

FDMで管理されるFTDでのAAA認証を使用したIPv6対応RAVPNの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[FDMでの構成](#)

[ISEでの設定](#)

[確認](#)

[トラブルシュート](#)

[関連情報](#)

はじめに

このドキュメントでは、FDMによって管理されるFTDでAAA認証を使用してIPv6対応リモートアクセスVPNを設定する手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Firepower Device Manager(FDM)仮想
- Cisco Secure Firewall Threat Defense(FTD)仮想
- VPN認証のフロー

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure FDM仮想7.6.0
- Cisco Secure FTD仮想7.6.0
- Cisco Secureクライアント5.1.6.103

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

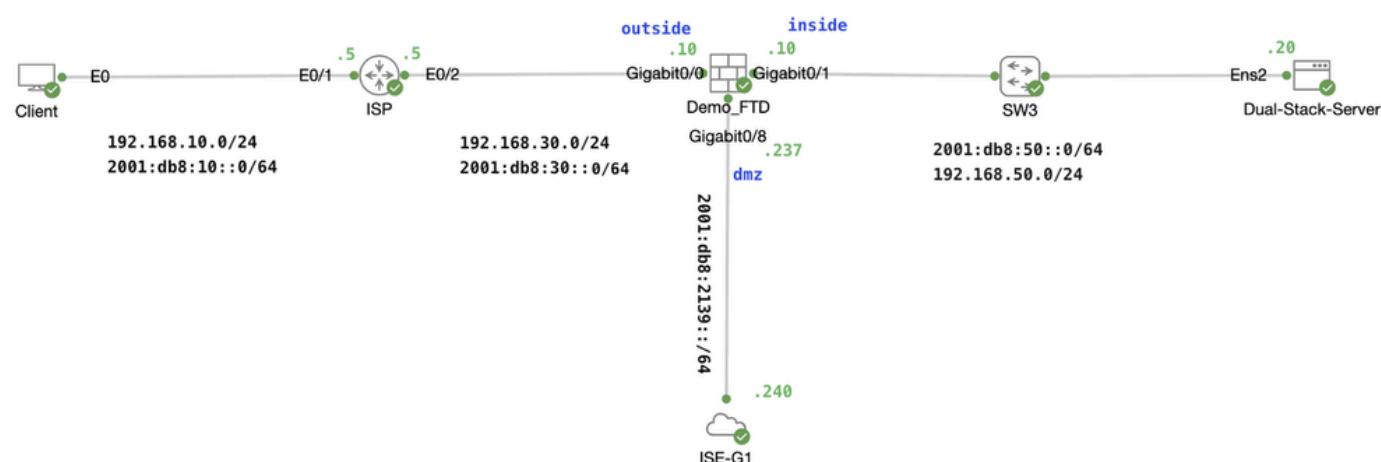
背景説明

IPv4アドレスは限られており、ほとんど使い果たされてきているため、世界がIPv4からIPv6へ移行するにつれ、IPv6リモートアクセスVPN(RAVPN)の重要性がますます高まっています。一方で、IPv6では、インターネットに接続するデバイスの増加に対応できる実質的に無制限のアドレス空間を提供しています。より多くのネットワークやサービスがIPv6に移行する中、IPv6機能を使用することで、ネットワークの互換性とアクセス性を維持できます。IPv6 RAVPNは、組織がネットワークの将来に備え、安全でスケーラブルなリモート接続を確保するのに役立ちます。

この例では、クライアントはサービスプロバイダーから提供されたIPv6アドレスを使用してVPNゲートウェイと通信しますが、認証IDソースとしてCisco Identity Service Engine(ISE)を使用して、VPNプールからIPv4アドレスとIPv6アドレスの両方を受信します。ISEはIPv6アドレスのみで設定されます。内部サーバは、デュアルスタックホストを表すIPv4アドレスとIPv6アドレスの両方で設定されます。クライアントは、必要に応じてIPv4またはIPv6 VPNアドレスを使用して内部リソースにアクセスできます。

設定

ネットワーク図



トポロジ

FDMでの構成

ステップ 1：ノード間のIPv4およびIPv6相互接続の事前設定が正常に完了していることを確認することが不可欠です。クライアントとFTDのゲートウェイは、関連するISPアドレスです。サーバのゲートウェイはFTDのIP内部にあります。ISEはFTDのDMZエリアにあります。

Firewall Device Manager

Monitoring Policies Objects **Device: ftdv760**

Device Summary
Interfaces

Cisco Secure Firewall Threat Defense for KVM

0/0 0/1 0/2 0/3 0/4 0/5 0/6 0/7 0/8

MONITOR

CONSOLE

Interfaces Virtual Tunnel Interfaces

10 Interfaces

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> ✓ GigabitEthernet0	outside	ON	Routed	192.168.30.10 2001:db8:30::10/64		Enabled	
> ✓ GigabitEthernet1	inside	ON	Routed	192.168.50.10 2001:db8:50::10/64		Enabled	
> ○ GigabitEthernet2		OFF	Routed			Enabled	
> ○ GigabitEthernet3		OFF	Routed			Enabled	
> ○ GigabitEthernet4		OFF	Routed			Enabled	
> ○ GigabitEthernet5		OFF	Routed			Enabled	
> ○ GigabitEthernet6		OFF	Routed			Enabled	
> ○ GigabitEthernet7		OFF	Routed			Enabled	
> ✓ GigabitEthernet8	dmz	ON	Routed	2001:db8:2139::237/64		Enabled	

