Configurando y resolviendo problemas la encripción de capa de red de Cisco: Fondo - Parte 1

Contenido

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.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

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

- Software Release 11.2 y Posterior de Cisco IOS®

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

Convenciones

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

Información previa y configuración de la encripción de capa de red

La característica de la encripción de capa de red fue introducida en el Software Release 11.2 de Cisco IOS®. Proporciona un mecanismo para la transmisión de datos seguros y consiste en dos componentes:

- **Autenticación del router:** Antes de pasar el tráfico encriptado, dos Routers realiza un de una sola vez, autenticación bidireccional usando las claves públicas del Digital Signature Standard (DSS) para firmar los desafíos al azar.
- **Encripción de capa de red:** Para el cifrado de la carga útil IP, el uso del Routers intercambio de claves Diffie-Hellman de generar con seguridad una clave de la sesión DES(40- o 56-bit), DES triple - 3DES(168-bit), o el Advanced Encryption Standard más reciente - AES(128-bit(default), o 192-bit, o clave del 256-bit), introducida en 12.2(13)T. Las nuevas claves de la sesión se generan en una base a la configuración. La política de encripción es fijada por los mapas de criptografía que utilizan las listas de acceso IP ampliado para definir que la red, la subred, el host, o los pares del protocolo deben ser cifrados entre el Routers.

Información previa de criptografía

El campo de la criptografía se refiere a mantener las comunicaciones privadas. La protección de comunicaciones delicadas ha sido la énfasis en la criptografía en mucho de su historial. El cifrado es la transformación de datos en una cierta forma ilegible. Su propósito es asegurar la aislamiento manteniendo la información ocultada de cualquier persona para quién no se piensa, incluso si él puede ver los datos encriptados. El desciframiento es el revés del cifrado: es la transformación de los datos encriptados nuevamente dentro de una forma inteligible.

El cifrado y el desciframiento requieren el uso de una cierta información secreta, referido generalmente como una “clave”. Dependiendo del mecanismo de encripción usado, la misma clave se pudo utilizar para el cifrado y el desciframiento; mientras que para otros mecanismos, las claves usadas para el cifrado y el desciframiento pudieron ser diferentes.

Una firma digital ata un documento al poseedor de una clave determinada, mientras que un grupo fecha/hora digital ata un documento a su creación en un momento determinado. Estos mecanismos criptográficos se pueden utilizar para controlar el acceso a una unidad de disco compartida, una instalación de alta seguridad, o a un canal de televisión del pago por visión.

Mientras que la criptografía moderna está creciendo cada vez más diversa, la criptografía se basa fundamental en los problemas que son difíciles de solucionar. Un problema puede ser difícil porque su solución requiere conocer la clave, tal como desencriptar un mensaje encriptado o firma de un cierto documento digital. El problema puede también ser difícil porque es intrínseco difícil completar, por ejemplo encontrar un mensaje que produzca un valor de troceo dado.

Pues el campo de la criptografía ha avanzado, las líneas divisorias para cuál es y cuál no es criptografía se han enmascarado. La criptografía se pudo resumir hoy como el estudio de las técnicas y de las aplicaciones que dependen de la existencia de problemas matemáticos que es difícil de solucionar. Un criptoanalista intenta comprometer los mecanismos criptográficos, y la criptología es la disciplina de la criptografía y del criptoanálisis combinados.

Definiciones

Esta sección define los términos relacionados usados en este documento.

