Configurando e pesquisando defeitos a criptografia de camada de rede Cisco: Fundo - Parte 1

Índice

Introdução

Este documento discute como configurar e resolver problemas relacionados à criptografia de camada de rede com o IPsec e o Internet Security Association and Key Management Protocol (ISAKMP) e fornece informações de apoio e a configuração básica do IPsec e o ISAKMP.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nas versões de software e hardware:

- Software Release 11.2 e Mais Recente de Cisco IOS®

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Informações de fundo e configuração da criptografia de camada de rede

A característica da criptografia de camada de rede foi introduzida no Software Release 11.2 de Cisco IOS®. Fornece um mecanismo para a transmissão dos dados seguros e consiste em dois componentes:

- **Autenticação de roteador:** Antes de passar o tráfego criptografado, dois Roteadores executam um único, autenticação em dois sentidos usando chaves públicas do Digital Signature Standard (DSS) para assinar desafios aleatórios.
- **Criptografia de camada de rede:** Para a criptografia da virulência IP, o intercâmbio chave Diffie-Hellman do uso do Roteadores para gerar firmemente uma chave de sessão DES(40- ou 56-bit), DES triplo - 3DES(168-bit), ou o Advanced Encryption Standard mais recente - AES(128-bit(default), ou 192-bit, ou chave do 256-bit), introduzida em 12.2(13)T. As chaves de sessão novas são geradas em uma base configurável. A política de criptografia é ajustada pelos mapas cript. que usam as lista de acesso IP estendido para definir que a rede, a sub-rede, o host, ou os pares do protocolo devem ser cifrada entre o Roteadores.

Background criptográfico

O campo da criptografia é estado relacionado com o mantimento de comunicações privadas. A proteção de comunicações sensíveis foi a ênfase de criptografia durante todo muita de sua história. A criptografia é a transformação dos dados em algum formulário ilegível. Sua finalidade é assegurar a privacidade mantendo a informação hidden de qualquer um para quem não se pretende, mesmo se pode ver os dados criptografados. A descriptografia é o reverso da criptografia: é a transformação dos dados criptografados de novo em um formulário inteligível.

A criptografia e a descriptografia exigem o uso de alguma informação secreta, referido geralmente como uma “chave”. Segundo o mecanismo de criptografia usado, a mesma chave pôde ser usada para a criptografia e a descriptografia; quando para outros mecanismos, as chaves usadas para a criptografia e a descriptografia puderam ser diferentes.

Uma assinatura digital liga um documento ao possuidor de uma chave particular, quando um timestamp digital ligar um documento a sua criação em uma estadia particular. Estes mecanismos criptográficos podem ser usados para controlar o acesso a uma unidade de disco compartilhada, uma instalação da segurança elevada, ou a um canal de televisão do pay-per-view.

Quando a criptografia moderna crescer cada vez mais diversa, a criptografia é baseada fundamentalmente nos problemas que são difíceis de resolver. Um problema pode ser difícil porque sua solução exige conhecer a chave, tal como a descriptografia de um mensagem codificada ou a assinatura de algum documento digital. O problema pode igualmente ser difícil porque é intrinsecamente difícil terminar, como encontrar uma mensagem que produza um valor de hash dado.

Porque o campo da criptografia avançou, as linhas de divisão para o que são e o que não é criptografia tornaram-se borrado. A criptografia hoje pôde ser resumida como o estudo das técnicas e dos aplicativos que dependem da existência de problemas matemáticos que é difícil de resolver. Um cryptanalyst tenta comprometer mecanismos criptográficos, e a criptologia é a disciplina da criptografia e da análise criptológica combinadas.

Definições

Esta seção define os termos relacionados usados durante todo este documento.

