# Configurar o acesso de LAN local para cliente seguro

## Contents

[Introdução](#)
[Pré-requisitos](#)
[Requisitos](#)
[Componentes Utilizados](#)
[Informações de Apoio](#)
[Configurar](#)
[configuração de FMC](#)
[Configuração do Secure Client](#)
[Verificar](#)
[Cliente seguro](#)
[CLI de FTD](#)
[Troubleshooting](#)

## Introdução

Este documento descreve como configurar o Cisco Secure Client para acessar a LAN local e ainda manter uma conexão segura com o headend.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento sobre estes tópicos:

- Cisco Secure Firewall Management Center (FMC)
- Defesa contra ameaças (FTD) do Cisco Firepower
- Cisco Secure Client (CSC)

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure Firewall Management Center Virtual Appliance Versão 7.3
- Dispositivo virtual Cisco Firepower Threat Defense versão 7.3
- Cisco Secure Client Versão 5.0.02075

As informações neste documento foram criadas a partir de dispositivos em um ambiente de

laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

# Informações de Apoio

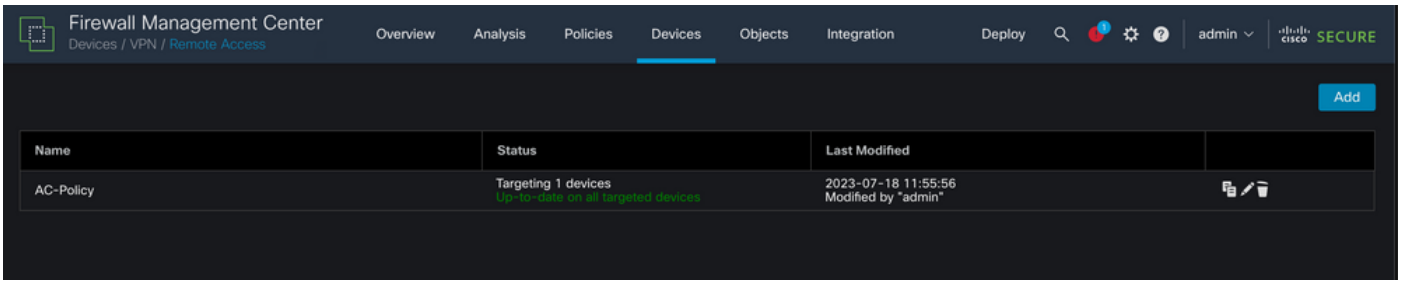
A configuração descrita neste documento permite que o Cisco Secure Client tenha acesso total à LAN local enquanto mantém uma conexão segura com o headend e os recursos corporativos. Isso pode ser usado para permitir que o cliente imprima ou acesse um Servidor de Acesso à Rede (NAS).

# Configurar

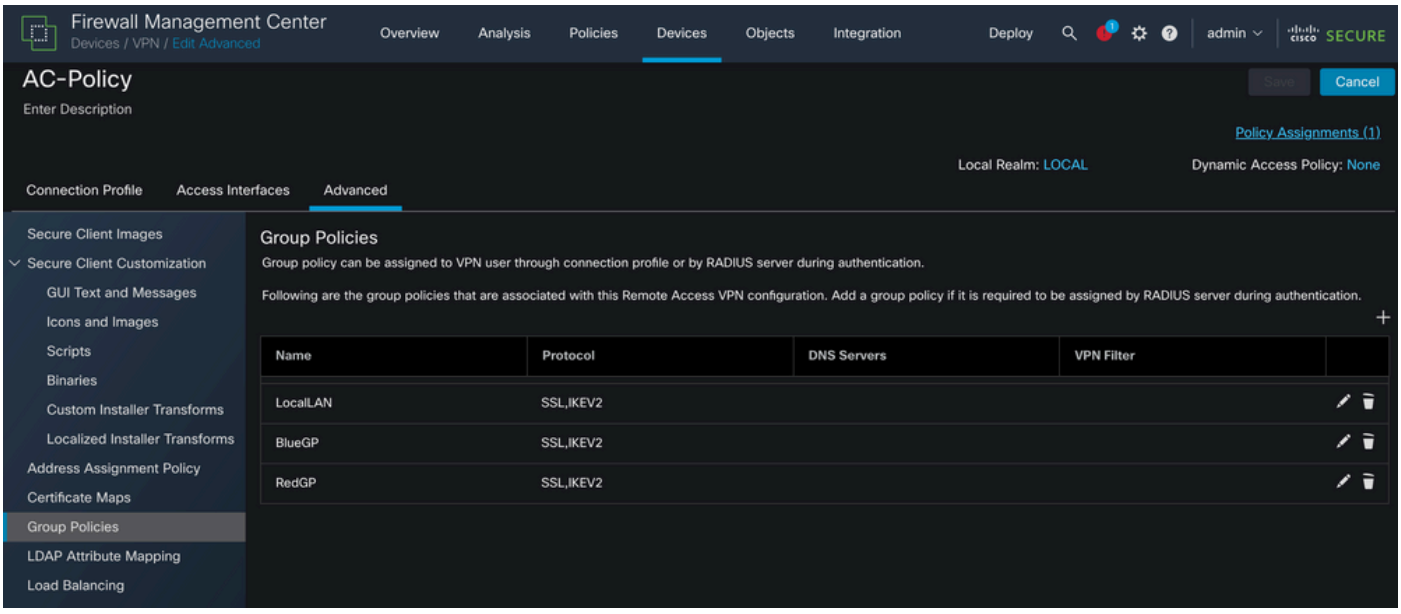
## configuração de FMC

Neste documento, supõe-se que você já tenha uma configuração de VPN de acesso remoto em funcionamento.

Para adicionar o recurso de acesso à LAN local, navegue para Devices > Remote Access e clique no botão Edit na política de acesso remoto apropriada.

