

# 为通过FDM的FTD上的安全客户端身份验证配置证书匹配

## 目录

---

### [简介](#)

### [先决条件](#)

#### [要求](#)

#### [使用的组件](#)

### [背景信息](#)

### [网络图](#)

### [配置](#)

#### [FDM中的配置](#)

##### [步骤1:配置FTD接口](#)

##### [第二步：确认思科安全客户端许可证](#)

##### [第三步：添加地址池](#)

##### [第四步：创建安全客户端配置文件](#)

##### [第五步：将安全客户端配置文件上传到FDM](#)

##### [第六步：添加组策略](#)

##### [步骤 7.添加FTD证书](#)

##### [步骤 8将CA添加到FTD](#)

##### [步骤 9添加远程访问VPN连接配置文件](#)

##### [步骤 10确认连接配置文件的摘要](#)

#### [在FTD CLI中确认](#)

#### [在VPN客户端中确认](#)

##### [步骤1:将安全客户端配置文件复制到VPN客户端](#)

##### [第二步：确认客户端证书](#)

##### [第三步：确认CA](#)

### [验证](#)

#### [步骤1:启动VPN连接](#)

#### [第二步：在FTD CLI中确认VPN会话](#)

### [故障排除](#)

### [相关信息](#)

---

## 简介

本文档介绍如何使用证书匹配进行身份验证，通过FDM在FTD上设置带SSL的Cisco安全客户端。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- Cisco Firepower设备管理器(FDM)虚拟
- 防火墙威胁防御(FTD)虚拟
- VPN身份验证流程

## 使用的组件

- 思科Firepower设备管理器虚拟7.2.8
- 思科防火墙威胁防御虚拟7.2.8
- 思科安全客户端5.1.4.74
- 配置文件编辑器(Windows) 5.1.4.74

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。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 背景信息

CertificateMatch是一项功能，允许管理员配置客户端必须用来选择客户端证书以使用VPN服务器进行身份验证的条件。此配置在客户端配置文件中指定，它是可使用配置文件编辑器管理或手动编辑的XML文件。CertificateMatch功能可用于增强VPN连接的安全性，方法是确保仅将具有特定属性的证书用于VPN连接。

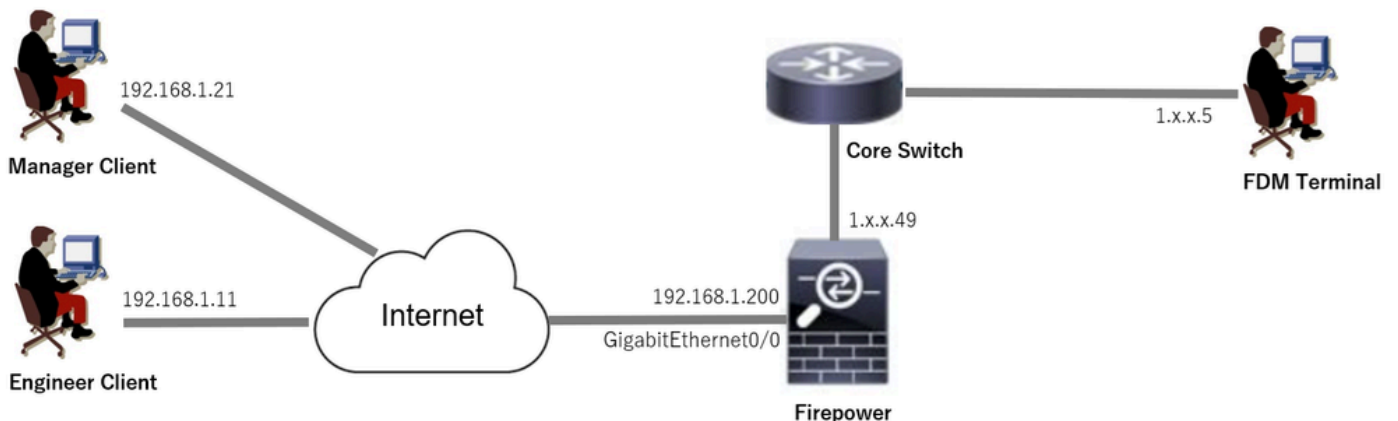
本文档介绍如何使用SSL证书中的公用名对Cisco安全客户端进行身份验证。

这些证书中包含用于授权目的的公用名称。

- CA：ftd-ra-ca-common-name
- 工程师VPN客户端证书：vpnEngineerClientCN
- 管理器VPN客户端证书：vpnManagerClientCN
- 服务器证书：192.168.1.200

## 网络图

下图显示本文档示例中使用的拓扑。



# 配置

## FDM中的配置

### 步骤1:配置FTD接口

导航到Device > Interfaces > View All Interfaces , 在Interfaces选项卡中配置FTD的内部和外部接口。

对于GigabitEthernet0/0 ,

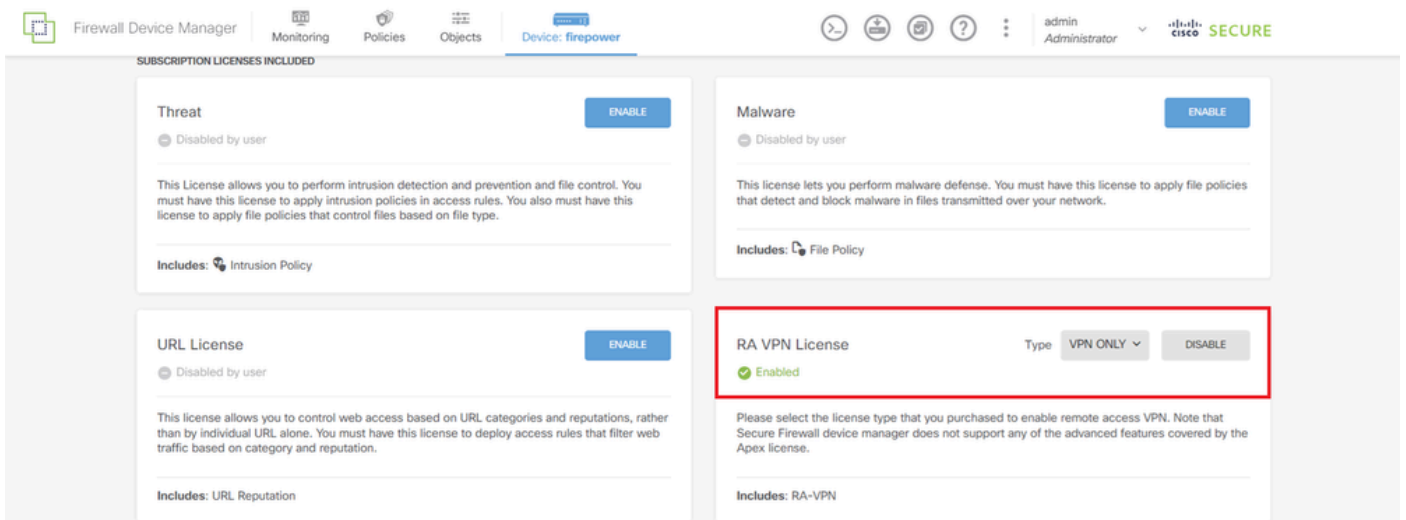
- 名称 : outside
- IP地址 : 192.168.1.200/24



FTD接口

### 第二步 : 确认思科安全客户端许可证

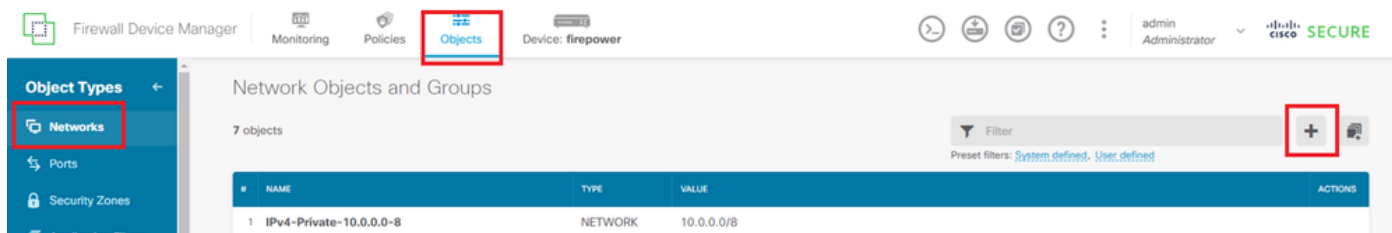
导航到设备>智能许可证>查看配置 , 确认RA VPN许可证项目中的思科安全客户端许可证。



