セキュアクライアントのローカルLANアクセスの設定

内容

概要

このドキュメントでは、ローカルLANにアクセスしながらヘッドエンドへのセキュアな接続を維持するようにCisco Secure Clientを設定する方法について説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

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

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Secure Firewall Management Center仮想アプライアンスバージョン7.3
- Cisco Firepower Threat Defense仮想アプライアンスバージョン7.3
- Cisco Secure Clientバージョン5.0.02075

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

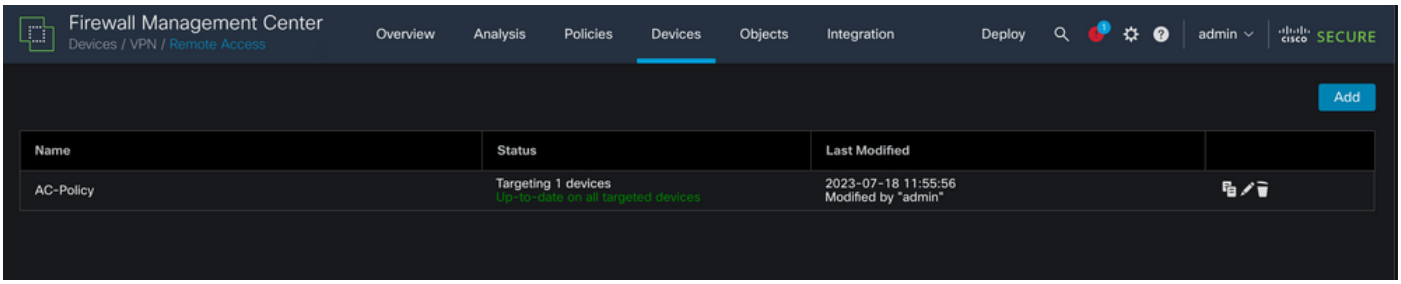
このドキュメントで説明する設定により、Cisco Secure Clientは、ヘッドエンドおよび企業リソースへのセキュアな接続を維持しながら、ローカルLANへのフルアクセスが可能になります。これは、クライアントがネットワークアクセスサーバ(NAS)を印刷またはアクセスできるようにするために使用できます。

設定

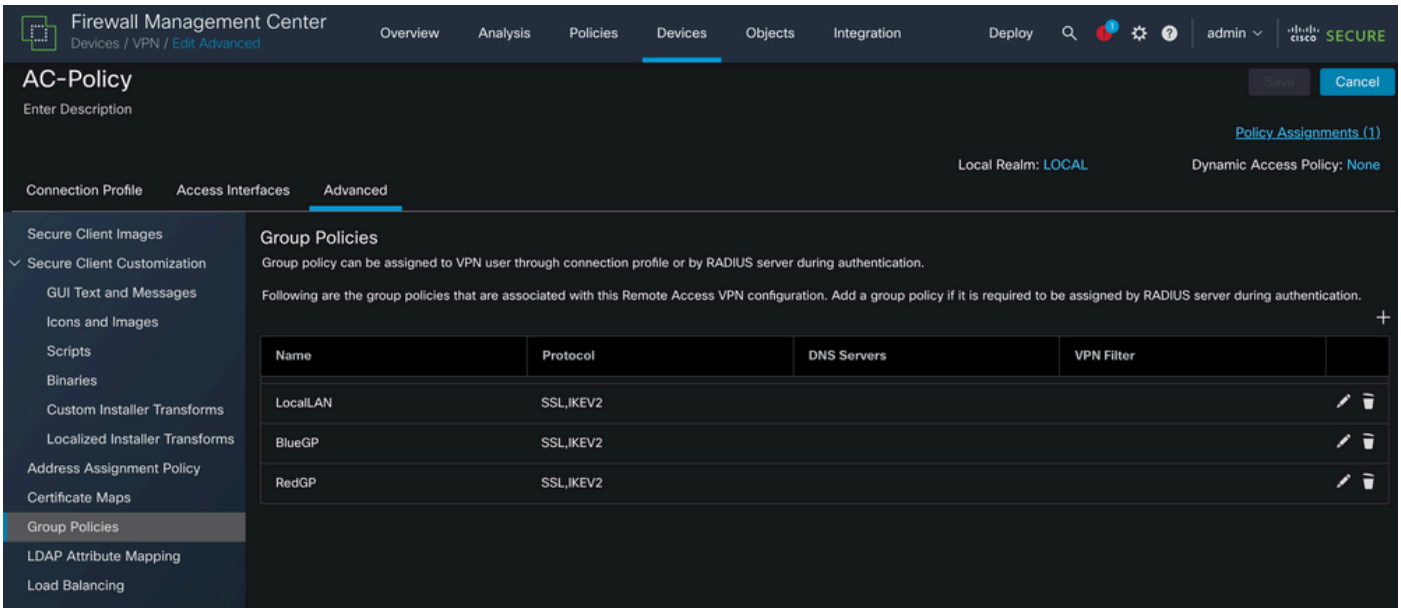
FMCの設定

このドキュメントでは、すでにリモートアクセスVPN(RVPN)設定が動作していることを前提としています。

ローカルLANアクセス機能を追加するには、Devices > Remote Accessの順に移動し、該当するリモートアクセスポリシーでEditボタンをクリックします。