FTD_インターフェイス_IP

Firewall Device Manager

Monitoring Policies Objects **Device: ftdv760**

Device Summary
Routing

Add Multiple Virtual Routers

Static Routing BGP OSPF EIGRP ECMP Traffic Zones

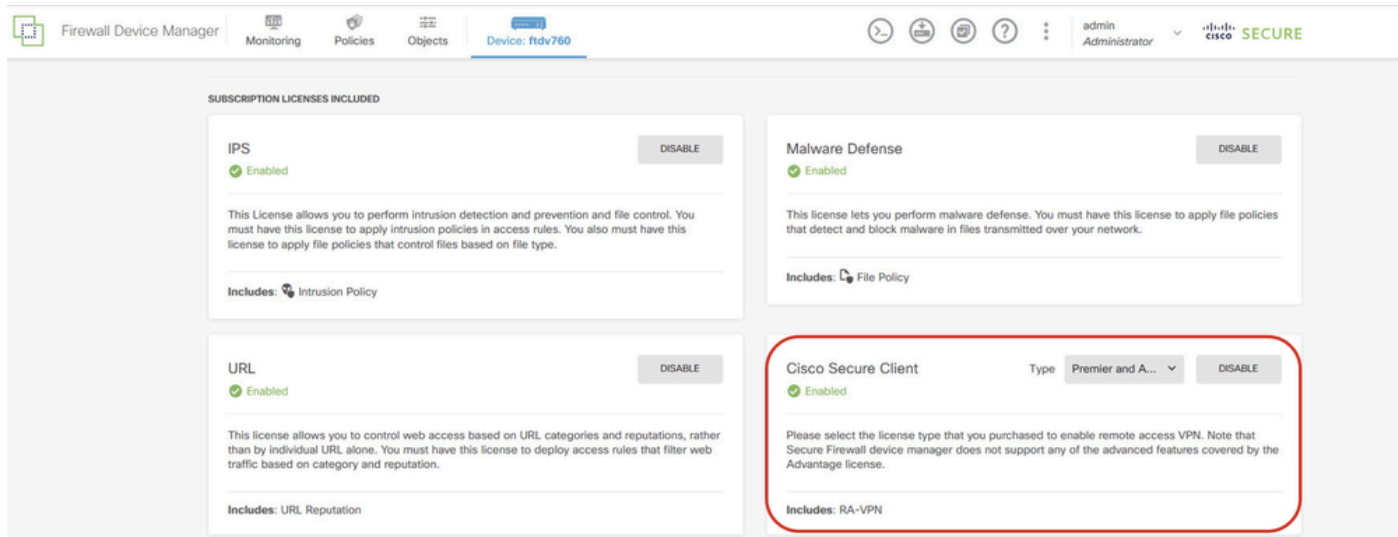
2 routes

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	TotSP_v4	outside	IPv4	0.0.0.0/0	192.168.30.5		1	
2	TotSP_v6	outside	IPv6	::/0	2001:db8:30::5		1	

FTD_Default_Route (デフォルトルート)

ステップ 2 : [Cisco Software Download](#)からCisco Secure Clientパッケージnamecisco-secure-client-win-5.1.6.103-webdeploy-k9.pkgをダウンロードし、ダウンロード後にダウンロードしたファイルのmd5チェックサムがCisco Software Download (登録ユーザ専用) ページと同じであることを確認して、ファイルが良好であることを確認します。

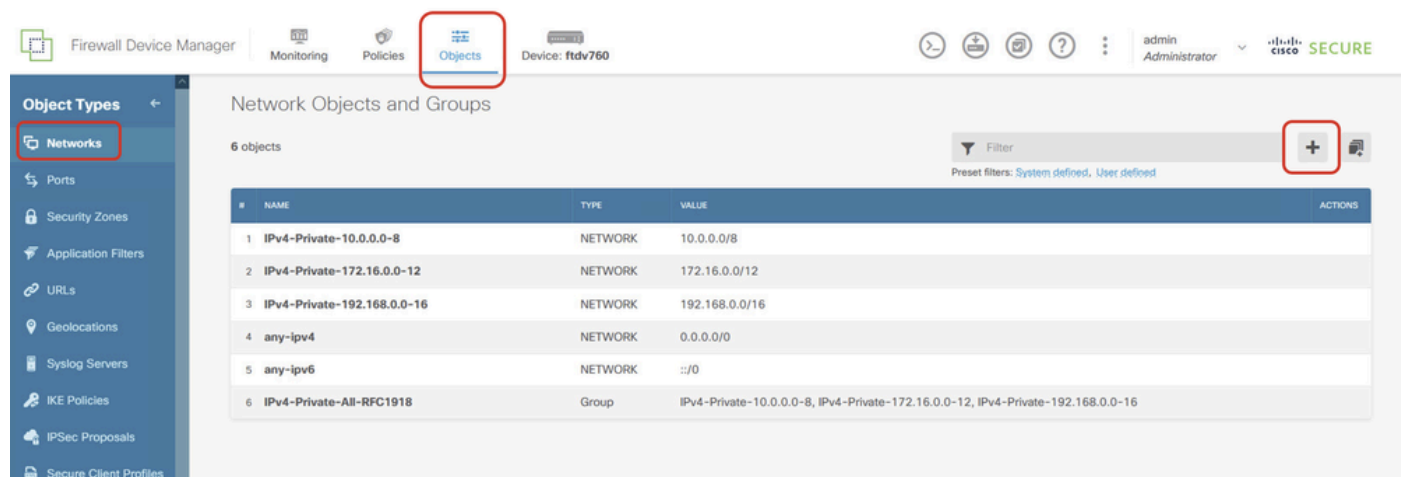
ステップ 3 : RAVPN関連ライセンスがFTDで有効になっていることを確認します。



FDM_ライセンス

ステップ 4：VPNアドレスプールを作成します。

ステップ 4.1： ネットワークオブジェクトを作成して、IPv6およびIPv4アドレスプールを作成します。 Objects > Networksの順に移動し、+ボタンをクリックします。



作成_VPN_アドレス_プール_1

ステップ 4.2： 各ネットワークオブジェクトに必要な情報を提供します。OKボタンをクリックします。

IPv4プールの場合は、[ネットワーク]または[範囲]でオブジェクトタイプを選択できます。この例では、デモ用にオブジェクトタイプとしてNetworkが選択されています。

- 名前： demo_ipvp4pool
- タイプ： ネットワーク
- ネットワーク： 10.37.254.16/30

Add Network Object



Name

demo_ipv4pool

Description

Type



Network



Host



FQDN



Range

Network

10.37.254.16/30

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

作成_VPN_アドレス_プール_2_IPv4

IPv6プールの場合は、現時点ではNetworkでのみオブジェクトタイプを選択できます。

- 名前 : demo_ipv6pool
- タイプ : ネットワーク
- ネットワーク : 2001:db8:1234:1234::/124

Add Network Object



Name

demo_ipv6pool

Description

Type



Network



Host



FQDN



Range

Network

2001:db8:1234:1234::/124

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

OK

作成_VPN_アドレスプール_2_IPv6

ステップ 5 : NAT免除の内部ネットワークを作成します。

ステップ 5.1 : Objects > Networksに移動し、+ボタンをクリックします。

Firewall Device Manager

Monitoring Policies **Objects** Device: ftdv760

Object Types

Networks

Ports

Security Zones

Application Filters

URLs

Geolocations

Syslog Servers

IKE Policies

IPSec Proposals

Secure Client Profiles

Network Objects and Groups

6 objects

Filter

Preset filters: System defined, User defined

#	NAME	TYPE	VALUE	ACTIONS
1	IPv4-Private-10.0.0.0-8	NETWORK	10.0.0.0/8	
2	IPv4-Private-172.16.0.0-12	NETWORK	172.16.0.0/12	
3	IPv4-Private-192.168.0.0-16	NETWORK	192.168.0.0/16	
4	any-ipv4	NETWORK	0.0.0.0/0	
5	any-ipv6	NETWORK	::/0	
6	IPv4-Private-All-RFC1918	Group	IPv4-Private-10.0.0.0-8, IPv4-Private-172.16.0.0-12, IPv4-Private-192.168.0.0-16	

