

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。

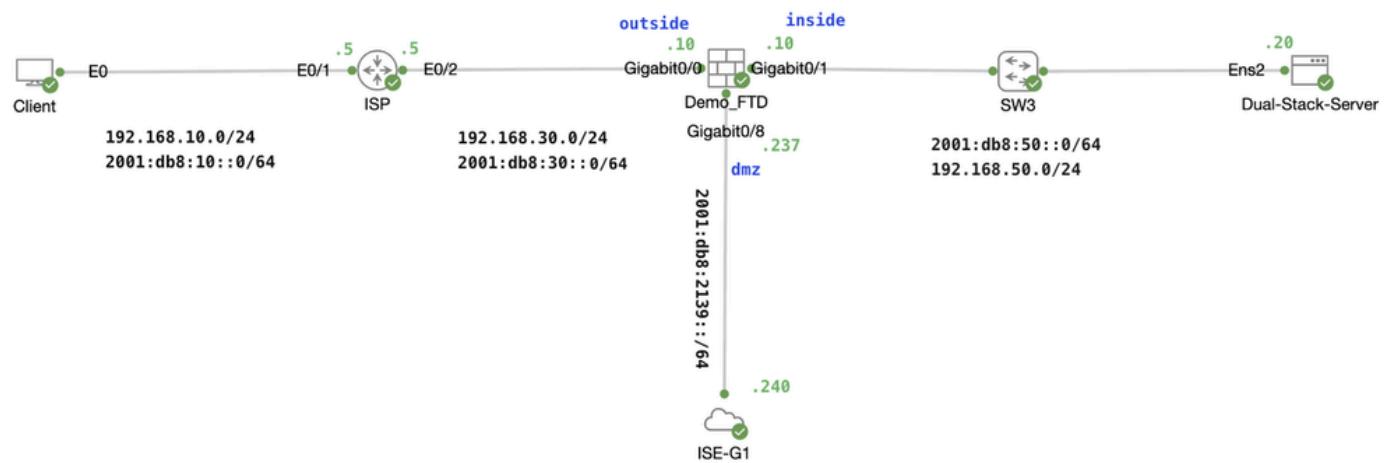
背景説明

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。

NAME	LOGICAL NAME	STATUS	MODE	IP ADDRESS	STANDBY ADDRESS	MONITOR FOR HA	ACTIONS
> GigabitEthernet0/0	outside		Routed	192.168.30.10 2001:db8:30::10/64		Enabled	
> GigabitEthernet0/1	inside		Routed	192.168.50.10 2001:db8:50::10/64		Enabled	
> GigabitEthernet0/2			Routed			Enabled	
> GigabitEthernet0/3			Routed			Enabled	
> GigabitEthernet0/4			Routed			Enabled	
> GigabitEthernet0/5			Routed			Enabled	
> GigabitEthernet0/6			Routed			Enabled	
> GigabitEthernet0/7			Routed			Enabled	
> GigabitEthernet0/8	dmz		Routed	2001:db8:2139::237/64		Enabled	

FTD_インターフェイス_IP

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	ToISP_v4	outside	IPv4	0.0.0.0/0	192.168.30.5		1	
2	ToISP_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。

SUBSCRIPTION LICENSES INCLUDED

- IPS** Enabled DISABLE
- Malware Defense** Enabled DISABLE
- URL** Enabled DISABLE
- Cisco Secure Client** Enabled Premier and A... DISABLE

This License allows you to perform intrusion detection and prevention and file control. You must have this license to apply intrusion policies in access rules. You also must have this license to apply file policies that control files based on file type.

This license lets you perform malware defense. You must have this license to apply file policies that detect and block malware in files transmitted over your network.

Please select the license type that you purchased to enable remote access VPN. Note that Secure Firewall device manager does not support any of the advanced features covered by the Advantage license.

