Uma introdução à criptografia de segurança de IP (IPSec)

Índice

Introdução

Este documento apresenta o IPSec aos usuários em uma forma rápida, mas sucinta. Este documento contém as configurações básicas do Internet Key Exchange (IKE) com chaves pré-compartilhadas, IKE com uma Autoridade de Certificação e IPsec. Este não é um documento cansativo. Porém, este original ajuda na compreensão das tarefas e da ordem na qual elas devem ser realizadas.

 **aviso:** Há umas restrições sérias na exportação da criptografia forte. Se você viola a Lei federal E.U., a seguir você, não Cisco, está guardado responsável. Se você tem quaisquer perguntas relativas ao controle de exportação, envie e email a export@cisco.com.

Nota: O Multicast e a transmissão não são apoiados no LAN normal aos túneis LAN ou nos clientes VPN que terminam em todos os dispositivos. O Multicast pode ser passado somente em

túneis GRE. Isto é apoiado somente no Roteadores e não nos VPN 3000 concentratores ou nos Firewall (ASA/PIX).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Background

O IPsec é a plataforma de criptografia da camada de rede da próxima geração para as plataformas de segurança de Cisco (Cisco IOS ® Software, PIX, e assim por diante). Descrito originalmente no RFCs 1825 com 1829, que são agora Obsoletos, o IPsec é discutido atualmente em um número de documentos apresentados pelo grupo em funcionamento da Segurança IP IETF . O IPsec apoia atualmente pacotes do unicast da versão IP 4. O IPv6 e o suporte multicast são chegar mais tarde.

O IPsec tem estas forças sobre ofertas criptos atuais de Cisco:

1. **Multivendor** — Desde que a estrutura do IPsec é estandardizada, os clientes não são travados em nenhuns produtos de fornecedor específicos. O IPsec é encontrado no Roteadores, nos Firewall, e nos desktop de cliente (Windows, Mac, e assim por diante).
2. **Escalabilidade** — O IPsec é projetado com grandes empresas na mente. Consequentemente, tem o gerenciamento chave incorporado.

Nota: Quando diversas plataformas Cisco puderem usar o IPsec, este documento está alinhado para o Cisco IOS Software.

Cripto língua (Vocabulário)

Você precisa de conhecer estes termos a fim compreender o IPsec, e ler o resto deste documento. Quando você vê acrônimos em outras parcelas deste documento, refira esta página para definições.

Advanced Encryption Standard (AES) — O AES foi finalizado como um padrão de processamento de informação federal (FIP) - algoritmo criptográfico aprovado a ser usado a fim proteger a transmissão de dados eletrônica (FIPS PUB 197). O AES é baseado no algoritmo Rijndael, que especifica como usar chaves com um comprimento do 128, 192, ou nos bit 256 para cifrar blocos com um comprimento dos bit 128, 192, ou 256. Todas as nove combinações de comprimento

chave e de extensão do bloqueio são possíveis.

Authentication Header (AH) — Este é um protocolo de segurança que proporcione a autenticação e serviços de detecção de replay opcionais. O AH é encaixado nos dados a ser protegidos, por exemplo, um IP datagram completo. O AH pode ser usado por si só ou com Encryption Service Payload (ESP). Consulte o RFC 2402 .

Autenticação — Esta é uma das funções da estrutura do IPsec. A autenticação estabelece a integridade do fluxo de dados e assegura-se de que não esteja alterada no trânsito. Igualmente fornece a confirmação sobre o origem de fluxo de dados.

Certification Authority (CA) — Esta é uma entidade da terceira com a responsabilidade emitir e revogar Certificados. Cada dispositivo que tem seus próprios certificado e chave pública de CA pode autenticar cada outro dispositivo dentro de um domínio dado de CA. Este termo igualmente aplica-se ao software do server que proporciona estes serviços.

Certificado — Um objeto criptograficamente assinado que contenha uma identidade e uma chave pública associadas com esta identidade.

Criptografia clássica — Este é mecanismo da criptografia proprietária de Cisco usado no Cisco IOS Software Release 11.2. A criptografia clássica está disponível no Cisco IOS Software Release 11.3. Mas, o IPsec não é adaptado ao Cisco IOS Software Release 11.2. Você pode igualmente ver a criptografia clássica do nome referida como criptografia expressa ou tecnologia de criptografia Cisco (CET) na literatura de marketing.

Certificate Revocation List (CRL) — Esta é uma mensagem digitalmente assinada que aliste toda a corrente mas revogou os Certificados alistados por CA dado. Isso é parecido com um catálogo de números de cartão de débito roubados que permite que as lojas recusem cartões de crédito inválidos.

Crypto map — Esta é uma entidade de configuração do Cisco IOS Software que execute duas funções principal. Primeiramente, seleciona os fluxos de dados que precisam o procedimento de segurança. Em segundo, define a política para estes fluxos e o crypto peer a que o tráfego precisa de ir.

Um crypto map é aplicado a uma relação. O conceito de um crypto map foi introduzido na criptografia clássica mas expandido para o IPsec.

Integridade de dados — Este é mecanismos de integridade de dados, com o uso dos algoritmos baseados ou chave pública baseados da chave secreta, que permitem que o receptor de uma parte de dados protegidos a fim verificar que os dados não estiveram alterados no trânsito.

Confidencialidade de dados — Este é o método onde os dados protegidos são manipulados de modo que nenhum atacante possa os ler. Essa proteção geralmente é fornecida pela criptografia de dados e chaves que só estão disponíveis para as partes envolvidas na comunicação.

Autenticação de origem de dados — Este é um serviço de segurança onde o receptor possa verificar que os dados protegidos puderam ter originado somente do remetente. Esse serviço requer um serviço de integridade de dados e um mecanismo principal de distribuição, no qual uma chave de segredo é compartilhada apenas com o remetente e o receptor.

Data Encryption Standard (DES) — O DES foi publicado em 1977 pelo instituto nacional de padrões e é um esquema de criptografia da chave secreta baseado no algoritmo Lucifer do IBM.

O contraste do DES é a chave pública. Cisco usa o DES na criptografia clássica (comprimentos chaves 40-bit e 56-bit), no IPsec cripto (chave 56-bit), e no PIX Firewall (chave 56-bit).

Diffie-Hellman — Este é um método do estabelecimento de uma chave compartilhada sobre uma mídia insegura. Diffie-Hellman é um componente de Oakley, que é definido nesta lista da definição.

DSS — Um Digital Signature Algorithm projetado pelo National Institute of Standards and Technology E.U. (NIST) baseado na criptografia de chave pública. O DSS não faz a criptografia do datagram de usuário. O DSS é um componente na criptografia clássica, assim como o cartão do IPsec de Redcreek, mas não no IPsec executados no Cisco IOS Software.

Encryption Service Adapter (ESA) — Este é um acelerador de criptografia baseado hardware em que seja usado:

- Cisco 7204 e 7206 Router
- VIP2-40s (Versatile Interface Processor2-40s) de segunda geração em todos os Cisco 7500 Series Routers
- VIP2-40 nos Cisco 7000 Series Router que têm os cartões do Cisco 7000 Series Route Switch Processor (RSP7000) e do Chassis Interface do Cisco 7000 Series (RSP7000CI) instalados.

O IPsec não usa a aceleração ESA, mas trabalha em uma caixa que tenha um cartão ESA em uma base somente software.

Encapsulating Security Payload (ESP) — Um protocolo de segurança que forneça a confidencialidade de dados e a proteção a autenticação opcional e os serviços de detecção de replay. O ESP encapsula completamente dados do usuário. O ESP pode ser usado por si só ou conjuntamente com o AH. Refira o RFC 2406: Encapsulating Security Payload (ESP) IP .

Mistura — Esta é uma função de uma maneira que tome um mensagem de entrada do comprimento arbitrário e produza um resumo do comprimento fixo. Cisco usa o Secure Hash Algorithm (SHA) e o message digest 5 (MD5) pica dentro de nossa aplicação da estrutura do IPsec. Veja a definição para o HMAC para mais informação.

HMAC — Este é um mecanismo para a autenticação de mensagem que os usos criptograficamente picam como o SHA e o MD5. Refira o RFC 2104 para uma discussão exaustiva do HMAC.

Internet Key Exchange (IKE) — Um protocolo híbrido que usasse a parte Oakley e parte de um outro conjunto de protocolos chamou o SKEME dentro da estrutura do Internet Security Association and Key Management Protocol (ISAKMP). O IKE é usado para estabelecer uma política de segurança compartilhada e umas chaves autenticadas para os serviços, tais como o IPsec, que exigem chaves. Antes que todo o tráfego de IPSec possa ser passado, cada roteador/Firewall/host devem poder verificar a identidade de seu par. Incorpore manualmente chaves pré-compartilhada em anfitriões, por um serviço de CA, ou o DNS seguro próximo (DNSSec) a fim fazer isto. Este é o protocolo conhecido anteriormente como o ISAKMP/Oakley, e é definido no RFC 2409: O Internet Key Exchange (IKE) . Um ponto potencial da confusão é que os acrônimos ISAKMP e IKE ambos estão usados no Cisco IOS Software a fim referir a mesma coisa. Estes dois artigos são um tanto diferentes.

Internet Security Association and Key Management Protocol (ISAKMP) — Este é um protocol framework que defina os mecânicos da aplicação de um protocolo de intercâmbio chave e da

negociação de uma política de segurança. O ISAKMP é definido no Internet Security Association and Key Management Protocol (ISAKMP).

