Konfiguration und Fehlerbehebung bei Cisco Network Layer Encryption: Hintergrund - Teil 1

Inhalt

Einführung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Hintergrundinformationen und Konfiguration zur Verschlüsselung auf Netzwerkebene
Kryptografischer Hintergrund
Definitionen
Vorläufige Informationen
Einsprüche
Cisco IOS Verschlüsselungskonfiguration auf Netzwerkebene
Schritt 1: Manuelles Generieren von DSS-Schlüsselpaaren
Schritt 2: Manueller Austausch der öffentlichen DSS-Schlüssel mit Peers (Out-of-Band)
Beispiel 1: Cisco IOS-Konfiguration für dedizierte Verbindung
Beispiel 2: Cisco IOS-Konfiguration für Multipoint Frame Relay
Beispiel 3: Verschlüsselung für und über einen Router
Beispiel 4: Verschlüsselung mit DDR
Beispiel 5: Verschlüsselung des IPX-Datenverkehrs in einem IP-Tunnel
Beispiel 6: Verschlüsseln von L2F-Tunneln
Fehlerbehebung
Fehlerbehebung beim Cisco 7200 mit ESA
Fehlerbehebung bei VIP2 mit ESA
Zugehörige Informationen

Einführung

In diesem Dokument wird die Konfiguration und Fehlerbehebung von Cisco Network-Layer Encryption mit IPSec und Internet Security Association und Key Management Protocol (ISAKMP) beschrieben. Darüber hinaus werden Hintergrundinformationen zur Verschlüsselung auf Netzwerkebene sowie die grundlegende Konfiguration zusammen mit IPSec und ISAKMP behandelt.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den Versionen Software und Hardware:

- Cisco IOS® Softwareversion 11.2 und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Hintergrundinformationen und Konfiguration zur Verschlüsselung auf Netzwerkebene

Die Verschlüsselungsfunktion auf Netzwerkebene wurde in Version 11.2 der Cisco IOS®-Software eingeführt. Es bietet einen Mechanismus für die sichere Datenübertragung und besteht aus zwei Komponenten:

- **Router-Authentifizierung:** Vor der Weiterleitung von verschlüsseltem Datenverkehr führen zwei Router eine einmalige Zwei-Wege-Authentifizierung mithilfe von öffentlichen DDSS-Schlüsseln (Digital Signature Standard) durch, um zufällige Herausforderungen zu signieren.
- **Verschlüsselung auf Netzwerkebene:** Für die IP-Nutzlastverschlüsselung verwenden die Router den Diffie-Hellman-Schlüsselaustausch, um sicher einen DES-(40- oder 56-Bit-Sitzungsschlüssel), Triple DES-3DES(168-Bit) oder den neueren Advanced Encryption Standard- AES(128-Bit(Standard)- oder 192-Bit- oder 256-Bit-Schlüssel zu generieren. in 12.2(13)T. Neue Sitzungsschlüssel werden konfigurierbar generiert. Die Verschlüsselungsrichtlinie wird durch Crypto-Maps festgelegt, die erweiterte IP-Zugriffslisten verwenden, um festzulegen, welche Netzwerk-, Subnetz-, Host- oder Protokollpaare zwischen Routern verschlüsselt werden sollen.

Kryptografischer Hintergrund

Im Bereich der Kryptografie geht es darum, die Kommunikation privat zu halten. Der Schutz vertraulicher Kommunikation war in der Geschichte des Landes der Schwerpunkt der Kryptografie. Verschlüsselung ist die Umwandlung von Daten in ein unlesbares Formular. Der Zweck besteht darin, die Privatsphäre zu gewährleisten, indem die Informationen vor Personen verborgen bleiben, für die sie nicht bestimmt sind, selbst wenn sie die verschlüsselten Daten sehen können. Die Entschlüsselung ist die umgekehrte Verschlüsselung: Es ist die Umwandlung verschlüsselter Daten zurück in eine verständliche Form.

Verschlüsselung und Entschlüsselung erfordern die Verwendung einiger geheimer Informationen, die in der Regel als "Schlüssel" bezeichnet werden. Je nach verwendetem

Verschlüsselungsmechanismus kann derselbe Schlüssel sowohl für die Verschlüsselung als auch für die Entschlüsselung verwendet werden. Während bei anderen Mechanismen die Schlüssel für Verschlüsselung und Entschlüsselung unterschiedlich sein können.

Eine digitale Signatur bindet ein Dokument an den Besitzer eines bestimmten Schlüssels, während ein digitaler Zeitstempel ein Dokument zu einem bestimmten Zeitpunkt an seine Erstellung bindet. Mithilfe dieser kryptografischen Mechanismen kann der Zugriff auf ein gemeinsam genutztes Laufwerk, eine Hochsicherheitsinstallation oder einen Pay-per-View-Fernsehkanal gesteuert werden.

Während die moderne Kryptografie immer vielfältiger wird, beruht die Kryptografie im Wesentlichen auf schwer zu lösenden Problemen. Ein Problem kann schwierig sein, da für seine Lösung die Kenntnis des Schlüssels erforderlich ist, z. B. das Entschlüsseln einer verschlüsselten Nachricht oder das Signieren eines digitalen Dokuments. Das Problem kann auch schwierig sein, weil es von Natur aus schwierig zu bewältigen ist, z. B. eine Nachricht zu finden, die einen bestimmten Hash-Wert erzeugt.

Im Bereich der Kryptografie haben sich die Trennlinien für das, was ist und was nicht Kryptografie ist, verwischt. Die Kryptografie von heute könnte als die Erforschung von Techniken und Anwendungen zusammengefasst werden, die von der Existenz mathematischer Probleme abhängen, die schwer zu lösen sind. Ein Kryptoanalyst versucht, kryptografische Mechanismen zu kompromittieren, und Kryptographie ist die Disziplin der Kryptografie und Kryptoanalyse zusammen.

Definitionen

In diesem Abschnitt werden die in diesem Dokument verwendeten Begriffe definiert.