Includes: RA-VPN

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。

Object Types

- Networks** (highlighted)
- Ports
- Security Zones
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- Secure Client Profiles

Network Objects and Groups

6 objects

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	

+ Filter Preset filters: System defined, User defined

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_ipv4pool
- 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 | admin Administrator | SECURE

Object Types

- Networks** (selected)
- Ports
- Security Zones
- Application Filters
- URLs
- Geolocations
- Syslog Servers
- IKE Policies
- IPSec Proposals
- Secure Client Profiles

Network Objects and Groups

6 objects

#	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	

+

作成_NAT_免除_ネットワーク_1

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::/64

CANCEL OK

作成_NAT_免除_ネットワーク_2_IPv4

- 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。

Object Types

Certificates

121 objects

#	NAME	TYPE
1	DefaultInternalCertificate	Internal Certificate
2	DefaultWebserverCertificate	Internal Certificate
3	NGFW-Default-InternalCA	Internal CA
4	AAA-Certificate-Services	Trusted CA Certificate
5	ACCVRAIZ1	Trusted CA Certificate
6	Acalis-Authentication-Root-CA	Trusted CA Certificate
7	AffirmTrust-Commercial	Trusted CA Certificate
8	AffirmTrust-Networking	Trusted CA Certificate
9	AffirmTrust-Premium	Trusted CA Certificate
10	AffirmTrust-Premium-ECC	Trusted CA Certificate
11	Amazon-Root-CA-1	Trusted CA Certificate
12	Amazon-Root-CA-2	Trusted CA Certificate
13	Amazon-Root-CA-3	Trusted CA Certificate
14	Cisco-Trusted-Authorities	Trusted CA Group

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

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.

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

Name: demovpn

Key Type: RSA

Key Size: 2048

Validity Period

Expiration Date: (UTC+08:00) Asia/Hong_Kong 02/15/2027 Set default

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



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



Search for attribute

Distinguished Name

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_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。

The screenshot shows the 'Object Types' section on the left with 'Identity Sources' selected. The main area displays 'Identity Sources' with one object named 'LocalIdentitySource' of type 'LOCAL'. A context menu is open on the right, with 'RADIUS Server' highlighted.

NAME	TYPE	VALUE
LocalIdentitySource	LOCAL	

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。

Create Radius Server Group

The screenshot shows the 'Create Radius Server Group' page in the Cisco Firewall Device Manager. The top navigation bar includes 'Monitoring', 'Policies', 'Objects' (selected), and 'Device: ftdv760'. On the left, a sidebar lists 'Object Types' such as Networks, Ports, Security Zones, Application Filters, URLs, Geolocations, Syslog Servers, IKE Policies, IPSec Proposals, and Secure Client Profiles. The main content area is titled 'Identity Sources' and shows two objects: 'LocalIdentitySource' (TYPE: LOCAL) and 'demo_ise' (TYPE: RADIUS, VALUE: 2001:db8:2139::241). A right-hand sidebar contains preset filters: RADIUS, AD Realm, SAML, Duo LDAP, and a dropdown menu with options: RADIUS Server (selected), AD Realm, AD Realm Sequence, Identity Services Engine, and SAML Server. A red box highlights the '+ v' button in the dropdown menu.

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 i

10

minutes

Maximum Failed Attempts

3

0-1440

1-5

Dynamic Authorization (for RA VPN only) i

Port

1700

1024-65535

Realm that Supports the RADIUS Server

Please select

RADIUS Server

i The servers in the group should be backups of each other



Filter

demo_ise

demo_ise

Create new RADIUS Server



CANCEL

OK

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。

The screenshot shows the Firewall Device Manager interface. The top navigation bar includes 'Firewall Device Manager', 'Monitoring', 'Policies', 'Objects', and 'Device: ftdv760'. On the left sidebar, 'RA VPN' is selected, followed by 'Connection Profiles' and 'Group Policies' (which is highlighted with a red box). Below these are 'SAML Server' and 'SAML Profile'. The main content area is titled 'Device Summary' and 'Group Policies', showing '2 objects'. A table lists one object: 'DftGrpPolicy'. The table columns are NAME, DNS SERVER, IPV4 SPLIT TUNNELING, IPV6 SPLIT TUNNELING, and SECURE CLIENT PROFILES. Under ACTIONS, there is a '+' button (also highlighted with a red box) and other icons.