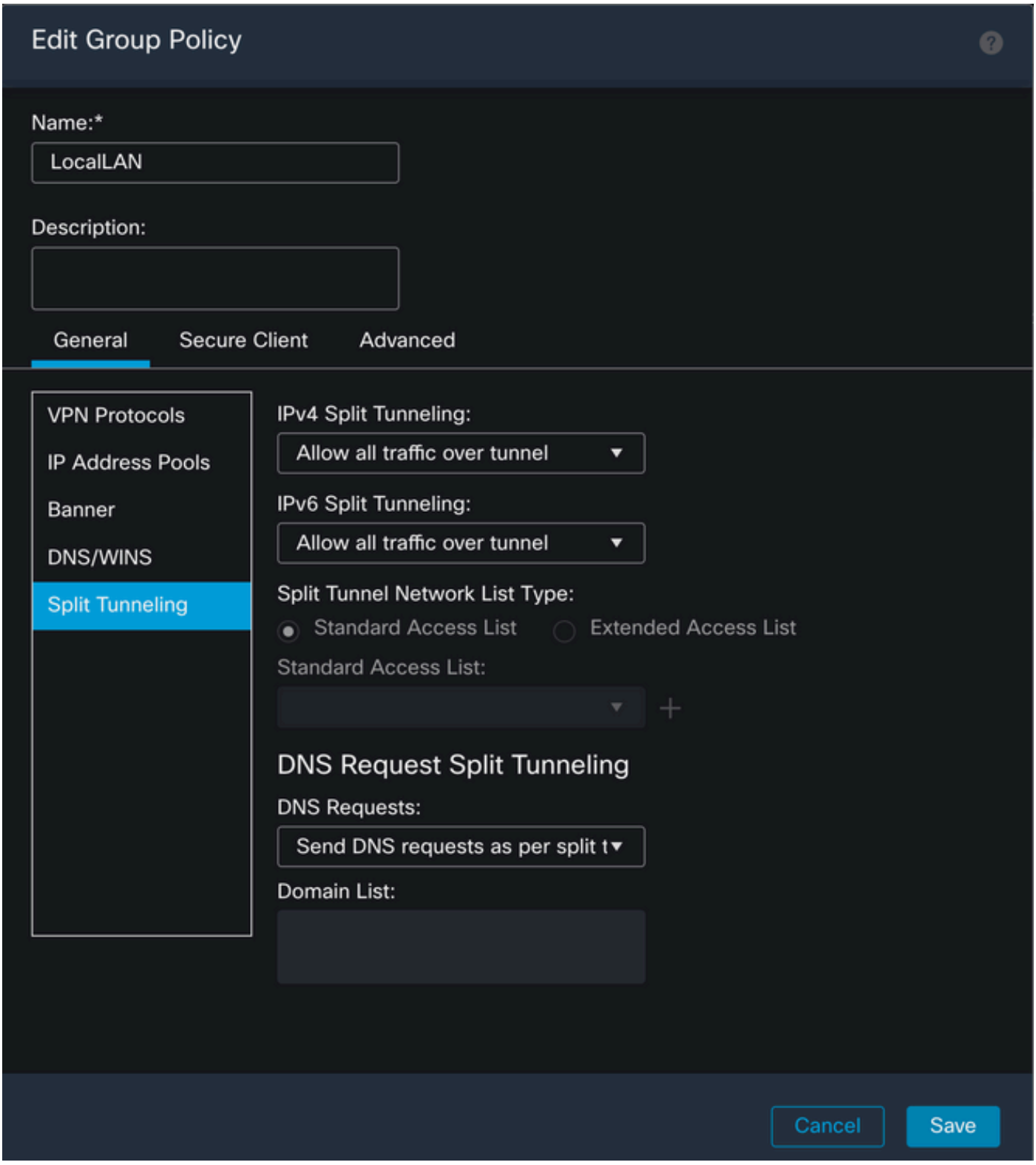



Em seguida, navegue até Avançado > Políticas de grupo.

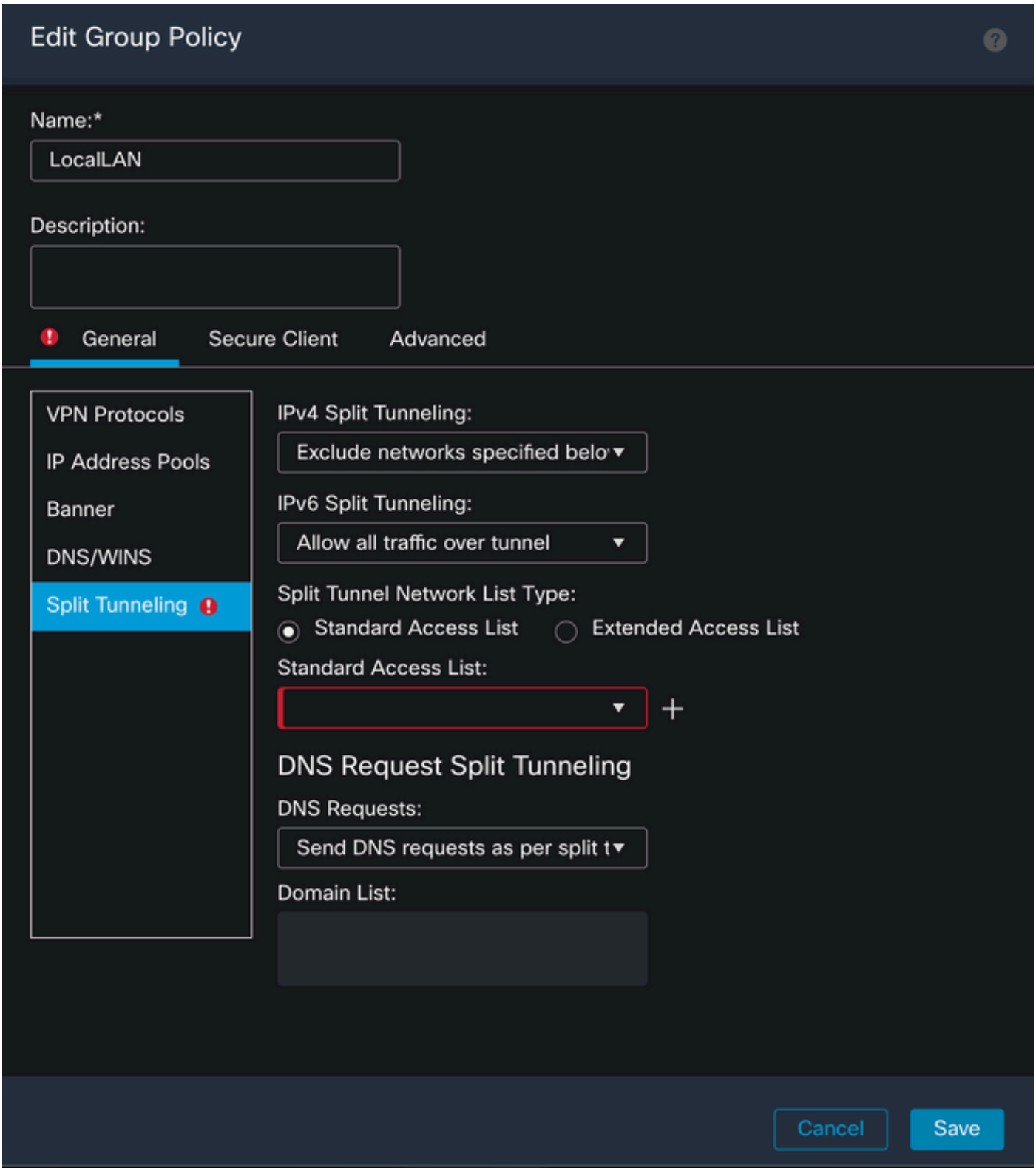



Clique no botão Edit na Group Policy onde você deseja configurar Local LAN Access e navegue

