Configuration et dépannage du chiffrement de couche réseau Cisco Contexte – 1re partie

Contenu

Introduction

Ce document traite de la configuration et du dépannage du cryptage de couche réseau Cisco avec IPSec et l'Internet Security Association and Key Management Protocol (ISAKMP) et couvre les informations de base du cryptage de couche réseau et la configuration de base, ainsi que IPSec et ISAKMP.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur les versions de logiciel et matériel suivantes :

- Logiciel Cisco IOS® version 11.2 et ultérieure

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

Pour plus d'informations sur les conventions des documents, référez-vous aux Conventions utilisées pour les conseils techniques de Cisco.

Informations générales et configuration du chiffrement de la couche réseau

La fonction de chiffrement de la couche réseau a été introduite dans le logiciel Cisco IOS® Version 11.2. Il fournit un mécanisme de transmission sécurisée des données et se compose de deux composants :

- **Authentification du routeur :** Avant de transmettre le trafic chiffré, deux routeurs effectuent une authentification unique et bidirectionnelle à l'aide de clés publiques DSS (Digital Signature Standard) pour signaler des problèmes aléatoires.
- **Cryptage de couche réseau :** Pour le cryptage de données utiles IP, les routeurs utilisent l'échange de clés Diffie-Hellman pour générer en toute sécurité une clé de session DES(40 ou 56 bits), Triple DES - 3DES(168 bits) ou la plus récente norme de cryptage avancé AES (128 bits (par défaut), 192 bits ou clé 256 bits), introduite dans le paragraphe 12.2(13)T. Les nouvelles clés de session sont générées sur une base configurable. La politique de chiffrement est définie par des crypto-cartes qui utilisent des listes d'accès IP étendues pour définir les paires de réseau, de sous-réseau, d'hôte ou de protocole à chiffrer entre les routeurs.

Contexte de la cryptographie

Le domaine de la cryptographie concerne le maintien des communications privées. La protection des communications sensibles a été au coeur de la cryptographie tout au long de son histoire. Le chiffrement est la transformation des données en une forme illisible. Son but est de garantir la confidentialité en gardant les informations cachées de quiconque pour qui elles ne sont pas destinées, même s'ils peuvent voir les données cryptées. Le déchiffrement est l'inverse du chiffrement : c'est la transformation des données chiffrées en une forme intelligible.

Le chiffrement et le déchiffrement nécessitent l'utilisation de certaines informations secrètes, généralement appelées « clés ». Selon le mécanisme de chiffrement utilisé, la même clé peut être utilisée pour le chiffrement et le déchiffrement ; alors que pour d'autres mécanismes, les clés utilisées pour le chiffrement et le déchiffrement peuvent être différentes.

Une signature numérique lie un document au détenteur d'une clé particulière, tandis qu'un horodatage numérique lie un document à sa création à un moment donné. Ces mécanismes

cryptographiques peuvent être utilisés pour contrôler l'accès à un lecteur de disque partagé, à une installation à haute sécurité ou à une chaîne de télévision payante.

Alors que la cryptographie moderne est de plus en plus diversifiée, la cryptographie est fondamentalement basée sur des problèmes difficiles à résoudre. Un problème peut être difficile car sa solution nécessite de connaître la clé, par exemple déchiffrer un message chiffré ou signer un document numérique. Le problème peut également être difficile car il est intrinsèquement difficile de le résoudre, par exemple en trouvant un message qui produit une valeur de hachage donnée.

Àmesure que le domaine de la cryptographie progresse, les lignes de séparation pour ce qui est et ce qui n'est pas de la cryptographie sont devenues floues. La cryptographie d'aujourd'hui pourrait être résumée comme l'étude de techniques et d'applications qui dépendent de l'existence de problèmes mathématiques difficiles à résoudre. Un cryptanalyste tente de compromettre les mécanismes cryptographiques, et la cryptologie est la discipline de la cryptographie et de l'analyse cryptographique combinée.

Définitions

Cette section définit les termes associés utilisés dans ce document.

