

# Konfigurieren des lokalen LAN-Zugriffs für den sicheren Client

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[FMC-Konfiguration](#)

[Sichere Client-Konfiguration](#)

[Überprüfung](#)

[Sicherer Client](#)

[FTD-CLI](#)

[Fehlerbehebung](#)

## Einleitung

In diesem Dokument wird beschrieben, wie Sie den Cisco Secure Client für den Zugriff auf das lokale LAN konfigurieren und gleichzeitig eine sichere Verbindung zum Headend aufrechterhalten.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse zu folgenden Themen verfügen:

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

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- 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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Hintergrundinformationen

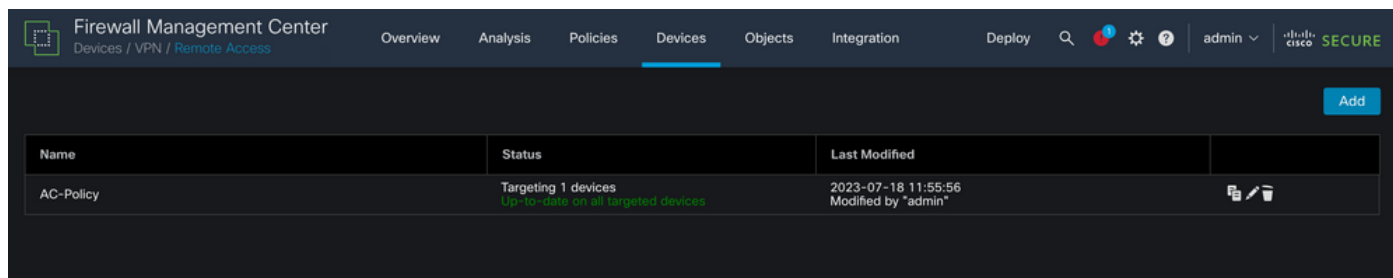
Die in diesem Dokument beschriebene Konfiguration ermöglicht dem Cisco Secure Client den uneingeschränkten Zugriff auf das lokale LAN, ohne dass eine sichere Verbindung zum Headend und zu den Unternehmensressourcen aufrecht erhalten wird. Damit kann der Client einen Netzwerkzugriffsserver (NAS) drucken oder darauf zugreifen.

