تكوين الوصول إلى شبكة LAN المحلية لعميل آمن

المحتويات

المقدمة

يصف هذا وثيقة كيف أن يشكل cisco يأمن زبون أن ينفذ ال LAN محلي ويحافظ على توصيل آمن إلى وحدة الاستقبال والبث.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة على هذا موضوع:

- مركز إدارة جدار الحماية الآمن (FMC) من Cisco
- الدفاع ضد تهديد FirePOWER (FTD) من Cisco
- العميل الآمن من Cisco (CSC)

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- الجهاز الظاهري Cisco Secure Firewall Management Center Virtual Appliance، الإصدار 7.3
- الجهاز الظاهري للدفاع عن التهديد FirePOWER من Cisco، الإصدار 7.3
- Cisco Secure Client، الإصدار 5.0.02075

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة.

بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

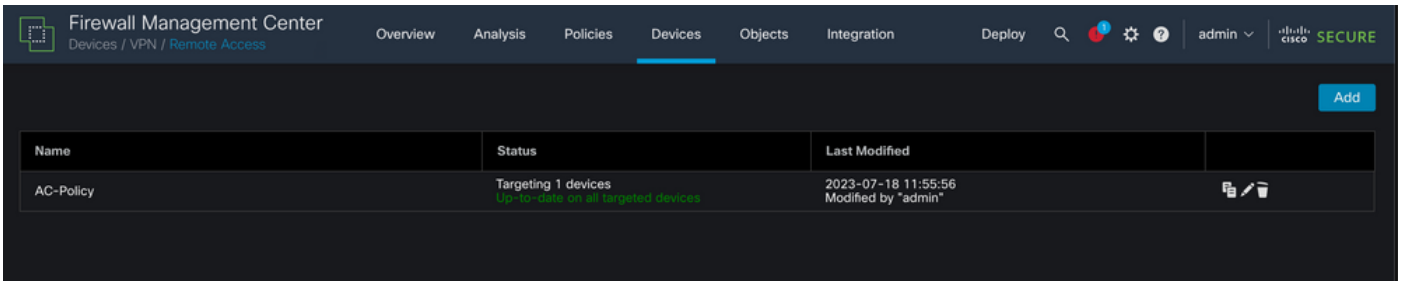
يتيح التكوين الموضح في هذا المستند لـ Cisco Secure Client إمكانية الوصول الكامل إلى شبكة LAN المحلية مع الحفاظ في الوقت نفسه على اتصال آمن بموارد وحدة الاستقبال والبث الخاصة بالشركة. يمكن إستخدام هذا للسماح للعميل بطباعة خادم Network Access (NAS) أو الوصول إليه.

التكوين

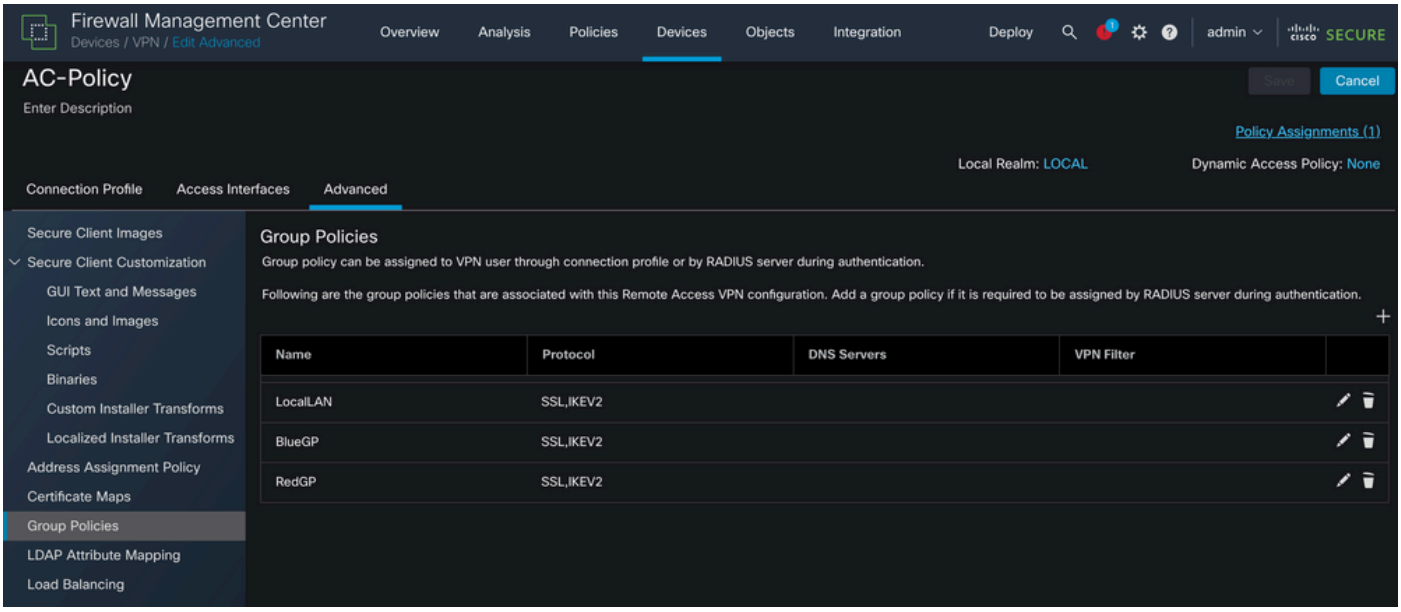
تكوين FMC

في هذا المستند، يفترض أن لديك بالفعل تكوين شبكة VPN للوصول عن بعد يعمل.