Transparência de NAT do IPsec — A característica da transparência de NAT do IPsec introduz o apoio para que o tráfego da Segurança IP (IPsec) viaje através do Network Address Translation (NAT) ou dos pontos da tradução de endereços do ponto (PANCADINHA) na rede endereçando muitas incompatibilidades conhecidas entre o NAT e o IPsec. O NAT Traversal é uma característica que seja automóvel detectado por dispositivos VPN. Não há nenhuma etapa de configuração para um roteador que execute o Cisco IOS Software Release 12.2(13)T e Mais Recente. Se ambos os dispositivos VPN são NAT-T capaz, o NAT Traversal é automóvel detectado e automóvel negociado.

ISAKMP/Oakley — Veja o IKE.

Message digest 5 (MD5) — Este é um algoritmo de hashing de uma maneira que produza uma mistura do 128-bit. o MD5 e o Secure Hash Algorithm (SHA) são variações no MD4, que é projetado reforçar a Segurança deste algoritmo de hashing. SHA é mais seguro que o MD4 e o MD5. Os usos de Cisco picam para a autenticação dentro da estrutura do IPsec.

Oakley — Este é um protocolo de intercâmbio chave que defina como adquirir o material de chaveamento autenticado. O mecanismo básico para o Oakley é o algoritmo de intercâmbio de chave Diffie-Hellman. Você pode encontrar o padrão no RFC 2412: O protocolo da determinação da chave OAKLEY .

Discrição perfeita adiante (PFS) — O PFS assegura-se de que uma chave dada IPsec SA não esteja derivada de nenhum outro segredo, como algumas outras chaves. Ou seja se alguém quebra uma chave, o PFS assegura-se de que o atacante não possa derivar nenhuma outra chave. Se o PFS não é permitido, alguém pode potencialmente quebrar a chave secreta IKE SA, copia todos os dados protegidos do IPsec, e usa então o conhecimento do segredo IKE SA a fim comprometer o sas de IPSec setup este IKE SA. Com PFS, quebrar o IKE não dá um acesso imediato do atacante ao IPsec. O atacante precisa de quebrar individualmente cada IPsec SA. A aplicação do Cisco IOS IPsec usa o grupo1 PFS (D-H 768 mordido) à revelia.

Repetição-detecção — Este é um serviço de segurança onde o receptor possa rejeitar velho ou pacotes duplicados a fim derrotar ataques de replay. Os ataques de replay confiam no atacante para mandar mais velho ou pacotes duplicados ao receptor e ao receptor para pensar que o tráfego falso é legítimo. a Repetição-detecção é feita pelo uso dos números de sequência combinados com a autenticação, e é uns recursos padrão do IPsec.

RSA — Este é um algoritmo criptográfico da chave pública, nomeado após seus inventores, Rivest, Shamir e Adleman, com um comprimento chave variável. A fraqueza principal do RSA é que é significativamente lenta computar comparado aos algoritmos populares da chave secreta, tais como o DES. A implementação IKE de Cisco usa um intercâmbio Diffie-Hellman a fim obter as chaves secretas. Esta troca pode ser autenticada com RSA, ou chaves pré-compartilhada. Com o intercâmbio Diffie-Hellman, a chave DES nunca cruza a rede, nem sequer no formulário criptografado, que não é o caso com o RSA cifra e assina a técnica. O RSA não é um public domain, e deve ser licenciado de Rsa Data Security.

Associação de segurança (SA) — Este é um exemplo da política de segurança e do material de ajuste aplicados a um fluxo de dados. o IKE e o IPsec usam SA, embora os SA sejam independente de um outro. O sas de IPSec é unidirecional e é original em cada protocolo de segurança. Um grupo de SA é precisado para uma tubulação dos dados protegidos, uma pela direção por protocolo. Por exemplo, se você tem uma tubulação que apoie o ESP entre pares, um

ESP SA é exigido para cada sentido. Os SA são identificados excepcionalmente pelo endereço do destino (ponto final de IPSec), pelo protocolo de segurança (AH ou ESP), e pelo Security Parameter Index (SPI).

O IKE negocia e estabelece SA em nome do IPsec. Um usuário pode igualmente estabelecer o sas de IPSec manualmente.

IKE SA é usado pelo IKE somente. Ao contrário IPsec SA, é bidirecional.

Secure Hash Algorithm (SHA) — Esta é uma mistura de uma maneira posta adiante pelo NIST. O SHA proximamente é modelado após o MD4 e produz um resumo do 160-bit. Porque o SHA produz um resumo do 160-bit, é mais resistente aos ataques de força bruta do que o 128-bit pica (como o MD5), mas é mais lento.

Split Tunneling — Este é o processo de permitir que um usuário remoto VPN a fim alcançar uma rede pública, o mais geralmente o Internet, ao mesmo tempo que é permitido ao usuário alcançar recursos no escritório remoto. Este método do acesso de rede permite o usuário de alcançar dispositivos remotos, tais como uma impressora conectada e server ao mesmo tempo que para alcançar a rede pública (Internet). Uma vantagem do uso do Split Tunneling é que alivia gargalos e conserva a largura de banda porque o tráfego do Internet não tem que passar através do servidor de VPN. Uma desvantagem deste método é que torna essencialmente o VPN vulnerável ao ataque porque é acessível através da rede pública, NON-segura.

Transforme — Uma transformação descreve um protocolo de segurança (AH ou ESP) com seus algoritmos correspondentes. Por exemplo, ESP com o algoritmo de cifra DES e HMAC-SHA para a autenticação.

Modo de transporte — Este é um modo de encapsulamento para o AH/ESP. O modo de transporte encapsula o payload da camada superior, tal como o Transmission Control Protocol (TCP) ou o User Datagram Protocol (UDP), da datagrama de IP original. Esse modo pode ser usado apenas quando os peers forem pontos finais da comunicação. O contraste do modo de transporte é modo de túnel.

Modo de túnel — Este é o encapsulamento do IP datagram completo para o IPsec. O modo de túnel é usado na ordem para proteger datagramas originados de ou destinado aos sistemas do NON-IPsec, tais como dentro uma encenação do Virtual Private Network (VPN).

Configurar o ISAKMP

O IKE existe para estabelecer somente SA para o IPsec. Antes que possa fazer este, o IKE deve negociar um relacionamento SA (ISAKMP SA) com o par. Desde que o IKE negocia sua própria política, é possível configurar indicações de política múltipla com instruções de configuração diferentes, a seguir deixa os dois anfitriões vir a um acordo. O ISAKMP negocia:

- **Um algoritmo de criptografia** — Isto é limitado à 56-bit DES somente.
- **Um algoritmo de hashing** — MD5 ou SHA
- **Autenticação** — Assinaturas de RSA, momentos criptografado RSA (números aleatórios), ou chaves pré-compartilhada
- **Vida do SA** — Nos segundos

Atualmente, há dois métodos usados a fim configurar o ISAKMP:

1. Use as chaves pré-compartilhada, que são simples configurar.
2. Use **CA**, que é escalável durante todo a empresa.

Nota: A negociação de IKE é feita em UDP 500. O IPsec usa 50 pés e 51 dos protocolos IP. Certifique-se que estes estão permitidos em todas as Listas de acesso que você tiver entre os pares.

1. Chaves pré-compartilhada

Este é o método rápido e sujo usado a fim configurar o IKE. Quando a configuração de IKE for simples e você não usa CA, não escala muito bem.

Você precisa de fazer estes a fim configurar o IKE:

- Configurar séries da proteção ISAKMP.
- Configurar a chave ISAKMP.

Configurar séries da proteção ISAKMP

Este comando cria o objeto da política de ISAKMP. É possível ter políticas múltiplas, mas há somente um neste exemplo:

```
dt3-45a(config)#crypto isakmp policy 1 dt3-45a(config-isakmp)#
```

Com o **comando group**, você pode declarar que módulo do tamanho a se usar para o cálculo de Diffie-Hellman. O grupo1 é 768 bit por muito tempo, e o grupo2 é 1024 bit por muito tempo. Por que você usaria um sobre o outro? Não todo o grupo de suporte 2. dos vendedores. Também, o grupo2 é igualmente significativamente mais utilização de CPU do que o grupo um. Por este motivo, você não quer usar o grupo2 em roteadores de extremidade baixa como o Cisco 2500 Series ou menos. Mas, o grupo2 é mais seguro do que o grupo1. Desde que este exemplo usa Cisco4500, o grupo2 é usado, e certifica-se que o par está configurado igualmente a fim usar o grupo2. O padrão é grupo1. Se você seleciona as propriedades padrão, as linhas do grupo1 não aparecem quando você faz um **comando write terminal**.

```
dt3-45a(config-isakmp)#group 2
```

O MD5 é nosso algoritmo de hashing nesta linha. Quando a aplicação do SHA e o MD5 forem ambo o imperativos, não todos os pares podem ser configurados a fim negociar um ou o outro. O padrão no Cisco IOS é SHA, que é mais seguro do que MD5.

```
dt3-45a(config-isakmp)#hash md5
```

A vida do SA, 500 segundos neste caso, é mostrada neste comando. Se você não ajusta uma vida, opta 86400 segundos, ou um dia. Quando a vida útil do temporizador expirar, o AS será renegociado como medida de segurança.

```
dt3-45a(config-isakmp)#lifetime 500
```

