Circuit matching voor beveiligde clientautorisatie op FTD via FDM configureren

Inhoud

| Inleiding |
|---|
| Voorwaarden |
| Vereisten |
| Gebruikte componenten |
| Achtergrondinformatie |
| <u>Netwerkdiagram</u> |
| Configuraties |
| Configuratie in FDM |
| Stap 1. FTD-interface configureren |
| Stap 2. Cisco Secure-clientlicentie bevestigen |
| Stap 3. Adresgroep toevoegen |
| Stap 4. Beveiligd clientprofiel maken |
| Stap 5. Beveiligd clientprofiel uploaden naar FDM |
| Stap 6. Groepsbeleid toevoegen |
| Stap 7. FTD-certificaat toevoegen |
| Stap 8. CA aan FTD toevoegen |
| Stap 9. VPN-verbindingsprofiel voor externe toegang toevoegen |
| Stap 10. Samenvatting voor verbindingsprofiel bevestigen |
| Bevestigen in FTD CLI |
| Bevestigen in VPN-client |
| Stap 1. Beveiligd clientprofiel naar VPN-client kopiëren |
| Stap 2. Clientcertificaat bevestigen |
| Stap 3. Bevestig CA |
| Verifiëren |
| Stap 1. VPN-verbinding starten |
| Stap 2. VPN-sessies in FTD CLI bevestigen |
| Problemen oplossen |
| Gerelateerde informatie |

Inleiding

Dit document beschrijft hoe u Cisco Secure Client met SSL op FTD via FDM kunt instellen met behulp van certificaatmatching voor verificatie.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

- Cisco Firepower Device Manager Virtual 7.2.8
- Cisco Firewall Threat Defense Virtual 7.2.8
- Cisco Secure-client 5.1.4.7
- Profieleditor (Windows) 5.1.4.74

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

CertificateMatch is een functie waarmee beheerders criteria kunnen configureren die de client moet gebruiken om een clientcertificaat te selecteren voor verificatie met de VPN-server. Deze configuratie wordt gespecificeerd in het clientprofiel, dat een XML-bestand is dat kan worden beheerd met de profieleditor of handmatig kan worden bewerkt. De optie CertificateMatch kan worden gebruikt om de beveiliging van VPN-verbindingen te verbeteren door ervoor te zorgen dat alleen een certificaat met specifieke kenmerken wordt gebruikt voor de VPN-verbinding.

Dit document beschrijft hoe u de Cisco Secure Client kunt verifiëren met behulp van de algemene naam van een SSL-certificaat.

In deze certificaten staat een gemeenschappelijke benaming, die voor vergunningsdoeleinden wordt gebruikt.

- CA: ftd-ra-ca-common-name
- Engineer VPN Clientcertificaat: vpnEngineerClientCN
- VPN-clientcertificaat voor Manager: vpnManagerClientCN
- Servercertificaat: 192.168.1.200

Netwerkdiagram

Dit beeld toont de topologie die bij het voorbeeld van dit document wordt gebruikt.



Netwerkdiagram

Configuraties

Configuratie in FDM

Stap 1. FTD-interface configureren

Navigeer naar apparaat > Interfaces > Alle interfaces weergeven, configureer binnen en buiten interface voor FTD in tabblad Interfaces.

Voor Gigabit Ethernet0/0,

- Naam: buiten
- IP-adres: 192.168.1.200/24

| Firewall | Device Manager Monitoring | Policies Objects | Device: firepower | | | |) (?) : | admin Administrator | cisco SECURE |
|----------|---|------------------|-------------------|-----------|----------------------|---|-----------------|------------------------|--------------|
| | Device Summary Interfaces | | | | | | | | |
| | Cisco Firepower Threat Defense for VMwa | 0/6 0/7 | ε | | | | | | |
| | 9 Interfaces | | | | | Ŧ | Filter | | + |
| | NAME | | LOGICAL NAME ST | ATUS MODE | IP ADDRESS | | STANDBY ADDRESS | MONITOR FOR H | ACTIONS |
| | > 🗸 GigabitEthernet0/0 | | outside | Routed | 192.168.1.200 Static | | | Enabled | |

FTD-interface

Stap 2. Cisco Secure-clientlicentie bevestigen

Navigeer naar apparaat > slimme licentie > Configuratie bekijken, bevestig de Cisco Secure Client-licentie in Licentie voor RA VPN.