- **Autenticación:** La propiedad de saber que los datos recibidos son enviados realmente por el remitente demandado.
- **Confidencialidad:** La propiedad de la comunicación de modo que los receptores deseados conozcan se está enviando qué pero los partidos involuntarios no puede determinar se envía qué.
- **Data Encryption Standard (DES):** El DES utiliza un método de la clave simétrica, también conocido como método de la clave secreta. Esto significa que si un bloque de los datos se cifra con la clave, el bloque cifrado se debe desencriptar con la misma clave, así que el encryptor y el decrypter deben utilizar la misma clave. Aunque se sabe y se publica bien el método de encripción, el método del ataque conocido del mejor está público con la fuerza bruta. Las claves se deben probar contra los bloques cifrados para considerar si pueden resolverlos correctamente. Mientras que los procesadores llegan a ser más potentes, la vida natural del DES está acercando a su extremo. Por ejemplo, un esfuerzo coordinado usando la potencia de procesamiento de repuesto de miles de computadoras a través de Internet puede encontrar la clave 56-bit a un mensaje DES cifrado en 21 días.El DES es validado cada cinco años por el National Security Agency E.E.U.U. (NSA) para resolver los propósitos del gobierno de los EE. UU. La autorización actual expira en 1998 y el NSA ha indicado que re-no certificarán el DES. Se están moviendo más allá del DES, otros algoritmos de encripción que también no tienen ninguna debilidades sabida con excepción de los ataques de fuerza bruta. Para la información adicional, vea DES FIP 46-2 por el National Institute of Standards and Technology (NIST) .
- **Desciframiento:** La aplicación reversa de un algoritmo de encripción a los datos encriptados, de tal modo restableciendo esos datos a su estado original, unencrypted.
- **DSS y Digital Signature Algorithm (DSA):** El DSA fue publicado por el NIST en el Digital Signature Standard (DSS), que es parte del proyecto del Capstone del gobierno E.E.U.U. El DSS fue seleccionado por el NIST, en cooperación con el NSA, para ser el estándar de autenticación digital del gobierno E.E.U.U. El estándar fue publicado en mayo 19, 1994.
- **Cifrado:** La aplicación de un algoritmo específico a los datos para alterar el aspecto de los

datos que lo hacen incomprensible a los que no se autorizan para ver la información.

- **Integridad:** La propiedad de asegurarse de que los datos estén transmitidos de la fuente al destino fuera alteración no detectada.
- **No renegación:** La propiedad de un receptor que puede probar que el remitente de un ciertos datos de hecho envió los datos aunque el remitente pudo desear más adelante de negar nunca el enviar de esos datos.
- **Cifrado de clave pública:** El cifrado tradicional se basa en el remitente y el receptor de un mensaje que conocen y que usan la misma clave secreta. El remitente utiliza la clave secreta para cifrar el mensaje, y el receptor utiliza la misma clave secreta para desencriptar el mensaje. Este método se conoce como la “clave secreta” o “criptografía simétrica.” La cuestión principal está consiguiendo el remitente y al receptor estar de acuerdo con la clave secreta sin nadie que descubre. Si están en las ubicaciones físicas separadas, deben confiar en un mensajero, o un sistema telefónico, o un poco de otro medio de transmisión para prevenir el acceso de la clave secreta que es comunicada. Cualquier persona que oye por casualidad o intercepta la clave adentro transita puede leer más adelante, modificar, y forjar todos los mensajes cifrados o autenticados usando esa clave. La generación, la transmisión, y el almacenamiento de las claves se llama administración de claves; todos los sistemas criptográficos deben ocuparse de los problemas de administración de claves. Porque todas las claves en un sistema criptográfico de clave secreta deben seguir siendo secretas, la criptografía de clave secreta tiene a menudo dificultad que provee de la administración de claves segura, especialmente en los sistemas operativos un gran número de usuarios.El concepto de Cifrado de clave pública fue introducido en 1976 por Whitfield Diffie y Martin Hellman para solucionar el problema de administración de claves. En su concepto, cada persona consigue un par de claves, uno llamado la clave pública y el otro llamado la clave privada. Se publica la clave pública de cada persona mientras que la clave privada se mantiene secreta. La necesidad del remitente y del receptor de compartir la información secreta se elimina y todas las comunicaciones implican solamente las claves públicas, y no se transmite ni se comparte ninguna clave privada nunca. Está no más necesaria confiar en el canal de algunas comunicaciones para ser segura en contra de escuchar detras de las puertas o la traición. El único requisito es que las claves públicas están asociadas a sus usuarios de una manera (autenticada) de confianza (por ejemplo, en un directorio de confianza). Cualquier persona puede enviar un mensaje confidencial simplemente usando la información pública, pero el mensaje se puede desencriptar solamente con una clave privada, que está en propiedad única del receptor deseado. Además, el Cifrado de clave pública se puede utilizar no sólo para la aislamiento (cifrado), pero para la autenticación (firmas digitales) también.
- **Firmas digitales de la clave pública:** Para firmar un mensaje, una persona realiza un cómputo que implica su clave privada y el mensaje sí mismo. La salida se llama la firma digital y se asocia al mensaje, que entonces se envía. Una segunda persona verifica la firma realizando un cómputo que implica el mensaje, la supuesta firma, y la clave pública de la primera persona. Si el resultado celebra correctamente en una relación matemática simple, la firma se verifica como siendo auténtica. Si no, la firma puede ser fraudulenta o el mensaje pudo haber sido alterado.
- **Encripción de clave pública:** Cuando una persona desea enviar un mensaje privado a otra persona, la primera persona mira para arriba la clave pública de la segunda persona en un directorio, la utiliza para cifrar el mensaje y la envía. La segunda persona entonces utiliza su clave privada para desencriptar el mensaje y para leerlo. Nadie que escucha adentro puede desencriptar el mensaje. Cualquier persona puede enviar un mensaje encriptado a la

