# Configure Local LAN Access for Secure Client

## Contents

Introduction
Prerequisites
Requirements
Components Used
Background Information
Configure
FMC configuration
Secure Client configuration
Verify
Secure Client
FTD CLI
Troubleshoot

## Introduction

This document describes how to configure Cisco Secure Client to access the Local LAN and still maintain a secure connection to the headend.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge on these topics:

- Cisco Secure Firewall Management Center (FMC)
- Cisco Firepower Threat Defense (FTD)
- Cisco Secure Client (CSC)

### Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Firewall Management Center Virtual Appliance Version 7.3
- Cisco Firepower Threat Defense Virtual Appliance Version 7.3
- Cisco Secure Client Version 5.0.02075

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

## Background Information

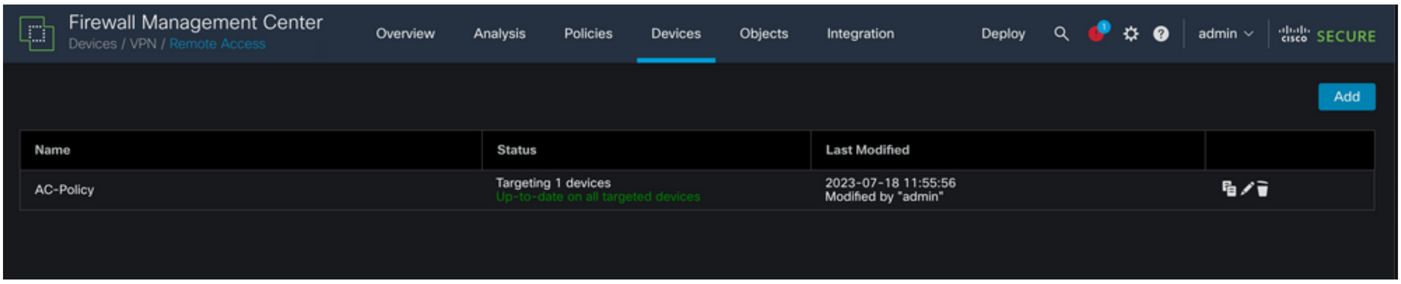
The configuration described on this document allows Cisco Secure Client to have full access to the local LAN while still maintaining a secure connection to the headend and corporate resources. This can be used to allow the client to print or access a Network Access Server (NAS).

# Configure

## FMC configuration

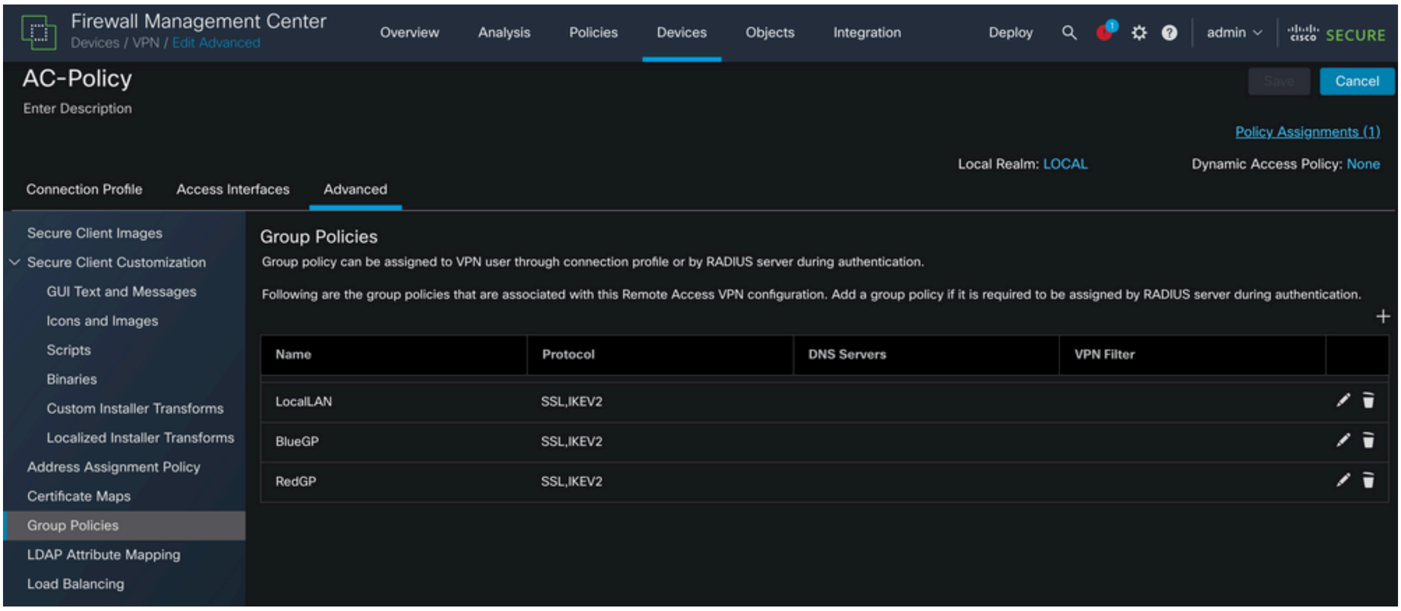
In this document, it is assumed that you already have a working Remote Access VPN configuration.

To add the Local LAN access capability, navigate to **Devices** > **Remote Access** and click the **Edit** button on the appropriate Remote Access policy.



| Name | Status | Last Modified |
|---|---|---|
| AC-Policy | Targeting 1 devices<br>Up-to-date on all targeted devices | 2023-07-18 11:55:56<br>Modified by "admin" |