Secure-clientlicentie

Stap 3. Adresgroep toevoegen

Navigeer naar Objecten > Netwerken en klik op +.

| Firewall Device Mana | ger Monitoring Policies Objects Device: f | firepower | -) (admin Administrator · · · · · · · · · · · · · · · · · · · |
|---|---|------------------|--|
| Óbject Types ← | Network Objects and Groups | | _ |
| C Networks | 7 objects | | ▼ Filter + 🛃 |
| S Ports | | | Preset filters: System defined, User defined |
| G Security Zones | # NAME | TYPE VALUE | ACTIONS |
| Application Eiltere | 1 IPv4-Private-10.0.0-8 | NETWORK 10.0.0/8 | |

Adresgroep toevoegen

Voer de benodigde informatie in om een nieuwe IPv4-adresgroep toe te voegen. klik op OK knop.

- Naam: ftd-cert-match-pool
- Type: bereik
- IP-bereik: 172.16.1.150-172.16.1.160

Add Network Object

| Name |
|---|
| ftd-cert-match-pool |
| Description |
| |
| Type |
| Network Host FQDN Range |
| IP Range |
| 172.16.1.150-172.16.1.160 |
| e.g. 192.168.2.1-192.168.2.24 or 2001:DB8:0:CD30::10-2001:DB8:0:CD30::100 |
| |
| CANCEL |

ค



Stap 4. Beveiligd clientprofiel maken

Download en installeer de Secure Client Profile Editor van de <u>Cisco Software</u>-site. Navigeer naar de serverlijst en klik op de knop Toevoegen. Voer de benodigde informatie in om een serverlijst toe te voegen en klik op OK.

- Display Naam: cert-match
- FQDN- of IP-adres: 192.168.1.2010
- Primair protocol: SSL

| (Part 1) (Part 2) | Server List Profile: Untit | led | | | | | | | | | | |
|---|-------------------------------|----------------|-----------------|------------------|----------------------------|-----------------|-----------------------|---------------------------|-----------------------|---------------------|-----------------------|-----------|
| ate Pinning ate Matching ate Enrollment | Hostname | Host Addr | User Group | Backup Ser | SCEP | Mobile Sett | Certificate | | | | | |
| ust | Note: it is hi | ighly recommer | nded that at le | ast one server t | e define <mark>l</mark> li | Ad C | el | | | | | |
| | | | | | | Server List | Entry Balancing Se | wers SCEP Mohi | le. Certificate Pinni | ng | | |
| | | | | | | Primary | Server | Ners Seer Hour | Conne | tion Information | | |
| | | | | | | Display FQDN | Name (requir | ed) cert-match User Gr | prima | SA gateway | ✓ | |
| | | | | | | 192.10 | 8.1.200 | 1 | A | uth Method During | IKE Negotiation EA | P-AnyConr |
| | | | | | | Group | URL 8.1.200 | | IK | E Identity (IOS gat | eway only) | |
| | | | | | | | | Backup Servers | | | | |
| | | | | | | | | Host Address | | | Add | |
| | | | | | | | | | | | Move Up | |
| | | | | | | | | | | | Move D | |
| | | | | | | | | | | | Delete | |
| | | | | | | | | | M Dennel | | | |

Invoer in serverlijst

Klik op de knop Toevoegen om naar Certificaat-matching te navigeren. Voer de benodigde informatie in om een onderscheidende naamvermelding toe te voegen en klik op OK.

- Naam: CN
- Patroon: vpnEngineerClientCN
- Exploitant: gelijk



Opmerking: controleer de optie MatchCase in dit document.

| 🚡 Cisco Secure Client Profile Editor | - VPN | | | | | | | | | |
|--|--|--|--|----------|--------|----------------|---|--|--|--|
| File Help | | | | | | | | | | |
| VPN Preferences (Part 1) Preferences (Part 2) | Certificate Matching Profile: C:\Users\jianzh3\OneDrive - Cisco\Desktop\vpnClient.xml | | | | | | | | | |
| Certificate Dinoing Certificate Enrolment Certificate Enrolment Mobile Policy | Key Usag Deci CRL Key Data Key Data Non Digi | e pher_Only _Sign _Cert_Sign _Agreem _Encipher _Encipherm. _Repudiat tal_Signa | Extended Key Us ServerAuth DVCS ClientAuth IKE Intermediate CodeSign EmailProtect IPSecEndSystem IPSecUser OCSPSign OCSPSign | | | | | | | |
| | Custom E | xtended Mat | ch Key (Ma. Add Delete | | | | Distinguished Name Entry X Name CN Pattern vpnEngineerClient | | | |
| | Match only certificates with Key Usage Match only certificates with Extended Key Usage Distinguished Name (Max | | | | | | Operator O Equal O Not Equal | | | |
| | Name | Pattern | Wildcard | Operator | MatchC | Edit Delete | OK Cancel | | | |

Benoemde naam

Sla het beveiligde clientprofiel op de lokale computer op en bevestig de gegevens van het profiel.

