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

本文档讨论使用IPSec和互联网安全关联和密钥管理协议(ISAKMP)配置思科网络层加密并排除其故障，并涵盖网络层加密背景信息和基本配置以及IPSec和ISAKMP。

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中引入。它提供了安全数据传输的机制，包括两个组件：

- **路由器身份验证：**在传递加密流量之前，两台路由器使用数字签名标准(DSS)公钥执行一次性双向身份验证，以签署随机质询。
- **网络层加密：**对于IP负载加密，路由器使用Diffie-Hellman密钥交换来安全地生成DES（40或56位会话密钥）、三重DES - 3DES（168位）或更新的高级加密标准 — AES(128位（默认）或192位，或256位密钥),12.2(13)T中引入。新会话密钥是按可配置方式生成的。加密策略由加密映射设置，加密映射使用扩展IP访问列表定义路由器之间要加密的网络、子网、主机或协议对。

加密背景

密码学领域涉及保持通信的私密性。在密码学的历史上，保护敏感通信一直是密码学的重点。加密是将数据转换为不可读的形式。其目的是通过将信息隐藏在任何不想要的人之外，确保隐私，即使他们可以看到加密的数据。解密与加密相反：而是将加密数据转换回可理解的形式。

加密和解密需要使用一些机密信息，通常称为“密钥”。 根据所使用的加密机制，加密和解密可能使用相同的密钥；而对于其他机制，用于加密和解密的密钥可能不同。

数字签名将文档绑定到特定密钥的占有者，而数字时间戳将文档绑定到在特定时间创建它。这些加密机制可用于控制对共享磁盘驱动器、高安全性安装或按次点播付费电视频道的访问。

当现代密码学日益多样化时，密码学从根本上讲是基于难以解决的问题。问题可能很难解决，因为其解决方案需要知道密钥，例如解密加密邮件或签署一些数字文档。问题可能也很难解决，因为它本质上很难完成，例如查找生成给定哈希值的消息。

随着密码学的发展，密码学的分界线变得模糊。今天的密码学也许可以总结为对依赖数学问题存在而难以解决的技术和应用的研究。密码分析师试图破坏加密机制，而密码学是密码学和密码分析相结合的学科。

定义

本部分定义本文档中使用的相关术语。

- **身份验证:**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每五年由美国国家安全局(NSA)验证一次，以满足美国政府的目的。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由美国国家标准与技术研究院在数字签名标准(DSS)中发布，该标准是美国政府课程项目的一部分。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

本节讨论一些基本的网络层加密概念。它包含您应该注意的加密方面。最初，这些问题对您来说可能不合理，但现在阅读这些问题并了解它们是个好主意，因为在您使用加密技术数月之后，这些问题将更有意义。

