Lokale LAN-toegang configureren voor beveiligde client

Inhoud

Inleiding

Dit document beschrijft hoe u Cisco Secure Client kunt configureren voor toegang tot het lokale LAN en toch een beveiligde verbinding met de head-end kunt onderhouden.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben over deze onderwerpen:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Firepower Threat Defence (FTD)
- Cisco Secure-client (CSC)

Gebruikte componenten

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

- Cisco Secure Firewall Management Center virtuele applicatie versie 7.3
- Cisco Firepower Threat Defense virtuele applicatie versie 7.3
- Cisco Secure-client versie 5.0.02075

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

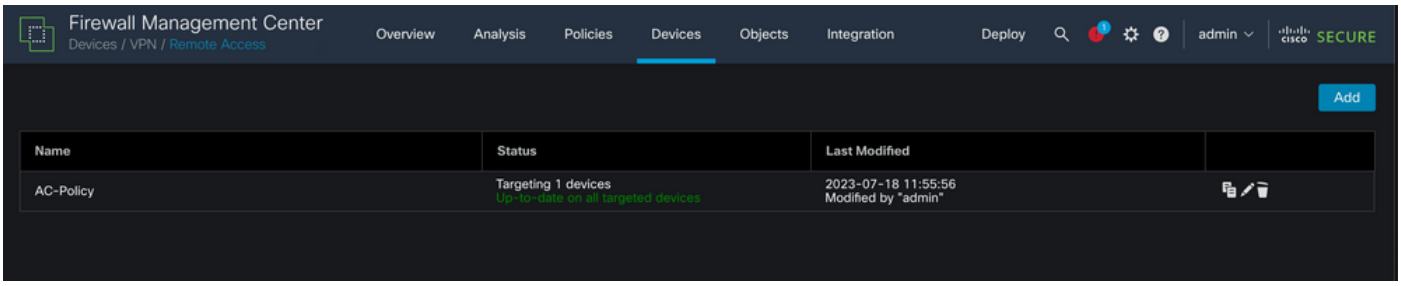
De configuratie die in dit document wordt beschreven, maakt het mogelijk voor Cisco Secure Client om volledige toegang tot het lokale LAN te hebben, terwijl er nog steeds een beveiligde verbinding met de head-end en bedrijfsresources is. Hiermee kan de client worden gebruikt om een Network Access Server (NAS) af te drukken of te openen.

Configureren

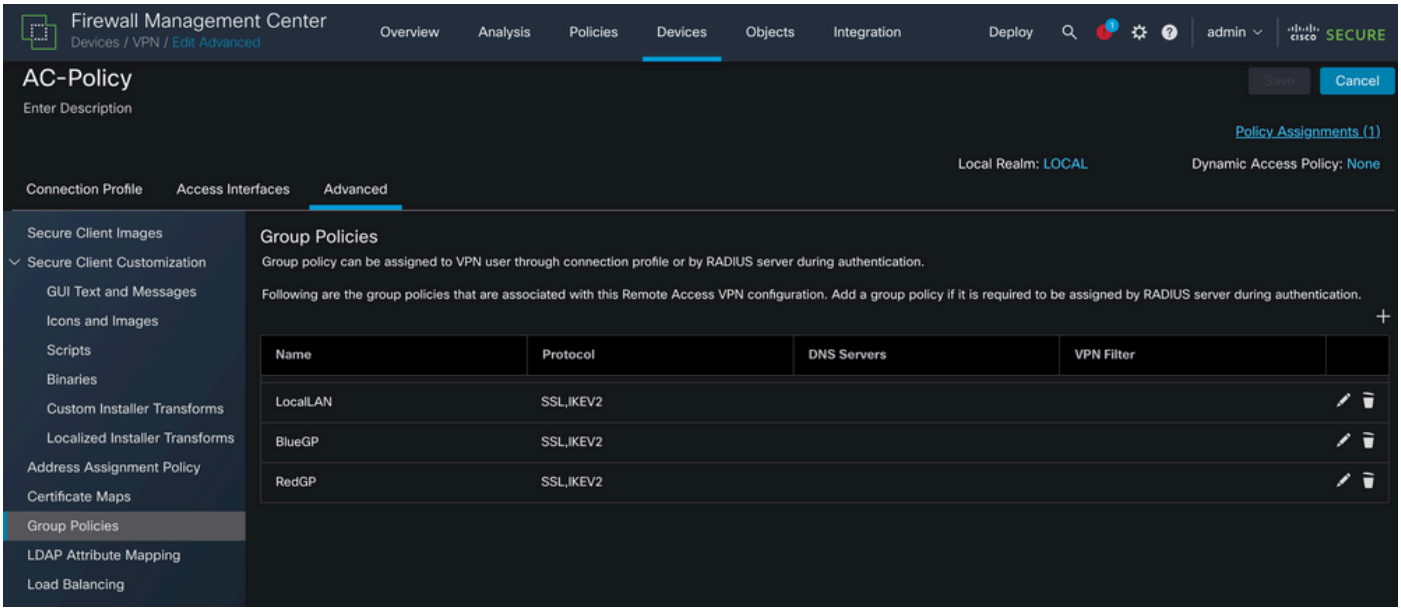
FMC-configuratie

In dit document wordt aangenomen dat u al een werkende Remote Access VPN-configuratie hebt.

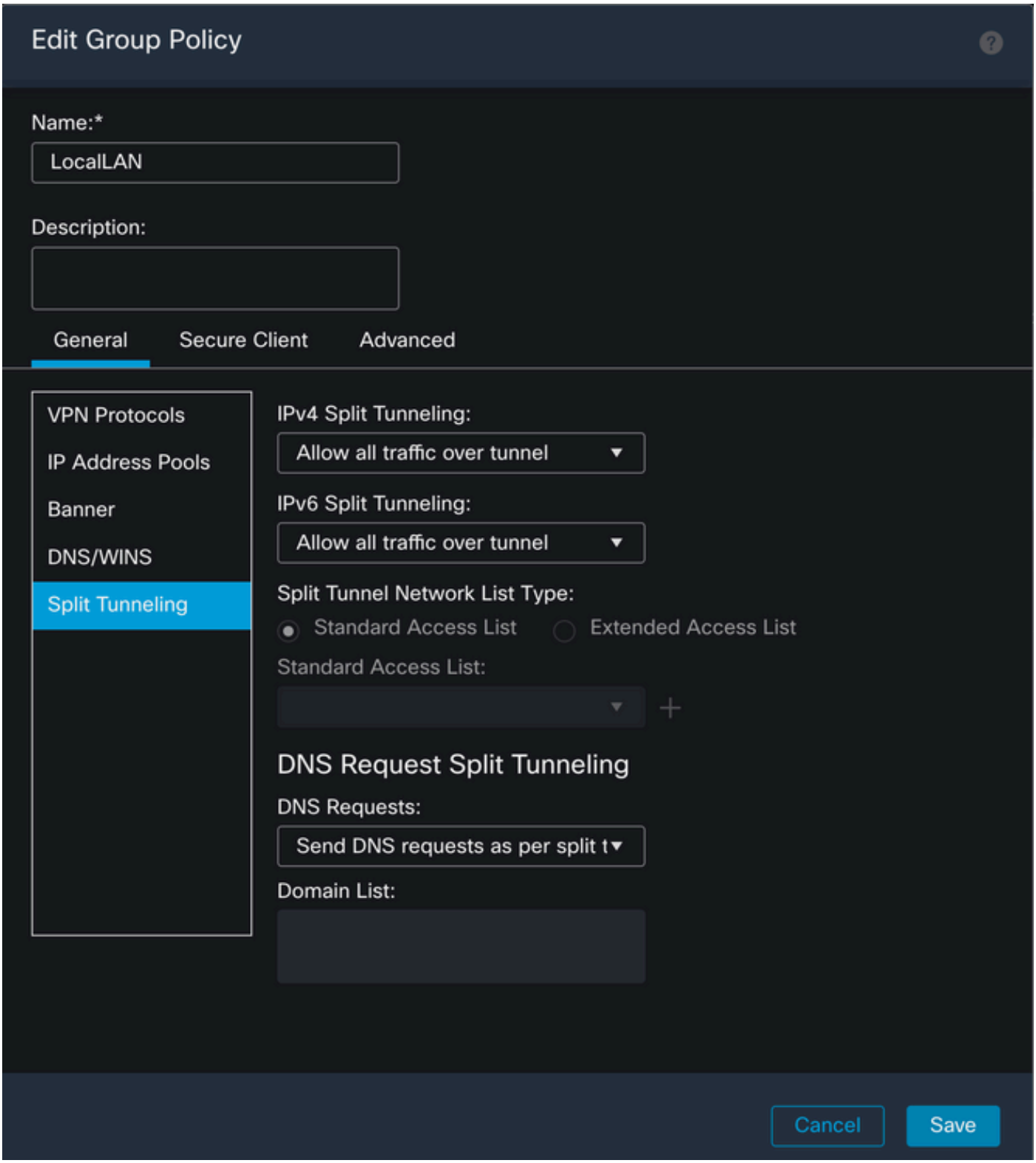
Als u de lokale LAN-toegangsmogelijkheid wilt toevoegen, navigeert u naar Apparaten > Externe toegang en klikt u op de knop Bewerken in het juiste beleid voor externe toegang.



