在ASA和路由器配置示例之间的站点到站点IKEv2通道

目录

简介

本文描述如何设置在思科可适应安全工具(ASA)和运行Cisco IOS软件的路由器之间的一个站点到站点互联网密钥交换版本2 (IKEv2)通道。

先决条件

要求

Cisco 建议您了解以下主题：

- 互联网密钥交换版本2 (IKEv2)
- 证书和公共密钥基础设施(PKI)
- 网络时间协议 (NTP)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件版本9.1(3)的Cisco ASA 5510自适应安全设备
- Cisco 2900系列集成业务路由器(ISR)该运行Cisco IOS软件版本15.3(3)M1

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。

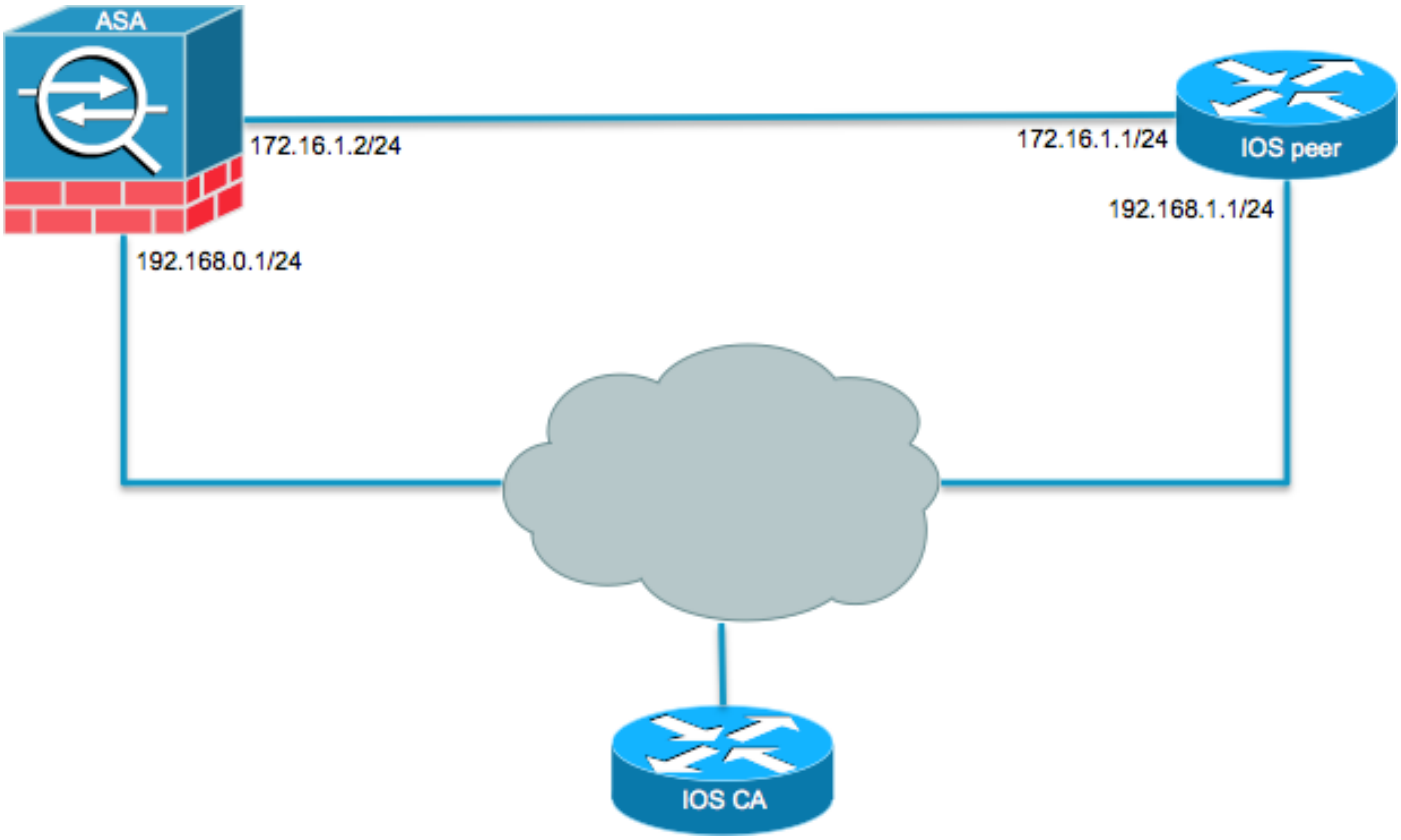
相关产品

本文档也可用于以下硬件和软件版本：

- 运行软件版本8.4(1)或以后的Cisco ASA
- Cisco ISR生成2 (G2)该运行Cisco IOS软件版本15.2(4)M或以上
- Cisco ASR 1000系列汇聚服务路由器该运行Cisco IOS XE软件版本15.2(4)S或以上
- Cisco连接运行软件版本15.2(4)M或以上的网格路由器