| ▼ <certificatematch> <matchoplycertswithku>false</matchoplycertswithku></certificatematch> |
|--|
| <pre>vCDistinguishedName> vCDistinguishedNameDefinition Operator="Equal" Wildcard="Disabled" MatchCase="Enabled"></pre> |
| |
| false |
| <autoserverselectionimprovement>20</autoserverselectionimprovement> |
| <pre></pre> |
| |
| <pre><retainvpnunlogottztaise <="" captiveportalremediationbrowserfailover="" retainvpnunlogottz="">false<!--/captivePortalRemediationBrowserFailover--></retainvpnunlogottztaise></pre> |
| <a>LowManua Host Input>true lowManua Host Input> |
| |
| ▼ <serverlist></serverlist> |
| ▼ <hostentry></hostentry> |
| <hostname>cert-match</hostname> |
| (HostAddress/192.108.1.200/HostAddress/ |
| Vierven istz |
| |

Beveiligd clientprofiel

Stap 5. Beveiligd clientprofiel uploaden naar FDM

Navigeer naar Objecten > Beveiligd clientprofiel en klik op de knop BEVEILIGD CLIENTPROFIEL MAKEN.

| Firewall Device Manager Monitoring | Policies Objects | Device: firepower | () admin Administrator | diality SECURE |
|------------------------------------|-----------------------|---------------------|---|------------------------------------|
| Object Types ← | Secure Client Profile | es | | |
| C Networks | | | F ilter | + |
| S Ports | # NAME | FILE NAME | ACTIONS | |
| G Security Zones | | | | _ |
| 🐬 Application Filters | | There are no S | Secure Client profile objects yet. | |
| C ^O URLs | | Start by creating t | the first Secure Client profile object. | |
| © Geolocations | | CREAT | TE SECURE CLIENT PROFILE | |
| Syslog Servers | | | | |
| 🔎 IKE Policies | | | | |
| n IPSec Proposals | | | | |
| Secure Client Profil | | | | |
| S Identity Sources | | | | |

Beveiligd clientprofiel maken

Voer de benodigde informatie in om een beveiligd clientprofiel toe te voegen en klik op OK.

- Naam: SecureClientProfile
- Secure Client Profile: SecureClientProfile.xml (uploaden vanaf lokale computer)

| Add Secure Client Profile | | | | | | |
|--------------------------------|----|---|--|--|--|--|
| Name secureClientProfile | | | | | | |
| Description | | 4 | | | | |
| UPLOAD secureClientProfile.xml | | | | | | |
| CANCEL | ОК | | | | | |

Stap 6. Groepsbeleid toevoegen

Navigeer naar Apparaat > Externe toegang VPN > Configuratie bekijken > Groepsbeleid, klik op + knop.

| Firewall Device M | anager Monitoring Policies Objects | Device: firepower | (Σ_{-}) | : ? 🕲 🏝 | admin Administrator | SECURE |
|---------------------|------------------------------------|-------------------|----------------------|----------------------|------------------------|---------|
| RA VPN ← | Device Summary Group Policies | | | | | |
| Connection Profiles | 2 objects | | | T Filter | | + |
| SAML Server | # NAME | DNS SERVER | IPV4 SPLIT TUNNELING | IPV6 SPLIT TUNNELING | SECURE CLIENT PROFILES | ACTIONS |
| | 1 DfltGrpPolicy | | Allow all traffic | Allow all traffic | | |

Groepsbeleid toevoegen

Voer de benodigde informatie in om een groepsbeleid toe te voegen en klik op OK.

- · Naam: ftd-cert-match-grp
- Beveiligde clientprofielen: beveiligdClientprofiel

| Add Group Policy | | 0 | × |
|--|---|----|---|
| Q. Search for attribute | Name ftd-cert-match-orp | | |
| Basic General Session Settings | Description | | |
| Advanced Address Assignment Split Tunneling Secure Client Traffic Filters Windows Browser Proxy | DNS Server Select DNS Group Banner Text for Authenticated Clients This message will be shown to successfully authenticated endpoints in the beggining of their VPN session Secure Client profiles | ~ | |
| Details van groepsbeleid | Create new Secure Client Profile CANCEL OK | ОК | |

Stap 7. FTD-certificaat toevoegen

Navigeer naar Objecten > Certificaten, klik op Intern certificaat toevoegen vanuit + item.