Neste comando, o IKE é dito manualmente que chave a se usar. Consequentemente, o **comando pre-share** é usado. As duas opções, além do comando pre-share, são os comandos rsa-encr e rsa-sig. O comando rsa-encr configura os momentos criptografados do RSA e o comando rsa-sig configura a assinatura do RSA. **O RSA-encr** e os **comandos rsa-sig** são endereçados no uso uma seção de CA. Por agora, recorde que o RSA-**SIG** é o padrão.

```
dt3-45a(config-isakmp)#authentication pre-share
```

Configurar a chave ISAKMP

Nestes comandos, o IKE é dito que chave a se usar. O par, 192.168.10.38 neste caso, deve ter a mesma Slurpee-máquina chave em sua configuração.

```
dt3-45a(config-isakmp)#exit dt3-45a(config)#crypto isakmp key Slurpee-Machine address 192.168.10.38
```

Você é feito agora com configuração de IKE. Estas linhas são a configuração de IKE do par. As configurações completas para ambo o Roteadores estão na seção de configurações da amostra deste documento:

```
crypto isakmp policy 1
 hash md5
 group 2
 authentication pre-share
crypto isakmp key Slurpee-Machine address 192.168.10.66
```

2. Use CA

O uso de CA é um método complexo usado a fim configurar o IKE. Desde que é muito escalável no IPsec, você precisa de usar o IPsec em vez da criptografia clássica. Quando o Cisco IOS Software Release 11.3(3) é liberado, está indo somente estar alguns vendedores de CA que enviam o produto. Inicialmente, a maioria de configurações são feitas com o uso das **chaves pré-compartilhada**. Verisign, confia, Microsoft e Netscape, e provavelmente um host de outro, está funcionando no Produtos de CA. Para este exemplo, Verisign CA é usado.

Você precisa de fazer estes a fim usar CA:

- Crie pares de chaves RSA para o roteador.
- Peça o certificado de CA.
- Registre Certificados para o roteador cliente.
- Configurar séries da proteção ISAKMP.

Crie pares de chaves RSA para o roteador

O comando das uso-**chaves dos rsa gen da chave de criptografia** pode confundi-lo. Este comando cria dois pares de chaves para o RSA:

- um par de chaves para a criptografia
- um par de chaves para assinaturas digital

Um par de chaves refere uma chave pública e sua chave secreta correspondente. Se você não especifica uso-chaves no fim do comando, o roteador gerencie somente um par de chaves RSA e usa-o para a criptografia e as assinaturas digital. Como um aviso, esse este comando pode ser usado a fim criar chaves DSS. Mas o DSS é parte de uma criptografia clássica, não IPsec.

```
dt3-45a(config)#crypto key gen rsa usage-keys The name for the keys will be: dt3-45a.cisco.com %You
already have RSA keys defined for dt3-45a.cisco.com. %Do you really want to replace them? [yes/no] yes
```

Desde que algumas chaves RSA já existem nesta caixa, pergunta se você quer obter livrado das chaves que existem. Desde que a resposta é sim, confirme o comando. Esta alerta é retornada:

```
Choose the size of the key modulus in the range of
   360 to 2048 for your Signature keys.
Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: <return>
Generating RSA keys...
[OK]
```

```
Choose the size of the key modulus in the range of
   360 to 2048 for your Encryption keys.
Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]: <return>
Generating RSA keys...
[OK]
dt3-45a(config)#
```

Os pares de chaves RSA com o módulo do 512-bit do padrão são criados agora. Retire fora do modo de configuração e inscreva um **comando show crypto key mypubkey rsa**. Você pode agora ver sua chave pública RSA. A parcela da chave privada do par de chaves é considerada nunca. Mesmo se você não tem chaves PRE-existentes, você vê a mesma coisa de previamente.

Nota: Recorde salvar sua configuração uma vez que você gerou seus pares de chaves.

Peça um certificado de CA

Você precisa agora de configurar o roteador a fim falar a CA. Isto envolve diversas etapas. Você precisa de coordenar eventualmente com seu administrador de CA.

Nestas linhas de configuração, um Domain Name é adicionado ao roteador. Isto cria um **ciscoca-ultra do** hostname, e diz ao roteador qual seu endereço IP de Um ou Mais Servidores Cisco ICM NT é, e os Nomes do servidor. Você precisa de ter os nomes de host definidos para CA ou um DNS que trabalhe na caixa. Cisco recomenda que você tem um DNS que trabalhe na caixa.

```
dt3-45a(config)#ip host ciscoca-ultra 171.69.54.46 dt3-45a(config)#ip domain-name cisco.com dt3-45a(config)#ip name-server 171.692.132 dt3-45a(config)#ip name-server 198.92.30.32
```

Comece configurar os parâmetros de CA. **o Verisign-Ca** é apenas um nome arbitrário.

```
dt3-45a(config)#crypto ca identity verisign-ca dt3-45a(ca-identity)#
```

Nesta saída, o protocolo do registro de Cisco usa o HTTP a fim falar a CA. O comando **dt3-45a(ca-identity)#enrollment URL http://ciscoca-ultra** diz o roteador para ir ao URL especificado a fim interagir com CA. **Os dt3-45a(ca-identity)#crypto Ca autenticam o** comando Verisign-**Ca** instruem o roteador buscar o certificado de CA. Antes que você possa se registrar em CA, você precisa de certificar-se de você conversa ao CA real verificar o certificado de CA com o administrador de CA a fim assegurar a autenticidade.

```
dt3-45a(ca-identity)#enrollment url http://ciscoca-ultra dt3-45a(ca-identity)#exit dt3-45a(ca-identity)#crypto ca authenticate verisign-ca
```

Registre Certificados para o roteador cliente

Emita o **Ca cripto registram o** comando Verisign-**Ca** a fim começar o registro com CA. Existem várias etapas para isso. Primeiramente, você tem que verificar a identidade de CA, a seguir CA tem que verificar a identidade do roteador. Se você precisa nunca de revogar seu certificado antes que expirar, se você renumber as relações de seu roteador ou se você acredita que seu certificado está comprometido, você precisa de fornecer uma senha ao administrador de CA. Entre nisso, como é ilustrado nesta saída. Depois que você incorpora a sua senha, o roteador continua.

```
dt3-45a(config)#crypto ca enroll verisign-ca %Start certificate enrollment .. %Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it. Password: Re-enter password:
```

Você vê agora as impressões digitais do CA verificar que as impressões digitais estão corretas com o administrador de CA. Além, se você faz um **comando show crypto ca cert**, você vê o certificado de CA, além do que seus próprios Certificados. Os certificados de CA são alistados como pendente neste tempo.

```
% The subject name for the keys will be: dt3-45a.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 01204044
% Include an IP address in the subject name? [yes/no]: yes
Interface: Ethernet 0
Request certificate from CA? [yes/no]: yes
```

Contacte o administrador de CA porque esta pessoa quer confirmar a identidade da mangueira antes que um certificado esteja emitido. Uma vez CA emite o certificado, o estado de nossas mudanças do certificado de pendente a disponível. Com isso, a inscrição CA está concluída. Mas, você não é feito. Você ainda precisa de configurar objetos da política de ISAKMP.

Configurar séries da proteção ISAKMP

O padrão RSA-**SIG** é usado nesta saída. É possível que haja várias suites de proteção, mas nesse exemplo há somente uma. No caso das suites de proteção múltipla, as políticas são apresentadas ao par em ordem numérica e o par negocia qual para usar-se. Você precisa de fazer este se você sabe que todos seus pares não apoiam determinadas características. O roteador não tenta negociar as coisas que não fazem o sentido. Por exemplo, se você configura sua política para o RSA-**SIG** e você não tem nenhum certificado, o roteador não negocia este.

```
dt3-45a(config)#crypto isakmp policy 1 dt3-45a(config-isakmp)#hash md5 dt3-45a(config-isakmp)#lifetime
4000 dt3-45a(config-isakmp)#exit
```

Configurar o IPsec

Se você usa chaves pré-compartilhada ou configura CA, uma vez que você setup o intercâmbio de chave de Internet IKE, você ainda tem que setup o IPsec. Apesar do que método IKE você usa, as etapas de configuração para o IPsec são as mesmas.

Você precisa de fazer estes a fim configurar o IPsec:

- Crie o ACL extendido.
- Crie o IPsec
- Crie o crypto map.
- Aplique o crypto map à relação.

Criar ACL estendido

Este comando é um ACL muito simples que permita que o Roteadores fale a um outro, por exemplo, um telnet de um roteador ao seguinte.

```
dt3-45a(config)#access-list 101 permit ip host 192.168.10.38 host 192.168.10.66
```

Um ACL mais realístico olha como este comando. Este comando é um ACL extendido ordinário, onde 192.168.3.0 seja uma sub-rede atrás do roteador na pergunta, e 10.3.2.0 é uma sub-rede em algum lugar atrás do roteador de peer. Recorde que a **licença** significa cifra e **nega** significa não cifra.

```
dt3-45a(config)#access-list 101 permit ip 192.168.3.0 0.0.0.255 10.3.2.0 0.0.0.255
```

Crie o IPsec

Crie três transformam grupos. O primeiro usa somente ESP, o segundo usa AH combinado com ESP e o último usa somente AH. Durante a negociação IPsec SA, todos os três são oferecidos ao par, que escolhe um. Também, para todos os três conjuntos de transformação, use o **modo de túnel do** padrão. O modo de transporte pode ser usado somente quando os pontos finais de criptografia são igualmente os valores-limite da comunicação. O modo de transporte pode ser especificado pelo comando mode transport sob a configuração do grupo de transformação. O modo de túnel é utilizado principalmente no cenário VPN. Igualmente note que **esp-rfc1829** e **ah-rfc1828** estão baseados nos RFC originais para esta tecnologia e são Obsoletos transformam incluído para para trás a compatibilidade. Não todos os vendedores apoiam estes transformam, mas os outros fornecedores apoiam somente estes transformam.

