

# 使用带自签名证书的主模式配置路由器和ASA之间的Easy VPN隧道

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[NTP](#)

[网络图](#)

[配置](#)

[验证](#)

[故障排除](#)

[相关的思科支持社区讨论](#)

## 简介

本文档介绍如何在思科自适应安全设备(ASA)和使用带自签名证书的主模式运行Cisco IOS®软件的路由器之间设置Easy VPN隧道。

## 先决条件

路由器到路由器Easy VPN解决方案的示例配置基于以下假设：Cisco Easy VPN服务器的IP地址是静态的，Cisco Easy VPN客户端的IP地址是静态的。

## 要求

Cisco 建议您了解以下主题：

- Internet 密钥交换 (IKE)
- 证书和公钥基础设施(PKI)

## 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8.4(7)的思科ASA 5510自适应安全设备
- 运行Cisco IOS软件版本15.2(4)M2的Cisco 2821系列集成多业务路由器(ISR)

## 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或更高版本的Cisco ASA
- 运行Cisco IOS软件版本15.0或更高版本的Cisco ISR代路由器

## 背景信息

本文档讨论在主模式下使用EzVPN ( 预共享密钥不支持此模式 )。但是，我们可以使用主模式和证书身份验证来克服与攻击性模式(CVE-2002-1623)相关的漏洞。

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。

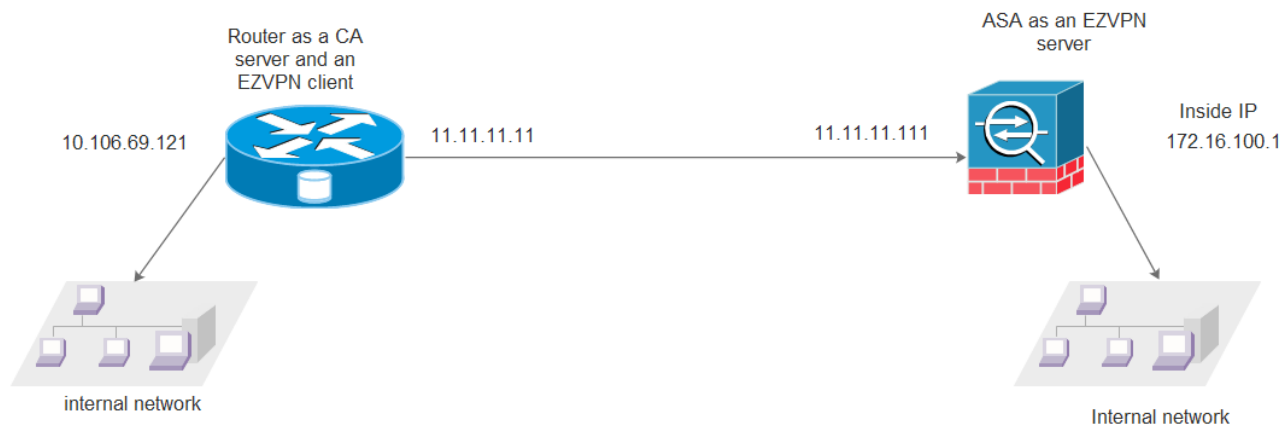
## 配置

### NTP

证书身份验证要求所有参与设备上的时钟同步到公共源。虽然可以在每台设备上手动设置时钟，但这并不太准确，而且可能很麻烦。同步所有设备时钟的最简单方法是使用NTP。NTP在一组分布式时间服务器和客户端之间同步计时。此同步允许在创建系统日志和发生其他特定时间的事件时关联事件。有关如何配置NTP的详细信息，请参阅网络时间协议：最佳实践白皮书。

<http://www.cisco.com/c/en/us/support/docs/availability/high-availability/19643-ntp.html>

### 网络图



## 配置

Router:

Current configuration : 6024 bytes

!

```

!
hostname CISCO_LAB_ROUTER
!
-----CA Server configuration

crypto pki server ASA
 issuer-name cn=ASA, ou=VPN, o=cisco, c=US
 grant auto
 lifetime ca-certificate 300
!
-----PKI Trustpoint configuration

crypto pki trustpoint router
 enrollment url http://11.11.11.11:80
 revocation-check none
!
!
crypto pki certificate chain router
 certificate 03
 30820225 3082018E A0030201 02020103 300D0609 2A864886 F70D0101 05050030
 39310B30 09060355 04061302 5553310E 300C0603 55040A13 05636973 636F310C
 300A0603 55040B13 0356504E 310C300A 06035504 03130341 5341301E 170D3135
 31313234 31383034 32365A17 0D313630 39313931 38303130 395A3027 31253023
 06092A86 4886F70D 01090216 1642474C 2E532E31 362D3238 30302D31 342E6369
 73636F30 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
 D7423408 DAEDB119 5E1D6F9B F627F80B 28F6691F 799AFCC5 ECBF5FAA 23D4D890
 335CDF2B 7C4717A7 979E6A73 515F70AB 905A4935 37873935 9D7406F8 D6986395
 A427410D FA3432E2 D71FDF8B FFA34C74 C3518E53 E23E5076 06C73C5A C83CC2F3
 A7EB4349 523571C8 84EA4D58 480ADF47 C4AB29AE EA1FF522 DBCDFEE8 8A9E40A5
 02030100 01A34F30 4D300B06 03551D0F 04040302 05A0301F 0603551D 23041830
 1680143B A9F1006C 39BCFFD6 9E8EF705 DD4FD606 268A1E30 1D060355 1D0E0416
 0414B13F D97C0877 63A7087E 7C31E429 C0D8ADD8 2B1A300D 06092A86 4886F70D
 01010505 00038181 0039C03A B8B91B3F BFE17248 F1777B78 EBF49CA3 F967C986
 268C16D4 6AFE2905 0237F56A 369A3BB8 E9A5C1C9 9CF77C9D 2EC71C81 ABB1A64C
 2FD44A78 3499A357 986D4B8E 08345355 80B481C4 A3AB3408 C3F6F1A6 E42E4585
 F7B02B33 A57E7D6F 2BD4862A 6DDD4253 B253B3C5 481B3E54 1FB7CEA9 97A01C50
 0414ECA9 A85CD3F9 EE
 quit
 certificate ca 01
 3082024B 308201B4 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 39310B30 09060355 04061302 5553310E 300C0603 55040A13 05636973 636F310C
 300A0603 55040B13 0356504E 310C300A 06035504 03130341 5341301E 170D3135
 31313234 31383031 30395A17 0D313630 39313931 38303130 395A3039 310B3009
 06035504 06130255 53310E30 0C060355 040A1305 63697363 6F310C30 0A060355
 040B1303 56504E31 0C300A06 03550403 13034153 4130819F 300D0609 2A864886
 F70D0101 01050003 818D0030 81890281 8100BAFF C15ABB3D 78778733 762F71A7
 9BE2C81C A2BEB6EF CFD98FB2 21D466D5 65301232 163FFCD0 1CCCCF07 6CAEABD8
 E3A1C3EB B48D916A AD4D56D8 0730C32B 97388937 193BCD22 729D3F61 5712E71A
 61315E75 A29E4D7B 881F37A2 3EA74B93 05C3FA73 E50A7DE9 CC2BBF15 F21E8615
 13EA3E0A 80C95C5E 866B92C7 D98AB734 C41D0203 010001A3 63306130 0F060355
 1D130101 FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301F0603
 551D2304 18301680 143BA9F1 006C39BC FFD69E8E F705DD4F D606268A 1E301D06
 03551D0E 04160414 3BA9F100 6C39BCFF D69E8EF7 05DD4FD6 06268A1E 300D0609
 2A864886 F70D0101 04050003 8181000B 34F5327C 95DD6B24 09E5F485 7B2B9918
 9BEBE081 B7CE0946 0402C1A2 3849B319 937E4CD7 DF24944E 35482A00 ED28FB5B
 804A2682 44CB5B81 938F3E68 30E34F33 C9F2E0BF D65CB235 2FFA5301 705ECD56
 8A3F80F9 12DAA450 CDA84849 1FD44822 79CBBF0B 75E507B5 9A75344E 206551B5
 BCA5865F 3DD16D61 935E074E FC04B9
 quit
 crypto pki certificate chain ASA
 certificate ca 01
 3082024B 308201B4 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
 39310B30 09060355 04061302 5553310E 300C0603 55040A13 05636973 636F310C
 300A0603 55040B13 0356504E 310C300A 06035504 03130341 5341301E 170D3135

