Configuração e Troubleshooting da Cisco Network-Layer Encryption: Histórico - Parte 1

Contents

Introduction

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.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Software Cisco IOS® versão 11.2 e posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

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

Informações e configuração do plano de fundo da criptografia da camada de rede

O recurso de criptografia de camada de rede foi introduzido no Cisco IOS® Software Release 11.2. Ele fornece um mecanismo para a transmissão segura de dados e consiste em dois componentes:

- **Autenticação do roteador:** Antes de transmitir tráfego criptografado, dois roteadores executam uma autenticação unidirecional usando chaves públicas DSS (Digital Signature Standard, padrão de assinatura digital) para assinar desafios aleatórios.
- **Criptografia da camada de rede:** Para a criptografia de payload IP, os roteadores usam a troca de chave Diffie-Hellman para gerar com segurança uma chave de sessão DES (40 ou 56 bits), Triple DES - 3DES (168 bits) ou a chave de criptografia avançada mais recente - AES(128 bits(padrão) ou 192 bits ou 256 bits), introduzido no ponto 13 do artigo 12.2.T. Novas chaves de sessão são geradas em uma base configurável. A política de criptografia é definida por mapas de criptografia que usam listas de acesso IP estendidas para definir quais pares de rede, sub-rede, host ou protocolo devem ser criptografados entre roteadores.

Histórico de criptografia

O campo da criptografia tem a ver com manter as comunicações privadas. A proteção das comunicações sensíveis tem sido a ênfase da criptografia ao longo de grande parte de sua história. A criptografia é a transformação de dados em uma forma ilegível. Seu objetivo é garantir a privacidade, mantendo as informações escondidas de qualquer pessoa para quem elas não se destinam, mesmo que possam ver os dados criptografados. A descriptografia é o inverso da criptografia: é a transformação de dados criptografados de volta em uma forma inteligível.

A criptografia e a descriptografia exigem o uso de algumas informações secretas, geralmente chamadas de "chave". Dependendo do mecanismo de criptografia usado, a mesma chave pode ser usada para criptografia e descriptografia; enquanto para outros mecanismos, as chaves usadas para criptografia e descriptografia podem ser diferentes.

Uma assinatura digital vincula um documento ao possuidor de uma chave específica, enquanto um timestamp digital vincula um documento à sua criação em um momento específico. Esses mecanismos de criptografia podem ser usados para controlar o acesso a uma unidade de disco

compartilhada, a uma instalação de alta segurança ou a um canal de televisão por exibição.

Embora a criptografia moderna esteja cada vez mais diversificada, a criptografia é fundamentalmente baseada em problemas que são difíceis de resolver. Um problema pode ser difícil porque sua solução exige saber a chave, como descriptografar uma mensagem criptografada ou assinar algum documento digital. O problema também pode ser difícil porque é intrinsecamente difícil de ser concluído, como encontrar uma mensagem que produza um determinado valor de hash.

Àmedida que o campo da criptografia avançou, as linhas divisórias do que é e do que não é criptografia se tornaram embaralhadas. A criptografia hoje pode ser resumida como o estudo de técnicas e aplicações que dependem da existência de problemas matemáticos difíceis de resolver. Um analista de criptografia tenta comprometer mecanismos criptográficos, e a criptografia é a disciplina de criptografia e análise de criptografia combinadas.

Definições

Esta seção define os termos relacionados usados neste documento.