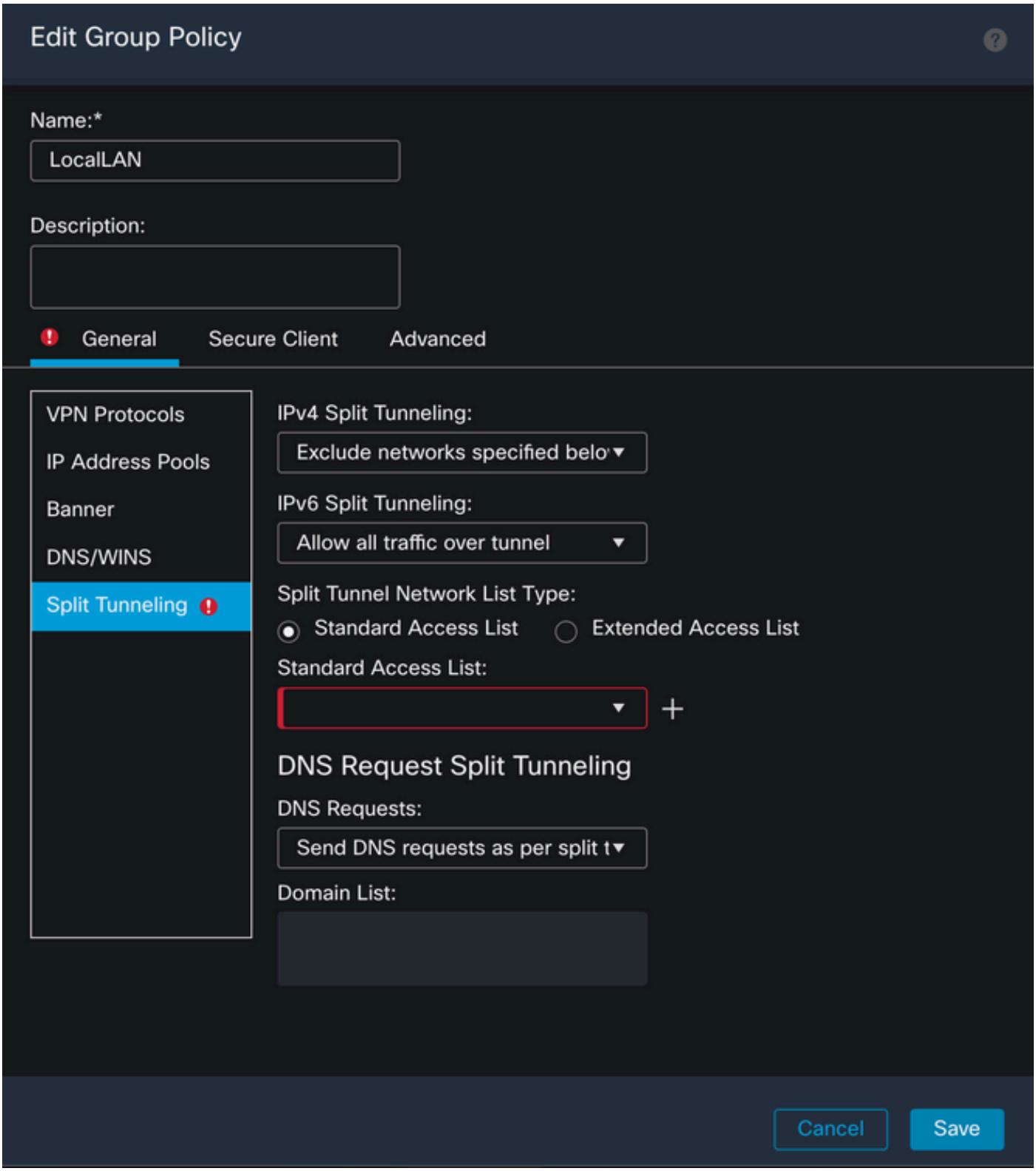
Blader vervolgens naar Geavanceerd > Groepsbeleid.