- **Authentification:** La propriété de savoir que les données reçues sont effectivement envoyées par l'expéditeur revendiqué.
- **Confidentialité :** Propriété de la communication de sorte que les destinataires visés sachent ce qui est envoyé, mais que les tiers non désirés ne puissent pas déterminer ce qui est envoyé.
- **Norme de chiffrement des données (DES) :** Le DES utilise une méthode de clé symétrique, également appelée méthode de clé secrète. Cela signifie que si un bloc de données est chiffré avec la clé, le bloc chiffré doit être déchiffré avec la même clé, de sorte que le crypteur et le décrypteur doivent tous deux utiliser la même clé. Même si la méthode de chiffrement est connue et bien publiée, la méthode d'attaque la plus connue publiquement est la force brute. Les clés doivent être testées par rapport aux blocs chiffrés pour voir si elles peuvent les résoudre correctement. À mesure que les processeurs deviennent plus puissants, la vie naturelle des DES touche à sa fin. Par exemple, un effort coordonné utilisant la puissance de traitement inutilisée de milliers d'ordinateurs sur Internet peut trouver la clé 56 bits d'un message codé DES en 21 jours.Le DES est validé tous les cinq ans par la National Security Agency (NSA) des États-Unis pour répondre aux objectifs du gouvernement américain. L'approbation actuelle expire en 1998 et la NSA a indiqué qu'elle ne recertifierait pas DES. Au-delà des DES, il existe d'autres algorithmes de chiffrement qui ne présentent pas non plus de faiblesses connues autres que les attaques par force brute. Pour de plus amples renseignements, voir DES FIPS 46-2 de l'Institut national des normes et de la technologie (NIST) .
- **Décryptage :** Application inverse d'un algorithme de chiffrement aux données chiffrées, ce qui permet de restaurer ces données dans leur état d'origine non chiffré.
- **DSS et DSA (Digital Signature Algorithm) :** La DSA a été publiée par le NIST dans la Digital Signature Standard (DSS), qui fait partie du projet Capstone du gouvernement américain. Le SSD a été choisi par le NIST, en coopération avec la NSA, comme norme d'authentification numérique du gouvernement américain. La norme a été émise le 19 mai 1994.
- **Chiffrement :** Application d'un algorithme spécifique aux données afin de modifier l'apparence des données, ce qui rend incompréhensible pour ceux qui ne sont pas autorisés à voir les

informations.

- **Intégrité :** Propriété consistant à s'assurer que les données sont transmises de la source à la destination sans altération non détectée.
- **Non-répudiation :** Propriété d'un récepteur capable de prouver que l'expéditeur de certaines données a effectivement envoyé les données, même si l'expéditeur peut ultérieurement refuser d'avoir envoyé ces données.
- **Cryptographie à clé publique :** La cryptographie traditionnelle est basée sur l'expéditeur et le destinataire d'un message connaissant et utilisant la même clé secrète. L'expéditeur utilise la clé secrète pour chiffrer le message, et le destinataire utilise la même clé secrète pour déchiffrer le message. Cette méthode est appelée « clé secrète » ou « cryptographie symétrique ». Le principal problème est de faire en sorte que l'expéditeur et le destinataire s'accordent sur la clé secrète sans que personne d'autre ne le découvre. S'ils se trouvent à des emplacements physiques distincts, ils doivent faire confiance à un service de messagerie, à un système téléphonique ou à un autre moyen de transmission pour empêcher la divulgation de la clé secrète d'être communiquée. Quiconque entend ou intercepte la clé en transit peut lire, modifier et falsifier ultérieurement tous les messages chiffrés ou authentifiés à l'aide de cette clé. La génération, la transmission et le stockage des clés sont appelés gestion des clés ; tous les systèmes de chiffrement doivent gérer les problèmes de gestion des clés. Comme toutes les clés d'un système de chiffrement à clé secrète doivent rester secrètes, la cryptographie à clé secrète a souvent de la difficulté à fournir une gestion des clés sécurisée, en particulier dans les systèmes ouverts avec un grand nombre d'utilisateurs.Le concept de cryptographie à clé publique a été introduit en 1976 par Whitfield Diffie et Martin Hellman afin de résoudre le problème de gestion des clés. Dans leur concept, chaque personne obtient une paire de clés, l'une appelée clé publique et l'autre appelée clé privée. La clé publique de chaque personne est publiée tandis que la clé privée est gardée secrète. La nécessité pour l'expéditeur et le destinataire de partager des informations secrètes est éliminée et toutes les communications ne concernent que les clés publiques, et aucune clé privée n'est jamais transmise ou partagée. Il n'est plus nécessaire de faire confiance à certains canaux de communication pour être sûr contre l'écoute électronique ou la trahison. La seule condition requise est que les clés publiques soient associées à leurs utilisateurs de manière fiable (authentifiée) (par exemple, dans un répertoire approuvé). N'importe qui peut envoyer un message confidentiel simplement en utilisant des informations publiques, mais le message ne peut être décrypté qu'avec une clé privée, qui est en la seule possession du destinataire prévu. En outre, la cryptographie à clé publique peut être utilisée non seulement pour la confidentialité (chiffrement), mais aussi pour l'authentification (signatures numériques).
- **Signatures numériques à clé publique :** Pour signer un message, une personne effectue un calcul impliquant à la fois sa clé privée et le message lui-même. La sortie est appelée signature numérique et est jointe au message, qui est ensuite envoyé. Une deuxième personne vérifie la signature en effectuant un calcul impliquant le message, la prétendue signature et la clé publique de la première personne. Si le résultat tient correctement dans une relation mathématique simple, la signature est vérifiée comme étant authentique. Sinon, la signature peut être frauduleuse ou le message peut avoir été modifié.
- **Chiffrement de clé publique :** Lorsqu'une personne souhaite envoyer un message secret à une autre personne, la première recherche la clé publique de la seconde personne dans un répertoire, l'utilise pour chiffrer le message et l'envoie. La deuxième personne utilise ensuite sa clé privée pour déchiffrer le message et le lire. Personne ne peut déchiffrer le message. N'importe qui peut envoyer un message chiffré à la deuxième personne, mais seule la deuxième peut le lire. Il est évident que personne ne peut trouver la clé privée à partir de la