- **Authentifizierung:** Die Eigenschaft, zu wissen, dass die empfangenen Daten tatsächlich vom angegebenen Absender gesendet werden.
- **Vertraulichkeit:** Die Eigenschaft der Kommunikation, sodass die beabsichtigten Empfänger wissen, was gesendet wird, aber unbeabsichtigte Parteien nicht bestimmen können, was gesendet wird.
- **DES (Data Encryption Standard):** DES verwendet eine symmetrische Schlüsselmethode, die auch als geheime Schlüsselmethode bezeichnet wird. Das bedeutet, dass bei der Verschlüsselung eines Datenblocks mit dem Schlüssel der verschlüsselte Block mit demselben Schlüssel entschlüsselt werden muss, sodass sowohl der Verschlüsseler als auch der Entschlüsseler denselben Schlüssel verwenden müssen. Obwohl die Verschlüsselungsmethode bekannt und gut veröffentlicht ist, ist die beste öffentlich bekannte Angriffsmethode Brute Force. Schlüssel müssen gegen die verschlüsselten Blöcke getestet werden, um festzustellen, ob sie sie korrekt beheben können. Mit der zunehmenden Leistungsfähigkeit von Prozessoren nähert sich das Leben des DES seinem Ende. So kann beispielsweise der 56-Bit-Schlüssel für eine DES-codierte Nachricht innerhalb von 21 Tagen bei koordinierter Anstrengung mithilfe von Ersatzleistung von Tausenden von Computern im Internet gefunden werden.DES wird alle fünf Jahre von der US National Security Agency (NSA) für die Zwecke der US-Regierung validiert. Die aktuelle Genehmigung läuft 1998 aus und die NSA hat angegeben, dass sie DES nicht erneut zertifizieren wird. Abgesehen von DES gibt es andere Verschlüsselungsalgorithmen, für die außer Brute-Force-Angriffen auch keine anderen bekannten Schwächen bekannt sind. Weitere Informationen finden Sie unter DES FIPS 46-2 des National Institute of Standards and Technology (NIST) .

- **Entschlüsselung:** Die umgekehrte Anwendung eines Verschlüsselungsalgorithmus auf verschlüsselte Daten, wodurch diese Daten in ihren ursprünglichen, unverschlüsselten Zustand zurückgesetzt werden.
- **DSS und DSA (Digital Signature Algorithm):** Die DSA wurde vom NIST im Digital Signature Standard (DSS) veröffentlicht, der Teil des Capstone-Projekts der US-Regierung ist. DSS wurde von NIST in Zusammenarbeit mit der NSA als digitaler Authentifizierungsstandard der US-Regierung ausgewählt. Der Standard wurde am 19. Mai 1994 veröffentlicht.
- **Verschlüsselung:** Die Anwendung eines bestimmten Algorithmus auf Daten, um das Aussehen der Daten zu verändern, sodass es für diejenigen, die nicht autorisiert sind, die Informationen zu sehen, unverständlich wird.
- **Integrität:** Die Eigenschaft, sicherzustellen, dass Daten ohne unerkannte Änderungen von der Quelle an das Ziel übertragen werden.
- **Nichtabstreitbarkeit:** Die Eigenschaft eines Empfängers, nachweisen zu können, dass der Absender einiger Daten die Daten tatsächlich gesendet hat, obwohl der Absender später versuchen könnte, die Übermittlung dieser Daten zu verweigern.
- **Public-Key-Verschlüsselung:** Herkömmliche Verschlüsselung basiert auf dem Absender und Empfänger einer Nachricht, der denselben geheimen Schlüssel kennt und verwendet. Der Absender verwendet den geheimen Schlüssel zur Verschlüsselung der Nachricht, und der Empfänger verwendet denselben geheimen Schlüssel zur Entschlüsselung der Nachricht. Diese Methode wird als "geheimer Schlüssel" oder "symmetrische Kryptografie" bezeichnet. Das Hauptproblem besteht darin, Absender und Empfänger dazu zu bringen, sich auf den geheimen Schlüssel zu einigen, ohne dass sonst jemand etwas herausfindet. Befinden sie sich an unterschiedlichen physischen Standorten, müssen sie einem Kurier, einem Telefonsystem oder einem anderen Übertragungsmedium vertrauen, um die Offenlegung des geheimen Schlüssels zu verhindern. Jeder, der den Schlüssel bei der Übertragung überhört oder abfängt, kann später alle Nachrichten lesen, ändern und fälschen, die mit diesem Schlüssel verschlüsselt oder authentifiziert wurden. Die Generierung, Übertragung und Speicherung von Schlüsseln wird als Schlüsselverwaltung bezeichnet. Alle Kryptosysteme müssen sich mit wichtigen Managementproblemen befassen. Da alle Schlüssel in einem geheimen Schlüssel-Kryptosystem geheim bleiben müssen, gestaltet sich die sichere Schlüsselverwaltung durch geheime Schlüsselverschlüsselung häufig schwierig, insbesondere in offenen Systemen mit einer großen Anzahl von Benutzern.Das Konzept der Public-Key-Kryptografie wurde 1976 von Whitfield Diffie und Martin Hellman eingeführt, um das Schlüsselverwaltungsproblem zu lösen. In ihrem Konzept erhält jede Person ein Paar Schlüssel, einen öffentlichen Schlüssel, den anderen privaten Schlüssel. Der öffentliche Schlüssel jeder Person wird veröffentlicht, während der private Schlüssel geheim gehalten wird. Absender und Empfänger müssen keine geheimen Informationen mehr weitergeben, und alle Kommunikation erfolgt ausschließlich über öffentliche Schlüssel, und es wird kein privater Schlüssel übertragen oder freigegeben. Manche Kommunikationskanäle müssen nicht mehr darauf vertrauen, dass sie sicher gegen Lauschangriffe oder Verrat sind. Die einzige Anforderung besteht darin, dass öffentliche Schlüssel ihren Benutzern auf vertrauenswürdige (authentifizierte) Weise (z. B. in einem vertrauenswürdigen Verzeichnis) zugeordnet werden. Jeder kann eine vertrauliche Nachricht einfach über öffentliche Informationen versenden. Die Nachricht kann jedoch nur mit einem privaten Schlüssel entschlüsselt werden, der sich im alleinigen Besitz des beabsichtigten Empfängers befindet. Darüber hinaus kann die Verschlüsselung öffentlicher Schlüssel nicht nur für den Datenschutz (Verschlüsselung), sondern auch für die Authentifizierung (digitale Signaturen) verwendet werden.