ステップ 5.2： 各ネットワークオブジェクトに必要な情報を提供します。[OK] ボタンをクリックします。

この例では、IPv4とIPv6の両方のネットワークが設定されています。

- 名前： inside_net_ipv4
- タイプ： ネットワーク
- ネットワーク： 192.168.50.0/24

Add Network Object

Name

inside_net_ipv4

Description

Type

☒ Network ☐ Host ☐ FQDN ☐ Range

Network

192.168.50.0/24

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL OK

- 名前： inside_net_ipv6
- タイプ： ネットワーク
- ネットワーク： 2001:db8:50::/64

Add Network Object



Name

inside_net_ipv6

Description

Type



Network



Host



FQDN



Range

Network

2001:db8:50::/64

e.g. 192.168.2.0/24 or 2001:DB8:0:CD30::/60

CANCEL

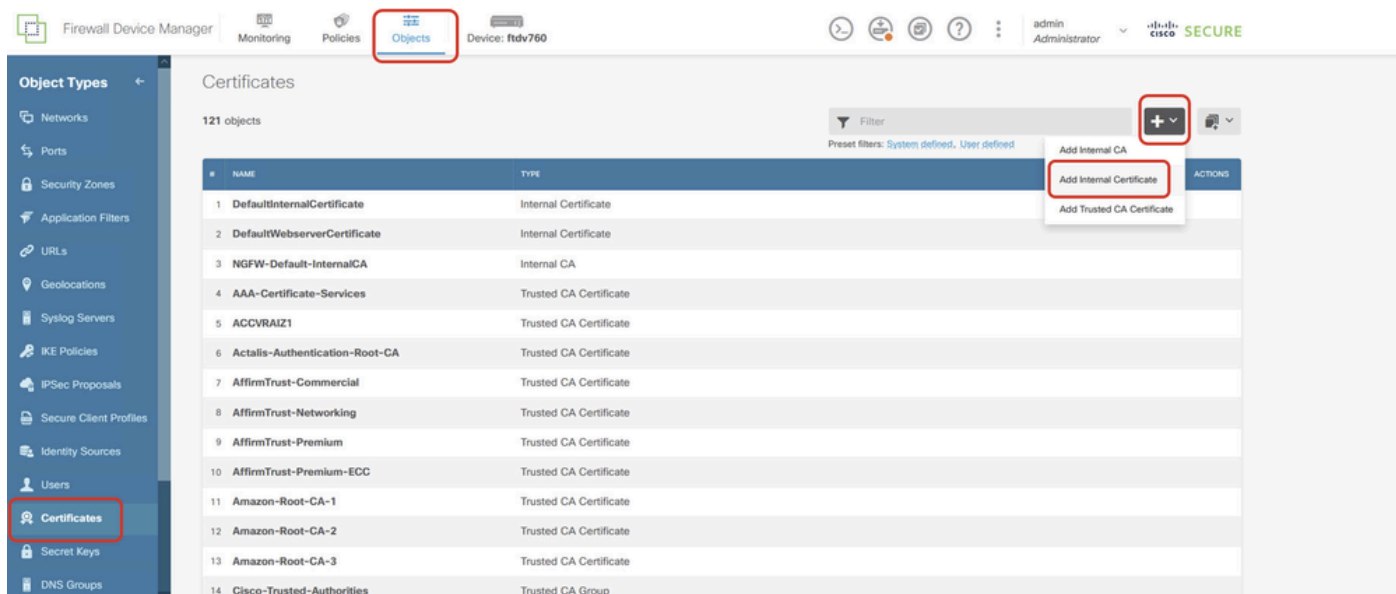
OK

作成_NAT_免除_ネットワーク_2_IPv6

手順 6 : RAVPNに使用する証明書を作成します。2つのオプションがあります。サードパーティの認証局(CA)によって署名された証明書をアップロードするか、新しい自己署名証明書を生成します。

この例では、デモ用にカスタマイズされた証明書の内容とともに、新しい自己署名証明書が使用されます。

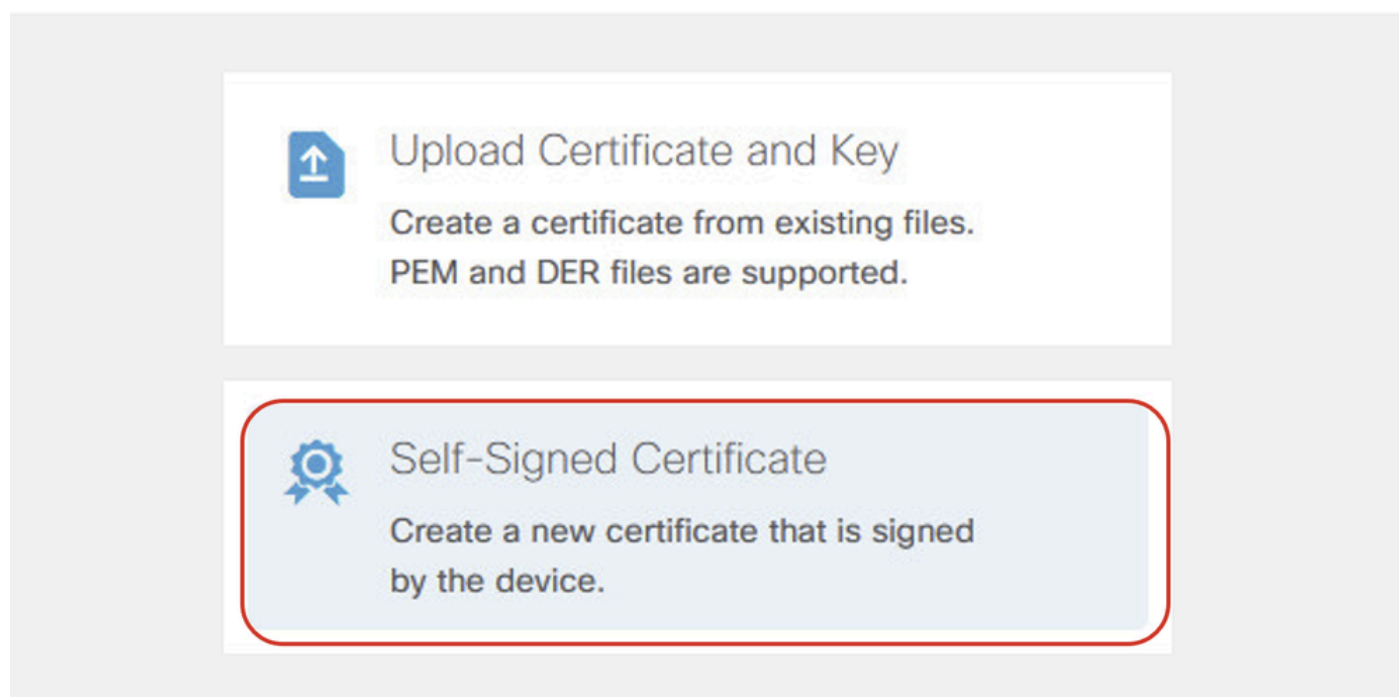
ステップ 6.1 : Objects > Certificatesの順に移動します。+ボタンをクリックして、Add Internal Certificateを選択します。



作成_証明書_1

ステップ 6.2 : Self-Signed Certificateをクリックします。

Choose the type of internal certificate you want to create



ステップ 6.3 : Generalタブをクリックして、必要な情報を入力します。

名前 : demovpn

キーの種類 : RSA

キーサイズ：2048

有効期間：デフォルト

有効期限日：デフォルト

特別なサービスの検証の使用：SSLサーバー

Add Internal Certificate

Search for attribute

General

Issuer

Subject

Name

demovpn

Key Type

RSA

Key Size

2048

Validity Period

By Date

By Number of Days

Expiration Date

(UTC+08:00) Asia/Hong_Kong

02/15/2027

Set default

Default: 02/15/2027 (calculated based on 825 days according to [Apple requirements](#))

Validation Usage for Special Services

SSL Server

CANCEL

SAVE

作成_証明書_3

ステップ 6.4：Issuerタブをクリックして、必要な情報を入力します。

国：米国

一般名：vpn.example.com

Add Internal Certificate

?