| Firewall Device Mar | ager Monitoring Policies Objects Device f | irepower | O → Ø ○ : ad Ad | imin Iministrator |
|------------------------|---|------------------------|--|----------------------------------|
| Object Types ← | Certificates | | | |
| C Networks | 121 objects | | Y Filter | + - 🔊 |
| S Ports | | | Preset filters: System defined, User defined | Add Internal CA |
| 8 Security Zones | B NAME | туре | | Add Internal Certificate ACTIONS |
| Application Filters | 1 AAA-Certificate-Services | Trusted CA Certificate | | Add Trusted CA Certificate |
| A 1101 ★ | 2 ACCVRAIZ1 | Trusted CA Certificate | | |
| C URLS | 3 Actalis-Authentication-Root-CA | Trusted CA Certificate | | |
| Geolocations | 4 AffirmTrust-Commercial | Trusted CA Certificate | | |
| Syslog Servers | 5 AffirmTrust-Networking | Trusted CA Certificate | | |
| 🔏 IKE Policies | 6 AffirmTrust-Premium | Trusted CA Certificate | | |
| 👍 IPSec Proposals | 7 AffirmTrust-Premium-ECC | Trusted CA Certificate | | |
| Secure Client Profiles | 8 Amazon-Root-CA-1 | Trusted CA Certificate | | |
| Identity Sources | 9 Amazon-Root-CA-2 | Trusted CA Certificate | | |
| Lisors | 10 Amazon-Root-CA-3 | Trusted CA Certificate | | |
| | 11 DefaultInternalCertificate | Internal Certificate | | |
| 및 Certificates | 12 DefaultWebserverCertificate | Internal Certificate | | |

Intern certificaat toevoegen

Klik op Certificaat en sleutel uploaden.



Uploadcertificaat en sleutel

Voer de benodigde informatie voor FTD-certificaat in, importeer een certificaat en een certificaatsleutel van een lokale computer en klik vervolgens op OK.

- Naam: ftd-vpn-cert
- · Gebruik van validatie voor speciale services: SSL-server

Add Internal Certificate



Ø

X

Gegevens van het interne certificaat

Stap 8. CA aan FTD toevoegen

Navigeer naar Objecten > Certificaten, klik op Vertrouwde CA-certificaat toevoegen vanuit + item.

| Firewall Device Manager | Monitoring Policies Objects Device: fireport | wer (>_ (@) (?) : | admin Administrator |
|-------------------------|--|--|----------------------------------|
| 🐬 Application Filters | Cortificator | | |
| 🖉 URLs | Certificates | | |
| Geolocations | 120 objects | T Filter | + - 🛃 - |
| E Durley Desum | | Preset filters: System defined. User defined | Add Internal CA |
| Syslog Servers | # NAME | туре | Add Internal Certificate ACTIONS |
| 🔎 IKE Policies | 1 NGFW-Default-InternalCA | Internal CA | Add Trusted CA Certificate |
| 🛖 IPSec Proposals | 2 AAA-Certificate-Services | Trusted CA Certificate | |
| Secure Client Profiles | 3 ACCVRAIZ1 | Trusted CA Certificate | |
| 🚉 Identity Sources | 4 Actalis-Authentication-Root-CA | Trusted CA Certificate | |
| 1 Users | 5 AffirmTrust-Commercial | Trusted CA Certificate | |
| Q Certificates | 6 AffirmTrust-Networking | Trusted CA Certificate | |
| | 7 AffirmTrust-Premium | Trusted CA Certificate | |
| - Secret Keys | - ME-T Possible FOO | T | |



Voer de benodigde informatie voor CA in en importeer een certificaat van een lokale computer.

- Naam: ftdvpn-ca-cert
- Gebruik van validatie voor speciale services: SSL-client

| Add Trusted CA Certificate | | 0 × |
|---|--|-------------------------------------|
| Name ftdvpn-ca-cert | | |
| Certificate Paste certificate, or choose a file (DER, PEM, CRT, CER)BEGIN CERTIFICATE MIIDbDCCA1SgAwIBAgIIUkKgLg229/@wDQYJKoZIhvcNAQEU BhMCS1AxDjAMBgNVBAgTBVRva31vMQ4wDAYDVQQHEwVUb2ts Collection Usage for Special Services Validation Usage for Special Services | LBQAwbTELMAkGA1UE 5bzEOMAwGA1UEChMF | ftd-ra-ca.crt Upload.Certificate |
| SSL Client × | CANCEL | ОК |

Stap 9. VPN-verbindingsprofiel voor externe toegang toevoegen

Navigeer naar Apparaat > Externe toegang VPN > Configuratie bekijken > Verbindingsprofielen, klik op de knop VERBINDINGSPROFIEL MAKEN.

| Firewall Device N | fanager Monitoring | Policies Objects | Device: firepower | S. 🖓 🕲 ? : admin Administrator | diale SECURE |
|-------------------|--------------------|---------------------------------|-------------------------|-----------------------------------|----------------------------------|
| RA VPN ← | | Device Summary Remote Access | VPN Connection Profiles | | |
| Group Policies | | | | F ilter | + |
| SAML Server | | # NAME | AAA GROUP POLICY | Y ACTIONS | |
| | | | There are no Remo | ote Access Connections yet. | |
| | 1 | | | | |
| | | | Start by creating | ng the first Connection | |

VPN-verbindingsprofiel voor externe toegang toevoegen

Voer de benodigde informatie in voor het verbindingsprofiel en klik op Volgende knop.