配置

网络图



背景信息

一个IKEv2通道的配置在ASA和一个路由器之间的有使用的预先共享密钥是直接的。然而，当您使用身份验证验证，那里是要记住的某些警告。

NTP

证书验证要求在所有参与的设备的时钟同步对共源。当时钟在每个设备时可以手工设置，这不是准确的，并且可以是笨重的。最容易的方法同步在所有设备的时钟是使用NTP。NTP同步在一套的计时分布式时间服务器和客户端中。此同步允许将关联的事件，当系统日志创建时，并且，当其他时间精确的事件发生时。关于如何配置NTP的更多信息，参考网络时间协议：最佳实践白皮书。

> **提示**：当使用时Cisco IOS软件Certificate Authority (CA)服务器，是惯例配置设备和Ntp master一样。在本例中， CA服务器也担当Ntp server。

基于HTTP URL的证书查找

当大证书转接时，根据HTTP URL的证书查找避免该的分段结果。默认情况下此功能在Cisco IOS软件设备启用，因此Cisco IOS软件使用cert req类型12。

如果没有Cisco Bug ID的CSCul48246修正的软件版本在ASA使用，则基于HTTP URL的查找在ASA没有协商，并且Cisco IOS软件导致授权尝试发生故障。

在ASA，如果IKEv2协议调试启用，这些消息出现：

```
IKEv2-PROTO-1: (139): Auth exchange failed
IKEv2-PROTO-1: (140): Unsupported cert encoding found or Peer requested
HTTP URL but never sent
HTTP_LOOKUP_SUPPORTED Notification
```

当并列与ASA时，为了避免此问题，请勿请使用**crypto ikev2 HTTP URL cert**命令为了禁用在路由器的此功能。

对等体ID验证

在IKE验证阶段互联网安全协会和密钥管理协议(ISAKMP)协商中，对等体必须彼此识别。然而，有在方式路由器的一差异，并且ASA选择他们的本地标识。

ISAKMP在路由器的ID选择

当IKEv2通道在路由器时使用，用于协商的本地标识取决于在IKEv2配置文件下的**标识本地命令**：

```
R1(config-ikev2-profile)#identity local ?
 address  address
 dn       Distinguished Name
 email    Fully qualified email string
 fqdn     Fully qualified domain name string
 key-id   key-id opaque string - proprietary types of identification
```

默认情况下，路由器使用地址作为本地标识。

ISAKMP在路由器的ID验证

预计对等体ID在同一配置文件手工也配置用**匹配标识remote command** ：

```
R1(config-ikev2-profile)#match identity remote ?
 address  IP Address(es)
 any      match any peer identity
 email    Fully qualified email string [Max. 255 char(s)]
```

```
 fqdn     Fully qualified domain name string [Max. 255 char(s)]
 key-id   key-id opaque string
```

ISAKMP在ASA的ID选择

在ASA， ISAKMP标识用**crypto isakmp identity命令**选择全局：

```
ciscoasa/vpn(config)# crypto isakmp identity ?
 configure mode commands/options:
 address   Use the IP address of the interface for the identity
 auto      Identity automatically determined by the connection type: IP
           address for preshared key and Cert DN for Cert based connections
 hostname  Use the hostname of the router for the identity
 key-id    Use the specified key-id for the identity
```

默认情况下，命令模式设置为自动，因此意味着ASA由连接类型确定ISAKMP协商：

- 预先共享密钥的IP地址。
- Cert辨别名称对于证书验证。

注意：Cisco Bug ID CSCul48099是能力的一个增强请求能配置根据一个每通道组基本类型而不是在全局配置里。

ISAKMP在ASA的ID验证

远程ID验证自动地完成(确定由连接类型)并且不可能更改。验证可以启用或禁用的根据一个每通道组基本类型用对等体id**验证**命令：

```
ciscoasa/vpn(config-tunnel-ipsec)# peer-id-validate ?
 tunnel-group-ipsec mode commands/options:
 cert     If supported by certificate
 nocheck  Do not check
 req      Required
```