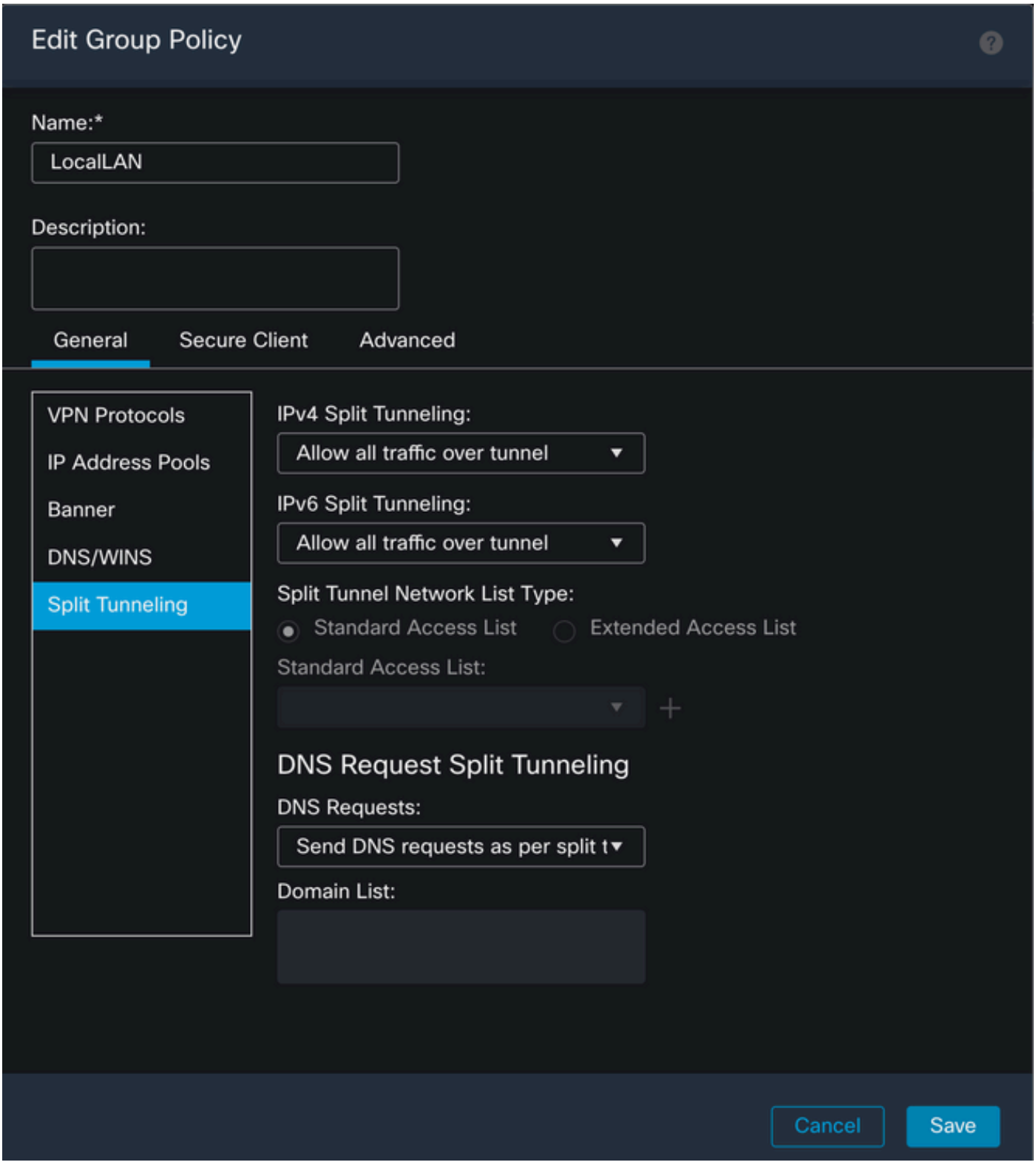


次に、Advanced > Group Policiesの順に移動します。

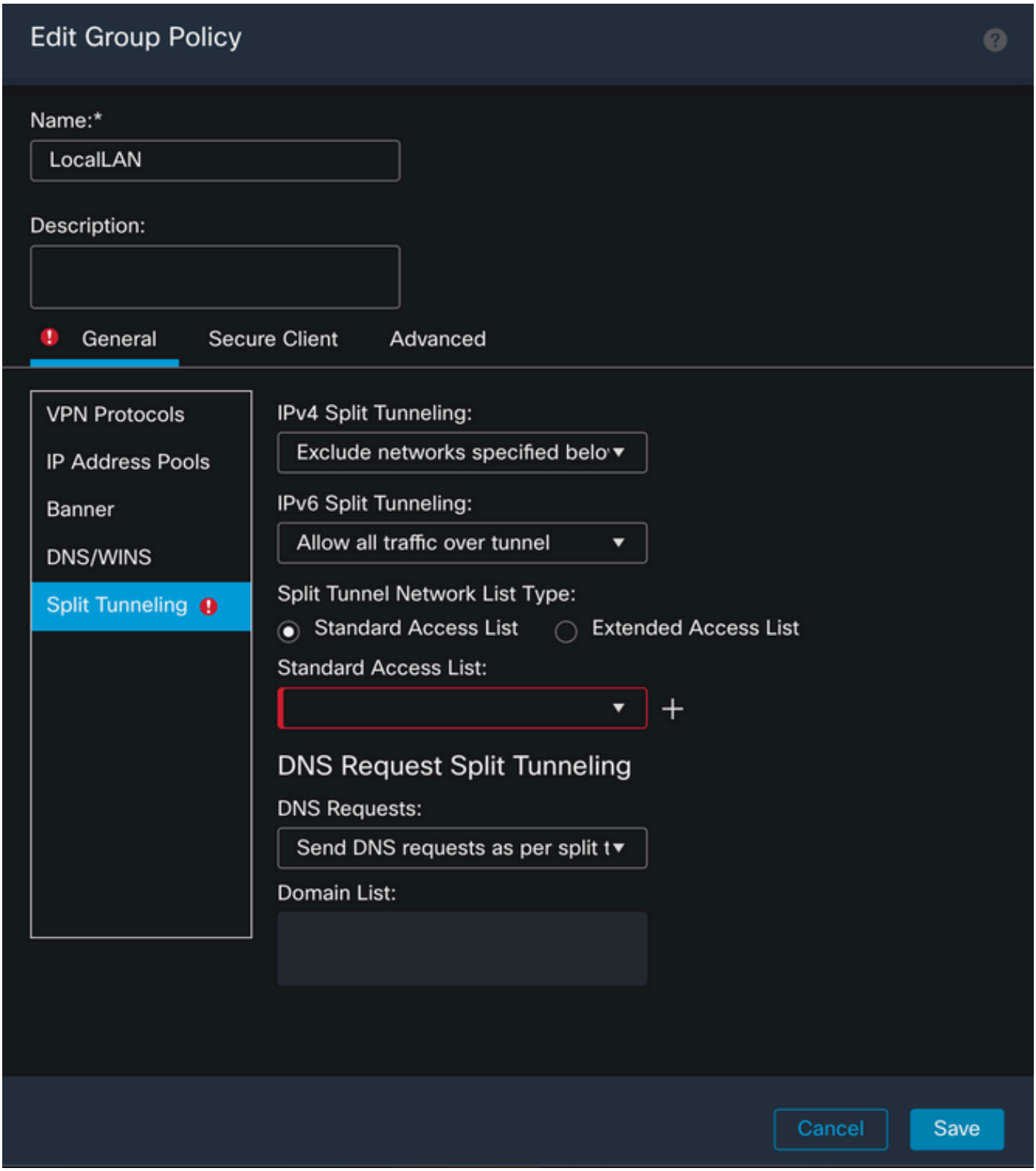


ローカルLANアクセスを設定するグループポリシーでEditボタンをクリックし、Split Tunnelingタ