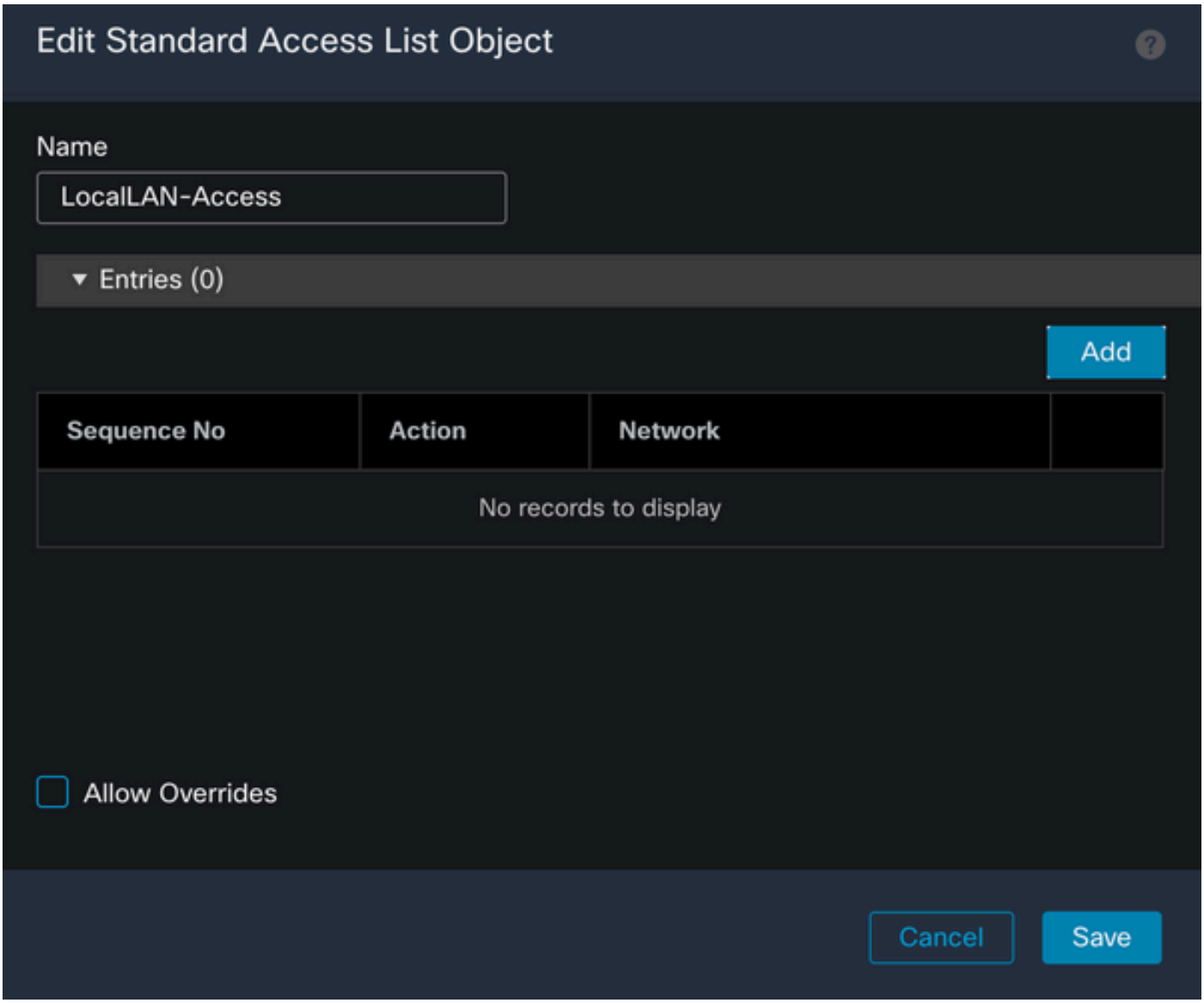
Klik op de knop Bewerken in het groepsbeleid waar u lokale LAN-toegang wilt configureren en naar het tabblad Split-tunneling wilt navigeren.



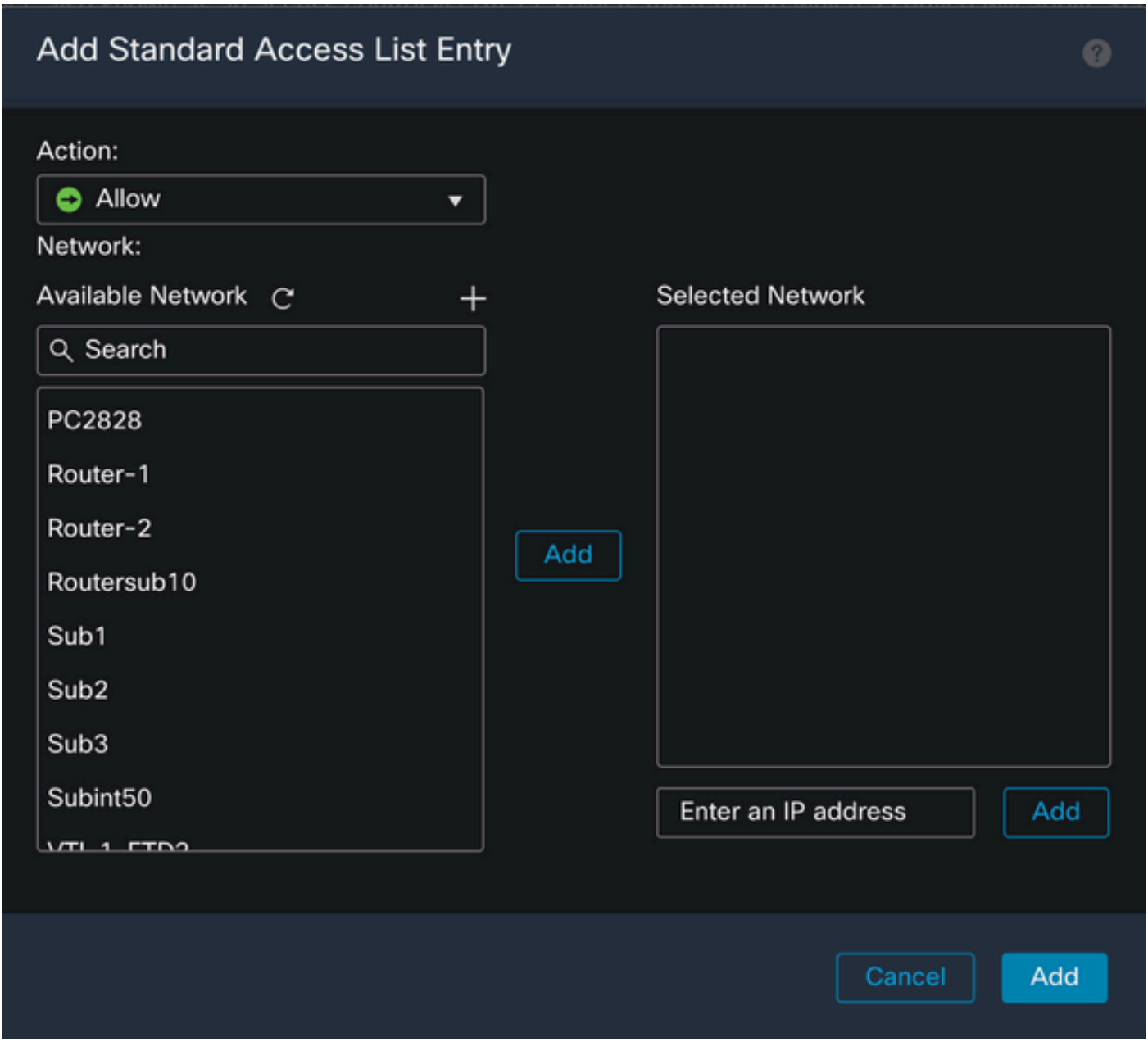
Selecteer in het gedeelte IPv4 Split-tunneling de optie Netwerken uitsluiten die hieronder zijn gespecificeerd. Dit vraagt om een selectie standaard toegangslijst.