segunda persona pero solamente la segunda persona puede leerlo. Claramente, un requisito es que nadie puede imaginar la clave privada de la clave pública correspondiente.
- **Análisis del tráfico:** El análisis del flujo del tráfico de la red con el fin de deducir la información que es útil a un adversario. Los ejemplos de tal información son frecuencia de transmisión, las identidades de los partidos de conversación, los tamaños de los paquetes, los identificadores del flujo usados, y así sucesivamente.

Información preliminar

Esta sección discute algunos conceptos básicos de la encripción de capa de red. Contiene los aspectos de encripción para los cuales usted debe mirar hacia fuera. Inicialmente, estos problemas no pueden tenerle sentido, sino que es una buena idea leerlos encima ahora y ser consciente de ellos porque tendrán más sentido después de que usted haya trabajado con el cifrado por varios meses.

- Es importante observar que el cifrado ocurre solamente en la salida de una interfaz y el desciframiento ocurre solamente sobre la entrada a la interfaz. Esta distinción es importante al acepillar su directiva. La política para encripción y el desciframiento es simétricos. Esto significa que eso la definición de uno da le a otro automáticamente. Con las correspondencias de criptografía y sus listas de acceso ampliadas asociadas, solamente la política de encripción se define explícitamente.La política de descifrado utiliza la información idéntica, pero cuando corresponder con los paquetes, él invierte las direcciones de origen y de destino y los puertos. Esta manera, los datos se protege en las ambas direcciones de una conexión dúplex. La declaración de la *coincidencia x de dirección* en el **comando crypto map** se utiliza para describir los paquetes que salen de una interfaz. Es decir está describiendo la encripción de paquetes. Sin embargo, los paquetes se deben también corresponder con para el desciframiento mientras que ingresan la interfaz. Esto es hecha automáticamente atravesando la lista de acceso con las direcciones de origen y de destino y los puertos invertidos. Esto proporciona la simetría para la conexión. La lista de acceso señalada por a la **correspondencia de criptografía** debe describir el tráfico en una dirección (saliente) solamente. Los paquetes del IP que no corresponden con la lista de acceso que usted define serán transmitidos pero no cifrados. “Niegue” en la lista de acceso indica que esos host no deben ser correspondidos con, que significa que no serán cifrados. “Niegue”, en este contexto, no significa que el paquete está caído.
- Tenga muy cuidado de usar la palabra “” en las listas de acceso ampliadas. Usando “cualquier” hace su tráfico ser caído a menos que se dirija a la interfaz “O.N.U-que cifra” que corresponde con. Además, con el IPSec en el Cisco IOS Software Release 11.3(3)T, “ninguno” no se permite.
- El uso de la “cualquier” palabra clave se desalienta en especificar a las direcciones de origen o de destino. Especificar “ningunos” puede causar los problemas con los Routing Protocol, el Network Time Protocol (NTP), la generación de eco, la respuesta de la generación de eco, y el tráfico Multicast, pues el router de recepción desecha silenciosamente este tráfico. Si se va “ninguno” a ser utilizado, debe ser precedida por “niega” las declaraciones para el tráfico que no debe ser cifrado, por ejemplo el “NTP”.
- Para salvar el tiempo, aseegurese le puede **hacer ping al** router del par con quien usted está intentando tener una asociación de encripción. También, tenga el ping de los dispositivos extremos (que depende de conseguir su tráfico cifrado) antes de que usted pase demasiada hora que resuelve problemas el problema incorrecto. Es decir aseegurese los trabajos de la

encaminamiento antes de intentar hacer **crypto**. El peer remoto puede no tener una ruta para la interfaz de egreso, en este caso usted no puede tener una sesión de encripción con ese par (usted puede poder utilizar el **IP innumerable** en esa interfaz serial).