互操作性问题

在ID选择/验证原因的差异两个独立的互操作性问题：

1. 当cert验证在ASA时使用， ASA设法验证从附属的替代方案名称(SAN)的对等体ID在已接收证书。如果对等体ID验证启用，并且，如果IKEv2平台调试在ASA启用，这些调试出现：

```
IKEv2-PROTO-3: (172): Getting configured policies
IKEv2-PLAT-3: attempting to find tunnel group for ID: 172.16.1.1
IKEv2-PLAT-3: mapped to tunnel group 172.16.1.1 using phase 1 ID
IKEv2-PLAT-3: (172) tg_name set to: 172.16.1.1
IKEv2-PLAT-3: (172) tunn grp type set to: L2L
IKEv2-PLAT-3: Peer ID check started, received ID type: IPv4 address
IKEv2-PLAT-2: Peer ID check: failed to retreive IP from SAN
IKEv2-PLAT-2: Peer ID check: failed to retreive DNS name from SAN
IKEv2-PLAT-2: Peer ID check: failed to retreive RFC822 name from SAN
IKEv2-PLAT-1: retrieving SAN for peer ID check
IKEv2-PLAT-1: Peer ID check failed
IKEv2-PROTO-1: (172): Failed to locate an item in the database
IKEv2-PROTO-1: (172):
IKEv2-PROTO-5: (172): SM Trace-> SA: I_SPI=833D2323FCB46093
R_SPI=F0B4D318DDDDB783 (I) MsgID = 00000001 CurState: I_PROC_AUTH
Event: EV_AUTH_FAIL
IKEv2-PROTO-3: (172): Verify auth failed
IKEv2-PROTO-5: (172): SM Trace-> SA: I_SPI=833D2323FCB46093
```

```
R_SPI=F0B4D318DDDDB783 (I) MsgID = 00000001 CurState: AUTH_DONE
Event: EV_FAIL
```

`IKEv2-PROTO-3: (172): Auth exchange failed` 对于此问题，或者证书的IP地址在对等体认证需要包括，或者对等体ID验证在ASA需要禁用。

2. 默认情况下同样地， ASA如此自动地选择本地ID，当使用时cert验证，它发送特有名(DN)作为标识。如果路由器配置收到地址作为远程ID，对等体ID验证在路由器失效。如果IKEv2调试在路由器启用，这些调试出现：

```
Nov 30 22:49:14.464: IKEv2:(SESSION ID = 172,SA ID = 1):SM Trace-> SA:
I_SPI=E9E4B7FD0A336C97 R_SPI=F2CF438C0CCA281C (R) MsgID = 1 CurState:
R_WAIT_AUTH Event: EV_GET_POLICY_BY_PEERID
Nov 30 22:49:14.464: IKEv2:(SESSION ID = 172,SA ID = 1):Searching policy
based on peer's identity 'hostname=asa.cisco.com' of type 'DER ASN1 DN'
Nov 30 22:49:14.464: IKEv2:%Profile could not be found by peer certificate.
Nov 30 22:49:14.468: IKEv2:% IKEv2 profile not found
Nov 30 22:49:14.468: IKEv2:(SESSION ID = 172,SA ID = 1):: Failed to
```

`locate an item in the database` 对于此问题，请配置路由器为了验证完全合格的域名(FQDN)或配置ASA为了使用地址作为ISAKMP ID。**注意**：在路由器上，附加对IKEv2配置文件的证书地图必须配置为了认可DN。*参考*证书对映射*互联网密钥交换的*部分的*IPsec VPN配置指南的*ISAKMP简档， *Cisco IOS XE版本3S* Cisco文档关于如何设置此的信息。

大小验证有效负载

如果证书(而不是预先共享密钥)使用验证，验证有效载荷显著地更加大。这通常导致分段，能然后造成验证发生故障，如果片段在路径丢失或丢弃。如果通道不出来由于验证有效负载的大小，通常原因是：

1. 控制在也许阻塞数据包的路由器的规划管制。
2. 不正确最大转换单元(MTU)协商，可以用**crypto ikev2分段MTU大小**命令更正。

在多个上下文模式的资源分配在ASA

自ASA版本9.0， ASA支持在多个上下文模式的VPN。然而，当您配置在多个上下文模式时的VPN，请务必指定在将使用VPN的系统的适当的资源。

欲知更多信息，参考关于思科ASA系列CLI配置指南的资源管理部分的信息， 9.0。

证书撤销列表的验证

证书撤销列表(CRL)是发出，并且随后取消由一给的CA. Certificates也许为一定数量的原因取消例如取消的certificates的列表：

- 使用一给的证书设备的失败或妥协。
- certificate使用的密钥对的妥协。
- 在一发出的certificate内的错误，例如一不正确标识或需要适应名称更改。

用于certificate撤销的机制在CRL取决于CA.取消的certificates代表由他们的序列号。如果网络设备尝试验证certificate的正确性，下载并且扫描提交证书的序列号的当前CRL。所以，如果CRL验证在任一对等体启用，必须配置适当的CRL URL，因此ID证书的正确性可以验证。

关于CRL的更多信息，参考什么是公共钥匙结构配置指南的CRL部分， Cisco IOS XE版本3S。

证书链的验证

如果ASA配置与有中间CA，并且的证书它是对等体也许或也许没有同样中间CA，则ASA需要明确地配置发送完整证书链到路由器。默认情况下路由器执行此。为了执行此，当您定义了信任点在加密映射下时添加链关键字如显示此处：

```
crypto map outside-map 1 set trustpoint ios-ca chain
```