- 必须注意的是，加密仅发生在接口的输出上，解密仅发生在接口的输入上。在规划策略时，这一区别非常重要。加密和解密策略是对称的。这意味着定义一个自动为您提供另一个。使用加密映射及其关联的扩展访问列表时，仅显式定义加密策略。解密策略使用相同的信息，但当匹配数据包时，它会反转源地址和目的地址以及端口。这样，数据在双工连接的两个方向上都受到保护。crypto map*命令中*的match address **x语**句用于描述离开接口的数据包。换句话说，它描述的是数据包的加密。但是，数据包进入接口时，也必须匹配才能解密。通过遍历访问列表自动完成此操作，源地址和目的地址以及端口颠倒。这为连接提供了对称性。加密映射指向的访问列**表应**仅描述一个（出站）方向的流量。与您定义的访问列表不匹配的IP数据包将被传输，但不会加密。访问列表中的“deny”表示不应匹配这些主机，这意味着它们不会被加密。在这种情况下，“deny”并不表示数据包被丢弃。
- 在扩展访问列表中使用“any”一词时要非常小心。使用“any”会导致流量被丢弃，除非流量流向匹配的“un-encrypting”接口。此外，在Cisco IOS软件版本11.3(3)T中使用IPSec时，不允许使用“any”。
- 在指定源地址或目标地址时不建议使用“any”关键字。指定“any”可能导致路由协议、网络时间协议(NTP)、回声、回声响应和组播流量出现问题，因为接收路由器以静默方式丢弃此流量。如果要使用“any”，则应在“deny”语句前面加上不要加密的流量，如“ntp”。
- 为节省时间，请确保**ping**您尝试与之建立加密关联的对等路由器。此外，在您花太多时间排除错误问题之前，请让终端设备（取决于其流量是否加密）彼此ping。换句话说，在尝试执行加密之前，请确保路由**工作**。远程对等体可能没有出口接口的路由，在这种情况下，您无法与该对等体进行加密会话(您可能可以在该串行接口上使用**ip unnumbered**)。
- 许多WAN点对点链路使用不可路由的IP地址，而Cisco IOS软件版本11.2加密依赖于互联网控制消息协议(ICMP)（这意味着它使用出口串行接口的IP地址进行ICMP）。 这可能会强制您在WAN**接口上**使用未编号的ip。请始终执行**ping**和**traceroute**命令，以确保两台对等（加密/解密）路由器的路由已就绪。
- 仅允许两台路由器共享Diffie-Hellman会话密钥。也就是说，一台路由器无法使用同一会话密钥将加密数据包交换给两个对等体；每对路由器必须具有会话密钥，该会话密钥是它们之间Diffie-Hellman交换的结果。
- 加密引擎位于Cisco IOS、VIP2 Cisco IOS或VIP2上的加密服务适配器(ESA)硬件中。如果没有VIP2,Cisco IOS加密引擎将管理所有端口上的加密策略。在使用VIP2的平台上，有多个加密引擎：一个在Cisco IOS中，一个在每个VIP2中。VIP2上的加密引擎控制位于主板上的端口的加密。
- 确保流量设置为到达准备加密的接口。如果流量以某种方式到达应用了加密映射的接口以外的**接口**，则会静默丢弃该流量。
- 在进行密钥交换时，它有助于控制台（或备用）访问两台路由器；在等待密钥时，可以使被动侧挂起。
- 在CPU**负载方面**,cfb-64比cfb-**8处理**效率更高。
- 路由器需要运行您希望与要使用的密码反馈(CFB)模式配合使用的算法；每个映像的默认值是映像名称（如“56”）(**cfb-64**)。
- 考虑更改密钥超时。30分钟的默认值非常短。尝试将其增加到一天（1440分钟）。
- 每次密钥到期时，密钥重新协商期间会丢弃IP流量。
- 仅选择您真正想要加密的流量（这可节省CPU周期）。
- 使用按需拨号路由(DDR)，使ICMP有趣，否则它永远不会拨出。

- 如果要加密IP以外的流量，请使用隧道。对于隧道，将加密映射应用到物理接口和隧道接口。请参阅示例5:IP隧道中IPX流量的加密，以了解详细信息。
- 两台加密对等路由器无需直接连接。
- 低端路由器可能会给您一条“CPU占用”消息。这可以忽略，因为它告诉您加密使用大量CPU资源。
- 请勿冗余地放置加密路由器，以便您解密和重新加密流量并浪费CPU。只需在两个端点进行加密。请参阅示例3:对路由器进行加密，以获取详细信息。
- 目前，不支持对广播和组播数据包进行加密。如果“安全”路由更新对网络设计非常重要，则应使用内置身份验证的协议，如增强型内部网关路由协议(EIGRP)、开放最短路径优先(OSPF)或路由信息协议版本2(RIPv2)，以确保更新的完整性。

注意事项

注意：下面提到的警告已全部解决。

- 使用ESA进行加密的Cisco 7200路由器无法解密一个会话密钥下的数据包，然后使用不同的会话密钥重新加密。请参阅Cisco Bug ID CSCdj82613(仅限注册客户)。
- 当两台路由器通过加密租用线路和ISDN备用线路连接时，如果租用线路断开，ISDN链路将正常运行。但是，当租用线路再次恢复时，发出ISDN呼叫的路由器会崩溃。请参阅Cisco Bug ID CSCdj00310(仅限注册客户)。
- 对于具有多个VIP的Cisco 7500系列路由器，如果加密映射应用于任何VIP的一个接口，则一个或多个VIP崩溃。请参阅Cisco Bug ID CSCdi88459(仅限注册客户)。
- 对于具有VIP2和ESA的Cisco 7500系列路由器，除非用户位于控制台端口，否则**show crypto card** 命令不显示输出。请参阅Cisco Bug ID CSCdj89070(仅限注册客户)。

Cisco IOS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。

本文档中的所有示例配置都来自Cisco IOS软件版本11.3。Cisco IOS软件版本11.2命令有几处更改，例如添加了以下字词：

- dss。
- 在某些**show** 命令和**crypto map**命令中，cisco可以区分Cisco的专有加密（如Cisco IOS软件版本11.2及更高版本中所示）和Cisco IOS软件版本11.3(2)T中的IPSec。