- **Autenticação:** A propriedade de saber que os dados recebidos são realmente enviados pelo remetente reivindicado.
- **Confidencialidade:** A propriedade de comunicar para que os destinatários desejados saibam o que está sendo enviado, mas as partes não desejadas não podem determinar o que está sendo enviado.
- **Padrão de criptografia de dados (DES):** O DES utiliza um método de chave simétrica, também conhecido como método de chave secreta. Isso significa que, se um bloco de dados for criptografado com a chave, o bloco criptografado deverá ser descriptografado com a mesma chave, de modo que tanto o criptografador quanto o descriptografador devem usar a mesma chave. Embora o método de criptografia seja conhecido e bem publicado, o melhor método de ataque publicamente conhecido é através da força bruta. As chaves devem ser testadas em relação aos blocos criptografados para ver se podem resolvê-las corretamente. À medida que os processadores se tornam mais poderosos, a vida natural do DES está se aproximando do fim. Por exemplo, um esforço coordenado usando poder de processamento sobressalente de milhares de computadores na Internet é capaz de encontrar a chave de 56 bits para uma mensagem codificada por DES em 21 dias.O DES é validado de cinco em cinco anos pela Agência de Segurança Nacional dos EUA (NSA) para cumprir os objetivos do governo dos EUA. A atual aprovação expira em 1998 e a NSA indicou que não irá renovar a certificação DES. Além do DES, há outros algoritmos de criptografia que também não têm nenhum ponto fraco conhecido além dos ataques de força bruta. Para mais informações, ver DES FIPS 46-2 do National Institute of Standards and Technology (NIST) .
- **Descriptografia:** A aplicação reversa de um algoritmo de criptografia para dados criptografados, restaurando, assim, esses dados em seu estado original e não criptografado.
- **DSS e DSA (Digital Signature Algorithm Algoritmo de Assinatura Digital):** O DSA foi publicado pelo NIST no Digital Signature Standard (DSS), que faz parte do projeto Capstone do governo dos EUA. O DSS foi selecionado pela NIST, em cooperação com a NSA, para ser o padrão de autenticação digital do governo dos EUA. O padrão foi emitido em 19 de maio de 1994.
- **Criptografia:** A aplicação de um algoritmo específico aos dados de forma a alterar a aparência dos dados tornando-os incompreensíveis para quem não está autorizado a ver as

informações.

- **Integridade:** A propriedade de assegurar que os dados sejam transmitidos da origem para o destino sem alteração não detectada.
- **Não-repúdio:** A propriedade de um receptor ser capaz de provar que o remetente de alguns dados realmente enviou os dados, mesmo que o remetente possa posteriormente desejar negar ter enviado esses dados.
- **Criptografia de chave pública:** A criptografia tradicional baseia-se no remetente e no receptor de uma mensagem que sabe e usa a mesma chave secreta. O remetente usa a chave secreta para criptografar a mensagem e o receptor usa a mesma chave secreta para descriptografá-la. Esse método é conhecido como "chave secreta" ou "criptografia simétrica". A questão principal é fazer com que o remetente e o receptor concordem com a chave secreta sem que ninguém mais descubra. Se estiverem em locais físicos separados, eles devem confiar em um correio, ou um sistema telefônico, ou em algum outro meio de transmissão para evitar que a divulgação da chave secreta seja comunicada. Qualquer pessoa que ouça ou intercepte a chave em trânsito pode posteriormente ler, modificar e forjar todas as mensagens criptografadas ou autenticadas usando essa chave. A geração, transmissão e armazenamento de chaves é chamada de gerenciamento principal; todos os sistemas criptografados devem lidar com problemas importantes de gerenciamento. Como todas as chaves em um sistema de criptografia de chave secreta devem permanecer secretas, a criptografia de chave secreta frequentemente tem dificuldade em fornecer gerenciamento de chave seguro, especialmente em sistemas abertos com um grande número de usuários.O conceito de criptografia de chave pública foi introduzido em 1976 por Whitfield Diffie e Martin Hellman para resolver o principal problema de gerenciamento. No seu conceito, cada pessoa recebe um par de chaves, uma chamada chave pública e outra chamada chave privada. A chave pública de cada pessoa é publicada enquanto a chave privada é mantida em segredo. A necessidade de o emissor e o receptor compartilharem informações secretas é eliminada e todas as comunicações envolvem apenas chaves públicas, e nenhuma chave privada é transmitida ou compartilhada. Não é mais necessário confiar em algum canal de comunicação para se proteger contra escutas ou traições. O único requisito é que as chaves públicas sejam associadas a seus usuários de maneira confiável (autenticada) (por exemplo, em um diretório confiável). Qualquer pessoa pode enviar uma mensagem confidencial simplesmente usando informações públicas, mas a mensagem só pode ser descriptografada com uma chave privada, que está na posse exclusiva do destinatário desejado. Além disso, a criptografia de chave pública pode ser usada não apenas para privacidade (criptografia), mas também para autenticação (assinaturas digitais).
- **Assinaturas digitais de chave pública:** Para assinar uma mensagem, uma pessoa realiza uma computação envolvendo sua chave privada e a própria mensagem. A saída é chamada de assinatura digital e é anexada à mensagem, que é enviada em seguida. Uma segunda pessoa verifica a assinatura executando um cálculo envolvendo a mensagem, a assinatura pretendida e a chave pública da primeira pessoa. Se o resultado se mantiver adequadamente numa relação matemática simples, a assinatura é verificada como sendo genuína. Caso contrário, a assinatura pode ser fraudulenta ou a mensagem pode ter sido alterada.
- **Criptografia de chave pública:** Quando uma pessoa deseja enviar uma mensagem secreta para outra pessoa, a primeira pessoa procura a chave pública da segunda em um diretório, a usa para criptografar a mensagem e a envia. A segunda pessoa, então, usa sua chave privada para descriptografar a mensagem e lê-la. Ninguém ouvindo pode descriptografar a mensagem. Qualquer pessoa pode enviar uma mensagem criptografada para a segunda pessoa, mas apenas a segunda pessoa pode lê-la. Claramente, um requisito é que ninguém