安全客户端许可证

### 第三步：添加地址池

导航到对象>网络，点击+按钮。



添加地址池

输入必要信息以添加新的IPv4地址池。单击OK 按钮。

- 名称：ftd-cert-match-pool
- 类型：范围
- IP范围：172.16.1.150-172.16.1.160

## Add Network Object

Name

ftd-cert-match-pool

Description

Type

Network  Host  FQDN  Range

IP Range

172.16.1.150-172.16.1.160

e.g. 192.168.2.1-192.168.2.24 or 2001:DB8:0:CD30::10-2001:DB8:0:CD30::100

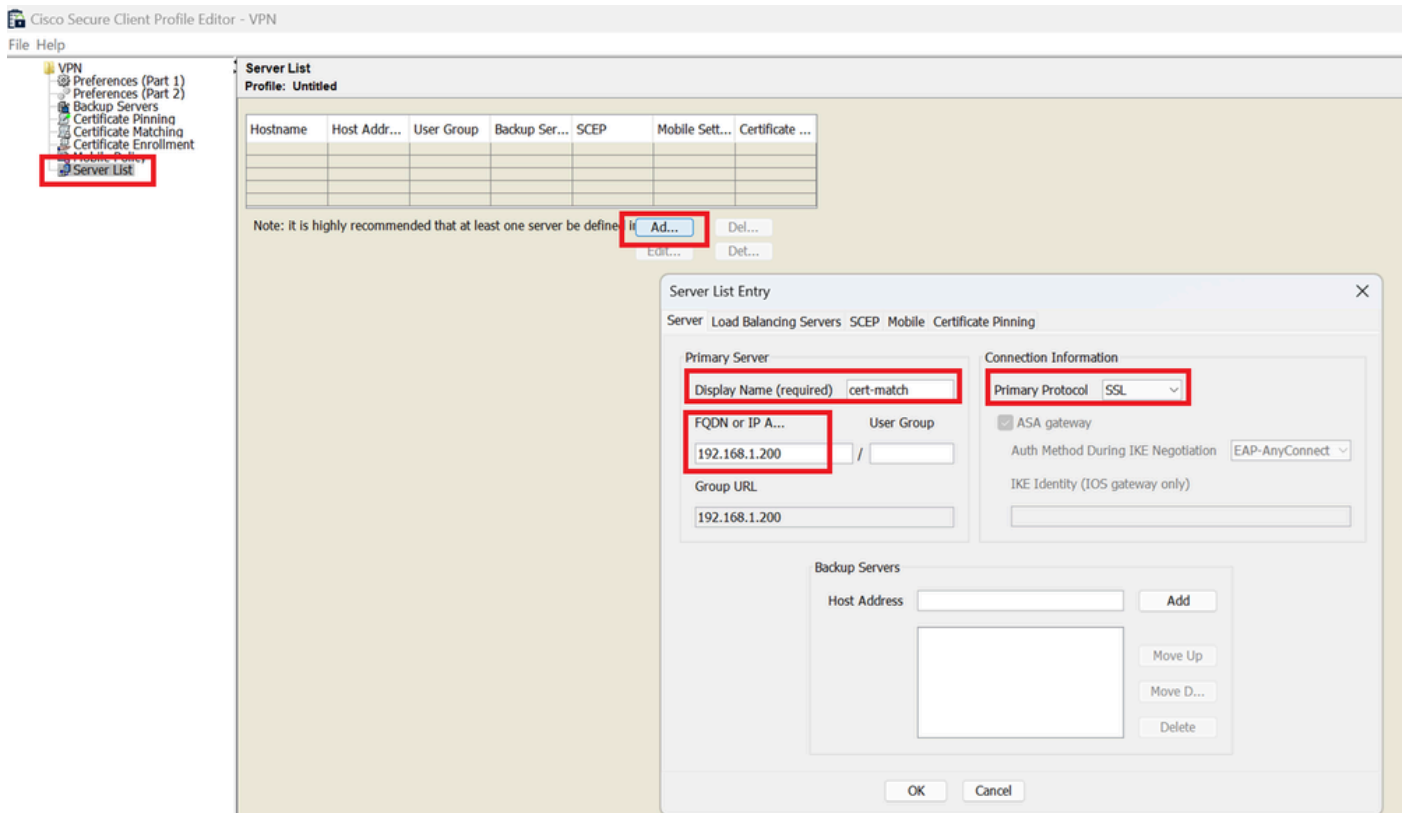
CANCEL OK

IPv4地址池的详细信息

#### 第四步：创建安全客户端配置文件

从[思科软件](#)站点下载并安装安全客户端配置文件编辑器。导航到Server List，单击Add按钮。输入必要信息以添加服务器列表条目，然后单击OK按钮。

- 显示名称：cert-match
- FQDN或IP地址：192.168.1.200
- 主要协议：SSL



服务器列表条目

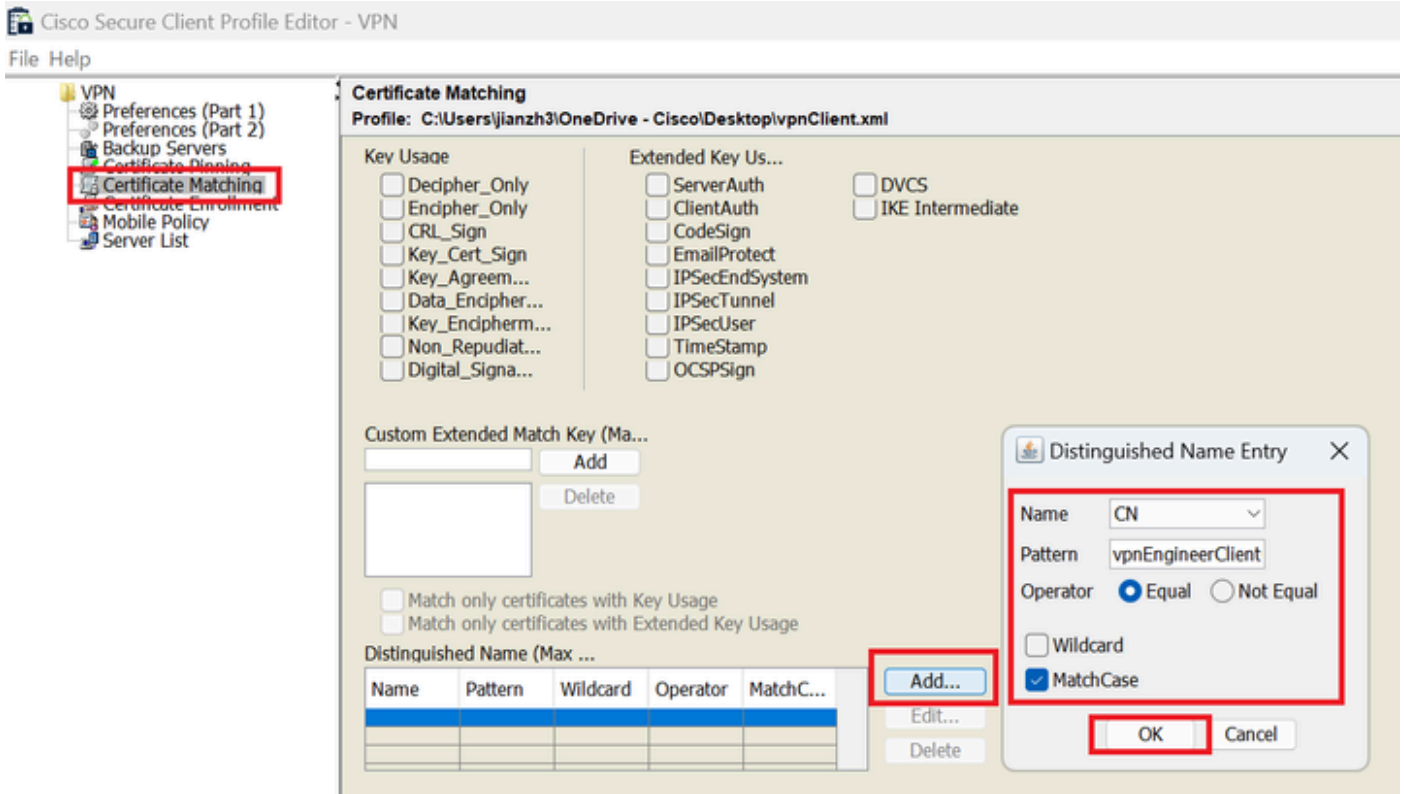
导航到证书匹配，单击添加按钮。输入必要信息以添加可分辨名称条目，然后单击OK按钮。