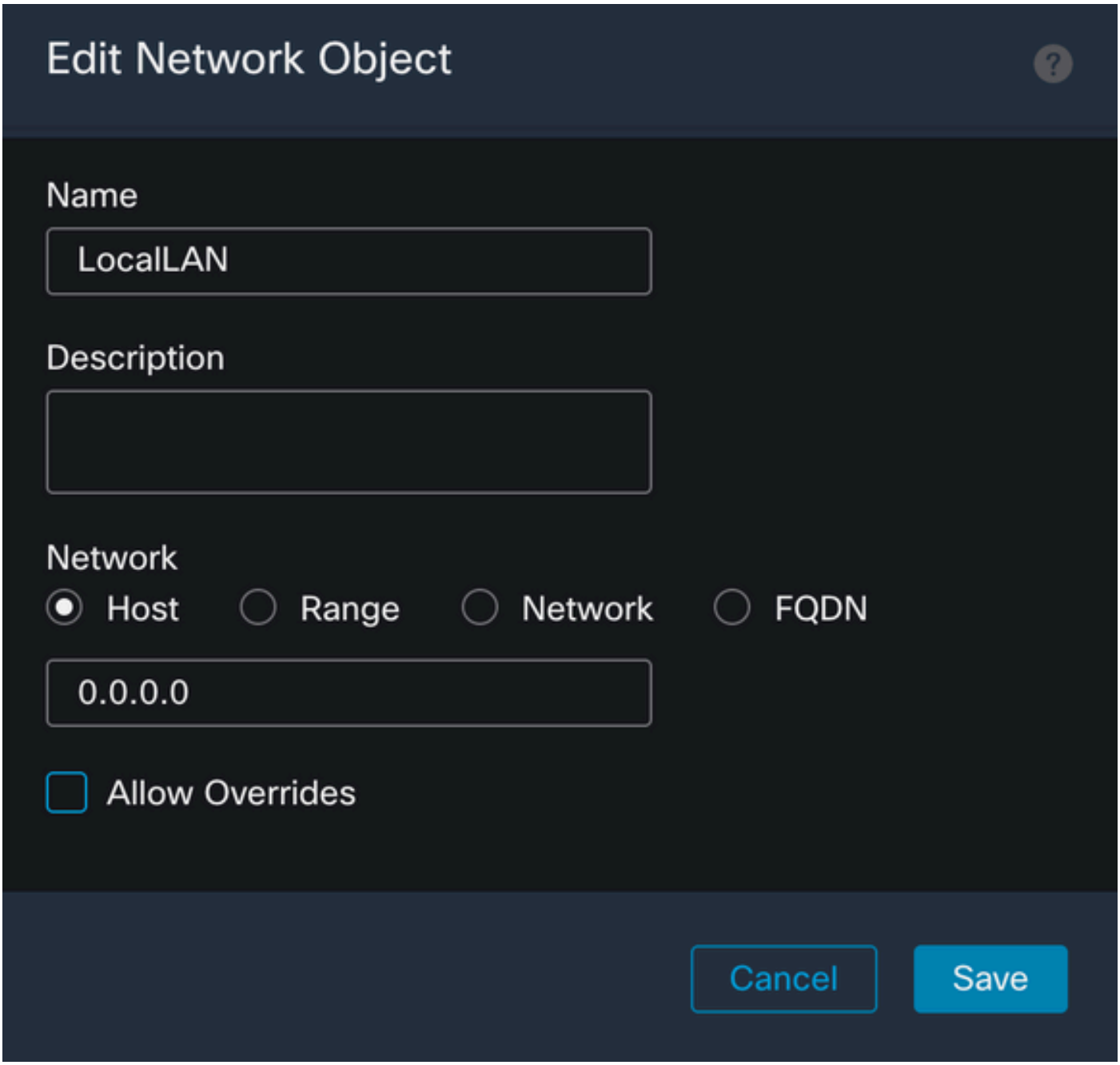
Klik op de knop + om een nieuwe standaardtoegangslijst te maken.



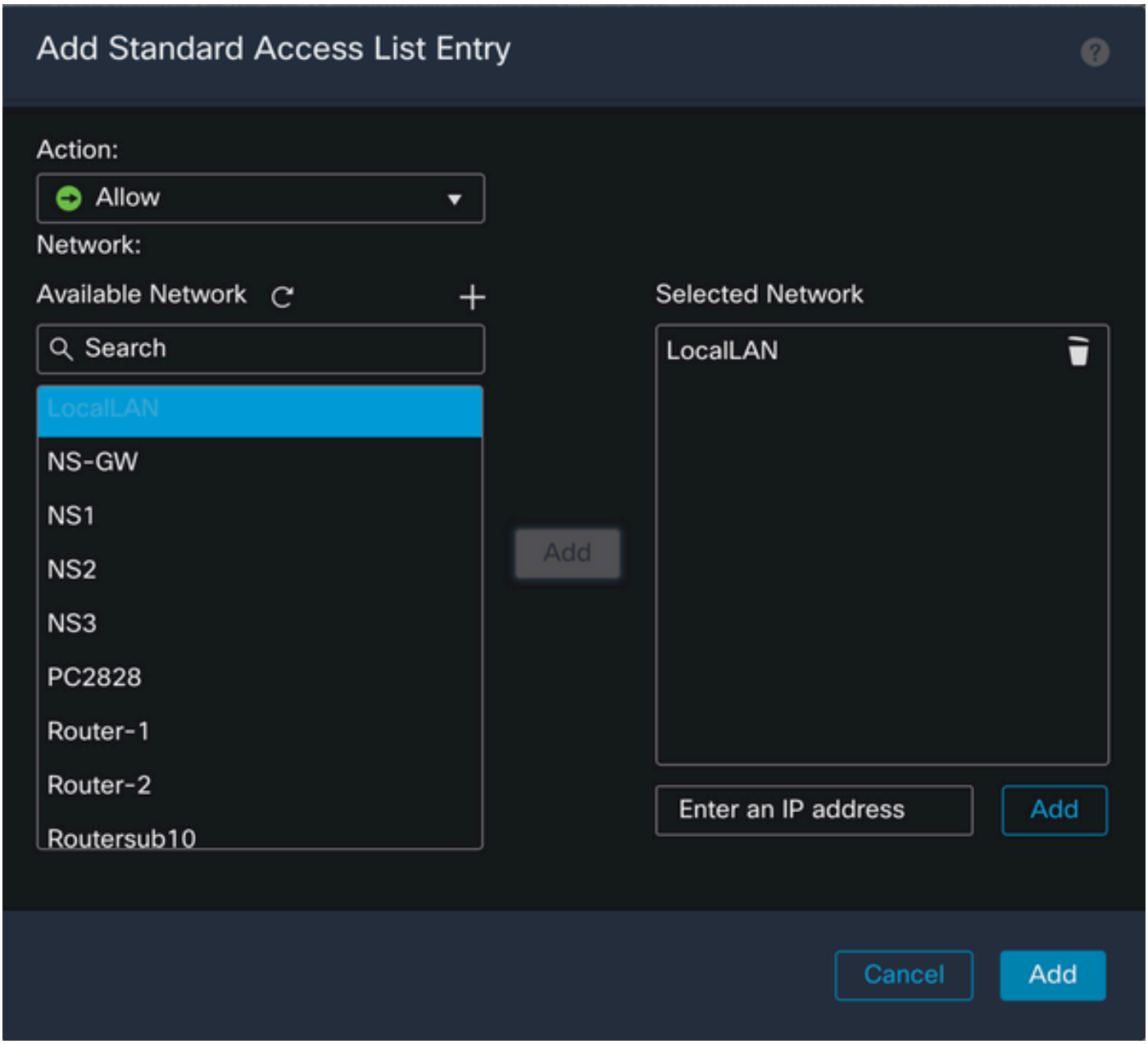
Klik op de knop Add om een standaard toegangslijst te maken. De handeling van dit item moet worden ingesteld op Toestaan.