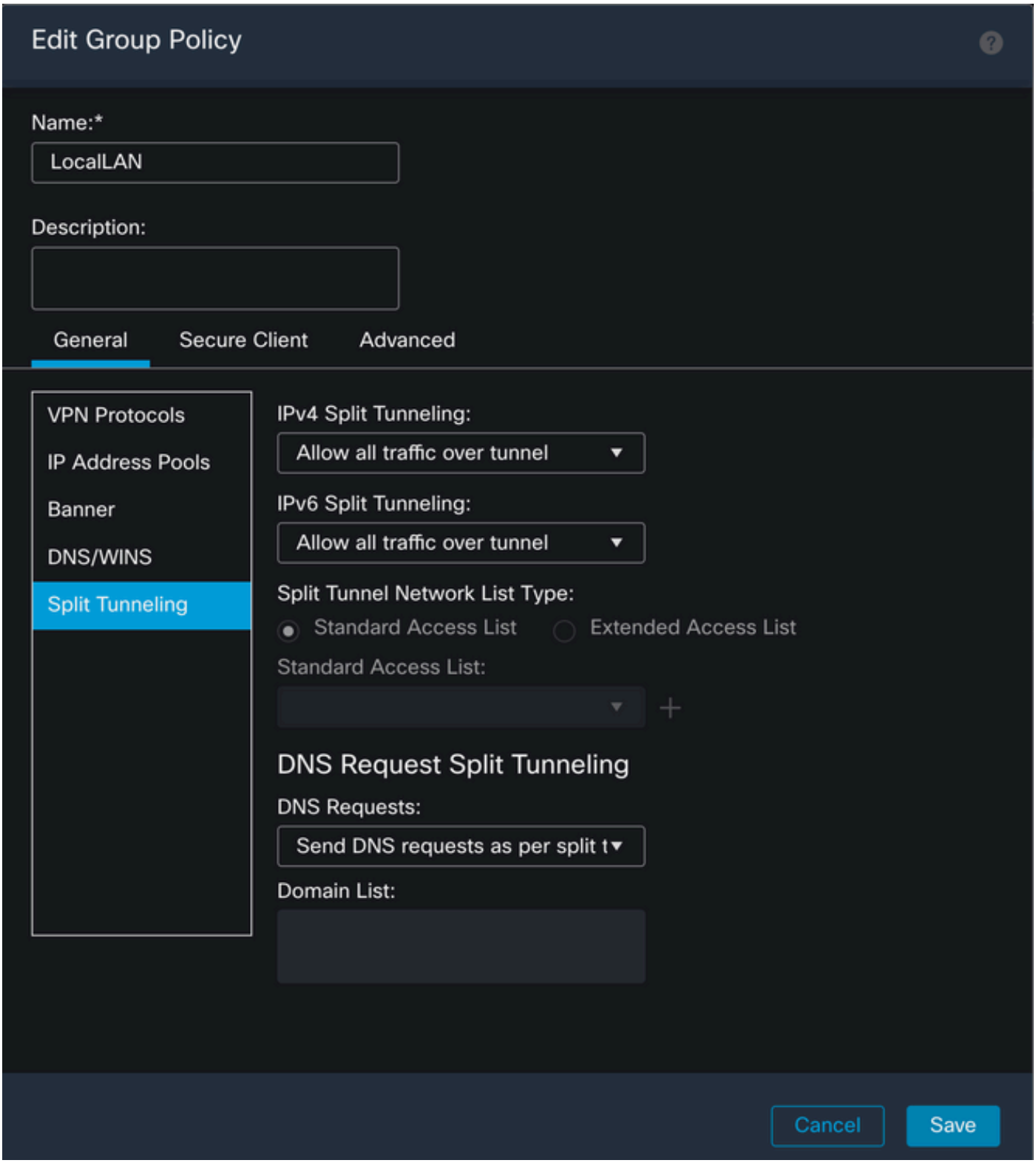
لإضافة إمكانية الوصول إلى شبكة LAN المحلية، انتقل إلى الأجهزة > الوصول عن بعد وانقر فوق الزر تحرير في نهج الوصول عن بعد المناسب.



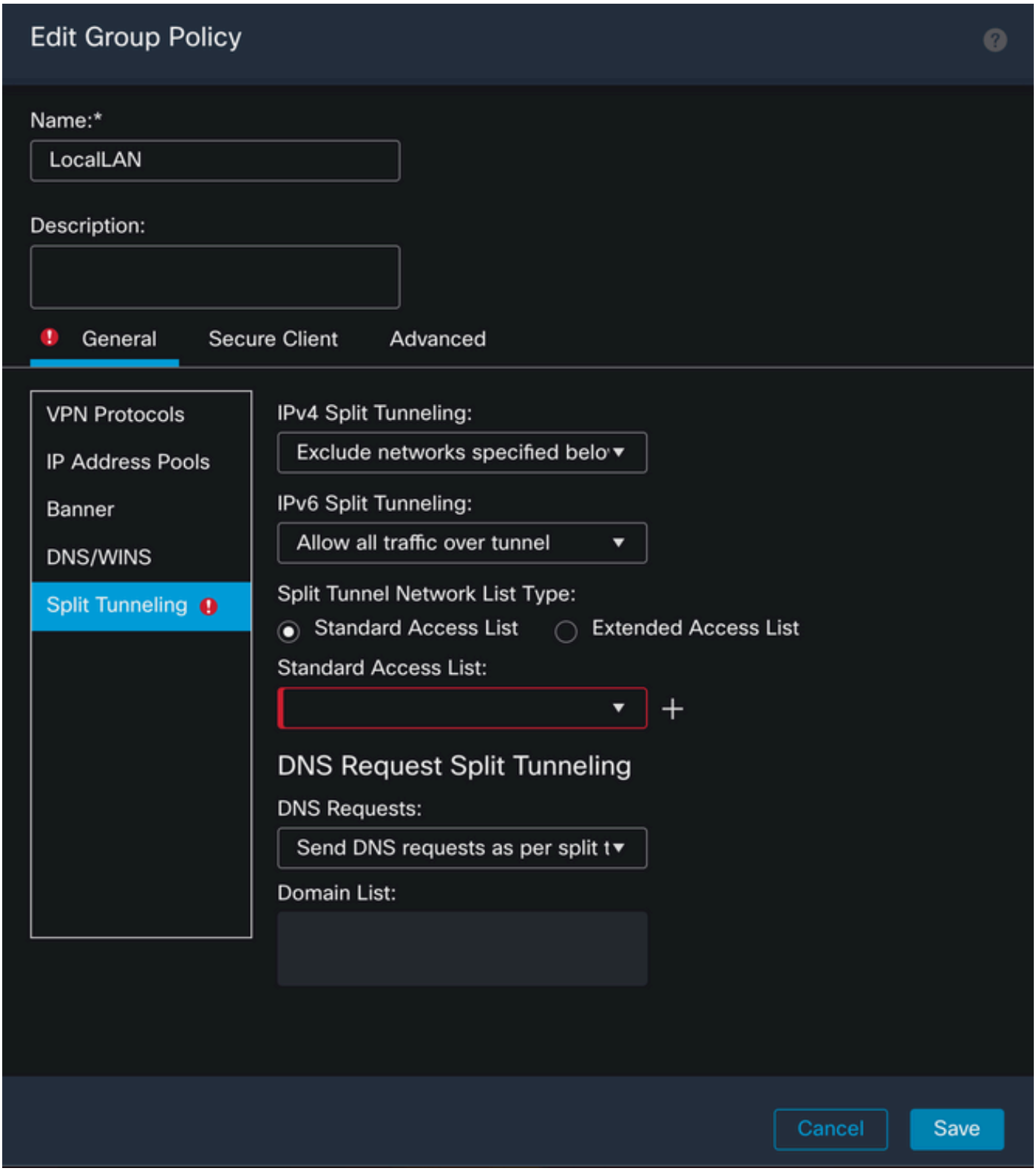
بعد ذلك، انتقل إلى متقدم > نهج المجموعة.