- 名称：CN
- 模式：vpnEngineerClientCN
- 运算符：等于



注意：选中本文档中的MatchCase选项。

---



可分辨名称条目

将安全客户端配置文件保存到本地计算机，并确认配置文件的详细信息。

```

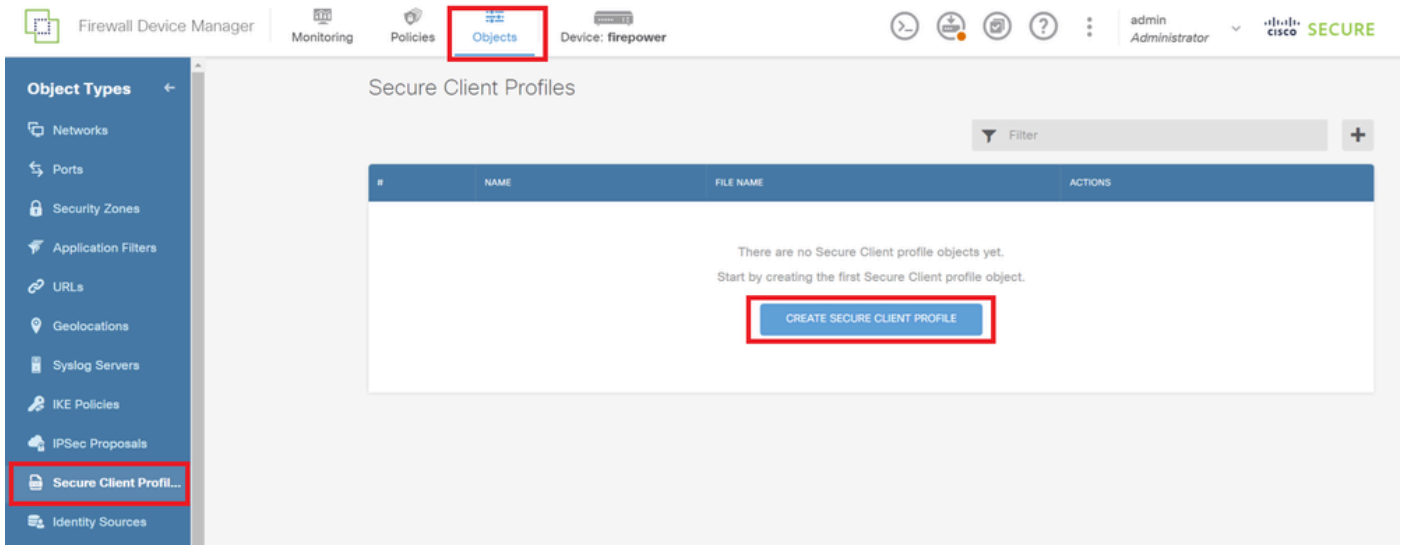
<CertificateMatch>
  <MatchOnlyCertsWithKUI>false</MatchOnlyCertsWithKUI>
  <DistinguishedName>
    <DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled" MatchCase="Enabled">
      <Name>CN</Name>
      <Pattern>vpnEngineerClientCN</Pattern>
    </DistinguishedNameDefinition>
  </DistinguishedName>
</CertificateMatch>
<EnableAutomaticServerSelection UserControllable="false">
  false
  <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
  <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
</EnableAutomaticServerSelection>
<RetainVpnOnLogoff>false </RetainVpnOnLogoff>
<CaptivePortalRemediationBrowserFailover>false</CaptivePortalRemediationBrowserFailover>
<AllowManualHostInput>>true</AllowManualHostInput>
</ClientInitialization>
<ServerList>
  <HostEntry>
    <HostName>cert-match</HostName>
    <HostAddress>192.168.1.200</HostAddress>
  </HostEntry>
</ServerList>
</AnyConnectProfile>

```

安全客户端配置文件

第五步：将安全客户端配置文件上传到FDM

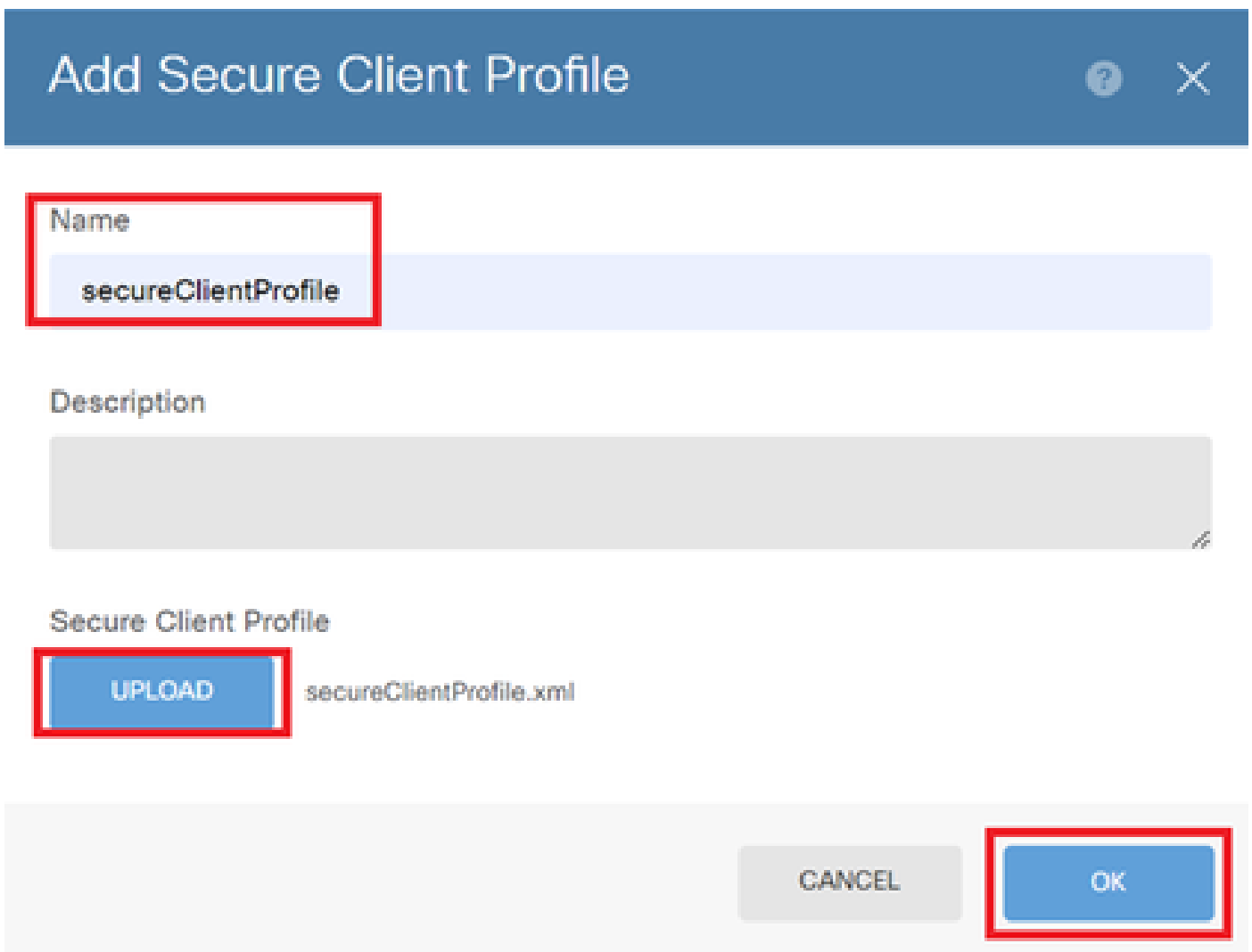
导航到对象>安全客户端配置文件，单击创建安全客户端配置文件按钮。



创建安全客户端配置文件

输入必要信息添加安全客户端配置文件，并单击OK按钮。

- 名称：secureClientProfile
- 安全客户端配置文件：secureClientProfile.xml (从本地计算机上传)