- Muchos enlaces punto a punto PÁLIDOS utilizan los IP Addresses no rutables, y el cifrado del Cisco IOS Software Release 11.2 confía en el Internet Control Message Protocol (ICMP) (significado que utiliza la dirección IP de la interfaz serial de la salida para el ICMP). Esto puede forzarle a utilizar el **IP innumerable** en la interfaz de WAN. Haga siempre un **comando ping and traceroute** de aseegurarse que el rutear existe para el dos (el cifrar/que desencripta) Routers de mirada.
- Se permite a solamente dos Routers compartir una clave de la sesión de Diffie Hellman. Es decir, un router no puede intercambiar los paquetes encriptados a dos pares que usan la misma clave de la sesión; cada par de Routers debe tener una clave de la sesión que sea un resultado de a intercambio Diffie-Hellman entre él.
- El motor de criptografía está en el Cisco IOS, el Cisco IOS VIP2, o en hardware el adaptador de los servicios de encripción (ESA) en un VIP2. Sin un VIP2, el motor de criptografía del Cisco IOS gobierna la política de encripción en todos los puertos. En las Plataformas usando el VIP2, hay motores de criptografía múltiples: uno en el Cisco IOS, y uno en cada VIP2. El motor de criptografía en un VIP2 gobierna el cifrado en los puertos que residen en la tarjeta.
- Aseegurese que el tráfico está fijado para llegar una interfaz preparada para cifrarla. Si el tráfico puede llegar de alguna manera en una interfaz con excepción de la que está con la **correspondencia de criptografía** aplicada, se cae silenciosamente.
- Ayuda a tener acceso de la consola (o suplente) a ambo Routers al hacer el intercambio de claves; es posible conseguir al lado pasivo colgar mientras que espera una clave.
- **El cfb-64** es más eficiente procesar que **cfb-8** en términos de carga de la CPU.
- El router necesita funcionar con el algoritmo que usted quiere utilizar con el modo del cifra-feedback (CFB) que usted quiere utilizar; los valores por defecto para cada imagen son el nombre de la imagen (tal como "56") con **cfb-64**.
- Consider que cambia el clave-descanso. El valor por defecto del 30 minutos es muy corto. Intento que lo aumenta a un día (1440 minutos).
- El tráfico IP se cae durante la renegociación dominante cada vez que expira la clave.
- Seleccione solamente el tráfico que usted quiere realmente cifrar (éste guarda los ciclos de la CPU).
- Con el Dial-on-Demand Routing (DDR), haga el ICMP interesante o nunca marcará hacia fuera.
- Si usted quiere cifrar el tráfico con excepción del IP, utilice un túnel. Con los túneles, aplique las correspondencias de criptografía a la comprobación y a las interfaces del túnel. Vea la muestra 5: Cifrado del tráfico IPX en un túnel IP para más información.
- El dos Routers del peer de encripción no necesita ser conectado directamente.
- Un router de menor capacidad puede darle un mensaje "CPU hog". Esto puede ser ignorada porque es diciéndole que el cifrado utiliza a muchos recursos de la CPU.
- No coloque a los routeres de encripción redundante de modo que usted desencripte y encripte nuevamente el tráfico y la basura CPU. Cifre simplemente en las dos puntos finales. Vea la muestra 3: Cifrado y a través de un router para más información.
- Actualmente, el cifrado del broadcast y los paquetes de multidifusión no se soporta. Si las actualizaciones de ruteo “seguras” son importantes para un diseño de red, un protocolo con la autenticación incorporada se debe utilizar, por ejemplo el Enhanced Interior Gateway Routing Protocol (EIGRP), el Open Shortest Path First (OSPF), o el Routing Information Protocol versión 2 (RIPv2) para asegurar la integridad de la actualización.

Advertencias

Nota: Las advertencias mencionadas abajo todos se han resuelto.

- Un Cisco 7200 Router que usa un ESA para el cifrado no puede desencriptar un paquete conforme a una clave de la sesión y después encriptarlo nuevamente conforme a una diversa clave de la sesión. Refiera al Id. de bug Cisco CSCdj82613 (clientes registrados solamente).
- Cuando dos Routers es conectado por una línea arrendada cifrada y una línea de backup ISDN, si la línea arrendada cae, el link ISDN sube muy bien. Sin embargo, cuando viene la línea arrendada salvaguardia otra vez, el router que puso la llamada ISDN causa un crash. Refiera al Id. de bug Cisco CSCdj00310 (clientes registrados solamente).
- Para los Cisco 7500 Series Router con el VIP múltiple, si una **correspondencia de criptografía** se aplica incluso a una interfaz de cualquier VIP, uno o más VIP causan un crash. Refiera al Id. de bug Cisco CSCdi88459 (clientes registrados solamente).
- Para los Cisco 7500 Series Router con un VIP2 y un ESA, el **comando show crypto card** no hace muestra del resultado a menos que el usuario esté en el puerto de la consola. Refiera al Id. de bug Cisco CSCdj89070 (clientes registrados solamente).