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 left sidebar has sections for 'Basic' (selected and highlighted with a red box) and 'Advanced' (Address Assignment, Split Tunneling, Secure Client, Traffic Filters, Windows Browser Proxy). The main area has fields for 'Name' (demo_gp), 'Description' (empty), 'DNS Server' (Select DNS Group dropdown), 'Banner Text for Authenticated Clients' (demo banner), 'Default domain' (empty), and 'Secure Client profiles' (empty). At the bottom are 'CANCEL' and 'OK' buttons.

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。

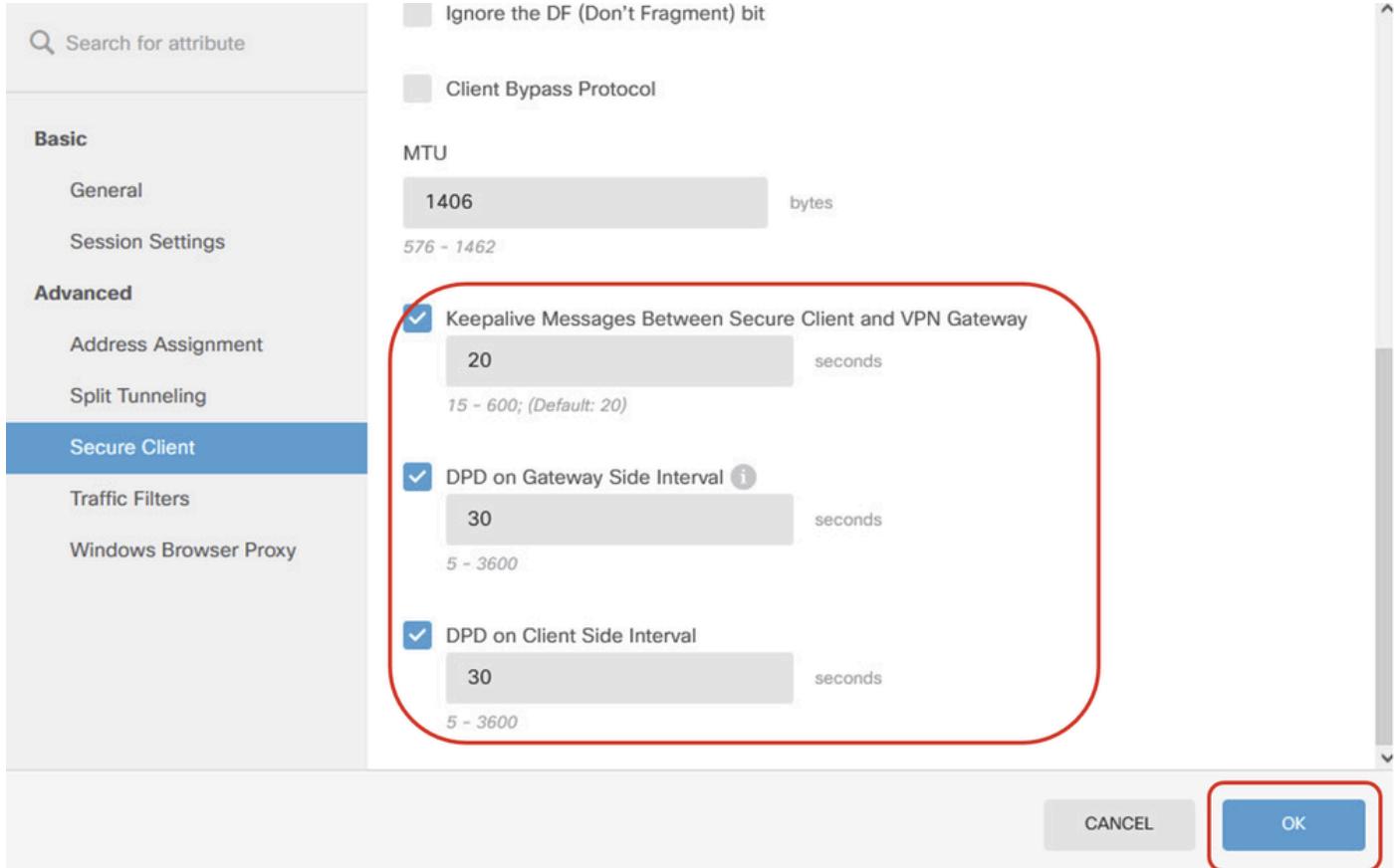
The screenshot shows the configuration interface for a Secure Client profile. On the left, a sidebar lists categories: Basic (General, Session Settings), Advanced (Address Assignment, Split Tunneling, Secure Client, Traffic Filters, Windows Browser Proxy). The 'Secure Client' option is highlighted with a red box. The main panel shows 'SSL SETTINGS' with a checked checkbox for 'Enable Datagram Transport Layer Security (DTLS)'. Other settings include 'DTLS Compression' (unchecked), 'SSL Compression' dropdown set to 'Disabled', 'SSL Rekey Method' dropdown set to 'None', and 'SSL Rekey Interval' set to 4 minutes. Below this is the 'CONNECTION SETTINGS' section with 'Ignore the DF (Don't Fragment) bit' and 'Client Bypass Protocol' checkboxes (both unchecked). At the bottom right are 'CANCEL' and 'OK' buttons.