Os grupos da transformação nestes comandos não são necessariamente os mais práticos. Por exemplo, PapaBear e BabyBear têm conjuntos de transformação do secundário-padrão. Use **esp-rfc1829** e **ah-rfc1828** junto no mesmo conjunto de transformação.

```
dt3-45a(config)#crypto ipsec transform-set PapaBear esp-rfc1829 dt3-45a(cfg-crypto-trans)#exit dt3-45a(config)#crypto ipsec transform-set MamaBear ah-md5-hmac esp-des dt3-45a(cfg-crypto-trans)#exit dt3-45a(config)#crypto ipsec transform-set BabyBear ah-rfc1828 dt3-45a(cfg-crypto-trans)#exit dt3-45a(config)#
```

Criar Cripto Mapa

A etiqueta IPsec-**ISAKMP** diz ao roteador que este crypto map é um crypto map do IPsec. Embora haja somente um par declarado neste crypto map, você pode ter peer múltiplos dentro de um crypto map dado. **A vida da chave de sessão** pode ser expressada em quilobytes (após uma x-quantidade de tráfego, mude a chave) ou em segundos, como é mostrado nestes comandos. O objetivo deste é fazer os esforços de um atacante potencial mais difíceis. **O comando set transform-set** é onde você associa transforma com o crypto map. Além, a ordem em que você declara que transforma é significativa. MamaBear é preferido mais nesta configuração, e então no resto no ordem decrescente de preferência completamente a BabyBear. Os meios do **comando match address 101** usar a lista de acessos 101 a fim determinar que tráfego é relevante. Você pode ter crypto map múltiplos com o mesmo nome, que é tatu, neste exemplo, e números de sequência diferentes, que é 10, neste exemplo. Os crypto map da combinação de múltiplo e os números de sequência diferentes permitem que você misture e criptografia clássica e IPsec do fósforo. Também é possível modificar as configurações do PFS aqui. O grupo1 PFS é o padrão neste exemplo. Você pode mudar o PFS ao grupo2, ou gire-o fora de tudo junto, que você não deve fazer.

```
dt3-45a(config)#crypto map armadillo 10 ipsec-isakmp dt3-45a(config-crypto-map)#set peer 192.168.10.38 dt3-45a(config-crypto-map)#set session-key lifetime seconds 4000 dt3-45a(config-crypto-map)#set transform-set MamaBear PapaBear BabyBear dt3-45a(config-crypto-map)#match address 101
```

Aplique o mapa de criptografia à interface

Estes comandos apply o crypto map à relação. Você pode atribuir somente um crypto map ajustado a uma relação. Se as entradas múltiplas do crypto map têm o mesmo nome de mapa mas um segs.-NUM diferente, são parte do mesmo grupo e são todas aplicadas à relação. A ferramenta de segurança avalia a entrada do **crypto map** com o mais baixo segs.-NUM primeiramente.

```
dt3-45a(config)#interface e0 dt3-45a(config-if)#crypto map armadillo
```

Considerações sobre memória e CPU

Os pacotes que são processados pelo IPsec são mais lentos do que os pacotes que são processados com a criptografia clássica. Há diversas razões para esta e puderam causar problemas de desempenho significativos:

1. O IPsec introduz a expansão de pacote, que é mais provável exigir a fragmentação e a remontagem correspondente de datagramas do IPsec.
2. Os pacotes criptografado são autenticados provavelmente, assim que significa que há duas operações criptográficas que são executadas para cada pacote.
3. Os algoritmos de autenticação são lentos, embora o trabalho seja feito para acelerar coisas como as computações de Diffie-Hellman.

Além, o intercâmbio chave Diffie-Hellman usado no IKE é uma exponenciação muito de números grandes (entre 768 e 1024 bytes) e pode tomar até quatro segundos em Cisco2500. O desempenho do RSA é dependente do tamanho do número primo escolhido para o par de chaves RSA.

Para cada roteador, o base de dados SA pega aproximadamente 300 bytes, mais 120 bytes para cada SA nisso. Nas situações onde há dois sas de IPSec, uns de entrada e um de partida, 540 bytes são exigidos, na maioria dos casos. Cada entrada IKE SA é aproximadamente 64 bytes cada um. A única vez que você tem um IPsec SA para um fluxo de dados é quando a comunicação é de sentido único.

IPsec e IKE impacta no desempenho quando active. Os intercâmbios chave Diffie-Hellman, a autenticação da chave pública, e a criptografia /descriptografia consomem uma quantidade significativa de recursos. Embora, muito esforço fosse feito a fim minimizar este impacto.

Há uma diminuição pequena no desempenho para os pacotes não codificados que atravessam uma relação que faça cripto. Isto é porque todos os pacotes têm que ser verificados contra o crypto map. Não há nenhum impacto no desempenho nos pacotes que atravessam o roteador que evita uma relação que faça cripto. O impacto o mais grande está nos fluxos dos dados criptografados.

Use o grupo1 para intercâmbios chave Diffie-Hellman dentro do IKE, use o MD5 como seu algoritmo de hashing, e use umas vidas mais longas a fim minimizar o impacto do subsistema de criptografia no resto do roteador. Nas trocas para este ajuste de desempenho, você pode obter a criptografia fraca. Finalmente, é até a política de segurança do cliente a fim determinar que características a se usar e qual a sair apenas.

Saída dos comandos show

Nota: As captações nestas seções são tomadas de uma série diferente de testes do que aquelas usadas nas seções anterior deste documento. Consequentemente, estas captações podem ter endereços IP de Um ou Mais Servidores Cisco ICM NT diferentes e refletir configurações levemente diferentes. Uma outra série de **comandos show** é fornecida na seção de informação debugar deste documento.

Saída relacionada ao IKE

Estude estes comandos a fim verificar o registro de Verisign CA. Estes comandos show as

chaves públicas que você se usa para a criptografia RSA e as assinaturas.

```
dt1-45a#show crypto key mypubkey rsa % Key pair was generated at: 11:31:59 PDT Apr 9 1998 Key name: dt1-
45a.cisco.com Usage: Signature Key Key Data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241
00C11854 39A9C75C 4E34C987 B4D7F36C A058D697 13172767 192166E1 661483DD 0FDB907B F9C10B7A CB5A034F
A41DF385 23BEB6A7 C14344BE E6915A12 1C86374F 83020301 0001 % Key pair was generated at: 11:32:02 PDT Apr
9 1998 Key name: dt1-45a.cisco.com Usage: Encryption Key Key Data: 305C300D 06092A86 4886F70D 01010105
00034B00 30480241 00DCF5AC 360DD5A6 C69704CF 47B2362D 65123BD4 424B6FF6 AD10C33E 89983D08 16F1EA58
3700BCF9 1EF17E71 5931A9FC 18D60D9A E0852DDD 3F25369C F09DFB75 05020301 0001
```

Este comando mostra aos Certificados que o roteador reconhece. Um certificado que tivesse o **status pendente** foi submetido a CA para a aprovação.

```
dt1-45a#show crypto ca certificates Certificate Subject Name Name: dt1-45a.cisco.com Serial Number:
01193485 Status: Available Certificate Serial Number: 650534996414E2BE701F4EF3170EDFAD Key Usage:
Signature CA Certificate Status: Available Certificate Serial Number: 3051DF7169BEE31B821DFE4B3A338E5F
Key Usage: Not Set Certificate Subject Name Name: dt1-45a.cisco.com Serial Number: 01193485 Status:
Available Certificate Serial Number: 1e621faf3b9902bc5b49d0f99dc66d14 Key Usage: Encryption
```

Esta saída mostra as chaves públicas do roteador e onde o roteador aprendeu sobre elas.

```
dt1-45a#show crypto key pubkey-chain rsa Codes: M - Manually configured, C - Extracted from certificate
Code Usage IP-Address Name C Signing Cisco SystemsDevtestCISCOCA-ULTRA C General 172.21.30.71 dt1-
7ka.cisco.com
```

Essa é a tabela SA ISAKMP (IKE). Aqui você vê que um SA existe atualmente entre 172.21.30.71 e 172.21.30.70. O par precisa de ter uma entrada SA no mesmo estado que a saída deste roteador.

```
dt1-7ka#show crypto isakmp sa dst src state conn-id slot 172.21.30.70 172.21.30.71 QM_IDLE 47 5
```

Estas linhas mostram os objetos da política configurados. Neste caso, as políticas **1**, **2**, e **4** são usadas, além do que o padrão. As políticas são propostas ao par em ordem, com **1** como o mais preferido.

```
dt1-45a#show crypto isakmp policy Protection suite of priority 1 encryption algorithm: DES - Data
Encryption Standard (56 bit keys). hash algorithm: Message Digest 5 authentication method: Rivest-Shamir-
Adleman Signature Diffie-Hellman group: #1 (768 bit) lifetime: 180 seconds, no volume limit Protection
suite of priority 2 encryption algorithm: DES - Data Encryption Standard (56 bit keys). hash algorithm:
Secure Hash Standard authentication method: Pre-Shared Key Diffie-Hellman group: #2 (1024 bit) lifetime:
180 seconds, no volume limit Protection suite of priority 4 encryption algorithm: DES - Data Encryption
Standard (56 bit keys). hash algorithm: Message Digest 5 authentication method: Pre-Shared Key Diffie-
Hellman group: #2 (1024 bit) lifetime: 180 seconds, no volume limit Default protection suite encryption
algorithm: DES - Data Encryption Standard (56 bit keys). hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature Diffie-Hellman group: #1 (768 bit) lifetime: 86400
seconds, no volume limit
```