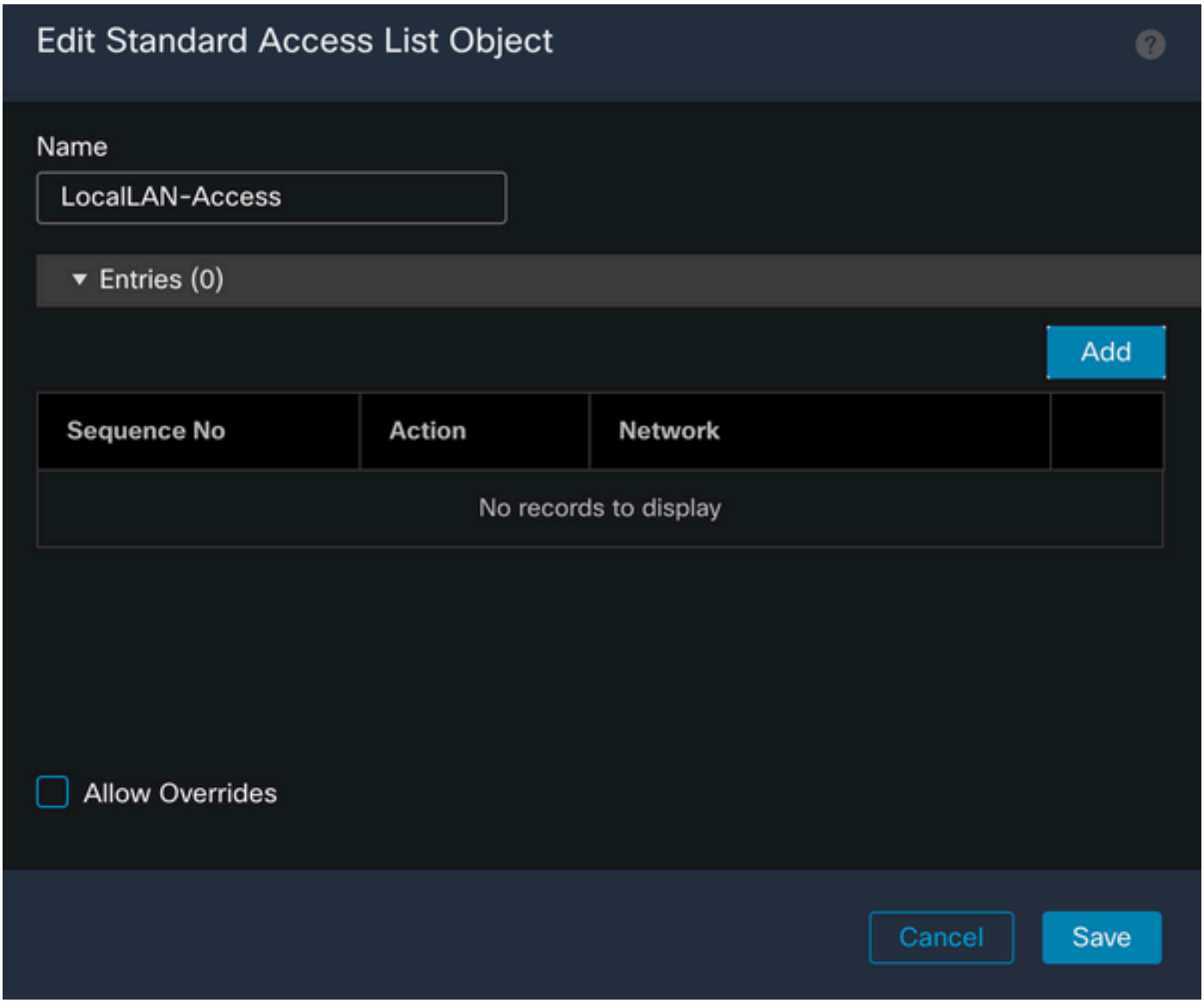
até a guia Split Tunneling.