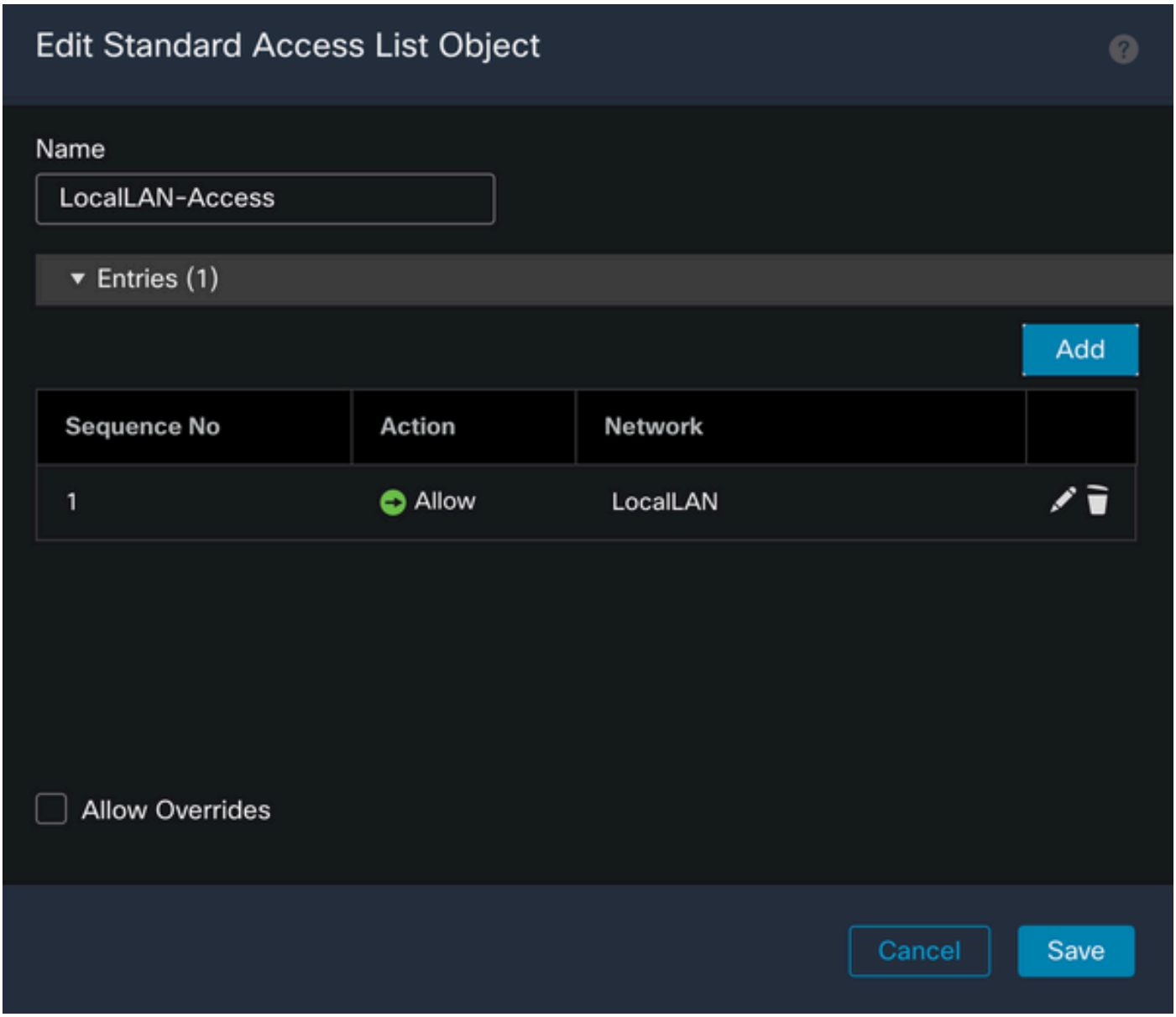
Klik op de knop + om een nieuw netwerkobject toe te voegen. Zorg ervoor dat dit object is ingesteld als host in het vak Netwerk en voer 0.0.0.0 in het vak in.



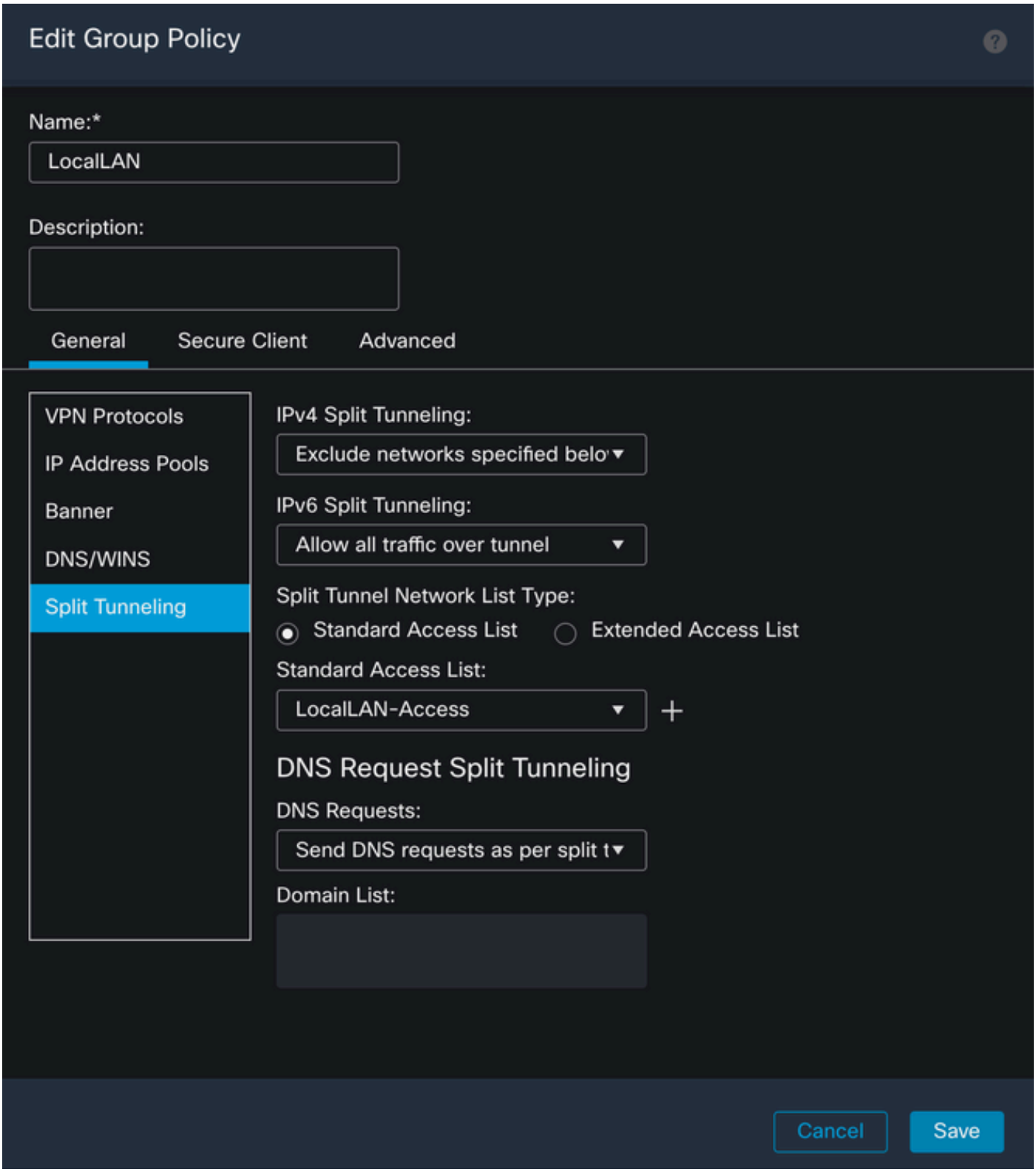
Klik op de knop Opslaan en selecteer het nieuwe object.