clé publique correspondante.
- **Analyse du trafic :** Analyse du flux de trafic réseau dans le but de réduire les informations utiles à un adversaire. Les exemples de ces informations sont la fréquence de transmission, les identités des interlocuteurs, la taille des paquets, les identificateurs de flux utilisés, etc.

Informations préliminaires

Cette section traite de certains concepts de base du chiffrement de la couche réseau. Il contient les aspects du chiffrement que vous devez surveiller. Au départ, ces problèmes peuvent ne pas avoir de sens pour vous, mais c'est une bonne idée de les lire maintenant et d'en être conscient car ils auront plus de sens après avoir travaillé avec le chiffrement pendant plusieurs mois.

- Il est important de noter que le chiffrement se produit uniquement sur la sortie d'une interface et que le déchiffrement se produit uniquement sur la saisie de l'interface. Cette distinction est importante lors de la planification de votre politique. La politique de chiffrement et de déchiffrement est symétrique. Cela signifie que définir l'un vous donne l'autre automatiquement. Avec les crypto-cartes et leurs listes d'accès étendues associées, seule la politique de chiffrement est explicitement définie.La stratégie de déchiffrement utilise les mêmes informations, mais lorsqu'elle correspond à des paquets, elle inverse les adresses et les ports source et de destination. De cette manière, les données sont protégées dans les deux directions d'une connexion bidirectionnelle. L'instruction *match address x* de la commande **crypto map** est utilisée pour décrire les paquets quittant une interface. En d'autres termes, il décrit le chiffrement des paquets. Cependant, les paquets doivent également être mis en correspondance pour le déchiffrement lorsqu'ils entrent dans l'interface. Pour ce faire, vous devez parcourir automatiquement la liste de contrôle d'accès avec les adresses source et de destination et les ports inversés. Cela fournit la symétrie pour la connexion. La liste d'accès pointée par la **carte de chiffrement** doit décrire le trafic dans une seule direction (sortant). Les paquets IP qui ne correspondent pas à la liste d'accès que vous définissez seront transmis, mais non chiffrés. Un refus dans la liste d'accès indique que ces hôtes ne doivent pas être associés, ce qui signifie qu'ils ne seront pas chiffrés. Dans ce contexte, le refus ne signifie pas que le paquet est abandonné.
- Faites très attention à utiliser le mot « any » dans les listes de contrôle d'accès étendues. L'utilisation de « any » entraîne l'abandon de votre trafic à moins qu'il ne soit dirigé vers l'interface correspondante de « non-chiffrement ». En outre, avec l'IPSec dans le logiciel Cisco IOS Version 11.3(3)T, « any » n'est pas autorisé.
- L'utilisation du mot clé « any » est déconseillée lors de la spécification des adresses source ou de destination. La spécification de « any » peut entraîner des problèmes avec les protocoles de routage, le protocole NTP (Network Time Protocol), l'écho, la réponse d'écho et le trafic de multidiffusion, car le routeur récepteur rejette silencieusement ce trafic. Si « any » doit être utilisé, il doit être précédé par des instructions « deny » pour le trafic qui ne doit pas être chiffré, comme « ntp ».
- Pour gagner du temps, assurez-vous que vous pouvez **envoyer une requête ping** au routeur homologue avec lequel vous essayez d'avoir une association de cryptage. Demandez également aux périphériques finaux (qui dépendent de la cryptage de leur trafic) de s'envoyer des requêtes ping avant de passer trop de temps à résoudre le mauvais problème. En d'autres termes, assurez-vous que le routage fonctionne avant d'essayer de faire **du chiffrement**. L'homologue distant ne dispose peut-être pas d'une route pour l'interface de sortie, auquel cas vous ne pouvez pas avoir de session de chiffrement avec cet homologue

(vous pouvez utiliser **ip unnumbered** sur cette interface série).