- Profielnaam verbinding: ftd-cert-match-vpn
- · Verificatietype: alleen clientcertificaat
- · Gebruikersnaam van certificaat: Kaartspecifiek veld
- Primair veld: CN (algemene naam)
- Secundair veld: OU (organisatorische eenheid)
- IPv4-adresgroepen: ftd-cert-match-pool

| Firewall Device Manager Monitoring Policies | Objects Device: firepower | (c) |
|---|--|--|
| Remote Access VPN | Connection and Client Configuration Configuration Configuration | 3 Global Settings 4 Summary |
| 🔁 Remote Users 📃 Secure C | ients — Internet ·········· Q Client Certificate ···· OUTSOE | PIREPOWER I DISCE VICE Orporate Resources Unce for User Authentication |
| | Connection and Client Config Specify how to authenticate remote users and the secure clients inside network. | guration they can use to connect to the |
| | Connection Profile Name This name is configured as a connection alias, it can be used to connect to the ftd-cert-match-vpn | VPN gateway |
| | Group Alias (one per line, up to 5) Group URL (one ftd-cert-match-upn | e per line, up to 5) |
| | Primary Identity Source Authentication Type Client Certificate Only | |
| | Username from Certificate Map Specific Field Primary Field CN (Common Name) V OU (Organisat | i ional Unit) 🗸 |
| | Use entire DN (distinguished name) as username Advanced | |
| | Authorization Server Accounting Server Please select | r V |
| | Client Address Pool Assignment IPv6 Address Pool Endpoints are provided an address from this pool Chapoints are provided Chapoints are provided C | I ed an address from this pool |
| | DHCP Servers | |

Details van VPN-verbindingsprofiel

Voer de benodigde informatie voor groepsbeleid in en klik op Volgende knop.

• Bekijk het groepsbeleid: ftd-cert-match-grp

| Firewall Device Manager Monitoring Policies Objects | Device: firepower | S (a) (a) (a) (b) (b) (b) (b) (b) (b) (b) (b) (b) (b |
|---|---|--|
| Remote Access VPN | Connection and Client Configuration Remote User Experience | 3 Global Settings 4 Summary |
| Remote Users Secure Cl | ents — Internet — Q Client Certificate — OUT SEE | FIREPOWER |
| | Remote User Experien A group policy is a collection of user-oriented session attributes wi VPN connection is established. Select or create a G View Group Policy Itd-cert-match-grp Policy Group Brief Details | Aich are assigned to client when a Broup Policy object. |
| | Earner Text for Authentic BACK NEXT | |

Groepsbeleid selecteren

Selecteer Certificaat van Apparaatidentiteit, Buiteninterface, Beveiligd clientpakket voor VPN-verbinding.

- Certificaat van identiteit apparaat: ftd-vpn-cert
- Externe interface: buiten (Gigabit Ethernet0/0)
- Secure-clientpakket: cisco-secure-client-win-5.1.4.74-webimplementation-k9.pkg



Opmerking: NAT-vrijstelling in dit document is uitgeschakeld.

| Firewall Device Manager Monitorin | g Policies Objects Device: firepower | Solution (1) So | SECURE |
|-----------------------------------|--|---|--------|
| n Remote Use | rs Secure Clients - Internet | tificate | |
| | Glo These settings control the basic function apply to all connection profiles; you ca | obal Settings oning of the connection. Changes to any of these options cannot configure different settings in different profiles. | |
| | Certificate of Device Identity ftd-vpn-cert (Validation Usinge: SSL Se Fully-qualified Domain Name for the Outsid e.g. ravpn.example.com Access Control for VPN Traffic Decypted VPN traffic is subjected to access control policy for decrypted traffic option bypasses the ac- and the authorization ACL downloaded from the AV Bypass Access Control policy for decrypted NAT Exempt () | time interface voting (GigabitEthernet0/0) v ide Interface Port 443 e.g. 8080 strol policy Inspection by default. Enabling the Bypass Access Control sccess control policy, but for remote access VPN, the VPN Filter ACL. AAA server are still applied to VPN traffic trypted traffic (sysopt permit-vpn) | |
| | Secure Client Package If a user does not already have the right secure clien installer when the client authenticates for the first to You can download secure client packages from so You must have the necessary secure client software Packages UPLOAD PACKAGE Windows: clisco-secure-client-win-5,1.4.74 | lient package installed, the system will launch the secure client t time. The user can then install the package from the system. Ioftware.clico.com C are license. | |

Details van wereldwijde instellingen

Stap 10. Samenvatting voor verbindingsprofiel bevestigen

Bevestig de informatie die u hebt ingevoerd voor een VPN-verbinding en klik op FINISH.