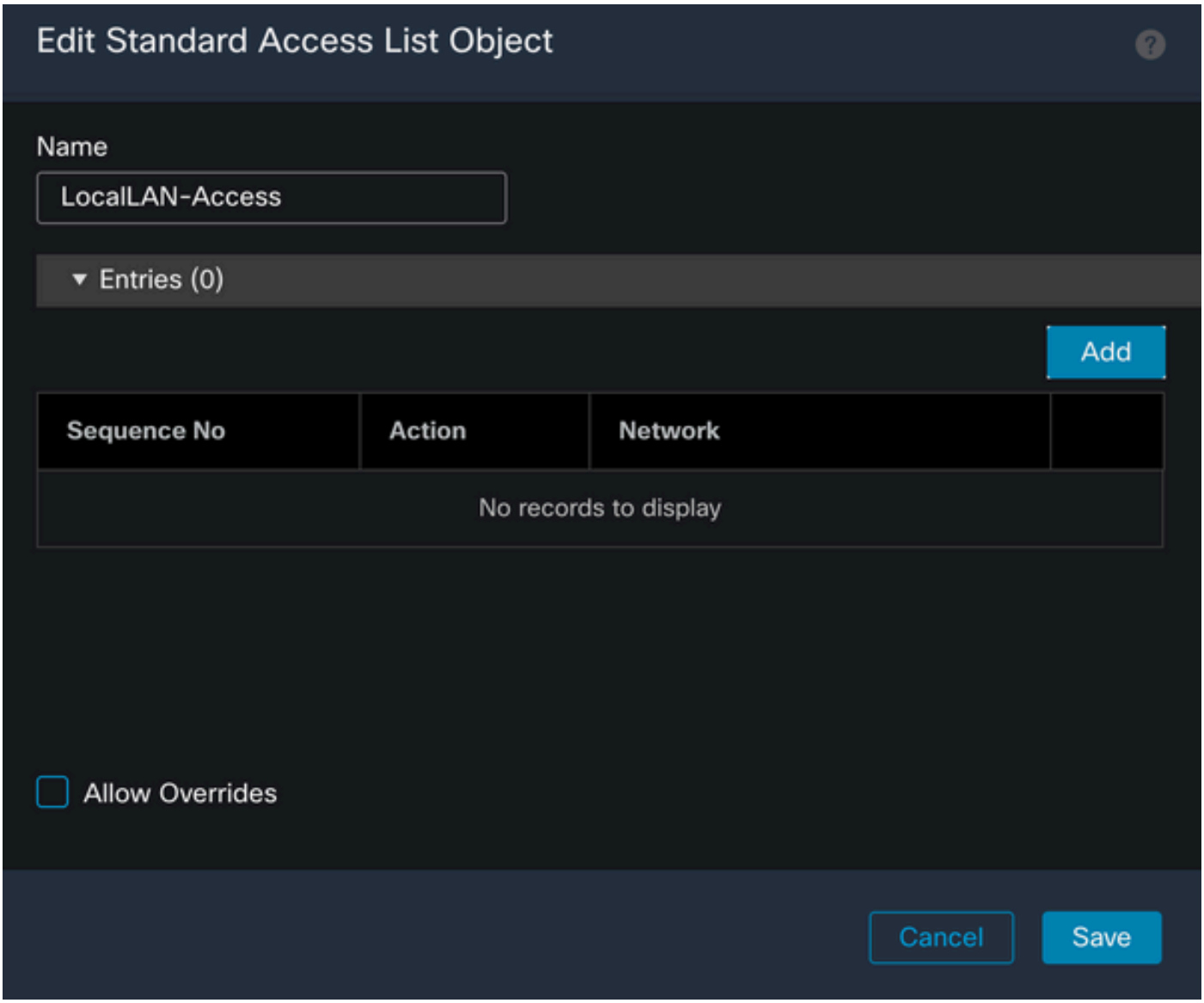
انقر فوق الزر تحرير في "نهج المجموعة" حيث تريد تكوين الوصول إلى شبكة LAN المحلية والانتقال إلى علامة التبويب تقسيم الاتصال النفقي.