- De nombreuses liaisons point à point WAN utilisent des adresses IP non routables, et le cryptage de la version 11.2 du logiciel Cisco IOS repose sur le protocole ICMP (Internet Control Message Protocol) (ce qui signifie qu'il utilise l'adresse IP de l'interface série de sortie pour ICMP). Cela peut vous forcer à utiliser **ip unnumbered** sur l'interface WAN. Exécutez toujours une commande **ping** et **traceroute** pour vous assurer que le routage est en place pour les deux routeurs d'appairage (chiffrement/déchiffrement).
- Seuls deux routeurs sont autorisés à partager une clé de session Diffie-Hellman. Autrement dit, un routeur ne peut pas échanger des paquets chiffrés avec deux homologues utilisant la même clé de session ; chaque paire de routeurs doit avoir une clé de session qui résulte d'un échange Diffie-Hellman entre eux.
- Le moteur de chiffrement se trouve soit dans Cisco IOS, le VIP2 Cisco IOS, soit dans le matériel de la carte de services de chiffrement (ESA) sur un VIP2. Sans VIP2, le moteur de chiffrement Cisco IOS régit la politique de chiffrement sur tous les ports. Sur les plates-formes utilisant le VIP2, il existe plusieurs moteurs de chiffrement : un dans Cisco IOS et un sur chaque VIP2. Le moteur de chiffrement d'un VIP2 régit le chiffrement sur les ports qui résident sur la carte.
- Assurez-vous que le trafic est configuré pour arriver à une interface prête à le chiffrer. Si le trafic peut d'une manière ou d'une autre arriver sur une interface autre que celle avec la **carte de chiffrement** appliquée, il est abandonné en silence.
- Il permet d’avoir un accès console (ou alternatif) aux deux routeurs lors de l’échange de clés ; il est possible de suspendre le côté passif en attendant une clé.
- Le **cfb-64** est plus efficace à traiter que **cfb-8** en termes de charge CPU.
- Le routeur doit exécuter l'algorithme que vous voulez utiliser avec le mode de chiffrement-retour (CFB) que vous voulez utiliser ; les valeurs par défaut de chaque image sont le nom de l'image (comme « 56 ») avec **cfb-64**.
- Envisagez de modifier le délai d'attente des clés. La valeur par défaut de 30 minutes est très courte. Essayez de le porter à un jour (1 440 minutes).
- Le trafic IP est abandonné lors de la renégociation de clé chaque fois que la clé expire.
- Sélectionnez uniquement le trafic que vous voulez réellement chiffrer (ce qui permet d'éviter les cycles de processeur).
- Avec le routage à établissement de connexion à la demande (DDR), rendez le protocole ICMP intéressant ou il ne sortira jamais.
- Si vous voulez chiffrer le trafic autre que IP, utilisez un tunnel. Avec les tunnels, appliquez les crypto-cartes aux interfaces physiques et de tunnel. Voir l'exemple 5 : Chiffrement du trafic IPX dans un tunnel IP pour plus d'informations.
- Les deux routeurs homologues de chiffrement n'ont pas besoin d'être connectés directement.
- Un routeur bas de gamme peut vous envoyer un message de « hog CPU ». Ceci peut être ignoré car il vous dit que le chiffrement utilise beaucoup de ressources CPU.
- Ne placez pas les routeurs de chiffrement de manière redondante afin de déchiffrer et de rechiffrer le trafic et le processeur de gaspillage. Chiffrez simplement aux deux points d'extrémité. Voir Exemple 3 : Chiffrement vers et via un routeur pour plus d'informations.
- Actuellement, le chiffrement des paquets de diffusion et de multidiffusion n'est pas pris en charge. Si des mises à jour de routage « sécurisées » sont importantes pour la conception d'un réseau, un protocole avec authentification intégrée doit être utilisé, tel que le protocole EIGRP (Enhanced Interior Gateway Routing Protocol), OSPF (Open Shortest Path First) ou RIPv2 (Routing Information Protocol Version 2) pour garantir l'intégrité des mises à jour.

Cavates

Note : Les Caveats mentionnés ci-dessous ont tous été résolus.