pode descobrir a chave privada a partir da chave pública correspondente.
- **Análise de tráfego:** A análise do fluxo de tráfego de rede com o objetivo de deduzir informações úteis para um adversário. Exemplos dessas informações são a frequência de transmissão, as identidades das partes de conversação, os tamanhos dos pacotes, os Identificadores de fluxo usados, etc.

Informações preliminares

Esta seção discute alguns conceitos básicos de Criptografia de Camada de Rede. Ele contém os aspectos da criptografia que você deve procurar. Inicialmente, essas questões podem não fazer sentido para você, mas é uma boa ideia lê-las agora e estar ciente delas porque elas farão mais sentido depois que você tiver trabalhado com criptografia por vários meses.

- Éimportante observar que a criptografia ocorre somente na saída de uma interface e a descriptografia ocorre somente na entrada da interface. Essa distinção é importante ao planejar sua política. A política de criptografia e descriptografia é simétrica. Isso significa que definir um lhe dá o outro automaticamente. Com os mapas de criptografia e suas listas de acesso estendidas associadas, somente a política de criptografia é explicitamente definida.A política de descriptografia usa as informações idênticas, mas ao combinar pacotes, inverte os endereços de origem e destino e as portas. Dessa forma, os dados são protegidos em ambas as direções de uma conexão duplex. A instrução *match address x* no comando **crypto map** é usada para descrever pacotes que saem de uma interface. Em outras palavras, está descrevendo a criptografia de pacotes. No entanto, os pacotes também devem ser correspondidos para descriptografia à medida que entram na interface. Isso é feito automaticamente ao atravessar a lista de acesso com os endereços de origem e destino e as portas invertidas. Isso fornece simetria para a conexão. A lista de acesso apontada pelo **mapa de criptografia** deve descrever o tráfego somente em uma direção (de saída). Os pacotes IP que não correspondem à lista de acesso que você define serão transmitidos, mas não criptografados. Uma "negação" na lista de acesso indica que esses hosts não devem ser correspondidos, o que significa que eles não serão criptografados. O "deny", nesse contexto, não significa que o pacote seja descartado.
- Tenha muito cuidado ao usar a palavra "any" nas listas de acesso estendidas. O uso de "any" faz com que o tráfego seja descartado, a menos que seja direcionado para a interface correspondente de "não criptografia". Além disso, com o IPSec no Cisco IOS Software Release 11.3(3)T, "any" não é permitido.
- O uso da palavra-chave "any" é desencorajado na especificação de endereços de origem ou de destino. Especificar "any" pode causar problemas com protocolos de roteamento, Network Time Protocol (NTP), eco, resposta de eco e tráfego multicast, já que o roteador receptor descarta silenciosamente esse tráfego. Se "any" for usado, ele deve ser precedido por instruções "deny" para o tráfego que não deve ser criptografado, como "ntp".
- Para economizar tempo, certifique-se de que você pode **fazer ping** no roteador peer com o qual você está tentando ter uma associação de criptografia. Além disso, faça com que os dispositivos finais (que dependem de ter o tráfego criptografado) façam ping entre si antes de você gastar muito tempo solucionando o problema errado. Em outras palavras, certifique-se de que o roteamento funcione antes de tentar fazer a **criptografia**. O peer remoto pode não ter uma rota para a interface de saída, caso em que você não pode ter uma sessão de criptografia com esse peer (você pode ser capaz de usar **ip não numerado** nessa interface serial).