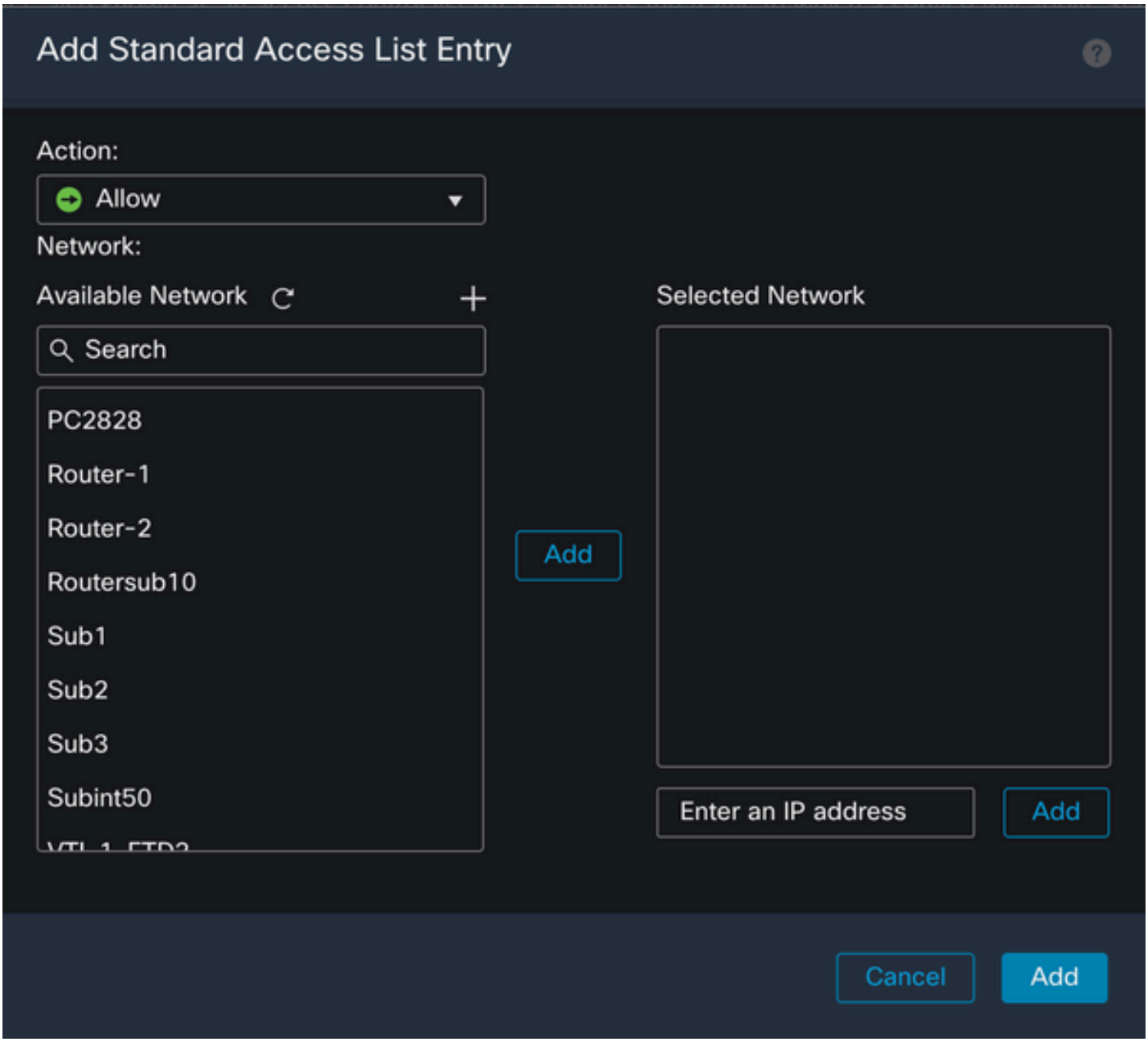
في قسم اتصال IPv4 النفقي، حدد خيار إستثناء الشبكات المحددة أدناه. وهذا يطالب بتحديد قائمة وصول قياسية.



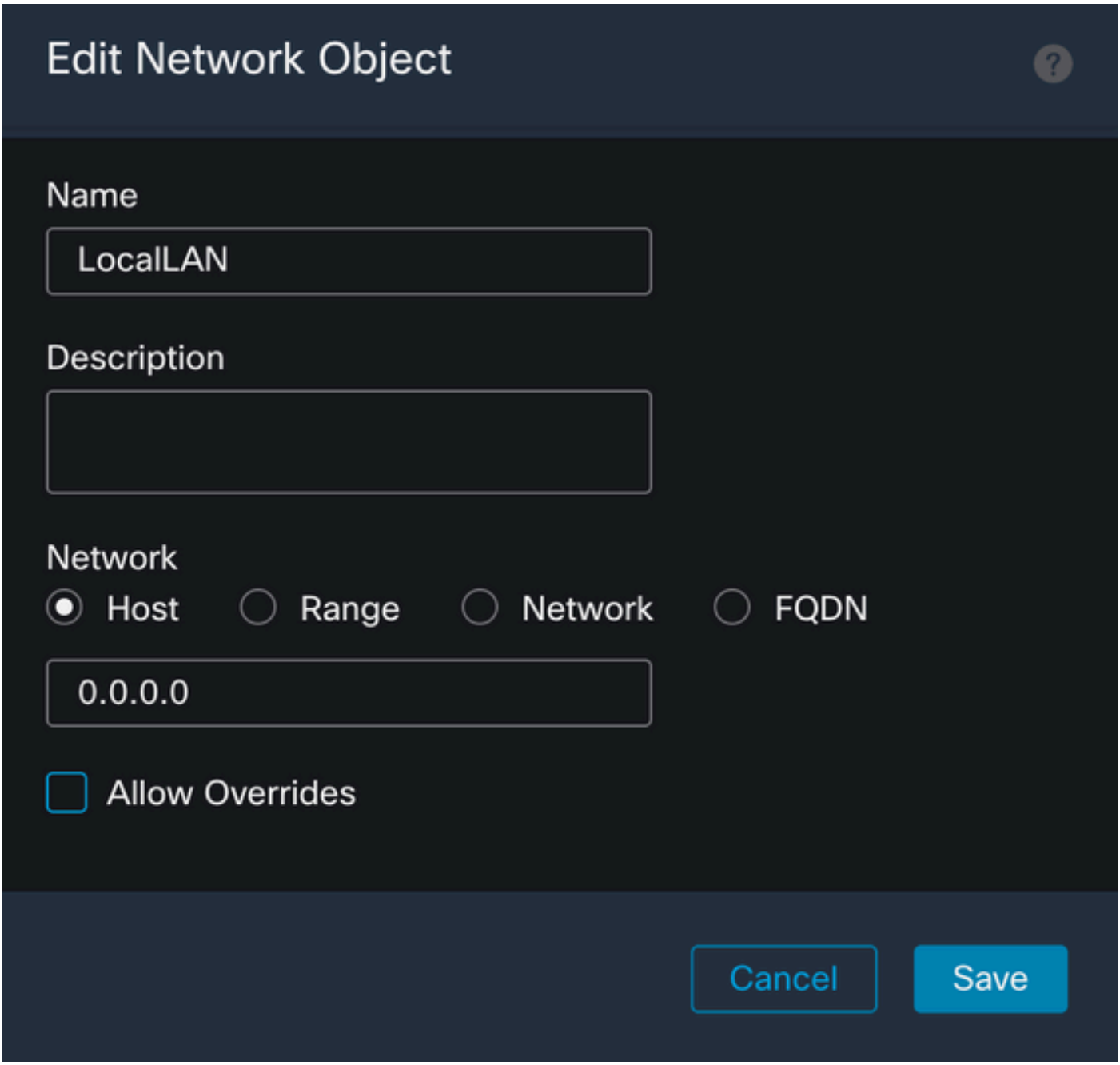
انقر فوق الزر + لإنشاء قائمة وصول قياسية جديدة.