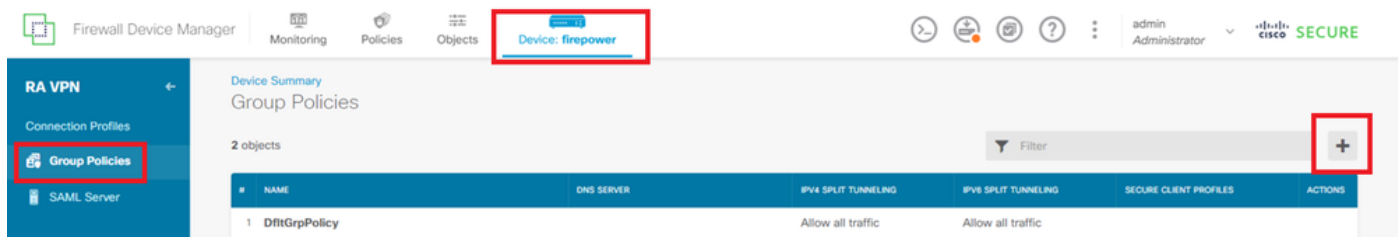


添加安全客户端配置文件



## 第六步：添加组策略

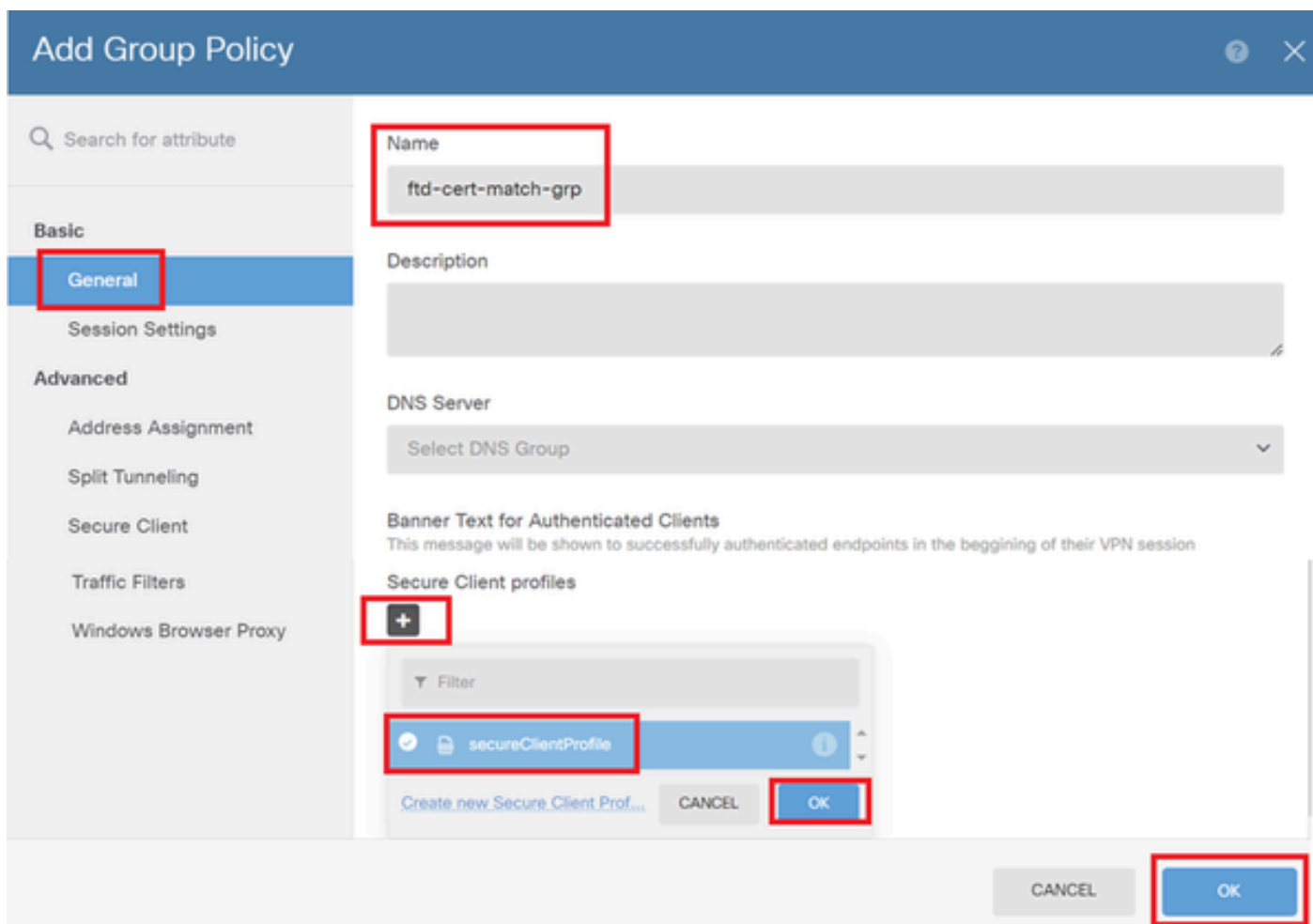
导航到Device > Remote Access VPN > View Configuration > Group Policies，点击+按钮。



添加组策略

输入必要信息添加组策略，然后单击OK按钮。

- 名称：ftd-cert-match-grp
- 安全客户端配置文件：secureClientProfile



组策略详细信息

## 步骤 7. 添加FTD证书

导航到对象>证书，在+项目中单击添加内部证书。

Firewall Device Manager | Monitoring | Policies | **Objects** | Device: firepower | admin Administrator | CISCO SECURE

Object Types

- Networks
- Ports
- Security Zones
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- Secure Client Profiles
- Identity Sources
- Users
- Certificates**

Certificates

121 objects

Filter

Preset filters: System defined, User defined

#	NAME	TYPE	ACTIONS
1	AAA-Certificate-Services	Trusted CA Certificate	
2	ACCVRAIZ1	Trusted CA Certificate	
3	Actalis-Authentication-Root-CA	Trusted CA Certificate	
4	AffirmTrust-Commercial	Trusted CA Certificate	
5	AffirmTrust-Networking	Trusted CA Certificate	
6	AffirmTrust-Premium	Trusted CA Certificate	
7	AffirmTrust-Premium-ECC	Trusted CA Certificate	
8	Amazon-Root-CA-1	Trusted CA Certificate	
9	Amazon-Root-CA-2	Trusted CA Certificate	
10	Amazon-Root-CA-3	Trusted CA Certificate	
11	DefaultInternalCertificate	Internal Certificate	
12	DefaultWebserverCertificate	Internal Certificate	

Actions: Add Internal CA, **Add Internal Certificate**, Add Trusted CA Certificate

添加内部证书

单击Upload Certificate and Key。

Choose the type of internal certificate you want to create

Choose the type of internal certificate you want to create

- Upload Certificate and Key**  
Create a certificate from existing files.  
PEM and DER files are supported.
- Self-Signed Certificate  
Create a new certificate that is signed by the device.

上传证书和密钥

输入FTD证书的必要信息，从本地计算机导入证书和证书密钥，然后单击OK按钮。

- 名称：ftd-vpn-cert
- 特殊服务的验证使用情况：SSL服务器

# Add Internal Certificate



Name

ftd-vpn-cert

Certificate

Paste certificate, or choose a file (DER, PEM, CRT, CER)

ftdCert.crt

[Upload Certificate](#)

```
-----BEGIN CERTIFICATE-----  
MIIDfDCCAmSgAwIBAgIIIkE99YS2cmwwDQYJKoZIhvcNAQELBQAwTELMAkGA1UE  
BhMCS1AxDjAMBgNVBAgTBVRva31vMQ4wDAYDVQQHEwVub2t5bzEOMAwGA1UEChMF  
O31-V38-wD4AMBgNVBAgTBVRva31vMQ4wDAYDVQQHEwVub2t5bzEOMAwGA1UEChMF
```

Certificate Key

Paste certificate key, or choose a file (KEY, PEM)

ftdCertKey.pem

[Upload Certificate Key](#)

```
-----BEGIN RSA PRIVATE KEY-----  
MIIEogIBAAKCAQEAXdn5eTUngo5+GUG2Ng2FjI/+xHRkRrf6o2OccGdzLYK1tzw8  
98HPu1YP0T/qwCffKXuMQ9DEVGWIjLRX9nvXd8NoaKUbZVzc03qM3Aje87p0h0t0  
+46h1W0Tz0u431+4w03w0+6YEE8+3U4140w738wT160wM7TVw0734w0wYw0C
```