- Muitos links ponto-a-ponto da WAN usam endereços IP não roteáveis e a criptografia do Cisco IOS Software Release 11.2 depende do Internet Control Message Protocol (ICMP) (o que significa que ele usa o endereço IP da interface serial de saída para ICMP). Isso pode forçá-lo a usar **ip unnumbered** na interface WAN. Sempre execute um **comando ping** e **traceroute** para garantir que o roteamento esteja estabelecido para os dois roteadores de peering (criptografia/descriptografia).
- Apenas dois roteadores têm permissão para compartilhar uma chave de sessão Diffie-Hellman. Ou seja, um roteador não pode trocar pacotes criptografados para dois peers usando a mesma chave de sessão; cada par de roteadores deve ter uma chave de sessão que seja resultado de uma troca Diffie-Hellman entre eles.
- O mecanismo de criptografia está no Cisco IOS, no VIP2 Cisco IOS ou no hardware, no Encryption Services Adapter (ESA) em um VIP2. Sem um VIP2, o mecanismo de criptografia do Cisco IOS rege a política de criptografia em todas as portas. Em plataformas que usam o VIP2, há vários mecanismos de criptografia: um no Cisco IOS e um em cada VIP2. O mecanismo de criptografia em um VIP2 rege a criptografia nas portas que residem na placa.
- Verifique se o tráfego está definido para chegar a uma interface preparada para criptografá-lo. Se o tráfego puder de alguma forma chegar em uma interface diferente daquela com **mapa de criptografia** aplicado, ele será descartado silenciosamente.
- Ele ajuda a ter acesso de console (ou alternativo) a ambos os roteadores ao fazer a troca de chaves; é possível fazer com que o lado passivo fique suspenso enquanto espera por uma chave.
- O **cfb-64** é mais eficiente no processamento do que o **cfb-8** em termos de carga da CPU.
- O roteador precisa estar executando o algoritmo que você deseja usar com o modo de feedback de cifra (CFB) que você deseja usar; os padrões para cada imagem são o nome da imagem (como "56") com **cfb-64**.
- Considere alterar o tempo limite da chave. O padrão de 30 minutos é muito curto. Tente aumentar para um dia (1440 minutos).
- O tráfego IP é descartado durante a renegociação de chave toda vez que a chave expira.
- Selecione apenas o tráfego que você realmente deseja criptografar (isso salva os ciclos da CPU).
- Com o DDR (dial-on-demand routing, roteamento de discagem sob demanda), torne o ICMP interessante ou ele nunca discará.
- Se quiser criptografar outro tráfego que não seja IP, use um túnel. Com túneis, aplique os mapas de criptografia às interfaces física e de túnel. Veja o exemplo 5: Criptografia do tráfego IPX em um túnel IP para obter mais informações.
- Os dois roteadores de peer de criptografia não precisam estar diretamente conectados.
- Um roteador low-end pode lhe dar uma mensagem de "CPU hog". Isso pode ser ignorado porque está dizendo que a criptografia usa muitos recursos da CPU.
- Não coloque roteadores de criptografia de forma redundante para que você descriptografe e criptografe novamente o tráfego e desperdice a CPU. Simplesmente criptografe nos dois endpoints. Ver exemplo 3: Criptografia para e através de um roteador para obter mais informações.
- Atualmente, não há suporte para criptografia de pacotes de broadcast e multicast. Se atualizações de roteamento "seguras" forem importantes para um projeto de rede, deve ser usado um protocolo com autenticação integrada, como Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) ou Routing Information Protocol Version 2 (RIPv2) para garantir a integridade da atualização.

Caveats

Observação: as advertências mencionadas abaixo foram todas resolvidas.

- Um roteador Cisco 7200 usando um ESA para criptografia não pode descriptografar um pacote sob uma chave de sessão e depois criptografá-lo novamente sob uma chave de sessão diferente. Consulte o bug da Cisco ID CSCdj82613 (somente clientes registrados) .
- Quando dois roteadores são conectados por uma linha alugada criptografada e uma linha de backup ISDN, se a linha alugada cair, o link ISDN é ativado corretamente. No entanto, quando a linha alugada volta a funcionar, o roteador que fez a chamada ISDN trava. Consulte o bug da Cisco ID CSCdj00310 (somente clientes registrados) .
- Para os roteadores da série Cisco 7500 com vários VIPs, se um **mapa de criptografia** for aplicado até mesmo a uma interface de qualquer VIP, um ou mais VIPs falharão. Consulte o bug da Cisco ID CSCdi88459 (somente clientes registrados) .
- Para os roteadores da série Cisco 7500 com VIP2 e ESA, o comando **show crypto card** não exibe a saída, a menos que o usuário esteja na porta do console. Consulte o bug da Cisco ID CSCdj89070 (somente clientes registrados) .