```

```
31313234 31383031 30395A17 0D313630 39313931 38303130 395A3039 310B3009
06035504 06130255 53310E30 0C060355 040A1305 63697363 6F310C30 0A060355
040B1303 56504E31 0C300A06 03550403 13034153 4130819F 300D0609 2A864886
F70D0101 01050003 818D0030 81890281 8100BAFF C15ABB3D 78778733 762F71A7
9BE2C81C A2BEB6EF CFD98FB2 21D466D5 65301232 163FFCD0 1CCCCF07 6CAEABD8
E3A1C3EB B48D916A AD4D56D8 0730C32B 97388937 193BCD22 729D3F61 5712E71A
61315E75 A29E4D7B 881F37A2 3EA74B93 05C3FA73 E50A7DE9 CC2BBF15 F21E8615
13EA3E0A 80C95C5E 866B92C7 D98AB734 C41D0203 010001A3 63306130 0F060355
1D130101 FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301F0603
551D2304 18301680 143BA9F1 006C39BC FFD69E8E F705DD4F D606268A 1E301D06
03551D0E 04160414 3BA9F100 6C39BCFF D69E8EF7 05DD4FD6 06268A1E 300D0609
2A864886 F70D0101 04050003 8181000B 34F5327C 95DD6B24 09E5F485 7B2B9918
9BEBE081 B7CE0946 0402C1A2 3849B319 937E4CD7 DF24944E 35482A00 ED28FB5B
804A2682 44CB5B81 938F3E68 30E34F33 C9F2E0BF D65CB235 2FFA5301 705ECD56
8A3F80F9 12DAA450 CDA84849 1FD44822 79CBBF0B 75E507B5 9A75344E 206551B5
BCA5865F 3DD16D61 935E074E FC04B9
```

quit

```
!
!
redundancy
```

```
!
!
-----EzVPN client configurtaion
```

```
crypto ipsec client ezvpn VPN
connect auto
mode network-extension
peer 11.11.11.111
xauth userid mode interactive
```

```
!
!-----IPSEC mapping on interfaces
```

```
interface GigabitEthernet0/0
ip address 11.11.11.11 255.255.255.0
duplex auto
speed auto
crypto ipsec client ezvpn VPN
```

```
!
interface GigabitEthernet0/1
ip address 10.106.69.121 255.255.255.0
duplex auto
speed auto
crypto ipsec client ezvpn VPN inside
```

```
!
ip forward-protocol nd
ip http server
no ip http secure-server
```

```
!
end
```

CISCO\_LAB\_ROUTER#

ASA:

ASA Version 8.4(7)

```
!
hostname CISCO_LAB_ASA
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
```

```

!
interface Ethernet0/0
 nameif CERT
 security-level 0
 ip address 11.11.11.111 255.255.255.0
!
interface Management0/0
 nameif tftp
 security-level 0
 ip address 10.106.69.107 255.255.255.0

!-----EZVPN Server configuration

crypto ipsec ikev1 transform-set VPN-SET esp-3des esp-sha-hmac
crypto dynamic-map dyn1 1 set reverse-route
crypto dynamic-map dynmap 10 set ikev1 transform-set VPN-SET
crypto map mymap 1 ipsec-isakmp dynamic dyn1
crypto map VPNMAP 1 ipsec-isakmp dynamic dynmap
crypto map VPNMAP interface CERT

!-----Trustpoint Configuration for SCEP

crypto ca trustpoint ASA
 enrollment url http://11.11.11.11:80
 ignore-ipsec-keyusage
 crl configure

-----Certificate Map configuration

crypto ca certificate map DefaultCertificateMap 1
 issuer-name attr cn eq asa
 issuer-name attr ou eq vpn

crypto ca certificate chain ASA
certificate ca 01
 3082024b 308201b4 a0030201 02020101 300d0609 2a864886 f70d0101 04050030
 39310b30 09060355 04061302 5553310e 300c0603 55040a13 05636973 636f310c
 300a0603 55040b13 0356504e 310c300a 06035504 03130341 5341301e 170d3135
 31313234 31383031 30395a17 0d313630 39313931 38303130 395a3039 310b3009
 06035504 06130255 53310e30 0c060355 040a1305 63697363 6f310c30 0a060355
 040b1303 56504e31 0c300a06 03550403 13034153 4130819f 300d0609 2a864886
 f70d0101 01050003 818d0030 81890281 8100baff c15abb3d 78778733 762f71a7
 9be2c81c a2beb6ef cfd98fb2 21d466d5 65301232 163ffcd0 1ccccf07 6caeabd8
 e3a1c3eb b48d916a addd56d8 0730c32b 97388937 193bcd22 729d3f61 5712e71a
 61315e75 a29e4d7b 881f37a2 3ea74b93 05c3fa73 e50a7de9 cc2bbf15 f21e8615
 13ea3e0a 80c95c5e 866b92c7 d98ab734 c41d0203 010001a3 63306130 0f060355
 1d130101 ff040530 030101ff 300e0603 551d0f01 01ff0404 03020186 301f0603
 551d2304 18301680 143ba9f1 006c39bc ffd69e8e f705dd4f d606268a 1e301d06
 03551d0e 04160414 3ba9f100 6c39bcff d69e8ef7 05dd4fd6 06268a1e 300d0609
 2a864886 f70d0101 04050003 8181000b 34f5327c 95dd6b24 09e5f485 7b2b9918
 9bebe081 b7ce0946 0402c1a2 3849b319 937e4cd7 df24944e 35482a00 ed28fb5b
 804a2682 44cb5b81 938f3e68 30e34f33 c9f2e0bf d65cb235 2ffa5301 705ecd56
 8a3f80f9 12daa450 cda84849 1fd44822 79cbbf0b 75e507b5 9a75344e 206551b5
 bca5865f 3dd16d61 935e074e fc04b9
quit
certificate 02

 30820243 308201ac a0030201 02020102 300d0609 2a864886 f70d0101 04050030
 39310b30 09060355 04061302 5553310e 300c0603 55040a13 05636973 636f310c
 300a0603 55040b13 0356504e 310c300a 06035504 03130341 5341301e 170d3135
 31313234 31383033 32315a17 0d313630 39313931 38303130 395a3023 3121301f
 06092a86 4886f70d 01090216 1262676c 2d532d31 362d4153 41353530 302d3130
 819f300d 06092a86 4886f70d 01010105 0003818d 00308189 02818100 efc22ac0