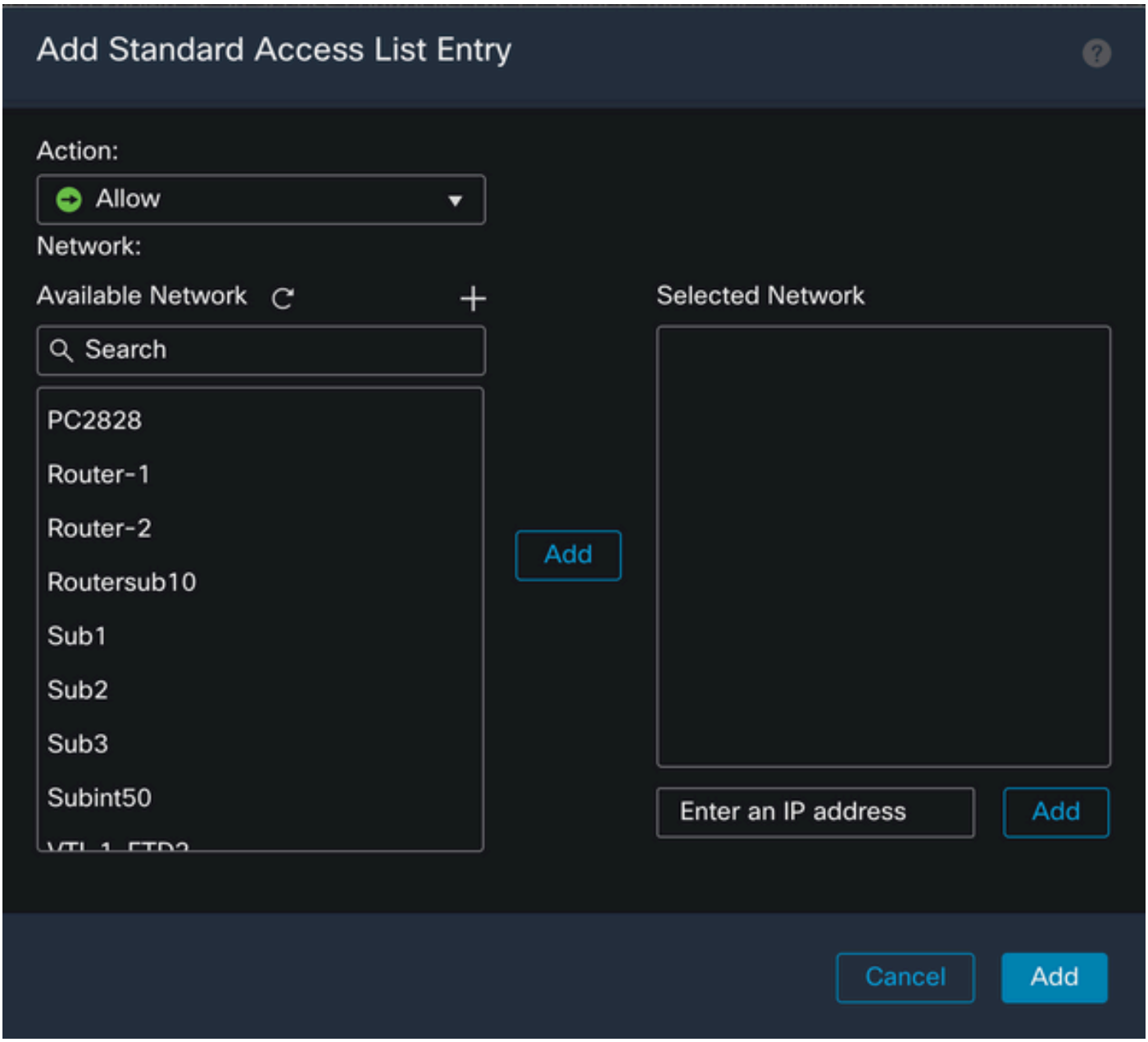

Na seção IPv4 Split Tunneling, selecione a opção Excluir redes especificadas abaixo. Isso solicita uma seleção de Lista de acesso padrão.



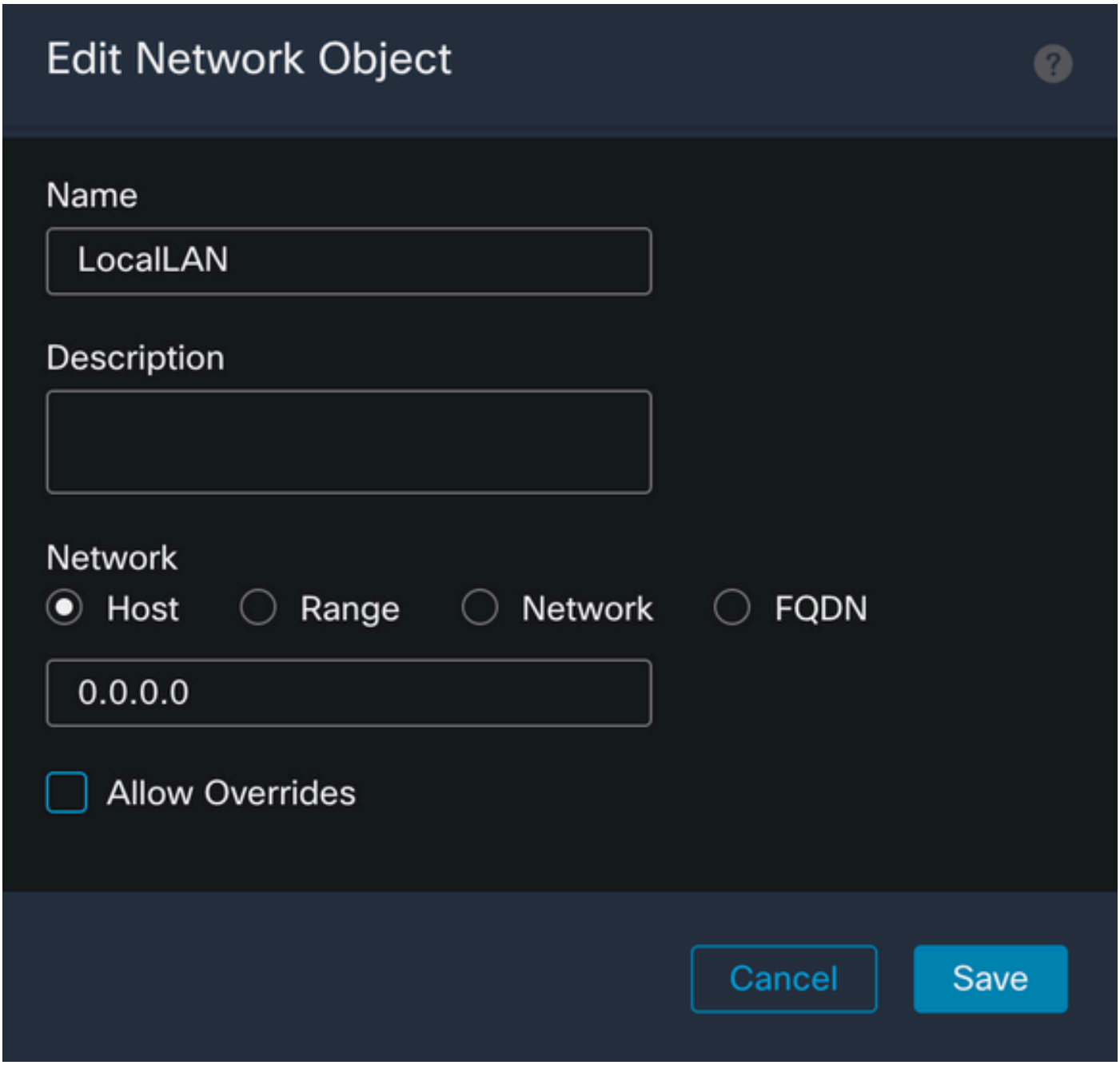

Clique no botão + para criar uma nova Lista de acesso padrão.