Comandos show IPsec-relacionados

Este comando mostra o crypto map **ToOtherRouter**, os ACL, e as propostas de transformação aplicadas a este crypto map, aos pares, e à chave vitalícia.

```
S3-2513-2#show crypto map Crypto Map "ToOtherRouter" 10 ipsec-isakmp Peer = 192.168.1.1 Extended IP
access list 101 access-list 101 permit ip source: addr = 192.168.45.0/0.0.0.255 dest: addr =
192.168.3.0/0.0.0.255 Connection Id = UNSET (0 established, 0 failed) Current peer: 192.168.1.1 Session
key lifetime: 4608000 kilobytes/3600 seconds PFS (Y/N): N Transform proposals={ Elvis, Bubba, BarneyDino,
}
```

Esta configuração usa o mesmo roteador como a saída precedente, mas comandos diferentes. Você vê todas as propostas de transformação, que os ajustes eles negociam, e os padrões.

```
S3-2513-2#show crypto ipsec transform-set Transform proposal Elvis: { ah-sha-hmac } supported settings =
{ Tunnel, }, default settings = { Tunnel, }, will negotiate = { Tunnel, }, { esp-des } supported settings
= { Tunnel, }, default settings = { Tunnel, }, will negotiate = { Tunnel, }, Transform proposal Bubba: {
```

```
ah-rfc1828 } supported settings = { Tunnel, }, default settings = { Tunnel, }, will negotiate = { Tunnel,
}, { esp-des esp-md5-hmac } supported settings = { Tunnel, }, default settings = { Tunnel, }, will
negotiate = { Tunnel, }, Transform proposal BarneyDino: { ah-md5-hmac } supported settings = { Tunnel, },
default settings = { Tunnel, }, will negotiate = { Tunnel, },
```

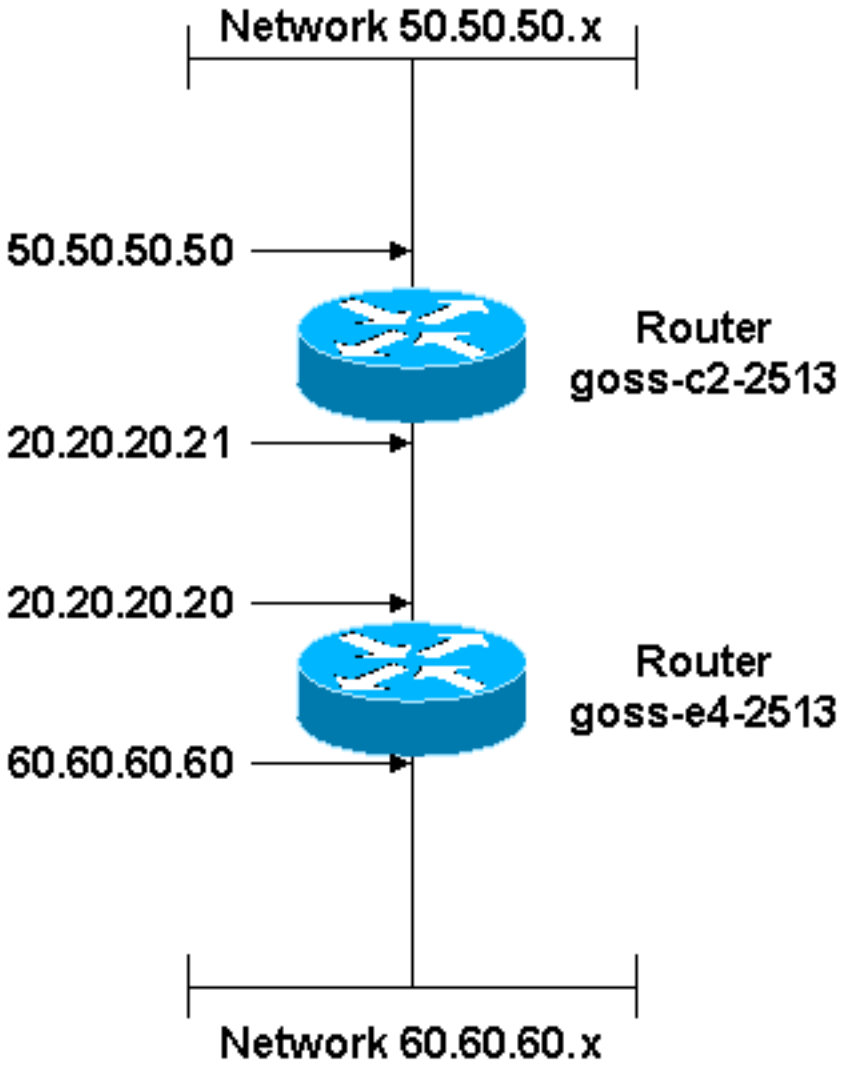
Este comando mostra as associações de segurança IPSec atuais deste roteador. O roteador tem um AH SA para entrante e que parte.

```
S3-2513-2#show crypto ip session Session key lifetime: 4608000 kilobytes/3600 seconds S3-2513-2#show
crypto ipsec sa interface: Ethernet0 Crypto map tag: ToOtherRouter, local addr. 192.168.1.2 local ident
(addr/mask/prot/port): (192.168.45.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port):
(192.168.3.0/255.255.255.0/0/0) current_peer: 192.168.1.1 PERMIT, flags={origin_is_acl,} #pkts encaps: 0,
#pkts encrypt: 0, #pkts digest 0 #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0 #send errors 5, #recv
errors 0 local crypto endpt.: 192.168.1.2, remote crypto endpt.: 192.168.1.1 path mtu 1500, media mtu
1500 current outbound spi: 25081A81 inbound esp sas: inbound ah sas: spi: 0x1EE91DDC(518594012)
transform: ah-md5-hmac , in use settings ={Tunnel, } slot: 0, conn id: 16, crypto map: ToOtherRouter sa
timing: remaining key lifetime (k/sec): (4608000/3423) replay detection support: Y outbound esp sas:
outbound ah sas: spi: 0x25081A81(621288065) transform: ah-md5-hmac , in use settings ={Tunnel, } slot: 0,
conn id: 17, crypto map: ToOtherRouter sa timing: remaining key lifetime (k/sec): (4608000/3424) replay
detection support: Y
```

Configurações de exemplo

Esta configuração usa **chaves pré-compartilhada**. Esta configuração de roteador é usada a fim criar o resultado do debug alistado na seção de informação debugar. Esta configuração permite uma rede chamada X situado atrás do roteador de origem para falar a uma rede chamada Y situado atrás do roteador de peer. Consulte a documentação do Cisco IOS Software para sua versão do Cisco IOS, ou use a ferramenta de consulta de comandos (clientes registrados somente) para obter mais informações sobre de um comando específico. Esta ferramenta permite que o usuário olhe acima uma descrição detalhada ou diretrizes de configuração para um comando específico.

Diagrama de Rede



Configurações

- Roteador de Origem
- Roteador do correspondente

Roteador de Origem

```
Current configuration:
!
version 11.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname goss-e4-2513
!
enable secret 5 $1$ZuRD$YBaAh3oIv4iltIn0TMCUX1
enable password ww
!
!--- IKE configuration crypto isakmp policy 1 hash md5
authentication pre-share crypto isakmp key Slurpee-Machine
address 20.20.20.21 ! !--- IPsec configuration crypto ipsec
transform-set BearPapa esp-rfc1829 crypto ipsec transform-set
BearMama ah-md5-hmac esp-des crypto ipsec transform-set
BearBaby ah-rfc1828 ! crypto map armadillo 1 ipsec-isakmp set
peer 20.20.20.21 set security-association lifetime seconds
190 set transform-set BearPapa BearMama BearBaby !--- Traffic
```

```
to encrypt match address 101 ! interface Ethernet0 ip address
60.60.60.60 255.255.255.0 no mop enabled ! interface Serial0
ip address 20.20.20.20 255.255.255.0 no ip mroute-cache no
fair-queue crypto map armadillo ! interface Serial1 no ip
address shutdown ! interface TokenRing0 no ip address
shutdown ! ip classless ip route 0.0.0.0 0.0.0.0 20.20.20.21
!--- Traffic to encrypt access-list 101 permit ip 60.60.60.0
0.0.0.255 50.50.50.0 0.0.0.255 dialer-list 1 protocol ip
permit dialer-list 1 protocol ipx permit ! line con 0 exec-
timeout 0 0 line aux 0 line vty 0 4 password ww login ! end
```

