

通过FMC为FTD上的安全客户端配置AAA和证书身份验证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[网络图](#)

[配置](#)

[FMC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：添加策略分配](#)

[第四步：连接配置文件的配置详细信息](#)

[第五步：为连接配置文件添加地址池](#)

[第六步：添加连接配置文件的组策略](#)

[步骤 7.为连接配置文件配置安全客户端映像](#)

[步骤 8连接配置文件的配置访问和证书](#)

[步骤 9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:确认客户端证书](#)

[第二步：确认CA](#)

[验证](#)

[步骤1:启动VPN连接](#)

[第二步：确认FMC中的活动会话](#)

[第三步：在FTD CLI中确认VPN会话](#)

[第四步：确认与服务器的通信](#)

[故障排除](#)

[参考](#)

简介

本文档介绍在由FMC管理的FTD上使用AAA和证书身份验证配置SSL思科安全客户端的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科Firepower管理中心(FMC)
- 防火墙威胁防御虚拟(FTD)
- VPN身份验证流程

使用的组件

- 思科VMWare Firepower管理中心7.4.1
- 思科防火墙威胁防御虚拟7.4.1
- 思科安全客户端5.1.3.62

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

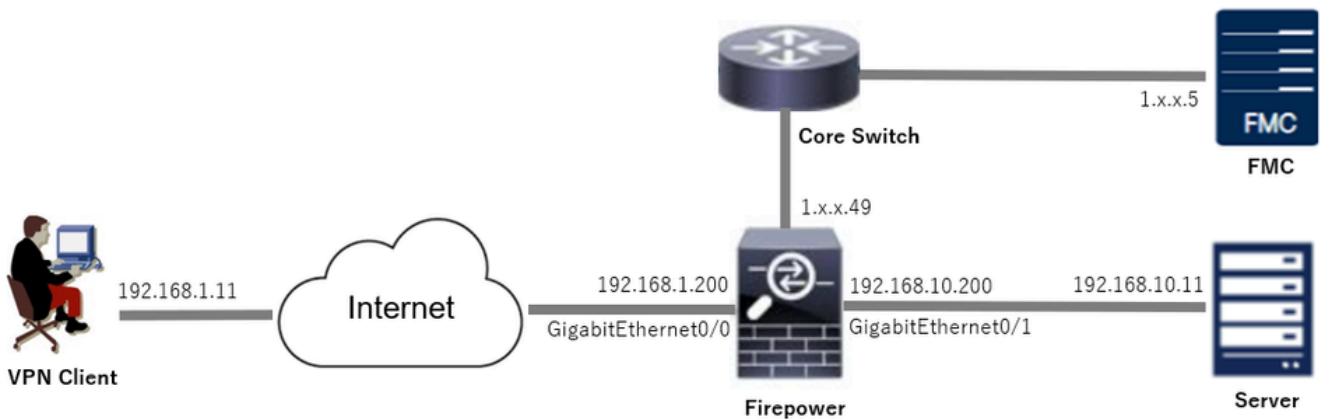
随着组织采取更严格的安全措施，将双因素身份验证(2FA)与基于证书的身份验证相结合已成为一种常见做法，可增强安全性并防范未经授权的访问。可以显著改善用户体验和安全性的功能之一是能够预填思科安全客户端中的用户名。此功能简化了登录过程并增强了远程访问的整体效率。本文档介绍如何在FTD上将预填充的用户名与Cisco Secure Client集成，以确保用户能够快速安全地连接到网络。

这些证书中包含用于授权目的的公用名称。

- CA : ftd-ra-ca-common-name
- 客户端证书 : ssIVPNClientCN
- 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。



网络图

配置

FMC中的配置

步骤1:配置FTD接口

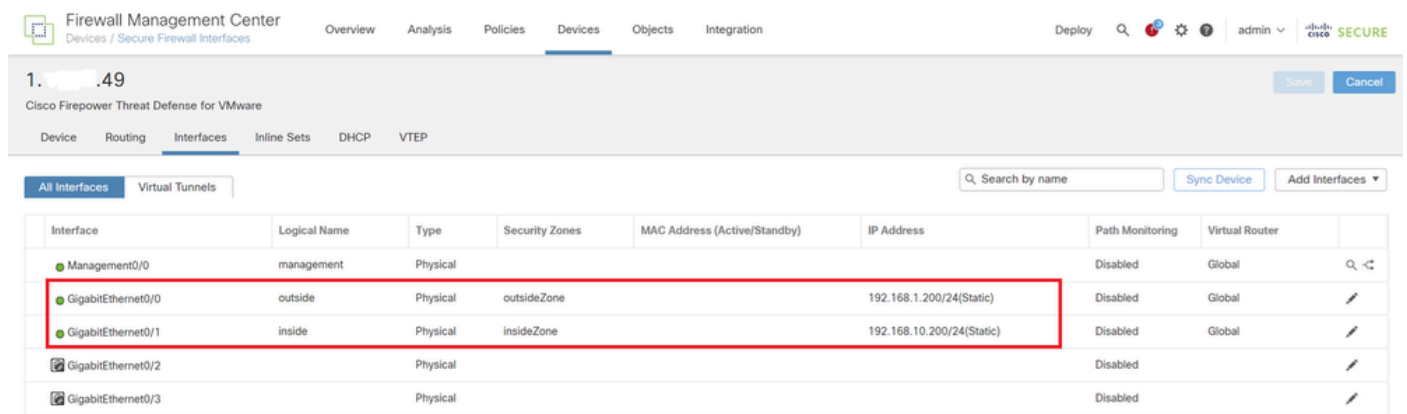
导航到Devices > Device Management，在Interfaces选项卡中编辑目标FTD设备，并为FTD配置内部和外部接口。