## Konfigurieren

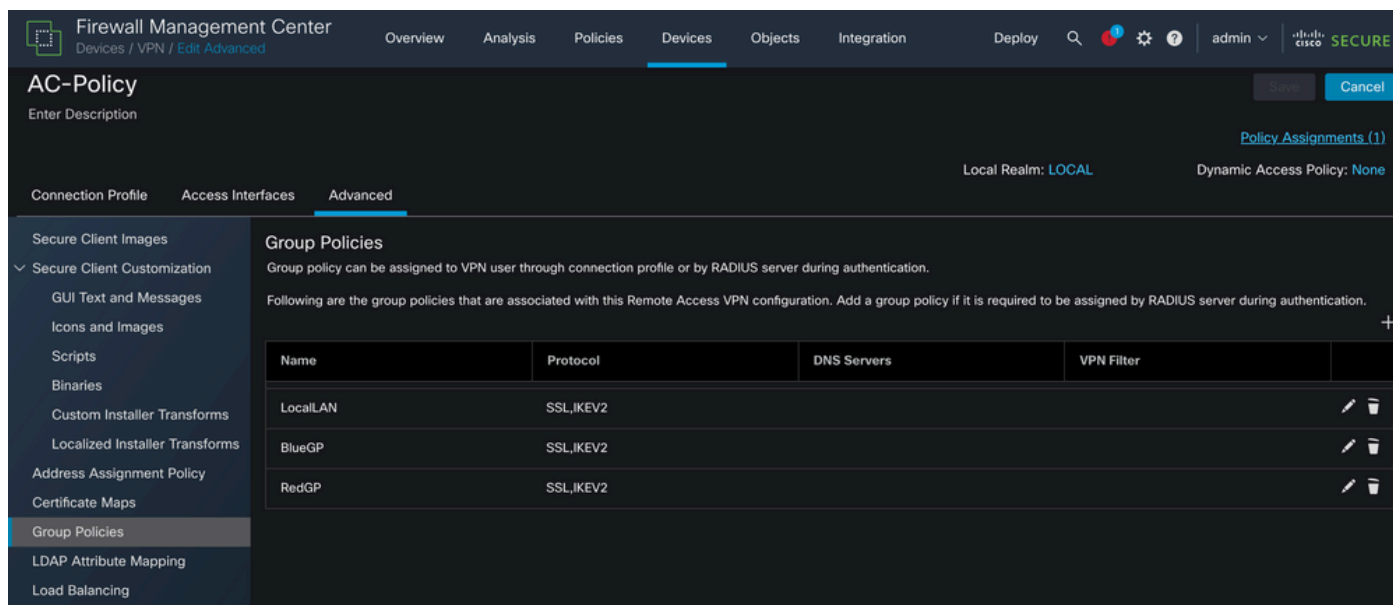
### FMC-Konfiguration

In diesem Dokument wird davon ausgegangen, dass Sie bereits über eine funktionierende VPN-Konfiguration verfügen.

Um die Funktion für lokalen LAN-Zugriff hinzuzufügen, navigieren Sie zu Geräte > Remotezugriff, und klicken Sie in der entsprechenden RAS-Richtlinie auf die Schaltfläche Bearbeiten.



Navigieren Sie dann zu Erweitert > Gruppenrichtlinien.



Klicken Sie in der Gruppenrichtlinie, in der Sie den lokalen LAN-Zugriff konfigurieren möchten, auf die Schaltfläche Edit, und navigieren Sie zur Registerkarte Split Tunneling.

**Edit Group Policy** ?

Name:\*  
LocalLAN

Description:

General    Secure Client    Advanced

VPN Protocols  
IP Address Pools  
Banner  
DNS/WINS  
**Split Tunneling**

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:

Cancel    Save

Wählen Sie im Abschnitt IPv4 Split Tunneling die Option Exclude networks (unten angegebene Netzwerke ausschließen) aus. Sie werden zur Auswahl einer Standard-Zugriffsliste aufgefordert.

## Edit Group Policy



Name:\*

LocalLAN

Description:



General

Secure Client

Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IPv4 Split Tunneling:

Exclude networks specified below ▼

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:

Cancel

Save

Klicken Sie auf die Schaltfläche +, um eine neue Standard-Zugriffsliste zu erstellen.

## Edit Standard Access List Object



Name

LocalLAN-Access

▼ Entries (0)

Add

Sequence No

Action

Network

No records to display

Allow Overrides

Cancel

Save

Klicken Sie auf die Schaltfläche Hinzufügen, um einen Eintrag in der Standard-Zugriffsliste zu erstellen. Die Aktion dieses Eintrags muss auf Zulassen eingestellt sein.

## Add Standard Access List Entry



Action:

Network:

Available Network

- PC2828
- Router-1
- Router-2
- Routersub10
- Sub1
- Sub2
- Sub3
- Subint50
- VLAN 1 - FTDP

Selected Network

Klicken Sie auf die Schaltfläche +, um ein neues Netzwerkobjekt hinzuzufügen. Stellen Sie sicher, dass dieses Objekt im Abschnitt Netzwerk als Host festgelegt ist, und geben Sie 0.0.0.0 in das Feld ein.

## Edit Network Object



Name

Description

Network

Host    Range    Network    FQDN

Allow Overrides

Cancel

Save

Klicken Sie auf die Schaltfläche Speichern, und wählen Sie das neu erstellte Objekt aus.

## Add Standard Access List Entry



Action:

Network:

Available Network

- LocalLAN
- NS-GW
- NS1
- NS2
- NS3
- PC2828
- Router-1
- Router-2
- Routersub10

Selected Network

LocalLAN

Klicken Sie auf die Schaltfläche Hinzufügen, um den Eintrag Standard-Zugriffsliste zu speichern.