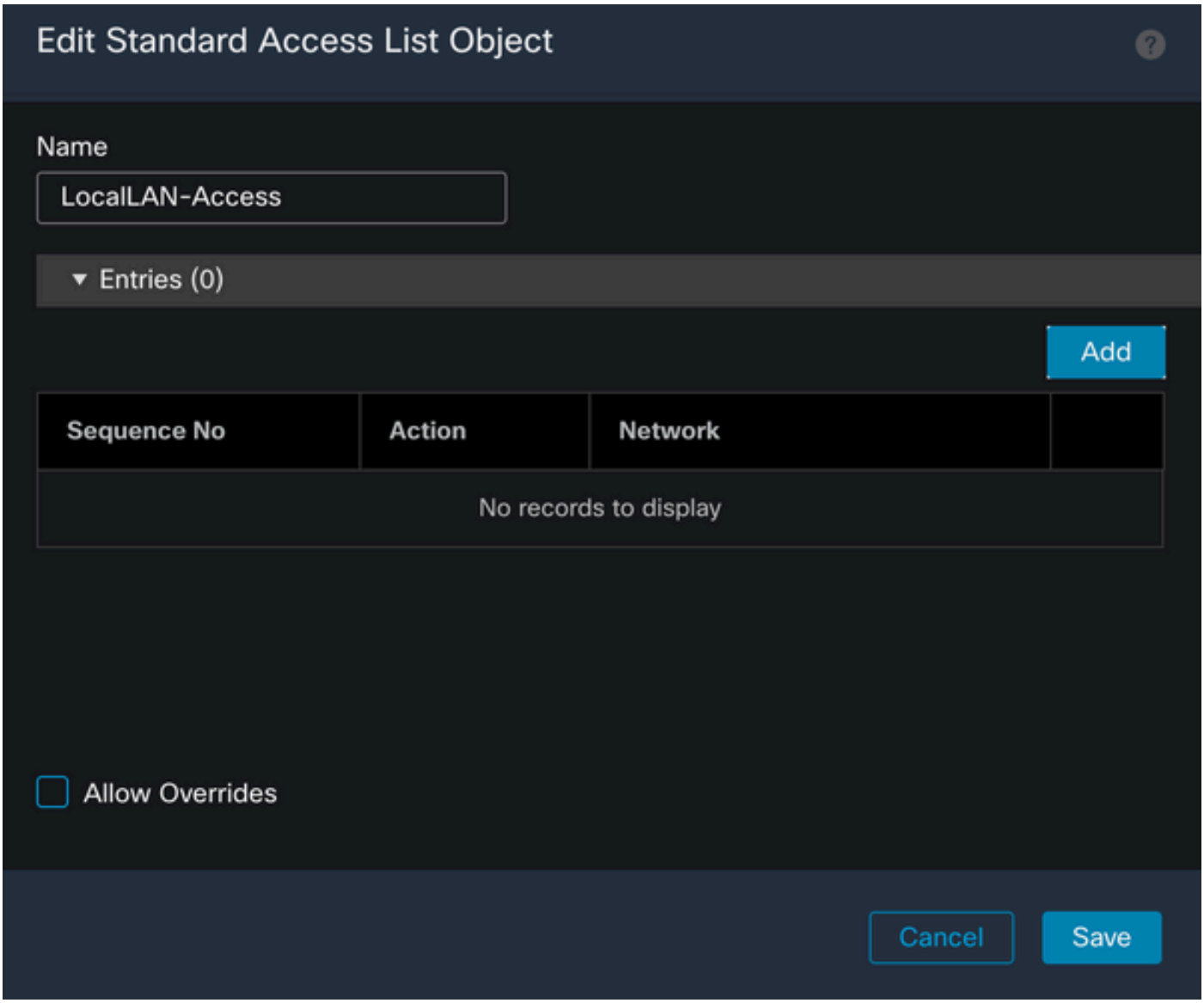
ブに移動します。



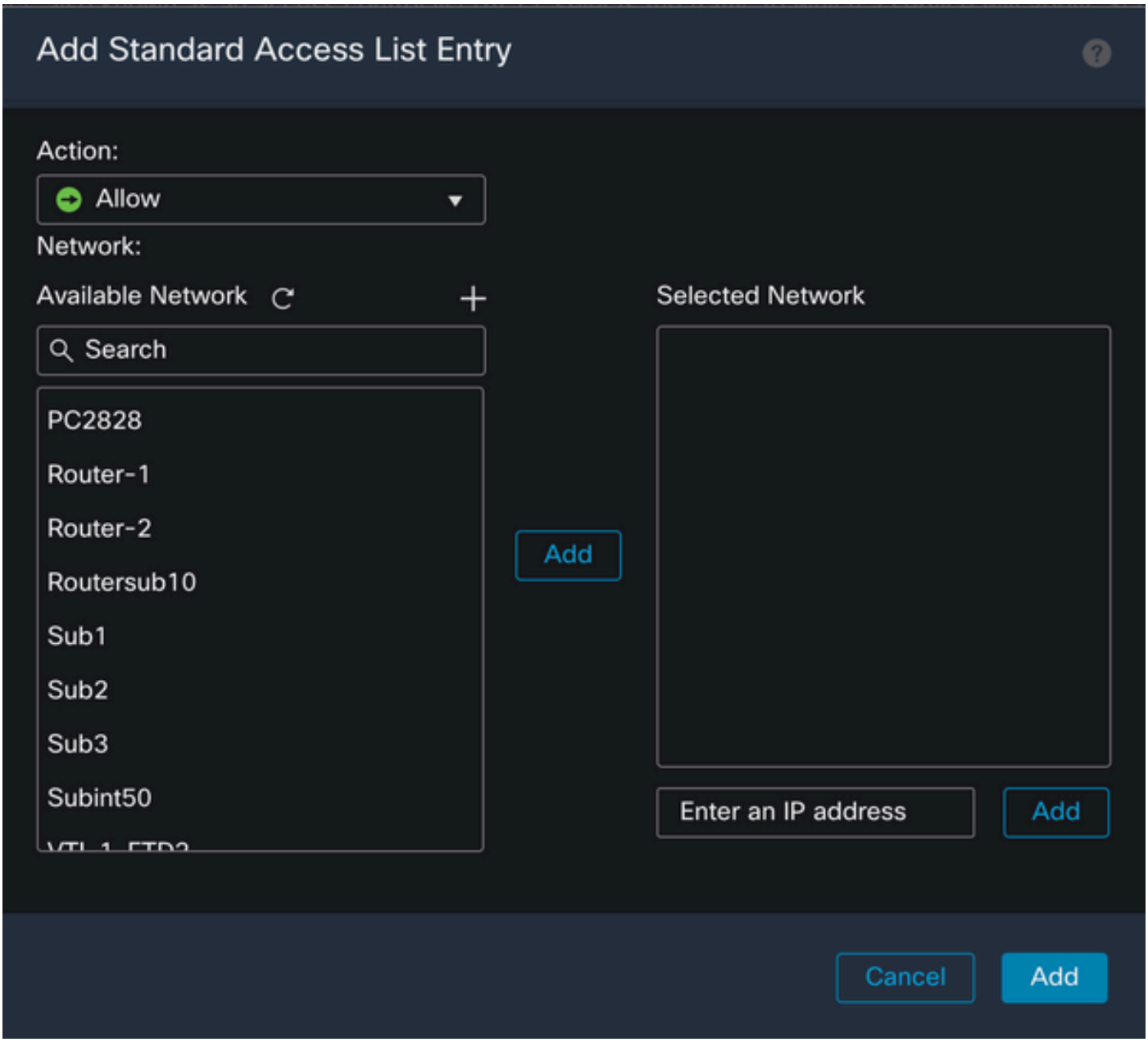
IPv4スプリットトンネリングセクションで、Exclude networks specified belowオプションを選択します。これにより、標準アクセスリストの選択が求められます。



