Cisco 网络层加密的配置与故障排除：IPSec 和 ISAKMP - 第 2 部分

目录

简介

本技术报告的第 I 部分涵盖网络层加密背景信息和基本网络层加密配置。本文档部分介绍 IP 安全 (IPSec) 和 Internet 安全连接和密钥管理协议 (ISAKMP)。

Cisco IOS 软件版本 11.3T 中引入了 IPSec。IPSec 提供了一种安全数据传输机制，它包括 ISAKMP/Oakley 和 IPSec。

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 11.3(T) 及更高版本

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

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。

IPSec 和 ISAKMP

本文档部分介绍 IPSec 和 ISAKMP。

Cisco IOS 软件版本 11.3T 中引入了 IPSec。IPSec 提供了一种安全数据传输机制，它包括 ISAKMP/Oakley 和 IPSec。

IPsec 协议

IPSec 协议 (RFC 1825) 提供 IP 网络层加密，并定义一组要添加到 IP 数据报的新报头。 这些新报头被放置在 IP 报头之后且在第 4 层协议（通常是 TCP 或 UDP）之前。它们提供有关保护 IP 数据包的有效负载安全的信息，如下所述：

可以并用认证报头(AH)和封装安全有效载荷(ESP)独立地或，虽然为多数应用程序他们中的一个是满足的。对于这两种协议来说，IPSec 不定义要使用的特定安全算法，而是提供一种实现行业标准算法的开放框架。最初， IPSec技术支持MD5的多数实施从RSA Data Security的或安全哈希算法(SHA)如定义由完整性和验证的美国政府。虽然定义如何使用许多其他加密系统（包括 IDEA、Blowfish 和 RC4）的 RFC 可用，但 DES 是目前最常提供的批量加密算法。

- **AH**（请参阅 RFC 1826 ）AH 是一种为 IP 数据报提供较强的完整性和身份验证的机制。它还可以提供不可否认性，这取决于所使用的加密算法和执行密钥的方式。例如，使用不对称数字签名算法（如 RSA）时可以提供不可否认性。AH 不提供机密性和流量分析保护。需要机密性的用户应考虑使用 IP ESP，可将其代替 AH 或与 AH 一起使用。AH 可以出现在每个跃点处都检查的任何其他报头之后，且在中间跃点处不检查的任何其他报头之前。正好位于 AH 前面的 IPv4 或 IPv6 报头的“下一报头”（或“协议”）字段中包含值 51。
- **ESP**（请参阅 RFC 1827 ）ESP 可以出现在 IP 报头之后且最终传输层协议之前的任何位置。Internet 地址分配机构已将协议号 50 分配给 ESP。正好位于 ESP 报头前面的报头的“下一报头”(IPv6) 或“协议”(IPv4) 字段中始终包含值 50。ESP 由未加密的报头以及其后的加密数据组成。加密数据包括受包括的 ESP 报头字段和受保护的用户数据，后者可以是整个 IP 数据报或上层协议帧（如 TCP 或 UDP）。IP ESP 通过加密要保护的数据并将加密数据放入到 IP ESP 的数据部分中，旨在提供机密性和完整性。根据用户的安全性要求，此机制可用于加密传输层分段（如 TCP、UDP、ICMP 或 IGMP）或者整个 IP 数据报。封装受保护的数据是为整个原始数据报提供机密性所必需的。使用此规范将增加参与系统的 IP 协议处理成本，并且还将增大通信延迟。延迟增大主要是因为需要对每个包含 ESP 的 IP 数据报进行加密和解密。在隧道模式 ESP

下，原始 IP 数据报被放置在 ESP 的加密部分，并且整个 ESP 帧被放置在具有未加密 IP 报头的数据报中。未加密 IP 报头中的信息用于将安全数据报从源位置路由到目标位置。IP 报头与 ESP 之间可能包括未加密的 IP 路由报头。此模式允许网络设备（如路由器）充当 IPSec 代理。也就是说，路由器代表主机执行加密。源位置的路由器加密数据包，然后沿 IPSec 隧道转发这些数据包。目标位置的路由器解密原始 IP 数据报，并将它转发到目标系统。隧道模式的主要优点是不需要修改终端系统就可以享受 IP 安全的各种好处。隧道模式还可以防止流量分析；在隧道模式下，攻击者只能确定隧道终点，而不能确定通过隧道发送的数据包的真正源位置和目标位置，即使它们与隧道终点相同亦如此。正如 IETF 所定义的那样，只有在源系统和目标系统都理解 IPSec 时，才能使用 IPSec 传输模式。在大多数情况下，都可采用隧道模式部署 IPSec。这样，您就可以在网络体系结构中实施 IPSec，而不需要修改 PC、服务器和主机上的操作系统或任何应用程序。在传输模式 ESP 下，ESP 报头被插入在 IP 数据报中传输层协议报头（如 TCP、UDP 或 ICMP）的正前面。在此模式下，由于没有加密的 IP 报头或 IP 选项，可以节省带宽。只有 IP 有效负载被加密，原始 IP 报头才会完整保留。此模式的优点是每个数据包中只增加了少量的字节。它还允许公共网络上的设备查看数据包的最终源和目标。通过此功能，您可以基于 IP 报头中的信息对媒介网络执行特殊处理（例如，服务质量）。然而，第 4 层报头将被加密，用于限制对数据包的检查。遗憾的是，通过以明文形式传输 IP 报头，该传输模式允许攻击者执行某些流量分析。例如，攻击者可以看到一个 CEO 何时将大量数据包发送给另一个 CEO。然而，攻击者只知道发送了 IP 数据包；攻击者无法确定这些 IP 数据包是电子邮件还是其他应用程序。

ISAKMP/Oakley

虽然 IPSec 是保护 IP 数据报安全的实际协议，但 ISAKMP 是协商策略的协议，它提供一种公共框架用于生成 IPSec 对等体共享的密钥。ISAKMP 不指定密钥管理或密钥交换的任何详细信息，并且不绑定到任何密钥生成技术。在 ISAKMP 内部，Cisco 使用 Oakley 作为密钥交换协议。通过 Oakley，您可以在五个“已知”组中进行选择。Cisco IOS 支持组 1（一个 768 位密钥）和组 2（一个 1024 位密钥）。Cisco IOS 软件版本 12.1(3)T 中引入了对组 5（一个 1536 位密钥）的支持。

ISAKMP/Oakley 在两个实体之间创建已通过身份验证的安全隧道，然后协商 IPSec 的安全关联。此过程要求这两个实体相互进行身份验证，并建立共享密钥。

双方必须相互进行身份验证。ISAKMP/Oakley 支持多种身份验证方法。双方必须通过使用 RSA 签名、RSA 加密随机密钥或预共享密钥的协商过程，商定一种公共身份验证协议。

双方必须有一个共享的会话密钥，以便加密 ISAKMP/Oakley 隧道。Diffie-Hellman 协议用于商定公共会话密钥。将按如上所述对交换进行身份验证，以防止“中间人”攻击。

这两个步骤，验证和密钥交换，创建ISAKMP/Oakley会话关联(SA)，是在两个设备之间的一个安全隧道。隧道的一端提供一组算法；然后，另一端必须接受其中一种算法或拒绝整个连接。当两端就要使用的算法达成一致时，他们必须生成密钥材料以用于 IPSec AH 和/或 ESP。

IPSec 使用的共享密钥不同于 ISAKMP/Oakley 使用的共享密钥。可以通过再次使用 Diffie-Hellman 以确保完全转发保密来生成 IPSec 共享密钥，也可以通过刷新根据原始 Diffie-Hellman 交换（它通过将其与伪随机数字（随机密钥）混合生成 ISAKMP/Oakley SA）生成的共享密钥来生成 IPSec 共享密钥。第一种方法可提供更好的安全性，但其速度较慢。在大多数实施中，使用这两种方法的组合。也就是说，使用 Diffie-Hellman 进行第一次密钥交换，然后本地策略规定何时使用 Diffie-Hellman 或仅仅进行密钥刷新。完成此操作后，就建立了 IPSec SA。

RSA 签名和 RSA 加密随机密钥都需要远程对等体的公钥，并且它们还要求远程对等体具有本地公钥。公钥在 ISAKMP 中以证书的形式交换。这些证书通过登记获取在Certificate Authority (CA)。如

果路由器中没有证书，当前 ISAKMP 不会协商保护套件 RSA 签名。

Cisco 路由器不创建证书。路由器将创建密钥，并且为这些密钥请求证书。将路由器的密钥绑定到其身份的证书由证书颁发机构创建并签署。这是一种管理功能，证书颁发机构总是要求进行某种验证，确保用户与其所声称的身份一致。这意味着您不能只即时创建新证书。

通信设备将交换它们从证书颁发机构获得的事先存在的证书。证书本身是公共信息，但相应的私钥必须对要使用证书来证明身份的任何人可用。但私钥同时不能让不应该使用该身份的任何人知道。

证书可以标识用户或机器。这取决于实施。大多数早期系统可能使用证书来标识机器。如果证书标识用户，则与该证书对应的私钥的存储方式必须使得相同计算机上的其他用户无法使用该私钥。这通常意味着密钥被加密，或者密钥保存在智能卡中。在早期实施中，更常见的一种情况是密钥被加密。无论在哪种情况下，每次激活密钥时，用户通常必须输入密码短语。

注意： ISAKMP/Oakley 使用 UDP 端口 500 进行协商。AH 的“协议”字段中包含 51，而 ESP 的“协议”字段中包含 50。请确保您不过滤它们。

有关本技术报告中使用的术语的详细信息，请参阅定义部分。

IPSec 和 ISAKMP 的 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。

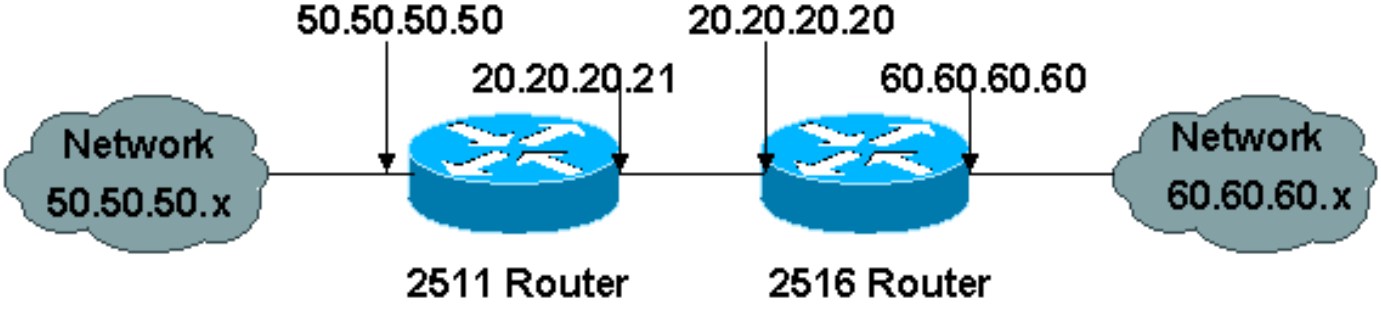
示例 1：ISAKMP 预共享密钥

通过预共享密钥进行身份验证是一种非公钥替代方法。使用此方法，每个对等体都共享已在带外交换或已在路由器中配置的秘密密钥。每端能够表明知道此秘密（不明确说出）的能力将使交换通过身份验证。此方法对于小型安装来说已足够，但存在扩展问题。下面使用了预共享密钥“sharedkey”。如果主机共享基于地址的预共享密钥，则它们必须使用其地址身份（为 Cisco IOS 软件中的默认值），以便它不显示在配置中：

```
crypto isakmp identity address
```

注意： 有时，ISAKMP 无法为 IPSec 建立策略和密钥。如果路由器中未定义证书，并且 ISAKMP 策略中只有基于公钥的身份验证方法，或者如果对等体没有证书且没有预共享的密钥（通过地址或通过配置了该地址的主机名直接共享），则 ISAKMP 无法与对等体协商，并且 IPSec 不起作用。

下图表示此配置的网络图。



以下是根据预共享密钥进行 IPSec 和 ISAKMP 身份验证的两个相邻路由器（Cisco 2511 和 Cisco 2516）的配置。首字符为感叹号的行表示注释行，这些行输入到路由器中后会被忽略。在下面的配

置中，某些配置行前面增加了注释以便对其进行说明。

Cisco 2511 配置

```
cl-2513-2A#write terminal Building configuration...
Current configuration: ! version 11.3 service timestamps
debug uptime service timestamps log uptime no service
password-encryption ! hostname cl-2513-2A ! !---
Override the default policy and use !--- preshared keys
for authentication. crypto isakmp policy 1
authentication pre-share group 2 ! !--- Define our
secret shared key so !--- you do not have to use RSA
keys. crypto isakmp key sharedkey address 20.20.20.20 !
!--- These are the authentication and encryption !---
settings defined for "auth2", !--- which is later
applied to the crypto map. crypto ipsec transform-set
auth2 esp-des esp-sha-hmac ! !--- The crypto map where
you define your peer, !--- transform auth2, and your
access list. crypto map test 10 ipsec-isakmp set peer
20.20.20.20 set transform-set auth2 match address 133 !
interface Ethernet0 ip address 50.50.50.50 255.255.255.0
! interface Serial0 ip address 20.20.20.21 255.255.255.0
no ip route-cache no ip mroute-cache !--- Nothing
happens unless you apply !--- the crypto map to an
interface. crypto map test ! ip route 0.0.0.0 0.0.0.0
20.20.20.20 ! !--- This is the access list referenced !-
-- in the crypto map; never use "any". !--- You are
encrypting traffic between !--- the remote Ethernet
LANs. access-list 133 permit ip 50.50.50.0 0.0.0.255
60.60.60.0 0.0.0.255 ! line con 0 line aux 0 line vty 0
4 login ! end
```