Configuración de la encripción de capa de red del Cisco IOS

Las configuraciones del Cisco IOS del ejemplo de funcionamiento en este documento vinieron directamente de los routeres del laboratorio. La única alteración hecha a ellas era el retiro de las configuraciones de la interfaz no relacionada. Todo el material aquí vino libremente de los recursos disponibles en Internet o en la sección de información relacionada en el extremo de este documento.

Todas las configuraciones de muestra en este documento son de Cisco IOS Software Release 11.3. Había varios cambios de los comandos del Cisco IOS Software Release 11.2, tales como la adición de las palabras siguientes:

- dss en algunos de los comandos configuration dominantes.
- Cisco en algunos de los **comandos show** y de los **comandos crypto map** de distinguir entre la encripción propietaria de Cisco (como se encuentra en el Cisco IOS Software Release 11.2 y Posterior) y el IPSec que está en el Cisco IOS Software Release 11.3(2)T.

Nota: Los IP Addresses usados en estos ejemplos de configuración fueron elegidos aleatoriamente en el laboratorio de Cisco y se piensan para ser totalmente genéricos.

Paso 1: Genere manualmente los pares claves DSS

Un par clave DSS (una clave pública y privada) necesita ser generado manualmente en cada router que participa en la sesión de encripción. Es decir cada router debe tener sus propias claves DSS para participar. Un motor de encripción puede tener solamente un DSS dominante que lo identifique únicamente. La palabra clave “dss” fue agregada en el Cisco IOS Software Release 11.3 para distinguir el DSS de las claves RSA. Usted puede especificar cualquier nombre para propias claves DSS del router (aunque, se recomienda para utilizar el nombre del host del router). En menos CPU potente (por ejemplo las Cisco 2500 Series), generación de par clave toma cerca de 5 segundos o menos.

El router genera un par de claves:

- Una clave pública (que se envía más adelante al Routers que participa en las sesiones de encripción).
- Una clave privada (que no se considera ni se intercambia por nadie; de hecho, se salva en una sección aparte de NVRAM que no se pueda ver).

Una vez que se ha generado el par clave DSS del router, se asocia únicamente al motor de criptografía en ese router. La generación de par clave se muestra en la salida del comando de ejemplo abajo.

```
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#
```

Porque usted puede generar solamente un par clave que identifique al router, usted puede sobregrabar su clave original y necesitar volver a enviar su clave pública con cada router en la asociación de encripción. Esto se muestra en la salida del comando de ejemplo abajo:

```
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 de propio par clave DSS del router es el primer paso en el establecimiento de una asociación de sesión de encripción. El siguiente paso es intercambiar las claves públicas por cada otro router. Usted puede ingresar estas claves públicas manualmente primero ingresando el **comando show crypto mypubkey** de visualizar la clave pública DSS del router. Usted después intercambia estas claves públicas (vía el correo electrónico, por ejemplo) y, por el **comando crypto key pubkey-chain dss**, corta y pegar la clave pública de su router del par en el router.

Usted puede también utilizar el **comando crypto key exchange dss** de tener las claves públicas del intercambio del Routers automáticamente. Si usted utiliza el método automatizado, aseegurese allí no son ninguna **sentencia de correspondencia de criptografía** en las interfaces usadas para el intercambio de claves. **Una clave del debug crypto** es útil aquí.

Nota: Es una buena idea **hacer ping a** su par antes de intentar intercambiar las 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 públicas DSS, aseegurese que ambo Routers tiene claves públicas de cada uno y que él hace juego, tal y como se muestra en de la salida de comando abajo.