- Un routeur Cisco 7200 utilisant un ESA pour le chiffrement ne peut pas déchiffrer un paquet sous une clé de session et le rechiffrer ensuite sous une autre clé de session. Référez-vous à l'ID de bogue Cisco CSCdj82613 (clients enregistrés uniquement).
- Lorsque deux routeurs sont connectés par une ligne louée cryptée et une ligne de secours RNIS, si la ligne louée tombe en panne, la liaison RNIS s'active correctement. Cependant, lorsque la ligne louée redémarre, le routeur qui a placé l'appel RNIS tombe en panne. Référez-vous à l'ID de bogue Cisco CSCdj00310 (clients enregistrés uniquement).
- Pour les routeurs de la gamme Cisco 7500 avec plusieurs VIP, si une **crypto-carte** est appliquée à une seule interface d'un VIP, à un ou plusieurs VIP s'écrasent. Référez-vous à l'ID de bogue Cisco CSCdi88459 (clients enregistrés uniquement).
- Pour les routeurs de la gamme Cisco 7500 dotés d'un VIP2 et d'un ESA, la commande **show crypto card** n'affiche pas le résultat, sauf si l'utilisateur se trouve sur le port de console. Référez-vous à l'ID de bogue Cisco CSCdj89070 (clients enregistrés uniquement).

Configuration du chiffrement de la couche réseau Cisco IOS

Les exemples de configuration de Cisco IOS dans ce document proviennent directement des routeurs des travaux pratiques. La seule modification qui leur a été apportée a été la suppression de configurations d'interface non liées. Tous les documents présentés ici proviennent de ressources disponibles gratuitement sur Internet ou dans la section Informations connexes à la fin de ce document.

Tous les exemples de configuration de ce document proviennent du logiciel Cisco IOS Version 11.3. Plusieurs modifications ont été apportées aux commandes de la version 11.2 du logiciel Cisco IOS, telles que l'ajout des mots suivants :

- dss dans certaines commandes de configuration de clé.
- cisco dans certaines des commandes **show** et les commandes **crypto map** pour distinguer le chiffrement propriétaire de Cisco (tel que trouvé dans le logiciel Cisco IOS Version 11.2 et ultérieure) et IPSec qui se trouve dans le logiciel Cisco IOS Version 11.3(2)T.

Remarque : les adresses IP utilisées dans ces exemples de configuration ont été choisies aléatoirement dans les travaux pratiques de Cisco et sont destinées à être entièrement génériques.

Étape 1 : Générer manuellement des paires de clés DSS

Une paire de clés DSS (clé publique et clé privée) doit être générée manuellement sur chaque routeur participant à la session de cryptage. En d'autres termes, chaque routeur doit avoir ses propres clés DSS pour pouvoir participer. Un moteur de cryptage ne peut avoir qu'une seule clé DSS qui l'identifie de manière unique. Le mot clé « dss » a été ajouté dans le logiciel Cisco IOS Version 11.3 afin de distinguer les clés DSS des clés RSA. Vous pouvez spécifier n'importe quel nom pour les propres clés DSS du routeur (bien qu'il soit recommandé d'utiliser le nom d'hôte du routeur). Sur un processeur moins puissant (tel que la gamme Cisco 2500), la génération de paires de clés prend environ 5 secondes ou moins.

Le routeur génère une paire de clés :

- Une clé publique (qui est ensuite envoyée aux routeurs participant aux sessions de cryptage).
- Une clé privée (qui n'est ni vue ni échangée avec personne d'autre ; en fait, il est stocké dans une section distincte de la mémoire vive non volatile (NVRAM).

Une fois que la paire de clés DSS du routeur a été générée, elle est associée de manière unique au moteur de chiffrement de ce routeur. La génération de paires de clés est présentée dans l'exemple de résultat de commande ci-dessous.

```
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#
```

Étant donné que vous ne pouvez générer qu'une seule paire de clés qui identifie le routeur, vous pouvez remplacer votre clé d'origine et devoir renvoyer votre clé publique avec chaque routeur de l'association de cryptage. Ceci est montré dans l'exemple de sortie de commande ci-dessous :

```
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.
```

Étape 2 : Échange manuel des clés publiques DSS avec des homologues (hors bande)

La création de la paire de clés DSS du routeur constitue la première étape de l'établissement d'une association de session de chiffrement. L'étape suivante consiste à échanger des clés publiques avec tous les autres routeurs. Vous pouvez entrer ces clés publiques manuellement en entrant d'abord la commande **show crypto mypubkey** pour afficher la clé publique DSS du routeur.

Vous échangez ensuite ces clés publiques (par e-mail, par exemple) et, avec la commande **crypto key pubkey-chain dss**, coupez et collez la clé publique de votre routeur homologue dans le routeur.

