

IPv6-compatibele RAVPN configureren met AAA-verificatie op FTD beheerd door FDM

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties op FDM](#)

[Configuraties op ISE](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

In dit document worden de stappen beschreven voor het configureren van een voor IPv6 geschikte externe VPN-toegang met AAA-verificatie op FTD die wordt beheerd door FDM.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure Firepower Device Manager (FDM) Virtual
- Cisco Secure Firewall Threat Defense (FTD) Virtual
- VPN-verificatiestroom

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure FDM Virtual 7.6.0
- Cisco Secure FTD Virtual 7.6.0
- Cisco Secure Client 5.1.6.103

De informatie in dit document is gebaseerd op de apparaten in een specifieke

laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

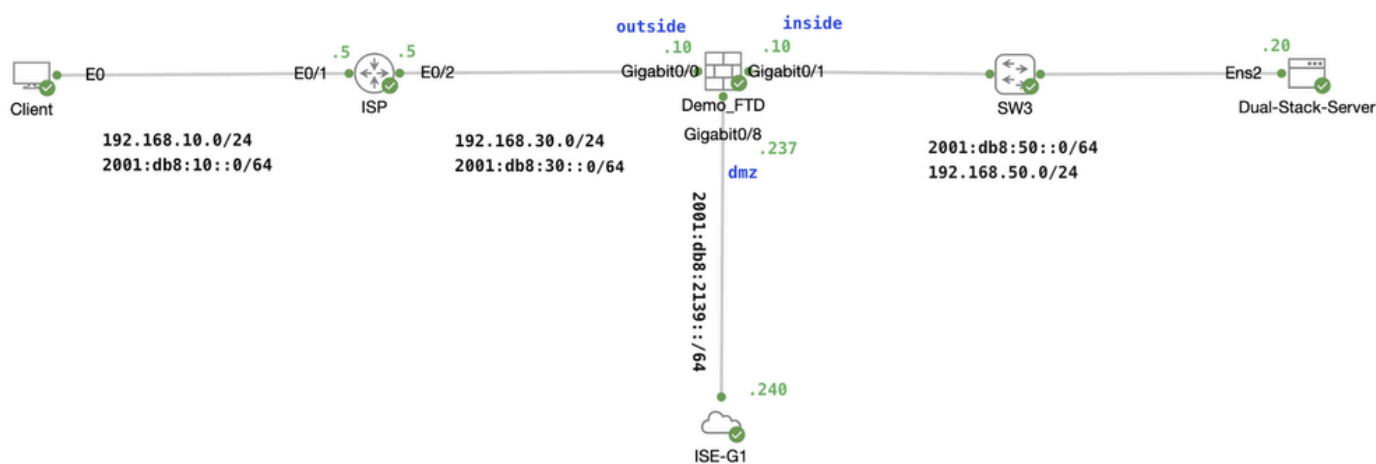
Achtergrondinformatie

IPv6 Remote Access VPN (RAVPN) wordt steeds belangrijker naarmate de wereld overgaat van IPv4 naar IPv6, omdat IPv4-adressen beperkt zijn en bijna uitgeput zijn, terwijl IPv6 een vrijwel onbeperkte adresruimte biedt, rekening houdend met het groeiende aantal met internet verbonden apparaten. Naarmate meer netwerken en services naar IPv6 gaan, zorgt de IPv6-mogelijkheid ervoor dat uw netwerk compatibel en toegankelijk blijft. IPv6 RAVPN helpt organisaties zich voor te bereiden op de toekomst van netwerken en zorgt voor veilige en schaalbare connectiviteit op afstand.

In dit voorbeeld communiceert de client met de VPN-gateway met behulp van een IPv6-adres dat door de serviceprovider is opgegeven, maar ontvangt zowel IPv4- als IPv6-adressen uit de VPN-pools, waarbij de Cisco Identity Service Engine (ISE) wordt gebruikt als bron voor de verificatie-identiteit. De ISE is alleen geconfigureerd met een IPv6-adres. De interne server is geconfigureerd met zowel IPv4- als IPv6-adressen, die hosts met twee stapels vertegenwoordigen. De client heeft toegang tot interne bronnen met het IPv4- of IPv6 VPN-adres, indien van toepassing.

Configureren

Netwerkdigram



Topologie

Configuraties op FDM

Stap 1. Het is van essentieel belang ervoor te zorgen dat de voorlopige configuratie van IPv4- en IPv6-interconnectie tussen knooppunten naar behoren is voltooid. De gateway van client en FTD is een gerelateerd ISP-adres. De gateway van de server bevindt zich binnen het IP van FTD. De ISE bevindt zich in het DMZ-gebied van FTD.

