Cisco 网络层加密的配置与故障排除：背景信息 - 第 1 部分

目录

简介

本文与IPSec和互联网安全协会和密钥管理协议(ISAKMP)讨论配置和排除故障Cisco网络层加密并且与IPSec和ISAKMP一起包括网络层加密背景信息和基本配置。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco IOS®软件版本11.2及以上版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

网络层加密背景信息和配置

网络层加密功能在Cisco IOS软件版本11.2介绍。它为安全数据传输提供一机制并且包括两个组件：

- **路由器验证**：在通过加密流量之前，两路由器执行一一次性，双向认证使用数字签字标准(DSS)公共密钥签署随机的挑战。
- **网络层加密**：对于IP有效载荷加密、路由器使用迪菲–赫尔曼密钥交换安全地生成DES(40-或56位会话密钥的)，三重DES - 3DES(168-bit)或者更加最近的高级加密标准- AES(128-bit(default)或者192-bit或者256-bit在12.2(13)T锁上)，介绍。新的会话密钥生成根据一个可配置基本类型。加密策略由使用扩展IP访问列表定义网络、子网、主机或者协议对将加密在路由器之间的加密映射设置。

密码学背景

加密算法字段牵涉到保持通信专用。敏感通信的保护是加密算法重点在其发展历史中。加密是数据的转换到一些不可读的表里。其目的将保证保密性通过保存信息隐藏从任何人为谁没有打算，即使他们能看到已加密数据。解密是加密反向：它是已加密数据的转换回到一可理解表。

加密和解密要求一些秘密信息，通常被称为的使用“密钥”。根据使用的加密机制，同一密钥也许用于加密和解密;当对于其他机制，用于加密的密钥和解密也许不同的时。

而一数字时间戳在特定时间，绑定文档对其创建数字签名绑定文档对一特定的密钥的持有人。这些加密机制可以用于控制访问对一个共享磁盘驱动器，高安全性安装，或者对收费电视电视频道。

当现代加密算法是增长逐渐多样化时，加密算法根据是很难解决的问题根本上。问题可能是困难，因为其解决方案要求认识密钥，例如解密加密的消息或签署某个数字文档。问题可能也是困难，因为完成是内在地难的，例如查找引起一个给的Hash值的消息。

因为加密算法字段提前，什么是，并且什么的分界线不是加密算法变得弄脏。加密算法今天也许被总结作为取决于数学问题的存在是很难解决技术和应用程序的研究。密码专家尝试减弱加密机制，并且隐语是联合的加密算法和密码分析学科。