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。



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。

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)

アカウンティングサーバ : 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



IPv6 Address Pool

Endpoints are provided an address from this pool



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。

A screenshot of the 'Remote User Experience' settings page in the Cisco FireWall Device Manager. The 'demo_gp' policy is selected. The 'NEXT' button is highlighted with a red box.

Remote User Experience

A group policy is a collection of user-unlimited 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

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

UPLOAD PACKAGE

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

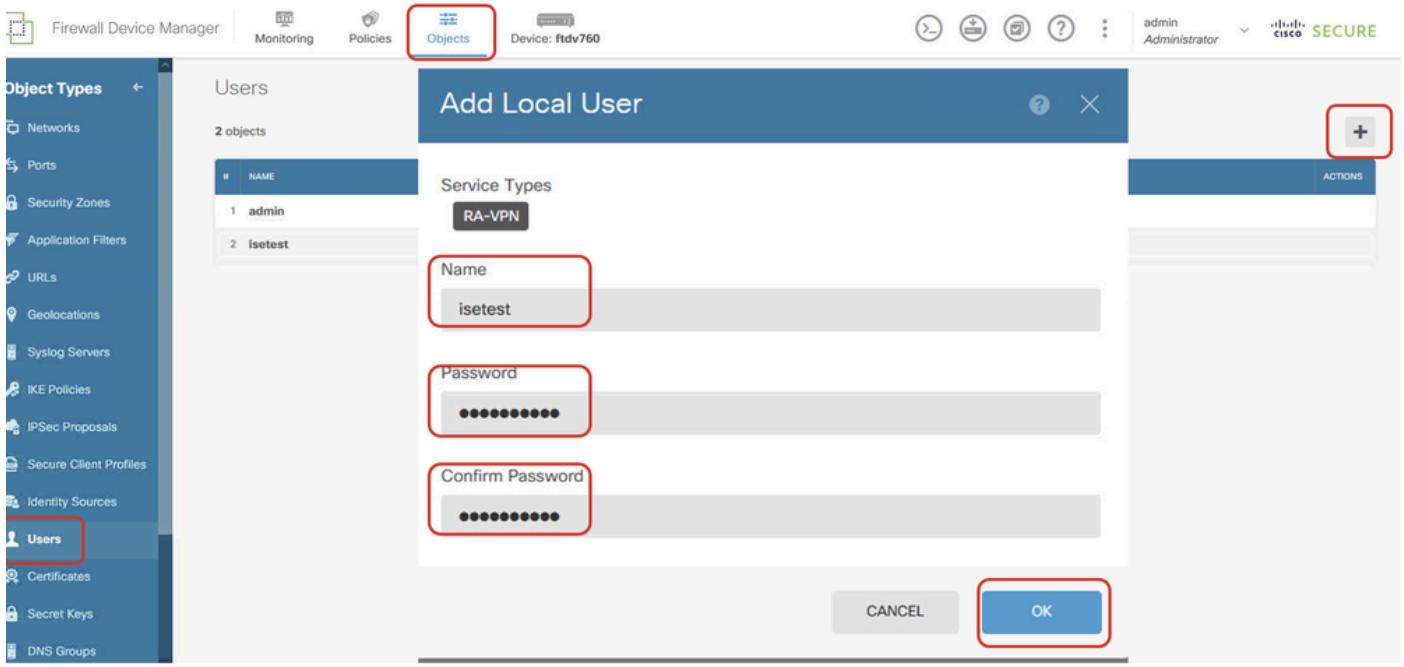