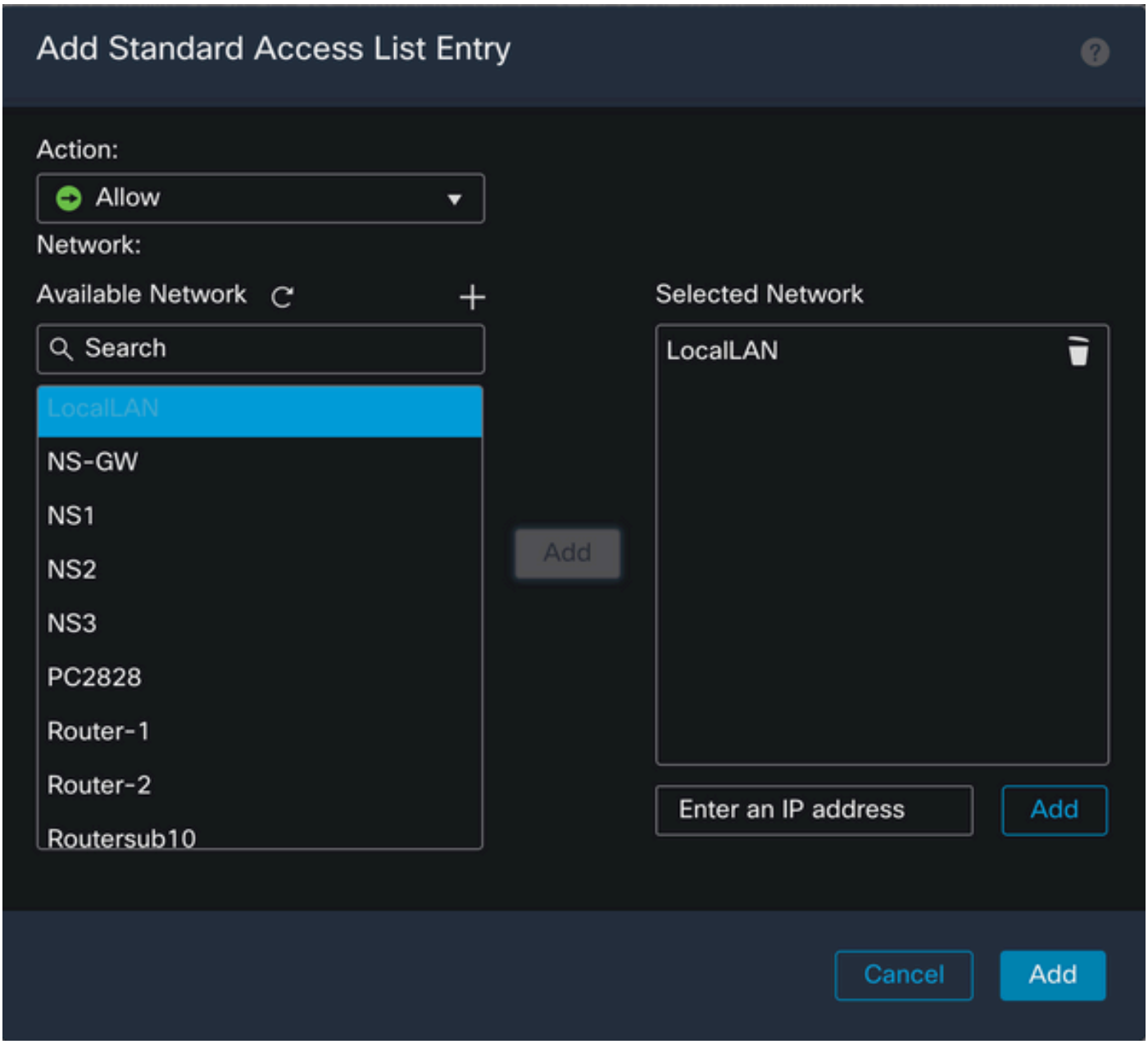
انقر فوق الزر إضافة لإنشاء إدخال قائمة وصول قياسية. يجب تعيين الإجراء لهذا الإدخال على السماح.



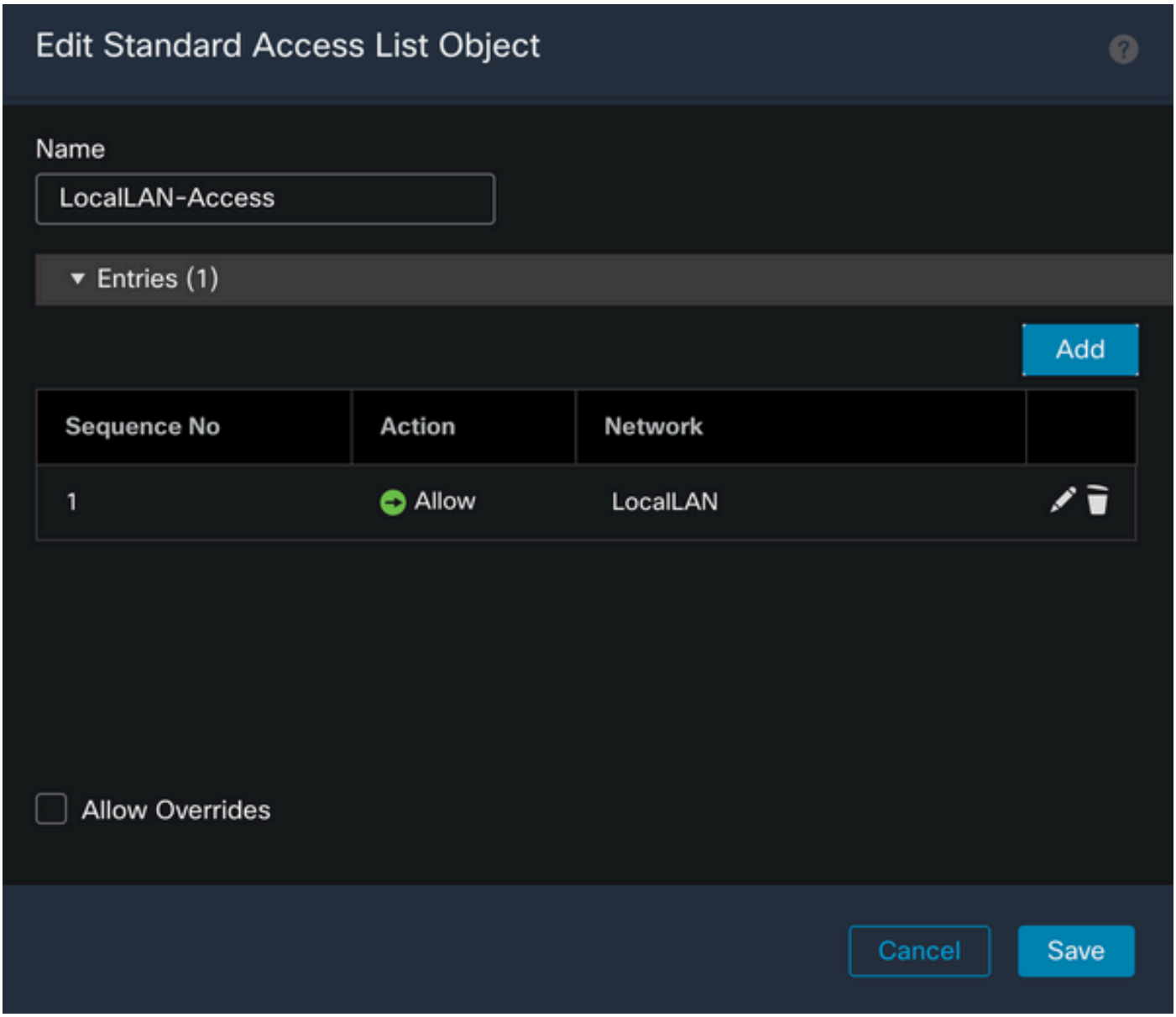
انقر فوق الزر + لإضافة كائن شبكة جديد. تأكد من تعيين هذا الكائن كمضيف في قسم الشبكة وأدخل 0.0.0.0 في المربع.