注意：这些配置示例中使用的IP地址是在思科实验室中随机选择的，旨在完全通用。

步骤 1：手动生成DSS密钥对

需要在参与加密会话的每台路由器上手动生成DSS密钥对（公钥和私钥）。换句话说，每台路由器必须拥有自己的DSS密钥才能参与。加密引擎只能有一个唯一标识它的DSS密钥。在Cisco IOS软件版本11.3中添加了关键字“dss”，以区分DSS和RSA密钥。您可以为路由器自己的DSS密钥指定任何名称（不过，建议使用路由器主机名）。 在功能较弱的CPU（如Cisco 2500系列）上，密钥对生成大约需要5秒或更短时间。

路由器生成一对密钥：

- 公钥（稍后将其发送到参与加密会话的路由器）。
- 私钥(未见或未与他人交换；实际上，它存储在NVRAM的单独部分，无法查看)。

一旦生成路由器的DSS密钥对，它就与该路由器中的加密引擎唯一关联。密钥对生成如以下示例命令输出所示。

```
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#
```

由于您只能生成一个标识路由器的密钥对，因此您可能会覆盖原始密钥，并且需要将公钥与加密关联中的每台路由器重新发送。以下示例命令输出中显示了此信息：

```
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：与对等体手动交换DSS公钥（带外）

生成路由器自己的DSS密钥对是建立加密会话关联的第一步。下一步是与其他路由器交换公钥。您可以手动输入这些公钥，方法是首先输入**show crypto mypubkey**命令来显示路由器的DSS公钥。然后，您交换这些公钥（例如通过电子邮件），并使用**crypto key pubkey-chain dss**命令将对等路由器的公钥剪切并粘贴到路由器中。

您还可以使用crypto key exchange dss**命令让路**由器自动交换公钥。如果使用自动方法，请确保用于密钥交换的接口**上没**有加密映射语句。调试**加密密钥**在此非常有用。

注意：最好在尝试交换密钥**之**前ping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#
```

现在已交换公有DSS密钥，请确保两台路由器都有彼此的公有密钥，且它们匹配，如下面的命令输出所示。

```
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

在每台路由器上生成DSS密钥并交换DSS公钥后，可以将**crypto map** 命令应用于接口。加密会话首先生成与加密映射使用的访问列表匹配的流量。

```
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#
```

示例 2：多点帧中继的Cisco IOS配置

以下命令输出示例来自集线器路由器。

```
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#
```

以下命令输出示例来自远程站点A。

```
WAN-2511a#write terminal
Building configuration...

Current configuration:
!
version 11.3
no service password-encryption
!
hostname WAN-2511a
!
enable password ww
!
no ip domain-lookup
!
crypto map mymap 10
 set peer fred
 match address 133
!
crypto key pubkey-chain dss
 named-key fred
  serial-number 02802219
  key-string
   56841777 4F27A574 5005E0F0 CF3C33F5 C6AAD000 5518A8FF 7422C592 021B295D
   D95AAB73 01235FD8 40D70284 3A63A38E 216582E8 EC1F8B0D 0256EFF5 0EE89436
  quit
!
interface Ethernet0
 ip address 210.210.210.210 255.255.255.0
 shutdown
!
interface Serial0
 ip address 19.19.19.21 255.255.255.0
 encapsulation frame-relay
 no fair-queue
 crypto map mymap
!
ip default-gateway 10.11.19.254
ip classless
ip route 190.190.190.0 255.255.255.0 19.19.19.19
access-list 133 permit ip 210.210.210.0 0.0.0.255 190.190.190.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line 1
 no exec
 transport input all
line 2 16
```

```
 no exec
line aux 0
line vty 0 4
 password ww
 login
!
end

WAN-2511a#
```

以下命令输出示例来自远程站点B。

```
StHelen#write terminal
Building configuration...