对于GigabitEthernet0/0，

- 名称：outside
- 安全区域：outsideZone
- IP地址：192.168.1.200/24

对于GigabitEthernet0/1，

- 名称：inside
- 安全区域：insideZone
- IP地址：192.168.10.200/24



Firewall Management Center
Devices / Secure Firewall Interfaces

Overview Analysis Policies Devices Objects Integration

Deploy Search Settings admin Cisco SECURE

1. .49 Save Cancel

Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP VTEP

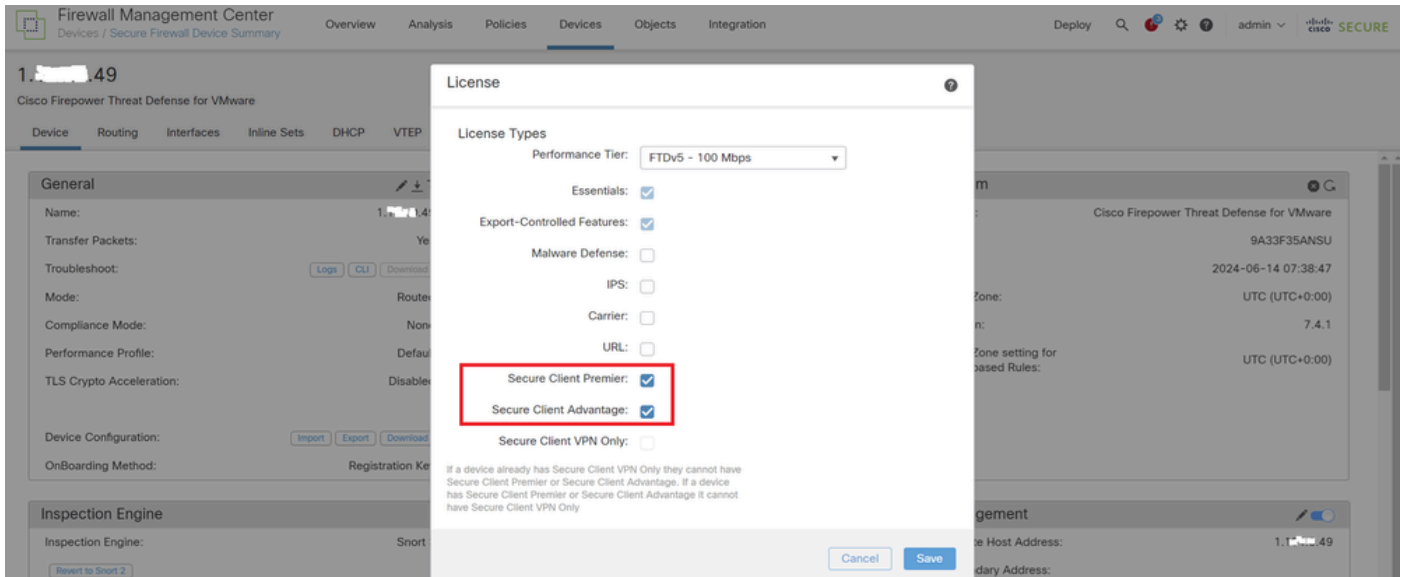
All Interfaces Virtual Tunnels Search by name Sync Device Add Interfaces

Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address	Path Monitoring	Virtual Router
Management0/0	management	Physical				Disabled	Global
GigabitEthernet0/0	outside	Physical	outsideZone		192.168.1.200/24(Static)	Disabled	Global
GigabitEthernet0/1	inside	Physical	insideZone		192.168.10.200/24(Static)	Disabled	Global
GigabitEthernet0/2		Physical				Disabled	
GigabitEthernet0/3		Physical				Disabled	

FTD接口

第二步：确认思科安全客户端许可证

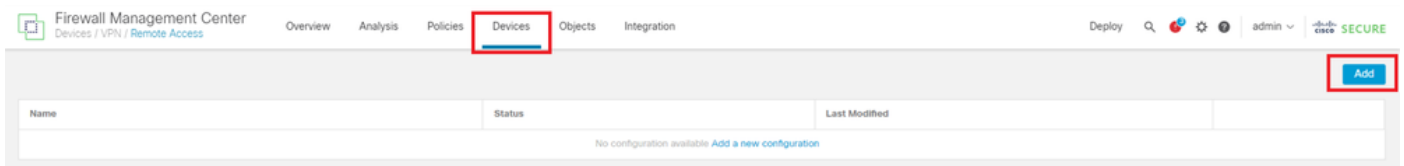
导航到设备>设备管理，编辑目标FTD设备，在设备选项卡中确认Cisco安全客户端许可证。



