Tu1
C        600 (NOVELL-ETHER),  Et0
R        400 [151/01] via      100.0000.0c3b.cc1e,   24s, Tu1


WAN-2511a#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 1    Serial0         20.20.20.21 set    DES_56_CFB64    207      207


WAN-2511a#ping 400.0000.0c3b.cc1e
Translating "400.0000.0c3b.cc1e"

Type escape sequence to abort.
Sending 5, 100-byte IPX cisco Echoes to 400.0000.0c3b.cc1e, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/35/48 ms


WAN-2511a#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 1    Serial0         20.20.20.21 set    DES_56_CFB64    212      212


WAN-2511a#ping 30.30.30.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.30.30.30, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms


WAN-2511a#show crypto engine connections active

ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 1    Serial0         20.20.20.21 set    DES_56_CFB64    212      212

WAN-2511a#
```

Ejemplo 6: Cifrado de túneles L2F

En este ejemplo, sólo se intenta cifrar el tráfico L2F para los usuarios que marcan en . Aquí, "user@cisco.com" llama al servidor de acceso a la red (NAS) local denominado "DEMO2" en su ciudad y se tuneliza al CD del gateway residencial. Todo el tráfico DEMO2 (junto con el de otros llamadores L2F) está cifrado. Debido a que L2F utiliza el puerto UDP 1701, así es como se construye la lista de acceso, determinando qué tráfico se cifra.

Nota: Si la asociación de cifrado no está configurada, lo que significa que la persona que llama es la primera persona en llamar y crear el túnel L2F, la persona que llama puede ser descartada debido al retraso en la configuración de la asociación de cifrado. Esto puede no ocurrir en routers con suficiente potencia de CPU. Además, es posible que desee aumentar el **tiempo de espera de la clave** para que la configuración y desactivación del cifrado sólo se produzca durante las horas de menor actividad.

El siguiente ejemplo de resultado del comando se tomó del NAS remoto.

```
DEMO2#write terminal
Building configuration...

Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname DEMO2
!
enable password ww
!
username NAS1 password 0 SECRET
username HomeGateway password 0 SECRET
no ip domain-lookup
vpdn enable
vpdn outgoing cisco.com NAS1 ip 20.20.20.20
!
crypto public-key wan2516 01698232
 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
 B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962
 quit
!
crypto map vpdn 10
 set peer wan2516
 match address 133
!
crypto key-timeout 1440
!
interface Ethernet0
 ip address 40.40.40.40 255.255.255.0
!
interface Serial0
 ip address 20.20.20.21 255.255.255.0
 encapsulation ppp
 no ip mroute-cache
 crypto map vpdn
!
interface Serial1
 no ip address
 shutdown
!
interface Group-Async1
 no ip address
 encapsulation ppp
 async mode dedicated
 no peer default ip address
 no cdp enable
 ppp authentication chap pap
 group-range 1 16
!
ip default-gateway 10.11.19.254
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.20
access-list 133 permit udp host 20.20.20.21 eq 1701
 host 20.20.20.20 eq 1701
!
!
line con 0
 exec-timeout 0 0
```

```
 password ww
 login
line 1 16
 modem InOut
 transport input all
 speed 115200
 flowcontrol hardware
line aux 0
 login local
 modem InOut
 transport input all
 flowcontrol hardware
line vty 0 4
 password ww
 login
!
end

DEMO2#
```

El siguiente ejemplo de resultado del comando se tomó del gateway de inicio.

```
CD#write terminal
Building configuration...

Current configuration:
!
version 11.2
no service pad
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname CD
!
enable password ww
!
username NAS1 password 0 SECRET
username HomeGateway password 0 SECRET
username user@cisco.com password 0 cisco
no ip domain-lookup
vpdn enable
vpdn incoming NAS1 HomeGateway virtual-template 1
!
crypto public-key wan2511 01496536
 C8EA7C21 DF3E48F5 C6C069DB 3A5E1B08 8B830AD4 4F1DABCE D62F5F46 ED08C81D
 5646DC78 DDC77EFC 823F302A F112AF97 668E39A1 E2FCDC05 545E0529 9B3C9553
 quit
!
crypto key-timeout 1440
!
crypto map vpdn 10
 set peer wan2511
 match address 144
!
!
hub ether 0 1
 link-test
 auto-polarity
!
interface Loopback0
 ip address 70.70.70.1 255.255.255.0
!
```