Klik op de knop Add om de ingang voor de standaard toegangslijst op te slaan.



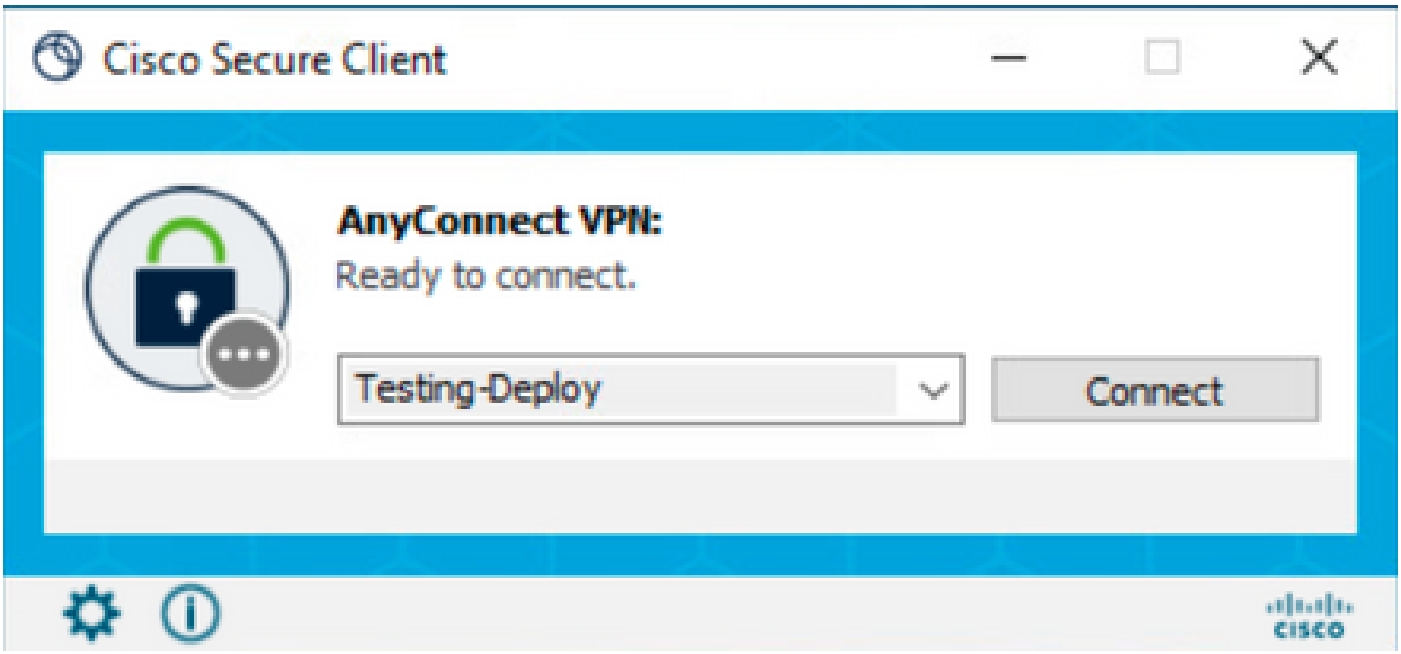
Klik op de knop Opslaan en de nieuwe standaardtoegangslijst wordt automatisch geselecteerd.



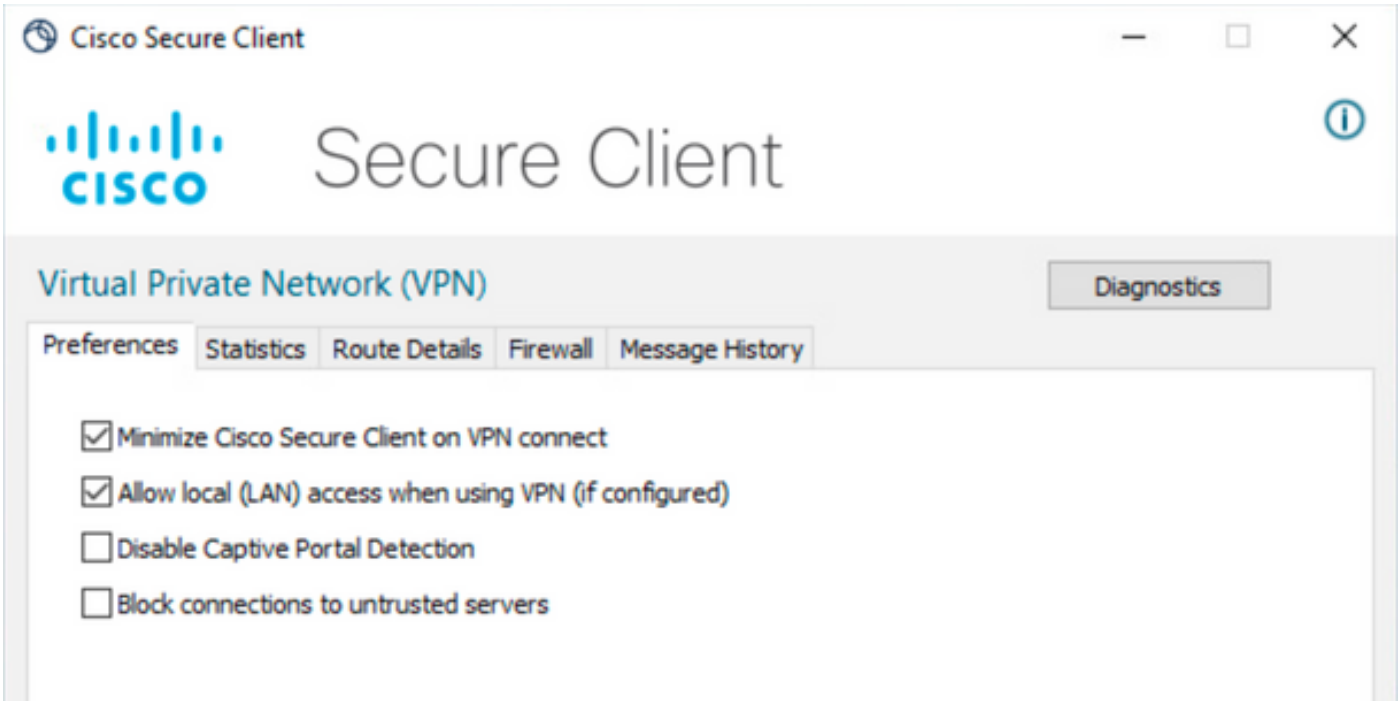
Klik op de knop Opslaan en voer de wijzigingen in.

Beveiligde clientconfiguratie

De standaardinstelling is dat de optie Local LAN Access is ingesteld op User Controlable (Gebruikerscontrole). Als u de optie wilt inschakelen, klikt u op het pictogram Gear in de Secure Client GUI.