安全客户端许可证

第三步：添加策略分配

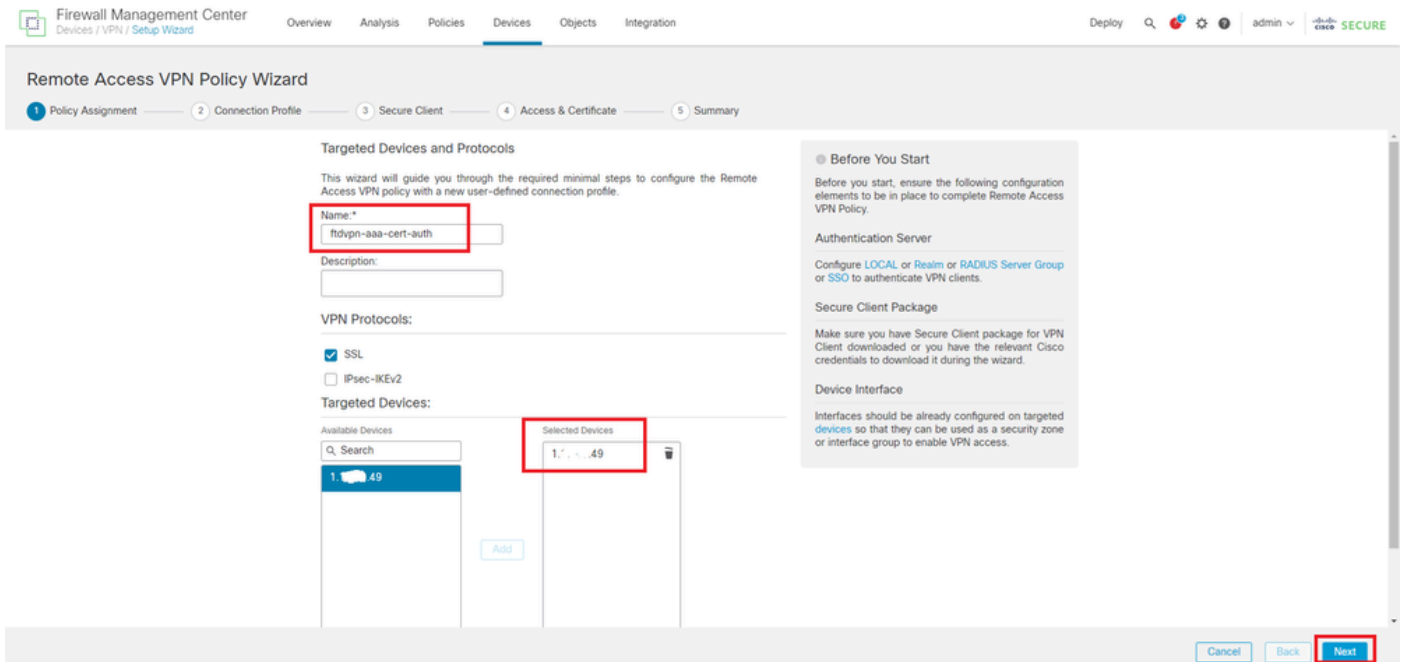
导航到Devices > VPN > Remote Access，单击Add按钮。



添加远程访问VPN

输入必要信息，然后单击Next按钮。

- 名称：ftdvpn-aaa-cert-auth
- VPN协议：SSL
- 目标设备：1.x.x.49

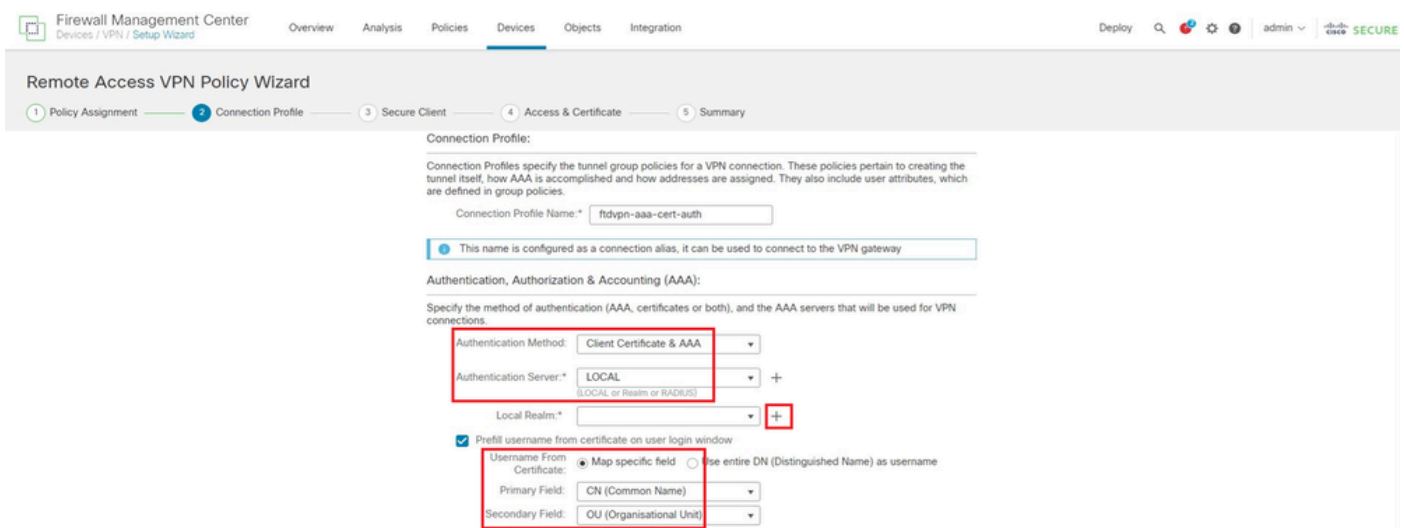


策略分配

第四步：连接配置文件的配置详细信息

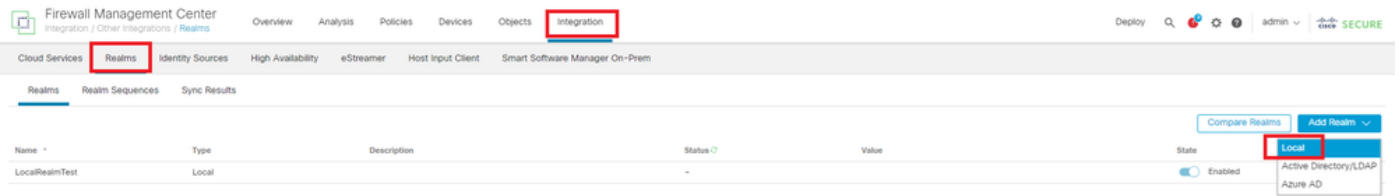
输入连接配置文件的必要信息，然后点击本地领域项目旁边的+按钮。

- 身份验证方法：客户端证书和AAA
- 身份验证服务器：本地
- 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)