- **Digitale Signaturen für öffentliche Schlüssel:** Um eine Nachricht zu signieren, führt eine Person eine Berechnung durch, die sowohl ihren privaten Schlüssel als auch die Nachricht selbst umfasst. Die Ausgabe wird als digitale Signatur bezeichnet und an die Nachricht angefügt, die dann gesendet wird. Eine zweite Person überprüft die Signatur, indem sie eine Berechnung mit der Nachricht, der angegebenen Signatur und dem öffentlichen Schlüssel der ersten Person durchführt. Wenn das Ergebnis korrekt in einer einfachen mathematischen Beziehung bleibt, wird die Signatur als echt verifiziert. Andernfalls kann die Signatur betrügerisch sein oder die Nachricht wurde geändert.
- **Public Key Encryption:** Wenn eine Person eine geheime Nachricht an eine andere Person senden möchte, sucht die erste Person den öffentlichen Schlüssel der zweiten Person in einem Verzeichnis, verwendet diesen zur Verschlüsselung der Nachricht und sendet sie ab. Die zweite Person verwendet dann ihren privaten Schlüssel, um die Nachricht zu entschlüsseln und zu lesen. Niemand, der zuhört, kann die Nachricht entschlüsseln. Jeder kann eine verschlüsselte Nachricht an die zweite Person senden, aber nur die zweite Person kann sie lesen. Eine Anforderung ist eindeutig, dass niemand den privaten Schlüssel aus dem entsprechenden öffentlichen Schlüssel herausfinden kann.
- **Datenverkehrsanalyse:** Die Analyse des Datenverkehrsflusses im Netzwerk zum Ableiten von Informationen, die für einen Angreifer nützlich sind. Beispiele für solche Informationen sind die Häufigkeit der Übertragung, die Identitäten der konvertierenden Parteien, die Größe der Pakete, verwendete Flow Identifiers usw.

Vorläufige Informationen

In diesem Abschnitt werden einige grundlegende Konzepte für die Verschlüsselung auf Netzwerkebene erläutert. Sie enthält die Aspekte der Verschlüsselung, die Sie beachten sollten. Anfänglich sind diese Probleme für Sie vielleicht nicht sinnvoll, aber es ist eine gute Idee, sie jetzt zu lesen und sich ihrer bewusst zu sein, weil sie nach der Arbeit mit Verschlüsselung über mehrere Monate mehr Sinn ergeben.

- Beachten Sie, dass die Verschlüsselung nur bei der Ausgabe einer Schnittstelle erfolgt und die Entschlüsselung nur bei der Eingabe in die Schnittstelle erfolgt. Diese Unterscheidung ist wichtig, wenn Sie Ihre Politik planen. Die Richtlinien für Verschlüsselung und Entschlüsselung sind symmetrisch. Das bedeutet, dass Sie bei der Definition eines Begriffs den anderen automatisch erhalten. Bei den Crypto-Maps und den zugehörigen erweiterten Zugriffslisten wird nur die Verschlüsselungsrichtlinie explizit definiert.Die Entschlüsselungsrichtlinie verwendet die gleichen Informationen. Beim Abgleich von Paketen werden jedoch Quell- und Zieladressen und -ports umgekehrt. Auf diese Weise werden die Daten in beide Richtungen einer Duplexverbindung geschützt. Die *x-**Anweisung*** der ***Match-Adresse*** im Befehl **crypto map** wird verwendet, um Pakete zu beschreiben, die eine Schnittstelle verlassen. Mit anderen Worten, es beschreibt die Verschlüsselung von Paketen. Pakete müssen jedoch auch bei der Eingabe in die Schnittstelle zur Entschlüsselung abgeglichen werden. Dies geschieht automatisch, indem die Quell- und Zieladressen sowie die Ports in der Zugriffsliste umgekehrt werden. Dadurch wird eine Symmetrie der Verbindung hergestellt. In der Zugriffsliste, auf die die **Crypto Map** verweist, sollte der Datenverkehr nur in eine (ausgehende) Richtung beschrieben werden. IP-Pakete, die nicht mit der von Ihnen definierten Zugriffsliste übereinstimmen, werden übertragen, aber nicht verschlüsselt. Eine "Verweigerung" in der Zugriffsliste gibt an, dass diese Hosts nicht zugeordnet werden sollten, d. h. sie werden nicht verschlüsselt. Die "Verweigerung" in diesem Kontext bedeutet nicht, dass das Paket

verworfen wird.