```
interface Ethernet0
 ip address 30.30.30.30 255.255.255.0
!
interface Virtual-Template1
 ip unnumbered Loopback0
 no ip mroute-cache
 peer default ip address pool default
 ppp authentication chap
!
interface Serial0
 ip address 20.20.20.20 255.255.255.0
 encapsulation ppp
 clockrate 2000000
 crypto map vpdn
!
interface Serial1
 no ip address
 shutdown
!
interface BRI0
 no ip address
 shutdown
!
ip local pool default 70.70.70.2 70.70.70.77
ip default-gateway 20.20.20.21
ip classless
ip route 0.0.0.0 0.0.0.0 20.20.20.21
access-list 144 permit udp host 20.20.20.20 eq 1701 host 20.20.20.21 eq 1701
!
line con 0
 exec-timeout 0 0
 password ww
 login
line aux 0
 password ww
 login
 modem InOut
 transport input all
 flowcontrol hardware
line vty 0 4
 password ww
 login
!
end
```

Resolución de problemas

Por lo general, es mejor comenzar cada sesión de troubleshooting reuniendo información usando los siguientes comandos **show**. Un asterisco (*) indica un comando especialmente útil. Consulte también Solución de problemas de seguridad IP - Introducción y uso de los comandos debug para obtener información adicional.

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos comandos “show” y ver un análisis del resultado de estos comandos.

Nota: Antes de ejecutar **comandos debug**, consulte Información Importante sobre Comandos Debug.

Comandos	
show crypto cisco algoritmos	show crypto cisco key-

	timeout
show crypto cisco pregen-dh-pairs	* show crypto engine connections active
show crypto engine connections drop-packet	show crypto engine configuration
show crypto key mypubkey dss	* show crypto key pubkey-chain dss
show crypto map interface serial 1	* show crypto map
debug crypto engine	* debug crypto sess
debug cry key	clear crypto connection
crypto zeroize	no crypto public-key

- **show crypto cisco algoritmos**- Debe habilitar todos los algoritmos de Estándar de cifrado de datos (DES) que se utilizan para comunicarse con cualquier otro router de cifrado de peer. Si no habilita un algoritmo DES, no podrá utilizar ese algoritmo, incluso si intenta asignar el algoritmo a un **mapa criptográfico** más adelante.Si el router intenta configurar una sesión de comunicación cifrada con un router peer y los dos routers no tienen el mismo algoritmo DES habilitado en ambos extremos, la sesión cifrada falla. Si se habilita al menos un algoritmo DES común en ambos extremos, la sesión cifrada puede continuar.**Nota:** La palabra adicional cisco aparece en la versión 11.3 del software del IOS de Cisco y es necesaria para distinguir entre el cifrado de propiedad de IPSec y de Cisco que se encuentra en la versión 11.2 del software del IOS de Cisco.

```
Loser#show crypto cisco algorithms
  des cfb-64
  des cfb-8
  40-bit-des cfb-64
  40-bit-des cfb-8
```

- **show crypto cisco key-timeout** - Después de establecer una sesión de comunicación cifrada, es válida por un período de tiempo específico. Después de este tiempo, la sesión se agota. Se debe negociar una nueva sesión y generar una nueva clave DES (sesión) para que la comunicación cifrada continúe. Utilice este comando para cambiar el tiempo que dura una sesión de comunicación cifrada antes de que caduque (tiempo de espera).

```
Loser#show crypto cisco key-timeout
Session keys will be re-negotiated every 30 minutes
```

Utilice estos comandos para determinar el tiempo que transcurre antes de que se renegocien las claves DES.