| þ | Firewall Device Manager | 题 Monitoring | © Policies | Dbjects | Device: firepower | \odot | ۲ | ? | ÷ | admin Administrator | Ŷ | cisco SECURE |
|---|-------------------------|-----------------|---------------|---------|-------------------|---------|---|---|---|------------------------|---|--------------|
| | | | | | | | | | | | | |

Summary

Review the summary of the Remote Access VPN configuration.

| STEP 1: CONNECTION AND CLIENT CONFIGURATION | DN |
|---|--|
| Primary Identity Source | - |
| Authentication Type | Client Certificate Only |
| Primary Identity Source | _ |
| Fallback Local Identity Source | - |
| Usemame from Cestificate | Man Specific Eield |
| Osemane non ceruncate | CN (Common Name) |
| Primary Field | GN (Common Name) |
| Secondary Field | OU (Organisational Unit) |
| Advanced | |
| Authorization Server | |
| Accounting Server | |
| Client Address Pool Assignment | |
| IPv4 Address Pool | C ftd-cert-match-pool |
| IPv6 Address Pool | - <i>6</i> |
| DHCP Servers | - |
| STEP 2: GROUP POLICY | |
| Group Policy Name | ₫ [®] ftd-cert-match-grp |
| Banner + DNS Server | |
| DNS Server | i - |
| Banner text for authenticated clients | - |
| Session Settings | |
| Maximum Connection Time / Alert Interval | Unlimited / 1 minutes |
| Idle Timeout / Alert Interval | 30 / 1 minutes |
| Simultaneous Login per User | 3 |
| Split Tunneling | |
| IPv4 Split Tunneling | Allow all traffic over tunnel |
| IPv6 Split Tunneling | Allow all traffic over tunnel |
| Secure Client | |
| Secure Client Profiles | a secureClientProfile |
| STEP 3: GLOBAL SETTINGS | |
| Certificate of Device Identity | |
| Outside Interface | GigabitEthernet0/0 (outside) |
| Fully-qualified Domain Name for the Outside | - |
| InterraCe | |
| Port | 445 |
| Access Control for VPN Traffic | NO |
| NAT Exempt | No. |
| NAT Exempt | no |
| Inside Interfaces | - |
| Inside Networks | - |
| Secure Client Package | |
| | Windows: cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg |

Samenvatting voor verbindingsprofiel bevestigen

Bevestigen in FTD CLI

Bevestig de VPN-verbindingsinstellingen in de FTD CLI na implementatie vanuit de FDM.

// Defines IP of interface interface GigabitEthernet0/0 speed auto nameif outside cts manual propagate sgt preserve-untag policy static sgt disabled trusted security-level 0 ip address 192.168.1.200 255.255.255.0 // Defines a pool of addresses ip local pool ftd-cert-match-pool 172.16.1.150-172.16.1.160 // Defines Trustpoint for Server Certificate crypto ca trustpoint ftd-vpn-cert enrollment terminal keypair ftd-vpn-cert crl configure // Server Certificate crypto ca certificate chain ftdvpn-ca-cert certificate ca 5242a02e0db6f7fd 3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7 quit // Defines Trustpoint for CA crypto ca trustpoint ftdvpn-ca-cert enrollment terminal validation-usage ssl-client crl configure // CA crypto ca certificate chain ftdvpn-ca-cert certificate ca 5242a02e0db6f7fd 3082036c 30820254 a0030201 02020852 42a02e0d b6f7fd30 0d06092a 864886f7 quit // Configures the FTD to allow Cisco Secure Client connections and the valid Cisco Secure Client images webvpn enable outside http-headers hsts-server enable max-age 31536000 include-sub-domains no preload hsts-client enable x-content-type-options x-xss-protection content-security-policy anyconnect image disk0:/anyconnpkgs/cisco-secure-client-win-5.1.4.74-webdeploy-k9.pkg 2 anyconnect profiles secureClientProfile disk0:/anyconncprofs/secureClientProfile.xml anyconnect enable tunnel-group-list enable cache disable error-recovery disable

// Configures the group-policy to allow SSL connections

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

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

Bevestigen in VPN-client

Stap 1. Beveiligd clientprofiel naar VPN-client kopiëren

Kopieer het beveiligde clientprofiel naar de VPN-client voor engineer en beheer van VPN-client.