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_Interface_IP

Firewall Device Manager

Monitoring Policies Objects **Device: ftdv760**

Device Summary
Routing

Add Multiple Virtual Routers

Static Routing BGP OSPF EIGRP ECMP Traffic Zones

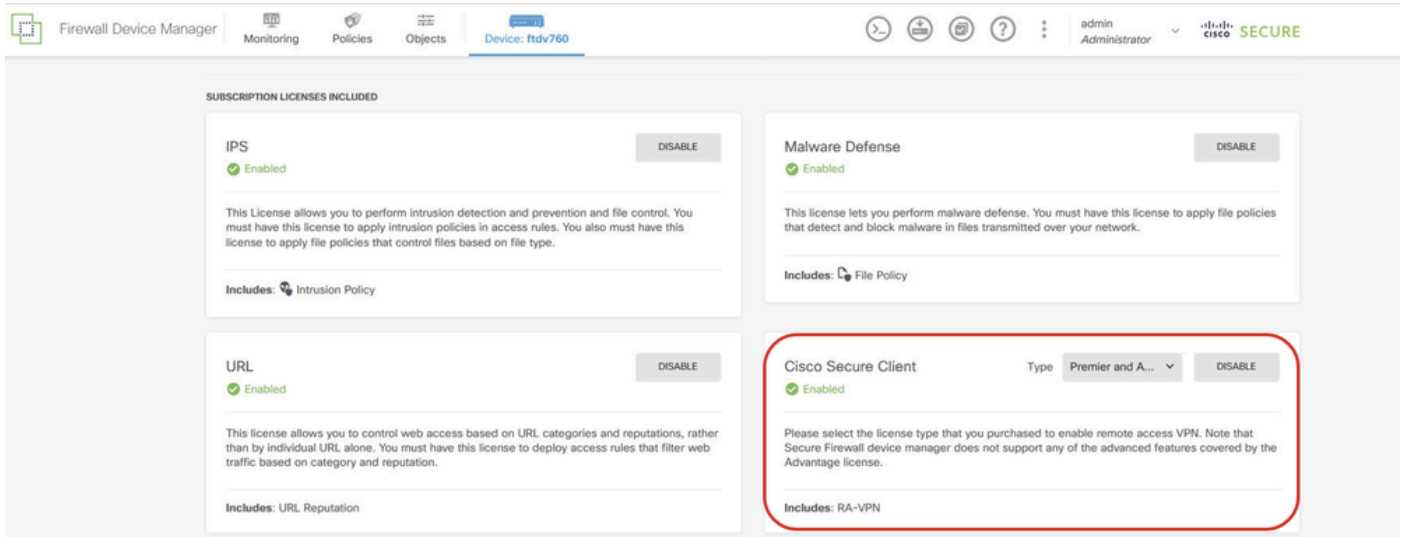
2 routes

#	NAME	INTERFACE	IP TYPE	NETWORKS	GATEWAY IP	SLA MONITOR	METRIC	ACTIONS
1	TotISP_v4	outside	IPv4	0.0.0.0/0	192.168.30.5		1	
2	TotISP_v6	outside	IPv6	::/0	2001:db8:30::5		1	

FTD_Default_Route

Stap 2. Download het Cisco Secure Client-pakket namecisco-secure-client-win-5.1.6.103-webdeploy-k9.pkg van [Cisco Software Download](#) en zorg ervoor dat het bestand goed is na het downloaden door te bevestigen dat de md5 checksum van het gedownloade bestand hetzelfde is als de Cisco Software Download pagina.

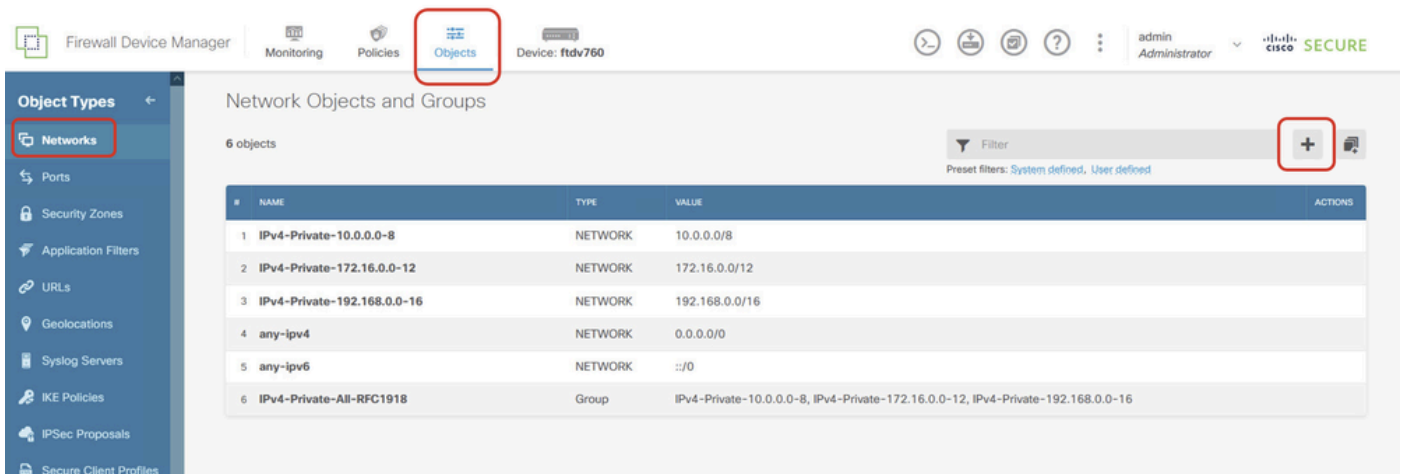
Stap 3. Controleer of RAVPN-gerelateerde licenties zijn ingeschakeld op FTD.



FDM_License

Stap 4. VPN-adresgroep maken.

Stap 4.1. IPv6- en IPv4-adresgroep maken door netwerkobjecten te maken. Navigeer naar Objecten > Netwerken en klik op de + knop.



Create_VPN_Address_Pool_1

Stap 4.2. Verstrek de nodige informatie over elk netwerkobject. Klik op de knop OK.