定义

本部分定义本文档中使用的相关术语。

- **验证**：一种确认属性，即收到的数据实际上是由所声明的发送方发送的。

- **机密性**：一种通信属性，它使得预定接收方知道所发送的内容，但非预定接收方不能确定所发送的内容。
- **数据加密标准(DES)**：DES 使用对称密钥方法，也称为秘密密钥方法。这意味着，如果数据块使用密钥加密，则必须使用相同的密钥解密已加密的数据块。因此，加密器和解密器必须使用相同的密钥。即使加密方法已知并且已完全公布，公认的最佳攻击方法仍是通过暴力攻击。必须针对已加密的数据块测试密钥，以了解密钥是否可以正确地解密它们。随着处理器日益强大，破解 DES 指日可待。例如，通过 Internet 中数以千计计算机的多余处理能力的共同努力，21 天就可以破解采用 DES 编码的消息的 56 位密钥。DES由美国国家安全局(NSA)验证每五年满足的美国政府的目的。当前审批已于 1998 到期，并且 NSA 已表明他们不会重新认证 DES。除 DES 外，还有许多其他加密算法。这些算法除了无法抵挡暴力攻击外，同样坚不可摧。有关其他信息，请参阅美国国家标准与技术研究所 (NIST) 的 DES FIPS 46-2。
- **解密**：数据加密算法的逆运算，能够将已加密的数据恢复成原样，即为未加密时的状态。
- **DSS和数字签名算法(DSA)**：DSA由在数字签字标准(DSS)的NIST发布，是美国政府的顶石项目的部分。NIST 通过与 NSA 合作，选择 DSS 作为美国政府的数字身份验证标准。该标准于 1994 年 5 月 19 日发布。
- **加密**：对数据应用特定的算法，改变数据的显示形式，使无权看到该信息的人无法理解数据内容。
- **完整性**：一种属性，它确保数据从源位置传输到目标位置的过程中没有未检测到的改变。
- **不可否认性**：接收方能够证明某些数据的发送方实际上发送了这些数据（即使该发送方后来可能拒绝承认曾发送过这些数据）的一种属性。
- **公钥加密术**：传统加密术基于的事实是，消息的发送方和接收方知道并使用相同秘密密钥。发送方使用秘密密钥来加密消息，而接收方使用相同秘密密钥来解密消息。此方法称为“秘密密钥”或“对称加密术”。此方法的主要问题是要让发送方和接收方同意秘密密钥，并且不能让任何其他人知道。如果他们位于不同的物理位置，则他们必须信任快递、电话系统或某种其他传输介质，以防止传送的秘密密钥泄露。在传输过程中窃听或拦截了密钥的任何人以后都可以读取、修改和伪造使用该密钥加密或进行身份验证的所有消息。密钥的生成、传输和存储称为密钥管理；所有加密系统都必须处理密钥管理问题。因为秘密密钥加密系统中的所有密钥都必须保密，秘密密钥加密术通常在提供安全密钥管理方面存在一些困难，尤其是在具有大量用户的开放式系统中。公钥加密术的概念是 Whitfield Diffie 和 Martin Hellman 于 1976 年提出的，其目的是解决密钥管理问题。在他们的概念中，每个人都获得一对密钥，一个称为公钥，另一个称为私钥。每个人的公钥都公开，而私钥则保密。这样，发送方和接收方就无需共享秘密信息，并且所有的通信都只涉及公钥，不需要传输或共享私钥。也不必再信任某个通信通道没有被窃听或泄密的危险。唯一的要求是公钥必须以信任（已通过身份验证的）方式与其用户关联（例如，位于信任的目录中）。任何人只需要使用公共信息就可以发送机密消息，但此消息只能使用私钥解密，而私钥只有预定接收方才拥有。此外，公钥加密术不仅可用于隐私（加密），还可以用于身份验证（数字签名）。
- **公钥数字签名**：要签署消息，一个用户需要执行同时涉及其私钥和消息自身的计算。计算的输出称为数字签名，它被附加到该消息中，然后再发送出去。另一个用户通过执行涉及该消息、可能的签名和第一个用户的公钥的计算来验证签名。如果计算结果正确证实存在简单的数学关系，则签名被证明是真的。否则，签名可能是假的，或者消息可能已更改。
- **公钥加密**：如果一个人要将秘密消息发送给另一个人，第一个人可以在目录中查找第二个人的公钥，使用该公钥加密消息并发送消息。然后，第二个人使用其私钥解密并读取该消息。任何窃听的人都无法解密该消息。任何人都可以发送加密消息给第二个人，但只有第二个人能读取该消息。很明显，此加密方法有一个要求，就是任何人都不能通过相应的公钥计算出私钥。
- **流量分析**：分析网络数据流，以便推断出对敌意者有用的信息。传输频率、通话方的身份、数据包的大小、使用的流标识符等就是这种信息的示例。

初步信息

此部分讨论一些基本网络层加密概念。它包含您应该寻找加密的方面。最初，这些问题不也许有道理对您，但是它是一个好想法读他们当前和知道他们，因为他们将有更多意义，在您与加密一起使用几个月后。