如果这没有执行，则通道只将得到协商，只要ASA是响应方。如果它是发起者，通道将出故障，并且PKI和IKEv2在路由器的调试将显示此：

```
2328304: Jun  8 19:14:38.051 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):
Get peer's authentication method
2328305: Jun  8 19:14:38.051 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):
Peer's authentication method is 'RSA'
2328306: Jun  8 19:14:38.051 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):
SM Trace-> SA: I_SPI=E4368647479E50EF R_SPI=97B2C8AA5268271A (R) MsgID = 1
CurState: R_VERIFY_AUTH Event: EV_CHK_CERT_ENC
2328307: Jun  8 19:14:38.051 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):
SM Trace-> SA: I_SPI=E4368647479E50EF R_SPI=97B2C8AA5268271A (R) MsgID = 1
CurState: R_VERIFY_AUTH Event: EV_VERIFY_X509_CERTS
2328308: Jun  8 19:14:38.051 GMT: CRYPTO_PKI: (A16A8) Adding peer certificate
2328309: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: Added x509 peer certificate -(1359) bytes
2328310: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: ip-ext-val: IP extension validation
not required
2328311: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: create new ca_req_context type
PKI_VERIFY_CHAIN_CONTEXT,ident 4177
2328312: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: (A16A8)validation path has 1 certs
2328313: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: (A16A8) Check for identical certs
2328314: Jun  8 19:14:38.055 GMT: CRYPTO_PKI : (A16A8) Validating non-trusted cert
2328315: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: (A16A8) Create a list of suitable
trustpoints
2328316: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: Unable to locate cert record by
issuername
2328317: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: No trust point for cert issuer,
looking up cert chain
2328318: Jun  8 19:14:38.055 GMT: CRYPTO_PKI: (A16A8) No suitable trustpoints found
2328319: Jun  8 19:14:38.059 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):: Platform
errors
2328320: Jun  8 19:14:38.059 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):SM Trace-> SA:
I_SPI=E4368647479E50EF R_SPI=97B2C8AA5268271A (R) MsgID = 1 CurState:
R_VERIFY_AUTH Event: EV_CERT_FAIL
2328321: Jun  8 19:14:38.059 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):Verify cert
failed
2328322: Jun  8 19:14:38.059 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68):
SM Trace-> SA: I_SPI=E4368647479E50EF R_SPI=97B2C8AA5268271A (R) MsgID = 1 CurState:
R_VERIFY_AUTH Event: EV_AUTH_FAIL
2328323: Jun  8 19:14:38.059 GMT: IKEv2:(SESSION ID = 14607,SA ID = 68)
:Verification of peer's authentication data FAILED
```