Roteador do correspondente

```
Current configuration:
!
version 11.3
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname goss-c2-2513
!
enable secret 5 $1$DBTl$Wtg2eS7Eb/Cw5l.nDhkEi/
enable password ww
!
ip subnet-zero
!
!--- IKE configuration crypto isakmp policy 1 hash md5
authentication pre-share crypto isakmp key Slurpee-Machine
address 20.20.20.20 ! !--- IPsec configuration crypto ipsec
transform-set PapaBear esp-rfc1829 crypto ipsec transform-set
MamaBear ah-md5-hmac esp-des crypto ipsec transform-set
BabyBear ah-rfc1828 ! ! crypto map armadillo 1 ipsec-isakmp
set peer 20.20.20.20 set security-association lifetime
seconds 190 set transform-set MamaBear PapaBear BabyBear !---
Traffic to encrypt match address 101 ! ! ! interface
Ethernet0 ip address 50.50.50.50 255.255.255.0 no ip
directed-broadcast ! interface Serial0 ip address 20.20.20.21
255.255.255.0 no ip directed-broadcast no ip mroute-cache no
fair-queue clockrate 9600 crypto map armadillo ! interface
Serial1 no ip address no ip directed-broadcast shutdown !
interface TokenRing0 no ip address no ip directed-broadcast
shutdown ! ip classless ip route 0.0.0.0 0.0.0.0 20.20.20.20
!--- Traffic to encrypt access-list 101 permit ip 50.50.50.0
0.0.0.255 60.60.60.0 0.0.0.255 dialer-list 1 protocol ip
permit dialer-list 1 protocol ipx permit ! ! line con 0 exec-
timeout 0 0 transport input none line aux 0 line aux 0 line
vty 0 4 password ww login ! end
```

Informações de debug

Esta seção tem o resultado do debug de uma sessão normal IKE/IPsec entre dois Roteadores. As configurações são provenientes da seção Configurações de exemplo neste documento. O Roteadores usa uma chave pré-compartilhada. Ambo o Roteadores tem o **isakmp do debug crypto**, o **IPsec do debug crypto**, e os **comandos debug crypto engine** permitidos. Isto foi testado com um ping estendido da interface Ethernet do roteador de origem à interface Ethernet do roteador de peer (60.60.60.60 a 50.50.50.50).

Nota: O azul, instruções em itálico neste exemplo de debug é notas para ajudá-lo a seguir o que acontece, eles não é parte do resultado do debug.

- Roteador de Origem
- Show command output (resultado do comando show) do roteador de origem após a negociação IKE/IPsec
- Roteador de peer com a mesma seqüência de ping, como visto no outro lado
- Comandos show de roteadores de peer

Roteador de Origem

```
goss-e4-2513#show clock goss-e4-2513#ping Protocol [ip]:
Target IP address: 50.50.50.50 Repeat count [5]: 10 Datagram
size [100]: Timeout in seconds [2]: Extended commands [n]: y
Source address or interface: 60.60.60.60 Type of service [0]:
Set DF bit in IP header? [no]: Validate reply data? [no]:
Data pattern [0xABCD]: Loose, Strict, Record, Timestamp,
Verbose[none]: Sweep range of sizes [n]: Type escape sequence
to abort. Sending 10, 100-byte ICMP Echos to 50.50.50.50,
timeout is 2 seconds: Apr 2 12:03:55.347: IPSEC(sa_request):
, (key eng. msg.) src= 20.20.20.20, dest= 20.20.20.21,
src_proxy= 60.60.60.0/255.255.255.0/0/0 (type=4), dest_proxy=
50.50.50.0/255.255.255.0/0/0 (type=4), protocol= ESP,
transform= esp-rfc1829 , lifedur= 190s and 4608000kb, spi=
0x0(0), conn_id= 0, keysize= 0, flags= 0x4004 Apr 2
12:03:55.355: IPSEC(sa_request): , (key eng. msg.) src=
20.20.20.20, dest= 20.20.20.21, src_proxy=
60.60.60.0/255.255.255.0/0/0 (type=4), dest_proxy=
50.50.50.0/255.255.255.0/0/0 (type=4), protocol= AH,
transform= ah-md5-hmac , lifedur= 190s and 4608000kb, spi=
0x0(0), conn_id= 0, keysize= 0, flags= 0x4004 Apr 2
12:03:55.363: IPSEC(sa_request): , (key eng. msg.) src=
20.20.20.20, dest= 20.20.20.21, src_proxy=
60.60.60.0/255.255.255.0/0/0 (type=4), dest_proxy=
50.50.50.0/255.255.255.0/0/0 (type=4), protocol= ESP,
transform= esp-des , lifedur= 190s and 4608000kb, spi=
0x0(0), conn_id= 0, keysi.ze= 0, flags= 0x4004 Apr 2
12:03:55.375: IPSEC(sa_request): , (key eng. msg.) src=
20.20.20.20, dest= 20.20.20.21, src_proxy=
60.60.60.0/255.255.255.0/0/0 (type=4), dest_proxy=
50.50.50.0/255.255.255.0/0/0 (type=4), protocol= AH,
transform= ah-rfc1828 , lifedur= 190s and 4608000kb, spi=
0x0(0), conn_id= 0, keysize= 0, flags= 0x4004 !--- Note that
the router offers to the peer all of the !--- available
transforms. Apr 2 12:03:55.391: ISAKMP (14): beginning Main
Mode exchange Apr 2 12:03:57.199: ISAKMP (14): processing SA
payload. message ID = 0 Apr 2 12:03:57.203: ISAKMP (14):
Checking ISAKMP transform 1 against priority 1 policy Apr 2
12:03:57.203: ISAKMP: encryption DES-CBC Apr 2 12:03:57.207:
ISAKMP: hash MD5 Apr 2 12:03:57.207: ISAKMP: default group 1
Apr 2 12:03:57.207: ISAKMP: auth pre-share Apr 2
12:03:57.211: ISAKMP (14): atts are acceptable. Next payload
is 0 Apr 2 12:03:57.215: Crypto engine 0: generate alg param
Apr 2 12:03:5.8.867: CRYPTO_ENGINE: Dh phase 1 status: 0 Apr
2 12:03:58.871: ISAKMP (14): SA is doing pre-shared key
authentication.. Apr 2 12:04:01.291: ISAKMP (14): processing
KE payload. message ID = 0 Apr 2 12:04:01.295: Crypto engine
0: generate alg param Apr 2 12:04:03.343: ISAKMP (14):
processing NONCE payload. message ID = 0 Apr 2 12:04:03.347:
Crypto engine 0: create ISAKMP SKEYID for conn id 14 Apr 2
12:04:03.363: ISAKMP (14): SKEYID state generated Apr 2
12:04:03.367: ISAKMP (14): processing vendor id payload Apr 2
12:04:03.371: ISAKMP (14): speaking to another IOS box! Apr 2
12:04:03.371: generate hmac context for conn id 14 Apr 2
12:04:03.615: ISAKMP (14): processing ID payload. message ID
```

= 0 Apr 2 12:04:03.615: ISAKMP (14): processing HASH payload. message ID = 0 Apr 2 12:04:03.619: generate hmac context for conn id 14 Apr 2 12:04:03.627: ISAKMP (14): SA has been authenticated Apr 2 12:04:03.627: ISAKMP (14): beginning Quick Mode exchange, M-ID of 1628162439 *!--- These lines represent verification that the policy !--- attributes are fine, and the final authentication of the IKE SA. !--- Once the IKE SA is authenticated, a valid IKE SA exists. !--- New IKE kicks off IPsec negotiation:* Apr 2 12:04:03.635: IPSEC(key_engine): got a queue event... Apr 2 12:04:03.635: IPSEC(spi_response): getting spi 303564824ld for SA .!!!from 20.20.20.21 to 20.20.20.20 for prot 3 Apr 2 12:04:03.639: IPSEC(spi_response): getting spi 423956280ld for SA from 20.20.20.21 to 20.20.20.20 for prot 2 Apr 2 12:04:03.643: IPSEC(spi_response): getting spi 415305621ld for SA from 20.20.20.21 to 20.20.20.20 for prot 3 Apr 2 12:04:03.647: IPSEC(spi_response): getting spi 218308976ld for SA from 20.20.20.21 to 20.20.20.20 for prot 2 Apr 2 12:04:03.891: generate hmac context for conn id 14 Apr 2 12:04:04.!! Success rate is 50 percent (5/10), round-trip min/avg/max = 264/265/268 ms goss-e4-2513#723: generate hmac context for conn id 14 Apr 2 12:04:04.731: ISAKMP (14): processing SA payload. message ID = 1628162439 Apr 2 12:04:04.731: ISAKMP (14): Checking IPSec proposal 1 Apr 2 12:04:04.735: ISAKMP: transform 1, ESP_DES_IV64 Apr 2 12:04:04.735: ISAKMP: attributes in transform: Apr 2 12:04:04.735: ISAKMP: encaps is 1 Apr 2 12:04:04.739: ISAKMP: SA life type in seconds Apr 2 12:04:04.739: ISAKMP: SA life duration (basic) of 190 Apr 2 12:04:04.739: ISAKMP: SA life type in kilobytes Apr 2 12:04:04.743: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 Apr 2 12:04:04.747: ISAKMP (14): atts are acceptable. *!--- The ISAKMP debug is listed because IKE is the !--- entity that negotiates IPsec SAs on behalf of IPsec.* Apr 2 12:04:04.747: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 20.20.20.21, src= 20.20.20.20, dest_proxy= 50.50.50.0/255.255.255.0/0/0 (type=4), src_proxy= 60.60.60.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-rfc1829 , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 Apr 2 12:04:04.759: ISAKMP (14): processing NONCE payload. message ID = 1628162439 Apr 2 12:04:04.759: ISAKMP (14): processing ID payload. message ID = 1628162439 Apr 2 12:04:04.763: ISAKMP (14): processing ID payload. message ID = 1628162439 Apr 2 12:04:04.767: generate hmac context for conn id 14 Apr 2 12:04:04.799: ISAKMP (14): Creating IPSec SAs Apr 2 12:04:04.803: inbound SA from 20.20.20.21 to 20.20.20.20 (proxy 50.50.50.0 to 60.60.60.0) Apr 2 12:04:04.803: has spi 303564824 and conn_id 15 and flags 4 Apr 2 12:04:04.807: lifetime of 190 seconds Apr 2 12:04:04.807: lifetime of 4608000 kilobytes Apr 2 12:04:04.811: outbound SA from 20.20.20.20 to 20.20.20.21 (proxy 60.60.60.0 to 50.50.50.0) Apr 2 12:04:04.811: has spi 183903875 and conn_id 16 and flags 4 Apr 2 12:04:04.815: lifetime of 190 seconds Apr 2 12:04:04.815: lifetime of 4608000 kilobytes Apr 2 12:04:04.823: IPSEC(key_engine): got a queue event... Apr 2 12:04:04.823: IPSEC(initialize_sas): , (key eng. msg.) dest= 20.20.20.20, src= 20.20.20.21, dest_proxy= 60.60.60.0/255.255.255.0/0/0 (type=4), src_proxy= 50.50.50.0/255.255.255.0/0/0 (type=4), protocol= ESP, transform= esp-rfc1829 , lifedur= 190s and 4608000kb, spi= 0x12180818(303564824), conn_id= 15, keysize= 0, flags= 0x4 Apr 2 12:04:04.831: IPSEC(initialize_sas): , (key eng. msg.) src= 20.20.20.20, dest= 20.20.20.21, src_proxy= 60.60.60.0/255.255.255.0/0/0 (type=4), dest_proxy= 50.50.50.0/255.255.255.0/0/0 (type=4), protocol= ESP,

```
transform= esp-rfc1829 , lifedur= 190s and 4608000kb, spi=
0xAF62683(183903875), conn_id= 16, keysize= 0, flags= 0x4 Apr
2 12:04:04.839: IPSEC(create_sa): sa created, (sa) sa_dest=
20.20.20.20, sa_prot= 50, sa_spi= 0x12180818(303564824),
sa_trans= esp-rfc1829 , sa_conn_id= 15 Apr 2 12:04:04.843:
IPSEC(create_sa): sa created, (sa) sa_dest= 20.20.20.21,
sa_prot= 50, sa_spi= 0xAF62683(183903875), sa_trans= esp-
rfc1829 , sa_conn_id= 16 !--- These lines show that IPsec SAs
are created and !--- encrypted traffic can now pass.
```