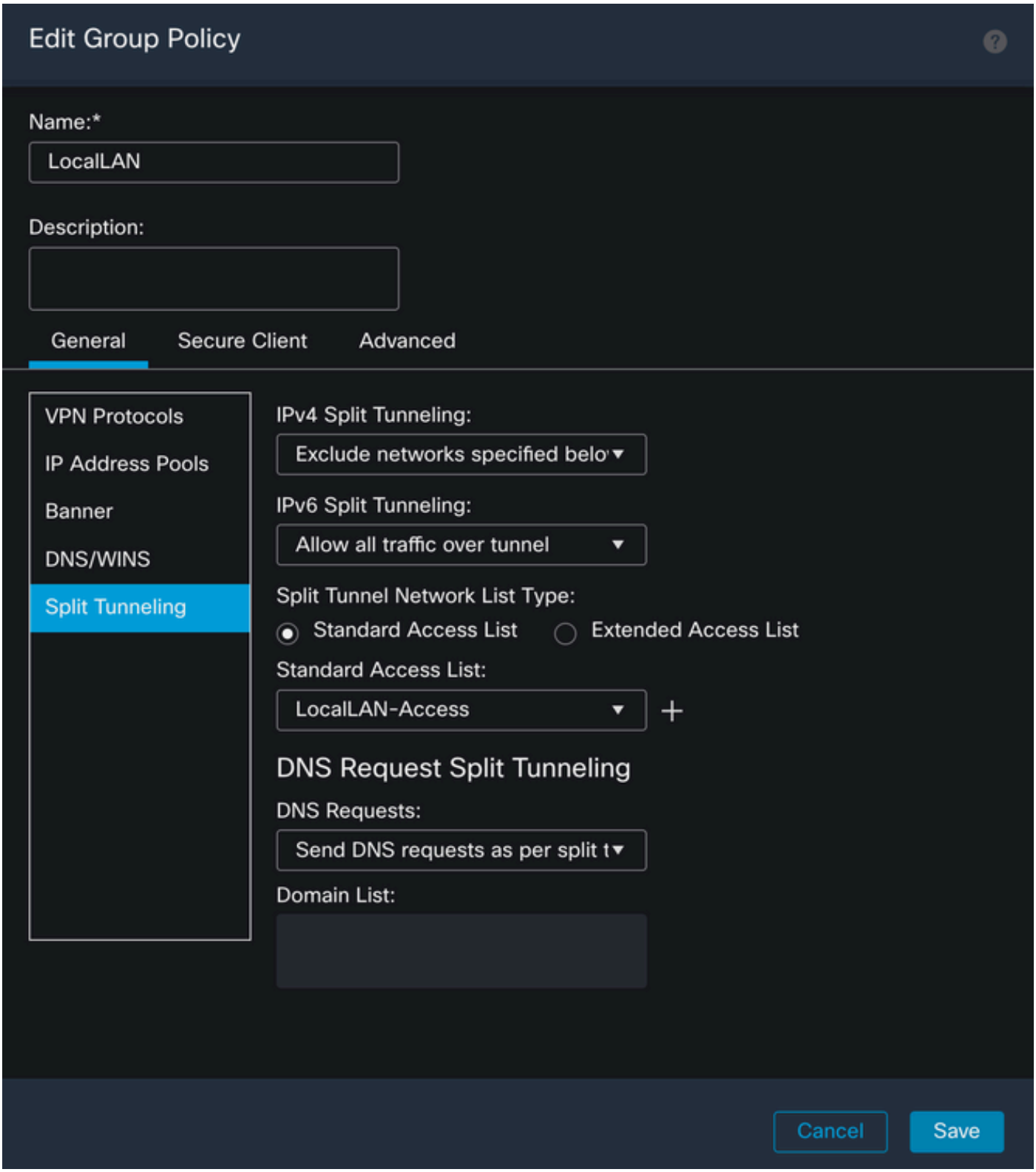
انقر زر حفظ وحدد الكائن الذي تم إنشاؤه حديثا.



انقر فوق الزر إضافة لحفظ إدخال قائمة الوصول القياسية.