Then, navigate to **Advanced** > **Group Policies.**



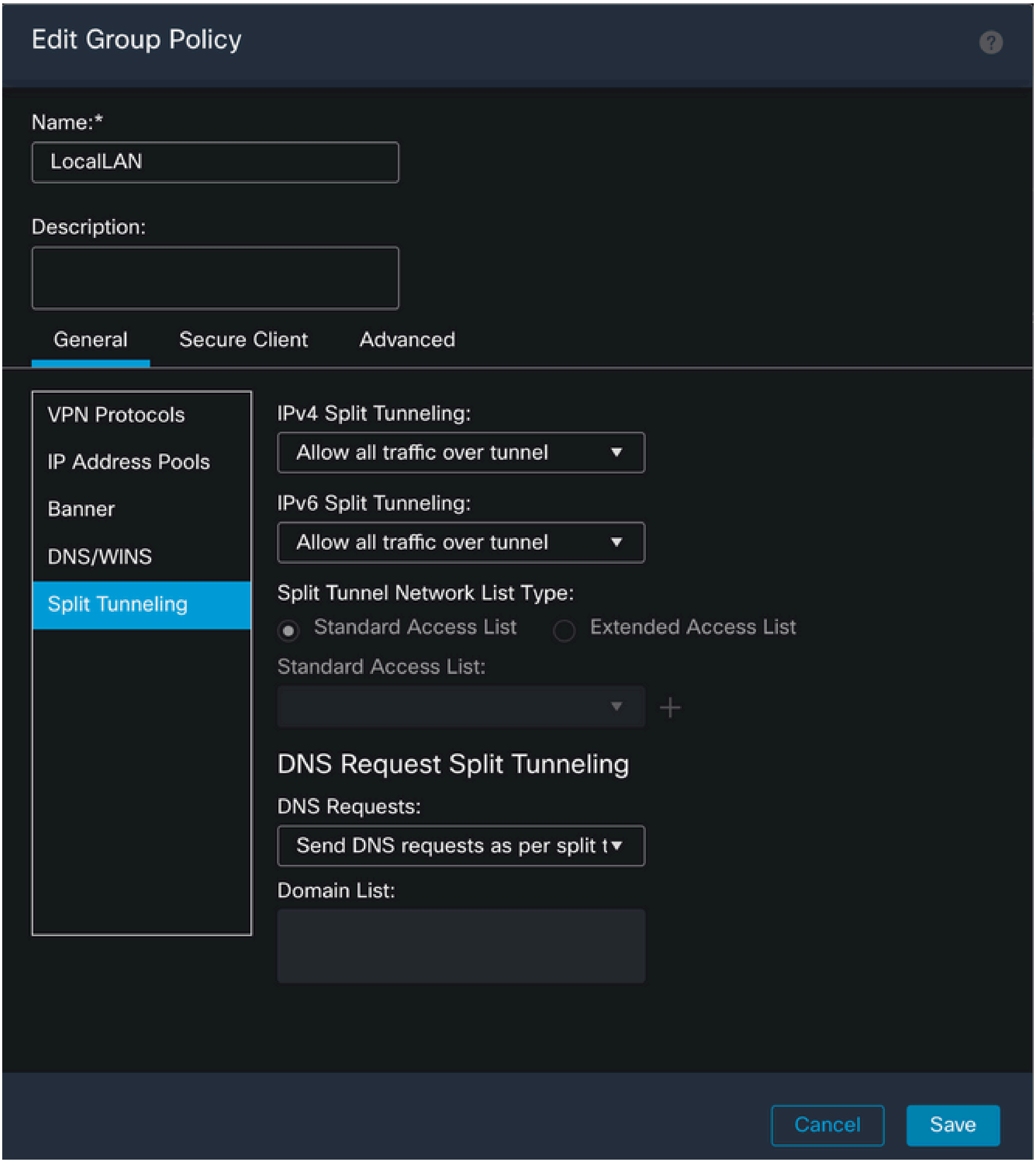
Group Policies

Group policy can be assigned to VPN user through connection profile or by RADIUS server during authentication.

Following are the group policies that are associated with this Remote Access VPN configuration. Add a group policy if it is required to be assigned by RADIUS server during authentication.

| Name | Protocol | DNS Servers | VPN Filter |
|---|---|---|---|
| LocalLAN | SSL,IKEV2 | | |
| BlueGP | SSL,IKEV2 | | |
| RedGP | SSL,IKEV2 | | |

Click the **Edit** button on the Group Policy where you want to configure Local LAN Access and navigate to the **Split Tunneling** tab.



Edit Group Policy

Name:* LocalLAN

Description:

IPv4 Split Tunneling: Allow all traffic over tunnel

IPv6 Split Tunneling: Allow all traffic over tunnel

Split Tunnel Network List Type: ● Standard Access List ○ Extended Access List

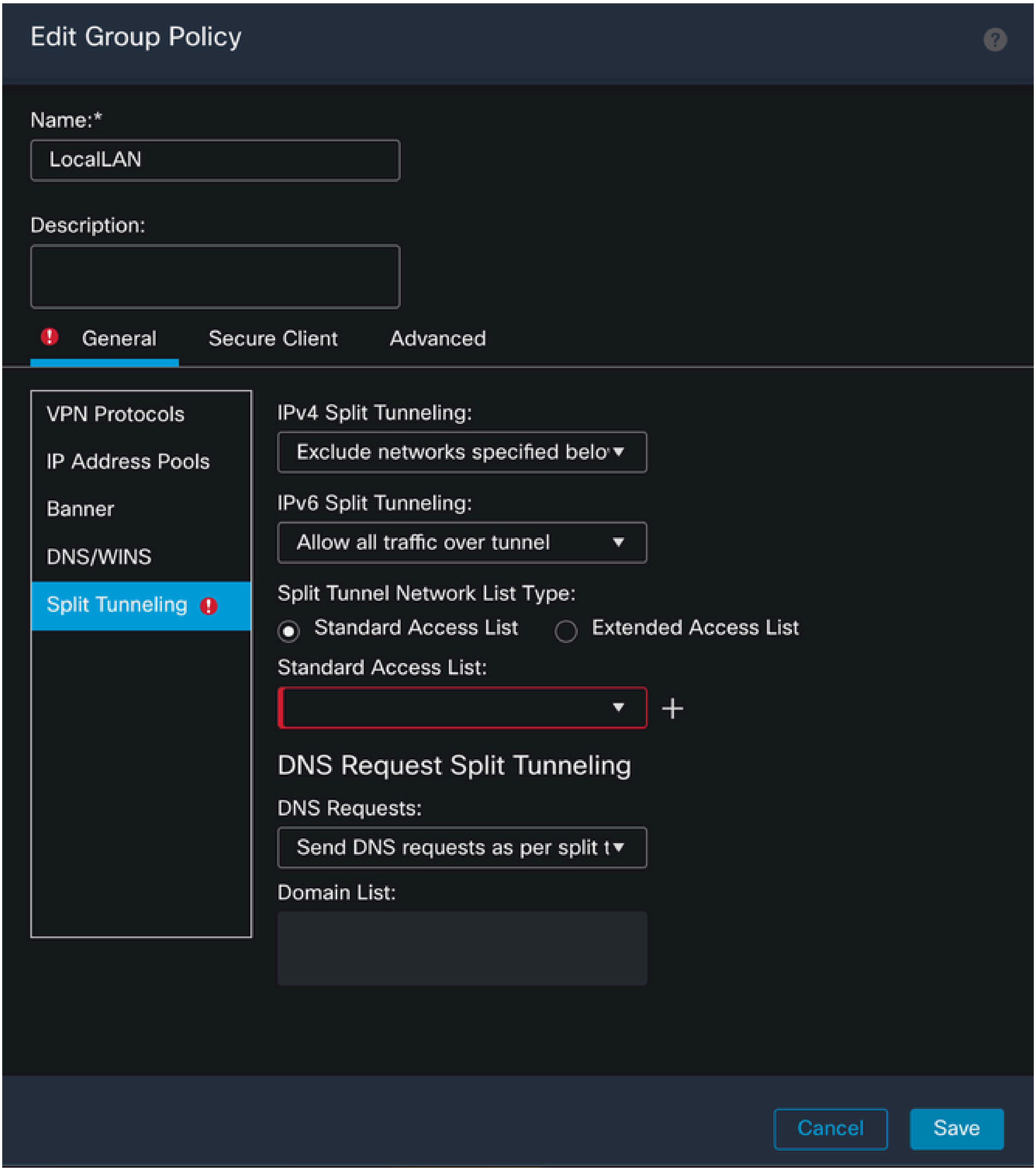
Standard Access List:

DNS Request Split Tunneling

DNS Requests: Send DNS requests as per split t

Domain List:

On the **IPv4 Split Tunneling** section, select the **Exclude networks specified below** option. This prompts for a **Standard Access List** selection.



Edit Group Policy

Name:* LocalLAN

Description:

General | Secure Client | Advanced

IPv4 Split Tunneling: Exclude networks specified belo

IPv6 Split Tunneling: Allow all traffic over tunnel

Split Tunnel Network List Type: ● Standard Access List ○ Extended Access List

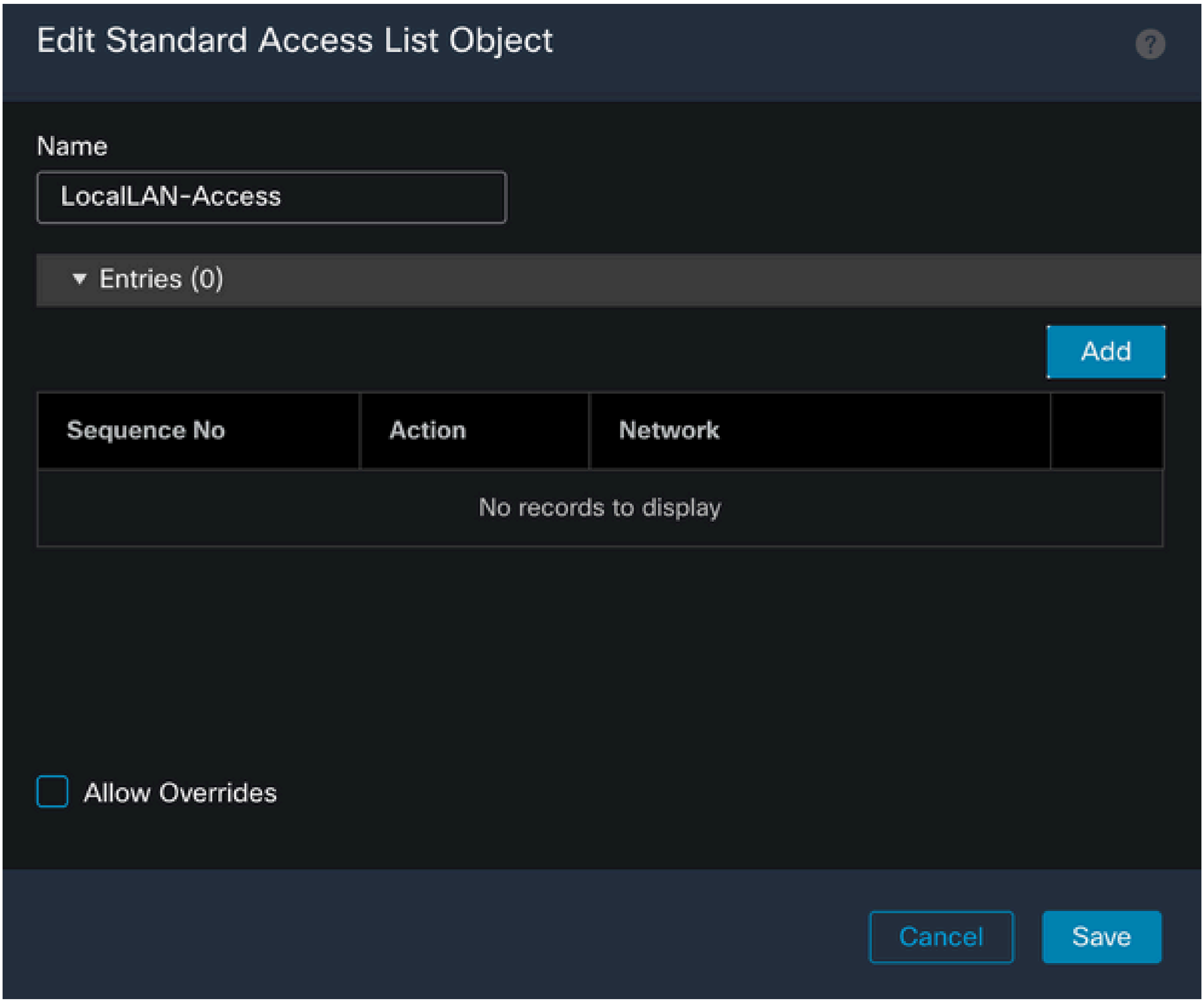
Standard Access List:

DNS Request Split Tunneling

DNS Requests: Send DNS requests as per split t

Domain List:

Click the + button to create a new Standard Access List.