Validation Usage for Special Services

SSL Server

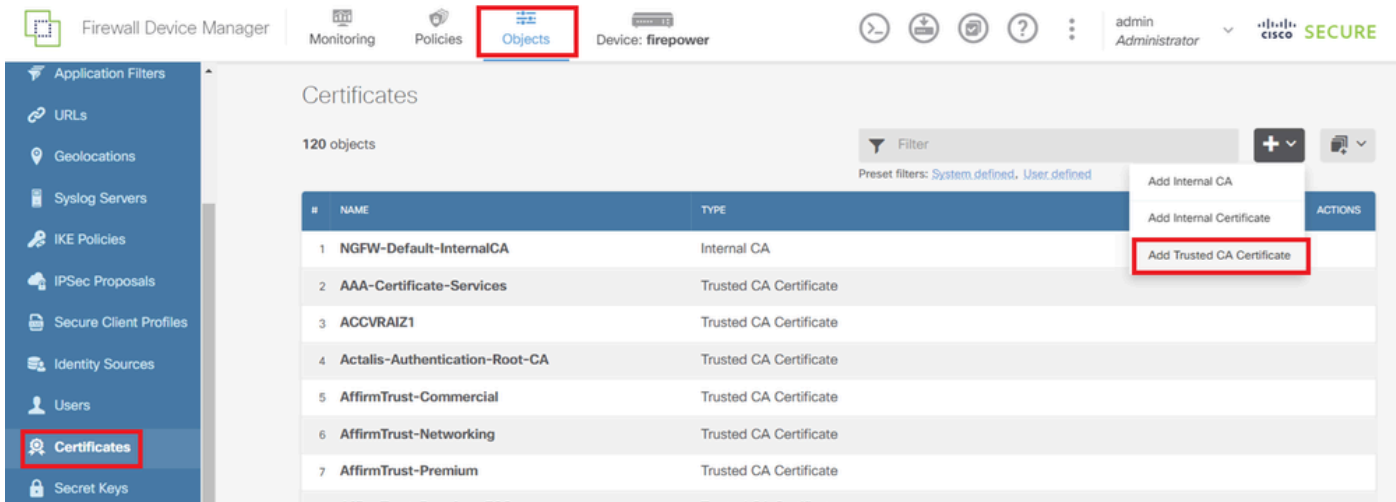
CANCEL

OK

内部证书的详细信息

步骤 8将CA添加到FTD

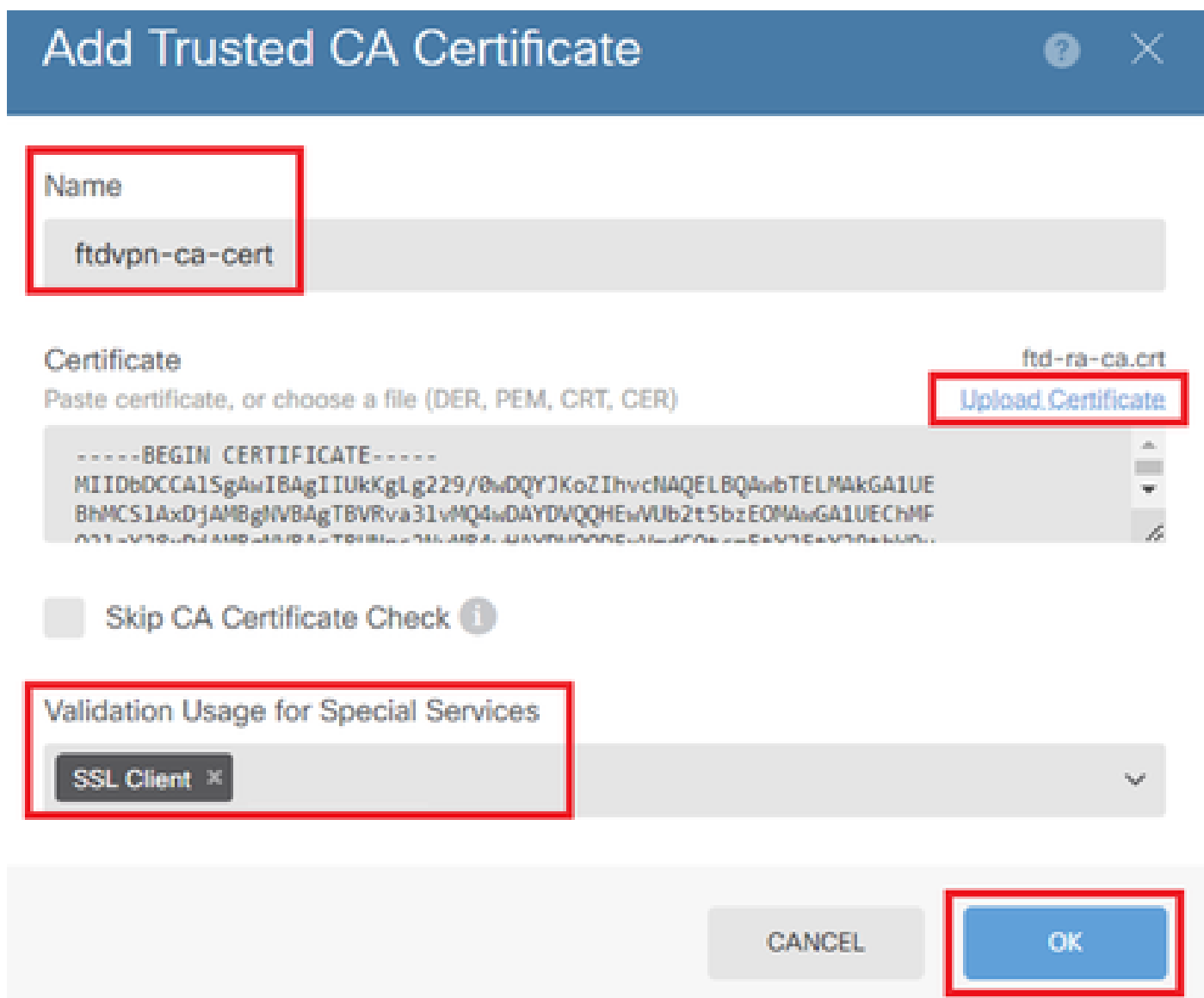
导航到对象>证书，在+项目中单击添加受信任CA证书。



添加受信任CA证书

输入CA的必要信息，从本地计算机导入证书。

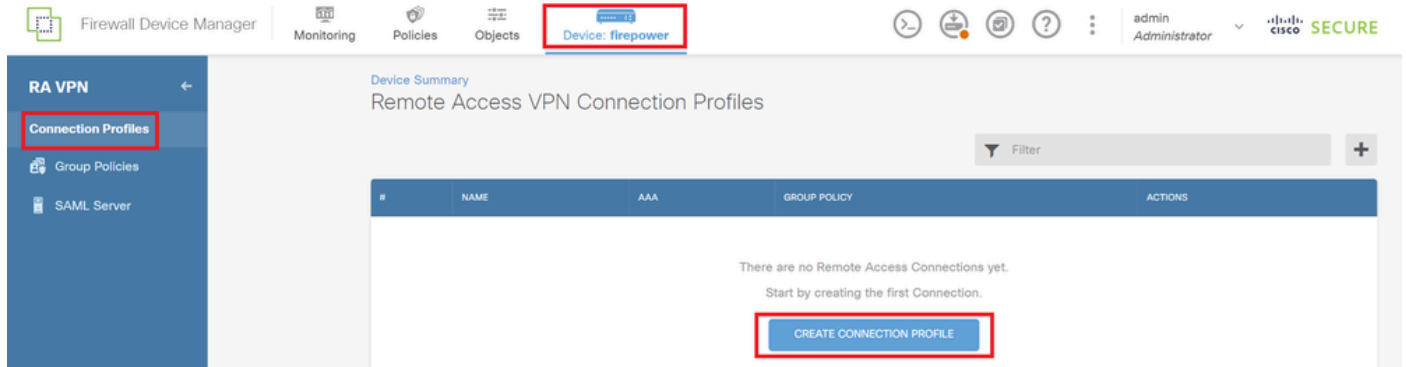
- 名称：ftdvpn-ca-cert
- 特殊服务的验证用法：SSL客户端



受信任CA证书的详细信息

## 步骤 9 添加远程访问VPN连接配置文件

导航到Device > Remote Access VPN > View Configuration > Connection Profiles，单击CREATE CONNECTION PROFILE按钮。



添加远程访问VPN连接配置文件

输入连接配置文件的必要信息，然后单击Next按钮。

- 连接配置文件名称：ftd-cert-match-vpn
- Authentication Type：仅客户端证书
- Username From Certificate：映射特定字段
- 主字段：CN（公用名）
- 辅助字段：OU（组织单位）
- IPv4地址池：ftd-cert-match-pool

Remote Access VPN | 1 Connection and Client Configuration | 2 Remote User Experience | 3 Global Settings | 4 Summary



### Connection and Client Configuration

Specify how to authenticate remote users and the secure clients they can use to connect to the inside network.

#### Connection Profile Name

This name is configured as a connection alias, it can be used to connect to the VPN gateway

ftd-cert-match-vpn

#### Group Alias (one per line, up to 5)

ftd-cert-match-vpn

#### Group URL (one per line, up to 5)

#### Primary Identity Source

##### Authentication Type

Client Certificate Only

#### Username from Certificate

##### Map Specific Field

Primary Field: CN (Common Name) | Secondary Field: OU (Organisational Unit)