示例ASA配置

```
domain-name cisco.com
!
interface outside
nameif outside
security-level 0
ip address 172.16.1.2 255.255.255.0
!
interface CA
nameif CA
security-level 50
```

```
ip address 192.168.0.1 255.255.255.0
!
! acl which defines crypto domains, must be mirror images on both peers
!
access-list cryacl extended permit ip 192.168.0.0 255.255.255.0 172.16.2.0
255.255.255.0
pager lines 24
logging console debugging
mtu outside 1500
mtu CA 1500
mtu backbone 1500
route outside 172.16.2.0 255.255.255.0 172.16.1.1 1
route CA 192.168.254.254 255.255.255.255 192.168.0.254 1
crypto ipsec ikev2 ipsec-proposal AES256
protocol esp encryption aes-256
protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal DES
protocol esp encryption des
protocol esp integrity sha-1 md5
crypto ipsec security-association pmtu-aging infinite
crypto map outside-map 1 match address cryacl
crypto map outside-map 1 set pfs
crypto map outside-map 1 set peer 172.16.1.1
crypto map outside-map 1 set ikev2 ipsec-proposal DES AES256
crypto map outside-map 1 set trustpoint ios-ca chain
crypto map outside-map interface outside
crypto ca trustpoint ios-ca
enrollment url http://192.168.254.254:80
fqdn asa.cisco.com
keypair ios-ca
crl configure
crypto ca certificate chain ios-ca
certificate ca 01
3082020f 30820178 a0030201 02020101 300d0609 2a864886 f70d0101 04050030
1b311930 17060355 04031310 696f732d 63612e63 6973636f 2e636f6d 301e170d
31333131 31353231 33353533 5a170d31 33313231 35323133 3535335a 301b3119
30170603 55040313 10696f73 2d63612e 63697363 6f2e636f 6d30819f 300d0609
2a864886 f70d0101 01050003 818d0030 81890281 81009ebb 48957c44 c940236f
a1cda758 aa930e8c 91390734 b8ef814d 0bf7aec9 7ec40379 7749d3c6 154f6a32
00738655 33b20207 037a9e15 3229fa72 478424fb 409f518d b13d328d e761be08
8023b4ff f410054b 4423156d 66c99788 69ab5956 966d5e1b 4d1c1120 a05ad08c
f036a134 3b2fc425 e4a2524f 36e0a129 2c8f6cee 971d0203 010001a3 63306130
0f060355 1d130101 ff040530 030101ff 300e0603 551d0f01 01ff0404 03020186
301f0603 551d2304 18301680 14082896 b9f4af20 75514321 d072f161 d09d2ec8
aa301d06 03551d0e 04160414 082896b9 f4af2075 514321d0 72f161d0 9d2ec8aa
300d0609 2a864886 f70d0101 04050003 81810087 a06d354a f7423e0e 64a7c5ec
6006fbde 914d7bfd f86ada50 b1a00d17 0bf06ec1 5423d514 fbeb0a76 986eb63f
f7fce99a 81c4b112 61fd69ce a2ce750e b1b3a6f9 84e92490 8f213613 451dd9a8
3fc3406a 854b20ed 27e4ddd8 62f6dea5 dd8b4396 1879b3e7 651cb9d1 3dd46b8b
32796963 9f6854f1 389f0060 aa0d1b8d f83e09
quit
certificate 08
3082028e 308201f7 a0030201 02020108 300d0609 2a864886 f70d0101 04050030
1b311930 17060355 04031310 696f732d 63612e63 6973636f 2e636f6d 301e170d
31333131 31383136 31383130 5a170d31 33313132 38313631 3831305a 301e311c
301a0609 2a864886 f70d0109 02160d61 73612e63 6973636f 2e636f6d 30819f30
0d06092a 864886f7 0d010101 05000381 8d003081 89028181 00c38ee5 75215237
2728cffd 3519cd15 ebcaab2c 48d63b92 7562d2fc f7db60bc ecb03b2c 4e4dff07
47ad5122 80899055 37f346d7 d10962e9 1e5edb06 8985ee7e 8a6da977 2460f82e
53679457 ed10372a 9ff2946e 449214e4 9be95cab 51d7681c 2db0382b 048fe807
1d1bb9b0 e4bd9de6 c99cafea c279e943 1e1f5d1b d1e6010c b7020301 0001a381
de3081db 30310603 551d2504 2a302806 082b0601 05050703 0106082b 06010505
07030506 082b0601 05050703 0606082b 06010505 07030730 3c060355 1d1f0435
30333031 a02fa02d 862b6874 74703a2f 2f313932 2e313638 2e323534 2e323534
```

```
2f696f73 2d636163 64702e69 6f732d63 612e6372 6c301806 03551d11 0411300f
820d6173 612e6369 73636f2e 636f6d30 0e060355 1d0f0101 ff040403 0205a030
1f060355 1d230418 30168014 082896b9 f4af2075 514321d0 72f161d0 9d2ec8aa
301d0603 551d0e04 1604145b 76de9ef0 d3255efe f4bc551b 69cd8398 d1596c30
0d06092a 864886f7 0d010104 05000381 81003fb0 ec7719cd 4f6162b2 90727db4
da5606f2 61441dc6 094fb3a6 defe62ef 5ff8f140 3bc3448c e0b42d26 07647607
fd7518cb 034139d3 e3648fd2 9d93b5e4 db3b828b 16d50dd5 3e18cdd6 74855de4
88a159d6 6ef51718 cf6cc4e4 53c2aca3 36442ff0 bb4b8493 22f0e632 a8b32b36
f287801f 8d47637f e4e9ee6a b4555094 c092
quit
!
! manually select the ISAKMP identity to use address on the ASA
crypto isakmp identity address
crypto ikev2 policy 1
encryption aes-256
integrity sha
group 14 5 2
prf sha
lifetime seconds 86400
crypto ikev2 policy 10
encryption aes-192
integrity sha256 sha
group 14 5 2
prf sha
lifetime seconds 86400
crypto ikev2 policy 30
encryption 3des
integrity sha
group 5 2
prf sha
lifetime seconds 86400
crypto ikev2 enable outside
!
! to allow pings from the CA interface that will bring up the tunnel during
testing.
!
management-access CA
!
group-policy GroupPolicy2 internal
group-policy GroupPolicy2 attributes
vpn-idle-timeout 30
vpn-tunnel-protocol ikev1 ikev2
tunnel-group 172.16.1.1 type ipsec-l2l
tunnel-group 172.16.1.1 general-attributes
default-group-policy GroupPolicy2
tunnel-group 172.16.1.1 ipsec-attributes
!
! disable peer-id validation
!
peer-id-validate nocheck
ikev2 remote-authentication certificate
ikev2 local-authentication certificate ios-ca
: end
! NTP configuration
ntp trusted-key 1
ntp server 192.168.254.254
```