Edit Standard Access List Object

Name

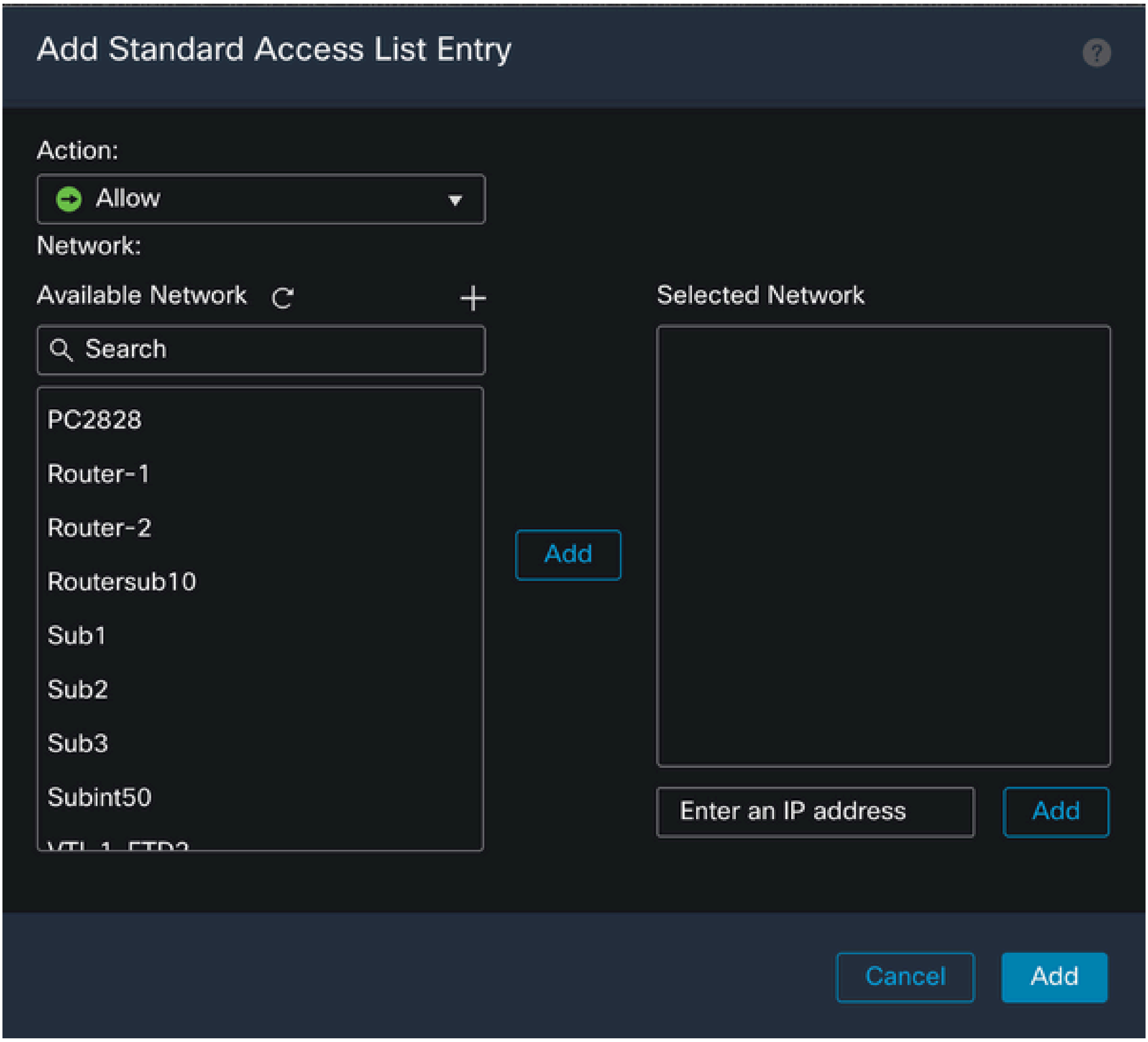
LocalLAN-Access

▾ Entries (0)

| Sequence No | Action | Network | |
|---|---|---|---|
| No records to display | | | |

□ Allow Overrides

Click the **Add** button to create a Standard Access List Entry. The **Action** of this entry must be set to **Allow.**

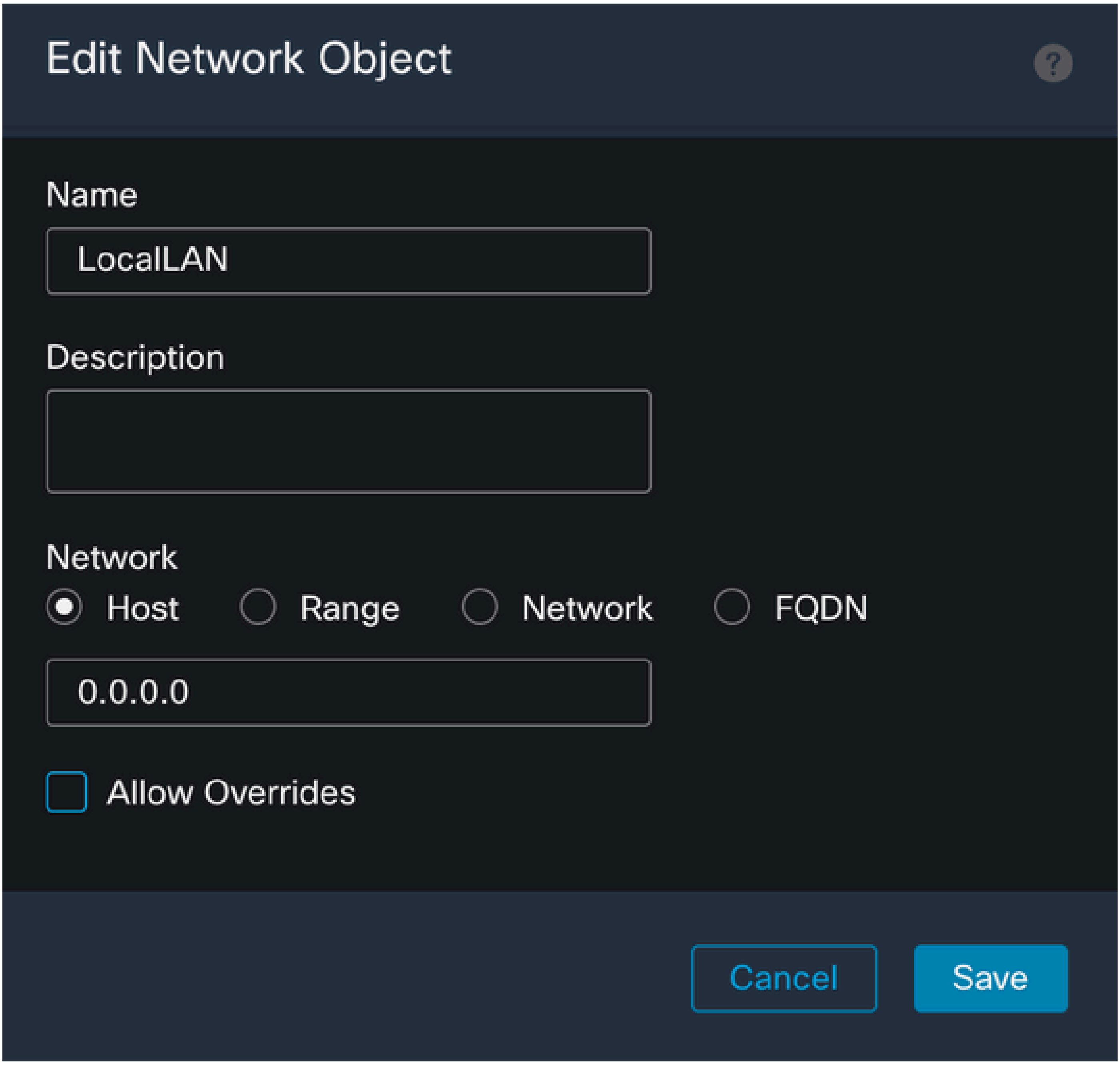


Add Standard Access List Entry

Action: Allow

Network:

Click the **+** button to add a new Network Object. Ensure that this object is set as a **Host** on the **Network** section and enter **0.0.0.0** in the box.