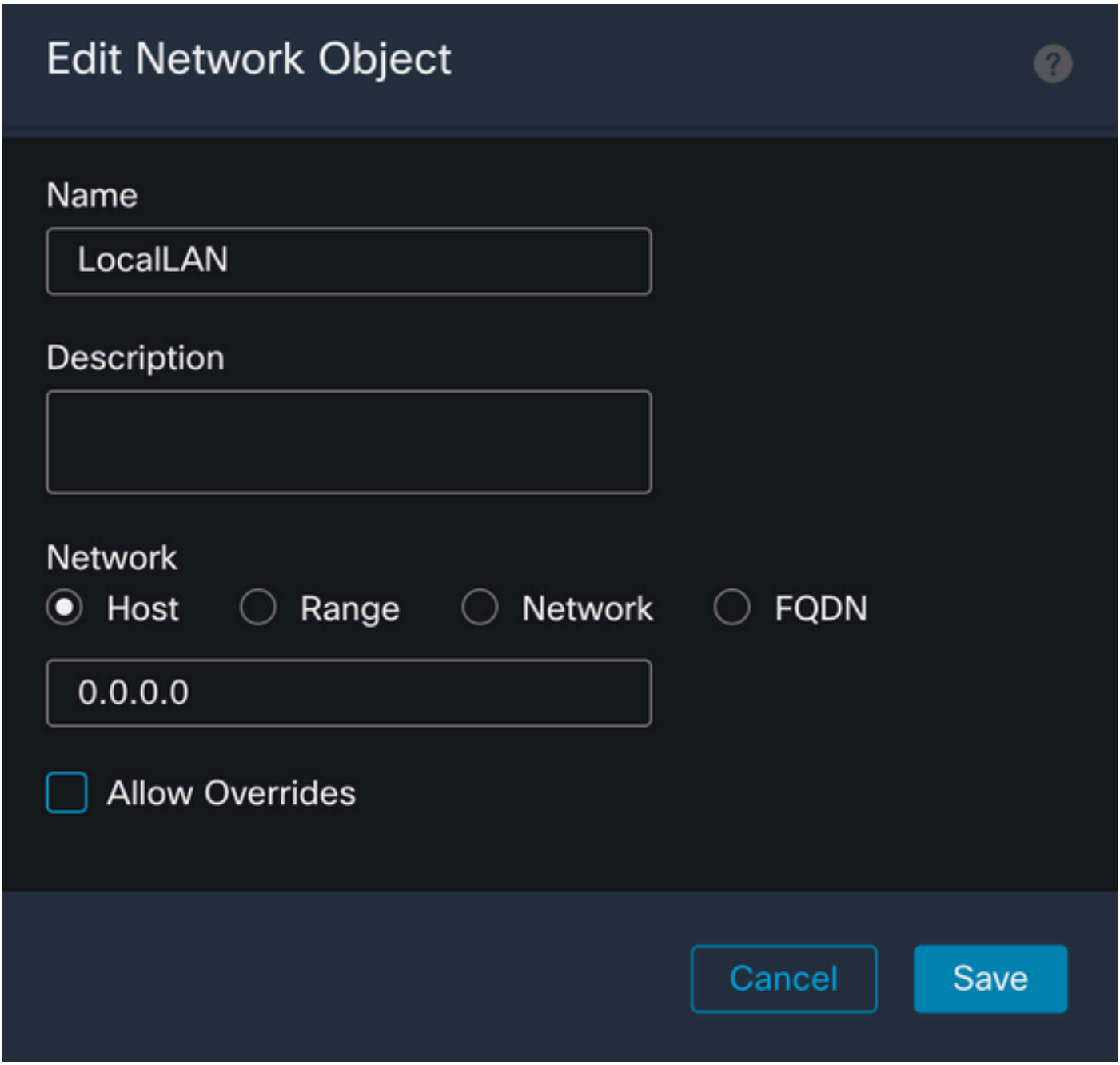
+ ボタンをクリックして、新しい標準アクセスリストを作成します。



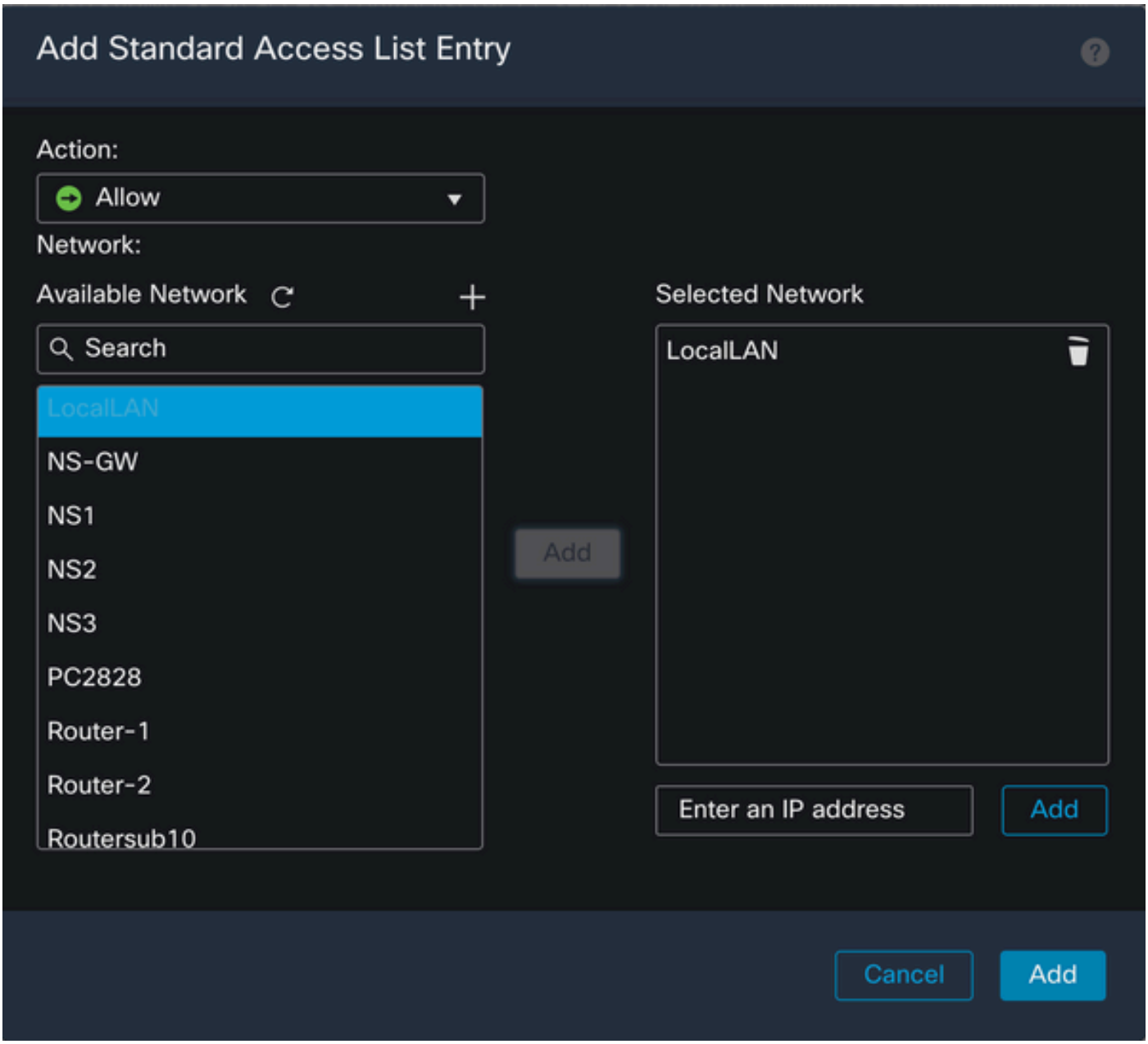
Addボタンをクリックして、標準アクセスリストエントリを作成します。このエントリのActionをAllowに設定する必要があります。