- 请注意加密在接口的输出仅发生，并且解密仅发生在输入对接口。当飞行您的策略时，此差异是重要。加密和解密的策略是对称的。这意味着定义一的那自动地给您其他。使用加密映射和他们相关的扩展访问列表，仅加密策略明确地定义。解密策略使用相同的信息，但是，当匹配时数据包，倒转源地址和目的地址和端口。这样，数据在一双工连接的两个方向保护。在**crypto map命令的***匹配地址x*语句用于描述离开接口的数据包。换句话说，它描述数据包的加密。然而，当他们进入接口，必须为解密也匹配数据包。这由横断访问列表自动地完成用被倒转的源地址和目的地址和端口。连接的此提供对称。访问列表指向由**加密映射**应该描述在仅一个(出站)方向的流量。不匹配的IP信息包您定义了的访问列表将传送，但是不已加密。“请拒绝”在访问列表表明不应该匹配那些主机，含义他们不会加密。“请在此上下文拒绝”，不意味着数据包丢弃。
- 非常小心使用词“其中任一”在扩展访问列表。使用“任何”造成您的流量丢弃，除非朝向对匹配的“解密”接口。另外，与在Cisco IOS软件版本11.3(3)T的IPSec，“其中任一”没有允许。
- 使用“所有”关键字在指定被劝阻来源或目的地址。因为接收路由器静静地丢弃此流量，指定“其中任一”能引起问题由于路由协议、网络时间协议(NTP)、响应、响应答复和组播数据流。如果“将使用其中任一”，应该在之后“拒绝”不将加密的流量的语句，例如“ntp”。
- 要节省时间，请确保您能**ping**您尝试有加密关联的对等`路由器。并且，请有(取决于获得他们的流量加密)的终端设备ping，在花费许多时刻排除故障错误的问题前的您。换句话说，请在要执行前**crypto的**尝试确保路由工作。远端对等体可能没有出口接口的一个路由，在不能有有该对等体的情况下(您加密会话可以能使用在该serial interfaces的**ip unnumbered**)。
- 许多广域网点对点链路使用不可路由的IP地址，并且Cisco IOS软件版本11.2加密依靠互联网控制消息协议(ICMP) (含义使用出口serial interfaces的IP地址ICMP)。这可能迫使您使用在广域网接口的**ip unnumbered**。总是请执行**ping和traceroute命令**确保，路由为两并列的(加密/解密)路由器是到位。
- 仅两路由器允许共享Diffie-Hellman会话密钥。即一个路由器不能交换加密的信息包对使用同一会话密钥的两对等体;每个对路由器必须有是一个Diffie-Hellman交换结果在他们之间的会话密钥。
- 加密引擎在Cisco IOS， VIP2 Cisco IOS，或者在硬件方面加密服务适配器(ESA)在VIP2。没有VIP2， Cisco IOS加密引擎管理在所有端口的加密策略。在平台上使用VIP2，有多加密引擎：一在Cisco IOS和一个在每个VIP2。在VIP2的加密引擎管理在板驻留的端口的加密。
- 确保流量设置到达在准备的接口加密它。如果流量在接口能莫名其妙地到达除那个之外与应用的**加密映射**，静静地丢弃。
- 它帮助得以进入对两路由器的控制台(或备选)，当执行密钥交换时;使被动端暂停是可能的，当等待密钥时。
- **cfb-64**比**cfb-8**是处理的更有效的根据CPU负载。
- 路由器需要运行您要以密码反馈的算法(CFB)模式使用您要使用;每镜像的默认是镜像名称(例如"56")与**cfb-64**。
- 考虑更改密钥超时。30分钟默认是非常短的。增加它的尝试对一天(1440分钟)。
- 每次密钥超时， IP数据流在关键重新协商时丢弃。
- 选择您真要加密仅的流量(这保存CPU周期)。
- 使用按需拨号路由(DDR)，请勿使ICMP有趣的或拨出。
- 除IP之外，如果要加密流量，请使用一个通道。使用通道，请应用加密映射对物理和隧道接口。请参阅示例5 ：IPX数据流的加密在一个IP隧道的欲知更多信息。
- 两加密对等体路由器不需要直接地连接。
- 低端路由器可能给您" CPU hog "消息。这可以忽略，因为它是告诉您加密使用很多CPU资源。