Voor de IPv4-pool kan het objecttype worden gekozen met Network of Bereik. In dit voorbeeld wordt het objecttype Network gekozen voor demodoeleinden.

- Naam: demo_ipv4pool
- Type: netwerk
- Netwerk: 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

Create_VPN_Address_Pool_2_IPv4

Voor de IPv6-pool kan vanaf nu alleen het objecttype met Network worden gekozen.

- Naam: demo_ipv6pool
- Type: netwerk
- Netwerk: 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

Create_VPN_Address_Pool_2_IPv6

Stap 5. Maak het interne netwerk voor NAT-vrijstelling.

Stap 5.1. Navigeer naar Objecten > Netwerken en klik op de knop +.

Firewall Device Manager

Monitoring Policies **Objects** Device: ftdv760

admin Administrator

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	

Stap 5.2. Verstrek de benodigde informatie over elk netwerkobject. Klik op de knop OK.

In dit voorbeeld worden zowel IPv4- als IPv6-netwerken geconfigureerd.

- Naam: inside_net_ipv4
- Type: netwerk
- Netwerk: 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

- Naam: inside_net_ipv6
- Type: netwerk
- Netwerk: 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

Create_NAT_Exempt_Network_2_IPv6

Stap 6. Maak een certificaat dat wordt gebruikt voor RAVPN. U hebt twee opties: u kunt een certificaat uploaden dat is ondertekend door een certificeringsinstantie van een derde partij of een nieuw zelf ondertekend certificaat genereren.

In dit voorbeeld wordt een nieuw zelf ondertekend certificaat gebruikt met aangepaste inhoud van het certificaat voor demodoeleinden.

Stap 6.1. Ga naar Objecten > Certificaten. Klik op de knop + en kies Intern certificaat toevoegen.

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
- Identity Sources
- Users
- Certificates**
- Secret Keys
- DNS Groups

Certificates

121 objects

Filter

Preset filters: System defined, User defined

#	NAME	TYPE	ACTIONS
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	Actalis-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	

Add Internal CA
 Add Internal Certificate
 Add Trusted CA Certificate

Create_Certificate_1

Stap 6.2. Klik op Certificaat met eigen handtekening.

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.

Stap 6.3. Klik op het tabblad Algemeen en geef de benodigde informatie op.

Naam: demovpn

Soort sleutel: RSA

Sleutelgrootte: 2048

Geldigheidsduur: Standaard

Vervaldatum: standaard

Gebruik van validatie voor speciale services: SSL-server

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

Create_Certificate_3

Stap 6.4. Klik op het tabblad Uitgever en geef de benodigde informatie op.

Land: Verenigde Staten (VS)

Algemene naam: 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

Create_Certificate_4

Stap 6.5. Klik op het tabblad Onderwerp, geef de benodigde informatie op en klik vervolgens op OPSLAAN.

Land: Verenigde Staten (VS)

Algemene naam: vpn.example.com

Add Internal Certificate

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.

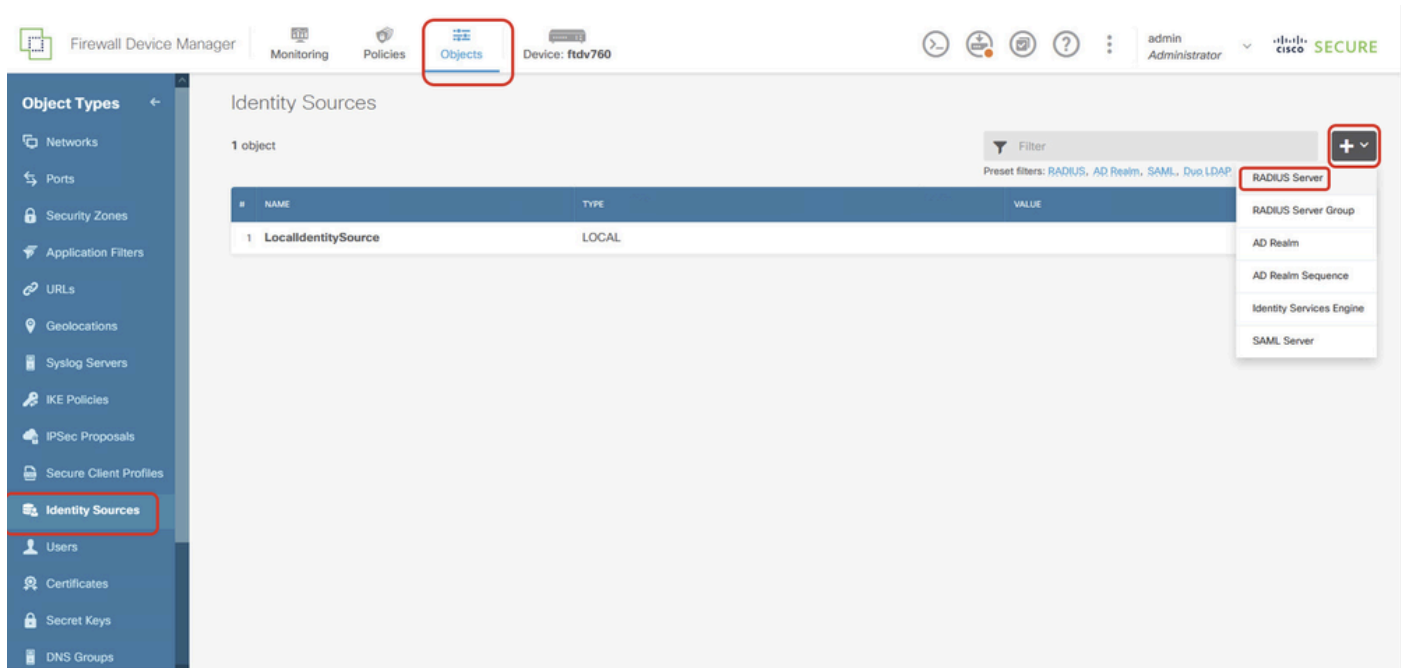
CANCEL

SAVE

Create_Certificate_5

Stap 7. Radius-server-identiteitsbron maken.