```

```
35960f71 9c197870 aa2b2a8c cd6ea4ef 150bc5ed f38812a2 baad0929 cde15a14
f5982e23 9208b79e decb58ed 04e1c552 c352a7b7 0458c205 a5548367 7a4ae377
93b0e711 05da2932 6621170e 93c0197d 4de3639e 6b1ce677 aac8c68e d9e7d098
40e5cb9f ee9a13e3 8e2a63e8 96186be0 9f1db880 0eb8b63a 0c17fe3d 02030100
01a37130 6f301d06 03551d11 04163014 82126267 6c2d532d 31362d41 53413535
30302d31 300e0603 551d0f01 01ff0404 030205a0 301f0603 551d2304 18301680
143ba9f1 006c39bc ffd69e8e f705dd4f d606268a 1e301d06 03551d0e 04160414
be1953e2 579f9901 cbc6d4e4 1290451b e4bbcec0 300d0609 2a864886 f70d0101
04050003 81810081 68d44005 d2cfa98f c2575dcb 724387af 852628be 4fe1b27f
edd49e5c 84f49a04 971a4d51 b23032c5 538f889d 8f25ffae d605fc40 9d7d49f3
904814ec 5b9bb2bf c5834a38 74f56df8 8afc2588 9fe78e2a 0e7ccbfe de339970
d4149dc1 a7f5417e 0617c566 507cb91d 0adddb77 192f727a 6fbbb413 82e72b83
1cd98cc7 77fbb4
quit
```

-----IKE configuration

```
crypto ikev1 enable CERT
crypto ikev1 policy 5
authentication rsa-sig
encryption 3des
hash sha
group 2
lifetime 86400
```

-----Group Policy Configuraiton

```
group-policy VPNPOLICY internal
group-policy VPNPOLICY attributes
re-xauth disable
split-tunnel-policy tunnelall
nem enable
```

```
username cisco password 3USUcOPFUimCO4Jk encrypted
```

-----Tunnel Group configuration

```
tunnel-group DefaultRAGroup general-attributes
default-group-policy VPNPOLICY
tunnel-group DefaultRAGroup ipsec-attributes
ikev1 trust-point ASA
tunnel-group VPN type remote-access
tunnel-group VPN general-attributes
default-group-policy VPNPOLICY
tunnel-group VPN ipsec-attributes
ikev1 trust-point ASA
tunnel-group-map enable rules
tunnel-group-map DefaultCertificateMap 1 VPN
!
: end
```

## 验证

要验证设备是否已成功注册到CA，请执行以下操作：

### 路由器

```
CISCO_LAB_ROUTER#show crypto pki certificates
Certificate
Status: Available
Certificate Serial Number (hex): 03
```