- **Autenticação:** A propriedade de saber que os dados recebidos estão enviados realmente pelo remetente reivindicado.
- **Confidencialidade:** A propriedade da comunicação de modo que os receptores intencionados conheçam o que está sendo enviado mas partidos sem intenção não pode determinar o que é enviado.
- **Data Encryption Standard (DES):** O DES utiliza um método da chave simétrica, igualmente conhecido como um método da chave secreta. Isto significa que se um bloco de dados é cifrado com a chave, o bloco cifrado deve ser decifrado com a mesma chave, assim que o encryptor e o decrypter devem usar a mesma chave. Mesmo que o método de criptografia seja sabido e publicado bem, o método do ataque conhecido do melhor publicamente é através da força bruta. As chaves devem ser testadas contra os blocos cifrados para considerar se podem corretamente os resolver. Enquanto os processadores se tornam mais poderosos, o ciclo de vida do DES está aproximando sua extremidade. Por exemplo, um esforço coordenado que usa a potência de processamento de reposição dos milhares de computadores através do Internet pode encontrar a chave 56-bit a um mensagem codificada em DES em 21 dias.O DES é validado cada cinco anos pelo National Security Agency E.U. (NSA) para encontrar as finalidades do governo dos EUA. A aprovação atual expira em 1998 e o NSA indicou que re-não certificarão o DES. Está movendo-se além do DES, outros algoritmos de criptografia que igualmente não têm nenhuma fraquezas conhecida diferentes dos ataques de força bruta. Para a informação adicional, veja DES FIP 46-2 pelo National Institute of Standards and Technology (NIST) .
- **Descriptografia:** O aplicativo reverso de um algoritmo de criptografia aos dados criptografados, restaurando desse modo esses dados a seu estado original, unencrypted.
- **DSS e Digital Signature Algorithm (DSA):** O DSA foi publicado pelo NIST no Digital Signature Standard (DSS), que é parte do projeto do Capstone do governo E.U. O DSS foi selecionado pelo NIST, em colaboração com o NSA, para ser o padrão de autenticação digital do governo E.U. O padrão foi emitido em maio 19, 1994.

- **Criptografia:** O aplicativo de um algoritmo específico aos dados para alterar a aparência dos dados que fazem a incompreensível àquelas que não são autorizadas para ver a informação.
- **Integridade:** A propriedade de assegurar-se de que os dados estejam transmitidos da fonte ao destino sem alteração não detectada.
- **Não-repudiação:** A propriedade de um receptor que pode mostrar que o remetente de alguns dados enviou de fato os dados mesmo que o remetente pudesse mais tarde desejar negar nunca ter enviado esses dados.
- **Criptografia de chave pública:** A Criptografia tradicional é baseada no remetente e no receptor de uma mensagem que conhecem e que usam a mesma chave secreta. O remetente usa a chave secreta para cifrar a mensagem, e o receptor usa a mesma chave secreta para decifrar a mensagem. Este método é sabido como a “chave secreta” ou a “criptografia simétrica.” A questão principal está conseguindo o remetente e o receptor concordar com a chave secreta sem o qualquer um encontrar outro. Se estão em locais físicos separados, devem confiar um correio, ou um sistema de telefone, ou algum outro meio de transmissão para impedir a divulgação da chave secreta que está sendo comunicada. Qualquer um que bisbilhota ou intercepta a chave no trânsito pode mais tarde ler, para alterar, e forjar todas as mensagens cifradas ou autenticadas usando essa chave. A geração, a transmissão, e o armazenamento das chaves são chamados gerenciamento chave; todos os sistemas criptográficos devem tratar as edições de gerenciamento chave. Porque todas as chaves em um sistema criptográfico da chave secreta devem permanecer secretas, a criptografia de chave secreta tem frequentemente a dificuldade que fornece o gerenciamento chave seguro, especialmente nos sistemas abertos um grande número usuários.O conceito da criptografia de chave pública foi introduzido em 1976 por Whitfield Diffie e por Martin Hellman a fim resolver o problema de gerenciamento chave. Em seu conceito, cada pessoa obtém um par de chaves, um chamado a chave pública e o outro chamado a chave privada. A chave pública de cada pessoa é publicada quando a chave privada for mantida secreta. A necessidade para que o remetente e o receptor compartilhe da informação secreta é eliminada e todas as comunicações envolvem somente chaves públicas, e nenhuma chave privada nunca é transmitida ou compartilhada. Já não é necessária confiar o canal de algumas comunicações para ser segura contra bisbilhotar ou traição. A única exigência é que as chaves públicas estão associadas com seus usuários em uma maneira (autenticada) confiada (por exemplo, em um diretório confiado). Qualquer um pode enviar um mensagem confidencial simplesmente usando a informação pública, mas a mensagem pode somente ser decifrada com uma chave privada, que seja em poder exclusivo dos receptores intencionados. Além disso, a criptografia de chave pública pode ser usada não somente para a privacidade (criptografia), mas para a autenticação (assinaturas digital) também.
- **Assinaturas digital da chave pública:** Para assinar uma mensagem, uma pessoa executa uma computação que envolve sua chave privada e a mensagem própria. A saída é chamada a assinatura digital e anexada à mensagem, que é enviada então. Uma segunda pessoa verifica a assinatura executando uma computação que envolve a mensagem, a assinatura legível, e a chave pública da primeira pessoa. Se o resultado realiza corretamente em uma relação matemática simples, a assinatura está verificada como sendo genuína. Se não, a assinatura pode ser fraudulenta ou a mensagem pôde ter sido alterada.
- **Criptografia de chave pública:** Quando uma pessoa deseja enviar um mensagem secreta a uma outra pessoa, a primeira pessoa olha acima a chave pública da segunda pessoa em um diretório, usa-a para cifrar a mensagem e envia-a fora. A segunda pessoa usa então sua chave privada para decifrar a mensagem e para lê-la. Ninguém que escuta dentro pode decifrar a mensagem. Qualquer um pode enviar um mensagem codificada à segunda pessoa