Cisco 2516 配置

```
cl-2513-2B#show run Building configuration... Current
configuration: ! version 11.3 service timestamps debug
uptime service timestamps log uptime no service
password-encryption ! hostname cl-2513-2B ! ip subnet-
zero ! !--- Override the default policy and use !---
preshared keys for authentication. crypto isakmp policy
1 authentication pre-share group 2 !--- Define the
secret shared key so you !--- do not have to use RSA
keys. crypto isakmp key sharedkey address 20.20.20.21 !-
-- These are the authentication and encryption !---
settings defined for "auth2," !--- which is later
applied to the crypto map. crypto ipsec transform-set
auth2 esp-des esp-sha-hmac !--- The crypto map where you
define the peer, !--- transform auth2, and the access
list. crypto map test 10 ipsec-isakmp set peer
20.20.20.21 set transform-set auth2 match address 144 !
interface Ethernet0 ip address 60.60.60.60 255.255.255.0
no ip directed-broadcast ! !--- Nothing happens unless
you apply !--- the crypto map to an interface. interface
Serial0 ip address 20.20.20.20 255.255.255.0 no ip
directed-broadcast no ip route-cache no ip mroute-cache
clockrate 800000 crypto map test ! ip classless ip route
0.0.0.0 0.0.0.0 20.20.20.21 ! !--- This is the access
list referenced !--- in the crypto map; never use "any".
!--- You are encrypting traffic between !--- the remote
Ethernet LANs. access-list 144 permit ip 60.60.60.0
0.0.0.255 50.50.50.0 0.0.0.255 ! line con 0 transport
input none line aux 0 line vty 0 4 login ! end
```

以下是 **debug** 命令的输出。

```
--------------- Preshare with RSA key defined
(need to remove RSA keys) -----

*Mar  1 00:14:48.579: ISAKMP (10): incorrect policy settings.
 Unable to initiate.
*Mar  1 00:14:48.587: ISAKMP (11): incorrect policy settings.
 Unable to initiate......

--------------- Preshare, wrong hostname ---------------

ISAKMP: no pre-shared key based on hostname wan-2511.cisco.com!
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Aggressive mode
 failed with peer at
20.20.20.21
--------------- Preshare, incompatable policy --------------
wan2511#
*Mar  1 00:33:34.839: ISAKMP (17): processing SA payload. message ID = 0
*Mar  1 00:33:34.843: ISAKMP (17): Checking ISAKMP transform 1
 against priority 1 policy
*Mar  1 00:33:34.843: ISAKMP:      encryption DES-CBC
*Mar  1 00:33:34.843: ISAKMP:      hash SHA
*Mar  1 00:33:34.847: ISAKMP:      default group 2
*Mar  1 00:33:34.847: ISAKMP:      auth pre-share
*Mar  1 00:33:34.847: ISAKMP:      life type in seconds
*Mar  1 00:33:34.851: ISAKMP:      life duration (basic) of 240
*Mar  1 00:33:34.851: ISAKMP (17): atts are acceptable.
 Next payload is 0
*Mar  1 00:33:43.735: ISAKMP (17): processing KE payload.
 message ID = 0
*Mar  1 00:33:54.307: ISAKMP (17): processing NONCE payload.
 message ID = 0
*Mar  1 00:33:54.311: ISAKMP (17): processing ID payload.
 message ID = 0
*Mar  1 00:33:54.331: ISAKMP (17): SKEYID state generated
*Mar  1 00:34:04.867: ISAKMP (17): processing HASH payload.
 message ID = 0
*Mar  1 00:34:04.879: ISAKMP (17): SA has been authenticated
*Mar  1 00:34:06.151: ISAKMP (17): processing SA payload.
 message ID = -1357683133
*Mar  1 00:34:06.155: ISAKMP (17): Checking IPSec proposal 1
*Mar  1 00:34:06.155: ISAKMP: transform 1, AH_MD5_HMAC
*Mar  1 00:34:06.159: ISAKMP:   attributes in transform:
*Mar  1 00:34:06.159: ISAKMP:      encaps is 1
*Mar  1 00:34:06.159: ISAKMP:      SA life type in seconds
*Mar  1 00:34:06.163: ISAKMP:      SA life duration (basic) of 3600
*Mar  1 00:34:06.163: ISAKMP:      SA life type in kilobytes
*Mar  1 00:34:06.163: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:34:06.167: ISAKMP (17): atts not acceptable.
 Next payload is 0
*Mar  1 00:34:06.171: ISAKMP (17): Checking IPSec proposal 1
*Mar  1 00:34:06.171: ISAKMP: transform 1, ESP_DES
*Mar  1 00:34:06.171: ISAKMP:   attributes in transform:
*Mar  1 00:34:06.175: ISAKMP:      encaps is 1
*Mar  1 00:34:06.175: ISAKMP:      SA life type in seconds
*Mar  1 00:34:06.175: ISAKMP:      SA life duration (basic) of 3600
*Mar  1 00:34:06.179: ISAKMP:      SA life type in kilobytes
*Mar  1 00:34:06.179: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:34:06.183: ISAKMP:      HMAC algorithm is SHA
*Mar  1 00:34:06.183: ISAKMP (17): atts are acceptable.
*Mar  1 00:34:06.187: ISAKMP (17): SA not acceptable!
%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Quick mode failed
with peer at 20.20.20.20
```

```
wan2511#

----------------- preshare, debug isakmp ------------------

wan2511#
*Mar  1 00:06:54.179: ISAKMP (1): processing SA payload.
 message ID = 0
*Mar  1 00:06:54.179: ISAKMP (1): Checking ISAKMP transform 1
 against priority 1 policy
*Mar  1 00:06:54.183: ISAKMP:      encryption DES-CBC
*Mar  1 00:06:54.183: ISAKMP:      hash SHA
*Mar  1 00:06:54.183: ISAKMP:      default group 2
*Mar  1 00:06:54.187: ISAKMP:      auth pre-share
*Mar  1 00:06:54.187: ISAKMP:      life type in seconds
*Mar  1 00:06:54.187: ISAKMP:      life duration (basic) of 240
*Mar  1 00:06:54.191: ISAKMP (1): atts are acceptable.
 Next payload is 0
*Mar  1 00:07:02.955: ISAKMP (1): processing KE payload.
 message ID = 0
*Mar  1 00:07:13.411: ISAKMP (1): processing NONCE payload.
 message ID = 0
*Mar  1 00:07:13.415: ISAKMP (1): processing ID payload.
 message ID = 0
*Mar  1 00:07:13.435: ISAKMP (1): SKEYID state generated
*Mar  1 00:07:23.903: ISAKMP (1): processing HASH payload.
 message ID = 0
*Mar  1 00:07:23.915: ISAKMP (1): SA has been authenticated
*Mar  1 00:07:25.187: ISAKMP (1): processing SA payload.
 message ID = 1435594195
*Mar  1 00:07:25.187: ISAKMP (1): Checking IPSec proposal 1
*Mar  1 00:07:25.191: ISAKMP: transform 1, AH_SHA_HMAC
*Mar  1 00:07:25.191: ISAKMP:   attributes in transform:
*Mar  1 00:07:25.191: ISAKMP:      encaps is 1
*Mar  1 00:07:25.195: ISAKMP:      SA life type in seconds
*Mar  1 00:07:25.195: ISAKMP:      SA life duration (basic) of 3600
*Mar  1 00:07:25.195: ISAKMP:      SA life type in kilobytes
*Mar  1 00:07:25.199: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:07:25.203: ISAKMP (1): atts are acceptable.
*Mar  1 00:07:25.203: ISAKMP (1): Checking IPSec proposal 1
*Mar  1 00:07:25.207: ISAKMP: transform 1, ESP_DES
*Mar  1 00:07:25.207: ISAKMP:   attributes in transform:
*Mar  1 00:07:25.207: ISAKMP:      encaps is 1
*Mar  1 00:07:25.211: ISAKMP:      SA life type in seconds
*Mar  1 00:07:25.211: ISAKMP:      SA life duration (basic) of 3600
*Mar  1 00:07:25.211: ISAKMP:      SA life type in kilobytes
*Mar  1 00:07:25.215: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:07:25.215: ISAKMP:      HMAC algorithm is SHA
*Mar  1 00:07:25.219: ISAKMP (1): atts are acceptable.
*Mar  1 00:07:25.223: ISAKMP (1): processing NONCE payload.
 message ID = 1435594195
*Mar  1 00:07:25.227: ISAKMP (1): processing ID payload.
 message ID = 1435594195
*Mar  1 00:07:25.227: ISAKMP (1): processing ID payload.
 message ID = 1435594195
*Mar  1 00:07:25.639: ISAKMP (1): Creating IPSec SAs
*Mar  1 00:07:25.643:         inbound SA from 20.20.20.20
     to 20.20.20.21
        (proxy 60.60.60.0      to 50.50.50.0     )
*Mar  1 00:07:25.647:         has spi 85067251 and
 conn_id 3 and flags 4
*Mar  1 00:07:25.647:         lifetime of 3600 seconds
*Mar  1 00:07:25.647:         lifetime of 4608000 kilobytes
```

```
*Mar  1 00:07:25.651:         outbound SA from 20.20.20.21
     to 20.20.20.20
        (proxy 50.50.50.0      to 60.60.60.0     )
*Mar  1 00:07:25.655:         has spi 57872298 and
 conn_id 4 and flags 4
*Mar  1 00:07:25.655:         lifetime of 3600 seconds
*Mar  1 00:07:25.655:         lifetime of 4608000 kilobytes
*Mar  1 00:07:25.659: ISAKMP (1): Creating IPSec SAs
*Mar  1 00:07:25.659:         inbound SA from 20.20.20.20
   to 20.20.20.21
        (proxy 60.60.60.0      to 50.50.50.0     )
*Mar  1 00:07:25.663:         has spi 538316566 and
 conn_id 5 and flags 4
*Mar  1 00:07:25.663:         lifetime of 3600 seconds
*Mar  1 00:07:25.667:         lifetime of 4608000 kilobytes
*Mar  1 00:07:25.667:         outbound SA from 20.20.20.21
 to 20.20.20.20
        (proxy 50.50.50.0      to 60.60.60.0     )
*Mar  1 00:07:25.671:         has spi 356000275 and
 conn_id 6 and flags 4
*Mar  1 00:07:25.671:         lifetime of 3600 seconds
*Mar  1 00:07:25.675:         lifetime of 4608000 kilobytes
wan2511#

----------------- preshare debug ipsec ------------------
wan2511#
*Mar  1 00:05:26.947: IPSEC(validate_proposal_request):
proposal part #1,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/0.0.0.0/0/0,
    src_proxy= 60.60.60.0/0.0.0.16/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 00:05:26.955: IPSEC(validate_proposal_request):
proposal part #2,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/0.0.0.0/0/0,
    src_proxy= 60.60.60.0/0.0.0.16/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 00:05:26.967: IPSEC(key_engine): got a queue event...
*Mar  1 00:05:26.971: IPSEC(spi_response): getting
 spi 203563166 for SA
        from 20.20.20.20     to 20.20.20.21     for prot 2
*Mar  1 00:05:26.975: IPSEC(spi_response): getting
 spi 194838793 for SA
        from 20.20.20.20     to 20.20.20.21     for prot 3
*Mar  1 00:05:27.379: IPSEC(key_engine): got a queue event...
*Mar  1 00:05:27.379: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/255.255.255.0/0/0,
    src_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xC22209E(203563166), conn_id= 3, keysize= 0, flags= 0x4
*Mar  1 00:05:27.387: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
    src_proxy= 50.50.50.0/255.255.255.0/0/0,
    dest_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x15E010D(22937869), conn_id= 4, keysize= 0, flags= 0x4
```

```
*Mar  1 00:05:27.395: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/255.255.255.0/0/0,
    src_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xB9D0109(194838793), conn_id= 5, keysize= 0, flags= 0x4
*Mar  1 00:05:27.403: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
    src_proxy= 50.50.50.0/255.255.255.0/0/0,
    dest_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xDED0AB4(233638580), conn_id= 6, keysize= 0, flags= 0x4
*Mar  1 00:05:27.415: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.21, sa_prot= 51,
    sa_spi= 0xC22209E(203563166),
    sa_trans= ah-sha-hmac , sa_conn_id= 3
*Mar  1 00:05:27.419: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.20, sa_prot= 51,
    sa_spi= 0x15E010D(22937869),
    sa_trans= ah-sha-hmac , sa_conn_id= 4
*Mar  1 00:05:27.423: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.21, sa_prot= 50,
    sa_spi= 0xB9D0109(194838793),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
*Mar  1 00:05:27.427: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.20, sa_prot= 50,
    sa_spi= 0xDED0AB4(233638580),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
wan2511#

--------------- Preshare, good connection ------
wan2511#
*Mar  1 00:09:45.095: ISAKMP (1): processing SA payload.
 message ID = 0
*Mar  1 00:09:45.099: ISAKMP (1): Checking ISAKMP transform
 1 against priority 1 policy
*Mar  1 00:09:45.099: ISAKMP:      encryption DES-CBC
*Mar  1 00:09:45.103: ISAKMP:      hash SHA
*Mar  1 00:09:45.103: ISAKMP:      default group 2
*Mar  1 00:09:45.103: ISAKMP:      auth pre-share
*Mar  1 00:09:45.107: ISAKMP:      life type in seconds
*Mar  1 00:09:45.107: ISAKMP:      life duration (basic) of 240
*Mar  1 00:09:45.107: ISAKMP (1): atts are acceptable.
Next payload is 0
*Mar  1 00:09:53.867: ISAKMP (1): processing KE payload.
 message ID = 0
*Mar  1 00:10:04.323: ISAKMP (1): processing NONCE payload.
 message ID = 0
*Mar  1 00:10:04.327: ISAKMP (1): processing ID payload.
 message ID = 0
*Mar  1 00:10:04.347: ISAKMP (1): SKEYID state generated
*Mar  1 00:10:15.103: ISAKMP (1): processing HASH payload.
 message ID = 0
*Mar  1 00:10:15.115: ISAKMP (1): SA has been authenticated
*Mar  1 00:10:16.391: ISAKMP (1): processing SA payload.
 message ID = 800032287
*Mar  1 00:10:16.391: ISAKMP (1): Checking IPSec proposal 1
*Mar  1 00:10:16.395: ISAKMP: transform 1, AH_SHA_HMAC
*Mar  1 00:10:16.395: ISAKMP:   attributes in transform:
*Mar  1 00:10:16.395: ISAKMP:      encaps is 1
*Mar  1 00:10:16.399: ISAKMP:      SA life type in seconds
*Mar  1 00:10:16.399: ISAKMP:      SA life duration (basic) of 3600
```