Opmerking: De map met het beveiligde clientprofiel op Windows-computer: C:\ProgramData\Cisco\Cisco Secure Client\VPN\Profile

| 📕 🛛 🛃 🗸 🕴 Profile | e | | | | | |
|-------------------|-------|-----------------------------------|----------------------------------|--------------------|---------------|---|
| File Home S | Share | View | | | | |
| ← → * ↑ 📙 | > Thi | is PC → Local Disk (C:) → Program | Data > Cisco > Cisco Secure Clie | nt > VPN > Profile | ~ | ් |
| - Quick access | | Name | Date modified | Туре | Size | |
| Desktop | * | MgmtTun | €, _ 3/2024 20:15 | File folder | 07 1/0 | |
| 🕹 Downloads | * | e secureClientProfile | 7 °2, 2024 21:44 | XML Document | 97 KB 4 KB | |
| 🚼 Documents | - * | | | | | |



Stap 2. Clientcertificaat bevestigen

In ingenieur VPN client, navigeer naar Certificaten - Huidige Gebruiker > Persoonlijk > Certificaten, controleer het clientcertificaat dat wordt gebruikt voor verificatie.



Certificaat voor Engineer VPN-client bevestigen

Dubbelklik op het clientcertificaat, navigeer naar Details, controleer de details van het onderwerp.

Onderwerp: CN = vpnEngineerClientCN

| Certificate X General Details Certification Path Show: <all> Field Value Valid to Wednesday, June 18, 2025 5: Subject vpnEngineerClentCN, vpnEngineerClentCN Public key parameters 05 00 Ø Key Usage Digital Signature, Key Encipher Ø Enhanced Key Usage Client Authentication (1.3.6.1) Ø Netscape Comment xca certificate Thu unbowint alnowithm dwa1 CN = vpnEngineerClentCN val Ø = Clsco L L = Tokyo S S = Tokyo C C = JP Edit Properties</all> | | | |
|---|---|--|--|
| General Details Certification P | ath | | |
| Show: <all></all> | \sim | | |
| Field | Value ^ Wednesday, June 18, 2025 5: | | |
| Subject | vpnEngineerClientCN, vpnEngi RSA (2048 Bits) | | |
| Key Usage Enhanced Key Usage | Digital Signature, Key Encipher Client Authentication (1.3.6.1 | | |
| Thumboriot algorithm | sha1 | | |
| CN = vpnEngineerClientCN O = Cisco L = Tokyo S = Tokyo C = JP | | | |
| | Edit Properties | | |
| | OK | | |

Details van Engineer client certificaat

Ga in de VPN-client voor het beheer naar Certificaten - Huidige gebruiker > Persoonlijk > Certificaten, controleer het clientcertificaat dat wordt gebruikt voor verificatie.



Certificaat voor beheer VPN-client bevestigen

Dubbelklik op het clientcertificaat, navigeer naar Details, controleer de details van het onderwerp.

• Onderwerp: CN = vpnManagerClientCN

| General Details Certification | Path |
|---|---|
| Show: <all></all> | \sim |
| Field | Value ^ Thursday, June 19, 2025 9:41 |
| Public key Public key parameters | RSA (2048 Bits) 05 00 |
| Key Usage Enhanced Key Usage | Digital Signature, Key Encipher Client Authentication (1.3.6.1 |
| CN = vnnManagerClientCN | cha 1 |
| O = Cisco L = Tokyo S = Tokyo C = JP | I |
| | Edit Properties Copy to File |
| | OK |

×

Details van clientcertificaat van Manager

Stap 3. Bevestig CA

🔊 Certificate

In zowel de client van ingenieur VPN als de client van manager VPN, navigeer naar Certificaten -Huidige Gebruiker > Trusted Root Certification Authorities > Certificates, controleer de CA die gebruikt wordt voor verificatie.