Configuração de criptografia da camada de rede do Cisco IOS

O exemplo de funcionamento das configurações do Cisco IOS neste documento veio diretamente dos roteadores do laboratório. A única alteração feita a eles foi a remoção de configurações de interface não relacionadas. Todo o material aqui veio de recursos livremente disponíveis na Internet ou na seção Informações Relacionadas no final deste documento.

Todas as configurações de exemplo neste documento são do Cisco IOS Software Release 11.3. Houve várias alterações nos comandos do Cisco IOS Software Release 11.2, como a adição das seguintes palavras:

- dss em alguns dos principais comandos de configuração.
- cisco em alguns dos comandos **show** e **crypto map** para distinguir entre a criptografia proprietária da Cisco (como encontrada no Cisco IOS Software Release 11.2 e posteriores) e IPSec que está no Cisco IOS Software Release 11.3(2)T.

Observação: os endereços IP usados nesses exemplos de configuração foram escolhidos aleatoriamente no laboratório da Cisco e se destinam a ser completamente genéricos.

Passo 1: Gerar manualmente pares de chaves DSS

Um par de chaves DSS (uma chave pública e privada) precisa ser gerado manualmente em cada roteador que participa da sessão de criptografia. Em outras palavras, cada roteador deve ter suas próprias chaves DSS para participar. Um mecanismo de criptografia pode ter apenas uma chave DSS que o identifica exclusivamente. A palavra-chave "dss" foi adicionada no Cisco IOS Software Release 11.3 para distinguir o DSS das chaves RSA. Você pode especificar qualquer nome para as próprias chaves DSS do roteador (embora, é recomendável usar o nome de host do roteador). Em uma CPU menos potente (como a série Cisco 2500), a geração de pares de chaves leva cerca de 5 segundos ou menos.

O roteador gera um par de chaves:

- Uma chave pública (que é enviada posteriormente aos roteadores que participam de sessões de criptografia).
- Uma chave privada (que não é vista nem trocada com qualquer outra pessoa; na verdade, ele é armazenado em uma seção separada da NVRAM que não pode ser vista).

Depois que o par de chaves DSS do roteador for gerado, ele será exclusivamente associado ao mecanismo de criptografia nesse roteador. A geração do par de chaves é mostrada na saída do comando de exemplo 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#
```

Como você pode gerar apenas um par de chaves que identifique o roteador, você pode substituir sua chave original e precisa reenviar sua chave pública com cada roteador na associação de criptografia. Isso é mostrado na saída do comando de exemplo 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 o próprio par de chaves DSS do roteador é a primeira etapa no estabelecimento de uma associação de sessão de criptografia. A próxima etapa é trocar chaves públicas com todos os outros roteadores. Você pode inserir essas chaves públicas manualmente, digitando primeiro o comando **show crypto mypubkey** para exibir a chave pública DSS do roteador. Em seguida, você

troca essas chaves públicas (por e-mail, por exemplo) e, com o comando **crypto key pubkey-chain dss**, corta e cole a chave pública do roteador de seu peer no roteador.

Você também pode usar o comando **crypto key exchange dss** para que os roteadores troquem chaves públicas automaticamente. Se você usar o método automatizado, verifique se não há instruções **crypto map** nas interfaces usadas para a troca de chaves. Uma **chave de criptografia de depuração** é útil aqui.

Observação: é uma boa ideia fazer **ping** no seu peer 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 DSS públicas foram trocadas, certifique-se de que ambos os roteadores tenham as chaves públicas um do outro e que elas correspondam, como mostrado na saída do comando 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 Cisco IOS para link dedicado

Depois que as chaves DSS tiverem sido geradas em cada roteador e as chaves públicas DSS tiverem sido trocadas, o comando **crypto map** poderá ser aplicado à interface. A sessão de criptografia começa gerando tráfego que corresponde à lista de acesso usada pelos mapas de criptografia.

```
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#
```

Exemplo 2: Configuração do Cisco IOS para Frame Relay Multiponto

O exemplo de saída de comando a seguir foi extraído do roteador 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 exemplo de saída de comando a seguir foi extraído 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 exemplo de saída de comando a seguir foi extraído 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#
```

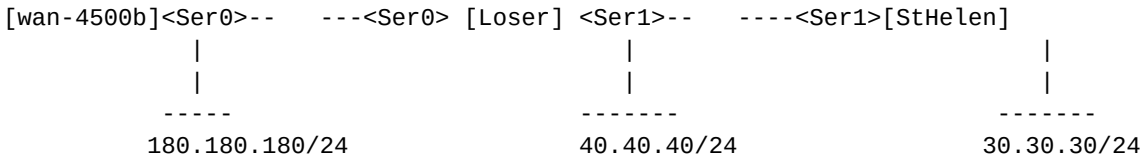
O exemplo de saída de comando a seguir foi extraído do switch Frame Relay.