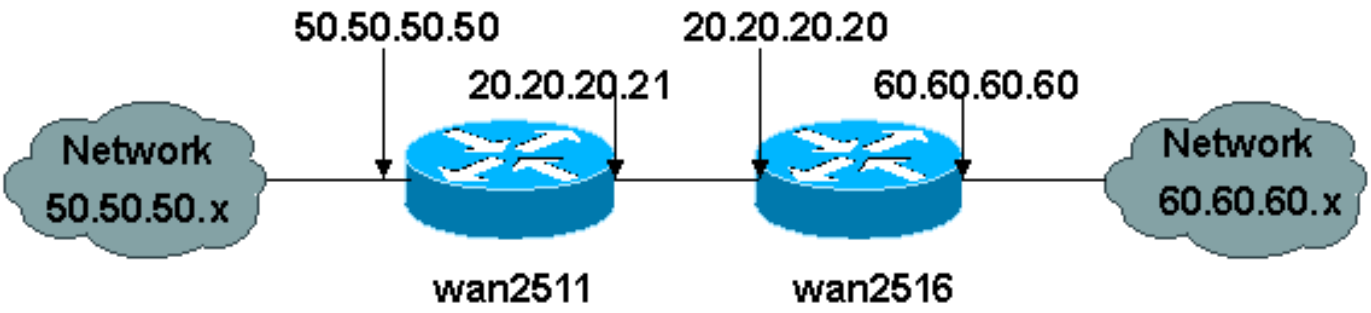
```
*Mar  1 00:10:16.399: ISAKMP:      SA life type in kilobytes
*Mar  1 00:10:16.403: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:10:16.407: ISAKMP (1): atts are acceptable.
*Mar  1 00:10:16.407: ISAKMP (1): Checking IPSec proposal 1
*Mar  1 00:10:16.411: ISAKMP: transform 1, ESP_DES
*Mar  1 00:10:16.411: ISAKMP:   attributes in transform:
*Mar  1 00:10:16.411: ISAKMP:      encaps is 1
*Mar  1 00:10:16.415: ISAKMP:      SA life type in seconds
*Mar  1 00:10:16.415: ISAKMP:      SA life duration (basic) of 3600
*Mar  1 00:10:16.415: ISAKMP:      SA life type in kilobytes
*Mar  1 00:10:16.419: ISAKMP:      SA life duration (VPI) of
  0x0 0x46 0x50 0x0
*Mar  1 00:10:16.419: ISAKMP:      HMAC algorithm is SHA
*Mar  1 00:10:16.423: ISAKMP (1): atts are acceptable.
*Mar  1 00:10:16.427: IPSEC(validate_proposal_request):
 proposal part #1,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/0.0.0.0/0/0,
    src_proxy= 60.60.60.0/0.0.0.16/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 00:10:16.435: IPSEC(validate_proposal_request):
 proposal part #2,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/0.0.0.0/0/0,
    src_proxy= 60.60.60.0/0.0.0.16/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 0s and 0kb,
    spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4
*Mar  1 00:10:16.443: ISAKMP (1): processing NONCE payload.
 message ID = 800032287
*Mar  1 00:10:16.443: ISAKMP (1): processing ID payload.
 message ID = 800032287
*Mar  1 00:10:16.447: ISAKMP (1): processing ID payload.
 message ID = 800032287
*Mar  1 00:10:16.451: IPSEC(key_engine): got a queue event...
*Mar  1 00:10:16.455: IPSEC(spi_response): getting
spi 16457800 for SA
        from 20.20.20.20     to 20.20.20.21     for prot 2
*Mar  1 00:10:16.459: IPSEC(spi_response): getting
spi 305534655 for SA
        from 20.20.20.20     to 20.20.20.21     for prot 3
*Mar  1 00:10:17.095: ISAKMP (1): Creating IPSec SAs
*Mar  1 00:10:17.095:         inbound SA from 20.20.20.20
     to 20.20.20.21
        (proxy 60.60.60.0      to 50.50.50.0     )
*Mar  1 00:10:17.099:         has spi 16457800 and conn_id 3
 and flags 4
*Mar  1 00:10:17.103:         lifetime of 3600 seconds
*Mar  1 00:10:17.103:         lifetime of 4608000 kilobytes
*Mar  1 00:10:17.103:         outbound SA from 20.20.20.21
     to 20.20.20.20
        (proxy 50.50.50.0      to 60.60.60.0     )
*Mar  1 00:10:17.107:         has spi 507120385 and conn_id 4
 and flags 4
*Mar  1 00:10:17.111:         lifetime of 3600 seconds
*Mar  1 00:10:17.111:         lifetime of 4608000 kilobytes
*Mar  1 00:10:17.115: ISAKMP (1): Creating IPSec SAs
*Mar  1 00:10:17.115:         inbound SA from 20.20.20.20
to 20.20.20.21
        (proxy 60.60.60.0      to 50.50.50.0     )
*Mar  1 00:10:17.119:         has spi 305534655 and
```

```
conn_id 5 and flags 4
*Mar  1 00:10:17.119:         lifetime of 3600 seconds
*Mar  1 00:10:17.123:         lifetime of 4608000 kilobytes
*Mar  1 00:10:17.123:         outbound SA from 20.20.20.21
     to 20.20.20.20
        (proxy 50.50.50.0      to 60.60.60.0     )
*Mar  1 00:10:17.127:         has spi 554175376 and
conn_id 6 and flags 4
*Mar  1 00:10:17.127:         lifetime of 3600 seconds
*Mar  1 00:10:17.131:         lifetime of 4608000 kilobytes
*Mar  1 00:10:17.139: IPSEC(key_engine): got a queue event...
*Mar  1 00:10:17.143: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/255.255.255.0/0/0,
    src_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0xFB2048(16457800), conn_id= 3, keysize= 0,
 flags= 0x4
*Mar  1 00:10:17.151: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
    src_proxy= 50.50.50.0/255.255.255.0/0/0,
    dest_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= AH, transform= ah-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x1E3A0B01(507120385), conn_id= 4, keysize= 0,
 flags= 0x4
*Mar  1 00:10:17.159: IPSEC(initialize_sas): ,
  (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
    dest_proxy= 50.50.50.0/255.255.255.0/0/0,
    src_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x123616BF(305534655), conn_id= 5, keysize= 0,
 flags= 0x4
*Mar  1 00:10:17.167: IPSEC(initialize_sas): ,
  (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20,
    src_proxy= 50.50.50.0/255.255.255.0/0/0,
    dest_proxy= 60.60.60.0/255.255.255.0/0/0,
    protocol= ESP, transform= esp-des esp-sha-hmac ,
    lifedur= 3600s and 4608000kb,
    spi= 0x21080B90(554175376), conn_id= 6, keysize= 0,
 flags= 0x4
*Mar  1 00:10:17.175: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.21, sa_prot= 51,
    sa_spi= 0xFB2048(16457800),
    sa_trans= ah-sha-hmac , sa_conn_id= 3
*Mar  1 00:10:17.179: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.20, sa_prot= 51,
    sa_spi= 0x1E3A0B01(507120385),
    sa_trans= ah-sha-hmac , sa_conn_id= 4
*Mar  1 00:10:17.183: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.21, sa_prot= 50,
    sa_spi= 0x123616BF(305534655),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5
*Mar  1 00:10:17.187: IPSEC(create_sa): sa created,
  (sa) sa_dest= 20.20.20.20, sa_prot= 50,
    sa_spi= 0x21080B90(554175376),
    sa_trans= esp-des esp-sha-hmac , sa_conn_id= 6
*Mar  1 00:10:36.583: ISADB: reaper checking SA, conn_id = 1
wan2511#
```

示例 2：ISAKMP ：RSA 加密的身份验证

在此方案中，不创建共享秘密密钥。每个路由器都生成其自己的 RSA 密钥。然后，每个路由器都需要配置对等体的 RSA 公钥。这是一个手动过程，它具有明显的扩展限制。换句话说，路由器需要具有它要与其建立安全关联的每个对等体的 RSA 公钥。

以下文档表示此配置示例的网络图。



在本示例中，每个路由器都生成一个 RSA 密钥对（您不会看到生成的 RSA 私钥），并配置远程对等体的 RSA 公钥。

wan2511(config)#**crypto key generate rsa** The name for the keys will be: wan2511.cisco.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: Generating RSA keys ... [OK] wan2511(config)#**^Z** wan2511# wan2511#**show crypto key mypubkey rsa** % Key pair was generated at: 00:09:04 UTC Mar 1 1993 Key name: wan2511.cisco.com Usage: General Purpose Key Key Data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E9007B E5CD7DC8 6E1C0423 92044254 92C972AD 0CCE9796 86797EAA B6C4EFF0 0F0A5378 6AFAE43B 3A2BD92F 98039DAC 08741E82 5D9053C4 D9CFABC1 AB54E0E2 BB020301 0001 wan2511# wan2511(config)#**crypto key pubkey-chain rsa** wan2511(config-pubkey-chain)#**named-key wan2516.cisco.com** wan2511(config-pubkey-key)#**key-string** Enter a public key as a hexidecimal number .... wan2511(config-pubkey)#**$86F70D 01010105 00034B00 30480241 00DC3DDC 59885F14** wan2511(config-pubkey)#**$D918DE FC7ADB76 B0B9DD1A ABAF4884 009E758C 4064C699** wan2511(config-pubkey)#**$220CB9 31E267F8 0259C640 F8DE4169 1F020301 0001** wan2511(config-pubkey)#**quit** wan2511(config-pubkey-key)#**^Z** wan2511# wan2511#**show crypto key pubkey-chain rsa** Key name: wan2516.cisco.com Key usage: general purpose Key source: manually entered Key data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DC3DDC 59885F14 1AB30DCB 794AB5C7 82D918DE FC7ADB76 B0B9DD1A ABAF4884 009E758C 4064C699 3BC9D17E C47581DC 50220CB9 31E267F8 0259C640 F8DE4169 1F020301 0001 wan2511# wan2511#**write terminal** Building configuration... Current configuration: ! version 11.3 service timestamps debug datetime msec no service password-encryption ! hostname wan2511 ! enable password ww ! no ip domain-lookup ip host wan2516.cisco.com 20.20.20.20 ip domain-name cisco.com ! crypto isakmp policy 1 authentication rsa-encr group 2 lifetime 240 crypto isakmp identity hostname ! crypto ipsec transform-set auth2 ah-sha-hmac esp-des esp-sha-hmac ! crypto map test 10 ipsec-isakmp set peer 20.20.20.20 set transform-set auth2 match address 133 ! crypto key pubkey-chain rsa named-key wan2516.cisco.com key-string 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DC3DDC 59885F14 1AB30DCB 794AB5C7 82D918DE FC7ADB76 B0B9DD1A ABAF4884 009E758C 4064C699 3BC9D17E C47581DC 50220CB9 31E267F8 0259C640 F8DE4169 1F020301 0001 quit ! interface Ethernet0 ip address 50.50.50.50 255.255.255.0 ! interface Serial0 ip address 20.20.20.21 255.255.255.0 encapsulation ppp no ip mroute-cache crypto map test ! interface Serial1 no ip address shutdown ! ip classless ip route 0.0.0.0 0.0.0.0 10.11.19.254 ip route 60.0.0.0 255.0.0.0 20.20.20.20 access-list 133 permit ip 50.50.50.0 0.0.0.255 60.60.60.0 0.0.0.255 ! line con 0 exec-timeout 0 0 password ww login line 1 6 modem InOut transport input all speed 115200 flowcontrol hardware line 7 16 autoselect ppp 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 wan2511# ----------------- wan2516(config)#**crypto key generate rsa** The name for the keys will be: wan2516.cisco.com Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes. How many bits in the modulus [512]: Generating RSA keys ... [OK] wan2516#**show crypto key mypubkey rsa** % Key pair was generated at: 00:06:35 UTC Mar 1 1993 Key name: wan2516.cisco.com Usage: General Purpose Key Key Data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00DC3DDC 59885F14 1AB30DCB 794AB5C7 82D918DE FC7ADB76 B0B9DD1A ABAF4884 009E758C 4064C699 3BC9D17E C47581DC 50220CB9 31E267F8 0259C640 F8DE4169 1F020301 0001 wan2516# -------