mas somente a segunda pessoa pode lê-lo. Claramente, uma exigência é que ninguém pode figurar para fora a chave privada da chave pública correspondente.
- **Análise de tráfego:** A análise do fluxo de tráfego de rede com a finalidade de deduzir a informação que é útil a um adversário. Os exemplos de tal informação são frequência de transmissão, as identidades dos partidos de conversa, tamanhos dos pacotes, os identificadores do fluxo usados, e assim por diante.

Informações preliminares

Esta seção discute alguns conceitos básicos da criptografia de camada de rede. Contém os aspectos da criptografia que você deve olhar para fora para. Inicialmente, estas edições não podem fazer-lhe o sentido, mas é uma boa ideia lê-las sobre agora e estar ciente delas porque farão mais sentido depois que você trabalhou com criptografia por diversos meses.

- Éimportante notar que a criptografia ocorre somente na saída de uma relação e a descriptografia ocorre somente em cima da entrada à relação. Esta distinção é importante ao aplanar sua política. A política de criptografia e a descriptografia são simétricas. Isto significa que aquela definir um dá lhe ao outro automaticamente. Com os crypto map e suas listas de acesso extendida associadas, somente a política de criptografia é definida explicitamente.A política de descriptografia usa a informação idêntica, mas quando combinar pacotes, ele inverte endereços de rementente e destinatário e portas. Esta maneira, os dados é protegida nos ambos sentidos de uma conexão frente e verso. A indicação do *endereço X do fósforo no* **comando crypto map** é usada para descrever os pacotes que saem de uma relação. Ou seja está descrevendo a criptografia de pacotes. Contudo, os pacotes devem igualmente ser combinados para a descriptografia enquanto incorporam a relação. Isto é feito automaticamente atravessando a lista de acessos com os endereços de rementente e destinatário e as portas invertidos. Isto fornece a simetria para a conexão. A lista de acessos apontada pelo **crypto map** deve descrever o tráfego em um sentido (de partida) somente. Os pacotes IP que não combinam a lista de acessos que você define serão transmitidos mas não cifrados. “Negue” na lista de acessos indica que aqueles anfitriões não devem ser combinados, que significa que não estarão cifrados. “Negue”, neste contexto, não significa que o pacote está deixado cair.
- Seja muito cuidadoso de usar a palavra “” nas listas de acesso extendida. Usar-se “alguma” faz com que seu tráfego seja deixado cair a menos que for dirigida à relação “decriptografia” de harmonização. Além, com o IPsec no Cisco IOS Software Release 11.3(3)T, “algum” não é permitido.
- O uso de “toda a” palavra-chave é desanimado em especificar endereços de origem ou de destino. Especificar “alguns” pode causar problemas com protocolos de roteamento, Network Time Protocol (NTP), eco, resposta do eco, e tráfego multicast, porque o roteador de recepção rejeita silenciosamente este tráfego. Se “algum” deve ser usada, deve ser precedido por “nega” indicações para o tráfego que não deve ser cifrada, como o “NTP”.
- Para ganhar o tempo, certifique-se que você pode **sibilar o** roteador de peer com que você está tentando ter uma associação de criptografia. Também, tenha seu tráfego cifrado) o sibilo dos dispositivos finais (de que depende de obter antes que você passe demasiada hora que pesquisa defeitos o problema errado. Ou seja certifique-se dos trabalhos do roteamento antes de tentar fazer **cripto**. O peer remoto não pode ter uma rota para a interface de saída, neste caso você não pode ter uma sessão de criptografia com esse par (você pode poder usar o **IP unnumbered n**essa interface serial).