连接配置文件的详细信息

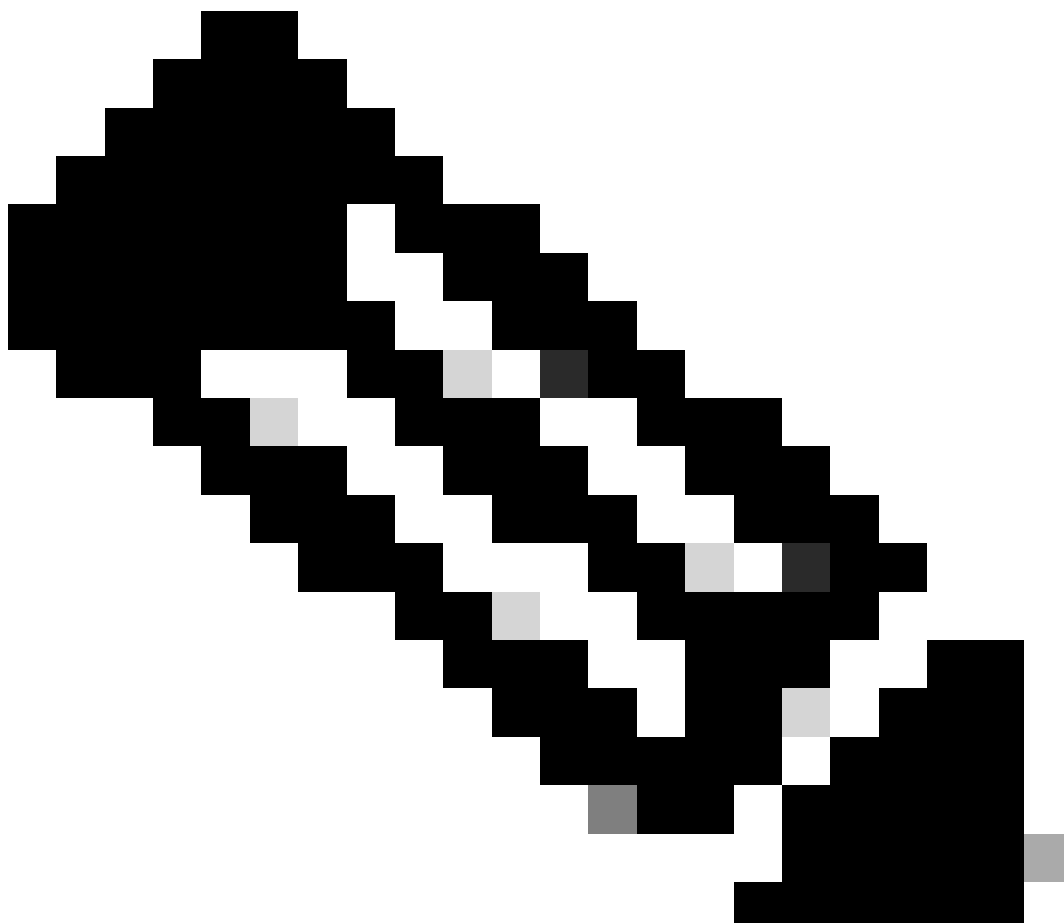
从Add Realm 下拉列表中单击Local，以便添加新的本地领域。



添加本地领域

输入本地领域的必要信息，然后单击Save按钮。

- 名称：LocalRealmTest
- 用户名：ssIVPNClientCN



注意：用户名等于客户端证书中的公用名

Add New Local Realm



Name*	Description
LocalRealmTest	

Local User Configuration

ssIVPNCilentCN

Username	ssIVPNCilentCN
Password	Confirm Password
.....

[Add another local user](#)

Cancel

Save

本地领域的详细信息

第五步：为连接配置文件添加地址池

单击IPv4地址池项目旁边的edit按钮。

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) ●

Use DHCP Servers

Use IP Address Pools

IPv4 Address Pools:

IPv6 Address Pools:

添加IPv4地址池

输入必要信息以添加新的IPv4地址池。为连接配置文件选择新的IPv4地址池。

- 名称：ftdvpn-aaa-cert-pool
- IPv4地址范围：172.16.1.40-172.16.1.50
- 掩码：255.255.255.0

Add IPv4 Pool



Name*
ftdvpn-aaa-cert-pool

Description

IPv4 Address Range*
172.16.1.40-172.16.1.50

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask*
255.255.255.0

Allow Overrides

i Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

► Override (0)

Cancel

Save

IPv4地址池的详细信息

第六步：添加连接配置文件的组策略

点击组策略项旁边的+按钮。

Group Policy:

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.

Group Policy:* +

[Edit Group Policy](#)

Cancel

Back

Next

添加组策略

输入必要信息以添加新的组策略。选择连接配置文件的新组策略。

- 名称：ftdvpn-aaa-cert-grp

- VPN协议 : SSL

Add Group Policy



Name:*
ftdvpn-aaa-cert-grp

Description:

General Secure Client Advanced

VPN Protocols

- IP Address Pools
- Banner
- DNS/WINS
- Split Tunneling

VPN Tunnel Protocol:
Specify the VPN tunnel types that user can use. At least one tunneling mode must be configured for users to connect over a VPN tunnel.