Vous pouvez également utiliser la commande **crypto key exchange dss** pour que les routeurs échangent automatiquement des clés publiques. Si vous utilisez la méthode automatisée, assurez-vous qu'il n'y a aucune instruction **crypto map** sur les interfaces utilisées pour l'échange de clés. Une **clé de chiffrement de débogage** est utile ici.

Remarque : Il est recommandé d'**envoyer une requête ping à** votre homologue avant d'essayer d'échanger des clés.

```
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#
```

Maintenant que les clés DSS publiques ont été échangées, assurez-vous que les deux routeurs ont les clés publiques de l'autre et qu'elles correspondent, comme indiqué dans le résultat de la commande ci-dessous.

```
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
```

Exemple 1 : Configuration de Cisco IOS pour liaison dédiée

Une fois les clés DSS générées sur chaque routeur et les clés publiques DSS échangées, la commande **crypto map** peut être appliquée à l'interface. La session de chiffrement commence par générer du trafic correspondant à la liste d'accès utilisée par les cartes de chiffrement.

```
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#
```

Exemple 2 : Configuration de Cisco IOS pour Multipoint Frame Relay

L'exemple de sortie de commande suivant a été extrait du routeur 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#
```

L'exemple de sortie de commande suivant a été extrait du site distant 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#
```

L'exemple de sortie de commande suivant a été extrait du site distant 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#
```

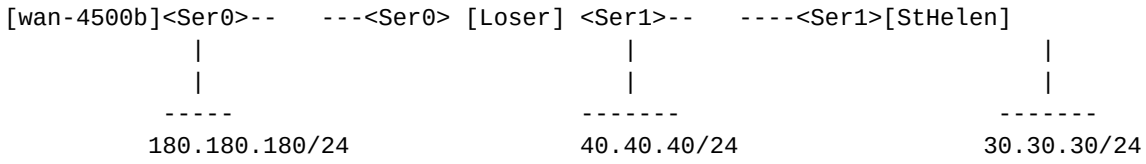
L’exemple de résultat suivant a été extrait du commutateur Frame Relay.

```
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
!
```

Exemple 3 : Chiffrement vers et via un routeur

Les routeurs homologues ne doivent pas être distants d'un saut. Vous pouvez créer une session d'appairage avec un routeur distant. Dans l'exemple suivant, l'objectif est de chiffrer tout le trafic réseau entre 180.180.180.0/24 et 40.40.40.0/24 et entre 180.180.180.0/24 et 30.30.30.0/24. Le chiffrement du trafic entre 40.40.40.0/24 et 30.30.30.0/24 ne pose aucun problème.

Le routeur wan-4500b possède une session de cryptage associée à Loser et également à StHelen. En chiffrant le trafic du segment Ethernet du wan-4500b au segment Ethernet de Sainte-Hélène, vous évitez l'étape de déchiffrement inutile à Loser. Loser transmet simplement le trafic chiffré à l'interface série de Sainte-Hélène, où il est déchiffré. Cela réduit le délai de trafic pour les paquets IP et les cycles CPU sur le routeur Loser. Plus important encore, cela augmente considérablement la sécurité du système, car un écouteur à Loser ne peut pas lire le trafic. Si Loser déchiffrait le trafic, il y aurait une chance que les données déchiffrées puissent être détournées.




```
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#
```

Exemple 4 : Crypto avec DDR

Puisque Cisco IOS s'appuie sur l'ICMP pour établir des sessions de cryptage, le trafic ICMP doit être classé comme intéressant dans la liste de numérotation lors du cryptage sur une liaison DDR.

Remarque : La compression fonctionne dans le logiciel Cisco IOS Version 11.3, mais elle n'est pas très utile pour les données chiffrées. Comme les données chiffrées sont assez aléatoires, la compression ne fait que ralentir les choses. Mais vous pouvez laisser la fonctionnalité activée pour le trafic non chiffré.

Dans certains cas, vous devrez effectuer une sauvegarde par numérotation sur le même routeur. Par exemple, il est utile lorsque les utilisateurs veulent se protéger contre la défaillance d'une liaison particulière dans leurs réseaux WAN. Si deux interfaces vont vers le même homologue, la même crypto-carte peut être utilisée sur les deux interfaces. L'interface de sauvegarde doit être utilisée pour que cette fonctionnalité fonctionne correctement. Si une conception de sauvegarde comporte une numérotation de routeur dans une autre boîte, différentes crypto-cartes doivent être créées et les homologues définis en conséquence. Là encore, la commande **backup interface** doit être utilisée.

```
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#
```

Exemple 5 : Chiffrement du trafic IPX dans un tunnel IP

Dans cet exemple, le trafic IPX dans un tunnel IP est chiffré.

Remarque : seul le trafic de ce tunnel (IPX) est chiffré. Tout autre trafic IP est laissé seul.