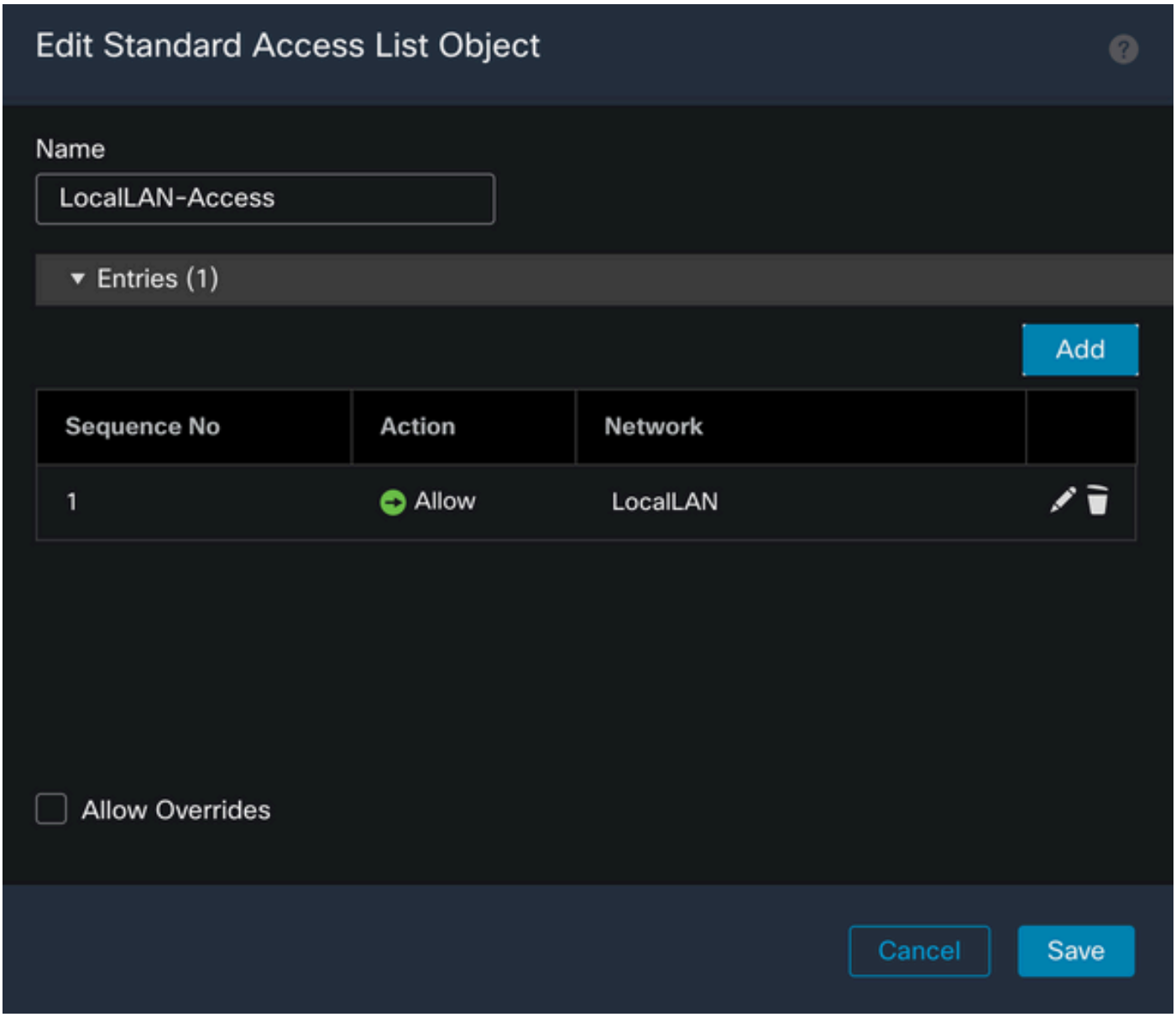
+ボタンをクリックして、新しいネットワークオブジェクトを追加します。このオブジェクトがHostとしてNetworkセクションに設定されていることを確認し、ボックスに0.0.0.0と入力します。