- Achten Sie darauf, das Wort "any" in erweiterten Zugriffslisten zu verwenden. Wenn Sie "any" verwenden, wird Ihr Datenverkehr verworfen, es sei denn, er wird an die entsprechende "unverschlüsselte" Schnittstelle geleitet. Darüber hinaus ist mit IPSec in Version 11.3(3)T der Cisco IOS-Software "any" nicht zulässig.
- Die Verwendung des Schlüsselworts "any" wird bei der Angabe von Quell- oder Zieladressen abgeraten. Die Angabe "any" kann Probleme mit Routing-Protokollen, NTP (Network Time Protocol), Echo, Echo-Antwort und Multicast-Datenverkehr verursachen, da der empfangende Router diesen Datenverkehr unauffällig verwirft. Wenn "any" verwendet werden soll, sollte der Anweisung "deny" (Ablehnen) Anweisungen für Datenverkehr vorangestellt werden, der nicht verschlüsselt werden soll, z. B. "ntp".
- Um Zeit zu sparen, stellen Sie sicher, dass Sie **einen Ping an** den Peer-Router senden können, mit dem Sie eine Verschlüsselungszuordnung herstellen möchten. Lassen Sie außerdem die Endgeräte (die darauf angewiesen sind, dass ihr Datenverkehr verschlüsselt wird) pingen, bevor Sie zu viel Zeit mit der Fehlerbehebung verbringen. Mit anderen Worten: Stellen Sie sicher, dass das Routing funktioniert, bevor Sie versuchen, eine **Verschlüsselung durchzuführen**. Der Remote-Peer verfügt möglicherweise nicht über eine Route für die Ausgangsschnittstelle. In diesem Fall können Sie keine Verschlüsselungssitzung mit diesem Peer führen (Sie können möglicherweise **ip unnumbered** auf dieser seriellen Schnittstelle verwenden).
- Viele Point-to-Point-WAN-Verbindungen verwenden nicht routbare IP-Adressen, und die Cisco IOS Software-Version 11.2 Encryption basiert auf dem Internet Control Message Protocol (ICMP) (d. h., dass die IP-Adresse der seriellen Ausgangsschnittstelle für ICMP verwendet wird). Dies kann dazu führen, dass Sie **ip unnumbered** auf der WAN-Schnittstelle verwenden müssen. Führen Sie immer einen **Ping**- und **Traceroute-**Befehl aus, um sicherzustellen, dass das Routing für die beiden Peering-Router (Verschlüsselung/Entschlüsselung) eingerichtet ist.
- Nur zwei Router können einen Diffie-Hellman-Sitzungsschlüssel gemeinsam nutzen. Das heißt, ein Router kann verschlüsselte Pakete nicht mit demselben Sitzungsschlüssel an zwei Peers austauschen. Jedes Router-Paar muss über einen Sitzungsschlüssel verfügen, der das Ergebnis eines Diffie-Hellman-Austauschs ist.
- Die Verschlüsselungs-Engine befindet sich entweder in Cisco IOS, dem VIP2 Cisco IOS oder in der Hardware im Encryption Services Adapter (ESA) auf einem VIP2. Ohne VIP2 regelt die Cisco IOS-Krypto-Engine die Verschlüsselungsrichtlinien aller Ports. Auf Plattformen, die das VIP2 verwenden, gibt es mehrere Krypto-Engines: eine im Cisco IOS und eine in jedem VIP2. Die Verschlüsselungs-Engine auf einem VIP2 steuert die Verschlüsselung der Ports, die sich auf dem Motherboard befinden.
- Stellen Sie sicher, dass der Datenverkehr an einer Schnittstelle ankommt, die zur Verschlüsselung vorbereitet ist. Wenn der Datenverkehr irgendwie an einer anderen Schnittstelle als der ankommen kann, auf der **Crypto Map** angewendet wurde, wird er stumm gelöscht.
- Es ermöglicht den Konsolenzugriff (oder alternativen Zugriff) auf beide Router bei der Durchführung des Schlüsselaustauschs. es ist möglich, die passive Seite während des Wartens auf eine Taste zu hängen.
- Die Verarbeitung des **cfb-64** ist hinsichtlich der CPU-Last effizienter als **cfb-8**.
- Der Router muss den Algorithmus ausführen, den Sie mit dem Verschlüsselungsfeedback (CFB)-Modus verwenden möchten. Standard für jedes Bild ist der Name des Bildes (z. B. "56") mit **cfb-64**.

- Ziehen Sie in Betracht, die Tastenüberschreitung zu ändern. Der Standardwert von 30 Minuten ist sehr kurz. Erhöhen Sie die Dosis auf einen Tag (1440 Minuten).
- IP-Datenverkehr wird bei jeder erneuten Aushandlung eines Schlüssels verworfen, wenn der Schlüssel abläuft.
- Wählen Sie nur den Datenverkehr aus, den Sie wirklich verschlüsseln möchten (dies spart CPU-Zyklen).
- Mit DDR (Dial-on-Demand Routing) machen Sie ICMP interessant, oder es wird niemals ein Anruf getätigt.
- Wenn Sie anderen Datenverkehr als IP verschlüsseln möchten, verwenden Sie einen Tunnel. Wenden Sie die Crypto-Maps bei Tunneln sowohl auf die physischen als auch auf die Tunnelschnittstellen an. Siehe Beispiel 5: Verschlüsselung des IPX-Datenverkehrs in einem IP-Tunnel für weitere Informationen.
- Die beiden Verschlüsselungs-Peer-Router müssen nicht direkt verbunden werden.
- Bei einem Low-End-Router wird möglicherweise die Meldung "CPU Hog" (CPU-Hog) angezeigt. Dies kann ignoriert werden, da die Verschlüsselung eine Menge CPU-Ressourcen verwendet.
- Platzieren Sie keine verschlüsselnden Router redundant, sodass Sie Datenverkehr entschlüsseln und neu verschlüsseln und CPU verschwenden. Verschlüsseln Sie einfach an den beiden Endpunkten. Siehe Beispiel 3: Verschlüsselung zu und über einen Router für weitere Informationen.
- Derzeit wird die Verschlüsselung von Broadcast- und Multicast-Paketen nicht unterstützt. Wenn für ein Netzwerkdesign "sichere" Routing-Updates wichtig sind, sollte ein Protokoll mit integrierter Authentifizierung verwendet werden, z. B. Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) oder Routing Information Protocol Version 2 (RIPv2), um die Aktualisierungsintegrität sicherzustellen.

Einsprüche

Hinweis: Die nachfolgend genannten Fälle wurden alle behoben.