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

Exemplo 3: Criptografia para e por meio de um roteador

Os roteadores pares não precisam estar a um salto de distância. Você pode criar uma sessão de peering com um roteador remoto. No exemplo a seguir, o objetivo é criptografar 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 preocupação com o 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 Loser e também com StHelen. Ao criptografar o tráfego do segmento Ethernet da wan-4500b para o segmento Ethernet da StHelen, você evita a etapa desnecessária de descriptografia em Loser (Perdido). O perdedor simplesmente passa o tráfego criptografado para a interface serial da StHelen, onde é descriptografado. Isso reduz o atraso de tráfego para os pacotes IP e ciclos de CPU no roteador Perdido. Mais importante, aumenta muito a segurança do sistema, já que um espião no Loser não pode ler o tráfego. Se o Loser estivesse descriptografando o tráfego, haveria uma chance de os dados descriptografados poderem ser desviados.




```
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#
```

Exemplo 4: Criptografia com DDR

Como o Cisco IOS depende do ICMP para estabelecer sessões de criptografia, o tráfego ICMP deve ser classificado como "interessante" na lista de discadores ao realizar a criptografia em um link DDR.

Observação: a compactação funciona no Cisco IOS Software Release 11.3, mas não é muito útil para dados criptografados. Como os dados criptografados têm aparência bastante aleatória, a compactação só retarda as coisas. Mas você pode deixar o recurso ativado para tráfego não criptografado.

Em algumas situações, você desejará fazer backup de discagem para o mesmo roteador. Por exemplo, é útil quando os usuários querem se proteger contra a falha de um link específico em suas redes WAN. Se duas interfaces forem para o mesmo peer, o mesmo mapa de criptografia pode ser usado em ambas as interfaces. A interface de backup deve ser usada para que esse recurso funcione corretamente. Se um projeto de backup tiver uma discagem de roteador em uma caixa diferente, mapas de criptografia diferentes devem ser criados e os correspondentes definidos de acordo. Novamente, 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#
```

Exemplo 5: Criptografia de tráfego IPX em um túnel IP

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

Observação: somente o tráfego neste túnel (IPX) é criptografado. Todo o 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#
```

Exemplo 6: Criptografando túneis L2F

Neste exemplo, somente a criptografia do tráfego L2F para usuários discando é tentada. Aqui, "user@cisco.com" chama o Network Access Server (NAS) local chamado "DEMO2" em sua cidade e é encapsulado no CD do gateway residencial. Todo o tráfego DEMO2 (juntamente com o

de outros chamadores L2F) é criptografado. Como L2F usa a porta UDP 1701, é assim que a lista de acesso é construída, determinando qual tráfego é criptografado.

Observação: se a associação de criptografia ainda não estiver configurada, o que significa que o chamador é a primeira pessoa a entrar e criar o túnel L2F, o chamador pode ser desligado devido ao atraso na configuração da associação de criptografia. Isso pode não acontecer em roteadores com energia de CPU suficiente. Além disso, talvez você queira aumentar o **tempo limite da chave** para que a configuração e o tempo limite da criptografia ocorram somente fora do horário de pico.

O exemplo de saída de comando a seguir foi extraído 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#
```

A saída de exemplo de comando a seguir foi retirada 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

Geralmente, é melhor começar cada sessão de solução de problemas coletando informações usando os seguintes comandos **show**. Um asterisco (*) indica um comando especialmente útil. Consulte também Solução de problemas de segurança de IP - Entendendo e usando comandos

debug para obter informações adicionais.

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

Observação: antes de emitir comandos **debug**, consulte Informações importantes sobre comandos debug.

Comandos	
show crypto cisco algorithms	show crypto cisco key-timeout
show crypto cisco pregen-dh-pairs	* show crypto engine connections ative
show crypto engine connections drop-packet	show crypto engine configuration
show crypto key mypubkey dss	* show crypto key pubkey-chain dss
show crypto map interface serial 1	* mostrar mapa de criptografia
debug crypto engine	* debug crypto sess
debug cry key	clear crypto connection
crypto zeroize	no crypto public-key

- **show crypto cisco algorithms**- Você deve habilitar todos os algoritmos DES (Data Encryption Standard, Padrão de Criptografia de Dados) usados para se comunicar com qualquer outro roteador de criptografia par. Se você não habilitar um algoritmo DES, não poderá usar esse algoritmo, mesmo que tente atribuir o algoritmo a um **mapa de criptografia** posteriormente.Se o roteador tentar configurar uma sessão de comunicação criptografada com um roteador peer e os dois roteadores não tiverem o mesmo algoritmo DES habilitado em ambas as extremidades, a sessão criptografada falhará. Se pelo menos um algoritmo DES comum estiver ativado em ambas as extremidades, a sessão criptografada poderá continuar.**Observação:** a palavra extra cisco aparece no Cisco IOS Software Release 11.3 e é necessária para distinguir entre IPSec e criptografia proprietária da Cisco encontrada 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
```