- Muitos link de ponto a ponto MACILENTOS usam endereços IP não-roteável, e a criptografia do Cisco IOS Software Release 11.2 confia no Internet Control Message Protocol (ICMP) (significado que usa o endereço IP de Um ou Mais Servidores Cisco ICM NT da interface serial da saída para o ICMP). Isto pode forçá-lo a usar o **IP unnumbered na** interface WAN. Faça sempre um **comando ping and traceroute** certificar-se de que distribuir é no lugar para os dois (criptografia/que decifra) Roteadores espreitando.
- A somente são permitidos dois Roteadores compartilhar de uma chave de sessão de Diffie-Hellman. Isto é, um roteador não pode trocar pacotes criptografado a dois pares que usam a mesma chave de sessão; cada par de Roteadores deve ter uma chave de sessão que seja um resultado de um intercâmbio Diffie-Hellman entre ele.
- A crypto-engine está no Cisco IOS, o Cisco IOS VIP2, ou no hardware o adaptador dos serviços de criptografia (ESA) em um VIP2. Sem um VIP2, a crypto-engine do Cisco IOS governa a política de criptografia em todas as portas. Em Plataformas usando o VIP2, há crypto-engines múltiplas: um no Cisco IOS, e um em cada VIP2. A crypto-engine em um VIP2 governa a criptografia nas portas que residem na placa.
- Certifique-se de que o tráfego está ajustado para chegar em uma relação preparada para a cifrar. Se o tráfego pode de algum modo chegar em uma relação a não ser essa com o **crypto map** aplicado, está deixado cair silenciosamente.
- Ajuda a ter o acesso do console (ou a substituição) a ambo o Roteadores ao fazer trocas de chave; é possível conseguir o lado passivo pendurar ao esperar uma chave.
- **O cfb-64** é mais eficiente a processar do que **cfb-8** em termos da carga de CPU.
- O roteador precisa de executar o algoritmo que você quer usar com o modo do cifra-feedback (CFB) que você quer usar; os padrões para cada imagem são o nome da imagem (tal como "56") com **cfb-64**.
- Consider que muda o chave-intervalo. O padrão 30-minute é muito curto. Tentativa que aumenta o a um dia (1440 minutos).
- O tráfego IP está deixado cair durante a negociação nova chave cada vez que a chave expira.
- Selecione somente o tráfego que você quer realmente cifrar (este salvar ciclos de CPU).
- Com Dial-on-Demand Routing (DDR), faça o ICMP interessante ou nunca discará para fora.
- Se você quer cifrar o tráfego a não ser o IP, use um túnel. Com túneis, aplique os crypto map ao exame e às interfaces de túnel. Veja a amostra 5: Criptografia do tráfego IPX em um túnel IP para mais informação.
- Os dois Roteadores do peer de encripção não precisam de ser conectados diretamente.
- Um roteador de extremidade baixa pode dar-lhe uma mensagem do “CPU hog”. Isto pode ser ignorado porque é dizendo lhe que a criptografia usa muitos recursos do CPU.
- Não coloque roteadores de criptografia redundantemente de modo que você o tráfego decifre e do recriptografar e o desperdício CPU. Cifre simplesmente nos dois valores-limite. Veja a amostra 3: Criptografia e através de um roteador para mais informação.
- Atualmente, a criptografia da transmissão e os pacotes de transmissão múltipla não são apoiados. Se as atualizações de roteamento “seguras” são importantes para um projeto de rede, um protocolo com a autenticação construída dentro deve ser usado, como o Enhanced Interior Gateway Routing Protocol (EIGRP), o Open Shortest Path First (OSPF), ou a versão 2 do protocolo de informação de roteamento protocolo de informação de roteamento (RIPv2) para assegurar a integridade da atualização.

Caveats

Nota: As advertências mencionadas abaixo tudo foram resolvidas.