Stap 7.1. Navigeer naar Objecten > Identiteitsbronnen, klik op + en kies RADIUS Server.



Create_Radius_Source_1

Stap 7.2. Verstrek de nodige informatie over de radius-server. Klik op de knop OK.

Naam: demo_ise

Servernaam of IP-adres: 2001:db8:2139:240

Verificatiepoort: 1812 (standaard)

Time-out: 10 (standaard)

Server Secret-sleutel: cisco

Interface gebruikt om verbinding te maken met Radius-server: kies handmatig interface. Kies in dit voorbeeld dmz (Gigabit Ethernet0/8).

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

Create_Radius_Source_2

Stap 7.3. Ga naar Objecten > Identiteitsbronnen. Klik op de knop + en kies RADIUS-servergroep.

Create Radius Server Group

Firewall Device Manager | Monitoring | Policies | **Objects** | Device: ftdv760

admin Administrator

Object Types

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

Identity Sources

2 objects

Filter

Preset filters: RADIUS, AD Realm, SAML, Duo LDAP

#	NAME	TYPE	VALUE
1	LocalIdentitySource	LOCAL	
2	demo_ise	RADIUS	2001:db8:2139::241

+ ▼

- RADIUS Server
- RADIUS Server Group**
- AD Realm
- AD Realm Sequence
- Identity Services Engine
- SAML Server

Create_Radius_Source_3

Stap 7.4. Geef de benodigde informatie over de radius-servergroep op. Klik op de knop OK.

Naam: demo_ise_group

Dode tijd: 10 (standaard)

Maximum aantal mislukte pogingen: 3 (standaard)

RADIUS-server: Klik op de knop +, selecteer de naam die is gemaakt in stap 6.2. In dit voorbeeld is het demo_ise.

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

Create new RADIUS Server

CANCEL

OK

OK

Stap 8. Groepsbeleid maken dat voor RAVPN wordt gebruikt. In dit voorbeeld worden aangepaste banner- en time-outinstellingen geconfigureerd voor demodoeleinden. U kunt wijzigen op basis van uw werkelijke behoeften.

Stap 8.1. Navigeer naar Remote Access VPN > Configuratie bekijken. Klik op Groepsbeleid in de linkerzijbalk en klik op de knop +.



Create_Group_Policy_1

Stap 8.2. Klik op Algemeen en geef de benodigde informatie op.

Naam: demo_gp

Bannertekst voor geverifieerde clients: demo-banner

Add Group Policy

Search for attribute

Basic

General

Session Settings

Advanced

Address Assignment

Split Tunneling

Secure Client

Traffic Filters

Windows Browser Proxy

Name

demo_gp

Description

DNS Server

Select DNS Group

Banner Text for Authenticated Clients

This message will be shown to successfully authenticated endpoints in the beginning of their VPN session

demo banner|

Default domain

Secure Client profiles

CANCEL OK

Create_Group_Policy_2

Stap 8.3. Klik op Beveiligde client en geef de benodigde informatie op.

Schakel Datagram Transport Layer Security (DTLS) in.

The screenshot shows the 'Secure Client' configuration window. On the left sidebar, 'Secure Client' is selected under the 'Advanced' section. The main area is titled 'SSL SETTINGS' and contains the following options:

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

Below the SSL settings is the 'CONNECTION SETTINGS' section:

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

At the bottom right are 'CANCEL' and 'OK' buttons.

Create_Group_Policy_3

Controleer Keepalive Berichten tussen Secure Client en VPN Gateway (standaardwaarde).

Controleer DPD op Gateway Side Interval (standaardwaarde).

Controleer DPD op Client Side Interval (standaardwaarde).

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

Create_Group_Policy_3_CONT

Stap 9. Maak een RAVPN-verbindingsprofiel.

Stap 9.1. Navigeer naar Remote Access VPN > Configuratie bekijken. Klik op Verbindingsprofiel in de linkerbalk en klik op de + knop om de wizard te starten.

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

Create_RAVPN_Wizard_1

Stap 9.2. Geef de benodigde informatie op in de sectie Verbinding en clientconfiguratie en klik op de knop VOLGENDE.

Naam verbindingsprofiel: demo_ravpn

Groepsalias: 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_Name

Primaire identiteitsbron > Verificatietype: alleen AAA

Primaire identiteitsbron > Primaire identiteitsbron: demo_ise_group (de naam die is geconfigureerd in stap 7.4.)

Bron lokale identiteit Fallback: LocalIdentitySource

Autorisatieserver: demo_ise_group (de naam die is geconfigureerd in stap 7.4.)

Accounting Server: demo_ise_group (de naam die is geconfigureerd in stap 7.4.)