Use entire DN (distinguished name) as username

##### Advanced

#### Authorization Server

Please select

#### Accounting Server

Please select

#### Client Address Pool Assignment

##### IPv4 Address Pool

Endpoints are provided an address from this pool

ftd-cert-match-pool

##### IPv6 Address Pool

Endpoints are provided an address from this pool

+

##### DHCP Servers

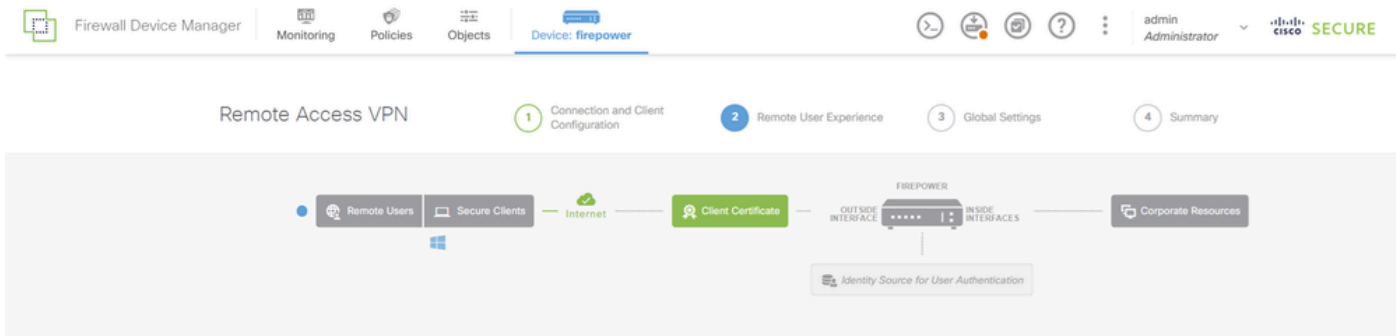
+

CANCEL | NEXT

VPN连接配置文件的详细信息

输入组策略的必要信息，然后单击Next按钮。

- 查看组策略：ftd-cert-match-grp



### Remote User Experience

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

View Group Policy

ftd-cert-match-grp

Policy Group Brief Details

DNS + BANNER Edit

DNS Server None

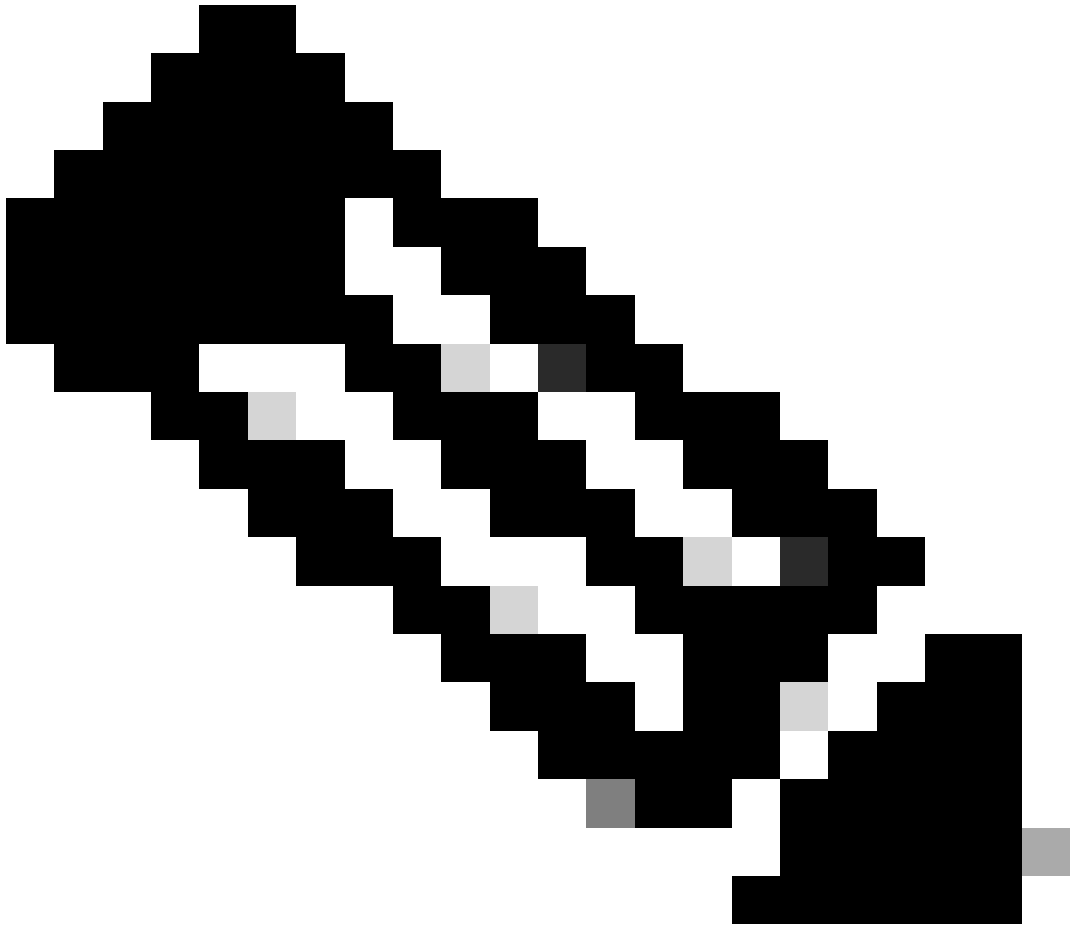
Banner Text for Authentication

BACK NEXT

选择组策略

为VPN连接选择Certificate of Device Identity、Outside Interface、Secure Client Package。

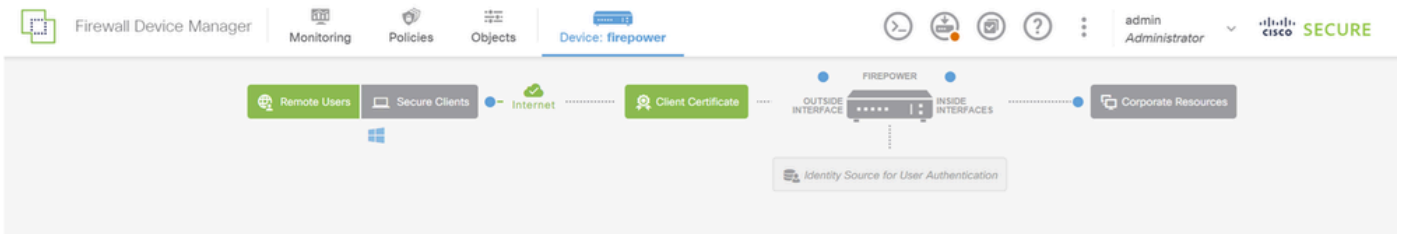
- 设备身份证书：ftd-vpn-cert
- 外部接口：外部(GigabitEthernet0/0)
- 安全客户端软件包：cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg



注意：本文档中禁用了NAT免除功能。

---





## Global Settings

These settings control the basic functioning of the connection. Changes to any of these options apply to all connection profiles; you cannot configure different settings in different profiles.

**Certificate of Device Identity**  
ftd-vpn-cert (Validation Usage: SSL Se...)

**Outside Interface**  
outside (GigabitEthernet0/0)

Fully-qualified Domain Name for the Outside Interface  
Port  
e.g. ravn.example.com 443  
e.g. 8080

**Access Control for VPN Traffic**  
Decrypted VPN traffic is subjected to access control policy inspection by default. Enabling the Bypass Access Control policy for decrypted traffic option bypasses the access control policy, but for remote access VPN, the VPN Filter ACL and the authorization ACL downloaded from the AAA server are still applied to VPN traffic.  
 Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

**NAT Exempt**

**Secure Client Package**  
If a user does not already have the right secure client package installed, the system will launch the secure client installer when the client authenticates for the first time. The user can then install the package from the system.  
You can download secure client packages from [software.cisco.com](https://software.cisco.com).  
You must have the necessary secure client software license.

**Packages**  
UPLOAD PACKAGE  
Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg

BACK NEXT

全局设置的详细信息

## 步骤 10 确认连接配置文件的摘要

确认输入的VPN连接信息，然后单击FINISH按钮。

^ Summary

Review the summary of the Remote Access VPN configuration.

### Ftd-Cert-Match-Vpn

**STEP 1: CONNECTION AND CLIENT CONFIGURATION**

Primary Identity Source

Authentication Type: Client Certificate Only

Primary Identity Source: -

Fallback Local Identity Source: -

Username from Certificate: Map Specific Field

Primary Field: CN (Common Name)

Secondary Field: OU (Organisational Unit)

Advanced

Authorization Server

Accounting Server

Client Address Pool Assignment

IPv4 Address Pool: ftd-cert-match-pool

IPv6 Address Pool: -

DHCP Servers: -

**STEP 2: GROUP POLICY**

Group Policy Name: ftd-cert-match-grp

Banner + DNS Server

DNS Server: -

Banner text for authenticated clients: -

Session Settings

Maximum Connection Time / Alert Interval: Unlimited / 1 minutes

Idle Timeout / Alert Interval: 30 / 1 minutes

Simultaneous Login per User: 3

Split Tunneling

IPv4 Split Tunneling: Allow all traffic over tunnel

IPv6 Split Tunneling: Allow all traffic over tunnel

Secure Client

Secure Client Profiles: secureClientProfile

**STEP 3: GLOBAL SETTINGS**

Certificate of Device Identity: ftd-vpn-cert

Outside Interface: GigabitEthernet0/0 (outside)