×

Q Search for attribute

General

Issuer

Subject

Country

United States (US)

State or Province

Locality or City

Organization

Organizational Unit (Department)

Common Name

vpn.example.com

You must specify a Common Name to use the certificate with remote access VPN.

CANCEL

SAVE

作成_証明書_4

ステップ 6.5 : Subjectタブをクリックして、必要な情報を入力してから、SAVEをクリックします。

国 : 米国

一般名 : vpn.example.com

Add Internal Certificate

?

×

Q Search for attribute

General

Issuer

Subject

Distinguished Name

Country

United States (US)

▼

State or Province

Locality or City

Organization

Organizational Unit (Department)

Common Name

vpn.example.com

You must specify a Common Name to use the certificate with remote access VPN.

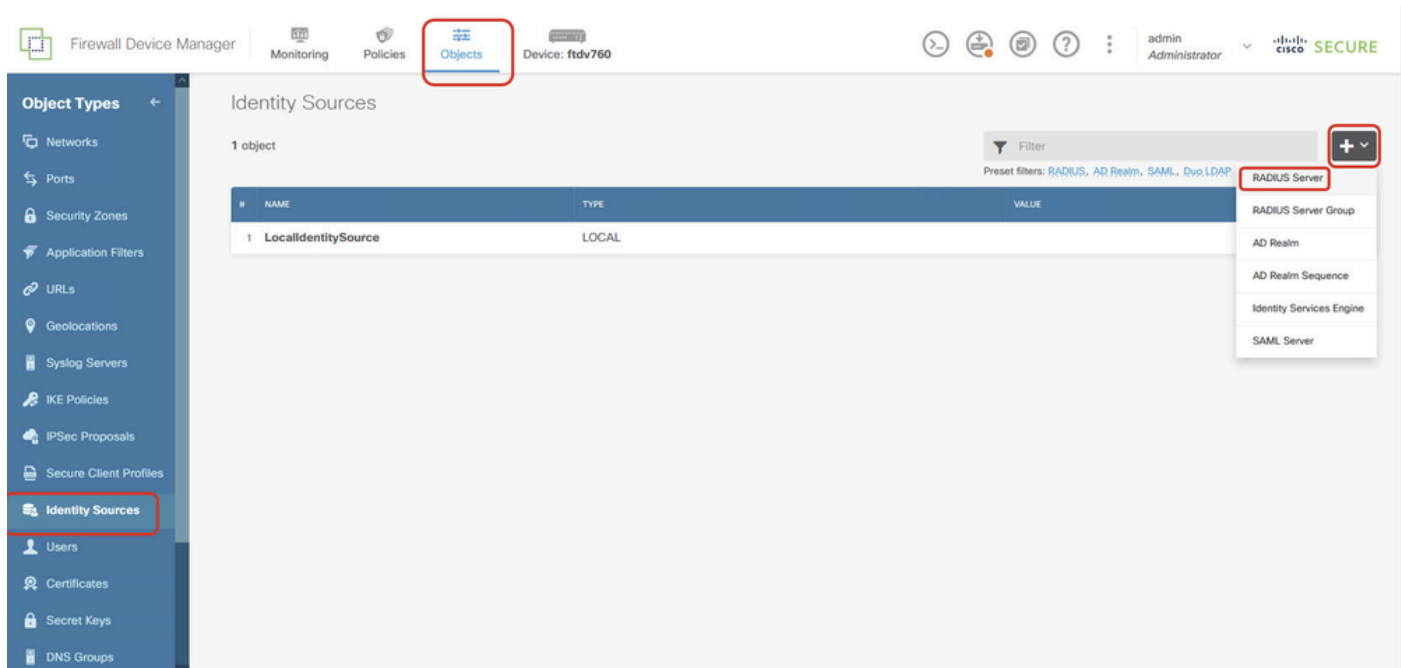
CANCEL

SAVE

作成_証明書_5

手順 7 : RADIUSサーバのIDソースを作成します。

ステップ 7.1 : Objects > Identity Sourcesの順に移動し、+ボタンをクリックして、RADIUS Serverを選択します。



作成_半径_ソース_1

ステップ 7.2 : RADIUSサーバに関する必要な情報を提供します。OKボタンをクリックします。

名前 : demo_ise

サーバ名またはIPアドレス : 2001:db8:2139::240

認証ポート : 1812 (デフォルト)

タイムアウト : 10 (デフォルト)

サーバシークレットキー : cisco

Radiusサーバへの接続に使用するインターフェイス : インターフェイスを手動で選択します。この例では、dmz(GigabitEthernet0/8)を選択します。

Add RADIUS Server



Name

demo_ise

Server Name or IP Address

2001:db8:2139::240

Authentication Port

1812

Timeout

10

seconds

1-60

Server Secret Key

●●●●●●●●



RA VPN Only (if this object is used in RA VPN Configuration)

Redirect ACL

Please select



Interface used to connect to Radius server



Resolve via route lookup



Manually choose interface

dmz (GigabitEthernet0/8)