- 请勿冗余放置加密路由器，以便您解码并且再加密流量和垃圾桶CPU。请加密在两个终端。请参阅示例3 ：加密对和通过一个路由器欲知更多信息。
- 目前，和组播信息包不支持广播的加密。如果“安全”路由更新对网络设计是重要，应该用于与安装的验证的一份协议，例如增强的内部网关路由选择协议(EIGRP)、开放最短路径优先(OSPF)或者路由信息协议版本2 (RIPv2)保证更新完整性。

警告

注意： 所有解决了如下所述的警告。

- 一个Cisco 7200路由器使用加密的ESA不能解码数据包在一会话密钥以下然后再加密它在一不同的会话密钥下。参考的Cisco Bug ID CSCdj82613 (仅限注册用户)。
- 当两路由器由一条已加密租用的线路和ISDN备份线路时连接，如果租用的线路下降， ISDN链路优良出来。然而，当租用的线路再时恢复，发出ISDN呼叫的路由器失败。参考的Cisco Bug ID CSCdj00310 (仅限注册用户)。
- 对于有多个VIP的思科7500系列路由器，如果**加密映射**应用对任何VIP一个接口，一个或更多VIP失败。参考的Cisco Bug ID CSCdi88459 (仅限注册用户)。
- 对于有VIP2和ESA的思科7500系列路由器，除非用户在控制台端口， **show crypto card命令不**显示输出。参考的Cisco Bug ID CSCdj89070 (仅限注册用户)。

Cisco IOS网络网络层加密配置

本文档中 Cisco IOS 配置的工作示例直接来自实验室中的路由器。所做的唯一更改是删除了不相关的接口配置。此处的所有资料都摘自 Internet 上免费提供的资源或本文档末尾的相关信息部分。

所有在本文的配置示例是从Cisco IOS软件版本11.3。有从Cisco IOS软件版本11.2命令的几更改，例如以下词的新增内容：

- 在某些的dss关键配置命令。
- 在某些的cisco**显示**命令和**加密映射**命令区分在Cisco的专有加密(在Cisco IOS软件版本11.2及以上版本中找到)和IPSec之间哪些在Cisco IOS软件版本11.3(2)T。

注意： 用于这些配置示例的IP地址在思科的实验室随机地选择和打算是完全普遍的。

步骤 1：请手工生成DSS密钥对

DSS密钥对(公共和专用密钥)在参加加密会话的每个路由器需要手工生成。换句话说，每个路由器必须有其自己的DSS密钥为了参与。独特识别它的加密引擎只能有关键一个的DSS。关键字“dss”在Cisco IOS软件版本11.3被添加为了与RSA密钥区分DSS。您能指定所有名称对于路由器的自己的DSS密钥(虽然，推荐使用路由器主机名)。在较弱的CPU (例如Cisco 2500系列)，密钥对产生采取大约5秒或较少。

路由器生成一个对密钥：

- 以后发送对参加加密会话)的路由器的公共密钥(。
- 没有在任何人看到亦不交换的专用密钥(;实际上，它在不可能查看) NVRAM的独立的部分存储。

一旦路由器的DSS密钥对生成，用在该路由器的加密引擎独特关联。密钥对产生在下面示例命令输出中显示。

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#

由于您只能生成识别路由器的一密钥对，您在加密关联中可能覆盖您的原始密钥和需要重新发送您的公共密钥用每个路由器。这在下面示例命令输出中显示：

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.