```
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#
```

Exemple 6 : Chiffrement des tunnels L2F

Dans cet exemple, seule la tentative de chiffrement du trafic L2F pour les utilisateurs entrant est effectuée. Ici, "user@cisco.com" appelle le serveur d'accès réseau local (NAS) nommé « DEMO2 » dans sa ville et est tunnelisé vers le CD de la passerelle domestique. Tout le trafic DEMO2 (ainsi que celui des autres appelants L2F) est chiffré. Puisque L2F utilise le port UDP 1701, c'est ainsi que la liste d'accès est construite, déterminant quel trafic est chiffré.

Remarque : si l'association de cryptage n'est pas déjà configurée, c'est-à-dire que l'appelant est la première personne à appeler et à créer le tunnel L2F, l'appelant peut être abandonné en raison du délai de configuration de l'association de cryptage. Cela peut ne pas se produire sur les routeurs dotés d'une puissance processeur suffisante. En outre, vous pouvez augmenter le **délai d'attente des clés** de sorte que la configuration et le démontage du chiffrement ne se produisent que pendant les heures creuses.

L'exemple de sortie de commande suivant a été extrait du NAS distant.

```
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#
```

L'exemple de sortie de commande suivant a été extrait de la passerelle Home.

```
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
```

Dépannage

Il est généralement préférable de commencer chaque session de dépannage en recueillant des informations à l'aide des commandes **show** suivantes. Un astérisque (*) indique une commande particulièrement utile. Consultez également Dépannage de la sécurité IP - Compréhension et utilisation des commandes de débogage pour plus d'informations.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

Note : Avant d'émettre des commandes **debug**, consultez Informations importantes sur les commandes de débogage.

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

- **show crypto cisco algorithmes**- Vous devez activer tous les algorithmes DES (Data Encryption Standard) utilisés pour communiquer avec tout autre routeur de chiffrement homologue. Si vous n'activez pas d'algorithme DES, vous ne pourrez pas utiliser cet algorithme, même si vous essayez d'attribuer l'algorithme à une **crypto-carte** ultérieurement.Si votre routeur tente de configurer une session de communication chiffrée avec un routeur homologue et que les deux routeurs n'ont pas le même algorithme DES activé aux deux extrémités, la session chiffrée échoue. Si au moins un algorithme DES commun est activé aux deux extrémités, la session chiffrée peut continuer.**Remarque :** le mot supplémentaire cisco apparaît dans le logiciel Cisco IOS Version 11.3 et est nécessaire pour distinguer le chiffrement IPSec du chiffrement propriétaire Cisco figurant dans le logiciel Cisco IOS Version 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** - Une fois qu'une session de communication chiffrée est établie, elle est valide pour une durée spécifique. Après cette durée, la session expire. Une nouvelle session doit être négociée et une nouvelle clé DES (session) doit être générée pour que la communication chiffrée puisse continuer. Utilisez cette commande pour modifier l'heure de durée d'une session de communication chiffrée avant son expiration.

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

Utilisez ces commandes pour déterminer la durée avant la renégociation des clés DES.

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


StHelen#show crypto key
```

```
Session keys will be re-negotiated every 30 minutes

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

- **show crypto cisco pregen-dh-paires** - Chaque session cryptée utilise une paire unique de numéros DH. Chaque fois qu'une nouvelle session est établie, de nouvelles paires de numéros DH doivent être générées. Une fois la session terminée, ces numéros sont ignorés. La génération de nouvelles paires de numéros DH est une activité gourmande en CPU, qui peut ralentir la configuration des sessions, en particulier pour les routeurs bas de gamme.Pour accélérer la configuration de la session, vous pouvez choisir d'avoir un nombre spécifié de paires de numéros DH prégénérées et conservées en réserve. Ensuite, lorsqu'une session de communication chiffrée est configurée, une paire de numéros DH est fournie à partir de cette réserve. Après l'utilisation d'une paire de numéros DH, la réserve est automatiquement réapprovisionnée avec une nouvelle paire de numéros DH, de sorte qu'il y a toujours une paire de numéros DH prête à être utilisée.Il n'est généralement pas nécessaire d'avoir plus d'une ou deux paires de numéros DH prégénérées, sauf si votre routeur configure plusieurs sessions cryptées si fréquemment qu'une réserve prégénérée d'une ou deux paires de numéros DH est épuisée trop rapidement.
```
Loser#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 10
```
- **show crypto cisco connections active**Voici un exemple de sortie de commande.
```
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**Voici un exemple de sortie de commande.
```
Loser#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

Serial1              19.19.19.19   39
```
- **show crypto engine configuration** (était **show crypto engine brief** dans le logiciel Cisco IOS Version 11.2)Voici un exemple de sortie de commande.
```
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**Voici un exemple de sortie de commande.
```
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**Voici un exemple de sortie de commande.
```
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**Voici un exemple de sortie de commande.
```
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
```

Notez la disparité de temps lorsque vous utilisez la commande **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**Voici un exemple de sortie de commande.