路由器配置示例

```
ip domain name cisco.com
!
crypto pki trustpoint tp_ikev2
enrollment url http://192.168.254.254:80
usage ike
```

```
fqdn R1.cisco.com
!
! necessary only in this example as no crl has been configured on the IOS CA.
On the ASA this is enabled by default. When using proper 3rd party
certificates this is not necessary.
!
revocation-check none
rsakeypair ikev2_cert
eku request server-auth
!
crypto pki certificate chain tp_ikev2
certificate 0B
308202F4 3082025D A0030201 0202010B 300D0609 2A864886 F70D0101 05050030
1B311930 17060355 04031310 696F732D 63612E63 6973636F 2E636F6D 301E170D
31333131 32353233 35363537 5A170D31 33313230 35323335 3635375A 301D311B
30190609 2A864886 F70D0109 02160C52 312E6369 73636F2E 636F6D30 82012230
0D06092A 864886F7 0D010101 05000382 010F0030 82010A02 82010100 A1032A61
A3F14539 87816C22 8C66A170 3A9661EA 4AF6F063 3FC305B8 E525B84D AA74A9CE
666B1BF5 3C7DF025 31FEB161 CE49845F 3EC2DE7B D3FCC685 D6F80C8C 0AA12772
1B4AB15C 90C04446 068A0DBA 7BFA4E40 E978364F A2B07F7C 02C691A8 921A5481
A4AF07B4 BA0C9DBA D35F4566 6CB70553 DAF09A45 F2948C5A 1621E5D2 98508D49
A2EF61D3 AAF3A9DB 87F2D763 89AD0BBE 916A6CF8 1B59C426 7960013B 061AA0A5
F6870319 87A35ABA 8C1B5CF5 42976739 B8C936D3 24276E56 F59E3CFD 9B9B4A0D
2E5294AB C4470376 5D96915F 275CBC78 586D6755 F45C7592 62DCA916 CEC1A450
3FF090A9 15088CD2 13B90391 B0795263 071C7002 8CBF98F2 89788A0B 02030100
01A381C1 3081BE30 3C060355 1D1F0435 30333031 A02FA02D 862B6874 74703A2F
2F313932 2E313638 2E323534 2E323534 2F696F73 2D636163 64702E69 6F732D63
612E6372 6C303106 03551D25 042A3028 06082B06 01050507 03010608 2B060105
05070305 06082B06 01050507 03060608 2B060105 05070307 300B0603 551D0F04
04030205 A0301F06 03551D23 04183016 80140828 96B9F4AF 20755143 21D072F1
61D09D2E C8AA301D 0603551D 0E041604 14C63949 4CA10DBB 2BBB6F98 BAFF0EE2
B3716CEE 3B300D06 092A8648 86F70D01 01050500 03818100 3080FEF6 9160357B
6F28ED60 428BA6CE 203706F6 F91DA273 AF6E81D3 46539E13 B4C89A9A 19E1F0BC
A631A418 C30DFC8E 0585039D EB07D35D E719F5FE A4EE47B5 CED31B12 745C9EE8
5B6B0F17 67C3B965 C927B379 C674933F 84E7A1F7 851A6CF0 8775B1C5 3A033D90
75965DCA 86E4A842 E2C35AC0 6BFA8144 699B1582 C094BF35
quit
certificate ca 01
3082020F 30820178 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
1B311930 17060355 04031310 696F732D 63612E63 6973636F 2E636F6D 301E170D
31333131 31353231 33353533 5A170D31 33313231 35323133 3535335A 301B3119
30170603 55040313 10696F73 2D63612E 63697363 6F2E636F 6D30819F 300D0609
2A864886 F70D0101 01050003 818D0030 81890281 81009EBB 48957C44 C940236F
A1CDA758 AA930E8C 91390734 B8EF814D 0BF7AEC9 7EC40379 7749D3C6 154F6A32
00738655 33B20207 037A9E15 3229FA72 478424FB 409F518D B13D328D E761BE08
8023B4FF F410054B 4423156D 66C99788 69AB5956 966D5E1B 4D1C1120 A05AD08C
F036A134 3B2FC425 E4A2524F 36E0A129 2C8F6CEE 971D0203 010001A3 63306130
0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186
301F0603 551D2304 18301680 14082896 B9F4AF20 75514321 D072F161 D09D2EC8
AA301D06 03551D0E 04160414 082896B9 F4AF2075 514321D0 72F161D0 9D2EC8AA
300D0609 2A864886 F70D0101 04050003 81810087 A06D354A F7423E0E 64A7C5EC
6006FBDE 914D7BFD F86ADA50 B1A00D17 0BF06EC1 5423D514 FBEB0A76 986EB63F
F7FCE99A 81C4B112 61FD69CE A2CE750E B1B3A6F9 84E92490 8F213613 451DD9A8
3FC3406A 854B20ED 27E4DDD8 62F6DEA5 DD8B4396 1879B3E7 651CB9D1 3DD46B8B
32796963 9F6854F1 389F0060 AA0D1B8D F83E09
quit
!
crypto ikev2 proposal aes-cbc-256-proposal
encryption aes-cbc-256
integrity sha1
group 5 2 14
!
crypto ikev2 policy policy1
match address local 172.16.1.1
```

```
proposal aes-cbc-256-proposal
!
crypto ikev2 profile profile1
description IKEv2 profile
!
! router configured to use address as the remote identity. By default local
identity is address
!
match address local 172.16.1.1
match identity remote address 172.16.1.2 255.255.255.255
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint tp_ikev2
!
! disable http-url based cert lookup
!
no crypto ikev2 http-url cert
!
crypto ipsec transform-set ESP-AES-SHA esp-aes 256 esp-sha-hmac
mode tunnel
!
crypto map SDM_CMAP_1 1 ipsec-isakmp
set peer 172.16.1.2
set transform-set ESP-AES-SHA
set pfs group2
set ikev2-profile profile1
match address 103
!
interface Loopback0
ip address 172.16.2.1 255.255.255.255
!
interface GigabitEthernet0/0
ip address 172.16.1.1 255.255.255.0
duplex auto
speed auto
crypto map SDM_CMAP_1
!
interface GigabitEthernet0/1
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
ip route 192.168.0.0 255.255.255.0 172.16.1.2
ip route 192.168.254.254 255.255.255.255 192.168.1.254
!
! access list that defines crypto domains, must be mirror images on both peers.
!
access-list 103 permit ip 172.16.2.0 0.0.0.255 192.168.0.0 0.0.0.255
!
! ntp configuration
!
ntp trusted-key 1
ntp server 192.168.254.254
!
end
```