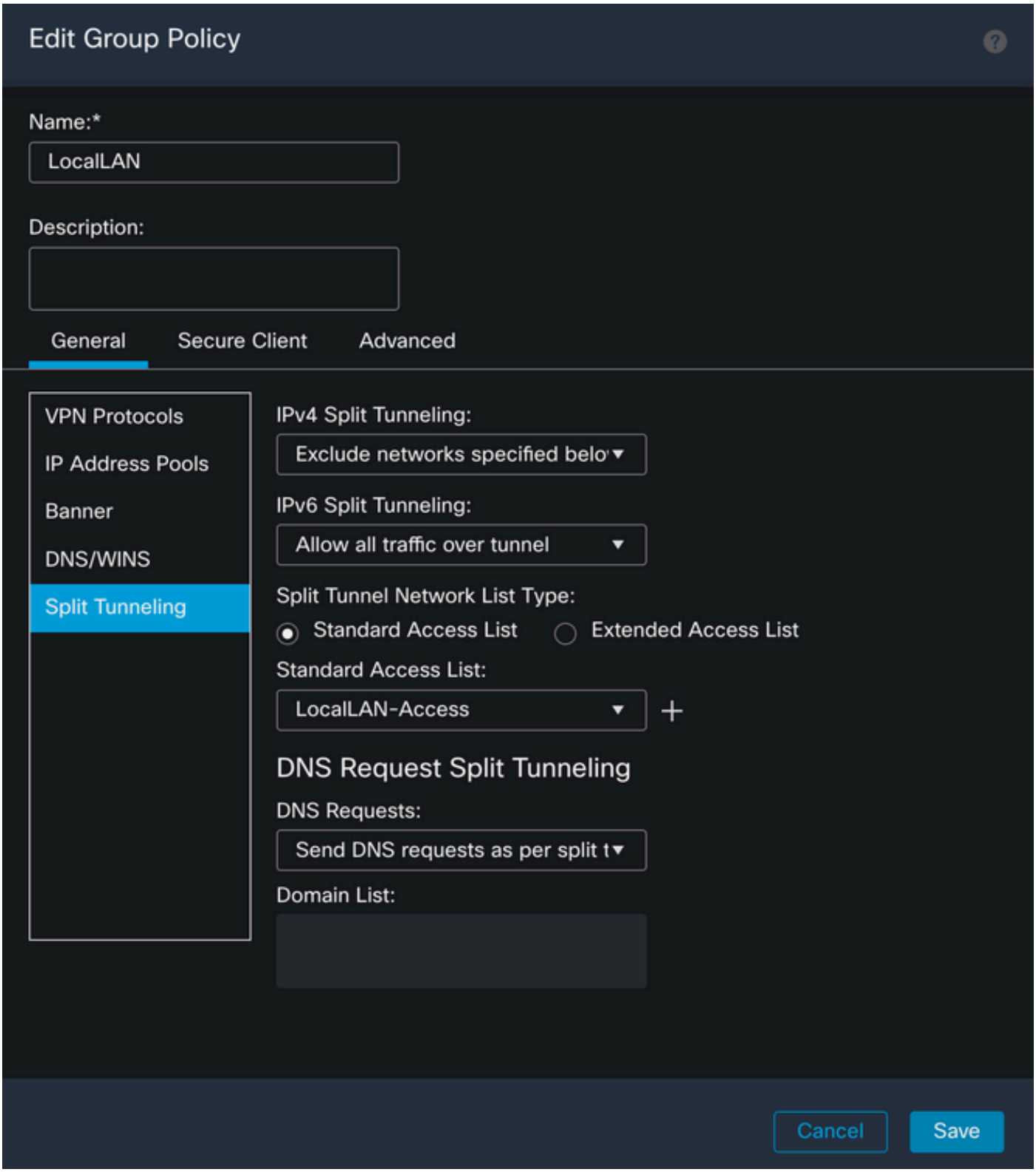
Saveボタンをクリックして、新しく作成したオブジェクトを選択します。



Addボタンをクリックして、標準アクセスリストエントリを保存します。



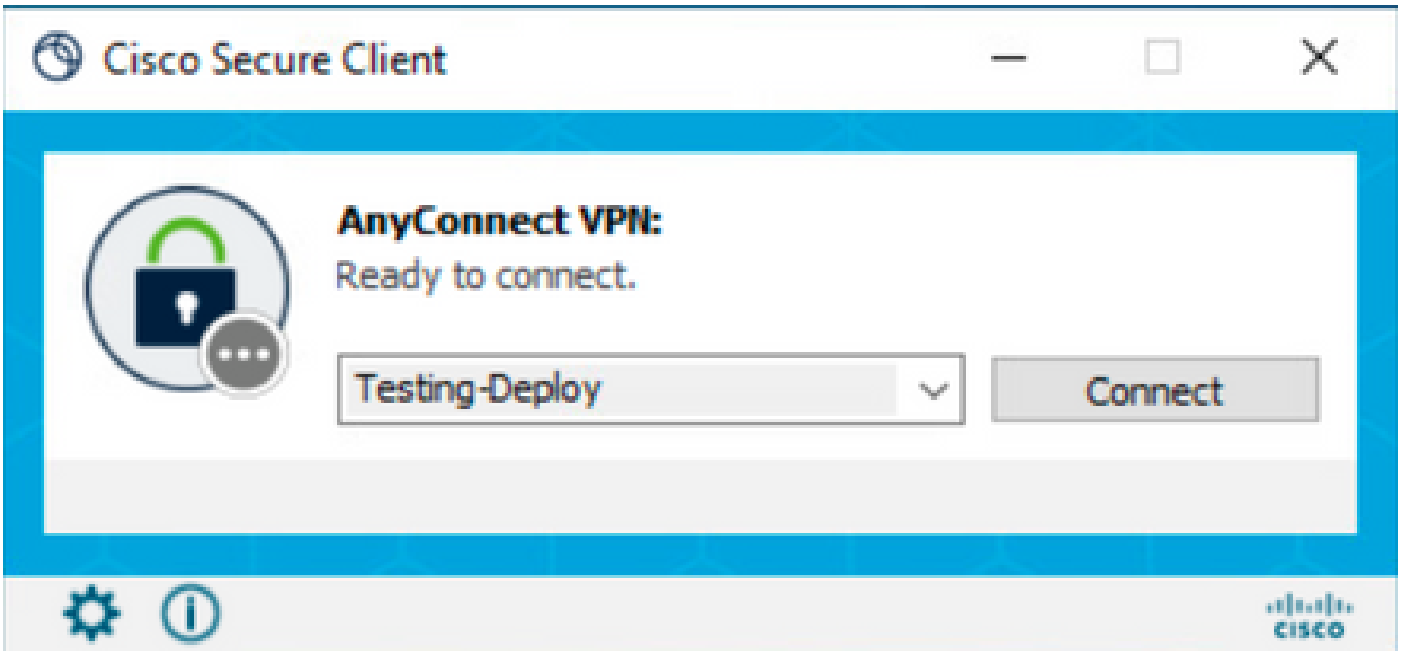
Saveボタンをクリックすると、新しく作成された標準アクセスリストが自動的に選択されます。