- Ein Cisco 7200-Router, der eine ESA für die Verschlüsselung verwendet, kann ein Paket nicht unter einem Sitzungsschlüssel entschlüsseln und dann unter einem anderen Sitzungsschlüssel erneut verschlüsseln. Weitere Informationen finden Sie unter Cisco Bug ID CSCdj82613 (nur registrierte Kunden).
- Wenn zwei Router über eine verschlüsselte Mietleitung und eine ISDN-Backup-Leitung angeschlossen sind, wird bei Ausfall der Mietleitung die ISDN-Verbindung einwandfrei aktiviert. Wenn die Mietleitung jedoch wieder verfügbar ist, stürzt der Router, der den ISDN-Anruf getätigt hat, ab. Weitere Informationen finden Sie unter Cisco Bug ID CSCdj00310 (nur registrierte Kunden).
- Bei Cisco Routern der Serie 7500 mit mehreren VIPs stürzt eine **Kryptoübersicht** auf eine Schnittstelle eines VIP ab, wenn eine oder mehrere VIPs abstürzen. Weitere Informationen finden Sie unter Cisco Bug ID CSCdi8459 (nur registrierte Kunden).
- Bei Cisco Routern der Serie 7500 mit VIP2 und ESA zeigt der Befehl **show crypto card** nur die Ausgabe an, wenn sich der Benutzer am Konsolenport befindet. Weitere Informationen finden Sie unter Cisco Bug ID CSCdj89070 (nur registrierte Kunden).

Cisco IOS Verschlüsselungskonfiguration auf Netzwerkebene

Die funktionierenden Cisco IOS-Konfigurationen in diesem Dokument stammen direkt von den Übungs-Routern. Die einzige Änderung an ihnen war das Entfernen von nicht verwandten Schnittstellenkonfigurationen. Das gesamte Material stammt aus frei verfügbaren Ressourcen im Internet oder im Abschnitt Zugehörige Informationen am Ende dieses Dokuments.

Alle Beispielkonfigurationen in diesem Dokument stammen aus der Cisco IOS Software, Version 11.3. Die Befehle in der Cisco IOS Software, Version 11.2, haben sich geändert, z. B. wurden folgende Begriffe hinzugefügt:

- dss in einigen der wichtigsten Konfigurationsbefehle.
- Cisco in einigen der **show**-Befehle und die **crypto map-**Befehle zur Unterscheidung zwischen der proprietären Verschlüsselung von Cisco (wie in Version 11.2 und höher der Cisco IOS-Software enthalten) und IPSec (in Version 11.3(2)T der Cisco IOS-Software).

Hinweis: Die in diesen Konfigurationsbeispielen verwendeten IP-Adressen wurden im Cisco Labor nach dem Zufallsprinzip ausgewählt und sind als generische Adressen gedacht.

Schritt 1: Manuelles Generieren von DSS-Schlüsselpaaren

Ein DSS-Schlüsselpaar (ein öffentlicher und ein privater Schlüssel) muss manuell auf jedem Router generiert werden, der an der Verschlüsselungssitzung teilnimmt. Anders ausgedrückt: Jeder Router muss über eigene DSS-Schlüssel verfügen, um teilzunehmen. Eine Verschlüsselungs-Engine kann nur über einen DSS-Schlüssel verfügen, der ihn eindeutig identifiziert. Das Schlüsselwort "dss" wurde in Version 11.3 der Cisco IOS-Software hinzugefügt, um DSS von RSA-Schlüsseln zu unterscheiden. Sie können einen beliebigen Namen für die eigenen DSS-Schlüssel des Routers angeben (es wird jedoch empfohlen, den Router-Hostnamen zu verwenden). Bei einer weniger leistungsfähigen CPU (z. B. der Cisco Serie 2500) dauert die Generierung von Schlüsselpaaren maximal fünf Sekunden.

Der Router generiert zwei Schlüssel:

- Ein öffentlicher Schlüssel (der später an Router gesendet wird, die an Verschlüsselungssitzungen teilnehmen).
- Ein privater Schlüssel (der nicht gesehen wird und nicht mit anderen ausgetauscht wird; Sie wird in einem separaten Abschnitt des NVRAM gespeichert, der nicht angezeigt werden kann).

Sobald das DSS-Schlüsselpaar des Routers generiert wurde, ist es eindeutig mit der Krypto-Engine in diesem Router verknüpft. Die Generierung von Schlüsselpaaren wird in der Beispielbefehlsausgabe unten gezeigt.

```
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#
```

Da Sie nur ein Schlüsselpaar generieren können, das den Router identifiziert, können Sie Ihren ursprünglichen Schlüssel überschreiben und den öffentlichen Schlüssel mit jedem Router in der Verschlüsselungszuordnung erneut senden. Dies wird in der Beispielausgabe des Befehls unten gezeigt:

```
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.
```

Schritt 2: Manueller Austausch der öffentlichen DSS-Schlüssel mit Peers (Out-of-Band)

Die Generierung des eigenen DSS-Schlüsselpaars des Routers ist der erste Schritt bei der Herstellung einer Verschlüsselungssitzungszuordnung. Im nächsten Schritt werden öffentliche Schlüssel mit jedem anderen Router ausgetauscht. Sie können diese öffentlichen Schlüssel manuell eingeben, indem Sie zuerst den Befehl **show crypto mypubkey** eingeben, um den öffentlichen DSS-Schlüssel des Routers anzuzeigen. Anschließend tauschen Sie diese öffentlichen Schlüssel (z. B. per E-Mail) aus und schneiden den öffentlichen Schlüssel des Peer-Routers mit dem Befehl **crypto key pubkey-chain dss**, und fügen ihn in den Router ein.

Sie können den Befehl **crypto key exchange dss** verwenden, damit die Router öffentliche Schlüssel automatisch austauschen lassen. Wenn Sie die automatisierte Methode verwenden, stellen Sie sicher, dass die für den Schlüsselaustausch verwendeten Schnittstellen keine Anweisungen für die **Crypto Map** enthalten. Hier ist ein **Schlüssel** für die **Debugging-Verschlüsselung** hilfreich.