Current configuration:
!
! Last configuration change at 19:00:34 UTC Tue Mar 10 1998
! NVRAM config last updated at 18:48:39 UTC Tue Mar 10 1998
!
version 11.3
service timestamps debug datetime msec
no service password-encryption
!
hostname StHelen
!
boot system flash c2500-is56-l
enable password ww
!
partition flash 2 8 8
!
no ip domain-lookup
!
crypto map wabba 10
 set peer fred
 match address 144
!
crypto key pubkey-chain dss
 named-key fred
  serial-number 02802219
  key-string
   56841777 4F27A574 5005E0F0 CF3C33F5 C6AAD000 5518A8FF 7422C592 021B295D
   D95AAB73 01235FD8 40D70284 3A63A38E 216582E8 EC1F8B0D 0256EFF5 0EE89436
  quit
!
interface Ethernet0
 ip address 200.200.200.200 255.255.255.0
!
interface Serial1
 ip address 19.19.19.20 255.255.255.0
 encapsulation frame-relay
 no ip mroute-cache
 crypto map wabba
!
ip default-gateway 10.11.19.254
ip classless
ip route 190.190.190.0 255.255.255.0 19.19.19.19
access-list 144 permit ip 200.200.200.0 0.0.0.255 190.190.190.0 0.0.0.255
!
line con 0
 exec-timeout 0 0
line aux 0
 transport input all
```

```
line vty 0 4
 password ww
 login
!
end

StHelen#
```

以下命令输出示例来自帧中继交换机。

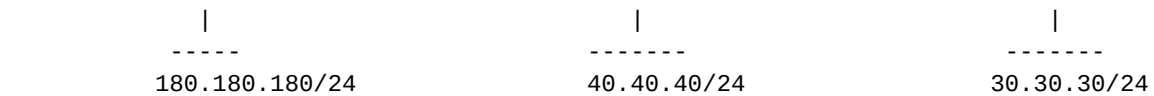
```
Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname wan-4700a
!
enable password ww
!
no ip domain-lookup
frame-relay switching
!
interface Serial0
 no ip address
 encapsulation frame-relay
 clockrate 500000
 frame-relay 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：对路由器进行加密和通过路由器进行加密

对等路由器不必一跳。您可以与远程路由器创建对等会话。在以下示例中，目标是加密180.180.180.0/24和40.40.40.0/24之间以及180.180.180.0/24和30.30.30.0/24之间的所有网络流量。加密40.40.40.0/24和30.30.30.0/24之间的流量时不考虑。

路由器wan-4500b与Loser和StHelen有加密会话关联。通过加密从wan-4500b的以太网段到StHelen的以太网段的流量，您避免了在Loser处执行不必要的解密步骤。失败者只需将已加密的流量传递到StHelen的串行接口，然后在该接口解密。这可减少路由器失败者上IP数据包和CPU周期的流量延迟。更重要的是，由于窃听者无法读取流量，因此大大提高了系统的安全性。如果失败者解密流量，则解密的数据有可能被转移。

```
[wan-4500b]<Ser0>--    ---<Ser0> [Loser] <Ser1>--    ----<Ser1>[StHelen]
             |                                |                              |
```




```
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#
```

示例 4：DDR加密

由于Cisco IOS依赖ICMP来建立加密会话，因此在通过DDR链路进行加密时，ICMP流量必须在拨号器列表中被分类为“相关”。

注意：压缩在Cisco IOS软件版本11.3中确实有效，但对加密数据而言，它并非非常有用。由于加密数据相当随机，压缩只会减慢速度。但是，对于非加密流量，可以将该功能保留为打开状态。

在某些情况下，您需要拨号备份到同一台路由器。例如，当用户希望防止其WAN网络中特定链路发生故障时，这种方法会很有用。如果两个接口转到同一对等体，则两个接口上可以使用相同的加密映射。必须使用备份接口，此功能才能正常运行。如果备份设计有路由器拨入不同的框，则应创建不同的加密映射并相应地设置对等体。同样，应**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：IP隧道中IPX流量的加密

在本例中，IP隧道中的IPX流量被加密。

注意：仅此隧道(IPX)中的流量会加密。所有其他IP流量都保持独立。

```
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隧道

在本示例中，仅尝试对拨入的用户的L2F流量进行加密。在此，“user@cisco.com”呼叫其所在城市中名为“DEMO2”的本地网络接入服务器(NAS)，并通过隧道连接到家庭网关CD。所有DEMO2流量（以及其他L2F呼叫方的流量）都已加密。由于L2F使用UDP端口1701，因此这就是访问列表的构建方式，用于确定加密的流量。

注意：如果尚未设置加密关联，即呼叫者是第一个呼入并创建L2F隧道的人，则呼叫者可能会因设置加密关联的延迟而被丢弃。在CPU功率足够的路由器上可能不会发生这种情况。此外，您可能希望增加**密钥超时**，以便加密设置和拆除仅在非高峰时段进行。

以下命令输出示例来自远程NAS。