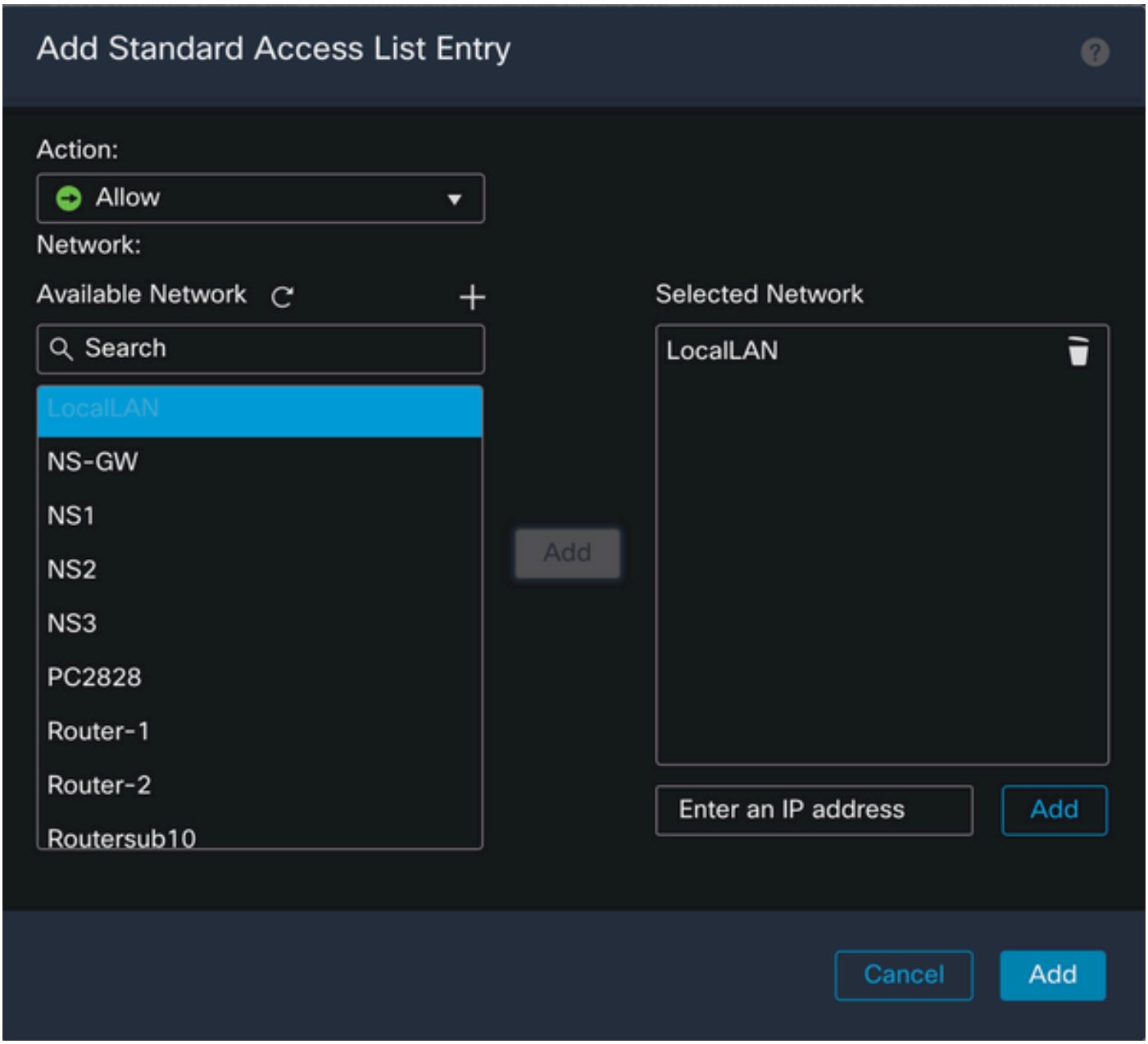

Clique no botão Adicionar para criar uma Entrada de Lista de Acesso Padrão. A Ação desta entrada deve ser definida como Permitir.