Fully-qualified Domain Name for the Outside Interface: -

Port: 443

Access Control for VPN Traffic: No

NAT Exempt

NAT Exempt: No

Inside Interfaces: -

Inside Networks: -

Secure Client Package

Packages: Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg

BACK FINISH

确认连接配置文件的摘要

在FTD CLI中确认

从FDM部署后，在FTD CLI中确认VPN连接设置。

```
// Defines IP of interface
interface GigabitEthernet0/0
speed auto
nameif outside
cts manual
propagate sgt preserve-untag
policy static sgt disabled trusted
security-level 0
ip address 192.168.1.200 255.255.255.0

// Defines a pool of addresses
ip local pool ftd-cert-match-pool 172.16.1.150-172.16.1.160

// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftd-vpn-cert
enrollment terminal
keypair ftd-vpn-cert
crl configure

// Server Certificate
crypto ca certificate chain ftdvpn-ca-cert
certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
.....
quit

// Defines Trustpoint for CA
crypto ca trustpoint ftdvpn-ca-cert
enrollment terminal
validation-usage ssl-client
crl configure

// CA
crypto ca certificate chain ftdvpn-ca-cert
certificate ca 5242a02e0db6f7fd
3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7
.....
quit

// Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images
webvpn
enable outside
http-headers
hsts-server
enable
max-age 31536000
include-sub-domains
no preload
hsts-client
enable
x-content-type-options
x-xss-protection
content-security-policy
anyconnect image disk0:/anyconnpkgs/cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg 2
anyconnect profiles secureClientProfile disk0:/anyconncprofs/secureClientProfile.xml
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Configures the group-policy to allow SSL connections
```

```

group-policy ftd-cert-match-grp internal
group-policy ftd-cert-match-grp attributes
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelall
ipv6-split-tunnel-policy tunnelall
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
msie-proxy method no-modify
vlan none
address-pools none
ipv6-address-pools none
webvpn
anyconnect ssl dtls none
anyconnect mtu 1406
anyconnect ssl keepalive none
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client none
anyconnect dpd-interval gateway none
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules none
anyconnect profiles value secureClientProfile type user
anyconnect ssl df-bit-ignore disable
always-on-vpn profile-setting

// Configures the tunnel-group to use the certificate authentication
tunnel-group ftd-cert-match-vpn type remote-access
tunnel-group ftd-cert-match-vpn general-attributes
address-pool ftd-cert-match-pool
default-group-policy ftd-cert-match-grp
tunnel-group ftd-cert-match-vpn webvpn-attributes
authentication certificate
group-alias ftd-cert-match-vpn enable

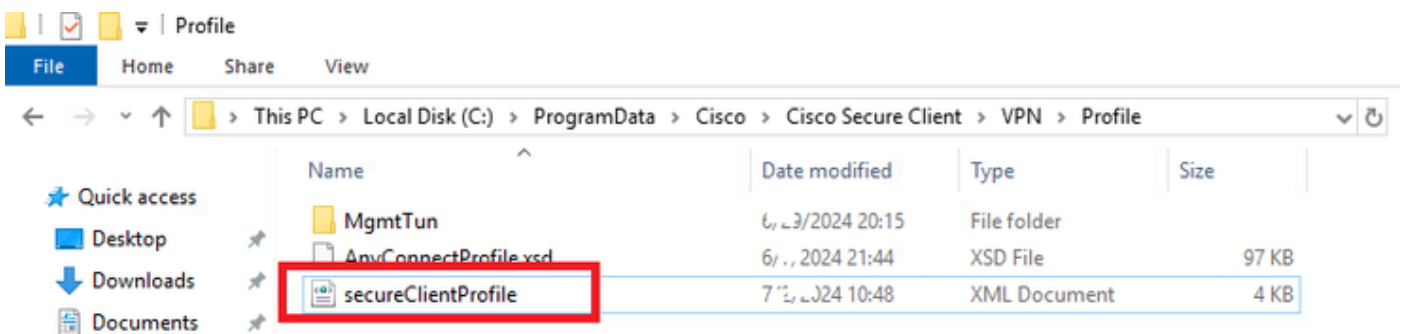
```

## 在VPN客户端中确认

步骤1:将安全客户端配置文件复制到VPN客户端

将安全客户端配置文件复制到工程师VPN客户端和管理器VPN客户端。

注意：Windows计算机中安全客户端配置文件的目录：C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile



将安全客户端配置文件复制到VPN客户端

## 第二步：确认客户端证书

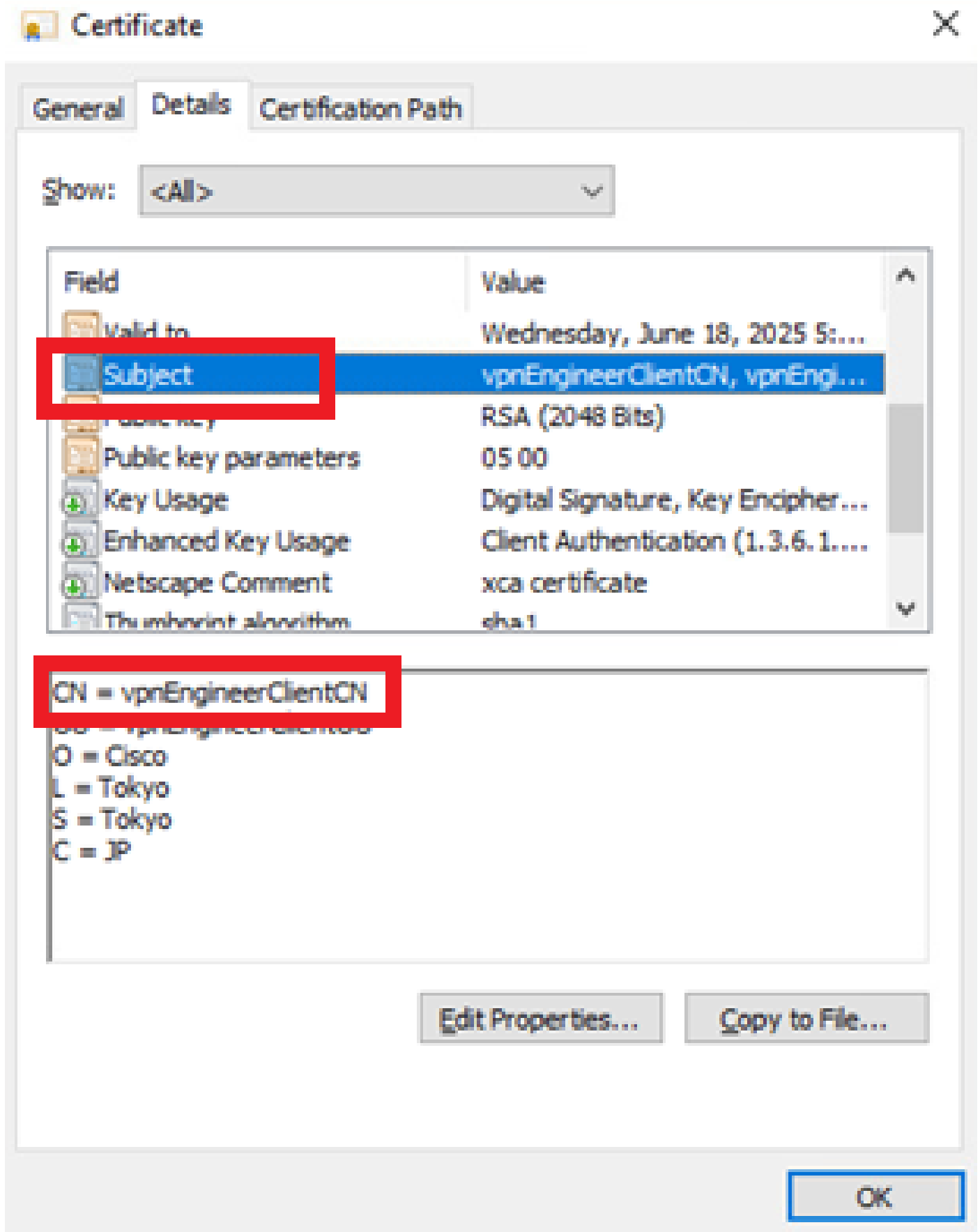
在工程师VPN客户端中，导航到证书-当前用户>个人>证书，检查用于身份验证的客户端证书。



确认工程师VPN客户端的证书

双击客户端证书，导航到详细信息，检查主题的信息。

- 主题 : CN = vpnEngineerClientCN



工程师客户端证书的详细信息

在Manager VPN Client中，导航到Certificates - Current User > Personal > Certificates，检查用于身份验证的客户端证书。



确认Manager VPN客户端的证书

双击客户端证书，导航到详细信息，检查主题的信息。

- 主题：CN = vpnManagerClientCN



# Certificate



General Details Certification Path

Show: <All>

Field	Value
Issued To	Thursday, June 19, 2025 9:41...
Subject	vpnManagerClientCN, vpnMan...
Public key	RSA (2048 Bits)
Public key parameters	05 00
Key Usage	Digital Signature, Key Encipher...
Enhanced Key Usage	Client Authentication (1.3.6.1....
Netscape Comment	xca certificate
Thumbprint algorithm	sha1

CN = vpnManagerClientCN

O = Cisco  
L = Tokyo  
S = Tokyo  
C = JP

Edit Properties...

Copy to File...