```
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**Voici un exemple de sortie de commande.

```
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**Voici un exemple de sortie de commande.

```
StHelen#debug crypto sessmgmt

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

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

Si l'homologue défini sur la carte de chiffrement est incorrect, vous recevez ce message d'erreur.

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

Si les algorithmes de chiffrement ne correspondent pas, vous recevez ce message d'erreur.

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

Si la clé DSS est manquante ou non valide, vous recevez ce message d'erreur.

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

- **debug crypto key**Voici un exemple de sortie de commande.

```
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**Voici un exemple de sortie de commande.

```
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**Voici un exemple de sortie de commande.

```
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**Voici un exemple de sortie de commande.

```
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#
```

Dépannage de Cisco 7200 avec ESA

Cisco propose également une option d'assistance matérielle pour le cryptage sur les routeurs de la gamme Cisco 7200, appelée ESA. L'ESA prend la forme d'une carte de port pour la carte VIP2-40 ou d'une carte de port autonome pour le Cisco 7200. Cette disposition permet l'utilisation d'un adaptateur matériel ou du moteur logiciel VIP2 pour chiffrer et déchiffrer les données qui entrent dans les interfaces de la carte VIP2 Cisco 7500 ou qui en sortent. Le Cisco 7200 permet une assistance matérielle pour chiffrer le trafic de toutes les interfaces du châssis Cisco 7200. L'utilisation d'une aide au chiffrement permet d'enregistrer des cycles CPU précieux qui peuvent être utilisés à d'autres fins, telles que le routage ou l'une des autres fonctions de Cisco IOS.

Sur un Cisco 7200, la carte de port autonome est configurée exactement de la même manière que le moteur de chiffrement du logiciel Cisco IOS, mais comporte quelques commandes supplémentaires qui sont uniquement utilisées pour le matériel et pour décider quel moteur (logiciel ou matériel) fera le cryptage.

Commencez par préparer le routeur au cryptage matériel :

```
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]
```

Activez ou désactivez le chiffrement matériel comme indiqué ci-dessous :

```
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.
```

Ensuite, générez des clés pour l'ESA avant de l'activer.

```
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#
```

Dépannage de VIP2 avec ESA

La carte de port matérielle ESA de la carte VIP2 est utilisée pour chiffrer et déchiffrer les données qui entrent dans les interfaces de la carte VIP2 ou qui en sortent. Comme pour le Cisco 7200, l'utilisation d'une assistance de cryptage permet d'économiser de précieux cycles de processeur. Dans ce cas, la commande **crypto esa enable** n'existe pas, car la carte de ports ESA effectue le chiffrement des ports de la carte VIP2 si le ESA est branché. Le **crypto clear-loch** doit être appliqué à ce logement si la carte de port ESA vient d'être installée pour la première fois, ou retirée puis réinstallée.

```
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#
```

Comme le module de chiffrement ESA a été extrait, vous obtiendrez le message d'erreur suivant jusqu'à ce que vous fassiez une commande **crypto clear-loch** sur ce logement, comme indiqué ci-dessous.

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

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

Si vous oubliez un mot de passe précédemment assigné, utilisez la commande **crypto zeroize** au lieu de la commande **crypto clear-loch** pour réinitialiser l'ESA. Après avoir exécuté la commande **crypto zeroize**, vous devez régénérer et rééchanger les clés DSS. Lorsque vous régénérez des clés DSS, vous êtes invité à créer un nouveau mot de passe. Un exemple est présenté ci-dessous.

```
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#
```

Informations connexes

- Configuration et dépannage du chiffrement de couche réseau Cisco IPSec et ISAKMP - Partie 2
- DES FIPS 46-2 à l'Institut national des normes et de la technologie (NIST)
- DSS FIPS 186 à l'Institut national des normes et de la technologie (NIST)
- Foire aux questions des laboratoires RSA sur la cryptographie d'aujourd'hui
- Normes de sécurité IETF
- Configuration du protocole IKE (Internet Key Exchange)
- Configuration de la sécurité des réseaux IPSec
- Page d'assistance IPsec
- Support technique - Cisco Systems