```
StHelen#show crypto conn
Connection Table
PE              UPE         Conn_id New_id Algorithm    Time
0.0.0.1         0.0.0.1        4    0      DES_56_CFB64 Mar 01 1993 03:16:09
                flags:TIME_KEYS


StHelen#show crypto key
Session keys will be re-negotiated every 30 minutes

StHelen#show clock
*03:21:23.031 UTC Mon Mar 1 1993
```

- **show crypto cisco pregen-dh-pares** - Cada sesión cifrada utiliza un par único de números DH. Cada vez que se establece una nueva sesión, se deben generar nuevos pares de números DH. Cuando finaliza la sesión, estos números se descartan. La generación de nuevos pares de números DH es una actividad intensiva en la CPU, que puede hacer que la configuración

de la sesión sea lenta, especialmente para los routers de menor capacidad.Para acelerar la configuración de la sesión, puede elegir que se generen previamente una cantidad específica de pares de números DH y se mantengan en reserva. A continuación, cuando se configura una sesión de comunicación cifrada, se proporciona un par de números DH de esa reserva. Después de utilizar un par de números DH, la reserva se repone automáticamente con un nuevo par de números DH, de modo que siempre hay un par de números DH listo para usar.Por lo general, no es necesario tener más de uno o dos pares de números DH pregenerados, a menos que su router esté configurando varias sesiones cifradas con tanta frecuencia que una reserva pregenerada de uno o dos pares de números DH se agote demasiado rápido.

```
Loser#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 10
```

- **show crypto cisco connections active**A continuación se muestra un ejemplo de resultado del comando.

```
Loser#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 16   Serial1         19.19.19.19 set    DES_56_CFB64    376      884
```

- **show crypto cisco engine connections drop-packet**A continuación se muestra un ejemplo de resultado del comando.

```
Loser#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

Serial1              19.19.19.19   39
```

- **show crypto engine configuration** (**show crypto engine brief** en Cisco IOS Software Release 11.2.)A continuación se muestra un ejemplo de resultado del comando.

```
Loser#show crypto engine configuration
slot:               0
engine name:        fred
engine type:        software
serial number:      02802219
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    465
input queue bot:    465
input queue count:  0
```

- **show crypto key mypubkey dss**A continuación se muestra un ejemplo de resultado del comando.

```
Loser#show crypto key mypubkey dss
crypto public-key fred 02802219
 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
quit
```

- **show crypto key pubkey-chain dss**A continuación se muestra un ejemplo de resultado del comando.

```
Loser#show crypto key pubkey-chain dss
crypto public-key barney 05694352
 B407A360 204CBFA3 F9A0C0B0 15D6185D 91FD7D3A 3232EBA2 F2D31D21 53AE24ED
 732EA43D 484DEB22 6E91515C 234B4019 38E51D64 04CB9F59 EE357477 91810341
quit
```

- **show crypto map interface serial 1**A continuación se muestra un ejemplo de resultado del comando.

```
Loser#show crypto map interface serial 1
Crypto Map "oldstyle" 10 cisco
        Connection Id = 16       (8 established,    0 failed)
```

```
        Peer = barney
        PE = 40.40.40.0
        UPE = 30.30.30.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 40.40.40.0/0.0.0.255
                dest:   addr = 30.30.30.0/0.0.0.255
```

Observe la disparidad de tiempo cuando utiliza el comando **ping**.

```
wan-5200b#ping 30.30.30.30

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.30.30.30, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/54/56 ms
wan-5200b#
-----------
wan-5200b#ping 30.30.30.31

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 30.30.30.31, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/53/56 ms
-----------------

wan-5200b#ping 19.19.19.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 19.19.19.20, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/21/24 ms
------------
```

- **show crypto map interface serial 1**A continuación se muestra un ejemplo de resultado del comando.

```
Loser#show crypto map
Crypto Map "oldstyle" 10 cisco
        Connection Id = 16       (8 established,    0 failed)
        Peer = barney
        PE = 40.40.40.0
        UPE = 30.30.30.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 40.40.40.0/0.0.0.255
                dest:   addr = 30.30.30.0/0.0.0.255
```

- **debug crypto engine**A continuación se muestra un ejemplo de resultado del comando.