步骤 2：Exchange有对等体的(带外)手工DSS公共密钥

生成路由器的自己的DSS密钥对是在设立加密会话关联的第一步。下一步是交换公共密钥用其他路由器。您能通过首先输入**show crypto mypubkey命令**手工输入这些公共密钥显示路由器的DSS公共密钥。您然后交换这些公共密钥(例如通过电子邮件)，并且，用**crypto key pubkey-chain dss命令**，剪贴您的对等`路由器的公共密钥到路由器。

您能自动地也使用**crypto key exchange dss命令**有路由器交换公共密钥。如果使用自动化方法，请确保那里是在用于密钥交换的接口的没有**加密映射语句**。**debug crypto key**有用的在这里。

注意： 它是一个好想法在交换前密钥的尝试**ping**您的对等体。

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#

即然公共DSS密钥被交换了，请确保两路由器有彼此的公共密钥，并且他们配比，如下面命令输出所显示。

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

示例 1：专用链路的Cisco IOS配置

在DSS密钥在每个路由器后生成，并且DSS公共密钥被交换了， **crypto map命令**可以应用到接口。crypto会话通过生成匹配访问列表使用由加密映射的流量开始。

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 1AeuFSMx7O/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#

示例 2：多点帧中继的Cisco IOS配置

以下示例命令输出从中心路由器被采取了。

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 1AeuFSMx7O/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#

以下示例命令输出从远程站点A.被采取了。

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#
```

以下示例命令输出从远程站点B.被采取了。

```
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#
```

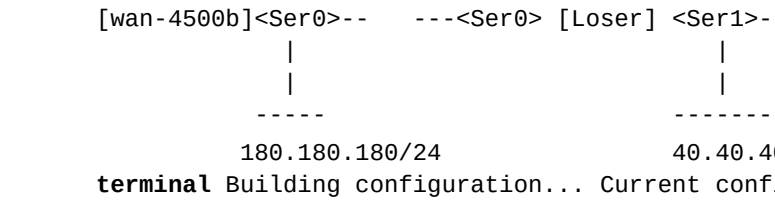
以下示例命令输出从帧中继交换机被采取了。

```
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
!
```

示例 3：加密对和通过路由器

对等`路由器不必须是离开一的跳。您能创建一次对等会话用远程路由器。在以下示例中，目标是加密所有网络流量180.180.180.0/24和40.40.40.0/24之间和180.180.180.0/24和30.30.30.0/24之间。没有与加密数据流的不安40.40.40.0/24和30.30.30.0/24之间。

路由器wan-4500b有一个加密会话关联有Loser的并且有StHelen的。通过加密流量从wan-4500b's以太网段到StHelen's以太网段，您避免多余的解密步骤在Loser。Loser传递加密流量到StHelen's serial interfaces，解密。这为IP信息包和CPU周期降低数据流延迟在路由器Loser。因为Loser的一窃听者不能读流量，更加重要地，它非常地强化系统的安全。如果Loser解密流量，有机会可能牵制解密的数据。



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 1AeuFSMx7O/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#

示例4 ：DDR加密

由于Cisco IOS依靠ICMP建立加密会话，必须分类ICMP流量作为“触发的”在拨号器列表，当执行在DDR链路时的加密。

注意： 压缩在Cisco IOS软件版本11.3工作，但是为已加密数据不是有用的。由于已加密数据相当随机查找，压缩只减速事。但是您能留下功能未加密的数据流的。

在某些状况下，您将想要拨号备份到同一路由器。例如，当用户要防止受到一个特定链路的失败在他们的广域网网络时的是有用的。如果两个接口去同一对等体，同一个加密映射在两个接口可以使用。必须用于备份接口为了此功能能正常运行。如果一备份设计安排一个路由器拨号到一个不同的方框，应该相应地创建不同的加密映射，并且对等体设置。再次，应该使用**backup interface命令**。