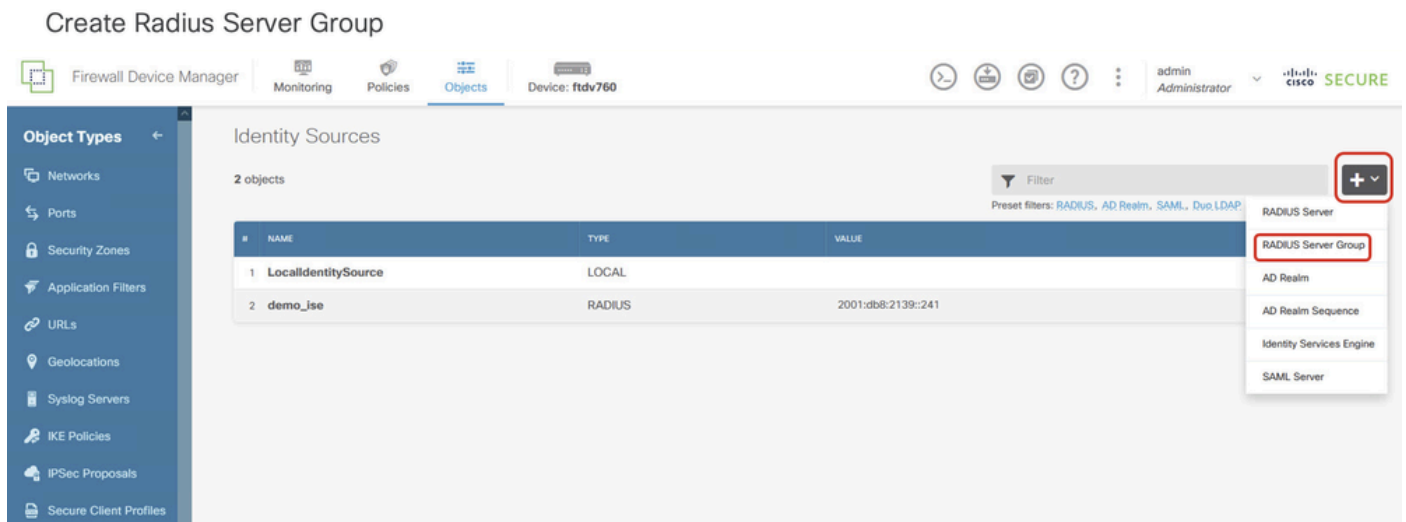


CANCEL

OK

作成_半径_ソース_2

ステップ 7.3 : Objects > Identity Sourcesの順に移動します。+ボタンをクリックして、RADIUS Server Groupを選択します。



作成_半径_ソース_3

ステップ 7.4 : RADIUSサーバグループに関する必要な情報を提供します。[OK] ボタンをクリックします。

名前 : demo_ise_group

Dead Time (デッドタイム) :10 (デフォルト)

最大試行回数 : 3 (デフォルト)

RADIUSサーバ : +ボタンをクリックし、ステップ6.2で作成した名前を選択します。この例では、demo_iseです。

Add RADIUS Server Group



Name

demo_ise_group

Dead Time

10

minutes

0-1440

Maximum Failed Attempts

3

1-5

☐ Dynamic Authorization (for RA VPN only)

Port

1700

1024-65535

Realm that Supports the RADIUS Server

Please select



RADIUS Server

The servers in the group should be backups of each other



Filter



demo_ise



CANCEL

OK

Create new RADIUS Server

CANCEL

OK

ステップ 8 : RAVPNに使用するグループポリシーを作成します。この例では、カスタマイズされたバナーとタイムアウト設定がデモ用に設定されています。実際の要件に基づいて変更できます。

ステップ 8.1 : Remote Access VPN > View Configurationの順に移動します。左側のサイドバーで Group Policiesをクリックし、+ボタンをクリックします。



作成_グループポリシー_1

ステップ 8.2 : Generalをクリックして、必要な情報を入力します。

名前 : demo_gp

認証されたクライアント用のバナーテキスト : デモバナー

The screenshot shows the 'Add Group Policy' dialog box. The 'General' tab is selected. The 'Name' field contains 'demo_gp'. The 'Description' field is empty. The 'DNS Server' dropdown is set to 'Select DNS Group'. The 'Banner Text for Authenticated Clients' field contains 'demo banner|'. The 'Default domain' field is empty. The 'Secure Client profiles' field is empty. The 'OK' button is highlighted.

作成_グループ_ポリシー_2

ステップ 8.3 : Secure Clientをクリックして、必要な情報を指定します。

Enable Datagram Transport Layer Security(DTLS)にチェックマークを付けます。

Search for attribute

Basic

- General
- Session Settings

Advanced

- Address Assignment
- Split Tunneling
- Secure Client**
- Traffic Filters
- Windows Browser Proxy

SSL SETTINGS

- ☒ Enable Datagram Transport Layer Security (DTLS)
- ☐ DTLS Compression
- SSL Compression: Disabled
- SSL Rekey Method: None
- SSL Rekey Interval: 4 minutes (4 ~ 10080)

CONNECTION SETTINGS

- ☐ Ignore the DF (Don't Fragment) bit
- ☐ Client Bypass Protocol
- MTU: 1500

CANCEL OK

作成_グループ_ポリシー_3

Secure ClientとVPN Gatewayの間のキープアライブメッセージを確認します (デフォルト値)。

Gateway Side Interval(Default value)のDPDをチェックします。

DPD on Client Side Interval (Default value)にチェックマークを付けます。

Search for attribute

Basic

General

Session Settings

Advanced

Address Assignment

Split Tunneling

Secure Client

Traffic Filters

Windows Browser Proxy

☐ Ignore the DF (Don't Fragment) bit

☐ Client Bypass Protocol

MTU

1406 bytes

576 - 1462

☒ Keepalive Messages Between Secure Client and VPN Gateway

20 seconds

15 - 600; (Default: 20)

☒ DPD on Gateway Side Interval ⓘ

30 seconds

5 - 3600

☒ DPD on Client Side Interval

30 seconds

5 - 3600

CANCEL OK

作成_グループ_ポリシー_3_続き

ステップ 9 : RAVPN接続プロファイルを作成します。

ステップ 9.1 : Remote Access VPN > View Configurationの順に移動します。左のサイドバーから Connection Profileをクリックし、+ボタンをクリックしてウィザードを開始します。

Config RAVPN Connection Profile

Firewall Device Manager Monitoring Policies Objects Device: ftdv760

RA VPN

Connection Profiles

Group Policies

SAML Server

Device Summary

Remote Access VPN Connection Profiles

Filter +

#	NAME	AAA	GROUP POLICY	ACTIONS
There are no Remote Access Connections yet. Start by creating the first Connection.				

CREATE CONNECTION PROFILE

作成_RAVPNウィザード_1

ステップ 9.2 : Connection and Client Configurationセクションで必要な情報を入力し、NEXTボタンをクリックします。

接続プロファイル名 : demo_ravpn

グループエイリアス : demo_ravpn

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

demo_ravpn

Group Alias (one per line, up to 5)

demo_ravpn

[Add Another Group Alias](#)

Group URL (one per line, up to 5)

[Add Another Group URL](#)

Create_RAVPN_Wizard_2_Conn_名前

Primary Identity Source > Authentication Type: AAA Only (プライマリIDソース>認証タイプ : AAAのみ)

Primary Identity Source > Primary Identity Source: demo_ise_group (ステップ7.4で設定した名前)

フォールバックローカルアイデンティティソース : LocalIdentitySource

認証サーバ : demo_ise_group (ステップ7.4で設定した名前)

アカウントिंगサーバ : demo_ise_group (ステップ7.4で設定した名前)