```
Loser#debug crypto engine
Mar 17 11:49:07.902: Crypto engine 0: generate alg param

Mar 17 11:49:07.906: CRYPTO_ENGINE: Dh phase 1 status: 0
Mar 17 11:49:07.910: Crypto engine 0: sign message using crypto engine
Mar 17 11:49:09.894: CRYPTO_ENGINE: packets dropped: State = 0
Mar 17 11:49:11.758: Crypto engine 0: generate alg param

Mar 17 11:49:12.246: CRYPTO_ENGINE: packets dropped: State = 0
Mar 17 11:49:13.342: CRYPTO ENGINE 0: get syndrome for conn id 25
Mar 17 11:49:13.346: Crypto engine 0: verify signature
Mar 17 11:49:14.054: CRYPTO_ENGINE: packets dropped: State = 0
Mar 17 11:49:14.402: Crypto engine 0: sign message using crypto engine
Mar 17 11:49:14.934: Crypto engine 0: create session for conn id 25
Mar 17 11:49:14.942: CRYPTO ENGINE 0: clear dh number for conn id 25
Mar 17 11:49:24.946: Crypto engine 0: generate alg param
```

- **debug crypto sessmgmt**A continuación se muestra un ejemplo de resultado del comando.

```
StHelen#debug crypto sessmgmt
```

```
Mar 17 11:49:08.918: IP: s=40.40.40.40 (Serial1), d=30.30.30.30, len 328,
              Found an ICMP connection message.

Mar 17 11:49:08.922: CRYPTO: Dequeued a message: CIM
Mar 17 11:49:08.926: CRYPTO-SDU: Key Timeout, Re-exchange Crypto Keys
Mar 17 11:49:09.978: CRYPTO: Verify done. Status=OK
Mar 17 11:49:09.994: CRYPTO: DH gen phase 1 status for conn_id 22 slot 0:OK
Mar 17 11:49:11.594: CRYPTO: DH gen phase 2 status for conn_id 22 slot 0:OK
Mar 17 11:49:11.598: CRYPTO: Syndrome gen status for conn_id 22 slot 0:OK
Mar 17 11:49:12.134: CRYPTO: Sign done. Status=OK
Mar 17 11:49:12.142: CRYPTO: ICMP message sent: s=19.19.19.20, d=19.19.19.19
Mar 17 11:49:12.146: CRYPTO-SDU: act_on_nnc_req: NNC Echo Reply sent
Mar 17 11:49:12.154: CRYPTO: Create encryption key for conn_id 22 slot 0:OK
Mar 17 11:49:15.366: CRYPTO: Dequeued a message: CCM
Mar 17 11:49:15.370: CRYPTO: Syndrome gen status for conn_id 22 slot 0:OK
Mar 17 11:49:16.430: CRYPTO: Verify done. Status=OK
Mar 17 11:49:16.434: CRYPTO: Replacing -23 in crypto maps with 22 (slot 0)
Mar 17 11:49:26.438: CRYPTO: Need to pregenerate 1 pairs for slot 0.
Mar 17 11:49:26.438: CRYPTO: Pregenerating DH for conn_id 32 slot 0
Mar 17 11:49:28.050: CRYPTO: DH phase 1 status for conn_id 32 slot 0:OK
                           ~~ <---------- This is good ----------> ~~
```

Si el par incorrecto establecido en el mapa criptográfico, recibe este mensaje de error.

```
Mar  2 12:19:12.639: CRYPTO-SDU:Far end authentication error:
         Connection message verify failed
```

Si los algoritmos criptográficos no coinciden, recibirá este mensaje de error.

```
Mar  2 12:26:51.091: CRYPTO-SDU: Connection
failed due to incompatible policy
```

Si falta la clave DSS o no es válida, recibirá este mensaje de error.

```
Mar 16 13:33:15.703: CRYPTO-SDU:Far end authentication error:
          Connection message verify failed
```

- **debug crypto key**A continuación se muestra un ejemplo de resultado del comando.

```
StHelen#debug crypto key
Mar 16 12:16:45.795: CRYPTO-KE: Sent 4 bytes.
Mar 16 12:16:45.795: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:45.799: CRYPTO-KE: Sent 6 bytes.
Mar 16 12:16:45.799: CRYPTO-KE: Sent 2 bytes.
Mar 16 12:16:45.803: CRYPTO-KE: Sent 64 bytes.