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_Identity_Source

IPv4-adrespool: demo_ipv4pool (de naam geconfigureerd in stap 4.2.)

IPv6-adrespool: demo_ipv6pool (de naam die is geconfigureerd in stap 4.2.)

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_Address_Pool

Stap 9.3. Kies het groepsbeleid dat is geconfigureerd in stap 8.2. in het gedeelte Externe gebruikerservaring en klik op de knop VOLGENDE.

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

Create_RAVPN_Wizard_3

Stap 9.4. Geef de benodigde informatie op in het gedeelte Globale instellingen en klik op de knop VOLGENDE.

Certificaat van apparaatidentiteit: demovpn (de naam die is geconfigureerd in stap 6.3)

Buitenkant interface: buitenkant

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

Create_RAVPN_Wizard_4

Toegangscontrole voor VPN-verkeer: Controleer het beleid voor toegangscontrole voor omzeilen voor gedecodeerd verkeer (sysopt permit-vpn).

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)

Create_RAVPN_Wizard_4_VPN_ACP

NAT-vrijstelling: klik op de schuifregelaar naar de positie Ingeschakeld

Binneninterfaces: binnenzijde

Binnen netwerken: inside_net_ipv4, inside_net_ipv6 (de naam geconfigureerd in stap 5.2.)

NAT Exempt



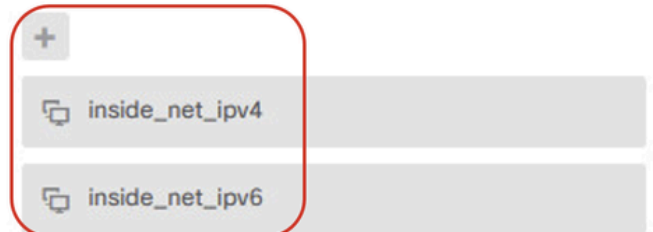
Inside Interfaces

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.



Create_RAVPN_Wizard_4_VPN_NATExempt

Beveiligd clientpakket: klik op **PAKKET UPLOADEN** en upload het pakket dienovereenkomstig. In dit voorbeeld wordt het Windows-pakket geüpload.

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



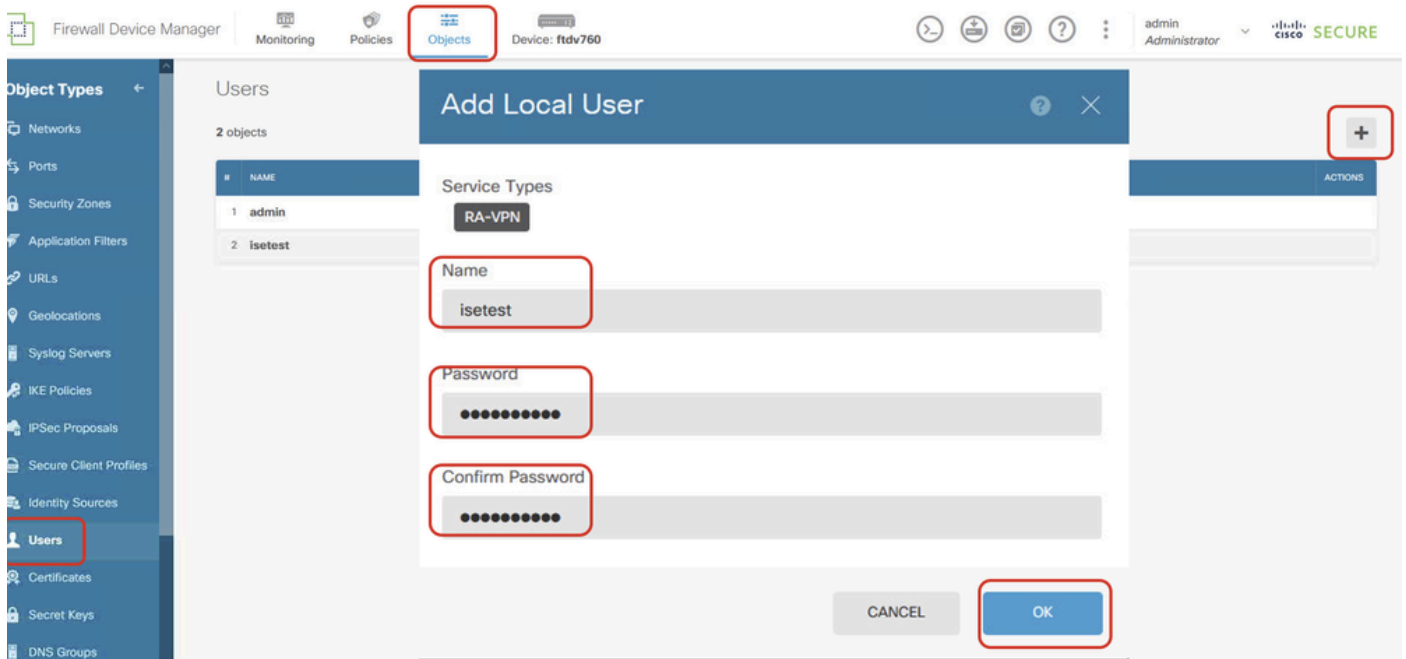
BACK

NEXT

Create_RAVPN_Wizard_4_Image

Stap 9.5. Bekijk de samenvatting. Als er iets moet worden gewijzigd, klikt u op de knop TERUG. Als alles goed is, klikt u op de knop FINISH.