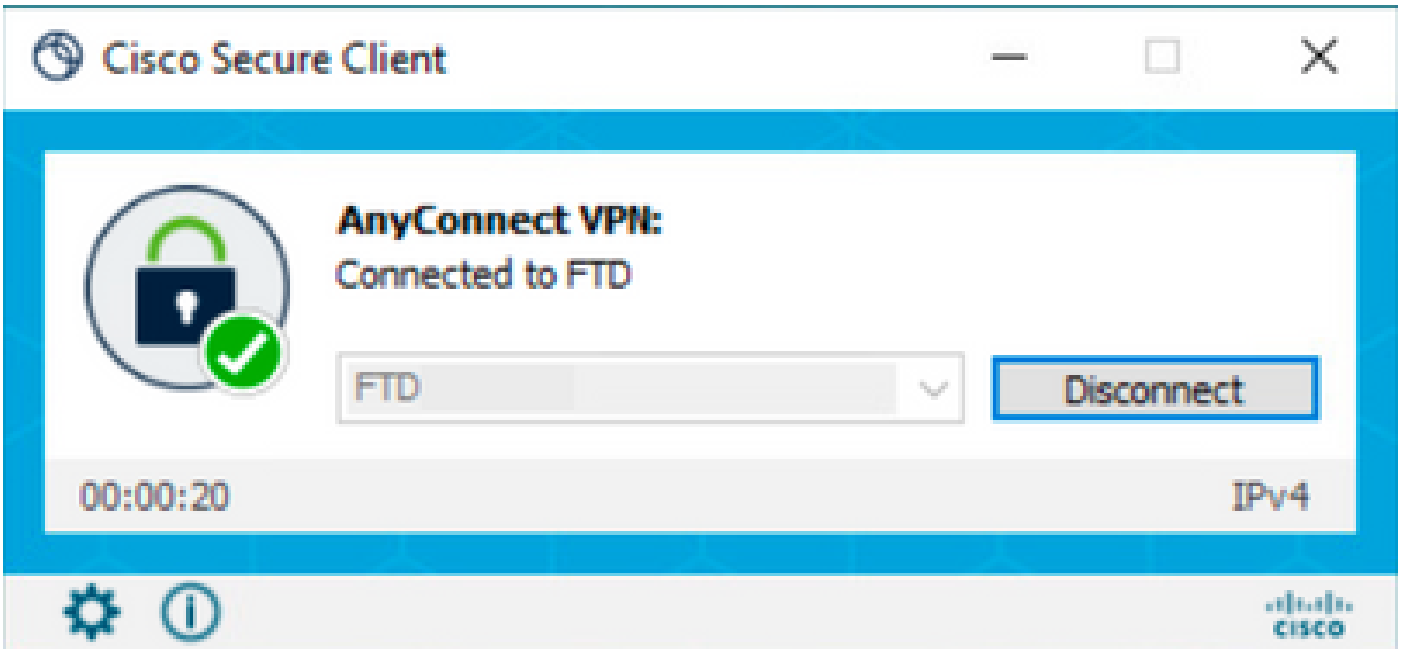
Navigeer naar Voorkeuren en zorg ervoor dat de optie Lokale (LAN) toegang toestaan bij gebruik van VPN (indien geconfigureerd) is ingeschakeld.



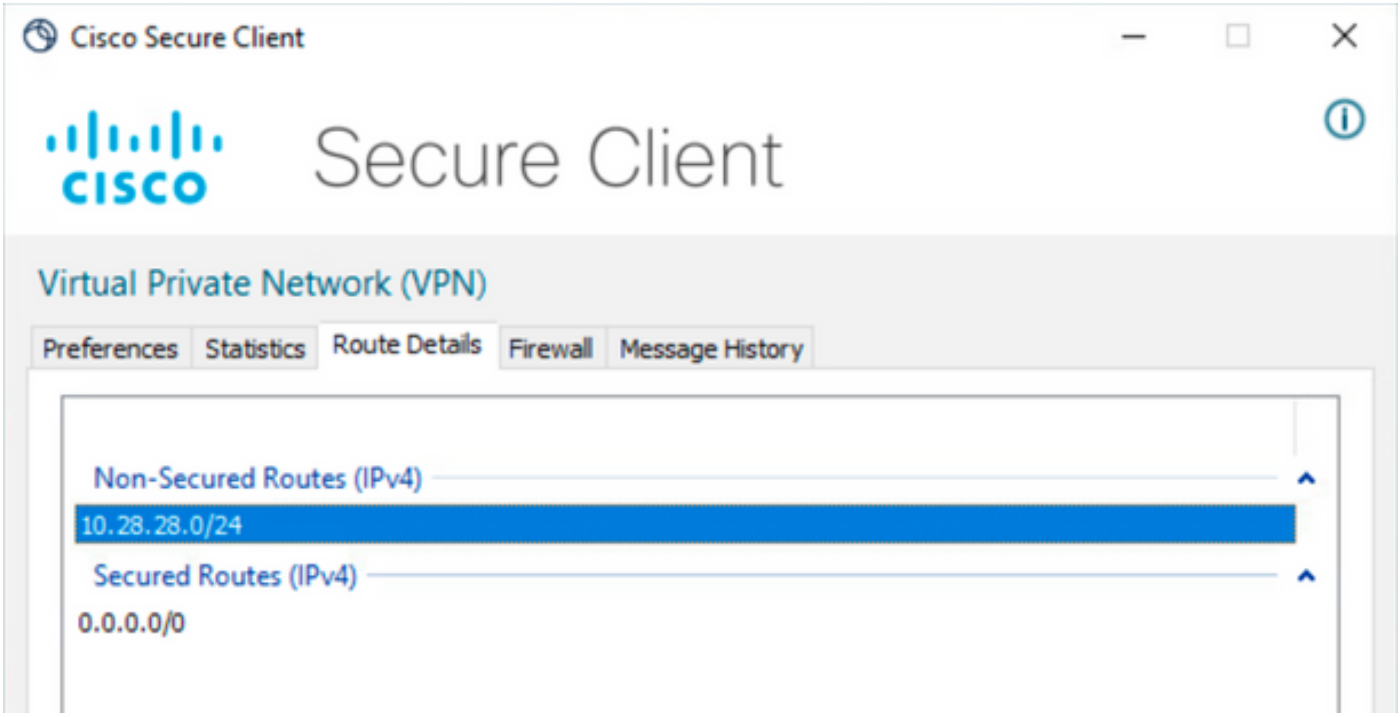
Verifiëren

Beveiligde client

Verbinding met de head-end maken met de beveiligde client.



Klik op het tandwielpictogram en navigeer naar routegegevens. Hier kunt u zien dat het lokale LAN automatisch wordt gedetecteerd en uitgesloten van de tunnel.



FTD CLI

Om te verifiëren of de configuratie met succes is toegepast, kunt u de CLI van de FTD gebruiken.