Show command output (resultado do comando show) do roteador de origem após a negociação IKE/IPsec

```
goss-e4-2513#
goss-e4-2513#show crypto isakmp sa dst src state conn-id slot
20.20.20.21 20.20.20.20 QM_IDLE 14 0 goss-e4-2513#show crypto
ipsec sa interface: Serial0 Crypto map tag: armadillo, local
addr. 20.20.20.20 local ident (addr/mask/prot/port):
(60.60.60.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (50.50.50.0/255.255.255.0/0/0)
current_peer: 20.20.20.21 PERMIT, flags={origin_is_acl,}
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest 0 #pkts
decaps: 5, #pkts decrypt: 5, #pkts verify 0 #send errors 5,
#recv errors 0 local crypto endpt.: 20.20.20.20, remote
crypto endpt.: 20.20.20.21 path mtu 1500, media mtu 1500
current outbound spi: AF62683 inbound esp sas: spi:
0x12180818(303564824) transform: esp-rfc1829 , in use
settings ={Var len IV, Tunnel, } slot: 0, conn id: 15, crypto
map: armadillo sa timing: remaining key lifetime (k/sec):
(4607999/135) IV size: 8 bytes replay detection support: N
inbound ah sas: outbound esp sas: spi: 0xAF62683(183903875)
transform: esp-rfc1829 , in use settings ={Var len IV,
Tunnel, } slot: 0, conn id: 16, crypto map: armadillo sa
timing: remaining key lifetime (k/sec): (4607999/117) IV
size: 8 bytes replay detection support: N outbound ah sas:
goss-e4-2513#show crypto isakmp policy Protection suite of
priority 1 encryption algorithm: DES - Data Encryption
Standard (56 bit keys). hash algorithm: Message Digest 5
authentication method: Pre-Shared Key Diffie-Hellman group:
#1 (768 bit) lifetime: 86400 seconds, no volume limit Default
protection suite encryption algorithm: DES - Data Encryption
Standard (56 bit keys). hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
Diffie-Hellman group: #1 (768 bit) lifetime: 86400 seconds,
no volume limit goss-e4-2513#show crypto map Crypto Map
"armadillo" 1 ipsec-isakmp Peer = 20.20.20.21 Extended IP
access list 101 access-list 101 permit ip 60.60.60.0
0.0.0.255 50.50.50.0 0.0.0.255 Current peer: 20.20.20.21
Security association lifetime: 4608000 kilobytes/190 seconds
PFS (Y/N): N Transform sets={ BearPapa, BearMama, BearBaby, }
```

Roteador de peer com a mesma seqüência de ping, como visto no outro lado

```
goss-c2-2513#show debug Cryptographic Subsystem: Crypto
ISAKMP debugging is on Crypto Engine debugging is on Crypto
IPSEC debugging is on goss-c2-2513# Apr 2 12:03:55.107:
ISAKMP (14): processing SA payload. message ID = 0 Apr 2
12:03:55.111: ISAKMP (14): Checking ISAKMP transform 1
against priority 1 policy Apr 2 12:03:55.111: ISAKMP:
encryption DES-CBC Apr 2 12:03:55.111: ISAKMP: hash MD5 Apr 2
12:03:55.115: ISAKMP: default group 1 Apr 2 12:03:55.115:
ISAKMP: auth pre-share Apr 2 12:03:55.115: ISAKMP (14): atts
are acceptable. Next payload is 0 !--- IKE performs its
operation, and then kicks off IPsec. Apr 2 12:03:55.119:
Crypto engine 0: generate alg param Apr 2 12:03:56.707:
```

```
CRYPTO_ENGINE: Dh phase 1 status: 0 Apr 2 12:03:56.711:
ISAKMP (14): SA is doing pre-shared key authentication Apr 2
12:03:58.667: ISAKMP (14): processing KE payload. message ID
= 0 Apr 2 12:03:58.671: Crypto engine 0: generate alg param
Apr 2 12:04:00.687: ISAKMP (14): processing NONCE payload.
message ID = 0 Apr 2 12:04:00.695: Crypto engine 0: create
ISAKMP SKEYID for conn id 14 Apr 2 12:04:00.707: ISAKMP (14):
SKEYID state generated Apr 2 12:04:00.711: ISAKMP (14):
processing vendor id payload Apr 2 12:04:00.715: ISAKMP (14):
speaking to another IOS box! Apr 2 12:04:03.095: ISAKMP (14):
processing ID payload. message ID = 0 Apr 2 12:04:03.095:
ISAKMP (14): processing HASH payload. message ID = 0 Apr 2
12:04:03.099: generate hmac context for conn id 14 Apr 2
12:04:03.107: ISAKMP (14): SA has been authenticated Apr 2
12:04:03.111: generate hmac context for conn id 14 Apr 2
12:04:03.835: generate hmac context for conn id 14 Apr 2
12:04:03.839: ISAKMP (14): processing SA payload. message ID
= 1628162439 Apr 2 12:04:03.843: ISAKMP (14): Checking IPSec
proposal 1 Apr 2 12:04:03.843: ISAKMP: transform 1,
ESP_DES_IV64 Apr 2 12:04:03.847: ISAKMP: attributes in
transform: Apr 2 12:04:03.847: ISAKMP: encaps is 1 Apr 2
12:04:03.847: ISAKMP: SA life type in seconds Apr 2
12:04:03.851: ISAKMP: SA life duration (basic) of 190 Apr 2
12:04:03.851: ISAKMP: SA life type in kilobytes Apr 2
12:04:03.855: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50
0x0 Apr 2 12:04:03.855: ISAKMP (14): atts are acceptable. Apr
2 12:04:03.859: IPSEC(validate_proposal_request): proposal
part #1, (key eng. msg.) dest= 20.20.20.21, src= 20.20.20.20,
dest_proxy= 50.50.50.0/255.255.255.0/0/0 (type=4), src_proxy=
60.60.60.0/255.255.255.0/0/0 (type=4), protocol= ESP,
transform= esp-rfc1829 , lifedur= 0s and 0kb, spi= 0x0(0),
conn_id= 0, keysize= 0, flags= 0x4 Apr 2 12:04:03.867: ISAKMP
(14): processing NONCE payload. message ID = 1628162439 Apr 2
12:04:03.871: ISAKMP (14): processing ID payload. message ID
= 1628162439 Apr 2 12:04:03.871: ISAKMP (14): processing ID
payload. message ID = 1628162439 Apr 2 12:04:03.879:
IPSEC(key_engine): got a queue event... Apr 2 12:04:03.879:
IPSEC(spi_response): getting spi 183903875ld for SA from
20.20.20.20 to 20.20.20.21 for prot 3 Apr 2 12:04:04.131:
generate hmac context for conn id 14 Apr 2 12:04:04.547:
generate hmac context for conn id 14 Apr 2 12:04:04.579:
ISAKMP (14): Creating IPSec SAs Apr 2 12:04:04.579: inbound
SA from 20.20.20.20 to 20.20.20.21 (proxy 60.60.60.0 to
50.50.50.0) Apr 2 12:04:04.583: has spi 183903875 and conn_id
15 and flags 4 Apr 2 12:04:04.583: lifetime of 190 seconds
Apr 2 12:04:04.587: lifetime of 4608000 kilobytes Apr 2
12:04:04.587: outbound SA from 20.20.20.21 to 20.20.20.20
(proxy 50.50.50.0 to 60.60.60.0) Apr 2 12:04:04.591: has spi
303564824 and conn_id 16 and flags 4 Apr 2 12:04:04.591:
lifetime of 190 seconds Apr 2 12:04:04.595: lifetime of
4608000 kilobytes Apr 2 12:04:04.599: IPSEC(key_engine): got
a queue event... Apr 2 12:04:04.599: IPSEC(initialize_sas): ,
(key eng. msg.) dest= 20.20.20.21, src= 20.20.20.20,
dest_proxy= 50.50.50.0/255.255.255.0/0/0 (type=4), src_proxy=
60.60.60.0/255.255.255.0/0/0 (type=4), protocol= ESP,
transform= esp-rfc1829 , lifedur= 190s and 4608000kb, spi=
0xAF62683(183903875), conn_id= 15, keysize= 0, flags= 0x4 Apr
2 12:04:04.607: IPSEC(initialize_sas): , (key eng. msg.) src=
20.20.20.21, dest= 20.20.20.20, src_proxy=
50.50.50.0/255.255.255.0/0/0 (type=4), dest_proxy=
60.60.60.0/255.255.255.0/0/0 (type=4), protocol= ESP,
transform= esp-rfc1829 , lifedur= 190s and 4608000kb, spi=
0x12180818(303564824), conn_id= 16, keysize= 0, flags= 0x4
Apr 2 12:04:04.615: IPSEC(create_sa): sa created, (sa)
```

```
sa_dest= 20.20.20.21, sa_prot= 50, sa_spi=
0xAF62683(183903875), sa_trans= esp-rfc1829 , sa_conn_id= 15
Apr 2 12:04:04.619: IPSEC(create_sa): sa created, (sa)
sa_dest= 20.20.20.20, sa_prot= 50, sa_spi=
0x12180818(303564824), sa_trans= esp-rfc1829 , sa_conn_id= 16
!--- The IPsec SAs are created, and ICMP traffic can flow.
```