Primary Identity Source

Authentication Type

AAA Only



Primary Identity Source for User Authentication

demo_ise_group



Fallback Local Identity Source ⚠

LocalIdentitySource



⌵ Advanced

Secondary Identity Source

Secondary Identity Source for User Authentication

Please Select Identity Source



⌵ Advanced

Authorization Server

demo_ise_group



Accounting Server

demo_ise_group



Create_RAVPN_Wizard_2_アイデンティティ_ソース

IPv4アドレスプール : demo_ipv4pool (ステップ4.2で設定した名前)

IPv6アドレスプール : demo_ipv6pool (ステップ4.2で設定した名前)

Client Address Pool Assignment

IPv4 Address Pool

Endpoints are provided an address from this pool

+

demo_ipv4pool

IPv6 Address Pool

Endpoints are provided an address from this pool

+

demo_ipv6pool

DHCP Servers

+

CANCEL

NEXT

Create_RAVPN_Wizard_2_アドレスプール

ステップ 9.3 : ステップ8.2の「リモートユーザエクスペリエンス」セクションで設定したグループポリシーを選択し、NEXTボタンをクリックします。

Firewall Device Manager

Monitoring

Policies

Objects

Device: ftdv760

admin Administrator

SECURE

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

demo_gp

Policy Group Brief Details

DNS - BANNER

DNS Server

None

Banner Text for Authenticated Clients

demo banner - fdm

SESSION SETTINGS

Maximum Connection Time / Alert Interval

Unlimited / 1 Minutes

Idle Time / Alert Interval

30 / 1 Minutes

Simultaneous Login per User

3

BACK

NEXT

作成_RAVPNウィザード_3

ステップ 9.4 : Global Settingセクションで必要な情報を入力し、NEXTボタンをクリックします。

デバイスID証明書 : demovpn(ステップ6.3で設定した名前)

Outsideインターフェイス : outside

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

demovpn (Validation Usage: SSL Server) ▼

Outside Interface

outside (GigabitEthernet0/0) ▼

Fully-qualified Domain Name for the Outside Interface

e.g. ravpn.example.com

Port

443

e.g. 8080

作成_RAVPNウィザード_4

Access Control for VPN Traffic: Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)にチェックマークを入れます。

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)

作成_RAVPN_ウィザード_4_VPN_ACP

NAT Exempt : スライダをクリックしてEnabledの位置にします

内部インターフェイス : 内部

内部ネットワーク : inside_net_ipv4、inside_net_ipv6 (ステップ5.2で設定した名前)

NAT Exempt



Inside Interfaces

The interfaces through which remote access VPN users can connect to the internal networks



Inside Networks

The internal networks remote access VPN users are allowed to use. The IP versions of the internal networks and address pools must match, either IPv4, IPv6, or both.



作成_RAVPN_ウィザード_4_VPN_NATExempt

Secure Client Package:UPLOAD PACKAGEをクリックし、それに応じてパッケージをアップロードします。この例では、Windowsパッケージがアップロードされます。

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.

You must have the necessary secure client software license.

Packages



Windows: cisco-secure-client-win-5.1.6.103-webdeploy-k9.pkg

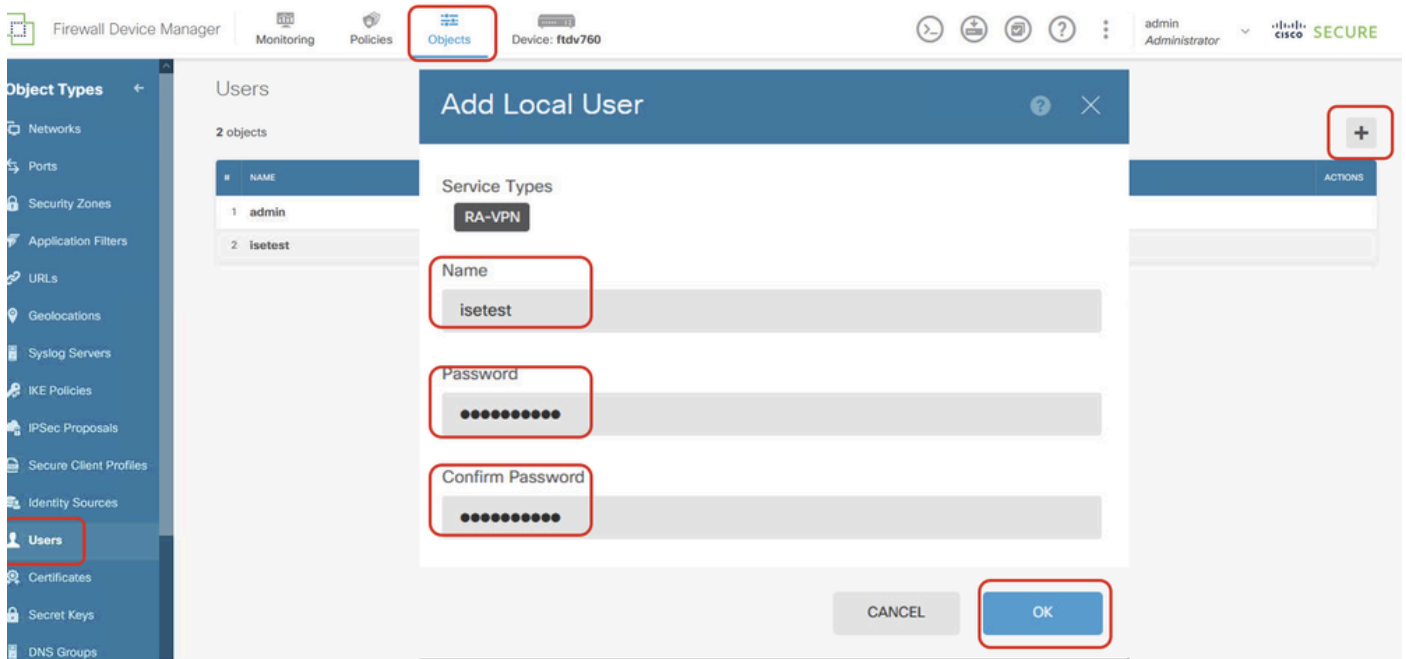
BACK

NEXT

Create_RAVPN_Wizard_4_イメージ

ステップ 9.5：概要を確認します。変更する必要がある場合は、BACKボタンをクリックします。問題がなければ、「FINISH」ボタンをクリックします。

ステップ 10：手順9.2でLocalIdentitySourcewithにFallback Local Identity Sourceを選択した場合は、ローカルユーザを作成します。ローカルユーザのパスワードは、ISEで設定されたものと同じである必要があります。



作成_ローカル_ユーザ

ステップ 11 設定変更を導入します。



配備_変更

ISEでの設定

ステップ 12 ネットワークデバイスを作成する。

ステップ 12.1 : Administration > Network Resources > Network Devicesの順に移動し、Addをクリックして、Name, IP Addressを指定し、ページを下にスクロールします。

Identity Services Engine Administration / Network Resources

Network Devices

Network Devices List > New Network Device

Network Devices

Name

Description

IP Address Subnet

作成_ネットワーク_デバイス

ステップ 12.2 : RADIUS Authentication Settingsのチェックボックスをオンにします。共有秘密を指定して、Submitをクリックします。