Hinweis: Es ist empfehlenswert, einen **Ping** an Ihren Peer zu senden, bevor Sie versuchen, Schlüssel auszutauschen.

```
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#
```

Nachdem nun öffentliche DSS-Schlüssel ausgetauscht wurden, stellen Sie sicher, dass beide Router die öffentlichen Schlüssel des anderen besitzen und dass diese übereinstimmen, wie in der Befehlsausgabe unten gezeigt.

```
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
```

Beispiel 1: Cisco IOS-Konfiguration für dedizierte Verbindung

Nachdem die DSS-Schlüssel auf jedem Router generiert und die öffentlichen DSS-Schlüssel ausgetauscht wurden, kann der Befehl **crypto map** auf die Schnittstelle angewendet werden. Die Crypto-Sitzung beginnt mit der Generierung von Datenverkehr, der mit der von den Crypto Maps verwendeten Zugriffsliste übereinstimmt.

```
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#
```

Beispiel 2: Cisco IOS-Konfiguration für Multipoint Frame Relay

Die folgende Beispielbefehlsausgabe wurde vom HUB-Router übernommen.

```
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#
```

Die folgende Beispielbefehlsausgabe wurde von Remote-Standort A übernommen.

```
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#
```

Die folgende Beispielbefehlsausgabe wurde von Remote-Standort B übernommen.

```
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#
```

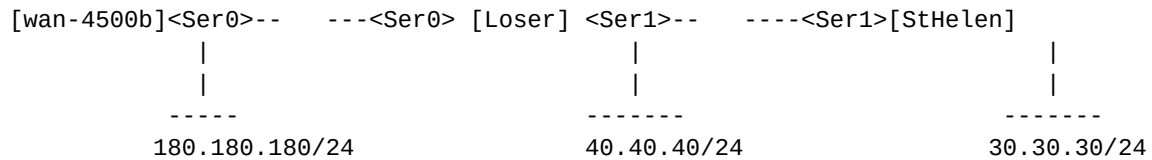
Die folgende Beispielbefehlsausgabe wurde vom Frame Relay Switch übernommen.

```
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
!
```

Beispiel 3: Verschlüsselung für und über einen Router

Peer-Router müssen nicht nur einen Hop entfernt sein. Sie können eine Peering-Sitzung mit einem Remote-Router erstellen. Im folgenden Beispiel ist das Ziel, den gesamten Netzwerkverkehr zwischen 180.180.180.0/24 und 40.40.40.0/24 sowie zwischen 180.180.180.0/24 und 30.30.30.0/24 zu verschlüsseln. Bei der Verschlüsselung des Datenverkehrs zwischen 40.40.40.0/24 und 30.30.30.0/24 bestehen keine Bedenken.

Der Router WAN-4500b verfügt über eine Verschlüsselungssitzung mit Loser und auch mit StHelen. Durch die Verschlüsselung des Datenverkehrs vom Ethernet-Segment des WAN-4500b zum Ethernet-Segment von StHelen vermeiden Sie den unnötigen Entschlüsselungsschritt bei Loser. Loser leitet den verschlüsselten Datenverkehr einfach an die serielle Schnittstelle von StHelen weiter, wo er entschlüsselt wird. Dies reduziert die Datenverkehrsverzögerung für die IP-Pakete und CPU-Zyklen auf dem Router Loser. Noch wichtiger ist, dass dadurch die Sicherheit des Systems erheblich erhöht wird, da ein Lauschkopf bei Loser den Datenverkehr nicht lesen kann. Wenn Loser den Datenverkehr entschlüsselt, besteht die Möglichkeit, dass die entschlüsselten Daten umgeleitet werden.




```
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#
```

Beispiel 4: Verschlüsselung mit DDR

Da Cisco IOS für die Erstellung von Verschlüsselungssitzungen auf den ICMP angewiesen ist, muss der ICMP-Datenverkehr bei der Verschlüsselung über eine DDR-Verbindung in der Wählerliste als "interessant" eingestuft werden.

Hinweis: Komprimierung funktioniert in Version 11.3 der Cisco IOS-Software, ist jedoch für verschlüsselte Daten nicht besonders hilfreich. Da die verschlüsselten Daten ziemlich zufällig aussehen, verlangsamt Komprimierung nur die Dinge. Sie können die Funktion jedoch auch für nicht verschlüsselten Datenverkehr aktivieren.

In einigen Situationen möchten Sie eine Sicherung mit demselben Router konfigurieren. Sie ist beispielsweise sinnvoll, wenn Benutzer vor dem Ausfall einer bestimmten Verbindung in ihren WAN-Netzwerken schützen möchten. Wenn zwei Schnittstellen zum gleichen Peer gehen, kann auf beiden Schnittstellen dieselbe Crypto Map verwendet werden. Damit diese Funktion ordnungsgemäß funktioniert, muss die Backup-Schnittstelle verwendet werden. Wenn bei einem Backup-Design ein Router in einem anderen Feld wählt, sollten verschiedene Kryptozuordnungen

erstellt und die Peers entsprechend eingestellt werden. Auch hier sollte der Befehl **backup interface** verwendet werden.

```
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#
```

Beispiel 5: Verschlüsselung des IPX-Datenverkehrs in einem IP-Tunnel

In diesem Beispiel wird der IPX-Datenverkehr in einem IP-Tunnel verschlüsselt.

Hinweis: Nur der Datenverkehr in diesem Tunnel (IPX) wird verschlüsselt. Der gesamte andere IP-Datenverkehr bleibt allein.

```
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#
```

Beispiel 6: Verschlüsseln von L2F-Tunneln

In diesem Beispiel wird nur versucht, den L2F-Datenverkehr für Benutzer zu verschlüsseln, die sich einwählen. Hier ruft "user@cisco.com" den lokalen Network Access Server (NAS) mit dem Namen "DEMO2" in der Stadt auf und wird auf die Home-Gateway-CD getunnelt. Der gesamte DEMO2-Datenverkehr (zusammen mit dem anderer L2F-Anrufer) wird verschlüsselt. Da L2F den UDP-Port 1701 verwendet, wird die Zugriffsliste auf diese Weise erstellt und bestimmt, welcher Datenverkehr verschlüsselt wird.