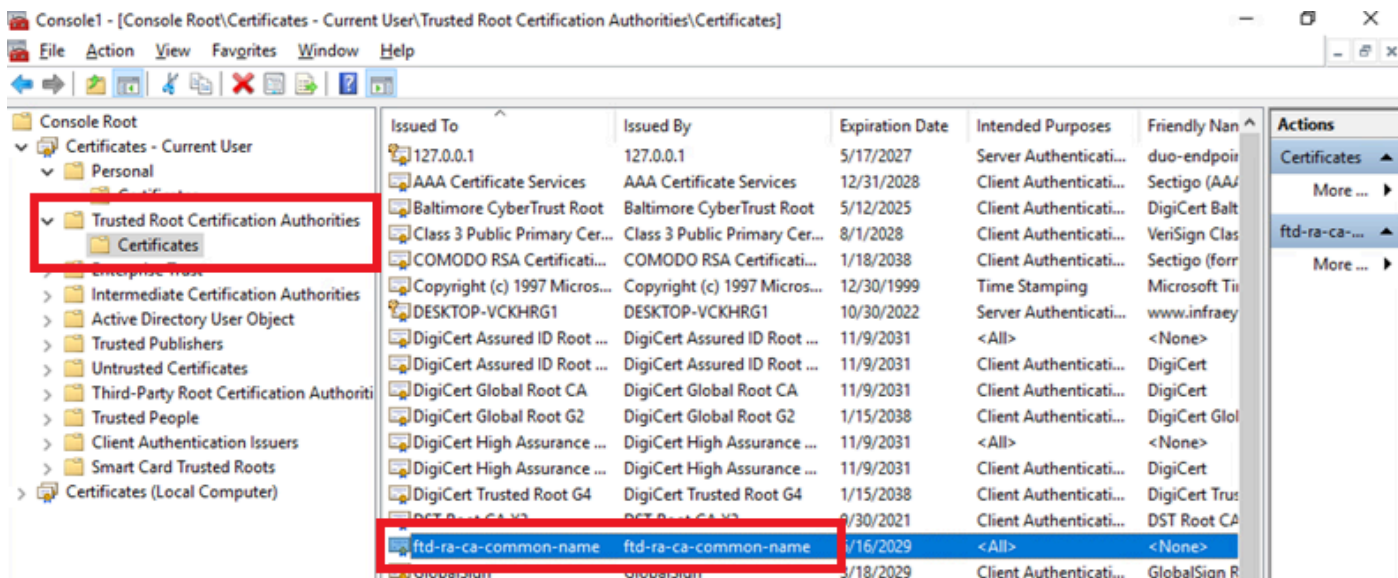
OK

Manager客户端证书的详细信息

第三步：确认CA

在工程师VPN客户端和管理器VPN客户端中，导航到证书-当前用户>受信任的根证书颁发机构>证书，检查用于身份验证的CA。

- 颁发者：ftd-ra-ca-common-name

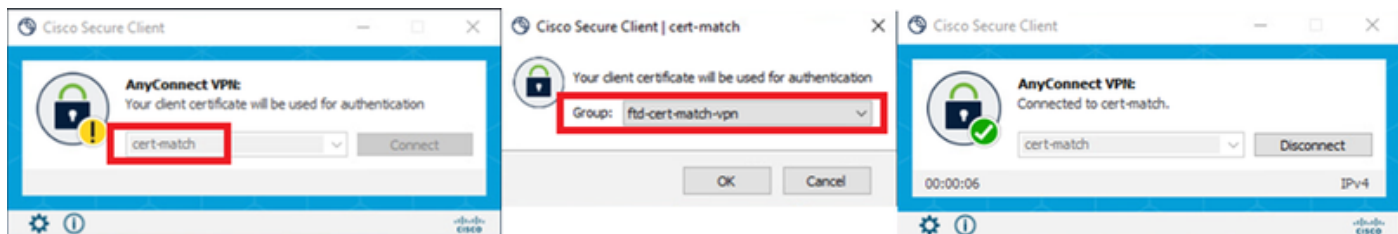


确认CA

## 验证

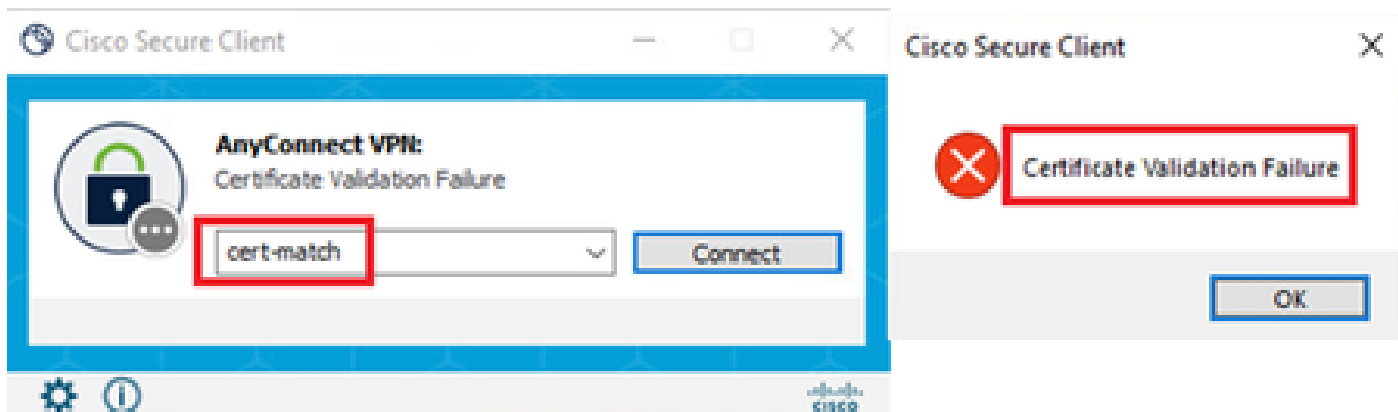
步骤1:启动VPN连接

在工程师VPN客户端中，启动Cisco安全客户端连接。无需输入用户名和密码，VPN连接成功。



工程师VPN客户端的VPN连接成功

在管理器VPN客户端中，启动Cisco安全客户端连接。由于证书验证失败，VPN连接失败。



## 第二步：在FTD CLI中确认VPN会话

在FTD (Lina) CLI中运行show vpn-sessiondb detail anyconnect命令，确认工程师的VPN会话。

```
firepower# show vpn-sessiondb detail anyconnect
```

Session Type: AnyConnect Detailed

Username : vpnEngineerClientCN Index : 32  
Assigned IP : 172.16.1.150 Public IP : 192.168.1.11  
Protocol : AnyConnect-Parent SSL-Tunnel  
License : AnyConnect Premium  
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-256  
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA384  
Bytes Tx : 14718 Bytes Rx : 12919  
Pkts Tx : 2 Pkts Rx : 51  
Pkts Tx Drop : 0 Pkts Rx Drop : 0  
Group Policy : ftd-cert-match-grp Tunnel Group : ftd-cert-match-vpn  
Login Time : 05:42:03 UTC Tue Jul 2 2024  
Duration : 0h:00m:11s  
Inactivity : 0h:00m:00s  
VLAN Mapping : N/A VLAN : none  
Audt Sess ID : 0000000000200006683932b  
Security Grp : none Tunnel Zone : 0

AnyConnect-Parent Tunnels: 1

SSL-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 32.1  
Public IP : 192.168.1.11  
Encryption : none Hashing : none  
TCP Src Port : 50170 TCP Dst Port : 443  
Auth Mode : Certificate  
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes  
Client OS : win  
Client OS Ver: 10.0.17763  
Client Type : AnyConnect  
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74  
Bytes Tx : 7359 Bytes Rx : 0  
Pkts Tx : 1 Pkts Rx : 0  
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 32.2  
Assigned IP : 172.16.1.150 Public IP : 192.168.1.11  
Encryption : AES-GCM-256 Hashing : SHA384  
Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384  
Encapsulation: TLSv1.2 TCP Src Port : 50177  
TCP Dst Port : 443 Auth Mode : Certificate  
Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes  
Client OS : Windows  
Client Type : SSL VPN Client  
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74

Bytes Tx : 7359 Bytes Rx : 12919

Pkts Tx : 1 Pkts Rx : 51

Pkts Tx Drop : 0 Pkts Rx Drop : 0

## 故障排除

您可以在Lina引擎的调试syslog和Windows计算机上的DART文件中找到有关VPN身份验证的信息。

这是从工程师客户端进行VPN连接期间Lina引擎中的调试日志示例。

Jul 02 2024 04:16:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClientCN

Jul 02 2024 04:16:03: %FTD-6-717022: Certificate was successfully validated. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClientCN

Jul 02 2024 04:16:04: %FTD-6-113009: AAA retrieved default group policy (ftd-cert-match-grp) for user = vpnEngineerClientCN

Jul 02 2024 04:16:09: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50158 to 192.168.1.200/443 for TLSv1.2 session

## 相关信息

[为Firepower 2100配置FDM机上管理服务](#)

[在FDM管理的FTD上配置远程访问VPN](#)

[配置并验证Firepower设备管理器中的系统日志](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。