```
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#
```

示例5 ：IPX数据流的加密在IP隧道的

在本例中，在IP隧道的IPX数据流加密。

注意： 在此通道(IPX)的仅流量加密。其他IP数据流被留下单独。

```
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#
```

示例6 ：加密L2F通道

在本例中，只加密拨号的用户的L2F流量尝试。这里， “user@cisco.com”呼叫本地网络接入服务器(NAS)在他们的城市命名了"DEMO2"并且建立隧道对家用网关CD。所有DEMO2流量(与那其他L2F呼叫方一起)加密。由于L2F使用UDP端口1701，这是访问列表如何被修建，确定哪个流量加密。

注意： 如果加密关联已经不将设置，含义呼叫方是呼叫的第一个人，并且创建L2F通道，呼叫方可能被撤销由于设置加密关联的延迟。这在有足够的CPU电源的路由器可能不发生。并且，您可以要增加**keytimeout**，以便加密设置在非高峰时间，并且卸载只发生。

以下示例命令输出从远程NAS被采取了。

```
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#
```

以下示例命令输出从家用网关被采取了。

```
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
```

排除故障

通过收集信息开始每故障排除过程使用以下通常是最佳的**显示**命令。星号 (*) 表示特别有用的命令。另请参阅 IP 安全故障排除 - 了解和使用 debug 命令，以获取其他信息。

命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令，使用此工具可以查看对 show 命令输出的分析。

注意： 在发出 **debug** 命令之前，请参阅有关 Debug 命令的重要信息。

命令	
show crypto cisco algorithms	show crypto cisco key-timeout
show crypto cisco pregen-dh-pairs	* show crypto engine connections active
show crypto engine connections dropped-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拨回零点	no crypto public-key

- **show crypto cisco algorithms**-您必须启用使用与其他对等体加密路由器联络的所有数据加密标准(DES)算法。如果不启用DES算法，您不能使用该算法，即使您以后尝试分配算法对**加密映射**。如果您的路由器尝试设置加密的通信会话用对等`路由器，并且两路由器没有同一种DES算法启用在两端，加密的会话出故障。如果至少一种共同性DES算法启用在两端，加密的会话能继续。**注意：** 额外的词cisco在Cisco IOS软件版本11.3出现并且是需要的区分在IPSec之间，并且Cisco专有加密在Cisco IOS软件版本11.2查找。`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** -在加密的通信会话建立后，它为一个特定时间长度是有效。在此时间长度以后，会话时间。必须协商个新会话，并且必须生成一新的DES (会话)密钥为了加密的通信能继续。请使用此命令更改加密的通信会话持续的时间，在超时前(时期)。`Loser#`**`show crypto cisco key-timeout`** `Session keys will be re-negotiated every 30 minutes` 在DES密钥重新协商前，请使用这些命令确定时间长度。`StHelen#`**`show crypto conn`** `Connection Table PE UPE Conn_id New_id Algorithm Time 0.0.0.1 0.0.0.1 4 0 DES_56_CFB64 Mar 01 1993 03:16:09 flags:TIME_KEYS StHelen#`**`show crypto key`** `Session keys will be re-negotiated every 30 minutes StHelen#`**`show clock`** `*03:21:23.031 UTC Mon Mar 1 1993`
- **show crypto cisco pregen-dh-pairs** -每加密的会话使用DH编号独有的。在个新会话设立时候，必须生成新建的DH编号对。当会话完成时，这些编号丢弃。生成新建的DH编号对是一个CPU密集型活动，能使会话设置变慢，特别是低端路由器的。要加速会话设置，您能选择有在

保留事前生成和保持的一个规定量DH编号对。然后，当加密的通信会话设置时， DH编号对从该保留提供。在使用后DH编号对，保留自动地重新补充与一个新的DH编号对，因此总是有准备好待用DH编号对。通常不是必要的安排超过一两个DH编号对事前生成，除非您的路由器那么频繁地设置广泛加密的会话一两个DH编号对事前生成的保留太迅速被耗尽。Loser#**show crypto cisco pregen-dh-pairs** Number of pregenerated DH pairs: 10

- **show crypto cisco connections active**下列是示例命令输出。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 dropped-packet**下列是示例命令输出。Loser#**show crypto engine connections dropped-packet** Interface IP-Address Drop Count Serial1 19.19.19.19 39
- **show crypto engine configuration** (是在Cisco IOS软件版本11.2的**show crypto engine brief**。)下列是示例命令输出。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**下列是示例命令输出。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**下列是示例命令输出。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**下列是示例命令输出。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 当您使用**ping命令时，请**注释时间差距。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**下列是示例命令输出。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**下列是示例命令输出。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**下列是示例命令输出。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 ----------> ~~ 如果在加密映射设置的错误对等体，您收到此错误消息。Mar 2 12:19:12.639: CRYPTO-SDU:Far end authentication error:

Connection message verify failed如果crypto算法不配比，您收到此错误消息。Mar 2 12:26:51.091: CRYPTO-SDU: Connection

failed due to incompatible policy如果DSS密钥缺失或无效，您收到此错误消息。Mar 16 13:33:15.703: CRYPTO-SDU:Far end authentication error:

Connection message verify failed

- **debug crypto key**下列是示例命令输出。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**下列是示例命令输出。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拨回零点**下列是示例命令输出。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**下列是示例命令输出。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#

排除故障与ESA的Cisco7200

Cisco也提供一个硬件协助选项执行在思科7200系列路由器的加密，呼叫ESA。以VIP2-40卡的端口适配器或Cisco7200的，一个独立端口适配器的形式ESA是。此安排允许使用硬件适配器或VIP2软件引擎加密和解密通过在Cisco 7500 VIP2卡的接口进入或离开的数据。Cisco7200允许硬件协助加密所有接口的流量在Cisco 7200机箱。使用加密协助保存能在其他目的使用的珍贵的CPU周期，例如路由或任何其他Cisco IOS功能。

在Cisco7200，独立端口适配器配置同一象Cisco IOS软件加密引擎，但是有只使用硬件和决定的一些额外的命令哪个引擎(软件或硬件)将执行加密。

首先，请准备硬件加密的路由器：