wan2516(config)#**crypto key exchange ?** dss Exchange DSS keys ------- wan2516(config)#**crypto key pubkey-chain rsa** wan2516(config-pubkey-chain)#**named-key wan2511.cisco.com** wan2516(config-pubkey-key)#**key-string** Enter a public key as a hexidecimal number .... wan2516(config-pubkey)#**$86F70D 01010105 00034B00 30480241 00E9007B E5CD7DC8** wan2516(config-pubkey)#**$C972AD 0CCE9796 86797EAA B6C4EFF0 0F0A5378 6AFAE43B** wan2516(config-pubkey)#**$741E82 5D9053C4 D9CFABC1 AB54E0E2 BB020301 0001** wan2516(config-pubkey)#**quit** wan2516(config-pubkey-key)#**^Z** wan2516#**show crypto key pubkey rsa** Key name: wan2511.cisco.com Key usage: general purpose Key source: manually entered Key data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E9007B E5CD7DC8 6E1C0423 92044254 92C972AD 0CCE9796 86797EAA B6C4EFF0 0F0A5378 6AFAE43B 3A2BD92F 98039DAC 08741E82 5D9053C4 D9CFABC1 AB54E0E2 BB020301 0001 wan2516# ---------- wan2516#**write terminal** Building configuration... Current configuration: ! version 11.3 no service pad service timestamps debug datetime msec no service password-encryption service udp-small-servers service tcp-small-servers ! hostname wan2516 ! enable password ww ! no ip domain-lookup ip host wan2511.cisco.com 20.20.20.21 ip domain-name cisco.com ! crypto isakmp policy 1 authentication rsa-encr group 2 lifetime 240 crypto isakmp identity hostname ! crypto ipsec transform-set auth2 ah-sha-hmac esp-des esp-sha-hmac ! crypto map test 10 ipsec-isakmp set peer 20.20.20.21 set transform-set auth2 match address 144 ! crypto key pubkey-chain rsa named-key wan2511.cisco.com key-string 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E9007B E5CD7DC8 6E1C0423 92044254 92C972AD 0CCE9796 86797EAA B6C4EFF0 0F0A5378 6AFAE43B 3A2BD92F 98039DAC 08741E82 5D9053C4 D9CFABC1 AB54E0E2 BB020301 0001 quit ! hub ether 0 1 link-test auto-polarity ! interface Loopback0 ip address 70.70.70.1 255.255.255.0 no ip route-cache no ip mroute-cache ! interface Ethernet0 ip address 60.60.60.60 255.255.255.0 ! interface Serial0 ip address 20.20.20.20 255.255.255.0 encapsulation ppp clockrate 2000000 crypto map test ! interface Serial1 no ip address no ip route-cache no ip mroute-cache shutdown ! interface BRI0 no ip address no ip route-cache no ip mroute-cache 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 60.60.60.0 0.0.0.255 50.50.50.0 0.0.0.255 ! 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 wan2516# ---------- RSA-enc missing RSA Keys --------- *Mar 1 00:02:51.147: ISAKMP: No cert, and no keys (public or pre-shared) with remote peer 20.20.20.21 *Mar 1 00:02:51.151: ISAKMP: No cert, and no keys (public or pre-shared) with remote peer 20.20.20.21 ---------- RSA-enc good connection ---------- wan2511# *Mar 1 00:21:46.375: ISAKMP (1): processing SA payload. message ID = 0 *Mar 1 00:21:46.379: ISAKMP (1): Checking ISAKMP transform 1 against priority 1 policy *Mar 1 00:21:46.379: ISAKMP: encryption DES-CBC *Mar 1 00:21:46.379: ISAKMP: hash SHA *Mar 1 00:21:46.383: ISAKMP: default group 2 *Mar 1 00:21:46.383: ISAKMP: auth RSA encr *Mar 1 00:21:46.383: ISAKMP: life type in seconds *Mar 1 00:21:46.387: ISAKMP: life duration (basic) of 240 *Mar 1 00:21:46.387: ISAKMP (1): atts are acceptable. Next payload is 0 *Mar 1 00:21:46.391: Crypto engine 0: generate alg param *Mar 1 00:21:55.159: CRYPTO_ENGINE: Dh phase 1 status: 0 *Mar 1 00:21:55.163: CRYPTO: DH gen phase 1 status for conn_id 1 slot 0:OK *Mar 1 00:21:55.167: ISAKMP (1): Unable to get router cert to find DN! *Mar 1 00:21:55.171: ISAKMP (1): SA is doing RSA encryption authentication *Mar 1 00:22:04.351: ISAKMP (1): processing KE payload. message ID = 0 *Mar 1 00:22:04.351: Crypto engine 0: generate alg param *Mar 1 00:22:14.767: CRYPTO: DH gen phase 2 status for conn_id 1 slot 0:OK *Mar 1 00:22:14.771: ISAKMP (1): processing ID payload. message ID = 0 *Mar 1 00:22:14.775: Crypto engine 0: RSA decrypt with private key *Mar 1 00:22:15.967: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:16.167: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:16.367: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:16.579: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:16.787: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:16.987: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:17.215: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:17.431: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:17.539: CRYPTO: RSA private decrypt finished with status=OK *Mar 1 00:22:17.543: ISAKMP (1): processing NONCE payload. message ID = 0 *Mar 1 00:22:17.543: Crypto engine 0: RSA decrypt with private key *Mar 1 00:22:18.735: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:18.947: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:19.155: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:19.359: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:19.567: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:19.767: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:19.975: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:20.223: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:20.335: CRYPTO: RSA private decrypt finished with status=OK *Mar 1 00:22:20.347: Crypto engine 0: create ISAKMP SKEYID for conn id 1 *Mar 1 00:22:20.363: ISAKMP (1): SKEYID state generated *Mar 1 00:22:20.367: Crypto engine 0: RSA encrypt with public key *Mar 1 00:22:20.567: CRYPTO: RSA public encrypt finished with status=OK *Mar 1 00:22:20.571: Crypto engine 0: RSA encrypt with public key *Mar 1 00:22:20.767: CRYPTO:

RSA public encrypt finished with status=OK *Mar 1 00:22:20.775: ISAKMP (1): processing KE payload. message ID = 0 *Mar 1 00:22:20.775: ISAKMP (1): processing ID payload. message ID = 0 *Mar 1 00:22:20.779: Crypto engine 0: RSA decrypt with private key *Mar 1 00:22:21.959: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:22.187: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:22.399: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:22.599: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:22.811: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:23.019: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:23.223: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:23.471: CRYPTO_ENGINE: key process suspended and continued *Mar 1 00:22:23.583: CRYPTO: RSA private decrypt finished with status=OK *Mar 1 00:22:23.583: ISAKMP (1): processing NONCE payload. message ID = 0 %CRYPTO-6-IKMP_AUTH_FAIL: Authentication method 4 failed with host 20.20.20.20 %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main mode failed with peer at 20.20.20.20 *Mar 1 00:22:36.955: ISAKMP (1): processing HASH payload. message ID = 0 *Mar 1 00:22:36.959: generate hmac context for conn id 1 *Mar 1 00:22:36.971: ISAKMP (1): SA has been authenticated *Mar 1 00:22:36.975: generate hmac context for conn id 1 *Mar 1 00:22:37.311: generate hmac context for conn id 1 *Mar 1 00:22:37.319: ISAKMP (1): processing SA payload. message ID = -114148384 *Mar 1 00:22:37.319: ISAKMP (1): Checking IPSec proposal 1 *Mar 1 00:22:37.323: ISAKMP: transform 1, AH_SHA_HMAC *Mar 1 00:22:37.323: ISAKMP: attributes in transform: *Mar 1 00:22:37.327: ISAKMP: encaps is 1 *Mar 1 00:22:37.327: ISAKMP: SA life type in seconds *Mar 1 00:22:37.327: ISAKMP: SA life duration (basic) of 3600 *Mar 1 00:22:37.331: ISAKMP: SA life type in kilobytes *Mar 1 00:22:37.331: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Mar 1 00:22:37.335: ISAKMP (1): atts are acceptable. *Mar 1 00:22:37.335: ISAKMP (1): Checking IPSec proposal 1 *Mar 1 00:22:37.339: ISAKMP: transform 1, ESP_DES *Mar 1 00:22:37.339: ISAKMP: attributes in transform: *Mar 1 00:22:37.339: ISAKMP: encaps is 1 *Mar 1 00:22:37.343: ISAKMP: SA life type in seconds *Mar 1 00:22:37.343: ISAKMP: SA life duration (basic) of 3600 *Mar 1 00:22:37.347: ISAKMP: SA life type in kilobytes *Mar 1 00:22:37.347: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Mar 1 00:22:37.351: ISAKMP: HMAC algorithm is SHA *Mar 1 00:22:37.351: ISAKMP (1): atts are acceptable. *Mar 1 00:22:37.355: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20, dest_proxy= 50.50.50.0/0.0.0.0/0/0, src_proxy= 60.60.60.0/0.0.0.16/0/0, protocol= AH, transform= ah-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 *Mar 1 00:22:37.363: IPSEC(validate_proposal_request): proposal part #2, (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20, dest_proxy= 50.50.50.0/0.0.0.0/0/0, src_proxy= 60.60.60.0/0.0.0.16/0/0, protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 *Mar 1 00:22:37.371: ISAKMP (1): processing NONCE payload. message ID = -114148384 *Mar 1 00:22:37.375: ISAKMP (1): processing ID payload. message ID = -114148384 *Mar 1 00:22:37.375: ISAKMP (1): processing ID payload. message ID = -114148384 *Mar 1 00:22:37.379: IPSEC(key_engine): got a queue event... *Mar 1 00:22:37.383: IPSEC(spi_response): getting spi 531040311 for SA from 20.20.20.20 to 20.20.20.21 for prot 2 *Mar 1 00:22:37.387: IPSEC(spi_response): getting spi 220210147 for SA from 20.20.20.20 to 20.20.20.21 for prot 3 *Mar 1 00:22:37.639: generate hmac context for conn id 1 *Mar 1 00:22:37.931: generate hmac context for conn id 1 *Mar 1 00:22:37.975: ISAKMP (1): Creating IPSec SAs *Mar 1 00:22:37.975: inbound SA from 20.20.20.20 to 20.20.20.21 (proxy 60.60.60.0 to 50.50.50.0) *Mar 1 00:22:37.979: has spi 531040311 and conn_id 2 and flags 4 *Mar 1 00:22:37.979: lifetime of 3600 seconds *Mar 1 00:22:37.983: lifetime of 4608000 kilobytes *Mar 1 00:22:37.983: outbound SA from 20.20.20.21 to 20.20.20.20 (proxy 50.50.50.0 to 60.60.60.0) *Mar 1 00:22:37.987: has spi 125043658 and conn_id 3 and flags 4 *Mar 1 00:22:37.987: lifetime of 3600 seconds *Mar 1 00:22:37.991: lifetime of 4608000 kilobytes *Mar 1 00:22:37.991: ISAKMP (1): Creating IPSec SAs *Mar 1 00:22:37.991: inbound SA from 20.20.20.20 to 20.20.20.21 (proxy 60.60.60.0 to 50.50.50.0) *Mar 1 00:22:37.995: has spi 220210147 and conn_id 4 and flags 4 *Mar 1 00:22:37.999: lifetime of 3600 seconds *Mar 1 00:22:37.999: lifetime of 4608000 kilobytes *Mar 1 00:22:38.003: outbound SA from 20.20.20.21 to 20.20.20.20 (proxy 50.50.50.0 to 60.60.60.0) *Mar 1 00:22:38.003: has spi 299247102 and conn_id 5 and flags 4 *Mar 1 00:22:38.007: lifetime of 3600 seconds *Mar 1 00:22:38.007: lifetime of 4608000 kilobytes *Mar 1 00:22:38.011: IPSEC(key_engine): got a queue event... *Mar 1 00:22:38.015: IPSEC(initialize_sas): , (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20, dest_proxy= 50.50.50.0/255.255.255.0/0/0, src_proxy= 60.60.60.0/255.255.255.0/0/0, protocol= AH, transform= ah-sha-hmac , lifedur= 3600s and 4608000kb, spi= 0x1FA70837(531040311), conn_id= 2, keysize= 0, flags= 0x4 *Mar 1 00:22:38.023: IPSEC(initialize_sas): , (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20, src_proxy= 50.50.50.0/255.255.255.0/0/0, dest_proxy= 60.60.60.0/255.255.255.0/0/0, protocol= AH, transform= ah-sha-hmac , lifedur= 3600s and 4608000kb, spi= 0x77403CA(125043658), conn_id= 3, keysize= 0, flags= 0x4 *Mar 1 00:22:38.031: IPSEC(initialize_sas): , (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20, dest_proxy= 50.50.50.0/255.255.255.0/0/0, src_proxy= 60.60.60.0/255.255.255.0/0/0, protocol= ESP, transform=