- Um Cisco 7200 Router que usa um ESA para a criptografia não pode decifrar um pacote sob uns chave de sessão e então recriptografar ele sob uma chave de sessão diferente. Refira a identificação de bug Cisco CSCdj82613 (clientes registrados somente).
- Quando dois Roteadores estão conectados por uma linha alugada cifrada e por uma linha de backup de ISDN, se a linha alugada deixa cair, o enlace de ISDN vem acima da multa. Contudo, quando a linha alugada vem apoio outra vez, o roteador que colocou a chamada ISDN causa um crash. Refira a identificação de bug Cisco CSCdj00310 (clientes registrados somente).
- Para Cisco 7500 Series Router com VIPs múltiplos, se um **crypto map** é aplicado mesmo a uma relação de qualquer VIP, uns ou vários VIP causam um crash. Refira a identificação de bug Cisco CSCdi88459 (clientes registrados somente).
- Para Cisco 7500 Series Router com um VIP2 e um ESA, o **comando show crypto card** não faz saídas de exibição a menos que o usuário estiver na porta de Console. Refira a identificação de bug Cisco CSCdj89070 (clientes registrados somente).

Configuração da criptografia de camada de rede do Cisco IOS

As configurações do IOS da Cisco do exemplo em funcionamento neste documento vieram diretamente dos roteadores de laboratório. A única alteração feita a elas era a remoção das configurações de interface não relacionada. Todo o material aqui veio livremente dos recursos disponíveis no Internet ou na seção Informação Relacionada na extremidade deste documento.

Todas as configurações de amostra neste documento são do Cisco IOS Software Release 11.3. Havia diversas mudanças dos comandos do Cisco IOS Software Release 11.2, tais como a adição das seguintes palavras:

- dss em alguns dos comandos configuration chaves.
- Cisco em alguns dos **comandos show** e dos **comandos crypto map** distinguir entre a criptografia proprietária de Cisco (como estabelecido no Cisco IOS Software Release 11.2 e Mais Recente) e o IPsec que está no Cisco IOS Software Release 11.3(2)T.

Nota: Os endereços IP de Um ou Mais Servidores Cisco ICM NT usados nestes exemplos de configuração foram escolhidos aleatoriamente no laboratório de Cisco e são pretendidos ser completamente genéricos.

Passo 1: Gerencia manualmente pares de chaves DSS

Um par de chaves DSS (uma chave pública e privada) precisa de ser gerado manualmente em cada roteador que participa na sessão de criptografia. Ou seja cada roteador deve ter suas próprias chaves DSS a fim participar. Um Engine de codificação pode ter somente um DSS chave que o identifica excepcionalmente. A palavra-chave “dss” foi adicionada no Cisco IOS Software Release 11.3 a fim distinguir o DSS das chaves RSA. Você pode especificar todo o nome para chaves DSS do roteador próprias (embora, se recomenda usar o nome de host do roteador). Em menos CPU potente (tal como o Cisco 2500 Series), a geração de par chave toma sobre os segundos 5 ou o menos.

O roteador gerencie um par de chaves:

- Uma chave pública (que é enviada mais tarde ao Roteadores que participa nas sessões de criptografia).
- Uma chave privada (que não é considerada nem é trocada com o qualquer um outro; de fato, é armazenada em uma seção separada do NVRAM que não possa ser vista).

Uma vez que o par de chaves DSS do roteador foi gerado, está associada excepcionalmente com a crypto-engine nesse roteador. A geração de par chave é mostrada no exemplo de saída de comando abaixo.

```
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 você pode gerar somente um par de chaves que identifica o roteador, você pode overwrite sua chave original e precisá-la de enviar novamente sua chave pública com cada roteador na associação de criptografia. Isto é mostrado no exemplo de saída de comando abaixo:

```
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.
```

Passo 2: Troca manual de chaves públicas DSS com correspondentes (fora de banda)

Gerar par de chaves DSS do roteador próprio é a primeira etapa em instituir uma associação de sessão de criptografia. A próxima etapa é trocar chaves públicas com cada outro roteador. Você pode incorporar estas chaves públicas manualmente primeiramente inscrevendo o **comando show crypto mypubkey** indicar a chave pública DSS do roteador. Você então troca estas chaves públicas (através do email, por exemplo) e, com o **comando crypto key pubkey-chain dss**, cortara-col a chave pública do seu roteador de peer no roteador.

Você pode igualmente usar o **comando crypto key exchange dss** ter as chaves públicas da troca do Roteadores automaticamente. Se você usa o método automático, certifique-se que não há nenhuma **instrução de mapa de criptografia nas** relações usadas para as trocas de chave. **Uma chave do debug crypto** é útil aqui.

Nota: É uma boa ideia **sibilar** seu par antes de tentar trocar chaves.

```
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#
```

Agora que as chaves públicas DSS foram trocadas, certifique-se de que ambo o Roteadores tem chaves públicas de cada um e de que combina, segundo as indicações do comando output abaixo.