```
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 del Cisco IOS para el link dedicado

Después de que las claves DSS se hayan generado en cada router y se han intercambiado las claves públicas DSS, el **comando crypto map** puede ser aplicado a la interfaz. La sesión de criptografía comienza generando el tráfico que hace juego la lista de acceso usada por las correspondencias de criptografía.

```
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#
```

Muestra 2: Configuración del Cisco IOS para el Frame Relay de tramas multipunto

Tomaron la salida del comando de ejemplo siguiente del router de eje de conexión.

```
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#
```

Tomaron la salida del comando de ejemplo siguiente 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#
```

Tomaron la salida del comando de ejemplo siguiente 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#
```

Tomaron la salida del comando de ejemplo siguiente del switch de 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
!
```

Muestra 3: Cifrado de y hasta un router

El Routers del par no tiene que ser un salto lejos. Usted puede crear a una sesión de peer con un router remoto. En el siguiente ejemplo, la meta es cifrar todo el tráfico de la 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 preocupación con el tráfico encriptado entre 40.40.40.0/24 y 30.30.30.0/24.

El router wan-4500b tiene una asociación de sesión de encripción con el perdedor y también con StHelen. Cifrando el tráfico del segmento Ethernet wan-4500b al segmento Ethernet del StHelen's, usted evita el paso innecesario del desciframiento en el perdedor. El perdedor pasa simplemente el tráfico encriptado encendido a la interfaz serial del StHelen's, donde se desencripta. Esto reduce el retraso de tráfico para los paquetes del IP y los ciclos de la CPU en el router Loser. Lo que es más importante, aumenta grandemente la Seguridad del sistema, puesto que un eavesdropper en el perdedor no puede leer el tráfico. Si el perdedor desencriptara el tráfico, habría una ocasión que los datos desencriptados podrían ser desviados.

```
[wan-4500b]<Ser0>--   ---<Ser0> [Loser] <Ser1>--   ----<Ser1>[StHelen]
             |                            |                          |
             |                            |                          |
           -----                        -------                    -------
          180.180.180/24                40.40.40/24                30.30.30/24 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#

Muestra 4: Crypto con DDR

Porque el Cisco IOS confía en el ICMP para establecer a las sesiones de encripción, el tráfico ICMP se debe clasificar como “interesante” en la lista del dialer al hacer el cifrado sobre un link DDR.

Nota: La compresión trabaja en el Cisco IOS Software Release 11.3, pero no es muy útil para los datos encriptados. Porque los datos encriptados al azar-están mirando bastante, la compresión reduce solamente las cosas. Pero usted puede dejar la característica encendido para el tráfico no encriptado.

En algunas situaciones, usted querrá el Respaldo de marcado al mismo router. Por ejemplo, es útil cuando los usuarios quieren proteger contra el error de un link determinado en sus redes WAN. Si dos interfaces van al mismo par, la misma correspondencia de criptografía se puede utilizar en ambas interfaces. La Interfaz de respaldo se debe utilizar para que esta característica funcione correctamente. Si un diseño de reserva tiene un dial del router en un diverso cuadro, diversas correspondencias de criptografía se deben ser creadas y los pares fijar por consiguiente. Una vez más el **comando backup interface** debe ser utilizado.

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 1oNe1wDbhBdcN6x9Y5gfuMjqh10 ! 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 1VdPYuA/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#
```

Muestra 5: Cifrado del tráfico IPX en un túnel IP

En este ejemplo, el tráfico IPX en un túnel IP se cifra.

Nota: Solamente el tráfico en este túnel (IPX) se cifra. 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#
```

Muestra 6: Cifrado de túneles L2F

En este ejemplo, solamente el tráfico L2F que cifra para los usuarios que marcan adentro se intenta. Aquí, “user@cisco.com” llama el servidor de acceso de la red local (NAS) nombró el

"DEMO2" en su ciudad y consigue hecho un túnel al CD del gateway de inicio. Se cifra todo el tráfico DEMO2 (junto con el de otros llamadores L2F). Porque el L2F utiliza el puerto 1701 UDP, éste es cómo la lista de acceso se construye, determinando se cifra qué tráfico.

Nota: Si la asociación de encripción no es ya configurar, significar al llamador es la primera persona a llamar adentro y crear el túnel L2F, el llamador puede conseguir caído debido al retardo en configurar la asociación de encripción. Esto puede no suceder en el Routers con bastantes energías en la CPU. También, usted puede querer aumentar el **keytimeout** de modo que el cifrado pusiera y el desmontaje ocurra solamente durante las horas no pico.

Tomaron la salida del comando de ejemplo siguiente del telecontrol NAS.

```
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#
```

Tomaron la salida del comando de ejemplo siguiente 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

Es generalmente el mejor comenzar a cada sesión de Troubleshooting recopilando la información usando los **comandos show** siguientes. Un asterisco (*) indica especialmente un comando útil. También vea por favor el Troubleshooting de IP Security - Entendiendo y con los comandos debug para la 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 un comando debug, consulte Información Importante sobre Comandos Debug.