• Afgegeven door: ftd-ra-ca-common-name

| 1 | Console1 - [Console Root\Certificates - Current | User\Trusted Root Certification A | uthorities\Certificates] | | | 1 | ٥ | > | < |
|----|--|--|--|---|---|---|---|-----------------------------|----------|
| | <u>File Action View Favorites Window</u> | Help | | | | | | - 8 | × |
| • | 🔿 🖄 📷 🤞 🐃 🞇 🖬 🖉 🛛 | 1 | | | | | | | |
| ~ | Console Root Certificates - Current User Personal Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Certificates Current Publishers Current Publishers Untrusted Publishers Untrusted Certificates Current Publishers Current Publishers Surface Publishers Current Publishers Surface Publishers Current Publishers Surface Publishers Current Publishers Surface Publishers Current Publishers Surface Publishers Current Publi | Issued To Issued To Issued To It27.0.0.1 AAA Certificate Services Baltimore CyberTrust Root Class 3 Public Primary Cer COMODO RSA Certificati Copyright (c) 1997 Micros DESKTOP-VCKHRG1 DigiCert Assured ID Root DigiCert Assured ID Root DigiCert Global Root CA DigiCert Global Root G2 DigiCert High Assurance DigiCert Trusted Root G4 DigiCert DigiCert Trusted Root G4 DigiCert DigiCert | Issued By 127.0.0.1 AAA Certificate Services Baltimore CyberTrust Root Class 3 Public Primary Cer COMODO RSA Certificati Copyright (c) 1997 Micros DESKTOP-VCKHRG1 DigiCert Assured ID Root DigiCert Assured ID Root DigiCert Global Root CA DigiCert Global Root G2 DigiCert High Assurance DigiCert Trusted Root G4 DCT DCA Y2 ftd-ra-ca-common-name Global Root | Expiration Date 5/17/2027 12/31/2028 5/12/2025 8/1/2028 1/18/2038 12/30/1999 10/30/2022 11/9/2031 11/9/2032 11/9/2031 11/9/2032 11/9/2031 11/9/2032 11/9/2032 11/9/2032 11/9/2032 11/9/2031 11/9/2032 11/9/2029 11/9/2029 11/9/2029 | Intended Purposes Server Authenticati Client Authenticati Client Authenticati Client Authenticati Client Authenticati <all> Client Authenticati Client Authenticati <all> Client Authenticati Client Authenticati Client Authenticati Client Authenticati Client Authenticati Client Authenticati Client Authenticati Client Authenticati</all></all> | Friendly Nan ^ duo-endpoir Sectigo (AA/ DigiCert Balt VeriSign Clas Sectigo (forr Microsoft Tii www.infraey <none> DigiCert DigiCert DigiCert Glol <none> DigiCert Tus DigiCert Trus DST Root CA CNone> GlobalSign R</none></none> | Action Certifie M ftd-ra- M | cates cates ca ore | * } * |
| Do | ventia CA | | | | | | | | |

Bevestig CA

Verifiëren

Stap 1. VPN-verbinding starten

Start in Engineer VPN client de Cisco Secure Client-verbinding. U hoeft de gebruikersnaam en het wachtwoord niet in te voeren, de VPN is met succes verbonden.

| S Cisco Secure Client − □ × | S Cisco Secure Client cert-match X | Sisco Secure Client | - 🗆 X |
|---|--|---|-------------------|
| AnyConnect VPH: Your clent certificate will be used for authentication | Your clent certificate will be used for authentication Group: ftd-cert-match-vpn | AnyConnect VPH: Connected to cert-match. | Disconnect |
| | OK Cancel | 00:00:06 | IPv4 |
| 🔅 🕕 | | \$ (1) | atjaalja CISCO |

VPN-verbinding geslaagd voor Engineer VPN-client

Start in het geval van een VPN-client voor beheer de Cisco Secure Client-verbinding. De VPNverbinding is mislukt vanwege een fout in de certificaatvalidatie.



VPN-verbinding mislukt voor VPN-client voor beheer

Stap 2. VPN-sessies in FTD CLI bevestigen

show vpn-sessiondb detail anyconnect Start de opdracht in FTD (Lina) CLI om de VPN-sessies van engineer te bevestigen.

firepower# show vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

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

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

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

Pkts Tx Drop: 0 Pkts Rx Drop: 0

SSL-Tunnel: Tunnel ID : 32.2 Assigned IP : 172.16.1.150 Public IP : 192.168.1.11 Encryption : AES-GCM-256 Hashing : SHA384 Ciphersuite : ECDHE-RSA-AES256-GCM-SHA384 Encapsulation: TLSv1.2 TCP Src Port : 50177 TCP Dst Port : 443 Auth Mode : Certificate Idle Time Out: 30 Minutes Idle TO Left : 30 Minutes Client OS : Windows Client Type : SSL VPN Client Client Ver : Cisco AnyConnect VPN Agent for Windows 5.1.4.74 Bytes Tx : 7359 Bytes Rx : 12919 Pkts Tx : 1 Pkts Rx : 51 Pkts Tx Drop : 0 Pkts Rx Drop : 0

Problemen oplossen

U kunt informatie over VPN-verificatie verwachten in de debug-syslog van Lina engine en in het DART-bestand op Windows-computer.

Dit is een voorbeeld van debug logs in de Lina engine tijdens VPN verbinding van engineer client.

Jul 02 2024 04:16:03: %FTD-7-717029: Identified client certificate within certificate chain. serial number: 7AF1C78ADCC8F941, subject name: CN=vpn Jul 02 2024 04:16:03: %FTD-6-717022: Certificate was successfully validated. serial number: 7AF1C78ADCC8F941, subject name: CN=vpnEngineerClient Jul 02 2024 04:16:04: %FTD-6-113009: AAA retrieved default group policy (ftd-cert-match-grp) for user = vpnEngineerClientCN Jul 02 2024 04:16:09: %FTD-6-725002: Device completed SSL handshake with client outside:192.168.1.11/50158 to 192.168.1.200/443 for TLSv1.2 sessi

Gerelateerde informatie

FDM On-Box Management Service configureren voor Firepower 2100Remote Access VPN configureren op FTD beheerde via FDMSyslog configureren en controleren in Firepower Device Manager

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.