Stap 10. Maak een lokale gebruiker aan als Fallback Local Identity Source is gekozen met LocalIdentitySource in stap 9.2. Het wachtwoord van de lokale gebruiker moet hetzelfde zijn als het wachtwoord dat op ISE is geconfigureerd.



Create_Local_User

Stap 11. Implementeer de configuratiewijzigingen.

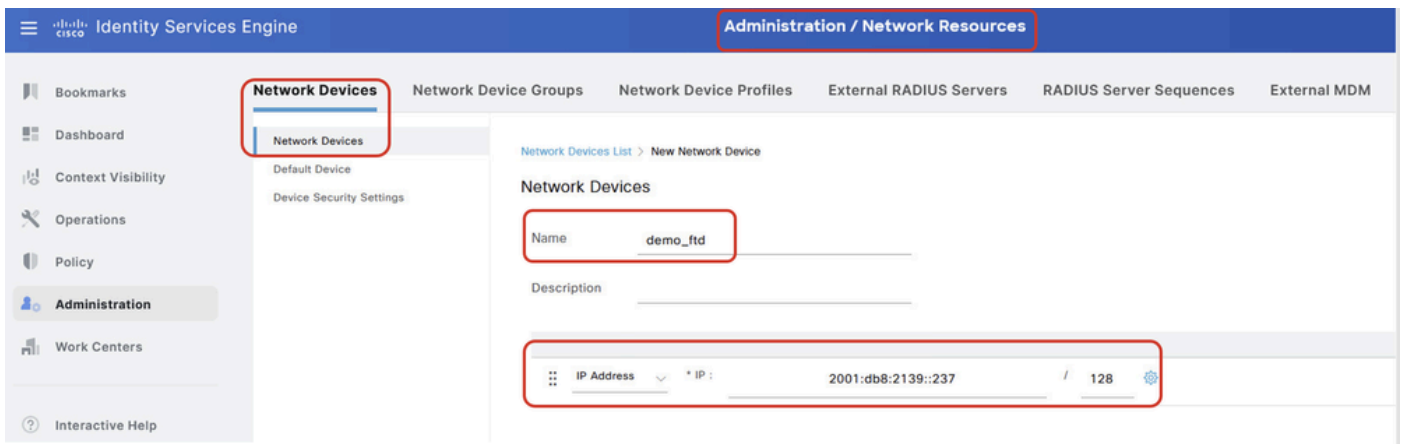


Implementeren_Wijzigingen

Configuraties op ISE

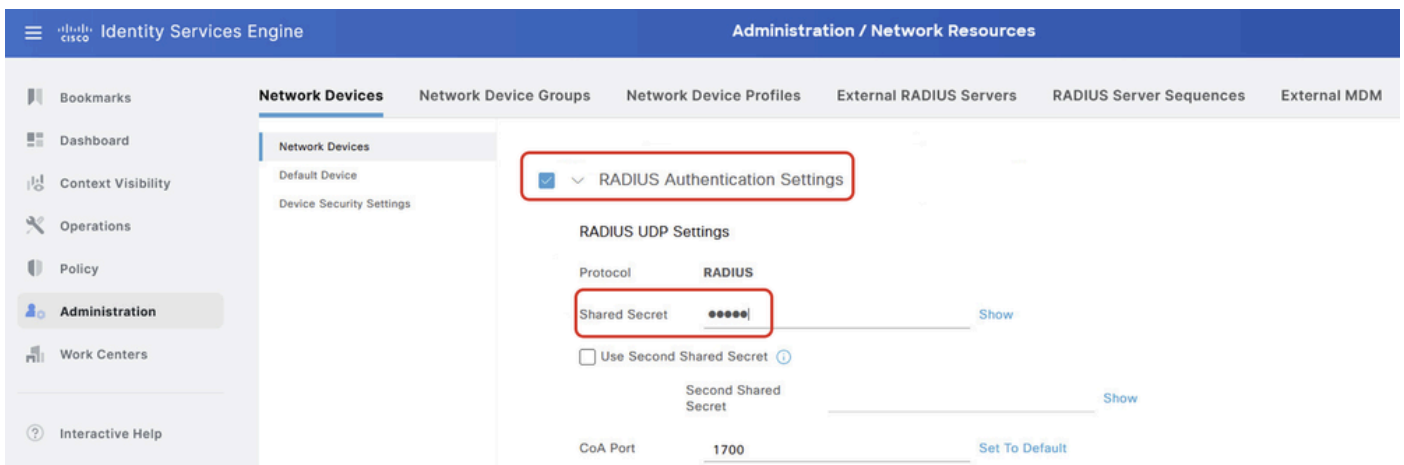
Stap 12. Netwerkkapparaten maken.

Stap 12.1. Navigeer naar Beheer > Netwerkbronnen > Netwerkkapparaten, klik op Toevoegen, geef de naam, het IP-adres op en blader naar beneden op de pagina.