```
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
```

Exemplo 1: Configuração do IOS da Cisco para o link dedicado

Depois que as chaves DSS estiveram geradas em cada roteador e as chaves públicas DSS estiveram trocadas, o **comando crypto map** pode ser aplicado à relação. A sessão de criptografia começa gerando o tráfego que combina a lista de acessos usada pelos crypto map.

```
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#
```

Amostra 2: Configuração do IOS da Cisco para o Frame Relay multiponto

O seguinte exemplo de saída de comando foi tomado do roteador de 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#
```

O seguinte exemplo de saída de comando foi tomado do local 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#
```

O seguinte exemplo de saída de comando foi tomado do local 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#
```

O seguinte exemplo de saída de comando foi tomado do Frame Relay Switch.

```
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
!
```

Amostra 3: Criptografia para e por meio de um roteador

Os roteadores de peer não têm que ser um salto afastado. Você pode criar uma sessão de peer com um roteador remoto. No exemplo seguinte, o objetivo é cifrar todo o tráfego de rede entre 180.180.180.0/24 e 40.40.40.0/24 e entre 180.180.180.0/24 e 30.30.30.0/24. Não há nenhum estar relacionado com tráfego de criptografia entre 40.40.40.0/24 e 30.30.30.0/24.

O roteador wan-4500b tem uma associação de sessão de criptografia com vencido e igualmente com StHelen. Cifrando o tráfego do segmento de Ethernet wan-4500b ao segmento de Ethernet do StHelen's, você evita a etapa desnecessária da descriptografia no vencido. O vencido passa simplesmente o tráfego criptografado sobre à interface serial do StHelen's, onde é decifrada. Isto reduz o retardo de tráfego para os pacotes IP e os ciclos de CPU no roteador Loser. Mais importante, aumenta extremamente a Segurança do sistema, desde que um eavesdropper no vencido não pode ler o tráfego. Se o vencido decifrava o tráfego, haveria uma possibilidade que os dados decifrados poderiam 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#
```

Amostra 4: Criptografia com DDR

Porque o Cisco IOS confia no ICMP para estabelecer sessões de criptografia, o tráfego ICMP deve ser classificado como “interessante” na lista de discadores ao fazer a criptografia sobre um link DDR.

Nota: A compressão trabalha no Cisco IOS Software Release 11.3, mas não é muito útil para dados criptografados. Porque os dados criptografados aleatório-estão olhando razoavelmente, a compressão retarda somente coisas para baixo. Mas você pode deixar a característica sobre para o tráfego não codificado.

Em algumas situações, você quererá o Dial backup ao mesmo roteador. Por exemplo, é útil quando os usuários querem proteger contra a falha de um enlace particular em suas redes de WAN. Se duas relações vão ao mesmo par, o mesmo crypto map pode ser usado em ambas as relações. A Interface de backup deve ser usada para que esta característica funcione corretamente. Se um projeto alternativo tem um seletor do roteador em uma caixa diferente, os crypto map diferentes devem ser criados e os pares ser ajustados em conformidade. Além disso, o **comando backup interface** deve ser usado.

```
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#
```

Amostra 5: Criptografia de tráfego IPX em um túnel IP

Neste exemplo, o tráfego IPX em um túnel IP é cifrado.

Nota: Somente o tráfego neste túnel (IPX) é cifrado. Todo tráfego IP restante é deixado sozinho.

```
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#
```

Amostra 6: Criptografando túneis L2F

Neste exemplo, somente o tráfego de criptografia L2F para os usuários que discam dentro é tentado. Aqui, “user@cisco.com” chama o servidor de acesso da rede local (NAS) nomeou "DEMO2" em sua cidade e obtém-no em túnel ao CD do Home Gateway. Todo o tráfego DEMO2

(junto com isso de outros chamadores L2F) é cifrado. Porque o L2F usa a porta 1701 UDP, este é como a lista de acessos é construída, determinando que tráfego é cifrado.

Nota: Se a associação de criptografia já não se estabelece, significar o chamador é a primeira pessoa a chamar dentro e para criar o túnel L2F, o chamador pode obter deixado cair devido ao atraso em estabelecer a associação de criptografia. Isto não pode acontecer no Roteadores com bastante potência de CPU. Também, você pode querer aumentar o **keytimeout** de modo que a criptografia setup e o rasgo-para baixo ocorra somente durante horas fora de pico.

O seguinte exemplo de saída de comando foi tomado do 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#
```

O seguinte exemplo de saída de comando foi tomado do Home Gateway.

```
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
```

Troubleshooting

Égeralmente o melhor começar cada sessão de Troubleshooting recolhendo a informação usando os seguintes **comandos show**. Um asterisco (*) indica especialmente um comando útil. Por favor igualmente veja o Troubleshooting de Segurança IP - Compreendendo e usando comandos debug para a informação adicional.