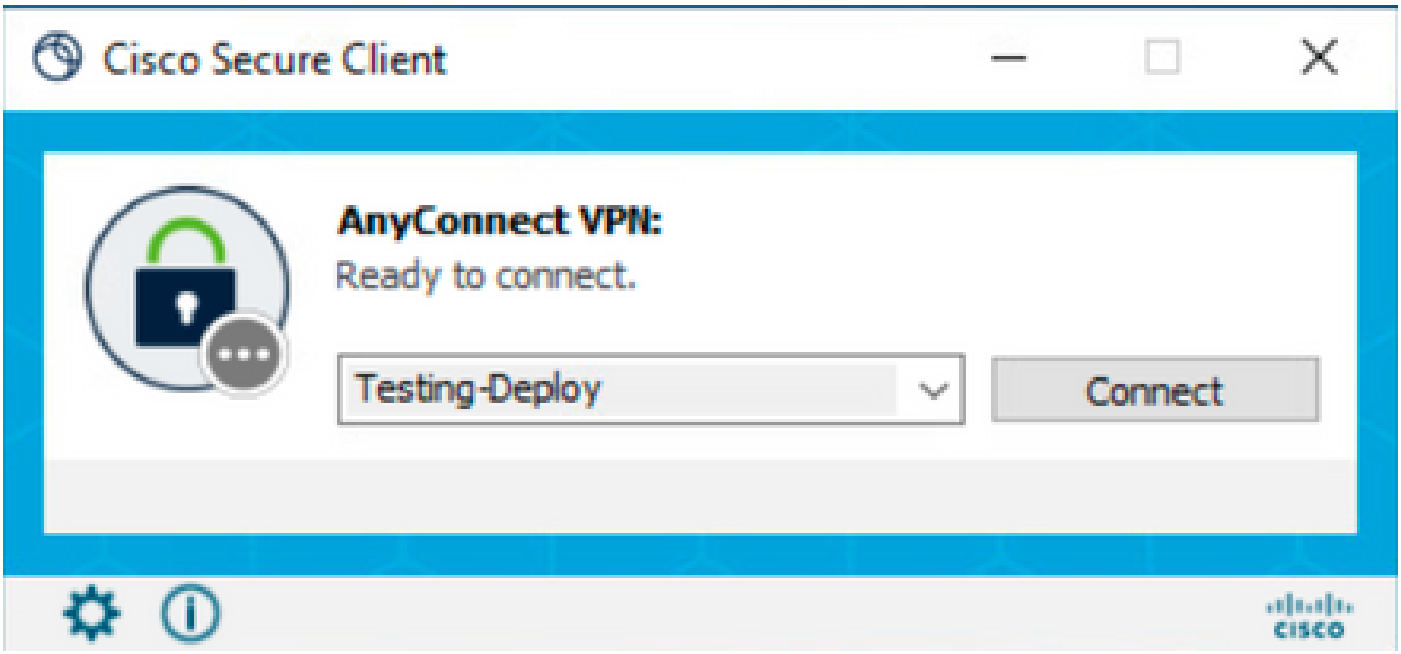
انقر فوق الزر حفظ ويتم تحديد قائمة الوصول القياسية التي تم إنشاؤها حديثا تلقائيا.



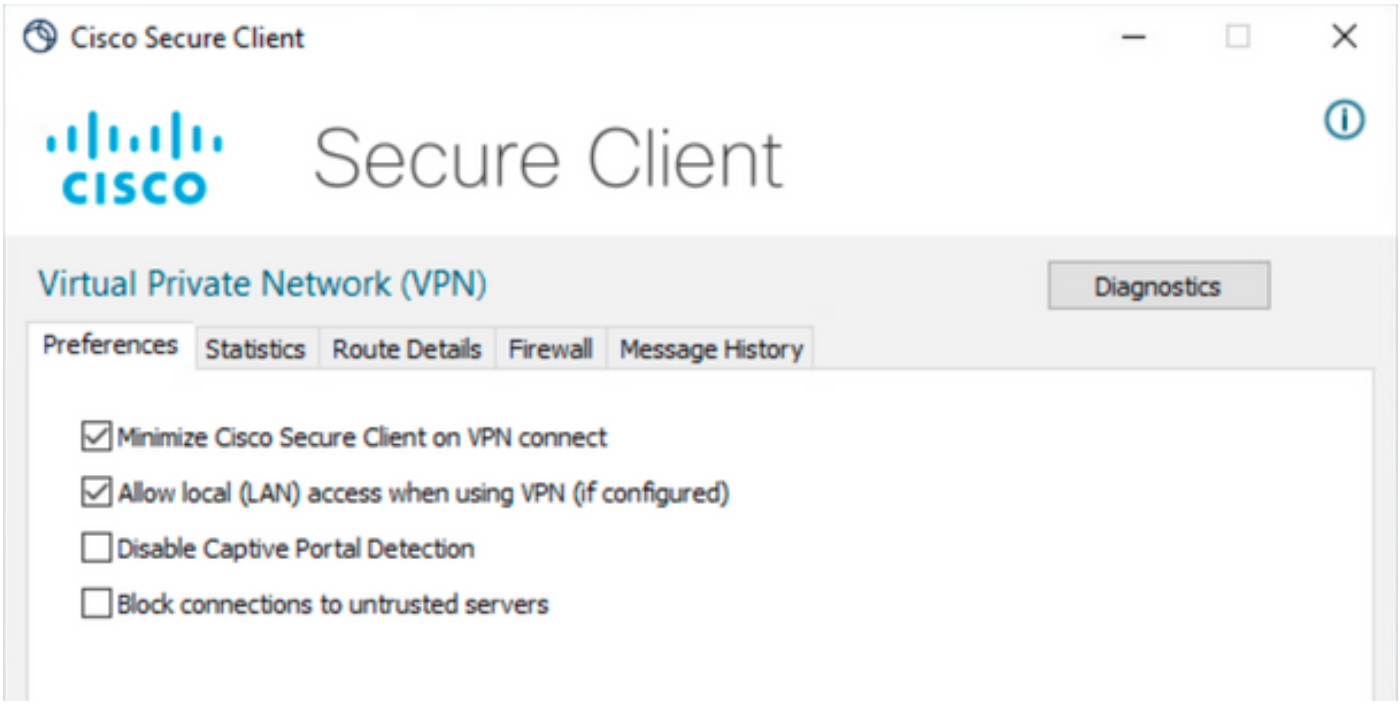
انقر فوق الزر حفظ وقم بنشر التغييرات.

تكوين العميل الآمن

بشكل افتراضي، يتم تعيين خيار الوصول إلى شبكة LAN المحلية إلى User ControlAble. لتمكين الخيار، انقر فوق رمز الترس في واجهة المستخدم الرسومية (GUI) الآمنة للعميل.