esp-des esp-sha-hmac , lifedur= 3600s and 4608000kb, spi= 0xD2023E3(220210147), conn_id= 4, keysize= 0, flags= 0x4 *Mar 1 00:22:38.039: IPSEC(initialize_sas): , (key eng. msg.) SRC= 20.20.20.21, dest= 20.20.20.20, src_proxy= 50.50.50.0/255.255.255.0/0/0, dest_proxy= 60.60.60.0/255.255.255.0/0/0, protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 3600s and 4608000kb, spi= 0x11D625FE(299247102), conn_id= 5, keysize= 0, flags= 0x4 *Mar 1 00:22:38.047: IPSEC(create_sa): sa created, (sa) sa_dest= 20.20.20.21, sa_prot= 51, sa_spi= 0x1FA70837(531040311), sa_trans= ah-sha-hmac , sa_conn_id= 2 *Mar 1 00:22:38.051: IPSEC(create_sa): sa created, (sa) sa_dest= 20.20.20.20, sa_prot= 51, sa_spi= 0x77403CA(125043658), sa_trans= ah-sha-hmac , sa_conn_id= 3 *Mar 1 00:22:38.055: IPSEC(create_sa): sa created, (sa) sa_dest= 20.20.20.21, sa_prot= 50, sa_spi= 0xD2023E3(220210147), sa_trans= esp-des esp-sha-hmac , sa_conn_id= 4 *Mar 1 00:22:38.063: IPSEC(create_sa): sa created, (sa) sa_dest= 20.20.20.20, sa_prot= 50, sa_spi= 0x11D625FE(299247102), sa_trans= esp-des esp-sha-hmac , sa_conn_id= 5 wan2511# ---------- RSA-ENC ISAKMP debugs good connection --- wan2511# *Mar 1 00:27:23.279: ISAKMP (6): processing SA payload. message ID = 0 *Mar 1 00:27:23.279: ISAKMP (6): Checking ISAKMP transform 1 against priority 1 policy *Mar 1 00:27:23.283: ISAKMP: encryption DES-CBC *Mar 1 00:27:23.283: ISAKMP: hash SHA *Mar 1 00:27:23.283: ISAKMP: default group 2 *Mar 1 00:27:23.287: ISAKMP: auth RSA encr *Mar 1 00:27:23.287: ISAKMP: life type in seconds *Mar 1 00:27:23.287: ISAKMP: life duration (basic) of 240 *Mar 1 00:27:23.291: ISAKMP (6): atts are acceptable. Next payload is 0 *Mar 1 00:27:32.055: ISAKMP (6): Unable to get router cert to find DN! *Mar 1 00:27:32.055: ISAKMP (6): SA is doing RSA encryption authentication *Mar 1 00:27:41.183: ISAKMP (6): processing KE payload. message ID = 0 *Mar 1 00:27:51.779: ISAKMP (6): processing ID payload. message ID = 0 *Mar 1 00:27:54.507: ISAKMP (6): processing NONCE payload. message ID = 0 *Mar 1 00:27:57.239: ISAKMP (6): SKEYID state generated *Mar 1 00:27:57.627: ISAKMP (6): processing KE payload. message ID = 0 *Mar 1 00:27:57.631: ISAKMP (6): processing ID payload. message ID = 0 *Mar 1 00:28:00.371: ISAKMP (6): processing NONCE payload. message ID = 0 %CRYPTO-6-IKMP_AUTH_FAIL: Authentication method 4 failed with host 20.20.20.20 %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main mode failed with peer at 20.20.20.20 *Mar 1 00:28:13.587: ISAKMP (6): processing HASH payload. message ID = 0 *Mar 1 00:28:13.599: ISAKMP (6): SA has been authenticated *Mar 1 00:28:13.939: ISAKMP (6): processing SA payload. message ID = -161552401 *Mar 1 00:28:13.943: ISAKMP (6): Checking IPSec proposal 1 *Mar 1 00:28:13.943: ISAKMP: transform 1, AH_SHA_HMAC *Mar 1 00:28:13.943: ISAKMP: attributes in transform: *Mar 1 00:28:13.947: ISAKMP: encaps is 1 *Mar 1 00:28:13.947: ISAKMP: SA life type in seconds *Mar 1 00:28:13.947: ISAKMP: SA life duration (basic) of 3600 *Mar 1 00:28:13.951: ISAKMP: SA life type in kilobytes *Mar 1 00:28:13.951: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Mar 1 00:28:13.955: ISAKMP (6): atts are acceptable. *Mar 1 00:28:13.959: ISAKMP (6): Checking IPSec proposal 1 *Mar 1 00:28:13.959: ISAKMP: transform 1, ESP_DES *Mar 1 00:28:13.959: ISAKMP: attributes in transform: *Mar 1 00:28:13.963: ISAKMP: encaps is 1 *Mar 1 00:28:13.963: ISAKMP: SA life type in seconds *Mar 1 00:28:13.963: ISAKMP: SA life duration (basic) of 3600 *Mar 1 00:28:13.967: ISAKMP: SA life type in kilobytes *Mar 1 00:28:13.967: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Mar 1 00:28:13.971: ISAKMP: HMAC algorithm is SHA *Mar 1 00:28:13.971: ISAKMP (6): atts are acceptable. *Mar 1 00:28:13.975: ISAKMP (6): processing NONCE payload. message ID = -161552401 *Mar 1 00:28:13.979: ISAKMP (6): processing ID payload. message ID = -161552401 *Mar 1 00:28:13.979: ISAKMP (6): processing ID payload. message ID = -161552401 *Mar 1 00:28:14.391: ISAKMP (6): Creating IPSec SAs *Mar 1 00:28:14.391: inbound SA from 20.20.20.20 to 20.20.20.21 (proxy 60.60.60.0 to 50.50.50.0) *Mar 1 00:28:14.395: has spi 437593758 and conn_id 7 and flags 4 *Mar 1 00:28:14.399: lifetime of 3600 seconds *Mar 1 00:28:14.399: lifetime of 4608000 kilobytes *Mar 1 00:28:14.403: outbound SA from 20.20.20.21 to 20.20.20.20 (proxy 50.50.50.0 to 60.60.60.0) *Mar 1 00:28:14.403: has spi 411835612 and conn_id 8 and flags 4 *Mar 1 00:28:14.407: lifetime of 3600 seconds *Mar 1 00:28:14.407: lifetime of 4608000 kilobytes *Mar 1 00:28:14.411: ISAKMP (6): Creating IPSec SAs *Mar 1 00:28:14.411: inbound SA from 20.20.20.20 to 20.20.20.21 (proxy 60.60.60.0 to 50.50.50.0) *Mar 1 00:28:14.415: has spi 216990519 and conn_id 9 and flags 4 *Mar 1 00:28:14.415: lifetime of 3600 seconds *Mar 1 00:28:14.419: lifetime of 4608000 kilobytes *Mar 1 00:28:14.419: outbound SA from 20.20.20.21 to 20.20.20.20 (proxy 50.50.50.0 to 60.60.60.0) *Mar 1 00:28:14.423: has spi 108733569 and conn_id 10 and flags 4 *Mar 1 00:28:14.423: lifetime of 3600 seconds *Mar 1 00:28:14.427: lifetime of 4608000 kilobytes wan2511# ------------------------- RSA-enc IPSEC debug ------- wan2511# *Mar 1 00:30:32.155: ISAKMP (11): Unable to get router cert to find DN! wan2511#**show debug** Cryptographic Subsystem: Crypto IPSEC debugging is on wan2511# wan2511# wan2511# %CRYPTO-6-IKMP_AUTH_FAIL: Authentication method 4 failed with host 20.20.20.20 %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main mode failed with peer at 20.20.20.20 *Mar 1 00:31:13.931: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20, dest_proxy= 50.50.50.0/0.0.0.0/0/0, src_proxy= 60.60.60.0/0.0.0.16/0/0, protocol= AH, transform= ah-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 *Mar 1 00:31:13.935:

```
IPSEC(validate_proposal_request): proposal part #2, (key eng. msg.) dest= 20.20.20.21, SRC=
20.20.20.20, dest_proxy= 50.50.50.0/0.0.0.0/0/0, src_proxy= 60.60.60.0/0.0.0.16/0/0, protocol=
ESP, transform= esp-des esp-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0,
flags= 0x4 *Mar 1 00:31:13.947: IPSEC(key_engine): got a queue event... *Mar 1 00:31:13.951:
IPSEC(spi_response): getting spi 436869446 for SA from 20.20.20.20 to 20.20.20.21 for prot 2
*Mar 1 00:31:13.955: IPSEC(spi_response): getting spi 285609740 for SA from 20.20.20.20 to
20.20.20.21 for prot 3 *Mar 1 00:31:14.367: IPSEC(key_engine): got a queue event... *Mar 1
00:31:14.367: IPSEC(initialize_sas): , (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20,
dest_proxy= 50.50.50.0/255.255.255.0/0/0, src_proxy= 60.60.60.0/255.255.255.0/0/0, protocol= AH,
transform= ah-sha-hmac , lifedur= 3600s and 4608000kb, spi= 0x1A0A1946(436869446), conn_id= 12,
keysize= 0, flags= 0x4 *Mar 1 00:31:14.375: IPSEC(initialize_sas): , (key eng. msg.) SRC=
20.20.20.21, dest= 20.20.20.20, src_proxy= 50.50.50.0/255.255.255.0/0/0, dest_proxy=
60.60.60.0/255.255.255.0/0/0, protocol= AH, transform= ah-sha-hmac , lifedur= 3600s and
4608000kb, spi= 0x2C40706(46401286), conn_id= 13, keysize= 0, flags= 0x4 *Mar 1 00:31:14.383:
IPSEC(initialize_sas): , (key eng. msg.) dest= 20.20.20.21, SRC= 20.20.20.20, dest_proxy=
50.50.50.0/255.255.255.0/0/0, src_proxy= 60.60.60.0/255.255.255.0/0/0, protocol= ESP, transform=
esp-des esp-sha-hmac , lifedur= 3600s and 4608000kb, spi= 0x11060F0C(285609740), conn_id= 14,
keysize= 0, flags= 0x4 *Mar 1 00:31:14.391: IPSEC(initialize_sas): , (key eng. msg.) SRC=
20.20.20.21, dest= 20.20.20.20, src_proxy= 50.50.50.0/255.255.255.0/0/0, dest_proxy=
60.60.60.0/255.255.255.0/0/0, protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 3600s
and 4608000kb, spi= 0x12881335(310907701), conn_id= 15, keysize= 0, flags= 0x4 *Mar 1
00:31:14.399: IPSEC(create_sa): sa created, (sa) sa_dest= 20.20.20.21, sa_prot= 51, sa_spi=
0x1A0A1946(436869446), sa_trans= ah-sha-hmac , sa_conn_id= 12 *Mar 1 00:31:14.407:
IPSEC(create_sa): sa created, (sa) sa_dest= 20.20.20.20, sa_prot= 51, sa_spi=
0x2C40706(46401286), sa_trans= ah-sha-hmac , sa_conn_id= 13 *Mar 1 00:31:14.411:
IPSEC(create_sa): sa created, (sa) sa_dest= 20.20.20.21, sa_prot= 50, sa_spi=
0x11060F0C(285609740), sa_trans= esp-des esp-sha-hmac , sa_conn_id= 14 *Mar 1 00:31:14.415:
IPSEC(create_sa): sa created, (sa) sa_dest= 20.20.20.20, sa_prot= 50, sa_spi=
0x12881335(310907701), sa_trans= esp-des esp-sha-hmac , sa_conn_id= 15 wan2511#
```

示例 3：ISAKMP ：RSA-SIG 身份验证/CA

本示例使用需要使用 CA 服务器的 RSA 签名。每个对等体都从 CA 服务器（通常是一台配置为发放证书的工作站）获取证书。当两个对等体都具有有效的 CA 证书时，它们将在 ISAKMP 协商过程中自动交换彼此的 RSA 公钥。此方案的所有要求是每个对等体必须向 CA 注册，并且必须获取证书。一个对等体不再需要保留网络中所有对等体的 RSA 公钥。

此外，请注意由于使用的是默认策略，因此未指定 ISAKMP 策略，如下所示：

```
lab-isdn1#show crypto isakmp policy Default protection suite encryption algorithm: DES - Data
Encryption Standard (56 bit keys). hash algorithm: Secure Hash Standard authentication method:
Rivest-Shamir-Adleman Signature Diffie-Hellman group: #1 (768 bit) lifetime: 86400 seconds, no
volume limit
```

首先，定义 CA 服务器的主机名并生成 RSA 密钥。

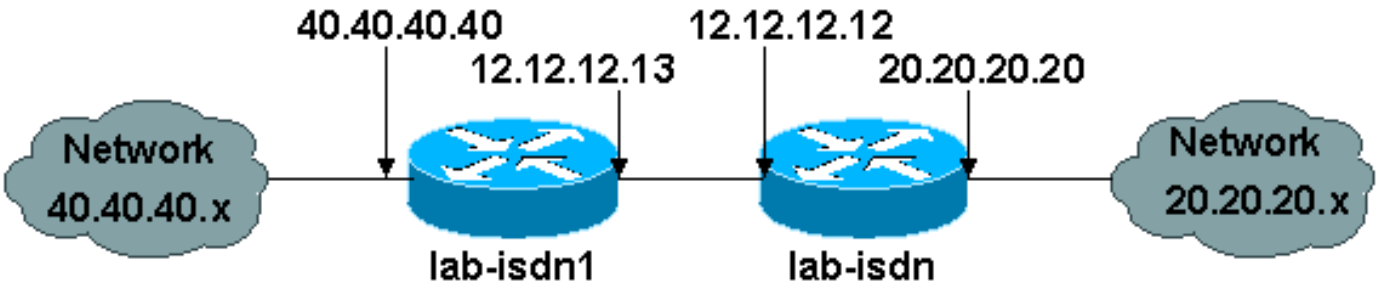
```
test1-isdn(config)#ip host cert-author 10.19.54.46 test1-isdn(config)#crypto key gen rsa usage
The name for the keys will be: test1-isdn.cisco.com Choose the size of the key modulus in the
range of 360 to 2048 for your Signature Keys. Choosing a key modulus greater than 512 may take a
few minutes. How many bits in the modulus [512]: Generating RSA keys ... [OK] Choose the size of
the key modulus in the range of 360 to 2048 for your Encryption Keys. Choosing a key modulus
greater than 512 may take a few minutes. How many bits in the modulus [512]: Generating RSA keys
... [OK]
```