Comandos	
muestre los algoritmos de Cisco crypto	muestre el clave-descanso crypto de Cisco
muestre el Pregen-dh-pairs crypto de Cisco	*show las conexiones del motor de criptografía activas
paquete perdidos del show crypto engine connections	configuración del show crypto engine
mypubkey dss del show crypto key	*show el pubkey-encadenamiento dss del crypto key
muestre el interface serial 1 de la correspondencia de criptografía	*show la correspondencia de criptografía
debug crypto engine	* sess del debug crypto
clave del grito del debug	clear crypto connection
zeroize crypto	ninguna clave pública crypto

- muestre los algoritmos de Cisco crypto- Usted debe habilitar todos los algoritmos del Data Encryption Standard (DES) que se utilicen para comunicar con cualquier otro router de encripción del par. Si usted no habilita un algoritmo DES, usted no podrá utilizar ese algoritmo, incluso si usted intenta asignar el algoritmo a una correspondencia de criptografía en otro momento.Si su router intenta configurar a una sesión de comunicación encriptada con un router del par, y el dos Routers no tiene el mismo algoritmo DES habilitado en los ambos extremos, la sesión encriptada falla. Si por lo menos un algoritmo común DES se habilita en los ambos extremos, la sesión encriptada puede proceder.**Nota:** La palabra adicional Cisco aparece en el Cisco IOS Software Release 11.3 y es necesaria distinguir entre el IPSec y la encripción propietaria de Cisco encontró en el Cisco IOS Software Release 11.2.`Loser#`**`show crypto cisco algorithms`** `des cfb-64 des cfb-8 40-bit-des cfb-64 40-bit-des cfb-8`
- muestre el clave-descanso crypto de Cisco - Después de que establezcan a una sesión de comunicación encriptada, es válido para una longitud del tiempo específica. Después de esta longitud del tiempo, los tiempos de la sesión hacia fuera. Una nueva sesión debe ser negociada, y una nueva clave DES (sesión) se debe generar para que la comunicación encriptada continúe. Utilice este comando de cambiar el tiempo que una sesión de comunicación encriptada dura antes de que expire (las épocas hacia fuera).`Loser#`**`show crypto cisco key-timeout`** `Session keys will be re-negotiated every 30 minutes` Utilice estos comandos de determinar la longitud del tiempo 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`
- muestre el Pregen-dh-pairs crypto de Cisco - Cada sesión encriptada utiliza un par único de números DH. Cada vez que se establece una nueva sesión, los nuevos números de par DH deben ser generados. Cuando la sesión completa, se desechan estos números. La generación de los nuevos números de par DH es una actividad Uso intensiva de la CPU, que puede hacer la configuración de la sesión lenta, especialmente para los routeres de menor capacidad.Para acelerar la configuración de la sesión, usted puede elegir tener una determinada cantidad de números de par DH pregenerated y llevados a cabo en la reserva.

Entonces, cuando están configurando a una sesión de comunicación encriptada, un número de par DH se proporciona de esa reserva. Después de que se utilice un número de par DH, la reserva se llena automáticamente con un nuevo número de par DH, de modo que haya siempre un número de par DH de manera operacional.No es generalmente necesario hacer más de uno o dos números de par DH pregenerated, a menos que su router esté configurando a las sesiones encriptadas múltiples tan con frecuencia que una reserva pregenerated de uno o dos números de par DH está agotada demasiado rápidamente.`Loser#`**`show crypto cisco pregen-dh-pairs`** `Number of pregenerated DH pairs: 10`

- **muestre el active crypto de las conexiones de Cisco**Lo que sigue es salida del comando de ejemplo.`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`
- **muestre el paquete perdidos crypto de las conexiones del motor de Cisco**Lo que sigue es salida del comando de ejemplo.`Loser#`**`show crypto engine connections dropped-packet`** `Interface IP-Address Drop Count Serial1 19.19.19.19 39`
- **configuración del show crypto engine** (era el **show crypto engine brief** en el Cisco IOS Software Release 11.2.)Lo que sigue es salida del comando de ejemplo.`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`
- **mypubkey dss del show crypto key**Lo que sigue es salida del comando de ejemplo.`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`
- **pubkey-encadenamiento dss del show crypto key**Lo que sigue es salida del comando de ejemplo.`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`
- **muestre el interface serial 1 de la correspondencia de criptografía**Lo que sigue es salida del comando de ejemplo.`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 del tiempo cuando usted 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 ------------`
- **muestre el interface serial 1 de la correspondencia de criptografía**Lo que sigue es salida del comando de ejemplo.`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**Lo que sigue es salida del comando de ejemplo.`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`