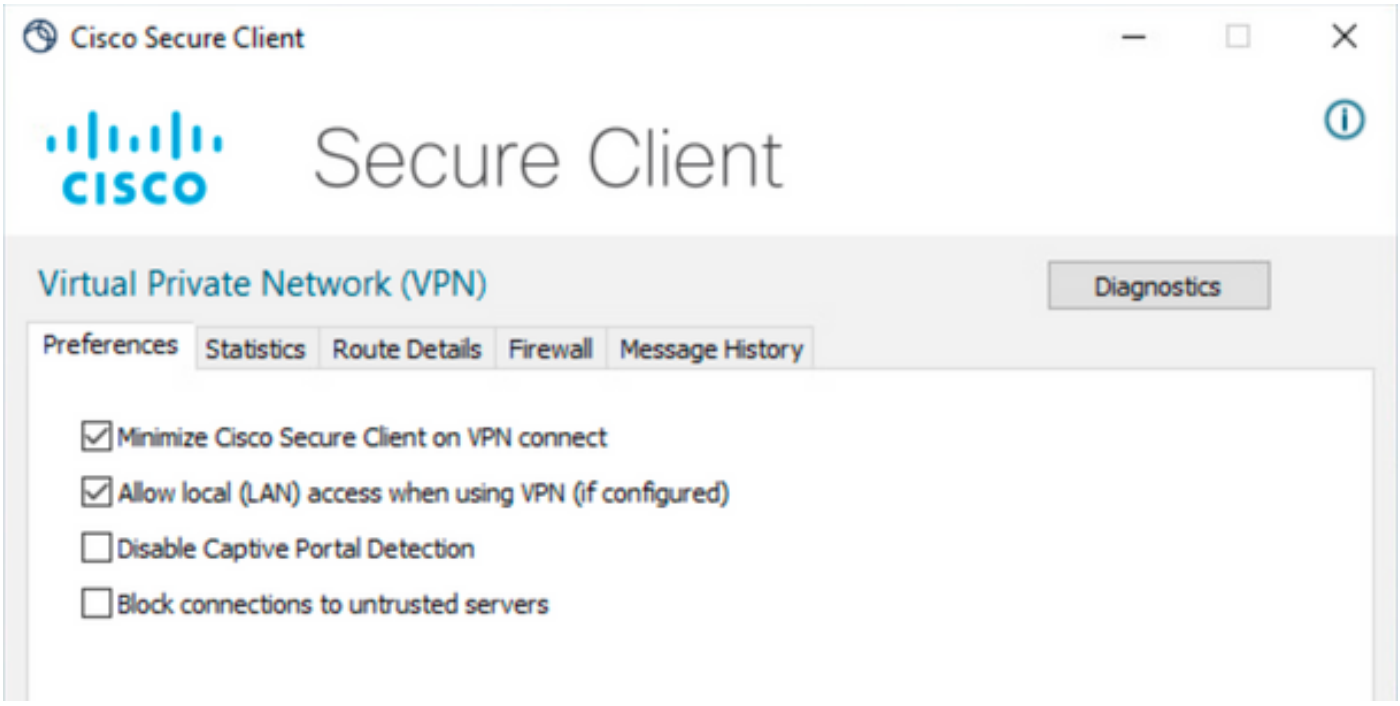
Saveボタンをクリックして、変更を展開します。

Secure Clientの設定

デフォルトでは、Local LAN AccessオプションはUser Controllableに設定されています。このオプションを有効にするには、セキュアクライアントGUIの歯車アイコンをクリックします。