接下来，使用名为“test1-isdn-ultra”的标记定义 CA 配置，并定义 CA 名称 URL。然后，向 CA 服务器进行身份验证并获取证书。最后，进行检查以确保您接收到的证书“可用”。

```
test1-isdn(config)#crypto ca identity test1-isdn-ultra test1-isdn(ca-identity)#enrollment url
http://cert-author test1-isdn(ca-identity)#crl optional test1-isdn(ca-identity)#exit ----------
------------------------ test1-isdn(config)#crypto ca authenticate test1-isdn-ultra Certificate
has the following attributes: Fingerprint: 71CA5A98 78828EF8 4987BA95 57830E5F % Do you accept
this certificate? [yes/no]: yes Apr 3 14:08:56.329: CRYPTO_PKI: http connection opened Apr 3
14:08:56.595: CRYPTO__PKI: All enrollment requests completed. Apr 3 14:08:56.599: CRYPTO_PKI:
```

```
transaction GetCACert completed Apr 3 14:08:56.599: CRYPTO_PKI: CA certificate received test1-isdn(config)# ---------------------------------- test1-isdn(config)#crypto ca enroll test1-isdn-ultra % Start certificate enrollment .. % Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it. Password: Re-enter password: % The subject name in the certificate will be: test1-isdn.cisco.com % Include the router serial number in the subject name? [yes/no]: yes % The serial number in the certificate will be: 04922418 % Include an IP address in the subject name? [yes/no]: yes Interface: bri0 Request certificate from CA? [yes/no]: yes % Certificate request sent to Certificate Authority % The certificate request fingerprint will be displayed. % The 'show crypto ca certificate' command will also show the fingerprint. ----------------- status: pending --------------- test1-isdn#show crypto ca certificate CA Certificate Status: Available Certificate Serial Number: 3051DF7169BEE31B821DFE4B3A338E5F Key Usage: Not Set Certificate Subject Name Name: test1-isdn.cisco.com IP Address: 10.18.117.189 Serial Number: 04922418 Status: Pending Key Usage: Signature Fingerprint: B1566229 472B1DDB 01A072C0 8202A985 00000000 Certificate Subject Name Name: test1-isdn.cisco.com IP Address: 10.18.117.189 Serial Number: 04922418 Status: Pending Key Usage: Encryption Fingerprint: 1EA39C07 D1B26FC7 7AD08BF4 ACA3AABD 00000000 ----------------- status: available --------------- test1-isdn#show crypto ca certificate Certificate Subject Name Name: test1-isdn.cisco.com Serial Number: 04922418 Status: Available Certificate Serial Number: 1BAFCBCA71F0434B59D192FAFB37D376 Key Usage: Encryption CA Certificate Status: Available Certificate Serial Number: 3051DF7169BEE31B821DFE4B3A338E5F Key Usage: Not Set Certificate Subject Name Name: test1-isdn.cisco.com Serial Number: 04922418 Status: Available Certificate Serial Number: 4B39EE2866814279CBA7534496DE1D99 Key Usage: Signature test1-isdn#
```

下图表示此配置示例的网络图。



下面的配置示例来自先前已获取 CA 证书（如上所示）并且打算以“rsa-sig”作为身份验证策略进行 ISAKMP 的两台 Cisco 1600 路由器。只有两个远程以太网 LAN 之间的流量被加密。

```
lab-isdn1#write terminal Building configuration... Current configuration: ! version 11.3 service timestamps debug datetime msec no service password-encryption service udp-small-servers service tcp-small-servers ! hostname lab-isdn1 ! enable secret 5 $1$VdPY$uA/BIVeEm9UAFEm.PPJFc. ! username lab-isdn password 0 cisco ip host ciscoca-ultra 171.69.54.46 ip host lab-isdn 12.12.12.12 ip domain-name cisco.com ip name-server 171.68.10.70 ip name-server 171.68.122.99 isdn switch-type basic-ni1 ! crypto ipsec transform-set mypolicy ah-sha-hmac esp-des esp-sha-hmac ! crypto map test 10 ipsec-isakmp set peer 12.12.12.12 set transform-set mypolicy match address 144 ! crypto ca identity bubba enrollment url http://ciscoca-ultra crl optional crypto ca certificate chain bubba certificate 3E1ED472BDA2CE0163FB6B0B004E5EEE 308201BC 30820166 A0030201 0202103E 1ED472BD A2CE0163 FB6B0B00 4E5EEE30 0D06092A 864886F7 0D010104 05003042 31163014 06035504 0A130D43 6973636F 20537973 74656D73 3110300E 06035504 0B130744 65767465 73743116 30140603 55040313 0D434953 434F4341 2D554C54 5241301E 170D3938 30343038 30303030 30305A17 0D393930 34303832 33353935 395A303B 31273025 06092A86 4886F70D 01090216 18737461 6E6E6F75 732D6973 646E312E 63697363 6F2E636F 6D311030 0E060355 04051307 35363739 39383730 5C300D06 092A8648 86F70D01 01010500 034B0030 48024100 D2D125FF BBFC6E56 93CB4385 5473C165 BC7CCAF6 45C35BED 554BAA0B 119AFA6F 0853F574 5E0B8492 2E39B5FA 84C4DD05 C19AA625 8184395C 6CBC7FA4 614F6177 02030100 01A33F30 3D300B06 03551D0F 04040302 05203023 0603551D 11041C30 1A821873 74616E6E 6F75732D 6973646E 312E6369 73636F2E 636F6D30 09060355 1D130402 3000300D 06092A86 4886F70D 01010405 00034100 04AF83B8 FE95F5D9 9C07C105 F1E88F1A 9320CE7D 0FA540CF 44C77829 FC85C94B 8CB4CA32 85FF9655 8E47AC9A B9D6BF1A 0C4846DE 5CB07C8E A32038EC 8AFD161A quit certificate ca 3051DF7169BEE31B821DFE4B3A338E5F 30820182 3082012C A0030201 02021030 51DF7169 BEE31B82 1DFE4B3A 338E5F30 0D06092A 864886F7 0D010104 05003042 31163014 06035504 0A130D43 6973636F 20537973 74656D73 3110300E 06035504 0B130744 65767465 73743116 30140603 55040313
```

0D434953 434F4341 2D554C54 5241301E 170D3937 31323032 30313036 32385A17 0D393831 32303230
31303632 385A3042 31163014 06035504 0A130D43 6973636F 20537973 74656D73 3110300E 06035504
0B130744 65767465 73743116 30140603 55040313 0D434953 434F4341 2D554C54 5241305C 300D0609
2A864886 F70D0101 01050003 4B003048 024100C1 B69D7BF6 34E4EE28 A84E0DC6 FCA4DEA8 04D89E50
C5EBE862 39D51890 D0D4B732 678BDBF2 80801430 E5E56E7C C126E2DD DBE9695A DF8E5BA7 E67BAE87
29375302 03010001 300D0609 2A864886 F70D0101 04050003 410035AA 82B5A406 32489413 A7FF9A9A
E349E5B4 74615E05 058BA3CE 7C5F00B4 019552A5 E892D2A3 86763A1F 2852297F C68EECE1 F41E9A7B
2F38D02A B1D2F817 3F7B quit certificate 503968D890F7D409475B7280162754D2 308201BC 30820166
A0030201 02021050 3968D890 F7D40947 5B728016 2754D230 0D06092A 864886F7 0D010104 05003042
31163014 06035504 0A130D43 6973636F 20537973 74656D73 3110300E 06035504 0B130744 65767465
73743116 30140603 55040313 0D434953 434F4341 2D554C54 5241301E 170D3938 30343038 30303030
30305A17 0D393930 34303832 33353935 395A303B 31273025 06092A86 4886F70D 01090216 18737461
6E6E6F75 732D6973 646E312E 63697363 6F2E636F 6D311030 0E060355 04051307 35363739 39383730
5C300D06 092A8648 86F70D01 01010500 034B0030 48024100 BECE2D8C B32E6B09 0ADE0D46 AF8D4A1F
37850034 35D0C729 3BF91518 0C9E4CF8 1A6A43AE E4F04687 B8E2859D 33D5CE04 2E5DDEA6 3DA54A31
2AD4255A 756014CB 02030100 01A33F30 3D300B06 03551D0F 04040302 07803023 0603551D 11041C30
1A821873 74616E6E 6F75732D 6973646E 312E6369 73636F2E 636F6D30 09060355 1D130402 3000300D
06092A86 4886F70D 01010405 00034100 B3AF6E71 CBD9AEDD A4711B71 6897F2CE D669A23A EE47B92B
B2BE942A 422DF4A5 7ACB9433 BD17EC7A BB3721EC E7D1175F 5C62BC58 C409F805 19691FBD FD925138 quit !
interface Ethernet0 ip address 40.40.40.40 255.255.255.0 no ip mroute-cache ! interface BRI0 ip
address 12.12.12.13 255.255.255.0 encapsulation ppp no ip mroute-cache dialer idle-timeout 99999
dialer map ip 12.12.12.12 name lab-isdn 4724171 dialer hold-queue 40 dialer-group 1 isdn spid1
919472411800 4724118 isdn spid2 919472411901 4724119 ppp authentication chap crypto map test !
ip classless ip route 0.0.0.0 0.0.0.0 12.12.12.12 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 lab-isdn1# ------------------ lab-isdn#**write terminal** Building
configuration... Current configuration: ! version 11.3 service timestamps debug datetime msec no
service password-encryption service udp-small-servers service tcp-small-servers ! hostname lab-
isdn ! enable secret 5 1oNe1$wDbhBdcN6x9Y5gfuMjqh10 ! username lab-isdn1 password 0 cisco ip
host ciscoca-ultra 171.69.54.46 ip host lab-isdn1 12.12.12.13 ip domain-name cisco.com ip name-
server 171.68.10.70 ip name-server 171.68.122.99 isdn switch-type basic-ni1 ! crypto ipsec
transform-set mypolicy ah-sha-hmac esp-des esp-sha-hmac ! crypto map test 10 ipsec-isakmp set
peer 12.12.12.13 set transform-set mypolicy match address 133 ! crypto ca identity lab
enrollment url http://ciscoca-ultra crl optional crypto ca certificate chain lab certificate
44FC6C531FC3446927E4EE307A806B20 308201E0 3082018A A0030201 02021044 FC6C531F C3446927 E4EE307A
806B2030 0D06092A 864886F7 0D010104 05003042 31163014 06035504 0A130D43 6973636F 20537973
74656D73 3110300E 06035504 0B130744 65767465 73743116 30140603 55040313 0D434953 434F4341
2D554C54 5241301E 170D3938 30343038 30303030 30305A17 0D393930 34303832 33353935 395A305A
31263024 06092A86 4886F70D 01090216 17737461 6E6E6F75 732D6973 646E2E63 6973636F 2E636F6D
311E301C 060A2B06 0104012A 020B0201 130E3137 312E3638 2E313137 2E313839 3110300E 06035504
05130735 36373939 3139305C 300D0609 2A864886 F70D0101 01050003 4B003048 024100B8 F4A17A70
FAB5C2E3 39186513 486779C7 61EF0AC1 3B6CFF83 810E6D28 B3E4C034 CD803CFF 5158C270 28FEBCDE
CB6EF2D4 83BDD9B3 EAF915DB 78266E96 500CD702 03010001 A3443042 300B0603 551D0F04 04030205
20302806 03551D11 0421301F 82177374 616E6E6F 75732D69 73646E2E 63697363 6F2E636F 6D8704AB
4475BD30 09060355 1D130402 3000300D 06092A86 4886F70D 01010405 00034100 BF65B931 0F960195
ABDD41D5 622743D9 C12B5499 B3A8EB30 5005E6CC 7FDF7C5B 51D13EB8 D46187E5 A1E7F711 AEB7B33B
AA4C6728 7A4BA692 00A44A05 C5CF973F quit certificate ca 3051DF7169BEE31B821DFE4B3A338E5F
30820182 3082012C A0030201 02021030 51DF7169 BEE31B82 1DFE4B3A 338E5F30 0D06092A 864886F7
0D010104 05003042 31163014 06035504 0A130D43 6973636F 20537973 74656D73 3110300E 06035504
0B130744 65767465 73743116 30140603 55040313 0D434953 434F4341 2D554C54 5241301E 170D3937
31323032 30313036 32385A17 0D393831 32303230 31303632 385A3042 31163014 06035504 0A130D43
6973636F 20537973 74656D73 3110300E 06035504 0B130744 65767465 73743116 30140603 55040313
0D434953 434F4341 2D554C54 5241305C 300D0609 2A864886 F70D0101 01050003 4B003048 024100C1
B69D7BF6 34E4EE28 A84E0DC6 FCA4DEA8 04D89E50 C5EBE862 39D51890 D0D4B732 678BDBF2 80801430
E5E56E7C C126E2DD DBE9695A DF8E5BA7 E67BAE87 29375302 03010001 300D0609 2A864886 F70D0101
04050003 410035AA 82B5A406 32489413 A7FF9A9A E349E5B4 74615E05 058BA3CE 7C5F00B4 019552A5
E892D2A3 86763A1F 2852297F C68EECE1 F41E9A7B 2F38D02A B1D2F817 3F7B quit certificate
52A46D5D10B18A6F51E6BC735A36508C 308201E0 3082018A A0030201 02021052 A46D5D10 B18A6F51 E6BC735A
36508C30 0D06092A 864886F7 0D010104 05003042 31163014 06035504 0A130D43 6973636F 20537973
74656D73 3110300E 06035504 0B130744 65767465 73743116 30140603 55040313 0D434953 434F4341
2D554C54 5241301E 170D3938 30343038 30303030 30305A17 0D393930 34303832 33353935 395A305A
31263024 06092A86 4886F70D 01090216 17737461 6E6E6F75 732D6973 646E2E63 6973636F 2E636F6D
311E301C 060A2B06 0104012A 020B0201 130E3137 312E3638 2E313137 2E313839 3110300E 06035504
05130735 36373939 3139305C 300D0609 2A864886 F70D0101 01050003 4B003048 024100D7 71AD5672