Edit Network Object

Name: LocalLAN

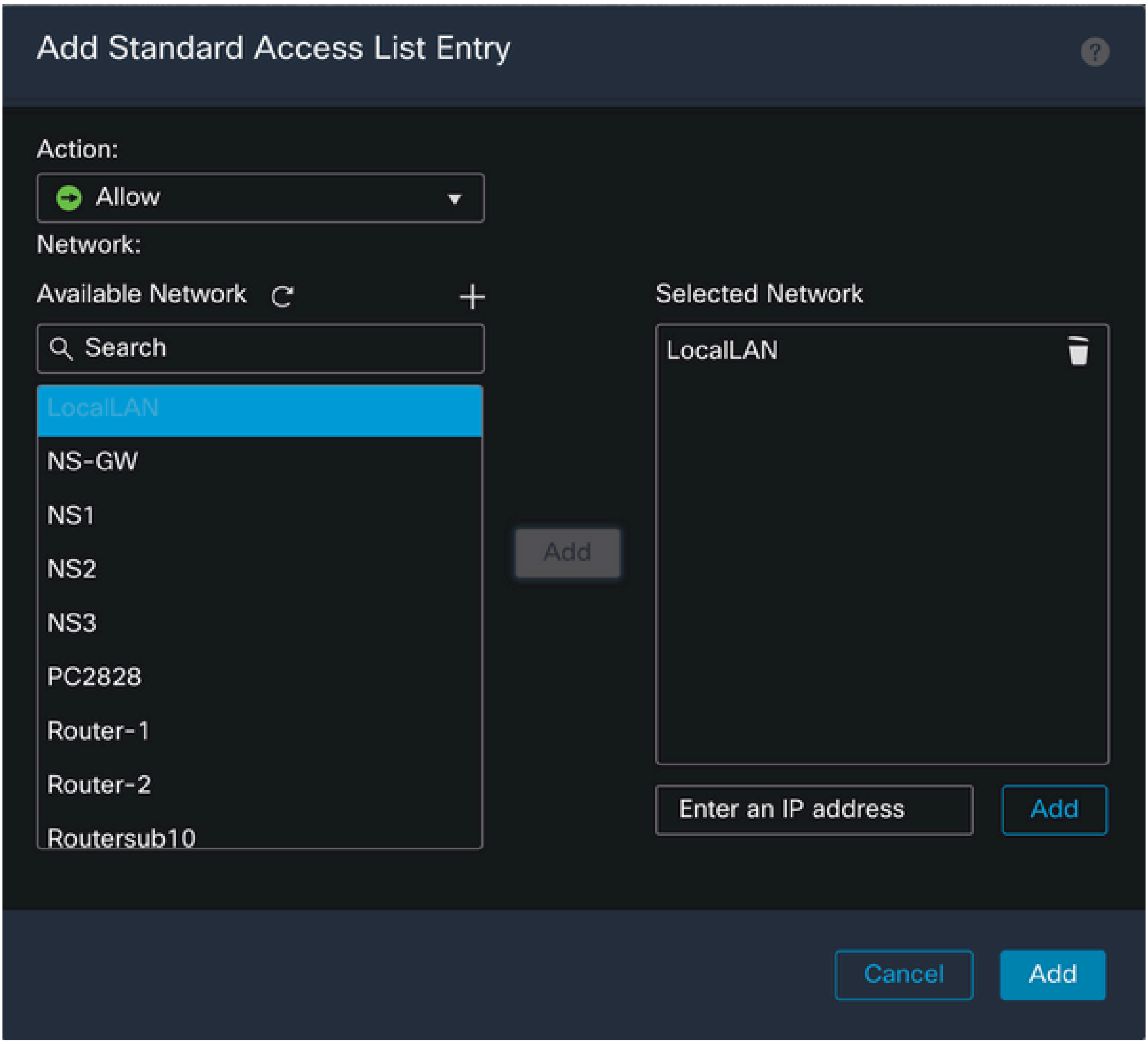
Description:

Network: ● Host ○ Range ○ Network ○ FQDN

0.0.0.0

□ Allow Overrides

Click the **Save** button and select the newly created object.



Add Standard Access List Entry

Action: Allow

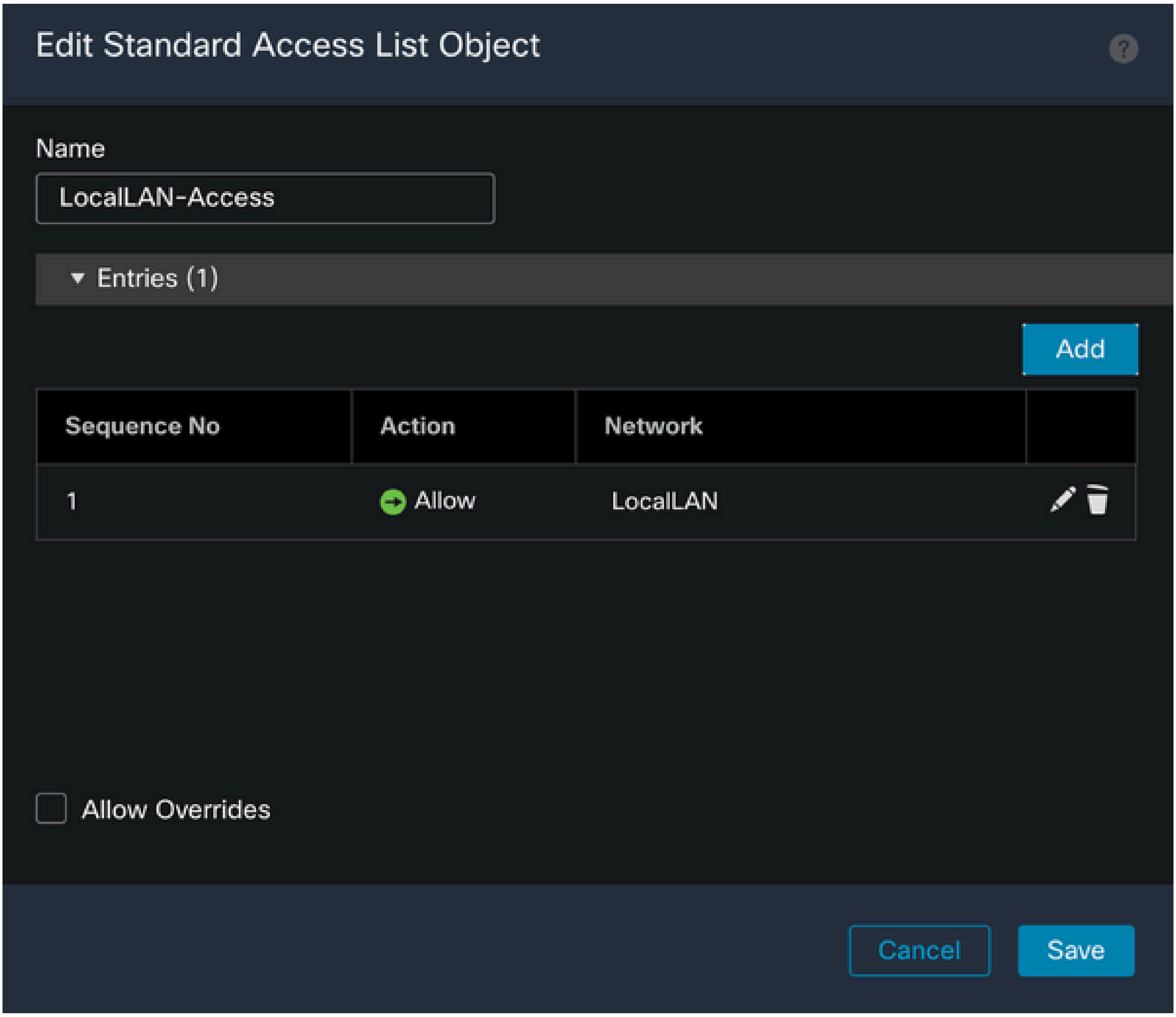
Network:

Available Network

Selected Network

LocalLAN

Click the **Add** button to save the Standard Access List entry.



Edit Standard Access List Object

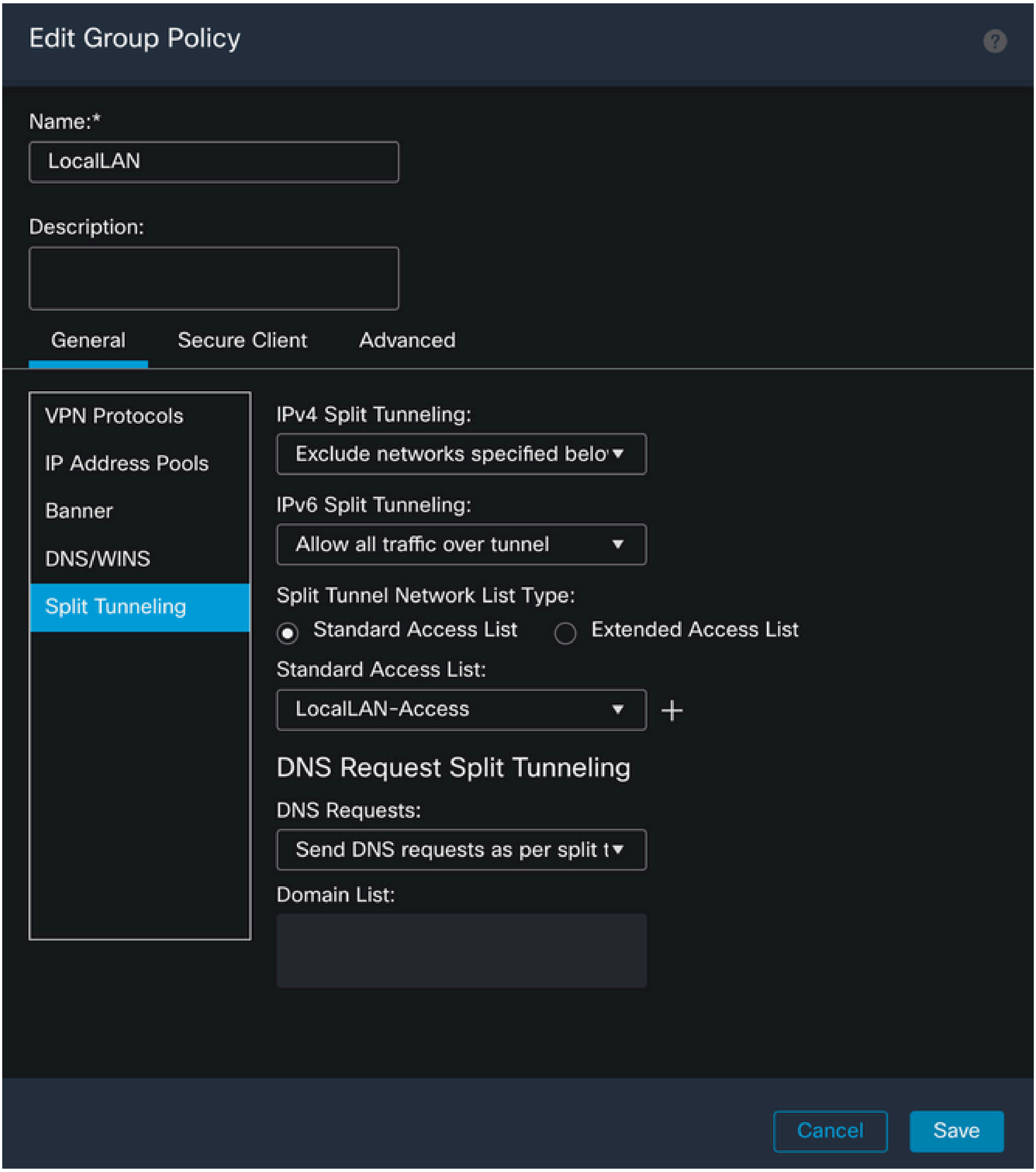
Name: LocalLAN-Access

▾ Entries (1)

| Sequence No | Action | Network | |
|---|---|---|---|
| 1 | Allow | LocalLAN | |

□ Allow Overrides

Click the **Save** button and the newly created Standard Access List is automatically selected.