示例IOS CA配置

```
ip domain name cisco.com
!
! CA server configuration
!
crypto pki server ios-ca
database archive pkcs12 password 7 02050D4808095E731F
```

```
issuer-name CN=ios-ca.cisco.com
grant auto
lifetime certificate 10
lifetime ca-certificate 30
cdp-url http://192.168.254.254/ios-cacdp.ios-ca.crl
eku server-auth ipsec-end-system ipsec-tunnel ipsec-user
!
! this trustpoint is generated automatically when the CA server is enabled.
!
crypto pki trustpoint ios-ca
revocation-check crl
rsakeypair ios-ca
!
!
crypto pki certificate chain ios-ca
certificate ca 01
3082020F 30820178 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
1B311930 17060355 04031310 696F732D 63612E63 6973636F 2E636F6D 301E170D
31333131 31353231 33353533 5A170D31 33313231 35323133 3535335A 301B3119
30170603 55040313 10696F73 2D63612E 63697363 6F2E636F 6D30819F 300D0609
2A864886 F70D0101 01050003 818D0030 81890281 81009EBB 48957C44 C940236F
A1CDA758 AA930E8C 91390734 B8EF814D 0BF7AEC9 7EC40379 7749D3C6 154F6A32
00738655 33B20207 037A9E15 3229FA72 478424FB 409F518D B13D328D E761BE08
8023B4FF F410054B 4423156D 66C99788 69AB5956 966D5E1B 4D1C1120 A05AD08C
F036A134 3B2FC425 E4A2524F 36E0A129 2C8F6CEE 971D0203 010001A3 63306130
0F060355 1D130101 FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186
301F0603 551D2304 18301680 14082896 B9F4AF20 75514321 D072F161 D09D2EC8
AA301D06 03551D0E 04160414 082896B9 F4AF2075 514321D0 72F161D0 9D2EC8AA
300D0609 2A864886 F70D0101 04050003 81810087 A06D354A F7423E0E 64A7C5EC
6006FBDE 914D7BFD F86ADA50 B1A00D17 0BF06EC1 5423D514 FBEB0A76 986EB63F
F7FCE99A 81C4B112 61FD69CE A2CE750E B1B3A6F9 84E92490 8F213613 451DD9A8
3FC3406A 854B20ED 27E4DDD8 62F6DEA5 DD8B4396 1879B3E7 651CB9D1 3DD46B8B
32796963 9F6854F1 389F0060 AA0D1B8D F83E09
quit
voice-card 0
!
!
interface Loopback0
ip address 192.168.254.254 255.255.255.255
!
interface GigabitEthernet0/0
ip address 192.168.0.254 255.255.255.0
duplex auto
speed auto
!
interface GigabitEthernet0/1
ip address 192.168.1.254 255.255.255.0
duplex auto
speed auto
!
! http-server needs to be enabeld for SCEP
!
ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.122.162.129
ip route 172.18.108.26 255.255.255.255 10.122.162.129
!
! ntp configuration
!
ntp trusted-key 1
ntp master 1
!
end
```