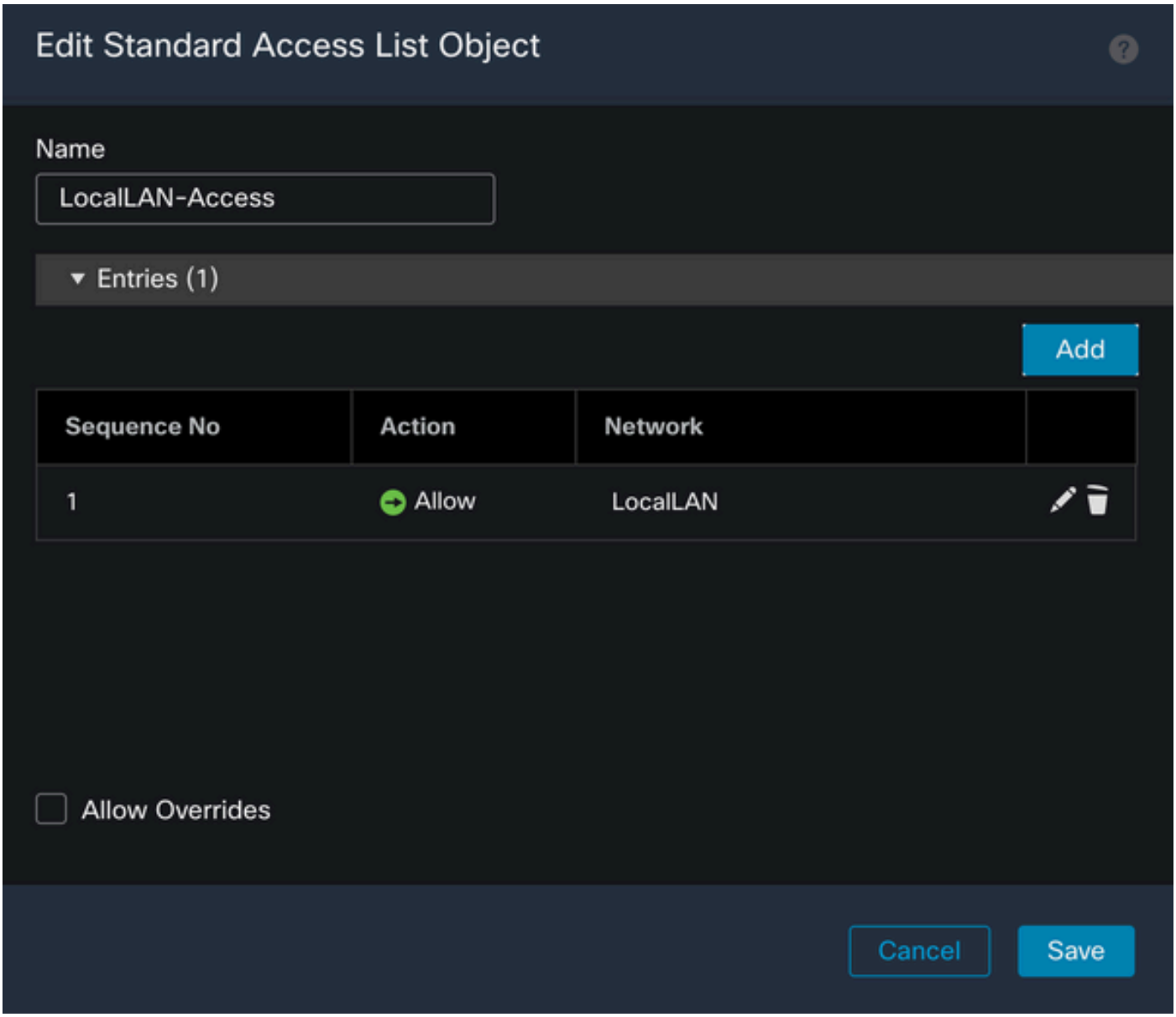

Clique no botão + para adicionar um novo objeto de rede. Certifique-se de que esse objeto esteja definido como um Host na seção Rede e digite 0.0.0.0 na caixa.



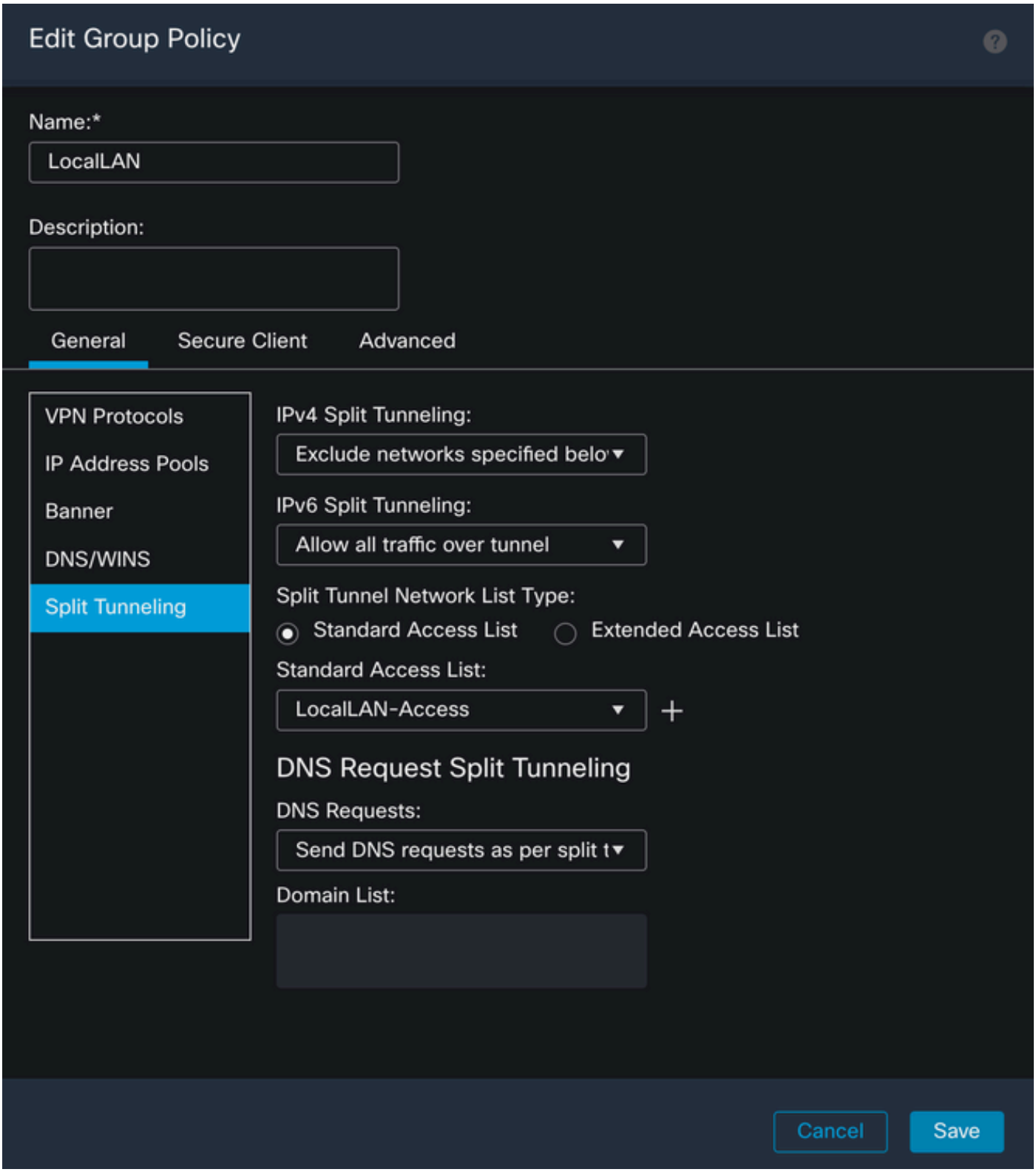

Clique no botão Salvar e selecione o objeto recém-criado.




Clique no botão Add para salvar a entrada da lista de acesso padrão.