B487A019 5ECD1954 6F919A3A 6270102E 5A9FF4DC 7A608480 FB27A181 715335F4 399D3E57 7F72B323 BF0620AB 60C371CF 4389BA4F C60EE6EA 21E06302 03010001 A3443042 300B0603 551D0F04 04030207 80302806 03551D11 0421301F 82177374 616E6E6F 75732D69 73646E2E 63697363 6F2E636F 6D8704AB 4475BD30 09060355 1D130402 3000300D 06092A86 4886F70D 01010405 00034100 8AD45375 54803CF3 013829A8 8DB225A8 25342160 94546F3C 4094BBA3 F2F5A378 97E2F06F DCFFC509 A07B930A FBE6C3CA E1FC7FD9 1E69B872 C402E62A A8814C09 quit ! interface Ethernet0 ip address 20.20.20.20 255.255.255.0 ! interface BRI0 description bri to rtp ip address 12.12.12.12 255.255.255.0 no ip proxy-arp encapsulation ppp no ip mroute-cache bandwidth 128 load-interval 30 dialer idle-timeout 99999 dialer hold-queue 40 dialer-group 1 isdn spid1 919472417100 4724171 isdn spid2 919472417201 4724172 ppp authentication chap crypto map test ! ip classless ip route 0.0.0.0 0.0.0.0 12.12.12.13 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 lab-isdn# ------------------ RSA-sig -------------------------- lab-isdn#**show debug**
Cryptographic Subsystem: Crypto ISAKMP debugging is on Crypto Engine debugging is on Crypto IPSEC debugging is on lab-isdn# lab-isdn# *Mar 21 20:16:50.871: ISAKMP (4): processing SA payload. message ID = 0 *Mar 21 20:16:50.871: ISAKMP (4): Checking ISAKMP transform 1 against priority 65535 policy *Mar 21 20:16:50.875: ISAKMP: encryption DES-CBC *Mar 21 20:16:50.875: ISAKMP: hash SHA *Mar 21 20:16:50.875: ISAKMP: default group 1 *Mar 21 20:16:50.875: ISAKMP: auth RSA sig *Mar 21 20:16:50.879: ISAKMP (4): atts are acceptable. Next payload is 0 *Mar 21 20:16:50.879: Crypto engine 0: generate alg param *Mar 21 20:16:54.070: CRYPTO_ENGINE: Dh phase 1 status: 0 *Mar 21 20:16:54.090: ISAKMP (4): SA is doing RSA signature authentication *Mar 21 20:16:57.343: ISAKMP (4): processing KE payload. message ID = 0 *Mar 21 20:16:57.347: Crypto engine 0: generate alg param *Mar 21 20:17:01.168: ISAKMP (4): processing NONCE payload. message ID = 0 *Mar 21 20:17:01.176: Crypto engine 0: create ISAKMP SKEYID for conn id 4 *Mar 21 20:17:01.188: ISAKMP (4): SKEYID state generated *Mar 21 20:17:07.331: ISAKMP (4): processing ID payload. message ID = 0 *Mar 21 20:17:07.331: ISAKMP (4): processing CERT payload. message ID = 0 *Mar 21 20:17:07.497: ISAKMP (4): cert approved with warning *Mar 21 20:17:07.600: ISAKMP (4): processing SIG payload. message ID = 0 *Mar 21 20:17:07.608: Crypto engine 0: RSA decrypt with public key *Mar 21 20:17:07.759: generate hmac context for conn id 4 *Mar 21 20:17:07.767: ISAKMP (4): SA has been authenticated *Mar 21 20:17:07.775: generate hmac context for conn id 4 *Mar 21 20:17:07.783: Crypto engine 0: RSA encrypt with private key *Mar 21 20:17:08.672: CRYPTO_ENGINE: key process suspended and continued *Mar 21 20:17:08.878: CRYPTO_ENGINE: key process suspended and continued *Mar 21 20:17:09.088: CRYPTO_ENGINE: key process suspended and continued *Mar 21 20:17:09.291: CRYPTO_ENGINE: key process suspended and continued *Mar 21 20:17:09.493: CRYPTO_ENGINE: key process suspended and continued *Mar 21 20:17:09.795: CRYPTO_ENGINE: key process suspended and continued *Mar 21 20:17:10.973: generate hmac context for conn id 4 *Mar 21 20:17:10.981: ISAKMP (4): processing SA payload. message ID = -538880964 *Mar 21 20:17:10.981: ISAKMP (4): Checking IPSec proposal 1 *Mar 21 20:17:10.981: ISAKMP: transform 1, AH_SHA_HMAC *Mar 21 20:17:10.985: ISAKMP: attributes in transform: *Mar 21 20:17:10.985: ISAKMP: encaps is 1 *Mar 21 20:17:10.985: ISAKMP: SA life type in seconds *Mar 21 20:17:10.985: ISAKMP: SA life duration (basic) of 3600 *Mar 21 20:17:10.989: ISAKMP: SA life type in kilobytes *Mar 21 20:17:10.989: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Mar 21 20:17:10.993: ISAKMP (4): atts are acceptable. *Mar 21 20:17:10.993: ISAKMP (4): Checking IPSec proposal 1 *Mar 21 20:17:10.993: ISAKMP: transform 1, ESP_DES *Mar 21 20:17:10.997: ISAKMP: attributes in transform: *Mar 21 20:17:10.997: ISAKMP: encaps is 1 *Mar 21 20:17:10.997: ISAKMP: SA life type in seconds *Mar 21 20:17:10.997: ISAKMP: SA life duration (basic) of 3600 *Mar 21 20:17:11.001: ISAKMP: SA life type in kilobytes *Mar 21 20:17:11.001: ISAKMP: SA life duration (VPI) of 0x0 0x46 0x50 0x0 *Mar 21 20:17:11.001: ISAKMP: HMAC algorithm is SHA *Mar 21 20:17:11.005: ISAKMP (4): atts are acceptable. *Mar 21 20:17:11.005: IPSEC(validate_proposal_request): proposal part #1, (key eng. msg.) dest= 12.12.12.12, SRC= 12.12.12.13, dest_proxy= 20.20.20.0/0.0.0.0/0/0, src_proxy= 40.40.40.0/0.0.0.16/0/0, protocol= AH, transform= ah-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 *Mar 21 20:17:11.013: IPSEC(validate_proposal_request): proposal part #2, (key eng. msg.) dest= 12.12.12.12, SRC= 12.12.12.13, dest_proxy= 20.20.20.0/0.0.0.0/0/0, src_proxy= 40.40.40.0/0.0.0.16/0/0, protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 0s and 0kb, spi= 0x0(0), conn_id= 0, keysize= 0, flags= 0x4 *Mar 21 20:17:11.021: ISAKMP (4): processing NONCE payload. message ID = -538880964 *Mar 21 20:17:11.021: ISAKMP (4): processing ID payload. message ID = -538880964 *Mar 21 20:17:11.021: ISAKMP (4): processing ID payload. message ID = -538880964 *Mar 21 20:17:11.025: IPSEC(key_engine): got a queue event... *Mar 21 20:17:11.029: IPSEC(spi_response): getting spi 112207019 for SA from 12.12.12.13 to 12.12.12.12 for prot 2 *Mar 21 20:17:11.033: IPSEC(spi_response): getting spi 425268832 for SA from 12.12.12.13 to 12.12.12.12 for prot 3 *Mar 21 20:17:11.279: generate hmac context for conn id 4 *Mar 21 20:17:11.612: generate hmac context for conn id 4 *Mar 21 20:17:11.644: ISAKMP (4): Creating IPSec SAs *Mar 21 20:17:11.644: inbound SA from 12.12.12.13 to 12.12.12.12 (proxy 40.40.40.0 to

```
20.20.20.0 ) *Mar 21 20:17:11.648: has spi 112207019 and conn_id 5 and flags 4 *Mar 21
20:17:11.648: lifetime of 3600 seconds *Mar 21 20:17:11.648: lifetime of 4608000 kilobytes *Mar
21 20:17:11.652: outbound SA from 12.12.12.12 to 12.12.12.13 (proxy 20.20.20.0 to 40.40.40.0 )
*Mar 21 20:17:11.652: has spi 83231845 and conn_id 6 and flags 4 *Mar 21 20:17:11.656: lifetime
of 3600 seconds *Mar 21 20:17:11.656: lifetime of 4608000 kilobytes *Mar 21 20:17:11.656: ISAKMP
(4): Creating IPSec SAs *Mar 21 20:17:11.656: inbound SA from 12.12.12.13 to 12.12.12.12 (proxy
40.40.40.0 to 20.20.20.0 ) *Mar 21 20:17:11.660: has spi 425268832 and conn_id 7 and flags 4
*Mar 21 20:17:11.660: lifetime of 3600 seconds *Mar 21 20:17:11.664: lifetime of 4608000
kilobytes *Mar 21 20:17:11.664: outbound SA from 12.12.12.12 to 12.12.12.13 (proxy 20.20.20.0 to
40.40.40.0 ) *Mar 21 20:17:11.668: has spi 556010247 and conn_id 8 and flags 4 *Mar 21
20:17:11.668: lifetime of 3600 seconds *Mar 21 20:17:11.668: lifetime of 4608000 kilobytes *Mar
21 20:17:11.676: IPSEC(key_engine): got a queue event... *Mar 21 20:17:11.676:
IPSEC(initialize_sas): , (key eng. msg.) dest= 12.12.12.12, SRC= 12.12.12.13, dest_proxy=
20.20.20.0/255.255.255.0/0/0, src_proxy= 40.40.40.0/255.255.255.0/0/0, protocol= AH, transform=
ah-sha-hmac , lifedur= 3600s and 4608000kb, spi= 0x6B024AB(112207019), conn_id= 5, keysize= 0,
flags= 0x4 *Mar 21 20:17:11.680: IPSEC(initialize_sas): , (key eng. msg.) SRC= 12.12.12.12,
dest= 12.12.12.13, src_proxy= 20.20.20.0/255.255.255.0/0/0, dest_proxy=
40.40.40.0/255.255.255.0/0/0, protocol= AH, transform= ah-sha-hmac , lifedur= 3600s and
4608000kb, spi= 0x4F60465(83231845), conn_id= 6, keysize= 0, flags= 0x4 *Mar 21 20:17:11.687:
IPSEC(initialize_sas): , (key eng. msg.) dest= 12.12.12.12, SRC= 12.12.12.13, dest_proxy=
20.20.20.0/255.255.255.0/0/0, src_proxy= 40.40.40.0/255.255.255.0/0/0, protocol= ESP, transform=
esp-des esp-sha-hmac , lifedur= 3600s and 4608000kb, spi= 0x19591660(425268832), conn_id= 7,
keysize= 0, flags= 0x4 *Mar 21 20:17:11.691: IPSEC(initialize_sas): , (key eng. msg.) SRC=
12.12.12.12, dest= 12.12.12.13, src_proxy= 20.20.20.0/255.255.255.0/0/0, dest_proxy=
40.40.40.0/255.255.255.0/0/0, protocol= ESP, transform= esp-des esp-sha-hmac , lifedur= 3600s
and 4608000kb, spi= 0x21240B07(556010247), conn_id= 8, keysize= 0, flags= 0x4 *Mar 21
20:17:11.699: IPSEC(create_sa): sa created, (sa) sa_dest= 12.12.12.12, sa_prot= 51, sa_spi=
0x6B024AB(112207019), sa_trans= ah-sha-hmac , sa_conn_id= 5 *Mar 21 20:17:11.703:
IPSEC(create_sa): sa created, (sa) sa_dest= 12.12.12.13, sa_prot= 51, sa_spi=
0x4F60465(83231845), sa_trans= ah-sha-hmac , sa_conn_id= 6 *Mar 21 20:17:11.707:
IPSEC(create_sa): sa created, (sa) sa_dest= 12.12.12.12, sa_prot= 50, sa_spi=
0x19591660(425268832), sa_trans= esp-des esp-sha-hmac , sa_conn_id= 7 *Mar 21 20:17:11.707:
IPSEC(create_sa): sa created, (sa) sa_dest= 12.12.12.13, sa_prot= 50, sa_spi=
0x21240B07(556010247), sa_trans= esp-des esp-sha-hmac , sa_conn_id= 8 *Mar 21 20:18:06.767:
ISADB: reaper checking SA, conn_id = 4 lab-isdn#
```

对 IPSec 和 ISAKMP 进行故障排除

通常，在开始每个故障排除会话之前，最好使用以下命令收集信息。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	
debug crypto pki trans	* debug crypto ipsec
* debug crypto isakmp	debug crypto key
debug crypto sess	debug crypto engine
show crypto engine connections active	show crypto engine connections dropped-packet
show crypto engine configuration	* show crypto ca certificates
* show crypto key mypubkey rsa	* show crypto key pubkey-chain rsa
show crypto isakmp	show crypto isakmp sa

policy	
show crypto ipsec sa	show crypto ipsec session-key
show crypto ipsec transform-proposal	show crypto map interface bri 0
show crypto map tag test	clear crypto connection <SA 的连接 ID>
* clear crypto isakmp	* clear crypto sa
clear crypto sa counters	clear crypto sa map
clear crypto sa peer	clear crypto sa spi
clear crypto sa counters	