```
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#
```

以下命令输出示例来自家庭网关。

```
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
```

故障排除

通常最好使用以下show命令收集信息，以开始每个故障排**除会**话。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	*显**示加密映射**
debug crypto engine	*调**试加密会话**
debug cry key	clear crypto connection
crypto zerize	no crypto public-key

- **show crypto cisco algorithms**— 必须启用用于与任何其他对等加密路由器通信的所有数据加密标准(DES)算法。如果不启用DES算法，则将无法使用该算法，即使稍后尝试将算法分配到加**密**映射也是如此。如果您的路由器尝试与对等路由器建立加密通信会话，并且两台路由器两端没有启用相同的DES算法，则加密会话会失败。如果两端至少启用了一个通用DES算法，则加密会话可以继续。**注意：**Cisco IOS软件版本11.3中显示了额外的cisco字，需要该字来区分IPSec和Cisco IOS软件版本11.2中的Cisco专有加密。

```
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** — 在建立加密通信会话后，该会话在特定时间段内有效。经过此时间后，会话超时。必须协商新会话，并且必须生成新DES（会话）密钥，加密通信才能继续。使用此命令可更改加密通信会话在到期之前持续的时间（超时）。

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

使用这些命令确定重新协商DES密钥之前的时间长度。

```
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** — 每个加密会话使用唯一的一对DH编号。每次建立新会话时，都必须生成新的DH编号对。会话完成后，这些号码将被丢弃。生成新的DH编号对是CPU密集型活动，会使会话设置速度变慢，尤其是对于低端路由器。要加速会话设置，您可以选择预生成并保留指定数量的DH编号对。然后，当建立加密通信会话时，从该保留提供DH编号对。在使用DH编号对后，将用新的DH编号对自动补充保留，以便始终有一个DH编号对可供使用。通常不需要预生成多个或两个DH编号对，除非您的路由器经常设置多个加密会话，以致一个或两个DH编号对的预生成保留会过快耗尽。

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

- **show crypto cisco connections active**以下是命令输出示例。

```
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**以下是命令输出示例。

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

Serial1              19.19.19.19   39
```

- **show crypto engine configuration**(在Cisco IOS软**件版本11.2**中是show crypto engine brief。)以下是命令输出示例。

```
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**以下是命令输出示例。

```
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**以下是命令输出示例。

```
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**以下是命令输出示例。

```
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
```

使用ping命令时，请注意时**间差**异。

```
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**以下是命令输出示例。

```
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**以下是命令输出示例。

```
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**以下是命令输出示例。

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

如果加密映射上设置了错误的对等体，您将收到此错误消息。

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

如果加密算法不匹配，您将收到此错误消息。

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

如果DSS密钥丢失或无效，您会收到此错误消息。

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

- **debug crypto key**以下是命令输出示例。

```
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**以下是命令输出示例。

```
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 zerize以下是命令输出示例。

```
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以下是命令输出示例。

```
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#
```

使用ESA排除Cisco 7200故障

思科还提供硬件辅助选项，用于在Cisco 7200系列路由器（称为ESA）上进行加密。ESA采用VIP2-40卡的端口适配器或Cisco 7200的独立端口适配器形式。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Cisco 7500 VIP2卡上的接口传入或传出的数据。Cisco 7200允许硬件协助加密Cisco 7200机箱上任何接口的流量。使用加密助手可节省宝贵的CPU周期，这些周期可用于其他用途，例如路由或任何其他Cisco IOS功能。

在Cisco 7200上，独立端口适配器的配置与Cisco IOS软件加密引擎完全相同，但有一些额外命令仅用于硬件和决定哪个引擎（软件或硬件）将执行加密。

首先，为硬件加密准备路由器：

```
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.
```

接下来，在启用ESA之前生成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#
```

使用ESA排除VIP2故障

VIP2卡上的ESA硬件端口适配器用于加密和解密通过VIP2卡上的接口传入或传出的数据。与Cisco 7200一样，使用加密辅助可节省宝贵的CPU周期。在这种情况下，**crypto esa enable**命令不存在，因为如果ESA已插入，ESA端口适配器会对VIP2卡上的端口进行加密。如果ESA端口适配器是首次安装的，则需要将加密清除锁存器应用到该插槽，或者将其移除并重新安装。

```
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#
```

由于已解压ESA加密模块，因此在对该插槽执行**crypto clear-latch**命令之前，您会收到以下错误消息，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
```

如果忘记了之前分配的密码，请使用**crypto zeroize**命令而不是**crypto clear-latch**命令重置ESA。发出crypto zeroize**命令**后，必须重新生成并重新交换DSS密钥。重新生成DSS密钥时，系统会提示您创建新密码。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