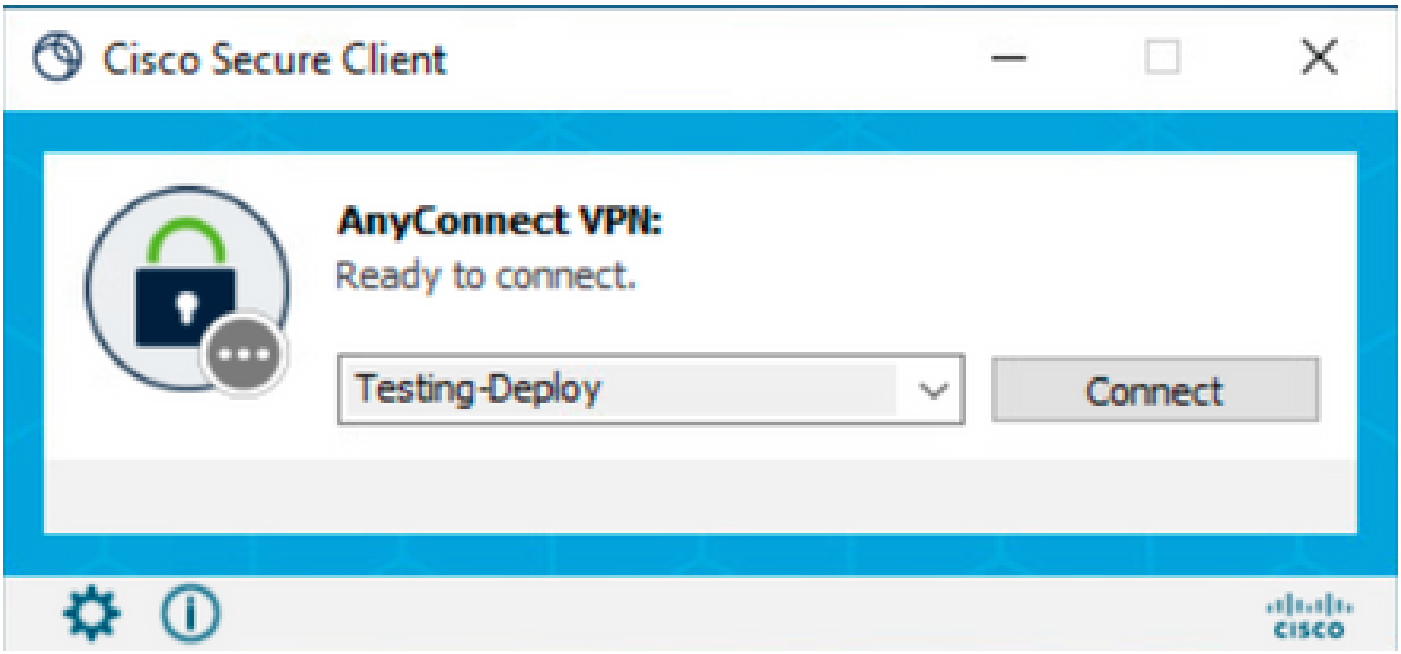

Clique no botão Salvar e a lista de acesso padrão recém-criada será selecionada automaticamente.



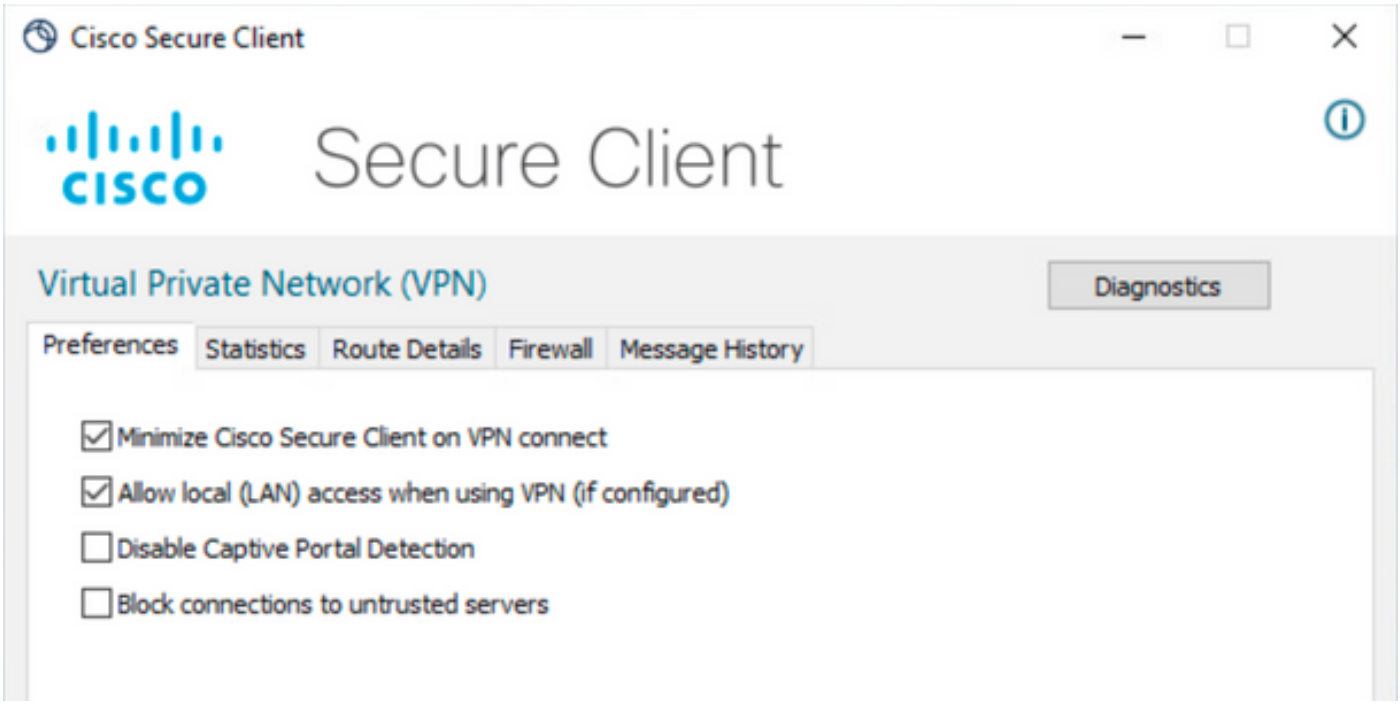

Clique no botão Save e implante as alterações.

## Configuração do Secure Client

Por padrão, a opção Local LAN Access é definida como User Controllable. Para habilitar a opção, clique no ícone Gear na GUI do Secure Client.