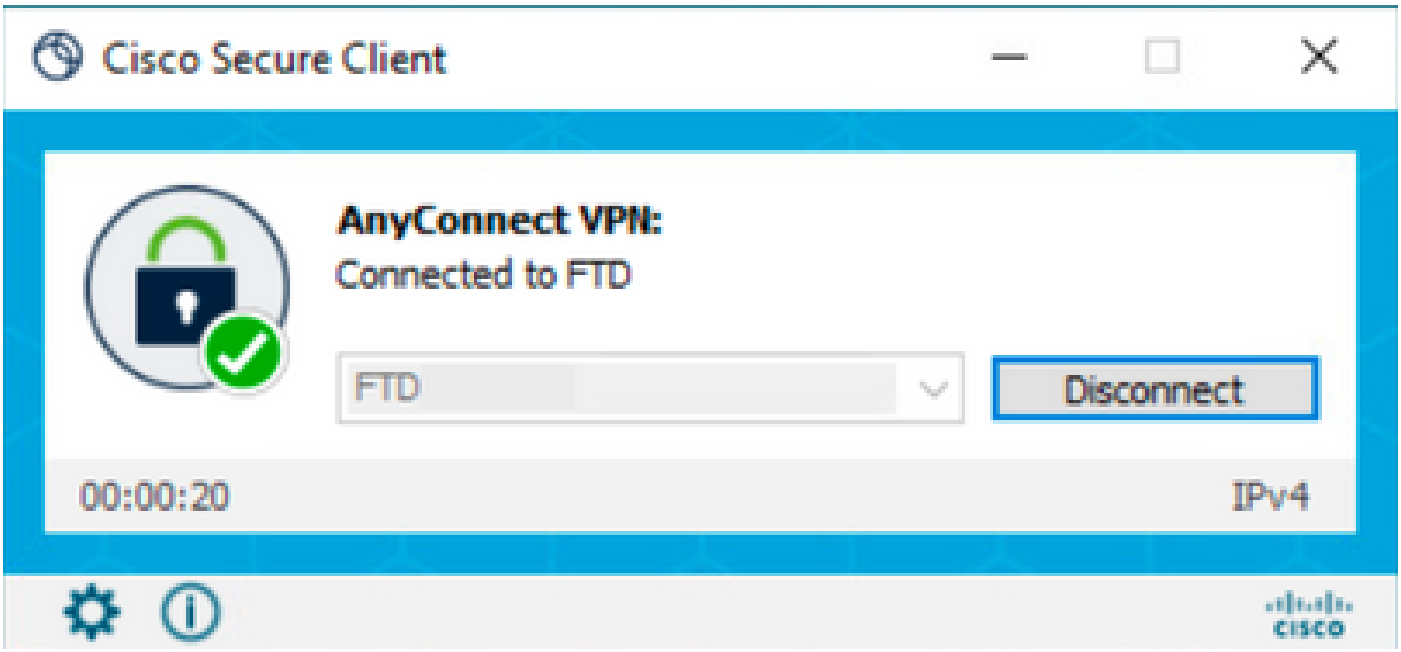
Preferencesに移動し、Allow local (LAN) access when using VPN (if configured)オプションが有効になっていることを確認します。



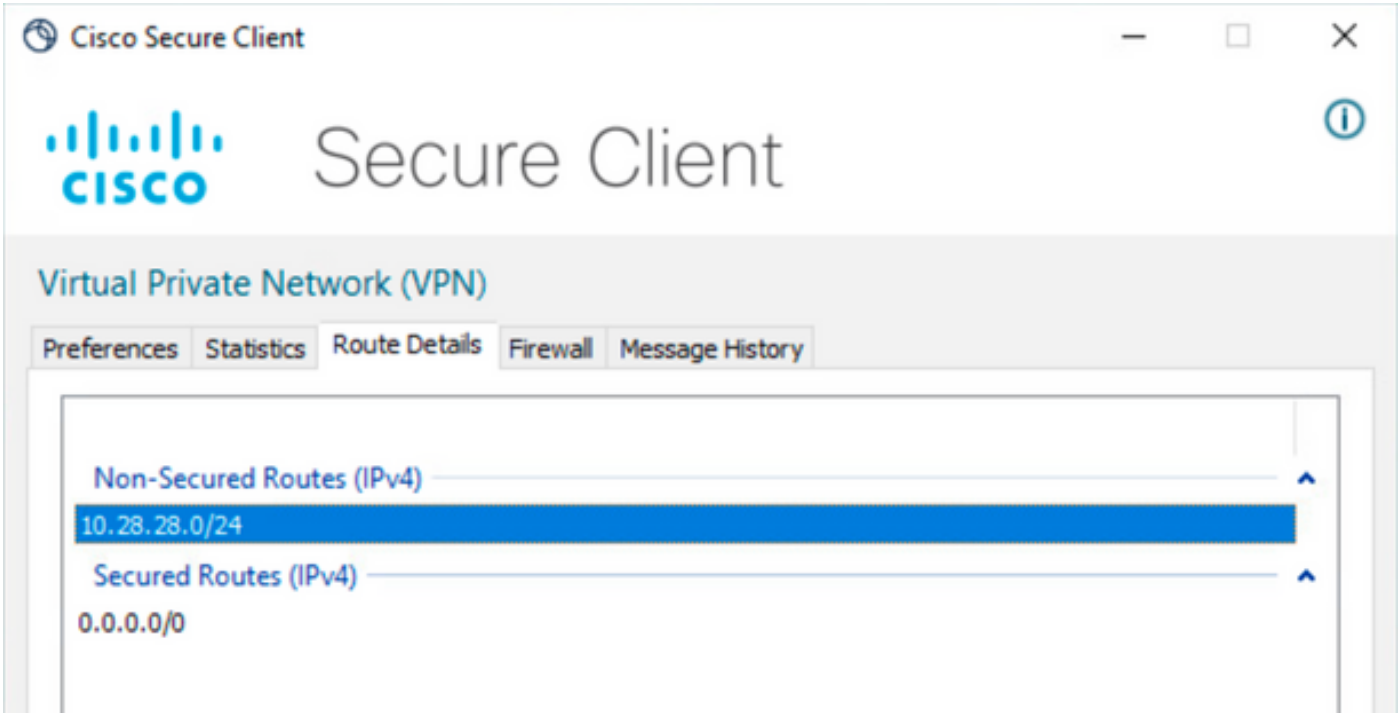
確認

セキュアなクライアント

セキュアクライアントを使用してヘッドエンドに接続します。



歯車アイコンをクリックし、ルートの詳細に移動します。ここでは、ローカルLANが自動的に検出され、トンネルから除外されることを確認できます。



FTDのCLI

設定が正常に適用されたかどうかを確認するには、FTDのCLIを使用します。

```
<#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
```

トラブルシュート

ローカルLANアクセス機能が適用されたかどうかを確認するには、次のデバッグを有効にします。

```
debug webvpn anyconnect 255
```

正常なデバッグ出力の例を次に示します。

<#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
```

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。