Hinweis: Wenn die Verschlüsselungszuordnung nicht bereits eingerichtet ist, d. h. der Anrufer ist die erste Person, die sich einwählt und den L2F-Tunnel erstellt, wird der Anrufer möglicherweise wegen der Verzögerung bei der Einrichtung der Verschlüsselungszuordnung abgebrochen. Bei Routern mit ausreichender CPU-Leistung ist dies möglicherweise nicht der Fall. Sie können auch das **keytimeout** erhöhen, sodass die Verschlüsselung nur außerhalb der Spitzenzeiten eingerichtet und beendet wird.

Die folgende Beispielbefehlsausgabe wurde vom Remote-NAS übernommen.

```
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#
```

Die folgende Beispielbefehlsausgabe wurde vom Home-Gateway übernommen.

```
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
```

Fehlerbehebung

Am besten beginnen Sie jede Sitzung zur Fehlerbehebung, indem Sie Informationen mithilfe der folgenden **show-**Befehle sammeln. Ein Sternchen (*) weist auf einen besonders nützlichen Befehl hin. Weitere Informationen finden Sie unter IP-Sicherheitsfehlerbehebung - Debugbefehle verstehen und verwenden.

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

Hinweis: Bevor Sie **Debugbefehle** ausgeben, lesen Sie Wichtige Informationen über Debug-Befehle.

Befehle	
Crypto Cisco Algorithmen anzeigen	**show crypto cisco key-timeout**
show crypto cisco pregen-dh pair	*** Zeigen Sie die**

	Verbindungen der Krypto-Engine an.
Anzeige von verworfenen Verschlüsselungs-Engine-Verbindungen	Konfiguration der Crypto Engine anzeigen
show crypto key mypubkey dgs	* show crypto key pubkey chain dss
show crypto map interface serial 1	* Crypto Map anzeigen
Debug-Krypto-Engine	* Verschlüsselung debuggen
Debug-Schrei-Schlüssel	Klarkryptoverbindung
Krypto-Zerosion	Keine Verschlüsselung des öffentlichen Schlüssels

- **Crypto Cisco Algorithmen anzeigen**- Sie müssen alle DES-Algorithmen (Data Encryption Standard) aktivieren, die für die Kommunikation mit anderen Peer-Verschlüsselungs-Routern verwendet werden. Wenn Sie einen DES-Algorithmus nicht aktivieren, können Sie diesen Algorithmus auch dann nicht verwenden, wenn Sie versuchen, den Algorithmus zu einem späteren Zeitpunkt einer **Crypto Map** zuzuordnen.Wenn Ihr Router versucht, eine verschlüsselte Kommunikationssitzung mit einem Peer-Router einzurichten, und auf beiden Routern nicht der gleiche DES-Algorithmus aktiviert ist, schlägt die verschlüsselte Sitzung fehl. Wenn an beiden Enden mindestens ein gemeinsamer DES-Algorithmus aktiviert ist, kann die verschlüsselte Sitzung fortgesetzt werden.**Hinweis:** Das zusätzliche Wort cisco wird in Version 11.3 der Cisco IOS-Software angezeigt und wird benötigt, um zwischen der in Version 11.2 der Cisco IOS-Software enthaltenen proprietären Verschlüsselung von IPSec und Cisco zu unterscheiden.

```
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** - Nachdem eine verschlüsselte Kommunikationssitzung erstellt wurde, ist sie für eine bestimmte Zeit gültig. Nach diesem Zeitraum ist die Sitzung abgelaufen. Es muss eine neue Sitzung ausgehandelt und ein neuer DES-Schlüssel (Session Key) erstellt werden, damit die verschlüsselte Kommunikation fortgesetzt werden kann. Mit diesem Befehl kann die Dauer einer verschlüsselten Kommunikationssitzung vor ihrem Ablauf (Timeout) geändert werden.

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

Verwenden Sie diese Befehle, um die Zeitspanne bis zur Neuverhandlung der DES-Schlüssel zu bestimmen.

```
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-pair** - Jede verschlüsselte Sitzung verwendet ein eindeutiges Paar DH-Nummern. Bei jeder Einrichtung einer neuen Sitzung müssen neue DH-Zahlenpaare generiert werden. Nach Abschluss der Sitzung werden diese Nummern verworfen. Die Generierung neuer DH-Zahlenpaare ist eine CPU-intensive Aktivität, die die Sitzungseinrichtung insbesondere bei Low-End-Routern verlangsamen kann.Um die Sitzungseinrichtung zu beschleunigen, können Sie festlegen, dass eine bestimmte Anzahl von DH-Zahlenpaaren vorab generiert und in Reserve gehalten wird. Wenn dann eine verschlüsselte Kommunikationssitzung eingerichtet wird, wird ein DH-Nummernpaar aus dieser Reserve bereitgestellt. Wenn ein DH-Zahlenpaar verwendet wird, wird die Reserve automatisch durch ein neues DH-Zahlenpaar aufgefüllt, sodass immer ein DH-Zahlenpaar einsatzbereit ist.In der Regel ist es nicht erforderlich, mehr als ein oder zwei DH-Zahlenpaare vorab zu erstellen, es sei denn, Ihr Router richtet mehrere verschlüsselte Sitzungen so häufig ein, dass eine vorgenerierte Reserve von ein oder zwei DH-Zahlenpaaren zu schnell ausgeschöpft wird.

```
Loser#show crypto cisco pregen-dh-pairs
Number of pregenerated DH pairs: 10
```

- **show crypto cisco connections active**Im Folgenden sehen Sie eine Beispielbefehlsausgabe.

```
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**Im Folgenden sehen Sie eine Beispielbefehlsausgabe.