SSL

IPsec-IKEv2

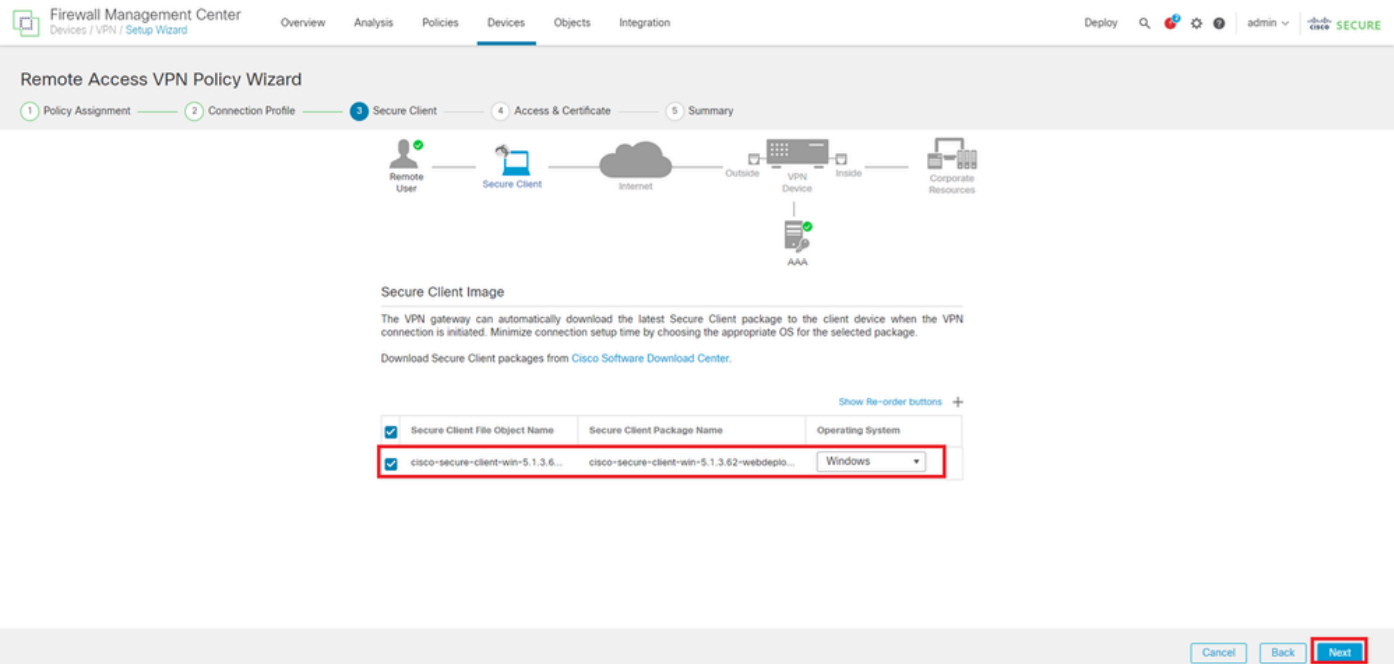
Cancel

Save

组策略详细信息

步骤 7.为连接配置文件配置安全客户端映像

选择secure client image file并单击Next按钮。



选择安全客户端镜像

步骤 8 连接配置文件的配置访问和证书

为VPN连接选择Security Zone，然后单击Certificate Enrollment项目旁边的+按钮。

- 接口组/安全区域：outsideZone



选择安全区域

输入FTD证书的必要信息，并从本地计算机导入PKCS12文件。

- 名称：ftdvpn-cert
- 注册类型：PKCS12文件

Add Cert Enrollment



Name*
ftdvpn-cert

Description

CA Information Certificate Parameters Key Revocation

Enrollment Type: PKCS12 File

PKCS12 File*: ftdCert.pfx [Browse PKCS12 File](#)

Passphrase*:

Validation Usage: IPsec Client SSL Client SSL Server
 Skip Check for CA flag in basic constraints of the CA Certificate

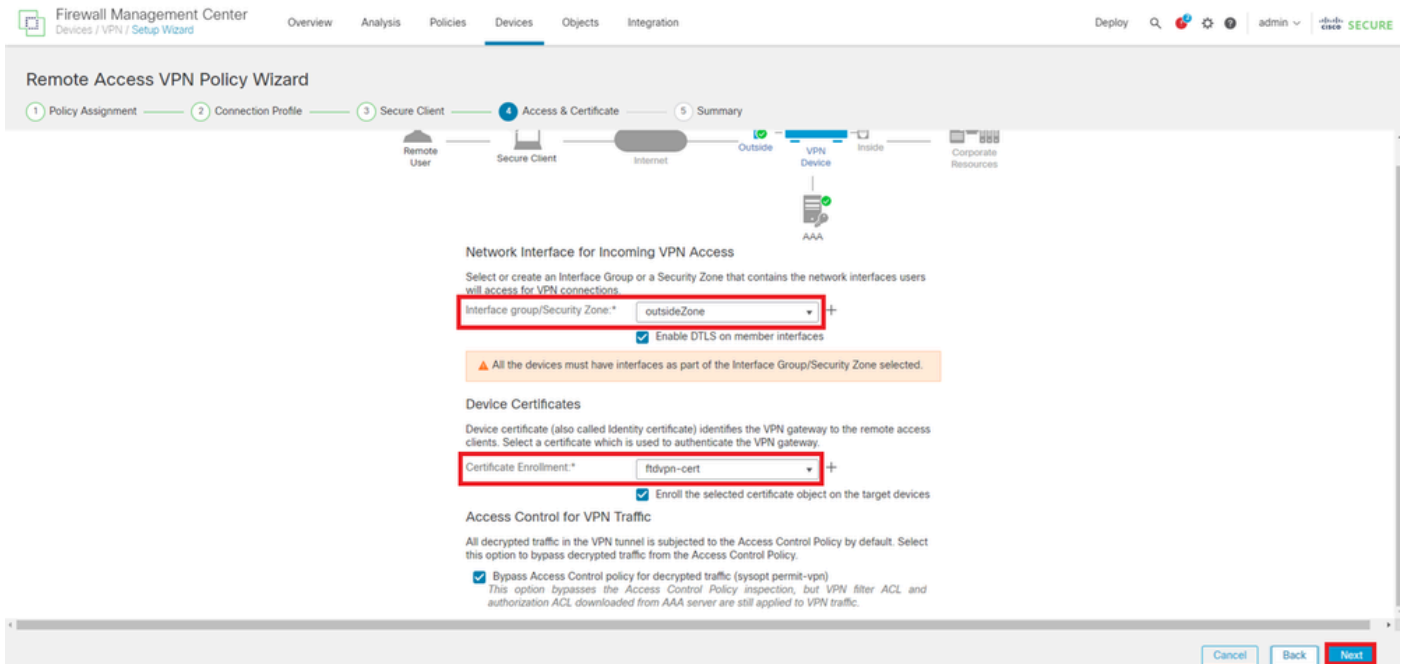
[Cancel](#) [Save](#)