BACK

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。

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。

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。

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。

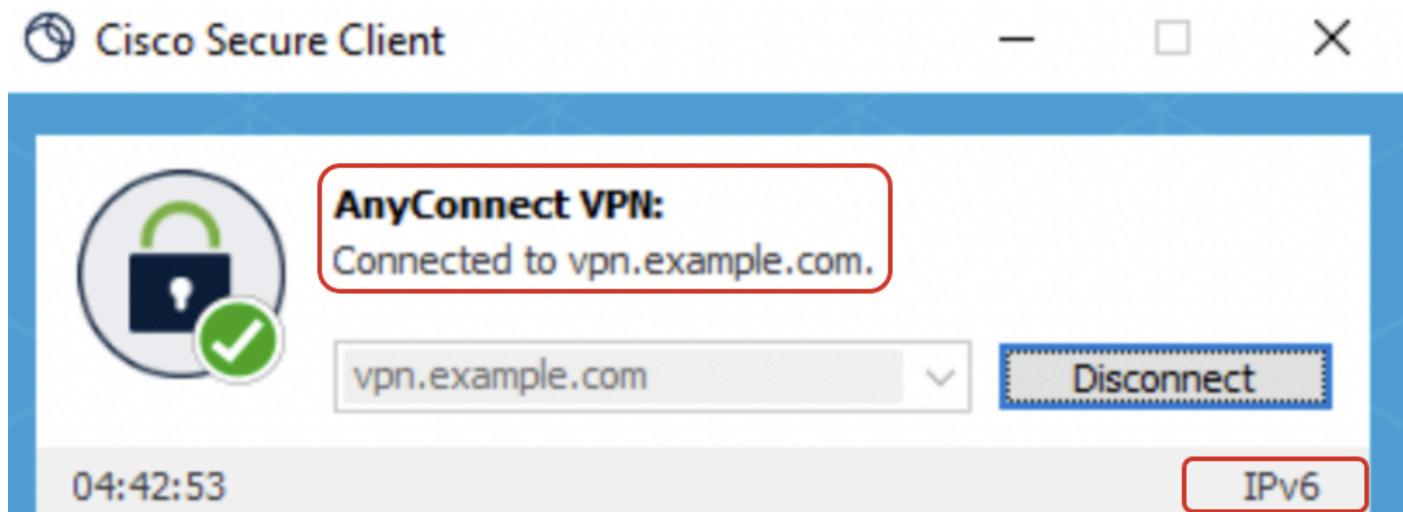
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
OK	SPRT		Radius-NAS-IP-Address EQUALS 10.48.26.61	Default Network Access	0	⚙️	↗️
OK	Wired		DEVICE-Device Type EQUALS All Device Types#Switch	Default Network Access	0	⚙️	↗️
OK	Firewall No Posture		DEVICE-Device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

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
Audit 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 T0 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

```

トラブルシュート

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。