<#root>

```
firepower#
```

```
show running-config group-policy LocalLAN
```

```
group-policy LocalLAN internal
group-policy LocalLAN attributes
banner value Local LAN Access is allowed
wins-server none
dns-server none
dhcp-network-scope none
vpn-simultaneous-logins 3
vpn-idle-timeout 30
vpn-idle-timeout alert-interval 1
vpn-session-timeout none
vpn-session-timeout alert-interval 1
vpn-filter none
vpn-tunnel-protocol ikev2 ssl-client
```

split-tunnel-policy excludespecified

```
ipv6-split-tunnel-policy tunnelall
```

split-tunnel-network-list value LocalLAN-Access

```
default-domain none
split-dns none
split-tunnel-all-dns disable
client-bypass-protocol disable
vlan none
address-pools value AC_Pool
webvpn
anyconnect ssl dtls enable
anyconnect mtu 1406
anyconnect firewall-rule client-interface public none
anyconnect firewall-rule client-interface private none
anyconnect ssl keepalive 20
anyconnect ssl rekey time none
anyconnect ssl rekey method none
anyconnect dpd-interval client 30
anyconnect dpd-interval gateway 30
anyconnect ssl compression none
anyconnect dtls compression none
anyconnect modules value none
anyconnect ask none default anyconnect
anyconnect ssl df-bit-ignore disable
```

Problemen oplossen

Om te controleren of de functie voor lokale LAN-toegang is toegepast, kunt u deze debugs inschakelen:

```
debug webvpn anyconnect 255
```

Dit is een voorbeeld van een succesvolle debug-uitvoer:

<#root>

```
firepower# debug webvpn anyconnect 255
Validating the session cookie...
Processing CSTP header line: 'webvpn=5E1823@15949824@D2CF@BF38A398B90D09039C60B55929055D33AE31BA05'
Found WebVPN cookie: 'webvpn=5E1823@15949824@D2CF@BF38A398B90D09039C60B55929055D33AE31BA05'
WebVPN Cookie: 'webvpn=5E1823@15949824@D2CF@BF38A398B90D09039C60B55929055D33AE31BA05'
Cookie validation successfull, session authenticated
http_parse_cstp_method()
...input: 'CONNECT /CSCOSSLC/tunnel HTTP/1.1'
webvpn_cstp_parse_request_field()
...input: 'Host: ftdv-cehidalg.cisco.com'
Processing CSTP header line: 'Host: ftdv-cehidalg.cisco.com'
webvpn_cstp_parse_request_field()
...input: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 5.0.02075'
Processing CSTP header line: 'User-Agent: Cisco AnyConnect VPN Agent for Windows 5.0.02075'
Setting user-agent to: 'Cisco AnyConnect VPN Agent for Windows 5.0.02075'
webvpn_cstp_parse_request_field()
...input: 'Cookie: webvpn=5E1823@15949824@D2CF@BF38A398B90D09039C60B55929055D33AE31BA05'
Processing CSTP header line: 'Cookie: webvpn=5E1823@15949824@D2CF@BF38A398B90D09039C60B55929055D33AE31BA
Session already authenticated, skip cookie validation
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Version: 1'
Processing CSTP header line: 'X-CSTP-Version: 1'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Hostname: DESKTOP-LPMOG6M'
Processing CSTP header line: 'X-CSTP-Hostname: DESKTOP-LPMOG6M'
Setting hostname to: 'DESKTOP-LPMOG6M'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-MTU: 1399'
Processing CSTP header line: 'X-CSTP-MTU: 1399'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Address-Type: IPv6,IPv4'
Processing CSTP header line: 'X-CSTP-Address-Type: IPv6,IPv4'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Local-Address-IP4: 10.28.28.7'
Processing CSTP header line: 'X-CSTP-Local-Address-IP4: 10.28.28.7'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Base-MTU: 1500'
Processing CSTP header line: 'X-CSTP-Base-MTU: 1500'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Remote-Address-IP4: 10.28.28.10'
Processing CSTP header line: 'X-CSTP-Remote-Address-IP4: 10.28.28.10'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Full-IPv6-Capability: true'
Processing CSTP header line: 'X-CSTP-Full-IPv6-Capability: true'
webvpn_cstp_parse_request_field()
...input: 'X-AnyConnect-STRAP-Pubkey: MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEkzG6nj9HDKz/zLa3Yz+QJDHOYWfT6
Processing CSTP header line: 'X-AnyConnect-STRAP-Pubkey: MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEkzG6nj9HDK
Setting Anyconnect STRAP rekey public key(len: 124): MFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAEkzG6nj9HDKz/zL
webvpn_cstp_parse_request_field()
...input: 'X-AnyConnect-STRAP-Verify: MEQCICzX1yDWLXQHnlOhOXV+/OI1/OlLjBic/Nu/K2+N6E5GAiA5CLAF6Bt0tcxhj
Processing CSTP header line: 'X-AnyConnect-STRAP-Verify: MEQCICzX1yDWLXQHnlOhOXV+/OI1/OlLjBic/Nu/K2+N6E
Setting Anyconnect STRAP client signature(len: 96): MEQCICzX1yDWLXQHnlOhOXV+/OI1/OlLjBic/Nu/K2+N6E5GAiA
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Master-Secret: 0224D83639071BBF29E2D77B15B762FE85BD50D1F0EF9758942B75DF9A97C709325C3E
Processing CSTP header line: 'X-DTLS-Master-Secret: 0224D83639071BBF29E2D77B15B762FE85BD50D1F0EF975894
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-RSA-AES128-GCM-SHA25
Processing CSTP header line: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-R
Skipping cipher selection using DTLSv1 since a higher version is set in ssl configuration
webvpn_cstp_parse_request_field()
...input: 'X-DTLS12-CipherSuite: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AE
```

```
Processing CSTP header line: 'X-DTLS12-CipherSuite: ECDHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-
Selecting cipher using DTLSv1.2
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Accept-Encoding: lzs'
Processing CSTL header line: 'X-DTLS-Accept-Encoding: lzs'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: lzs,deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lzs,deflate'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
Processing CSTP header line: 'X-CSTP-Protocol: Copyright (c) 2004 Cisco Systems, Inc.'
cstp_util_address_ipv4_accept: address asigned: 172.16.28.15
cstp_util_address_ipv6_accept: No IPv6 Address
np_svc_create_session(0xF36000, 0x000014d37b17c080, TRUE)
webvpn_svc_np_setup
SVC ACL Name: NULL
SVC ACL ID: -1
No SVC ACL
Iphdr=20 base-mtu=1500 def-mtu=1500 conf-mtu=1406
tcp-mss = 1460
path-mtu = 1460(mss)
TLS Block size = 16, version = 0x304
mtu = 1460(path-mtu) - 0(opts) - 5(ssl) = 1455
mod-mtu = 1455(mtu) & 0xfff0(complement) = 1440
tls-mtu = 1440(mod-mtu) - 8(cstp) - 32(mac) - 1(pad) = 1399
DTLS Block size = 16
mtu = 1500(base-mtu) - 20(ip) - 8(udp) - 13(dtlshdr) - 16(dtlsiv) = 1443
mod-mtu = 1443(mtu) & 0xfff0(complement) = 1440
dtls-mtu = 1440(mod-mtu) - 1(cdtp) - 48(mac) - 1(pad) = 1390
computed tls-mtu=1399 dtls-mtu=1390 conf-mtu=1406
DTLS enabled for intf=2 (outside)
tls-mtu=1399 dtls-mtu=1390
SVC: adding to sessmgmt
```

Sending X-CSTP-Split-Exclude msgs: for ACL - LocalLAN-Access: Start

Sending X-CSTP-Split-Exclude: 0.0.0.0/255.255.255.255

```
Sending X-CSTP-MTU: 1399
Sending X-DTLS-MTU: 1390
Sending X-DTLS12-CipherSuite: ECDHE-ECDSA-AES256-GCM-SHA384
Sending X-CSTP-FW-RULE msgs: Start
Sending X-CSTP-FW-RULE msgs: Done
Sending X-CSTP-Quarantine: false
Sending X-CSTP-Disable-Always-On-VPN: false
Sending X-CSTP-Client-Bypass-Protocol: false
```

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.