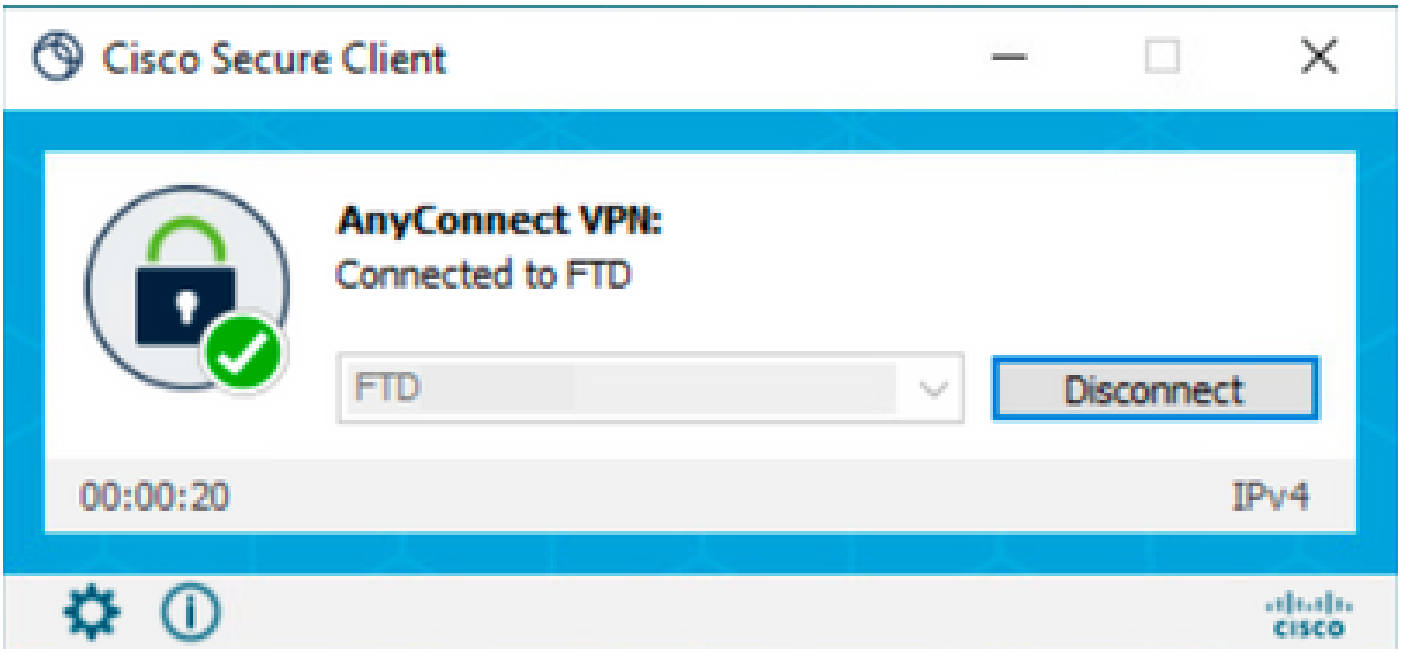

Navegue até Preferences e verifique se a opção Allow local (LAN) access when using VPN (if configured) está habilitada.



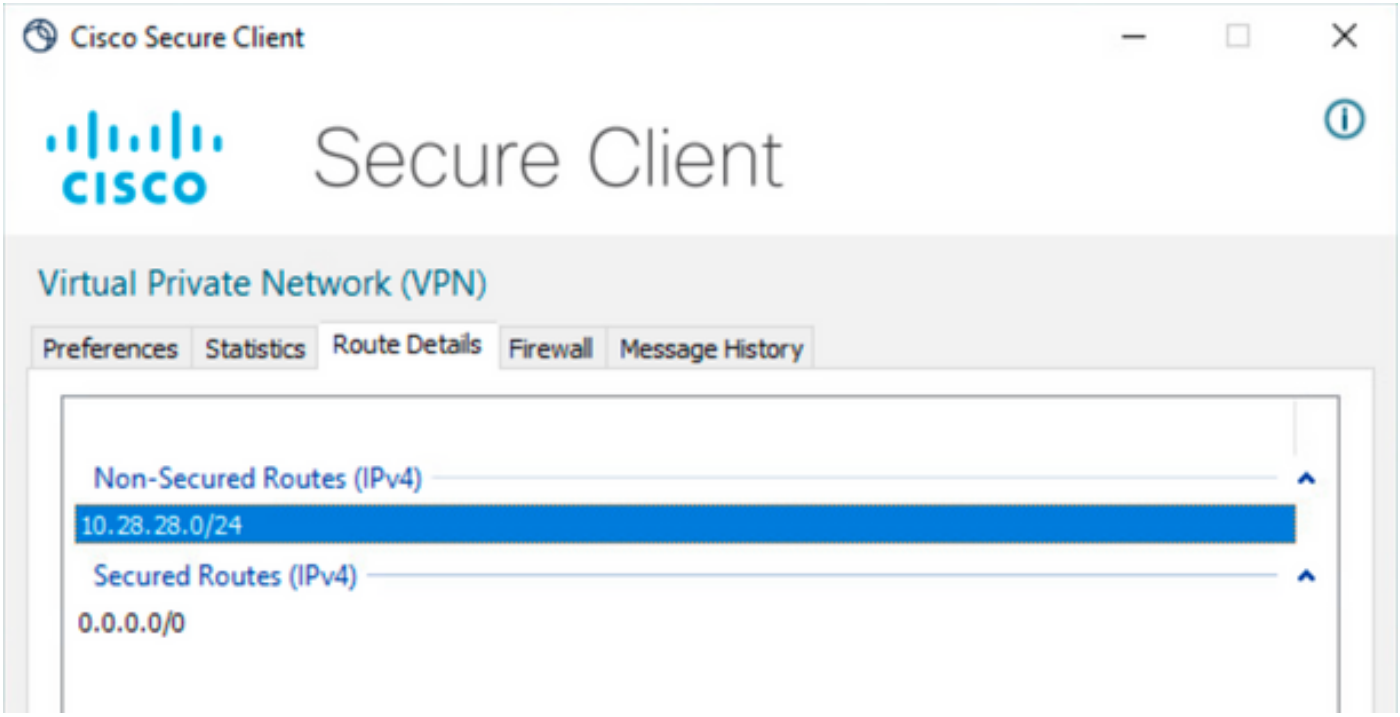

# Verificar

## Cliente seguro

Conecte ao headend usando o Secure Client.




Clique no ícone de engrenagem e navegue até Detalhes da rota. Aqui você pode ver que a LAN local é automaticamente detectada e excluída do túnel.




## CLI de FTD

Para verificar se a configuração foi aplicada com êxito, você pode usar a CLI do FTD.

<#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
```

# Troubleshooting

Para verificar se o recurso de acesso à LAN local foi aplicado, você pode habilitar estas depurações:

```
debug webvpn anyconnect 255
```

Este é um exemplo de uma saída de depuração bem-sucedida:

<#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
```

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.