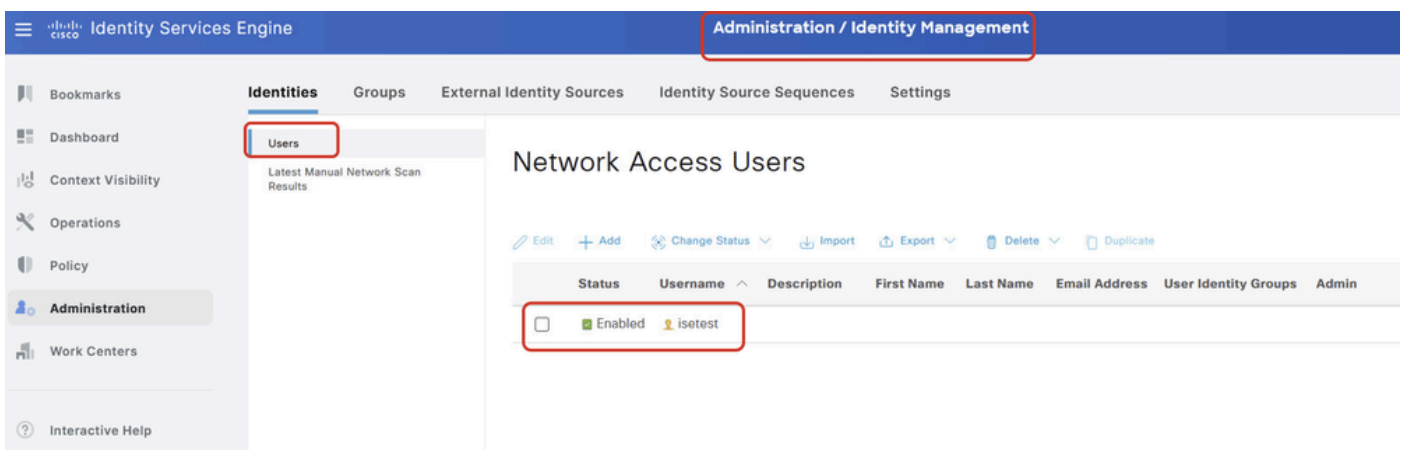
Create_Network_Devices

Stap 12.2. Schakel het selectievakje RADIUS-verificatie-instellingen in. Geef het gedeelde geheim op en klik op Indienen.



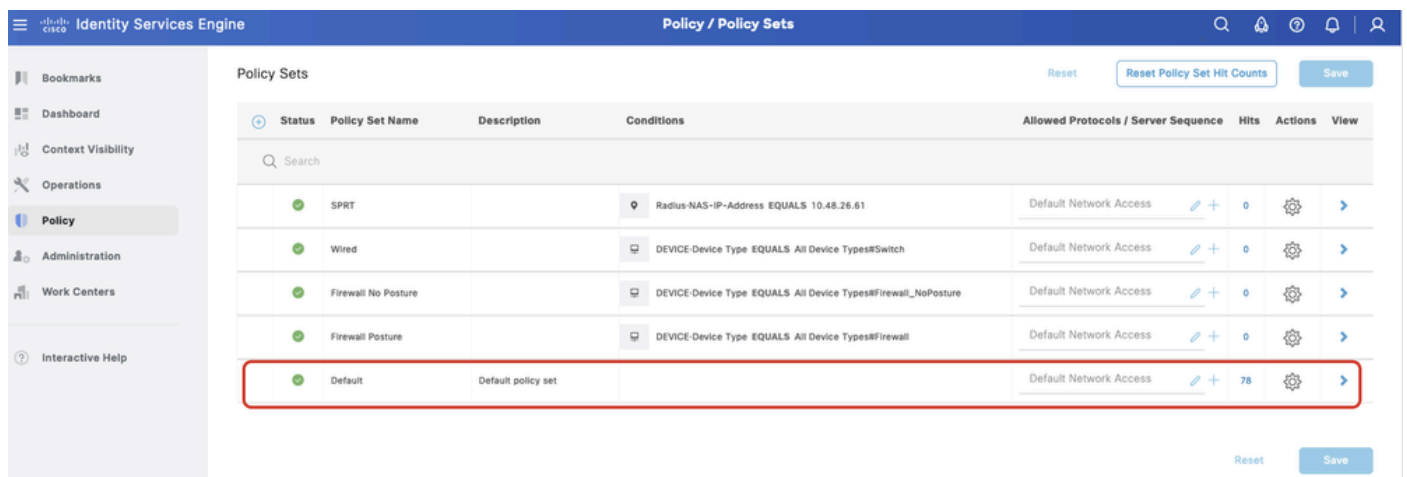
Create_Network_Devices_Cont

Stap 13. Netwerktogangebruikers maken. Navigeer naar Beheer > Identiteitsbeheer > Identiteiten. Klik op Toevoegen om een nieuwe gebruiker aan te maken. Het wachtwoord is hetzelfde als bij de lokale FDM-gebruiker die is gemaakt in stap 10. om ervoor te zorgen dat de terugvalfunctie werkt.



Create_ISE_User

Stap 14. (Optioneel) Maak een nieuwe beleidsset met aangepaste verificatieregel en autorisatieregel. In dit voorbeeld wordt de standaardbeleidsset gebruikt voor demodoeleinden.