Mar 16 12:16:56.083: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.087: CRYPTO-KE: Received 4 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 2 bytes.
Mar 16 12:16:56.091: CRYPTO-KE: Received 52 bytes.
Mar 16 12:16:56.095: CRYPTO-KE: Received 12 bytes.
```

- **clear crypto connection**A continuación se muestra un ejemplo de resultado del comando.

```
wan-2511#show crypto engine connections act
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 9    Serial0         20.20.20.21 set    DES_56_CFB64    29       28

wan-2511#clear crypto connection 9
wan-2511#
*Mar  5 04:58:20.690: CRYPTO: Replacing 9 in crypto maps with 0 (slot 0)
*Mar  5 04:58:20.694: Crypto engine 0: delete connection 9
*Mar  5 04:58:20.694: CRYPTO: Crypto Engine clear conn_id 9 slot 0: OK
wan-2511#
wan-2511#show crypto engine connections act
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt

wan-2511#
```

- **crypto zeroize**A continuación se muestra un ejemplo de resultado del comando.

```
wan-2511#show crypto mypubkey
```

```
crypto public-key wan2511 01496536
 11F43C02 70C0ADB7 5DD50600 A0219E04 C867A5AF C40A4FE5 CE99CCAB A8ECA840
 EB95FBEE D727ED5B F0A6F042 BDB5529B DBB0698D DB0B2756 F6CABE8F 05E4B27F
quit

wan-2511#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
wan-2511(config)#crypto zeroize
Warning! Zeroize will remove your DSS signature keys.
Do you want to continue? [yes/no]: yes
% Keys to be removed are named wan2511.
Do you really want to remove these keys? [yes/no]: yes
% Zeroize done.

wan-2511(config)#^Z
wan-2511#
wan-2511#show crypto mypubkey
wan-2511#
```

- **no crypto public-key**A continuación se muestra un ejemplo de resultado del comando.

```
wan-2511#show crypto pubkey
crypto public-key wan2516 01698232
 B1C127B0 78D79CAA 67ECAD80 03D354B1 9012C80E 0C1266BE 25AEDE60 37A192A2
 B066D299 77174D48 7FBAB5FC 2B60893A 37E5CB7B 62F6D902 9495733B 98046962
quit

wan-2511#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
wan-2511(config)#crypto public-key ?
  WORD  Peer name

wan-2511(config)#
wan-2511(config)#no crypto public-key wan2516 01698232
wan-2511(config)#^Z
wan-2511#
wan-2511#show crypto pubkey
wan-2511#
```

Resolución de problemas de Cisco 7200 con ESA

Cisco también proporciona una opción de asistencia de hardware para realizar el cifrado en los Cisco 7200 Series Routers, que se denomina ESA. El ESA está en la forma de un adaptador de puerto para la tarjeta VIP2-40 o un adaptador de puerto independiente para el Cisco 7200. Esta disposición permite el uso de un adaptador de hardware o del motor de software VIP2 para cifrar y descifrar los datos que entran o salen a través de las interfaces en la tarjeta Cisco 7500 VIP2. El Cisco 7200 permite que el hardware ayude a cifrar el tráfico para cualquier interfaz del chasis Cisco 7200. El uso de una ayuda de cifrado guarda los ciclos de CPU valiosos que se pueden utilizar para otros fines, como el ruteo o cualquiera de las otras funciones de Cisco IOS.

En un Cisco 7200, el adaptador de puerto independiente se configura exactamente igual que el motor crypto del software Cisco IOS, pero tiene unos cuantos comandos adicionales que sólo se utilizan para el hardware y para decidir qué motor (software o hardware) realizará el cifrado.

En primer lugar, prepare el router para el cifrado de hardware:

```
wan-7206a(config)#
%OIR-6-REMCARD: Card removed from slot 3, interfaces disabled
*Mar  2 08:17:16.739: ...switching to SW crypto engine
```