Certificate Usage: General Purpose

Issuer:

cn=ASA

ou=VPN

o=cisco

c=US

Subject:

Name: CISCO\_LAB\_ROUTER.cisco

hostname=CISCO\_LAB\_ROUTER.cisco

Validity Date:

start date: 18:04:26 UTC Nov 24 2015

end date: 18:01:09 UTC Sep 19 2016

Associated Trustpoints: router

Storage: nvram:ASA#3.cer

CA Certificate

Status: Available

Certificate Serial Number (hex): 01

Certificate Usage: Signature

Issuer:

cn=ASA

ou=VPN

o=cisco

c=US

Subject:

cn=ASA

ou=VPN

o=cisco

c=US

Validity Date:

start date: 18:01:09 UTC Nov 24 2015

end date: 18:01:09 UTC Sep 19 2016

Associated Trustpoints: ASA router

Storage: nvram:ASA#1CA.cer

## ASA

CISCO\_LAB\_ASA# show crypto ca certificates

Certificate

Status: Available

Certificate Serial Number: 02

Certificate Usage: General Purpose

Public Key Type: RSA (1024 bits)

Signature Algorithm: MD5 with RSA Encryption

Issuer Name:

cn=ASA

ou=VPN

o=cisco

c=US

Subject Name:

hostname=CISCO\_LAB\_ASA

Validity Date:

start date: 18:03:21 UTC Nov 24 2015

end date: 18:01:09 UTC Sep 19 2016

Associated Trustpoints: ASA

CA Certificate

Status: Available

Certificate Serial Number: 01

Certificate Usage: Signature

Public Key Type: RSA (1024 bits)

Signature Algorithm: MD5 with RSA Encryption

Issuer Name:

cn=ASA

ou=VPN

```
o=cisco
c=US
Subject Name:
cn=ASA
ou=VPN
o=cisco
c=US
Validity Date:
start date: 18:01:09 UTC Nov 24 2015
end date: 18:01:09 UTC Sep 19 2016
Associated Trustpoints: ASA
```

要验证隧道是否已启用

## 路由器

### 第1阶段验证：

```
CISCO_LAB_ROUTER # show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id status
11.11.11.111 11.11.11.11  QM_IDLE        1114 ACTIVE
```

### 第2阶段验证：

```
CISCO_LAB_ROUTER# show crypto ipsec sa

interface: GigabitEthernet0/0
  Crypto map tag: GigabitEthernet0/0-head-0, local addr 11.11.11.11

protected vrf: (none)
  local ident (addr/mask/prot/port): (10.106.69.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  current_peer 11.11.11.111 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
    #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
```

## ASA

### 第1阶段验证：

```
CISCO_LAB_ASA# show crypto isakmp sa

IKEv1 SAs:

  Active SA: 1
  Rekey SA: 0 (A tunnel will report 1 Active and 1 Rekey SA during rekey)
Total IKE SA: 1

1  IKE Peer: 11.11.11.11
   Type    : user          Role    : responder
   Rekey   : no          State   : MM_ACTIVE  -----> MM denotes main mode
```

```
IPv6 Crypto ISAKMP SA
```

### 第2阶段验证：



```
CISCO_LAB_ASA#show crypto ipsec sa
interface: CERT
  Crypto map tag: dynmap, seq num: 10, local addr: 11.11.11.111

  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
  remote ident (addr/mask/prot/port): (10.106.69.0/255.255.255.0/0/0)
  current_peer: 11.11.11.11, username: cisco
  dynamic allocated peer ip: 0.0.0.0

  #pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
  #pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
```

## 故障排除

### ASA上的调试

**警告：**在ASA上，可以设置各种调试级别；默认情况下，使用1级。如果更改调试级别，调试的详细程度可能会增加。

建议使用条件调试仅查看单个对等体的调试：

```
debug crypto condition peer <peer ip address>
```

请谨慎执行此操作，尤其是在生产环境中。

隧道协商的ASA调试包括：

```
debug crypto ikev1 <0-255>
debug crypto ipsec <0-255>
```

证书身份验证的ASA调试为：

```
debug crypto ca
```

### 路由器调试

用于隧道协商的路由器调试如下：

```
debug crypto ikev1
debug crypto ikev1 error
debug crypto ikev1 internal
```

用于证书身份验证的路由器调试如下：

```
debug crypto pki validation
debug crypto pki transaction
debug crypto pki messages
```