```
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]
```

启用或禁用硬件加密如下所示：

```
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.
```

其次，在您启用它前，请生成ESA的密钥。

```
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#
```

排除故障带ESA的VIP2

在VIP2卡的ESA硬件端口适配器用于加密和解密通过在VIP2卡的接口进入或离开的数据。如同Cisco7200，使用加密协助保存珍贵的CPU周期。在这种情况下， **crypto esa enable命令不**存在，因为ESA端口适配器执行端口的加密VIP2卡的，如果接通ESA。**crypto clear-latch**需要应用到该slot，如果ESA端口适配器第一次安装，或者删除然后重新安装。

```
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#
```

由于ESA crypto模块解压缩，您将收到以下错误消息，直到您执行一**crypto clear-latch命令**在该slot，如下所示。

```
----
*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
```

如果忘记一个以前已分配密码，请使用**crypto zeroize命令**而不是**crypto clear-latch命令**重置ESA。在发出**crypto zeroize命令以后**，您必须重新生成和重新交换DSS密钥。当您重新生成DSS密钥时，提示您创建新密码。示例如下所示。

```
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#

相关信息

- Cisco 网络层加密的配置与故障排除：IPSec 和 ISAKMP - 第 2 部分
- 美国国家标准与技术研究所 (NIST) 发布的 DES FIPS 46-2
- 美国国家标准与技术研究所 (NIST) 发布的 DSS FIPS 186
- RSA 实验室关于当前加密术的常见问题
- IETF 安全标准
- 配置 Internet 密钥交换安全协议
- 配置 IPSec 网络安全
- IPSec 支持页面
- 技术支持 - Cisco Systems