```
wan-7206a#show crypto card 3

Crypto card in slot: 3

Tampered:        No
Xtracted:        Yes
Password set:    Yes
DSS Key set:     Yes
FW version       0x5049702
wan-7206a#

wan-7206a(config)#

wan-7206a(config)#crypto zeroize 3
Warning! Zeroize will remove your DSS signature keys.
Do you want to continue? [yes/no]: yes
% Keys to be removed are named hard.
Do you really want to remove these keys? [yes/no]: yes
[OK]
```

Active o desactive el cifrado de hardware como se muestra a continuación:

```
wan-7206a(config)#crypto esa shutdown 3
...switching to SW crypto engine


wan-7206a(config)#crypto esa enable 3
There are no keys on the ESA in slot 3- ESA not enabled.
```

A continuación, genere claves para el ESA antes de habilitarlo.

```
wan-7206a(config)#crypto gen-signature-keys hard
% Initialize the crypto card password. You will need
   this password in order to generate new signature
   keys or clear the crypto card extraction latch.

Password:
Re-enter password:
Generating DSS keys ....
 [OK]

wan-7206a(config)#
wan-7206a#show crypto mypubkey
crypto public-key hard 00000052
 EE691A1F BD013874 5BA26DC4 91F17595 C8C06F4E F7F736F1 AD0CACEC 74AB8905
 DF426171 29257F8E B26D49B3 A8E11FB0 A3501B13 D3F19623 DCCE7322 3D97B804
quit

wan-7206a#
wan-7206a(config)#crypto esa enable 3
...switching to HW crypto engine

wan-7206a#show crypto engine brie
crypto engine name:   hard
crypto engine type:   ESA
serial number:        00000052
crypto engine state:  installed
crypto firmware version:  5049702
crypto engine in slot: 3

wan-7206a#
```

Resolución de problemas de VIP2 con ESA

El adaptador de puerto de hardware ESA en la tarjeta VIP2 se utiliza para cifrar y descifrar los datos que entran o salen a través de las interfaces en la tarjeta VIP2. Al igual que con el Cisco 7200, el uso de una ayuda de cifrado ahorra preciosos ciclos de CPU. En este caso, el comando **crypto esa enable** no existe porque el adaptador de puerto ESA hace el cifrado para los puertos en la tarjeta VIP2 si el ESA está conectado. El **clear-latch criptográfico** debe aplicarse a ese slot si el adaptador de puerto ESA se instaló por primera vez o se quitó luego se reinstaló.

```
Router#show crypto card 11

Crypto card in slot: 11

Tampered:        No
Xtracted:        Yes
Password set:    Yes
DSS Key set:     Yes
FW version       0x5049702
Router#
```

Debido a que se extrajo el módulo crypto ESA, recibirá el siguiente mensaje de error hasta que ejecute un comando **crypto clear-latch** en ese slot, como se muestra a continuación.

```
----
*Jan 24 02:57:09.583: CRYPTO: Sign done. Status= Extraction latch set. Request not allowed.
-----
Router(config)#crypto clear-latch ?
  <0-15>  Chassis slot number

Router(config)#crypto clear-latch 11
% Enter the crypto card password.
Password:
Router(config)#^Z
```

Si olvida una contraseña asignada previamente, utilice el comando **crypto zeroize** en lugar del comando **crypto clear-latch** para restablecer el ESA. Después de ejecutar el comando **crypto zeroize**, debe regenerar e intercambiar claves DSS. Cuando se regeneran las claves DSS, se le solicita que cree una nueva contraseña. Se presenta un ejemplo a continuación:

```
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#show crypto card 11

Crypto card in slot: 11

Tampered:        No
Xtracted:        No
Password set:    Yes
DSS Key set:     Yes
FW version       0x5049702
Router#

-------------------------------------------------


Router#show crypto engine brief
crypto engine name:   TERT
crypto engine type:   software
serial number:        0459FC8C
```

```
crypto engine state:  dss key generated
crypto lib version:   5.0.0
crypto engine in slot: 6

crypto engine name:   WAAA
crypto engine type:   ESA
serial number:        00000078
crypto engine state:  dss key generated
crypto firmware version:  5049702
crypto engine in slot: 11

Router#
-----------
Router(config)#crypto zeroize
Warning! Zeroize will remove your DSS signature keys.
Do you want to continue? [yes/no]: yes
% Keys to be removed are named TERT.
Do you really want to remove these keys? [yes/no]: yes
% Zeroize done.