添加FTD证书

确认在访问和证书向导中输入的信息，然后单击下一步按钮。



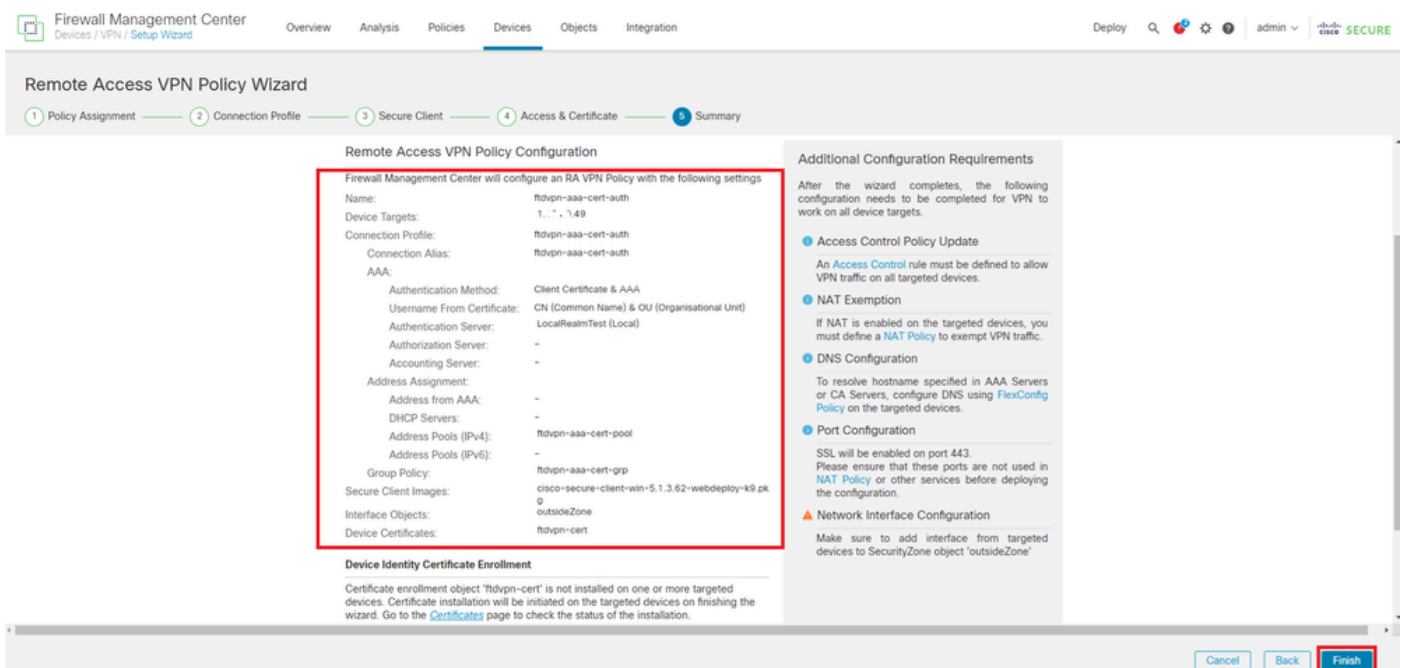
注意：启用解密流量的旁路访问控制策略(sysopt permit-vpn)，以使解密的VPN流量不会受到访问控制策略检查。



确认访问和证书中的设置

步骤 9 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。



确认VPN连接的设置

确认远程访问VPN策略的摘要并将设置部署到FTD。

Firewall Management Center
Devices / VPN / Edit Connection Profile

Overview Analysis Policies **Devices** Objects Integration

Deploy Search Settings Admin Cisco SECURE

ftdvpn-aaa-cert-auth

Enter Description

Policy Assignments (1)

Local Realm: LocalRealmTest Dynamic Access Policy: None

Connection Profile Access Interfaces Advanced

Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DefaultGrpPolicy
ftdvpn-aaa-cert-auth	Authentication: Client Certificate & LOCAL Authorization: None Accounting: None	ftdvpn-aaa-cert-grp

远程访问VPN策略摘要

在FTD CLI中确认

从FMC部署后，在FTD CLI中确认VPN连接设置。

```
// Defines IP of interface
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 192.168.1.200 255.255.255.0
interface GigabitEthernet0/1
nameif inside
security-level 0
ip address 192.168.10.200 255.255.255.0
```

```
// Defines a pool of addresses
ip local pool ftdvpn-aaa-cert-pool 172.16.1.40-172.16.1.50 mask 255.255.255.0
```

```
// Defines a local user
username sslVPNClientCN password ***** encrypted
```

```
// Defines Trustpoint for Server Certificate
crypto ca trustpoint ftdvpn-cert
keypair ftdvpn-cert
cr1 configure
```

```
// Server Certificate Chain
crypto ca certificate chain ftdvpn-cert
certificate 22413df584b6726c
3082037c 30820264 a0030201 02020822 413df584 b6726c30 0d06092a 864886f7
.....
quit
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:/csm/cisco-secure-client-win-5.1.3.62-webdeploy-k9.pkg 1 regex "Windows"
anyconnect enable
tunnel-group-list enable
cache
disable
error-recovery disable

// Bypass Access Control policy for decrypted traffic
// This setting is displayed in the 'show run all' command output
sysopt connection permit-vpn

// Configures the group-policy to allow SSL connections
group-policy ftdvpn-aaa-cert-grp internal
group-policy ftdvpn-aaa-cert-grp attributes
banner none
wins-server none
dns-server none
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-tunnel-network-list none
default-domain none
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
vlan none
address-pools none
webvpn
anyconnect ssl dtls enable
anyconnect mtu 1406
anyconnect firewall-rule client-interface public none
anyconnect firewall-rule client-interface private none
anyconnect ssl keepalive 20
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client 30
anyconnect dpd-interval gateway 30
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules value none
anyconnect ask none default anyconnect
anyconnect ssl df-bit-ignore disable

// Configures the tunnel-group to use the aaa & certificate authentication
tunnel-group ftdvpn-aaa-cert-auth type remote-access
tunnel-group ftdvpn-aaa-cert-auth general-attributes
address-pool ftdvpn-aaa-cert-pool
default-group-policy ftdvpn-aaa-cert-grp
// These settings are displayed in the 'show run all' command output. Start
authentication-server-group LOCAL
secondary-authentication-server-group none
```

```
no accounting-server-group
default-group-policy ftdvpn-aaa-cert-grp
username-from-certificate CN OU
secondary-username-from-certificate CN OU
authentication-attr-from-server primary
authenticated-session-username primary
username-from-certificate-choice second-certificate
secondary-username-from-certificate-choice second-certificate
// These settings are displayed in the 'show run all' command output. End
tunnel-group ftdvpn-aaa-cert-auth webvpn-attributes
authentication aaa certificate
pre-fill-username client
group-alias ftdvpn-aaa-cert-auth enable
```