Identity Services Engine Administration / Network Resources

Network Devices

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

Shared Secret [Show](#)

☐ Use Second Shared Secret [?](#)

Second Shared Secret [Show](#)

CoA Port [Set To Default](#)

作成_ネットワーク_デバイス_続き

ステップ 13ネットワークアクセスユーザを作成します。[Administration] > [Identity Management] > [Identities] の順に移動します。Addをクリックして新しいユーザを作成します。フォールバックが機能していることを確認するため、パスワードは手順10で作成したFDMローカルユーザと同じです。

Identity Services Engine Administration / Identity Management

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Latest Manual Network Scan Results

Network Access Users

[Edit](#) [+ Add](#) [Change Status](#) [Import](#) [Export](#) [Delete](#) [Duplicate](#)

Status	Username	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/>	Enabled isetest						

作成_ISE_ユーザ

ステップ14: (オプション) カスタマイズした認証ルールと認可ルールを使用して新しいポリシーセットを作成します。この例では、デフォルトのポリシーセットがデモ用に使用されます。

Identity Services Engine

Policy / Policy Sets

Bookmarks

Dashboard

Context Visibility

Operations

Policy

Administration

Work Centers

Interactive Help

Policy Sets

Reset

Reset Policy Set Hit Counts

Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
+	Search						
✔	SPRT		Radius-NAS-IP-Address EQUALS 10.48.26.61	Default Network Access	0		
✔	Wired		DEVICE-Device Type EQUALS All Device Types#Switch	Default Network Access	0		
✔	Firewall No Posture		DEVICE-Device Type EQUALS All Device Types#Firewall_NoPosture	Default Network Access	0		
✔	Firewall Posture		DEVICE-Device Type EQUALS All Device Types#Firewall	Default Network Access	0		
✔	Default	Default policy set		Default Network Access	78		

Reset

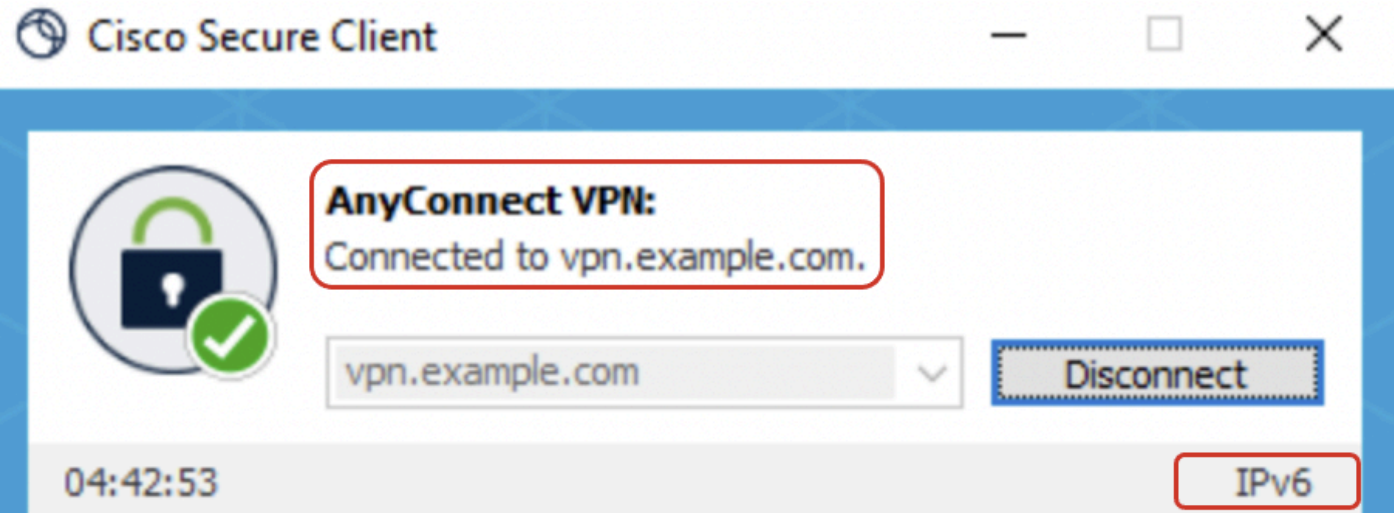
Save

ISE_Default_Policy_セット

確認

ここでは、設定が正常に機能しているかどうかを確認します。

ステップ 15 : クライアントのIPv6アドレスを使用してVPNゲートウェイを接続します。VPN接続に成功しました。



Verify_Connection_成功

ステップ 16 : SSHまたはコンソールを使用して、FTDのCLIに移動します。 FTD(Lina)CLIで show vpn-sessiondb detail anyconnectコマンドを実行して、VPNセッションの詳細を確認します。

<#root>

```
ftdv760# show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

Username : isetest

Index : 2

Assigned IP : 10.37.254.17

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

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 : 15402 Bytes Rx : 14883

Pkts Tx : 10 Pkts Rx : 78

Pkts Tx Drop : 0 Pkts Rx Drop : 10

Group Policy : demo_gp Tunnel Group : demo_ravpn

Login Time : 05:22:30 UTC Mon Dec 23 2024

Duration : 0h:05m:05s

Inactivity : 0h:00m:00s

VLAN Mapping : N/A VLAN : none

Audt Sess ID : c0a81e0a000020006768f396

Security Grp : none Tunnel Zone : 0

AnyConnect-Parent Tunnels: 1

SSL-Tunnel Tunnels: 1

DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 2.1

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Encryption : none Hashing : none

TCP Src Port : 58339 TCP Dst Port : 443

Auth Mode : userPassword

Idle Time Out: 30 Minutes Idle TO Left : 24 Minutes

Client OS : win

Client OS Ver: 10.0.19042

Client Type : AnyConnect

Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.6.103

Bytes Tx : 7421 Bytes Rx : 0

Pkts Tx : 1 Pkts Rx : 0

Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 2.2

Assigned IP : 10.37.254.17

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 58352
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 25 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.6.103
Bytes Tx : 7421 Bytes Rx : 152
Pkts Tx : 1 Pkts Rx : 2
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 2.3

Assigned IP : 10.37.254.17

Public IP : 2001:db8:10:0:a8a5:6647:b275:acc2

Assigned IPv6: 2001:db8:1234:1234::1

Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 58191
UDP Dst Port : 443 Auth Mode : 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 5.1.6.103
Bytes Tx : 560 Bytes Rx : 14731
Pkts Tx : 8 Pkts Rx : 76
Pkts Tx Drop : 0 Pkts Rx Drop : 10

ステップ 17: クライアントでpingテストを実行します。この例では、クライアントはサーバのIPv4アドレスとIPv6アドレスの両方に対して正常にpingを実行します。

Command Prompt