Router(config)#crypto zeroize  11
Warning! Zeroize will remove your DSS signature keys.
Do you want to continue? [yes/no]: yes
% Keys to be removed are named WAAA.
Do you really want to remove these keys? [yes/no]: yes
[OK]

Router(config)#^Z
Router#show crypto engine brief
crypto engine name:   unknown
crypto engine type:   software
serial number:        0459FC8C
crypto engine state:  installed
crypto lib version:   5.0.0
crypto engine in slot: 6

crypto engine name:   unknown
crypto engine type:   ESA
serial number:        00000078
crypto engine state:  installed
crypto firmware version:  5049702
crypto engine in slot: 11

Router#
--------------
Router(config)#crypto gen-signature-keys VIPESA 11
% Initialize the crypto card password. You will need
   this password in order to generate new signature
   keys or clear the crypto card extraction latch.

Password:
Re-enter password:
Generating DSS keys ....
 [OK]

Router(config)#
*Jan 24 01:39:52.923: Crypto engine 11: create key pairs.
^Z
Router#
------
Router#show crypto engine brief
crypto engine name:   unknown
crypto engine type:   software
serial number:        0459FC8C
```

```
crypto engine state:  installed
crypto lib version:   5.0.0
crypto engine in slot: 6

crypto engine name:   VIPESA
crypto engine type:   ESA
serial number:        00000078
crypto engine state:  dss key generated
crypto firmware version:  5049702
crypto engine in slot: 11

Router#
----------
Router#show crypto engine connections active 11
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 2    Serial11/0/0    20.20.20.21 set    DES_56_CFB64    9996     9996

Router#
Router#clear crypto connection 2 11
Router#
*Jan 24 01:41:04.611: CRYPTO: Replacing 2 in crypto maps with 0 (slot 11)
*Jan 24 01:41:04.611: Crypto engine 11: delete connection 2
*Jan 24 01:41:04.611: CRYPTO: Crypto Engine clear conn_id 2 slot 11: OK
Router#show crypto engine connections active 11
No connections.

Router#
*Jan 24 01:41:29.355: CRYPTO ENGINE:Number of connection entries
received from VIP 0
------------

Router#show crypto mypub
% Key for slot 11:
crypto public-key VIPESA 00000078
 CF33BA60 56FCEE01 2D4E32A2 5D7ADE70 6AF361EE 2964F3ED A7CE08BD A87BF7FE
 90A39F1C DF96143A 9B7B9C78 5F59445C 27860F1E 4CD92B6C FBC4CBCC 32D64508
quit

Router#show crypto pub
crypto public-key wan2516 01698232
 C5DE8C46 8A69932C 70C92A2C 729449B3 FD10AC4D 1773A997 7F6BA37D 61997AC3
 DBEDBEA7 51BF3ADD 2BB35CB5 B9126B4D 13ACF93E 0DF0CD22 CFAAC1A8 9CE82985
quit

Router#
----------
interface Serial11/0/0
 ip address 20.20.20.21 255.255.255.0
 encapsulation ppp
 ip route-cache distributed
 no fair-queue
 no cdp enable
 crypto map test
!
----------
Router#show crypto eng conn act 11
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 3    Serial11/0/0    20.20.20.21 set    DES_56_CFB64    761      760

Router#
*Jan 24 01:50:43.555: CRYPTO ENGINE:Number of connection
entries received from VIP 1

Router#
```

Información Relacionada

- Configuración y resolución de problemas del cifrado de la capa de red de Cisco: IPSec e ISAKMP - Parte 2
- DES FIPS 46-2 en el Instituto Nacional de Normas y Tecnología (NIST)
- DSS FIPS 186 en el Instituto Nacional de Normas y Tecnología (NIST)
- Preguntas frecuentes de RSA Laboratories sobre criptografía de hoy
- Estándares de seguridad IETF
- Configuración del protocolo de seguridad de intercambio de claves de Internet
- Configuración de seguridad de red IPSec
- Página de soporte de IPSec
- Soporte Técnico - Cisco Systems