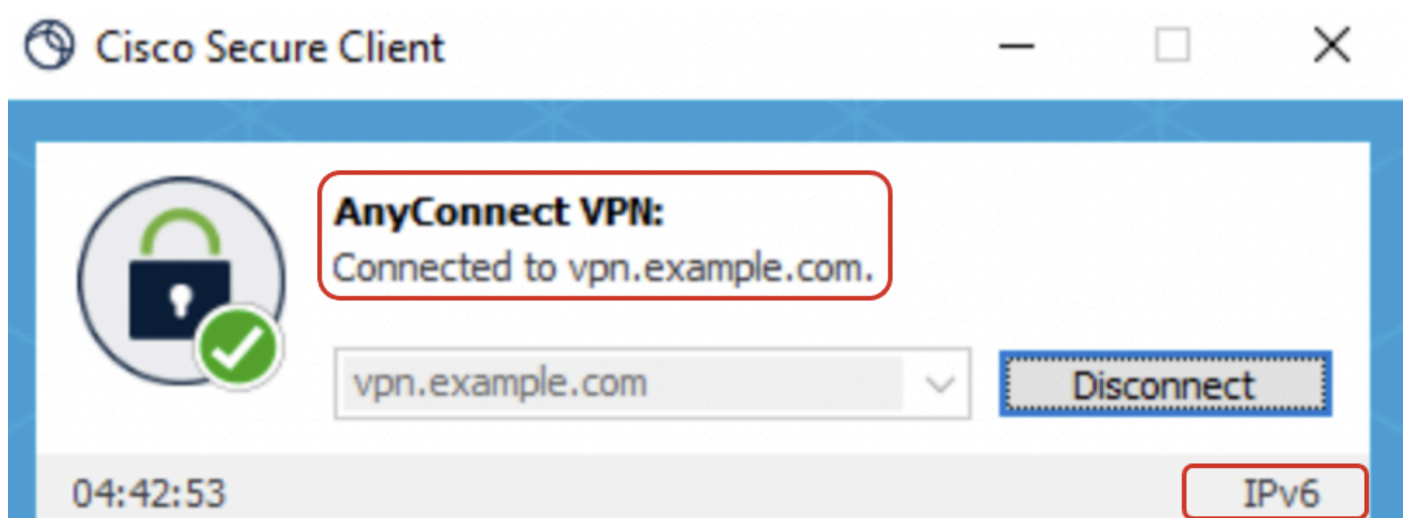
Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
OK	SPRT		Radius-NAS-IP-Address EQUALS 10.48.26.61	Default Network Access	0		
OK	Wired		DEVICE-Device Type EQUALS All Device Types#Switch	Default Network Access	0		
OK	Firewall No Posture		DEVICE-Device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

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Stap 15. Verbind de VPN-gateway via het IPv6-adres op de client. De VPN verbinding is succesvol.



Verify_Connection_Succesvol

Stap 16. Navigeer naar de CLI van FTD via SSH of console. Run command show vpn-sessiondb detail any connect in FTD (Lina) CLI om de VPN-sessiedetails te controleren.

<#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

Stap 17. Pingtest bij de klant. In dit voorbeeld pingt de client zowel het IPv4- als het IPv6-adres van de server.

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
```

Verify_Cisco_Secure_Client_Ping

Stap 18. ISE radius live log toont succesvolle authenticatie.

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

Stap 19. Test FTD-verificatie gaat naar LOKAAL wanneer FTD ISE niet kan bereiken.

Stap 19.1. Wanneer FTD-verificatie naar ISE gaat, voert u de opdracht show aaa-server in FTD (Lina) CLI uit om de statistieken te controleren.

In dit voorbeeld zijn er geen tellers voor LOKAAL en wordt de verificatie naar de RADIUS-server geleid.

<#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

Stap 19.2. Sluit de ISE-interface af om te simuleren dat FTD geen respons van ISE kan ontvangen.

<#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)

Stap 19.3. De client start de VPN-verbinding en voert hetzelfde wachtwoord voor de gebruikersnaam in dat is gemaakt in stap 10. De VPN-verbinding is nog steeds succesvol.

Opdracht uitvoeren toont aaa-server in FTD (Lina) CLI opnieuw om de statistiek te controleren, de authenticatie, autorisatie en acceptaties tellers voor LOKAAL zijn nu verhoogd. De acceptatieteller voor de RADIUS-server is niet verhoogd.

<#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

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

U kunt deze opdrachten uitvoeren op FTD Lina om problemen met de VPN-sectie op te lossen.

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

U kunt een DART-bestand van de client verzamelen voor VPN-probleemoplossing om te bepalen of het probleem zich voordoet met de beveiligde client. Raadpleeg voor meer informatie het relevante CCO-document [Collect DART Bundle for Secure Client](#).

U kunt deze opdrachten uitvoeren op FTD Lina om problemen op te lossen in het gedeelte Radius.

```
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>
```

U kunt deze bekijken om het verkeersgerelateerde probleem op te lossen nadat de VPN-verbinding succesvol is verlopen.

1. Leg verkeer vast op FTD Lina om te zien of Lina het verkeer laat vallen, verwijzend naar dit CCO-document; [Gebruik Firepower Threat Defense Captures en Packet Tracer - Cisco](#).
2. Controleer het toegangscontrolebeleid om ervoor te zorgen dat het gerelateerde VPN-verkeer mag worden doorgegeven als het beleid voor toegangscontrole voor gedecodeerd verkeer is uitgeschakeld.
3. De NAT-vrijstelling herzien om ervoor te zorgen dat VPN-verkeer wordt uitgesloten van NAT.

Gerelateerde informatie

- [FDM Configuratiegids van RAVPN - Cisco](#)
- [Verzamel DART-bundel voor beveiligde client - Cisco](#)
- [Firepower Threat Defense Captures en Packet Tracer gebruiken - Cisco](#)
- [Problemen oplossen met Cisco Secure Client - Cisco](#)
- [Cisco Technical Support en downloads](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.