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

Nota: Antes de emitir **comandos debug**, consulte Informações importantes sobre comandos debug.

Comandos	
mostre algoritmos criptos de Cisco	mostre o chave-intervalo cripto de Cisco
mostre o Pregen-dh-pairs cripto de Cisco	cryptos engine connection do *show ativos
pacote descartado do show crypto engine connections	configuração do show crypto engine
mypubkey dss do show crypto key	pubkey-corrente dss da chave de criptografia do *show
mostre o interface serial 1 do crypto map	crypto map do *show
debug crypto engine	* sess do debug crypto
debugar a chave do grito	clear crypto connection
zeroize cripto	nenhuma chave pública cripto

- **mostre algoritmos criptos de Cisco**- Você deve permitir todos os algoritmos do Data Encryption Standard (DES) que são usados para se comunicar com todo o outro roteador peer encrypting. Se você não permite um algoritmo de DES, você não poderá usar esse algoritmo, mesmo se você tenta atribuir mais tarde o algoritmo a um **crypto map**.Se seu roteador tenta estabelecer uma sessão de comunicação criptografada com um roteador de peer, e os dois Roteadores não têm o mesmo algoritmo de DES permitido no ambas as extremidades, a sessão de criptografia falha. Se pelo menos um algoritmo DES comum é permitido no ambas as extremidades, a sessão de criptografia pode continuar.**Nota:** A palavra extra Cisco aparece no Cisco IOS Software Release 11.3 e é precisada de distinguir entre o IPsec e a criptografia proprietária de Cisco encontrou no 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`
- **mostre o chave-intervalo cripto de Cisco** - Depois que uma sessão de comunicação criptografada é estabelecida, é válido para um intervalo de tempo específico. Após este intervalo de tempo, o tempo de sessão para fora. Uma sessão nova deve ser negociada, e uma chave nova DES (sessão) deve ser gerada para que uma comunicação codificada continue. Use este comando mudar o tempo que uma sessão de comunicação criptografada dura antes que expire (épocas para fora).`Loser#`**`show crypto cisco key-timeout`** `Session keys will be re-negotiated every 30 minutes` Use estes comandos determinar o intervalo de tempo antes que as chaves DES estejam renegociadas.`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`
- **mostre o Pregen-dh-pairs cripto de Cisco** - Cada sessão de criptografia usa um par original de números DH. Cada vez que uma sessão nova é estabelecida, os números par novos DH devem ser gerados. Quando a sessão termina, estes números estão rejeitados. Gerar números par novos DH é uma atividade do processo intensivo de cpu, que possa fazer a configuração de sessão lenta, especialmente para roteadores de extremidade baixa.Para acelerar a configuração de sessão, você pode escolher ter uma quantidade especificada de números par DH pregenerated e realizados na reserva. Então, quando uma sessão de comunicação criptografada se está estabelecendo, um número par DH é fornecido dessa reserva. Depois que um número par DH é usado, a reserva está reabastecida

automaticamente com um número par novo DH, de modo que haja sempre um número par DH de modo operacional.Não é geralmente necessário ter mais de um ou dois números par DH pregenerated, a menos que seu roteador estiver estabelecendo sessões de criptografia múltiplas tão frequentemente que uma reserva pregenerated de um ou dois números par DH está esgotada demasiado rapidamente.`Loser#`**`show crypto cisco pregen-dh-pairs`** `Number of pregenerated DH pairs: 10`