- **sessmgmt del debug crypto**Lo que sigue es salida del comando de ejemplo.`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 peer incorrecto fijó en la correspondencia de criptografía, usted recibe este mensaje de error.`Mar 2 12:19:12.639: CRYPTO-SDU:Far end authentication error: Connection message verify failed`Si los algoritmos de cifrado no hacen juego, usted recibe este mensaje de error.`Mar 2 12:26:51.091: CRYPTO-SDU: Connection failed due to incompatible policy`Si la clave DSS es que falta o inválida, usted recibe este mensaje de error.`Mar 16 13:33:15.703: CRYPTO-SDU:Far end authentication error: Connection message verify failed`
- **clave del debug crypto**Lo que sigue es salida del comando de ejemplo.`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**Lo que sigue es salida del comando de ejemplo.`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#`
- **zeroize crypto**Lo que sigue es salida del comando de ejemplo.`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#`
- **ninguna clave pública crypto**Lo que sigue es salida del comando de ejemplo.`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#`

Resolver problemas el Cisco 7200 con el ESA

Cisco también proporciona una opción de asistencia por hardware de hacer el cifrado en los Cisco 7200 Series Router, que se llama el ESA. El ESA está bajo la forma de adaptador de puerto para

el indicador luminoso LED amarillo de la placa muestra gravedad menor VIP2-40 o un adaptador de puerto independiente para el Cisco 7200. Este arreglo permite el uso de un adaptador de hardware o del motor de software VIP2 de cifrar y de desencriptar los datos que entran en o se van a través de las interfaces en el indicador luminoso LED amarillo de la placa muestra gravedad menor del Cisco 7500 VIP2. El Cisco 7200 permite que la asistencia por hardware cifre el tráfico para cualquier interfaz en el chasis del Cisco 7200. Usando una asistencia de encripción guarda los ciclos de la CPU preciosos que se pueden utilizar para otros fines, por ejemplo la encaminamiento o un de los otras funciones del Cisco IOS.

En un Cisco 7200, el adaptador de puerto independiente se configura exactamente lo mismo que el motor de criptografía del Cisco IOS Software, pero tiene algunos comandos adicionales que se utilicen solamente para el hardware y para decidir a qué motor (software o soporte físico) hará el cifrado.

Primero, prepare al router para la encripción por 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]
```

Habilite o inhabilite la encripción por hardware como se muestra abajo:

```
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.
```

Después, genere las claves para el ESA antes de que usted lo habilite.

```
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#
```

Resolver problemas el VIP2 con ESA

El adaptador del puerto de hardware ESA en el indicador luminoso LED amarillo de la placa muestra gravedad menor VIP2 se utiliza para cifrar y para desencriptar los datos que entran en o se van a través de las interfaces en el indicador luminoso LED amarillo de la placa muestra gravedad menor VIP2. Como con el Cisco 7200, usando una asistencia de encripción guarda los ciclos de la CPU preciosos. En este caso, el **comando crypto esa enable** no existe porque el adaptador de puerto ESA hace el cifrado para los puertos en el indicador luminoso LED amarillo de la placa muestra gravedad menor VIP2 si se enchufa el ESA. **El claro-cierre crypto** necesita ser aplicado a ese slot si el adaptador de puerto ESA acaba de ser instalado por primera vez, o quitó entonces reinstalado.

```
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#
```

Porque el módulo criptográfico ESA fue extraído, usted conseguirá el mensaje de error siguiente

hasta que usted haga un **comando crypto clear-latch** en ese slot, como se muestra abajo.

```
----
*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 usted olvida una contraseña previamente asignada, utilice el **comando crypto zeroize** en vez del **comando crypto clear-latch** de reajustar el ESA. Después de publicar el **comando crypto zeroize**, usted debe regenerar y las claves del re intercambio DSS. Cuando usted regenera las claves DSS, a le indican 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

- Configurando y resolviendo problemas la encripción de capa de red de Cisco: IPSec y ISAKMP - Parte 2
- DES FIP 46-2 en el National Institute of Standards and Technology (NIST)
- DSS FIP 186 en el National Institute of Standards and Technology (NIST)

- Las preguntas frecuentes de los laboratorios RSA sobre la 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