在VPN客户端中确认

步骤1:确认客户端证书

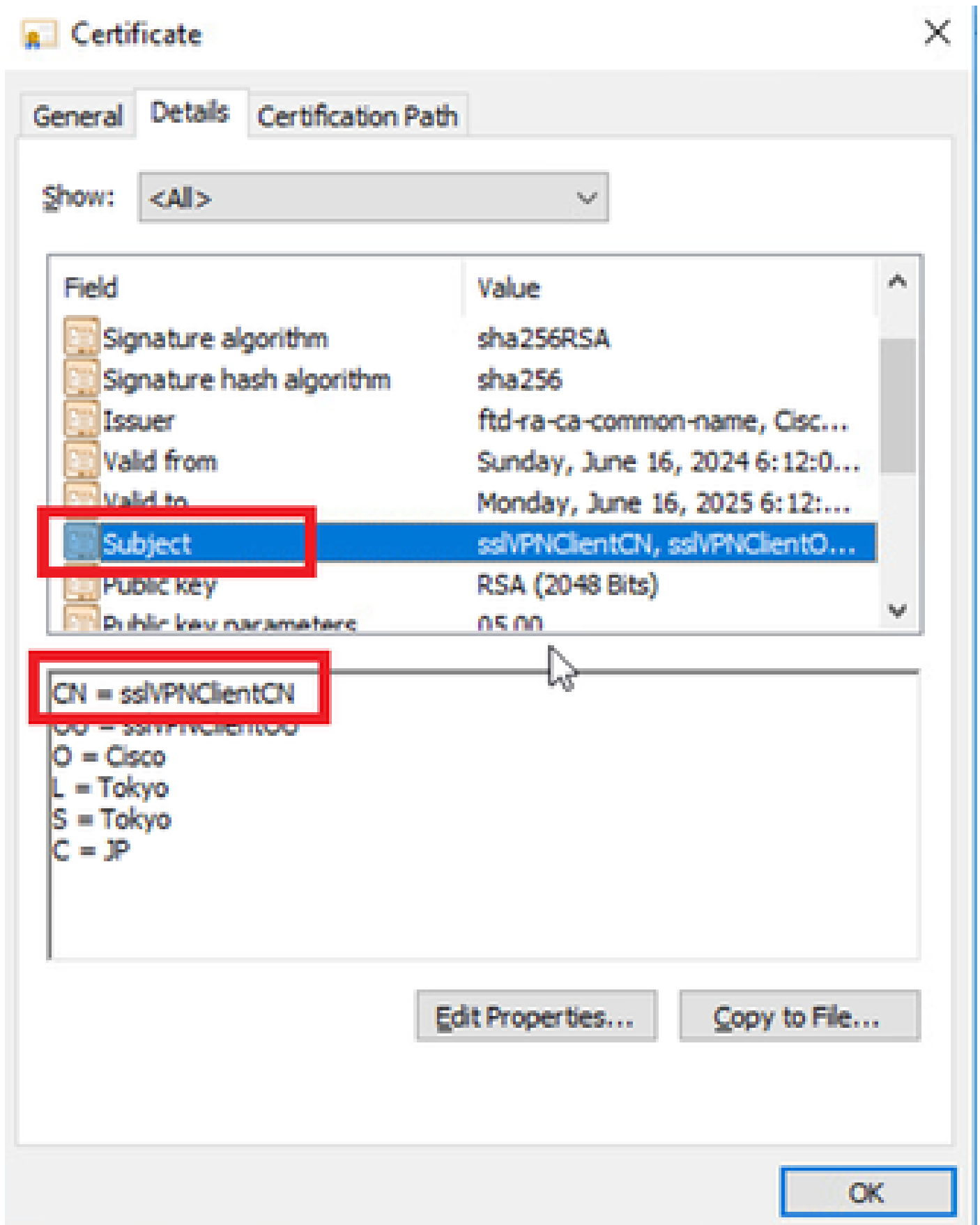
导航到证书-当前用户>个人>证书，检查用于身份验证的客户端证书。



确认客户端证书

双击客户端证书，导航到详细信息，检查主题的详细信息。

- 主题 : CN = ssIVPNClientCN

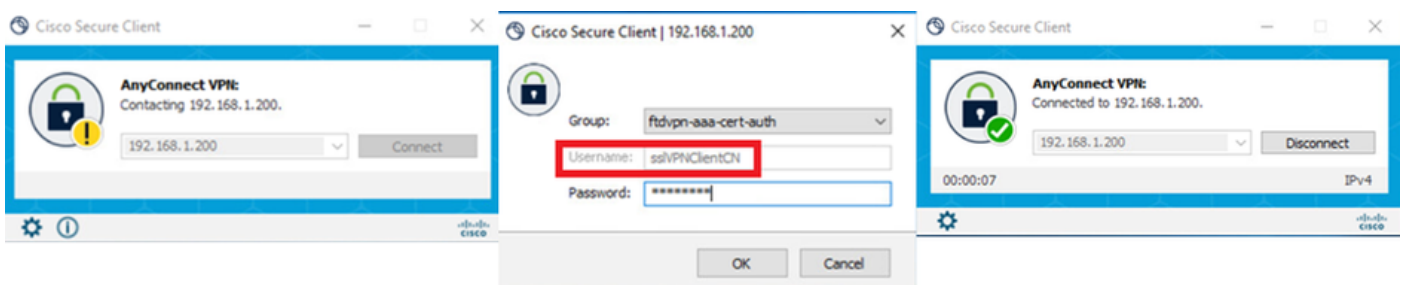


客户端证书的详细信息

第二步：确认CA

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。

注意：用户名提取自本文档中客户端证书的CN（公用名）字段。



启动VPN连接

第二步：确认FMC中的活动会话

导航到分析>用户>活动会话，检查VPN身份验证的活动会话。

Session ID	Login Time	RealName	Last Step	Authentication Type	Current IP	Real IP	Username	First Name	Last Name	Email	Department	Phone Number	Discovery Application	Device
	2024-06-17 11:38:22	LocalRealmTestsslVPNClientCN	2024-06-17 11:38:22	VPN Authentication	172.16.1.40	LocalRealmTest	sslVPNClientCN						LDAP	1.149

确认活动会话

第三步：在FTD CLI中确认VPN会话

在FTD (Lina) CLI中运行show vpn-sessiondb detail anyconnect命令以确认VPN会话。

```
ftd702# show vpn-sessiondb detail anyconnect
```

Session Type: AnyConnect Detailed

```
Username : sslVPNClientCN Index : 7
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 14780 Bytes Rx : 15386
Pkts Tx : 2 Pkts Rx : 37
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : ftdvpn-aaa-cert-grp Tunnel Group : ftdvpn-aaa-cert-auth
Login Time : 02:38:22 UTC Mon Jun 17 2024
Duration : 0h:01m:22s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb00718200007000666fa19e
Security Grp : none Tunnel Zone : 0
```

```
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

```
AnyConnect-Parent:
Tunnel ID : 7.1
Public IP : 192.168.1.11
Encryption : none Hashing : none
TCP Src Port : 50035 TCP Dst Port : 443
Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : win
Client OS Ver: 10.0.15063
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7390 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

```
SSL-Tunnel:
Tunnel ID : 7.2
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-128 Hashing : SHA256
```

Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 50042
TCP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 7390 Bytes Rx : 2292
Pkts Tx : 1 Pkts Rx : 3
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:

Tunnel ID : 7.3
Assigned IP : 172.16.1.40 Public IP : 192.168.1.11
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 56382
UDP Dst Port : 443 Auth Mode : Certificate and userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.3.62
Bytes Tx : 0 Bytes Rx : 13094
Pkts Tx : 0 Pkts Rx : 34
Pkts Tx Drop : 0 Pkts Rx Drop : 0

第四步：确认与服务器的通信

从VPN客户端向服务器发出ping命令，确认VPN客户端与服务器的通信成功。

```
C:\Users\CALO>ping 192.168.10.11

Pinging 192.168.10.11 with 32 bytes of data:
Reply from 192.168.10.11: bytes=32 time=12ms TTL=128
Reply from 192.168.10.11: bytes=32 time=87ms TTL=128
Reply from 192.168.10.11: bytes=32 time=3ms TTL=128
Reply from 192.168.10.11: bytes=32 time=3ms TTL=128

Ping statistics for 192.168.10.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 87ms, Average = 26ms
```

Ping成功

在FTD (Lina) CLI中运行capture in interface inside real-time命令以确认数据包捕获。

<#root>

ftd702#

capture in interface inside real-time

Use ctrl-c to terminate real-time capture

```
1: 03:39:25.729881 172.16.1.40 > 192.168.10.11 icmp: echo request
2: 03:39:25.730766 192.168.10.11 > 172.16.1.40 icmp: echo reply
3: 03:39:26.816211 172.16.1.40 > 192.168.10.11 icmp: echo request
4: 03:39:26.818683 192.168.10.11 > 172.16.1.40 icmp: echo reply
5: 03:39:27.791676 172.16.1.40 > 192.168.10.11 icmp: echo request
6: 03:39:27.792195 192.168.10.11 > 172.16.1.40 icmp: echo reply
7: 03:39:28.807789 172.16.1.40 > 192.168.10.11 icmp: echo request
8: 03:39:28.808399 192.168.10.11 > 172.16.1.40 icmp: echo reply
```

故障排除

您可以在Lina引擎的调试系统日志和Windows PC上的DART文件中找到有关VPN身份验证的信息。

这是Lina引擎中的调试日志示例。

```
// Certificate Authentication
```

```
Jun 17 2024 02:38:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 6EC79930B231EDAF, subject name: CN=sslV
```

```
Jun 17 2024 02:38:03: %FTD-6-717028: Certificate chain was successfully validated with warning, revocation status was not checked.
```

```
Jun 17 2024 02:38:03: %FTD-6-717022: Certificate was successfully validated. serial number: 6EC79930B231EDAF, subject name: CN=sslVPNClientC
```

```
// Extract username from the CN (Common Name) field
```

```
Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has been requested. [Request 5]
```

```
Jun 17 2024 02:38:03: %FTD-7-113028: Extraction of username from VPN client certificate has completed. [Request 5]
```

```
// AAA Authentication
```

```
Jun 17 2024 02:38:22: %FTD-6-113012: AAA user authentication Successful : local database : user = sslVPNClientCN
```

```
Jun 17 2024 02:38:22: %FTD-6-113009: AAA retrieved default group policy (ftdvpn-aaa-cert-grp) for user = sslVPNClientCN
```

```
Jun 17 2024 02:38:22: %FTD-6-113008: AAA transaction status ACCEPT : user = sslVPNClientCN
```

这些调试可以从FTD的诊断CLI运行，CLI提供可用于对配置进行故障排除的信息。

- debug crypto ca 14
- debug webvpn anyconnect 255
- debug crypto ike-common 255

参考

[在FTD上配置AnyConnect远程访问VPN](#)

[为移动访问配置基于Anyconnect证书的身份验证](#)

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）。