Edit Group Policy

Name:* LocalLAN

Description:

IPv4 Split Tunneling: Exclude networks specified belo

IPv6 Split Tunneling: Allow all traffic over tunnel

Split Tunnel Network List Type: ● Standard Access List ○ Extended Access List

Standard Access List: LocalLAN-Access

DNS Request Split Tunneling

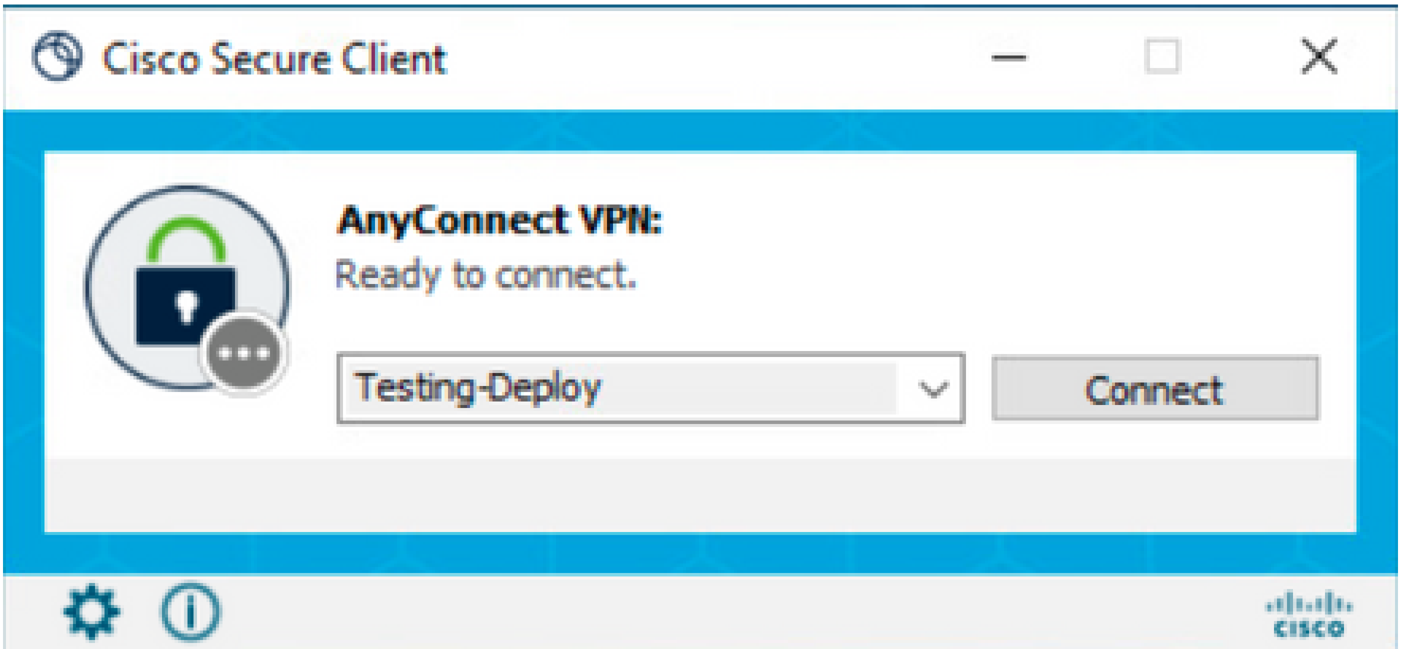
DNS Requests: Send DNS requests as per split t

Domain List:

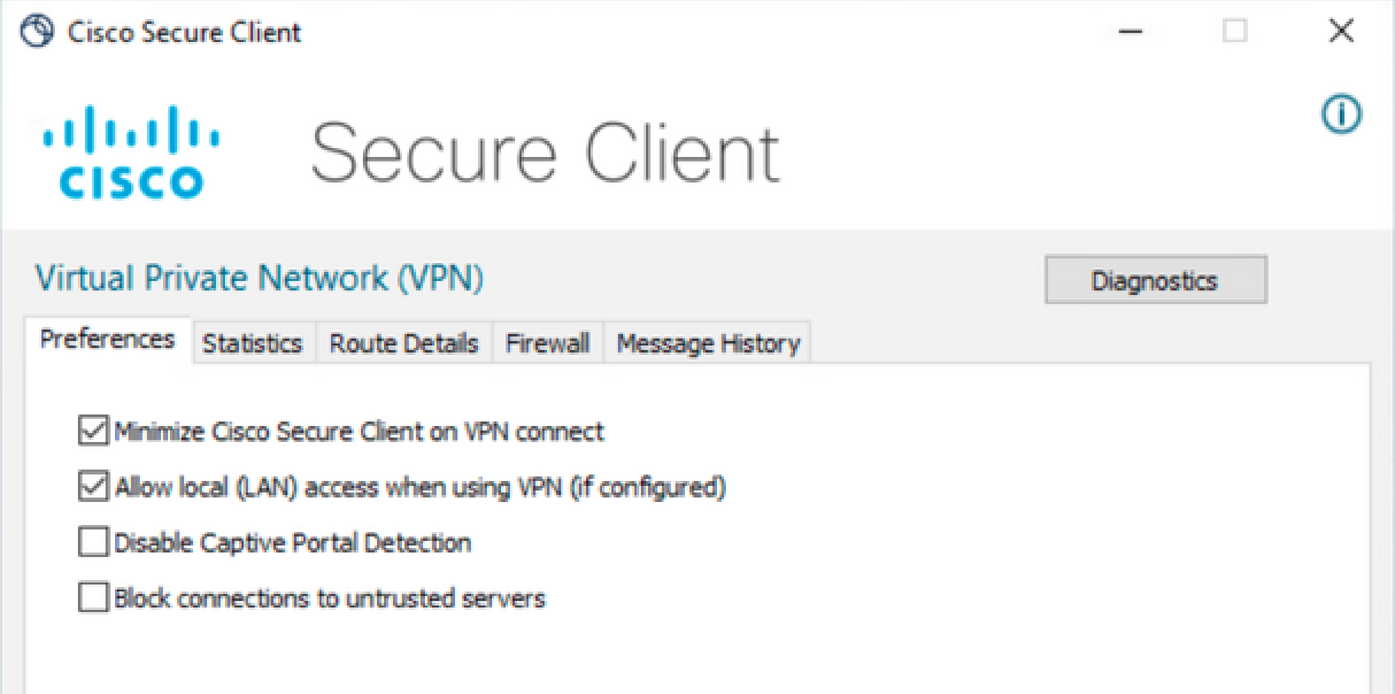
Click the **Save** button and deploy the changes.

## Secure Client configuration

By default, the Local LAN Access option is set to **User Controllable**. To enable the option, click the Gear icon on the Secure Client GUI.



Navigate to **Preferences** and ensure that the **Allow local (LAN) access when using VPN (if configured)** option is enabled.