- **show crypto cisco key-timeout** - Depois que uma sessão de comunicação criptografada é estabelecida, ela é válida por um período de tempo específico. Após esse período, a sessão expira. Uma nova sessão deve ser negociada e uma nova chave DES (session) deve ser gerada para que a comunicação criptografada continue. Use este comando para alterar o tempo que uma sessão de comunicação criptografada dura antes de expirar (expira).

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

Use esses comandos para determinar o período de tempo antes que as chaves DES sejam 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
```

- **show crypto cisco pregen-dh-pairs** - Cada sessão criptografada usa um par exclusivo de números DH. Toda vez que uma nova sessão é estabelecida, novos pares de números DH devem ser gerados. Quando a sessão é concluída, esses números são descartados. A geração de novos pares de números DH é uma atividade que exige muito da CPU, o que pode tornar a configuração de sessão lenta, especialmente para roteadores low-end.Para acelerar a configuração da sessão, você pode optar por ter uma quantidade especificada de pares de números DH pré-gerados e mantidos na reserva. Então, quando uma sessão de comunicação criptografada está sendo configurada, um par de números DH é fornecido a partir dessa reserva. Depois que um par de números DH é usado, a reserva é automaticamente reabastecida com um novo par de números DH, de modo que sempre haja um par de números DH pronto para uso.Geralmente, não é necessário ter mais de um ou dois pares de números DH pré-gerados, a menos que o roteador esteja configurando várias sessões criptografadas com tanta frequência que uma reserva pré-gerada de um ou dois pares de números DH esteja esgotada muito rapidamente.
```
Loser#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 10
```
- **show crypto cisco connections ative**A seguir está um exemplo de saída do comando.
```
Loser#show crypto engine connections active
ID    Interface       IP-Address  State  Algorithm       Encrypt  Decrypt
 16   Serial1         19.19.19.19 set    DES_56_CFB64    376      884
```
- **show crypto cisco engine connections drop-packet**A seguir está um exemplo de saída do comando.
```
Loser#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

Serial1              19.19.19.19   39
```
- **show crypto engine configuration** (era **show crypto engine brief** no Cisco IOS Software Release 11.2.)A seguir está um exemplo de saída do comando.
```
Loser#show crypto engine configuration
slot:               0
engine name:        fred
engine type:        software
serial number:      02802219
platform:           rp crypto engine
crypto lib version: 10.0.0

Encryption Process Info:
input queue top:    465
input queue bot:    465
input queue count:  0
```
- **show crypto key mypubkey dss**A seguir está um exemplo de saída do comando.
```
Loser#show crypto key mypubkey dss
crypto public-key fred 02802219
 79CED212 AF191D29 702A9301 B3E06602 D4FB26B3 316E58C8 05D4930C CE891810
 C0064492 5F6684CD 3FC326E5 679BCA46 BB155402 D443F68D 93487F7E 5ABE182E
quit
```
- **show crypto key pubkey-chain dss**A seguir está um exemplo de saída do comando.
```
Loser#show crypto key pubkey-chain dss
```

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

- **show crypto map interface serial 1**A seguir está um exemplo de saída do comando.

```
Loser#show crypto map interface serial 1
Crypto Map "oldstyle" 10 cisco
        Connection Id = 16       (8 established,    0 failed)
        Peer = barney
        PE = 40.40.40.0
        UPE = 30.30.30.0
        Extended IP access list 133
            access-list 133 permit ip
                source: addr = 40.40.40.0/0.0.0.255
                dest:   addr = 30.30.30.0/0.0.0.255
```

Observe a disparidade de 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
------------
```

- **show crypto map interface serial 1**A seguir está um exemplo de saída do comando.