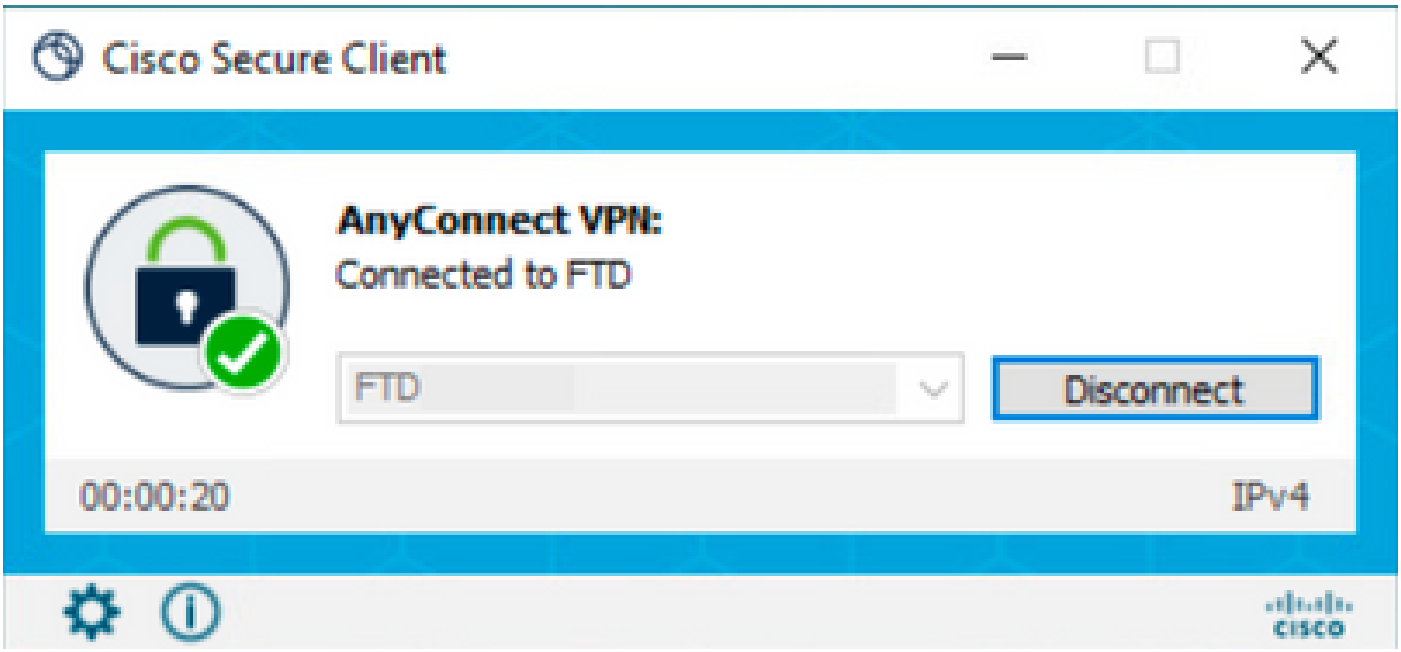
انتقل إلى التفضيلات وتأكد من تمكين خيار السماح بالوصول المحلي (LAN) عند إستخدام شبكة VPN (في حالة تكوينها).



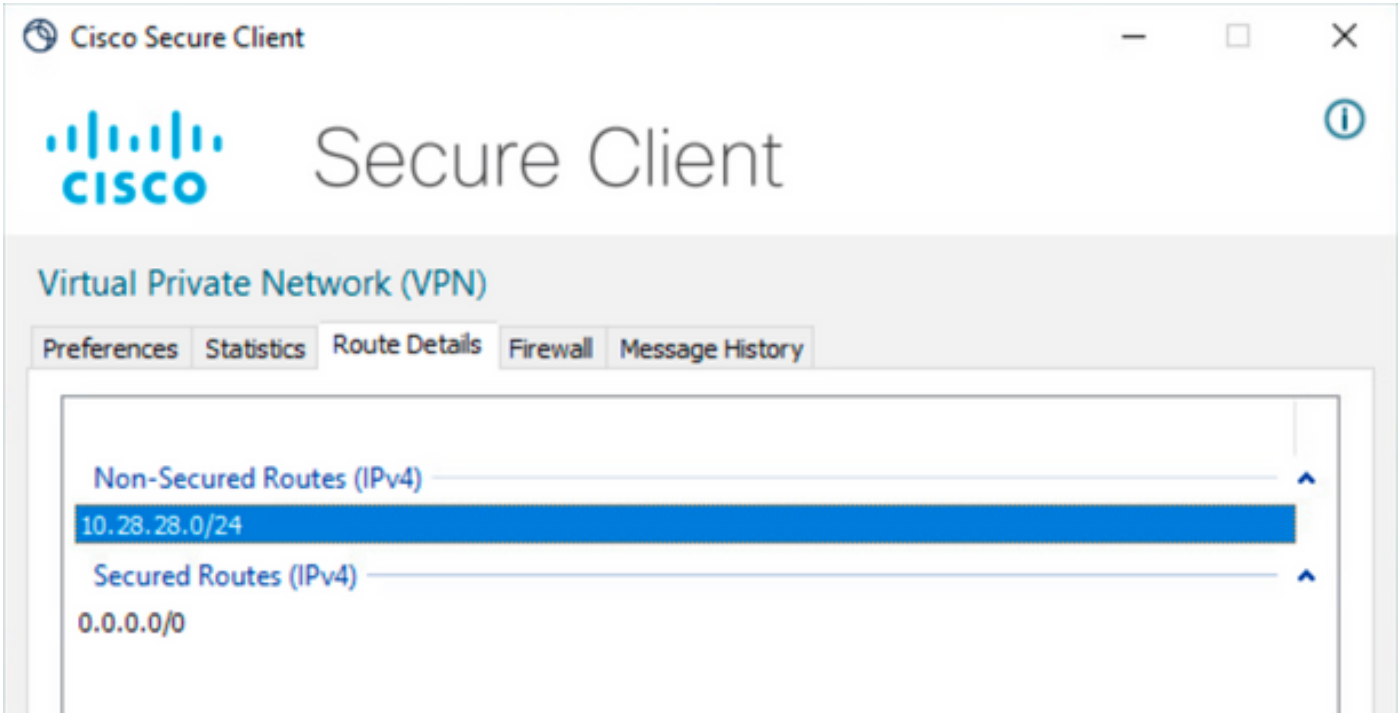
التحقق من الصحة

العميل الآمن

قم بالاتصال بمحطة الاستقبال والبث باستخدام "العميل الآمن".



انقر أيقونة الترس وانتقل إلى تفاصيل المسار. هنا أنت يستطيع رأيت أن ال LAN محلي تلقائيا كشفت واستبعدت من النفق.



واجهة سطر الأوامر في FTD

للتحقق من ما إذا تم تطبيق التكوين بنجاح، يمكنك إستخدام CLI (واجهة سطر الأوامر) الخاصة ب 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
```

استكشاف الأخطاء وإصلاحها

للتحقق من تطبيق ميزة الوصول إلى شبكة LAN المحلية، يمكنك تمكين تصحيح الأخطاء التالية:

```
debug webvpn anyconnect 255
```

هذا مثال على إخراج تصحيح أخطاء ناجح:

<#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
```

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).