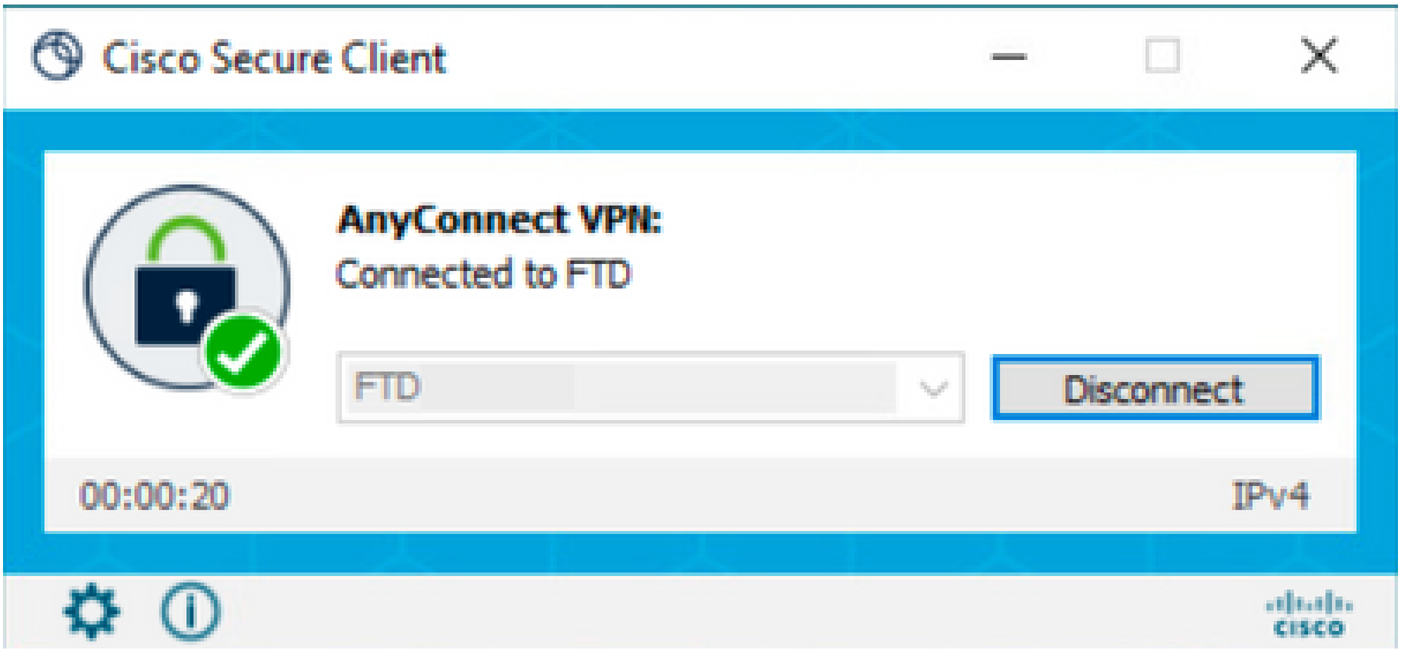


☑ Minimize Cisco Secure Client on VPN connect
☑ Allow local (LAN) access when using VPN (if configured)
□ Disable Captive Portal Detection
□ Block connections to untrusted servers

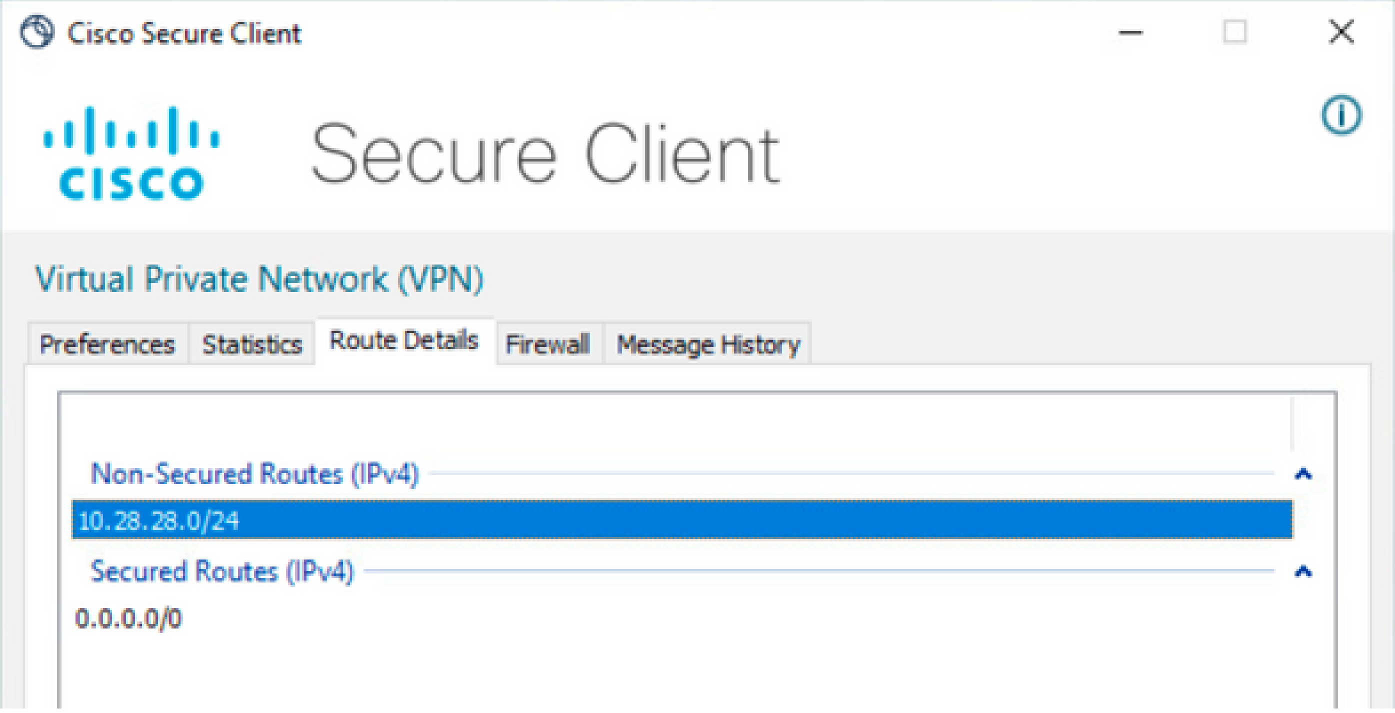
# Verify

## Secure Client

Connect to the headend using the Secure Client.



Click the gear icon and navigate to **Route Details.** Here you can see that the local LAN is automatically detected and excluded from the tunnel.



Non-Secured Routes (IPv4)
10.28.28.0/24
Secured Routes (IPv4)
0.0.0.0/0

## FTD CLI

To verify if the configuration was applied successfuly, you can use the CLI of the 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
```

# Troubleshoot

In order to verify if the Local LAN access feature was applied, you can enable these debugs:

```
debug webvpn anyconnect 255
```

This is an example of a successful debug output:

<#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: 0224D83639071BBF29E2D77B15B762FE85BD50D1F0EF9758942
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
```