- **mostre o active cripto das conexões de Cisco**O seguinte é exemplo de saída de 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`
- **mostre o pacote descartado cripto das conexões de Engine de Cisco**O seguinte é exemplo de saída de comando.`Loser#`**`show crypto engine connections dropped-packet`** `Interface IP-Address Drop Count Serial1 19.19.19.19 39`
- **configuração do show crypto engine** (era o **show crypto engine brief no** Cisco IOS Software Release 11.2.)O seguinte é exemplo de saída de 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`
- **mypubkey dss do show crypto key**O seguinte é exemplo de saída de 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`
- **pubkey-corrente dss do show crypto key**O seguinte é exemplo de saída de 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`
- **mostre o interface serial 1 do crypto map**O seguinte é exemplo de saída de 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` Note a disparidade do tempo quando você usa o **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 ----------`
- **mostre o interface serial 1 do crypto map**O seguinte é exemplo de saída de 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**O seguinte é exemplo de saída de 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`
- **sessmgmt do debug crypto**O seguinte é exemplo de saída de 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 ----------> ~~ Se o peer errado se ajustou no crypto map, você recebe este Mensagem de Erro.`Mar 2 12:19:12.639: CRYPTO-SDU:Far end authentication error: Connection message verify failed`Se os algoritmos de criptografia não combinam, você recebe este Mensagem de Erro.`Mar 2 12:26:51.091: CRYPTO-SDU: Connection failed due to incompatible policy`Se a chave DSS é faltante ou inválida, você recebe este Mensagem de Erro.`Mar 16 13:33:15.703: CRYPTO-SDU:Far end authentication error: Connection message verify failed`

- **chave do debug crypto**O seguinte é exemplo de saída de 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**O seguinte é exemplo de saída de 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#
- **zeroize cripto**O seguinte é exemplo de saída de 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#
- **nenhuma chave pública cripto**O seguinte é exemplo de saída de 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#

Pesquisando defeitos o Cisco 7200 com ESA

Cisco igualmente fornece uma opção de assistência de hardware fazer a criptografia nos Cisco 7200 Series Router, que é chamada o ESA. O ESA é sob a forma de um adaptador de porta para o cartão VIP2-40 ou de um adaptador de porta independente para o Cisco 7200. Este arranjo permite o uso de um adaptador de hardware ou do Engine de Software VIP2 cifrar e decifrar os dados que entram ou saem através das relações no cartão do Cisco 7500 VIP2. O Cisco 7200 permite que a assistência de hardware cifre o tráfego para todas as relações no chassi do Cisco 7200. Usar uma ajuda de criptografia salvar os ciclos de CPU preciosos que podem ser usados

para outros fins, como o roteamento ou o algum das outras funções do Cisco IOS.

Em um Cisco 7200, o adaptador de porta independente é configurado exatamente o mesmos que a crypto-engine do Cisco IOS Software, mas tem alguns comandos extra que são usados somente para o hardware e decidindo que motor (software ou hardware) fará a criptografia.

Primeiramente, prepare o roteador para a criptografia 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]
```

Permita ou desabilite a criptografia de hardware como mostrado abaixo:

```
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.
```

Em seguida, gerencia chaves para o ESA antes que você o permita.

```
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#
```

Pesquisando defeitos o VIP2 com ESA

O adaptador da porta de hardware ESA no cartão VIP2 é usado para cifrar e decifrar os dados que entram ou saem através das relações no cartão VIP2. Como com o Cisco 7200, usar uma ajuda de criptografia salvar ciclos de CPU preciosos. Neste caso, o **comando crypto esa enable** não existe porque o adaptador de porta ESA faz a criptografia para as portas no cartão VIP2 se o ESA é obstruído dentro. **A claro-trava cripto** precisa de ser aplicada a esse entalhe se o adaptador de porta ESA foi instalado apenas pela primeira vez, ou removeu reinstalado então.

```
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 o módulo de criptografia ESA foi extraído, você receberá o seguinte Mensagem de Erro até que você faça um **comando crypto clear-latch n**esse entalhe, como mostrado abaixo.

```
----
*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
```

Se você esquece uma senha previamente atribuída, use o **comando crypto zeroize** em vez do **comando crypto clear-latch** restaurar o ESA. Após ter emitido o **comando crypto zeroize**, você deve regenerar e chaves da re-troca DSS. Quando você regenera chaves DSS, você está alertado criar uma senha nova. Um exemplo é mostrado abaixo.

```
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#
```

Informações Relacionadas

- Configurando e pesquisando defeitos a criptografia de camada de rede Cisco: IPsec e ISAKMP - Parte 2
- DES FIP 46-2 no National Institute of Standards and Technology (NIST)
- DSS FIP 186 no National Institute of Standards and Technology (NIST)
- As perguntas mais frequentes dos laboratórios RSA sobre a criptografia de hoje
- Padrões de segurança IETF
- Configurando o protocolo de segurança do intercâmbio chave de Internet
- Configurando a segurança da rede IPSec
- Página de suporte do IPSec
- Suporte Técnico - Cisco Systems