验证

使用本部分可确认配置能否正常运行。

> **注意**：命令输出解释程序工具（仅限注册用户）支持某些 **show** 命令。请使用Output Interpreter Tool为了查看show命令输出分析。

这些命令在ASA和路由器运作：

- **显示crypto ikev2 sa** -显示相位1安全关联(SA)的状态。
- **show crypto ipsec sa** -显示第2阶段SA的状态。

> **注意**：在此输出中，不同于在IKEv1，完善的转发秘密(PFS) Diffie-Hellman (DH)组的值显示作为'PFS是/否：N， DH组：无'在第一隧道协商时;在重新生成密钥发生后，正确值出现。这不是bug，即使行为在Cisco Bug ID CSCug67056描述。
>
> 在IKEv1和IKEv2之间的区别是作为验证交换一部分，在IKEv2，孩子SAS创建。在重新生成密钥期间， DH组配置在加密映射下仅使用。因此，您看到'PFS是/否：N， DH组：什么都'直到第一不重新生成密钥。使用IKEv1，您看到一种不同的行为在快速模式期间，因为SA儿童创建发生，并且CREATE_CHILD_SA消息有提供传送密钥交换有效负载，指定DH参数派生新建的共享机密。

阶段1验证

此步骤验证相位1活动：

1. 输入**显示crypto sa ikev2** on命令路由器：

```
R1#show crypto ikev2 sa
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf    Status
1         172.16.1.1/500        172.16.1.2/500        none/none    READY
     Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:14, Auth sign: RSA,
Auth verify: RSA
     Life/Active Time: 86400/53 sec
 IPv6 Crypto IKEv2  SA
```

2. 输入在ASA的**显示crypto ikev2 sacommand** ：

```
ciscoasa/vpn(config)# show crypto ikev2 sa

IKEv2 SAs:

Session-id:138, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                  Remote     Status   Role
45926289  172.16.1.2/500         172.16.1.1/500       READY    INITIATOR
     Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:14, Auth sign: RSA,
Auth verify: RSA
     Life/Active Time: 86400/4 sec
Child sa: local selector  192.168.0.0/0 - 192.168.0.255/65535
          remote selector 172.16.2.0/0 - 172.16.2.255/65535
          ESP spi in/out: 0xa84caabb/0xf18dce57
```

第2阶段验证

此步骤描述如何验证，如果安全参数索引(SPI)在两对等体正确地协商：

1. 输入**show crypto ipsec sa|我spi** on命令路由器：

```
R1#show crypto ipsec sa | i spi
    current outbound spi: 0xA84CAABB(2823596731)
     spi: 0xF18DCE57(4052602455)
     spi: 0xA84CAABB(2823596731)
```

2. 输入**show crypto ipsec sa|我**在ASA的**spicommand** ：

```
ciscoasa/vpn(config)# show crypto ipsec sa | i spi
     current outbound spi: F18DCE57
     current inbound spi : A84CAABB
     spi: 0xA84CAABB (2823596731)
     spi: 0xF18DCE57 (4052602455)
```

此步骤描述如何确认是否在通道间的通信流：

1. 输入**show crypto ipsec sa|我pkts** on命令路由器：

```
R1#show crypto ipsec sa | i pkts
   #pkts encaps: 21, #pkts encrypt: 21, #pkts digest: 21
   #pkts decaps: 30, #pkts decrypt: 30, #pkts verify: 30
   #pkts compressed: 0, #pkts decompressed: 0
   #pkts not compressed: 0, #pkts compr. failed: 0
   #pkts not decompressed: 0, #pkts decompress failed: 0
```

2. 输入**show crypto ipsec sa|我**在ASA的**pktscommand** ：

```
ciscoasa/vpn(config)# show crypto ipsec sa | i pkts
     #pkts encaps: 4, #pkts encrypt: 4, #pkts digest: 4
     #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 4, #pkts comp failed: 0, #pkts decomp
failed: 0
```

故障排除

本部分提供了可用于对配置进行故障排除的信息。

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

在ASA的调试

> **警告**：在ASA，您能设置多种调试级别;默认情况下，使用1级。如果改变调试级别，调试的冗余也许增加。执行此小心地，特别是在生产环境!

隧道协商的ASA调试是：

- **debug crypto ikev2协议**
- **debug crypto ikev2平台**

证书验证的ASA调试是：

- debug crypto ca

在路由器的调试

隧道协商的路由器调试是：

- debug crypto ikev2
- debug crypto ikev2错误
- 内部的debug crypto ikev2

证书验证的路由器调试是：

- 调试啼声pki验证
- 调试啼声pki处理
- 调试啼声pki消息