```
C:\Users\admin>
C:\Users\admin>ping 2001:db8:50::20

Pinging 2001:db8:50::20 with 32 bytes of data:
Request timed out.
Reply from 2001:db8:50::20: time=4ms
Reply from 2001:db8:50::20: time=4ms
Reply from 2001:db8:50::20: time=3ms

Ping statistics for 2001:db8:50::20:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

Select Command Prompt

```
C:\Users\admin>
C:\Users\admin>ping 192.168.50.20

Pinging 192.168.50.20 with 32 bytes of data:
Reply from 192.168.50.20: bytes=32 time=3ms TTL=64
Reply from 192.168.50.20: bytes=32 time=3ms TTL=64
Reply from 192.168.50.20: bytes=32 time=3ms TTL=64
Reply from 192.168.50.20: bytes=32 time=4ms TTL=64

Ping statistics for 192.168.50.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

確認_Cisco_Secure_Client_Ping

ステップ 18 : ISE RADIUSライブログに認証の成功が表示されます。

Overview

Event	5200 Authentication succeeded
Username	isetest
Endpoint Id	52:54:00:16:12:64 ⓘ
Endpoint Profile	Windows10-Workstation
Authentication Policy	Default >> Default
Authorization Policy	Default >> Basic_Authenticated_Access
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2024-12-09 10:56:38.389
Received Timestamp	2024-12-09 10:56:38.389
Policy Server	cmlise-psn
Event	5200 Authentication succeeded
Username	isetest
User Type	User
Endpoint Id	52:54:00:16:12:64
Calling Station Id	192.168.10.1
Endpoint Profile	Windows10-Workstation
Authentication Identity Store	Internal Users

ISE_Authentication_Success_Log

ステップ 19 : FTDがISEに到達できないときに、FTD認証がローカルに行われるかどうかをテスト

トします。

ステップ 19.1 : FTD認証でISEにアクセスする場合は、統計情報を確認するためにFTD(Lina)CLIでコマンドshow aaa-serverを実行します。

この例では、LOCALのカウンタはなく、認証はRADIUSサーバに送信されます。

<#root>

ftdv760# show aaa-server

```
Server Group:    LOCAL
Server Protocol: Local database
Server Address:  None
Server port:     None
Server status:   ACTIVE, Last transaction at 08:18:11 UTC Fri Dec 6 2024
Number of pending requests      0
Average round trip time         0ms
Number of authentication requests  0
Number of authorization requests  0
Number of accounting requests    0
Number of retransmissions        0
Number of accepts                0
Number of rejects                0
Number of challenges             0
Number of bad authenticators      0
Number of timeouts              0
Number of unrecognized responses  0
Server Group:    demo_ise_group
Server Protocol: radius
```

Server Address: 2001:db8:2139::240

```
Server port:      1812(authentication), 1646(accounting)
Server status:    ACTIVE, Last transaction at 02:56:41 UTC Mon Dec 9 2024
Number of pending requests      0
Average round trip time         100ms
```

Number of authentication requests 1 <== Increased

Number of authorization requests 1 <== Increased

Number of accounting requests 1 <== Increased

Number of retransmissions 0

Number of accepts 2 <== Increased

Number of rejects 0

Number of challenges 0

Number of bad authenticators 0

Number of timeouts 0

Number of unrecognized responses 0

ステップ 19.2 : FTDがISEから応答を受信できないことをシミュレートするためにISEインターフェイスをシャットダウンします。

<#root>

```
ftdv760# ping 2001:db8:2139::240
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2001:db8:2139::240, timeout is 2 seconds:

???

Success rate is 0 percent (0/3)

ステップ 19.3 : クライアントがVPN接続を開始し、ステップ10で作成したのと同じユーザ名のパスワードを入力すると、VPN接続は成功します。

もう一度FTD(Lina)CLIでコマンドshow aaa-serverを実行して、統計情報を確認し、LOCALの認証、認可、および許可のカウンタが増加していることを確認します。RADIUSサーバのacceptsカウンタが増加していない。

<#root>

```
ftdv760# show aaa-server
```

Server Group: LOCAL

Server Protocol: Local database

Server Address: None

Server port: None

Server status: ACTIVE, Last transaction at 03:36:26 UTC Mon Dec 9 2024

Number of pending requests 0

Average round trip time 0ms

Number of authentication requests 1 <== Increased

Number of authorization requests 1 <== Increased

Number of accounting requests 0

Number of retransmissions 0

Number of accepts 2 <== Increased

Number of rejects 0

Number of challenges 0

Number of bad authenticators 0

Number of timeouts 0

Number of unrecognized responses 0

Server Group: demo_ise_group

Server Protocol: radius

Server Address: 2001:db8:2139::240

Server port: 1812(authentication), 1646(accounting)

Server status: ACTIVE, Last transaction at 03:36:41 UTC Mon Dec 9 2024

Number of pending requests	0
Average round trip time	100ms
Number of authentication requests	2
Number of authorization requests	1
Number of accounting requests	6
Number of retransmissions	0
Number of accepts	2 <== Not increased
Number of rejects	0
Number of challenges	0
Number of bad authenticators	0
Number of timeouts	6
Number of unrecognized responses	0

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

VPNセクションのトラブルシューティングを行うには、FTD回線で次のコマンドを実行できます。

```
debug webvpn 255
debug webvpn anyconnect 255
```

問題がセキュアクライアントにあるかどうかを判断するために、VPNのトラブルシューティング用にクライアントからDARTファイルを収集できます。ガイダンスについては、関連するCCOドキュメント『[Collect DART Bundle for Secure Client](#)』を参照してください。

RADIUSセクションのトラブルシューティングを行うには、FTD回線でこれらのコマンドを実行できます。

```
ftdv760# debug radius ?

all          All debug options
decode       Decode debug option
dynamic-authorization CoA listener debug option
session      Session debug option
user         User debug option
<cr>
```

```
ftdv760# debug aaa ?
```

```
accounting
authentication
```

```
authorization
common
condition
internal
shim
url-redirect
<cr>
```

VPN接続後にトラフィック関連の問題をトラブルシューティングするには、次の項目を確認します。

1. FTD Linaでトラフィックをキャプチャし、Linaでトラフィックがドロップされるかどうかを確認します。CCOについてはこのドキュメントを参照してください。[Firepower Threat Defense\(FTD\)のキャプチャとPacket Tracerを使用してください。シスコ](#)
2. 復号化されたトラフィックのアクセスコントロールポリシーのバイパスが無効になっている場合は、関連するVPNトラフィックが通過を許可されることを確認するためにアクセスコントロールポリシーを確認します。
3. VPNトラフィックがNATから除外されていることを確認するには、NAT免除を確認します。

関連情報

- [RAVPNのFDM設定ガイド：シスコ](#)
- [セキュアクライアント用DARTバンドルの収集 - シスコ](#)
- [Firepower Threat Defense\(FTD\)のキャプチャとPacket Tracerの使用：シスコ](#)
- [Cisco Secure Clientのトラブルシューティング：シスコ](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。