```
Loser#show crypto engine connections dropped-packet
Interface            IP-Address    Drop Count

Serial1              19.19.19.19   39
```

- **show crypto engine configuration** (was **crypto engine brief** in Cisco IOS Software Release 11.2)Im Folgenden sehen Sie eine Beispielbefehlsausgabe.

```
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 dgs**Im Folgenden sehen Sie eine Beispielbefehlsausgabe.

```
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**Im Folgenden sehen Sie eine Beispielbefehlsausgabe.

```
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**Im Folgenden sehen Sie eine Beispielbefehlsausgabe.

```
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
```

  Beachten Sie die Zeitunterschiede, wenn Sie den **Ping-**Befehl verwenden.

```
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**Im Folgenden sehen Sie eine Beispielbefehlsausgabe.

```
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-Krypto-Engine**Im Folgenden sehen Sie eine Beispielbefehlsausgabe.

```
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
```

- **debuggen crypto sessmgmt**Im Folgenden sehen Sie eine Beispielbefehlsausgabe.

```
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 ----------> ~~
```

Wenn der falsche Peer auf der Crypto Map eingestellt ist, erhalten Sie diese Fehlermeldung.

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

Wenn die Verschlüsselungsalgorithmen nicht übereinstimmen, erhalten Sie diese Fehlermeldung.

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

Wenn der DSS-Schlüssel fehlt oder ungültig ist, erhalten Sie diese Fehlermeldung.

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

- **Verschlüsselungsschlüssel debuggen**Im Folgenden sehen Sie eine Beispielbefehlsausgabe.

```
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.
```

- **Klarkryptoverbindung**Im Folgenden sehen Sie eine Beispielbefehlsausgabe.

```
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#
```

- **Krypto-Zerosion**Im Folgenden sehen Sie eine Beispielbefehlsausgabe.

```
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#
```

- **Keine Verschlüsselung des öffentlichen Schlüssels**Im Folgenden sehen Sie eine Beispielbefehlsausgabe.

```
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#
```

Fehlerbehebung beim Cisco 7200 mit ESA

Cisco bietet auch eine Hardware-Unterstützung für die Verschlüsselung auf den Cisco Routern der Serie 7200, die als ESA bezeichnet wird. Die ESA ist ein Port-Adapter für die VIP2-40-Karte oder ein Standalone-Port-Adapter für den Cisco 7200. Diese Anordnung ermöglicht die Verwendung eines Hardware-Adapters oder der VIP2-Software-Engine zur Verschlüsselung und Entschlüsselung von Daten, die in die Schnittstellen der Cisco 7500 VIP2-Karte eingehen oder diese verlassen. Der Cisco 7200 ermöglicht Hardware-Unterstützung bei der Verschlüsselung des Datenverkehrs für alle Schnittstellen im Cisco 7200-Chassis. Durch die Verwendung einer Verschlüsselungsunterstützung können wertvolle CPU-Zyklen gespart werden, die für andere Zwecke, z. B. für das Routing oder eine andere Cisco IOS-Funktion, verwendet werden können.

Auf einem Cisco 7200 ist der Standalone-Port-Adapter genau wie die Cisco IOS Software Crypto Engine konfiguriert, verfügt aber über einige zusätzliche Befehle, die nur für Hardware und zur Entscheidung der Engine (Software oder Hardware) verwendet werden, die die Verschlüsselung übernimmt.

Bereiten Sie den Router zunächst auf die Hardwareverschlüsselung vor:

```
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]
```

Aktivieren oder deaktivieren Sie die Hardwareverschlüsselung, wie unten gezeigt:

```
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.
```

Generieren Sie anschließend Schlüssel für die ESA, bevor Sie sie aktivieren.

```
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#
```

Fehlerbehebung bei VIP2 mit ESA

Der ESA-Hardware-Port-Adapter auf der VIP2-Karte wird verwendet, um Daten zu verschlüsseln und zu entschlüsseln, die in die Schnittstellen der VIP2-Karte eingehen oder diese verlassen. Wie beim Cisco 7200 können auch beim Einsatz einer Verschlüsselung wertvolle CPU-Zyklen eingespart werden. In diesem Fall existiert der Befehl **crypto esa enable** nicht, da der ESA-Port-Adapter die Verschlüsselung der Ports auf der VIP2-Karte übernimmt, wenn die ESA angeschlossen ist. Der **Krypto-Riegel** muss auf diesen Steckplatz angewendet werden, wenn der ESA-Port-Adapter gerade erst zum ersten Mal installiert oder entfernt und dann neu installiert wurde.

```
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#
```

Da das ESA-Krypto-Modul extrahiert wurde, erhalten Sie die folgende Fehlermeldung, bis Sie wie unten gezeigt einen Befehl **crypto clear-rieche** an diesem Steckplatz ausführen.

```
----
*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
```

Wenn Sie ein zuvor zugewiesenes Kennwort vergessen haben, verwenden Sie den Befehl **crypto zeroize** (**Krypto-Zeroize)** anstelle des Befehls **crypto clear-rieche**, um die ESA zurückzusetzen. Nachdem Sie den Befehl **crypto zeroize** (Krypto-Zeroize) ausgegeben haben, müssen Sie die DSS-Schlüssel regenerieren und erneut austauschen. Wenn Sie DSS-Schlüssel neu generieren, werden Sie aufgefordert, ein neues Kennwort zu erstellen. Ein Beispiel ist unten dargestellt.

```
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#
```

Zugehörige Informationen

- Konfiguration und Fehlerbehebung bei Cisco Network Layer Encryption: IPSec und ISAKMP - Teil 2
- DES FIPS 46-2 am National Institute of Standards and Technology (NIST)
- DSS FIPS 186 am National Institute of Standards and Technology (NIST)
- Häufig gestellte Fragen von RSA Laboratories zur heutigen Kryptografie
- IETF-Sicherheitsstandards
- Konfigurieren des Internet Key Exchange Security Protocol
- Konfigurieren der IPSec-Netzwerksicherheit
- IPSec-Support-Seite
- Technischer Support - Cisco Systems