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

- **debug crypto engine**A seguir está um exemplo de saída do comando.

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

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

Mar 17 11:49:12.246: CRYPTO_ENGINE: packets dropped: State = 0
Mar 17 11:49:13.342: CRYPTO ENGINE 0: get syndrome for conn id 25
Mar 17 11:49:13.346: Crypto engine 0: verify signature
```

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

- **debug crypto sessmgmt**A seguir está um exemplo de saída do 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 estiver definido no Mapa de criptografia, você receberá esta 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 corresponderem, você receberá esta mensagem de erro.

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

Se a chave DSS estiver ausente ou for inválida, você receberá esta mensagem de erro.

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

- **debug crypto key**A seguir está um exemplo de saída do comando.

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

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

- **clear crypto connection**A seguir está um exemplo de saída do comando.

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

wan-2511#clear crypto connection 9
wan-2511#
*Mar  5 04:58:20.690: CRYPTO: Replacing 9 in crypto maps with 0 (slot 0)
```

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

wan-2511#
```

- **crypto zeroize**A seguir está um exemplo de saída do comando.

```
wan-2511#show crypto mypubkey
crypto public-key wan2511 01496536
 11F43C02 70C0ADB7 5DD50600 A0219E04 C867A5AF C40A4FE5 CE99CCAB A8ECA840
 EB95FBEE D727ED5B F0A6F042 BDB5529B DBB0698D DB0B2756 F6CABE8F 05E4B27F
quit

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

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

- **no crypto public-key**A seguir está um exemplo de saída do 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#
```

Solução de problemas do Cisco 7200 com ESA

A Cisco também oferece uma opção de assistência de hardware para fazer criptografia nos roteadores da série Cisco 7200, chamada ESA. O ESA está na forma de um adaptador de porta para a placa VIP2-40 ou um adaptador de porta autônomo para o Cisco 7200. Esta disposição permite o uso de um adaptador de hardware ou do mecanismo de software VIP2 para criptografar e descriptografar dados que entram ou saem pelas interfaces da placa Cisco 7500 VIP2. O Cisco 7200 permite assistência de hardware para criptografar o tráfego para qualquer interface no chassi do Cisco 7200. O uso de uma ajuda de criptografia salva ciclos preciosos da CPU que podem ser usados para outros fins, como roteamento ou qualquer outra função do Cisco IOS.

Em um Cisco 7200, o adaptador de porta autônomo é configurado exatamente igual ao mecanismo de criptografia do software Cisco IOS, mas tem alguns comandos extras que são

usados somente para hardware e para decidir qual mecanismo (software ou hardware) fará a criptografia.

Primeiro, 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]
```

Ative ou desative a criptografia de hardware conforme 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, gere chaves para o ESA antes de ativá-lo.

```
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#
```

Solução de problemas de VIP2 com ESA

O adaptador de porta de hardware ESA na placa VIP2 é usado para criptografar e descriptografar dados que entram ou saem através das interfaces na placa VIP2. Como no Cisco 7200, o uso de uma ajuda de criptografia economiza ciclos preciosos da CPU. Nesse caso, o comando **crypto esa enable** não existe porque o adaptador de porta ESA faz a criptografia para as portas na placa VIP2 se o ESA estiver conectado. O **crypto clear-latch** precisa ser aplicado a esse slot se o adaptador de porta ESA tiver sido instalado pela primeira vez ou removido e 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#
```

Como o módulo de criptografia ESA foi extraído, você receberá a seguinte mensagem de erro até executar um comando **crypto clear-latch** nesse slot, 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 esquecer uma senha atribuída anteriormente, use o comando **crypto zeroize** em vez do comando **crypto clear-latch** para redefinir o ESA. Depois de emitir o comando **crypto zeroize**, você deve regenerar e trocar novamente as chaves DSS. Quando você regenera as chaves DSS, é solicitado que você crie uma nova senha. 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

- Configuração e Troubleshooting da Cisco Network-Layer Encryption: IPSec e ISAKMP - Parte 2
- DES FIPS 46-2 no National Institute of Standards and Technology (NIST)
- DSS FIPS 186 no National Institute of Standards and Technology (NIST)
- Perguntas frequentes dos laboratórios RSA sobre a criptografia de hoje
- Padrões de segurança IETF
- Configurando o protocolo de segurança do intercâmbio chave de Internet
- Configuração da segurança de rede IPSec
- Página de suporte do IPSec
- Suporte Técnico - Cisco Systems