Comandos show de roteadores de peer

```
!--- This illustrates a series of show command output after
!--- IKE/IPsec negotiation takes place. goss-c2-2513#show
crypto isakmp sa dst src state conn-id slot 20.20.20.21
20.20.20.20 QM_IDLE 14 0 goss-c2-2513#show crypto ipsec sa
interface: Serial0 Crypto map tag: armadillo, local addr.
20.20.20.21 local ident (addr/mask/prot/port):
(50.50.50.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (60.60.60.0/255.255.255.0/0/0)
current_peer: 20.20.20.20 PERMIT, flags={origin_is_acl,}
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest 0 #pkts
decaps: 5, #pkts decrypt: 5, #pkts verify 0 #send errors 0,
#recv errors 0 local crypto endpt.: 20.20.20.21, remote
crypto endpt.: 20.20.20.20 path mtu 1500, media mtu 1500
current outbound spi: 12180818 inbound esp sas: spi:
0xAF62683(183903875) transform: esp-rfc1829 , in use settings
={Var len IV, Tunnel, } slot: 0, conn id: 15, crypto map:
armadillo sa timing: remaining key lifetime (k/sec):
(4607999/118) IV size: 8 bytes replay detection support: N
inbound ah sas: outbound esp sas: spi: 0x12180818(303564824)
transform: esp-rfc1829 , in use settings ={Var len IV,
Tunnel, } slot: 0, conn id: 16, crypto map: armadillo sa
timing: remaining key lifetime (k/sec): (4607999/109) IV
size: 8 bytes replay detection support: N outbound ah sas:
goss-c2-2513#show crypto isakmp policy Protection suite of
priority 1 encryption algorithm: DES - Data Encryption
Standard (56 bit keys). hash algorithm: Message Digest 5
authentication method: Pre-Shared Key Diffie-Hellman group:
#1 (768 bit) lifetime: 86400 seconds, no volume limit Default
protection suite encryption algorithm: DES - Data Encryption
Standard (56 bit keys). hash algorithm: Secure Hash Standard
authentication method: Rivest-Shamir-Adleman Signature
Diffie-Hellman group: #1 (768 bit) lifetime: 86400 seconds,
no volume limit goss-c2-2513#show crypto map Crypto Map
"armadillo" 1 ipsec-isakmp Peer = 20.20.20.20 Extended IP
access list 101 access-list 101 permit ip 50.50.50.0
0.0.0.255 60.60.60.0 0.0.0.255 Current peer: 20.20.20.20
Security association lifetime: 4608000 kilobytes/190 seconds
PFS (Y/N): N Transform sets={ MamaBear, PapaBear, BabyBear, }
```

Dicas de implementação para o IPsec

Estes são alguns dicas de implementação para o IPsec:

- Assegure que você tenha a Conectividade entre os valores-limite da comunicação antes que você configure cripto.
- Certifique-se de que o DNS trabalha no roteador, ou você entraram no hostname de CA, se você usa CA.
- O IPsec usa 50 pés e 51 dos protocolos IP, e o tráfego IKE passa sobre o protocolo 17, a porta 500 (UDP 500). Certifique-se que estes estão permitidos apropriadamente.
- Seja cuidadoso não usar a palavra em seu ACL. Isto causa problemas. Refira os Diretriz de

Uso para a **lista de acesso na** referência de comando PIX para mais informação.

- As combinações de transformação recomendadas são:`esp-des and esp-sha-hmac ah-sha-hmac and esp-des`
- Lembre-se de que o AH é apenas um cabeçalho autenticado. O fluxo de dados real do usuário não é cifrado. Você precisa o ESP para a criptografia de fluxo de dados. Se você usa somente o AH e vê o texto não criptografado ir através da rede, não esteja surpreendido. Igualmente use o ESP se você usa o AH. Note que o ESP pode igualmente executar a autenticação. Portanto, é possível utilizar uma combinação de transformação como esp-des e esp-sha-hmac.
- **ah-rfc1828** e **esp-rfc1829** são Obsoletos transformam incluído para para trás a compatibilidade com aplicações mais velhas do IPsec. Se o par não apoia mais novo transforma, tenta estes pelo contrário.
- O SHA é mais lento e mais seguro do que o MD5, visto que o MD5 é mais rapidamente e menos seguro esse SHA. Em algumas comunidades, o conforto em nível com MD5 é muito baixo.
- Em caso de dúvida, modo de túnel do uso. O modo de túnel é o padrão é pode ser usado em modo de transporte bem como para os seus recursos de VPN.
- Para os usuários de criptografia clássica que promovem ao Cisco IOS Software Release 11.3, os métodos do armazenamento dos comandos crypto na configuração mudaram a fim permitir o IPsec. Consequentemente, se os usuários de criptografia clássica revertem nunca ao Cisco IOS Software Release 11.2, estes usuários têm que reenter suas configurações de criptografia.
- Se você faz um teste de ping através do link criptografado quando você termina sua configuração, o processo de negociação pode tomar alguma hora, aproximadamente seis segundos em Cisco4500, e aproximadamente 20 segundos em Cisco2500, porque os SA não foram negociados ainda. Mesmo que tudo seja configurado corretamente, seu sibilo pode inicialmente falhar. **Os comandos debug crypto ipsec e debug crypto isakmp** mostram lhe o que acontece. Uma vez que seus fluxos de dados cifrados terminaram seu estabelecido, o sibilo trabalha muito bem.
- Se você é executado no problema com suas negociações e faz alterações de configuração, use o **cripto claro é** e **comandos clear crypto sa** a fim nivelar os bases de dados antes que você experimente de novo. Isto força a negociação para começar de novo, sem nenhuma negociação legada a obter na maneira. **O cripto claro é** e os **comandos clear cry sa** são muito úteis desse modo.

Links de ajuda e links relevantes

Informação IPSec

- Página de suporte IPSec
- Políticas de criptografia e procedimentos ECRA — Envie um email a export@cisco.com

Mais configurações de amostra para o IPsec

- Configurando e pesquisando defeitos a criptografia de camada de rede de Cisco: IPSec e ISAKMP
- Vista geral da Segurança de rede IPSec

- Documentação da configuração IPSec do PIX FirewallPIX 5.1PIX 5.2PIX 5.3PIX 6.0PIX 6.1PIX 6.2PIX 6.3

Contacte o Suporte técnico de Cisco no (800) 553-24hr, (408) 526-7209, ou envie-o e email a tac@cisco.com se você exige a assistência adicional com IPsec.

Referências

Harkins, *especificação funcional de unidade de software da característica de* D. *ISAKMP/Oakley Protocolo.* Cisco Systems do Rev A. do ENG-0000.

Madson, Cisco Systems do *Rev F. da especificação funcional de unidade de software ENG-17610 de* C. *IPsec*.

Kaufman, C. Perlman R. e Spencer, *segurança de rede* M.*: Uma comunicação privada em um mundo público.* Prentice hall, 1995.

Schneier, *criptografia aplicada* B.*: Protocolos, algoritmos, e código de origem no C.* Em segundo Ed. John wiley & sons, Inc.

Vários trabalhar-esboços da Segurança IP IETF

Informações Relacionadas

- Página de suporte IPSec
- Como as redes privadas virtuais funcionam
- Soluções de Troubleshooting Mais Comuns de VPN IPsec L2L e de Acesso Remoto
- Suporte Técnico e Documentação - Cisco Systems