如下所示是其中一些命令的示例输出。

```
wan2511#show crypto engine connections active ID Interface IP-Address State Algorithm Encrypt
Decrypt 9 Serial0 20.20.20.21 set HMAC_SHA 0 240 10 Serial0 20.20.20.21 set HMAC_SHA 240 0
wan2511#show crypto engine connections dropped-packet Interface IP-Address Drop Count
wan2511#show crypto engine configuration slot: 0 engine name: unknown engine type: software
serial number: 01496536 platform: rp crypto engine crypto lib version: 10.0.0 Encryption Process
Info: input queue top: 140 input queue bot: 140 input queue count: 0 wan2511#show crypto key
mypubkey rsa % Key pair was generated at: 00:09:04 UTC Mar 1 1993 Key name: wan2511.cisco.com
Usage: General Purpose Key Key Data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241
00E9007B E5CD7DC8 6E1C0423 92044254 92C972AD 0CCE9796 86797EAA B6C4EFF0 0F0A5378 6AFAE43B
3A2BD92F 98039DAC 08741E82 5D9053C4 D9CFABC1 AB54E0E2 BB020301 0001 wan2511#show crypto key
pubkey-chain rsa wan2511# wan2511#show crypto isakmp policy Protection suite of priority 1
encryption algorithm: DES - Data Encryption Standard (56 bit keys). hash algorithm: Secure Hash
Standard authentication method: Pre-Shared Key Diffie-Hellman group: #2 (1024 bit) lifetime: 240
seconds, no volume limit Default protection suite encryption algorithm: DES - Data Encryption
Standard (56 bit keys). hash algorithm: Secure Hash Standard authentication method: Rivest-
Shamir-Adleman Signature Diffie-Hellman group: #1 (768 bit) lifetime: 86400 seconds, no volume
limit wan2511#show crypto isakmp sa dst src state conn-id slot 20.20.20.21 20.20.20.20 QM_IDLE 7
0 wan2511# wan2511#show crypto ipsec sa interface: Serial0 Crypto map tag: test, local addr.
20.20.20.21 local ident (addr/mask/prot/port): (50.50.50.0/255.255.255.0/0/0) remote ident
(addr/mask/prot/port): (60.60.60.0/255.255.255.0/0/0) current_peer: 20.20.20.20 PERMIT,
flags={origin_is_acl,ident_is_ipsec,} #pkts encaps: 320, #pkts encrypt: 320, #pkts digest 320
#pkts decaps: 320, #pkts decrypt: 320, #pkts verify 320 #send errors 0, #recv errors 0 local
crypto endpt.: 20.20.20.21, remote crypto endpt.: 20.20.20.20 path mtu 1500, media mtu 1500
current outbound spi: 6625CD inbound esp sas: spi: 0x1925112F(421859631) transform: esp-des esp-
sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 11, crypto map: test sa timing:
remaining key lifetime (k/sec): (4607971/3354) IV size: 8 bytes replay detection support: Y
inbound ah sas: spi: 0x12050DD2(302321106) transform: ah-sha-hmac , in use settings ={Tunnel, }
slot: 0, conn id: 9, crypto map: test sa timing: remaining key lifetime (k/sec): (4607958/3354)
replay detection support: Y outbound esp sas: spi: 0x3262313(52830995) transform: esp-des esp-
sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 12, crypto map: test sa timing:
remaining key lifetime (k/sec): (4607971/3354) IV size: 8 bytes replay detection support: Y
outbound ah sas: spi: 0x6625CD(6694349) transform: ah-sha-hmac , in use settings ={Tunnel, }
slot: 0, conn id: 10, crypto map: test sa timing: remaining key lifetime (k/sec): (4607958/3354)
replay detection support: Y wan2511#show crypto ipsec session-key Session key lifetime: 4608000
kilobytes/3600 seconds wan2511#show crypto ipsec transform-proposal Transform proposal auth2: {
ah-sha-hmac } supported settings = { Tunnel, }, default settings = { Tunnel, }, will negotiate =
{ Tunnel, }, { esp-des esp-sha-hmac } supported settings = { Tunnel, }, default settings = {
Tunnel, }, will negotiate = { Tunnel, }, wan2511#show crypto map interface serial 0 Crypto Map
"test" 10 ipsec-isakmp Peer = 20.20.20.20 Extended IP access list 133 access-list 133 permit ip
source: addr = 50.50.50.0/0.0.0.255 dest: addr = 60.60.60.0/0.0.0.255 Current peer: 20.20.20.20
Session key lifetime: 4608000 kilobytes/3600 seconds PFS (Y/N): N Transform proposals={ auth2, }
wan2511#show crypto map tag test Crypto Map "test" 10 ipsec-isakmp Peer = 20.20.20.20 Extended
IP access list 133 access-list 133 permit ip source: addr = 50.50.50.0/0.0.0.255 dest: addr =
60.60.60.0/0.0.0.255 Current peer: 20.20.20.20 Session key lifetime: 4608000 kilobytes/3600
seconds PFS (Y/N): N Transform proposals={ auth2, } wan2511# ---------------------- lab-
isdn1#show crypto engine connections active ID Interface IP-Address State Algorithm Encrypt
```

Decrypt 5 BRI0 12.12.12.13 set HMAC_SHA 0 89 6 BRI0 12.12.12.13 set HMAC_SHA 89 0 lab-isdn1#**show crypto engine connections dropped-packet** Interface IP-Address Drop Count BRI0 12.12.12.13 4 lab-isdn1#**show crypto engine configuration** slot: 0 engine name: unknown engine type: software serial number: 05679987 platform: rp crypto engine crypto lib version: 10.0.0 Encryption Process Info: input queue top: 243 input queue bot: 243 input queue count: 0 lab-isdn1#**show crypto ca cert** Certificate Subject Name Name: lab-isdn1.cisco.com Serial Number: 05679987 Status: Available Certificate Serial Number: 3E1ED472BDA2CE0163FB6B0B004E5EEE Key Usage: Encryption CA Certificate Status: Available Certificate Serial Number: 3051DF7169BEE31B821DFE4B3A338E5F Key Usage: Not Set Certificate Subject Name Name: lab-isdn1.cisco.com Serial Number: 05679987 Status: Available Certificate Serial Number: 503968D890F7D409475B7280162754D2 Key Usage: Signature lab-isdn1#**show crypto key mypubkey rsa** % Key pair was generated at: 03:10:23 UTC Mar 21 1993 Key name: lab-isdn1.cisco.com Usage: Signature Key Key Data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00BECE2D 8CB32E6B 090ADE0D 46AF8D4A 1F378500 3435D0C7 293BF915 180C9E4C F81A6A43 AEE4F046 87B8E285 9D33D5CE 042E5DDE A63DA54A 312AD425 5A756014 CB020301 0001 % Key pair was generated at: 03:11:17 UTC Mar 21 1993 Key name: lab-isdn1.cisco.com Usage: Encryption Key Key Data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D2D125 FFBBFC6E 5693CB43 855473C1 65BC7CCA F645C35B ED554BAA 0B119AFA 6F0853F5 745E0B84 922E39B5 FA84C4DD 05C19AA6 25818439 5C6CBC7F A4614F61 77020301 0001 lab-isdn1#**show crypto key pubkey-chain rsa** Key name: Cisco SystemsDevtestCISCOCA-ULTRA Key serial number: C7040262 Key usage: signatures only Key source: certificate Key data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C1B69D 7BF634E4 EE28A84E 0DC6FCA4 DEA804D8 9E50C5EB E86239D5 1890D0D4 B732678B DBF28080 1430E5E5 6E7CC126 E2DDDBE9 695ADF8E 5BA7E67B AE872937 53020301 0001 Key name: lab-isdn.cisco.com Key address: 171.68.117.189 Key serial number: 05679919 Key usage: general purpose Key source: certificate Key data: 305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D771AD 5672B487 A0195ECD 19546F91 9A3A6270 102E5A9F F4DC7A60 8480FB27 A1817153 35F4399D 3E577F72 B323BF06 20AB60C3 71CF4389 BA4FC60E E6EA21E0 63020301 0001 lab-isdn1#**show crypto isakmp policy** Default protection suite encryption algorithm: DES - Data Encryption Standard (56 bit keys). hash algorithm: Secure Hash Standard authentication method: Rivest-Shamir-Adleman Signature Diffie-Hellman group: #1 (768 bit) lifetime: 86400 seconds, no volume limit lab-isdn1#**show crypto isakmp sa** dst src state conn-id slot 12.12.12.12 12.12.12.13 QM_IDLE 4 0 lab-isdn1#**show crypto ipsec sa** interface: BRI0 Crypto map tag: test, local addr. 12.12.12.13 local ident (addr/mask/prot/port): (40.40.40.0/255.255.255.0/0/0) remote ident (addr/mask/prot/port): (20.20.20.0/255.255.255.0/0/0) current_peer: 12.12.12.12 PERMIT, flags={origin_is_acl,ident_is_ipsec,} #pkts encaps: 89, #pkts encrypt: 89, #pkts digest 89 #pkts decaps: 89, #pkts decrypt: 89, #pkts verify 89 #send errors 11, #recv errors 0 local crypto endpt.: 12.12.12.13, remote crypto endpt.: 12.12.12.12 path mtu 1500, media mtu 1500 current outbound spi: 6B024AB inbound esp sas: spi: 0x21240B07(556010247) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 7, crypto map: test sa timing: remaining key lifetime (k/sec): (4607989/3062) IV size: 8 bytes replay detection support: Y inbound ah sas: spi: 0x4F60465(83231845) transform: ah-sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 5, crypto map: test sa timing: remaining key lifetime (k/sec): (4607984/3062) replay detection support: Y outbound esp sas: spi: 0x19591660(425268832) transform: esp-des esp-sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 8, crypto map: test sa timing: remaining key lifetime (k/sec): (4607989/3062) IV size: 8 bytes replay detection support: Y outbound ah sas: spi: 0x6B024AB(112207019) transform: ah-sha-hmac , in use settings ={Tunnel, } slot: 0, conn id: 6, crypto map: test sa timing: remaining key lifetime (k/sec): (4607984/3062) replay detection support: Y lab-isdn1#**show crypto ipsec session-key** Session key lifetime: 4608000 kilobytes/3600 seconds lab-isdn1#**show crypto ipsec transform-proposal** Transform proposal mypolicy: { ah-sha-hmac } supported settings = { Tunnel, }, default settings = { Tunnel, }, will negotiate = { Tunnel, }, { esp-des esp-sha-hmac } supported settings = { Tunnel, }, default settings = { Tunnel, }, will negotiate = { Tunnel, }, lab-isdn1#**show crypto map interface bri 0** Crypto Map "test" 10 ipsec-isakmp Peer = 12.12.12.12 Extended IP access list 144 access-list 144 permit ip source: addr = 40.40.40.0/0.0.0.255 dest: addr = 20.20.20.0/0.0.0.255 Current peer: 12.12.12.12 Session key lifetime: 4608000 kilobytes/3600 seconds PFS (Y/N): N Transform proposals={ mypolicy, } lab-isdn1#**show crypto map tag test** Crypto Map "test" 10 ipsec-isakmp Peer = 12.12.12.12 Extended IP access list 144 access-list 144 permit ip source: addr = 40.40.40.0/0.0.0.255 dest: addr = 20.20.20.0/0.0.0.255 Current peer: 12.12.12.12 Session key lifetime: 4608000 kilobytes/3600 seconds PFS (Y/N): N Transform proposals={ mypolicy, } lab-isdn1# ---------- lab-isdn1#**clear crypto isakmp** lab-isdn1# *Mar 21 20:58:34.503: ISADB: reaper checking SA, conn_id = 4 DELETE IT! *Mar 21 20:58:34.507: generate hmac context for conn id 4 *Mar 21 20:58:34.519: CRYPTO(epa_release_crypto_conn_entry): released conn 4 lab-isdn1# lab-isdn1#**clear crypto sa** lab-isdn1# *Mar 21 20:58:42.495: IPSEC(delete_sa): deleting SA, (sa) sa_dest= 12.12.12.13, sa_prot= 51, sa_spi= 0x4F60465(83231845), sa_trans= ah-sha-hmac , sa_conn_id= 5 *Mar 21 20:58:42.499: CRYPTO(epa_release_crypto_conn_entry): released

```
conn 5 *Mar 21 20:58:42.499: IPSEC(delete_sa): deleting SA, (sa) sa_dest= 12.12.12.12, sa_prot=
51, sa_spi= 0x6B024AB(112207019), sa_trans= ah-sha-hmac , sa_conn_id= 6 *Mar 21 20:58:42.503:
CRYPTO(epa_release_crypto_conn_entry): released conn 6 *Mar 21 20:58:42.503: IPSEC(delete_sa):
deleting SA, (sa) sa_dest= 12.12.12.13, sa_prot= 50, sa_spi= 0x21240B07(556010247), sa_trans=
esp-des esp-sha-hmac , sa_conn_id= 7 *Mar 21 20:58:42.507:
CRYPTO(epa_release_crypto_conn_entry): released conn 7 *Mar 21 20:58:42.507: IPSEC(delete_sa):
deleting SA, (sa) sa_dest= 12.12.12.12, sa_prot= 50, sa_spi= 0x19591660(425268832), sa_trans=
esp-des esp-sha-hmac , sa_conn_id= 8 *Mar 21 20:58:42.511:
CRYPTO(epa_release_crypto_conn_entry): released conn 8 lab-isdn1#
```

相关信息

- Cisco 网络层加密的配置与故障排除：背景信息 - 第 1 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