## Edit Standard Access List Object






Name

LocalLAN-Access

▼ Entries (1)

Add

Sequence No	Action	Network	
1	 Allow	LocalLAN	 

Allow Overrides

Cancel

Save

Klicken Sie auf die Schaltfläche Speichern, und die neu erstellte Standard-Zugriffsliste wird automatisch ausgewählt.

## Edit Group Policy ?

Name:\*

Description:

**General**   Secure Client   Advanced

VPN Protocols

IP Address Pools

Banner

DNS/WINS

Split Tunneling

IPv4 Split Tunneling:

IPv6 Split Tunneling:

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

Standard Access List:  
 +

**DNS Request Split Tunneling**

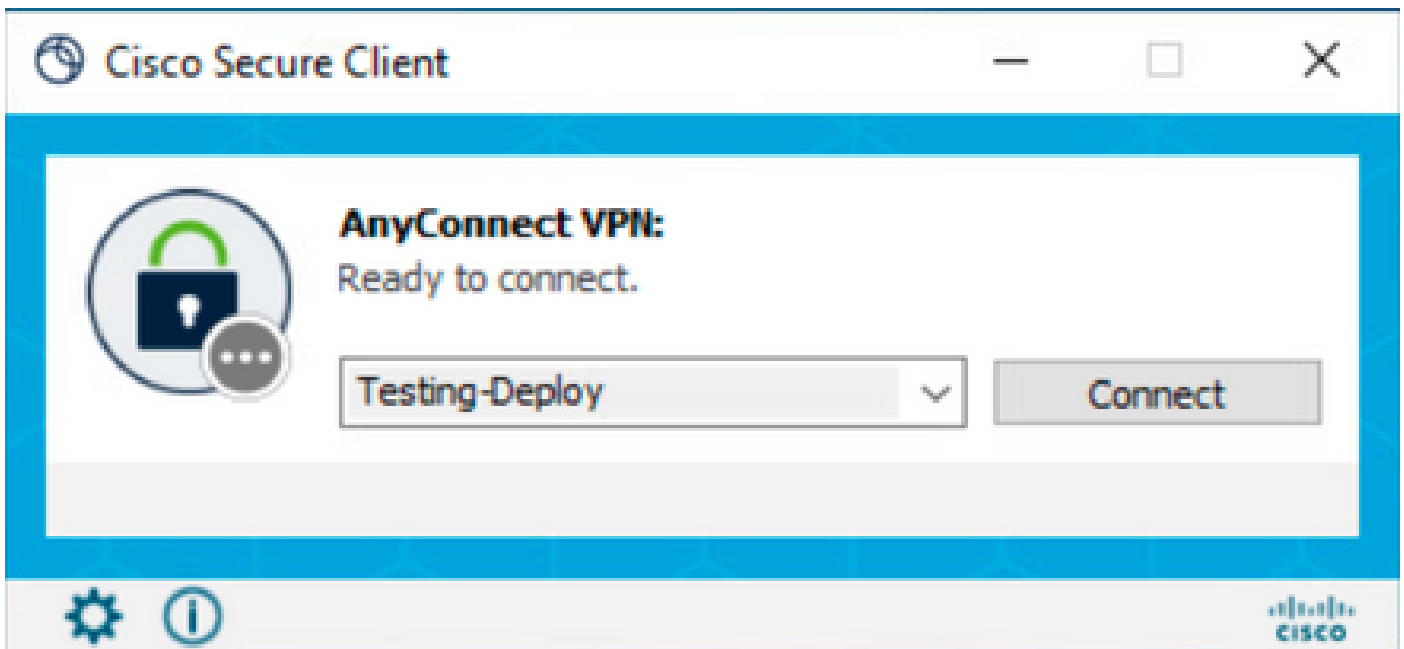
DNS Requests:

Domain List:

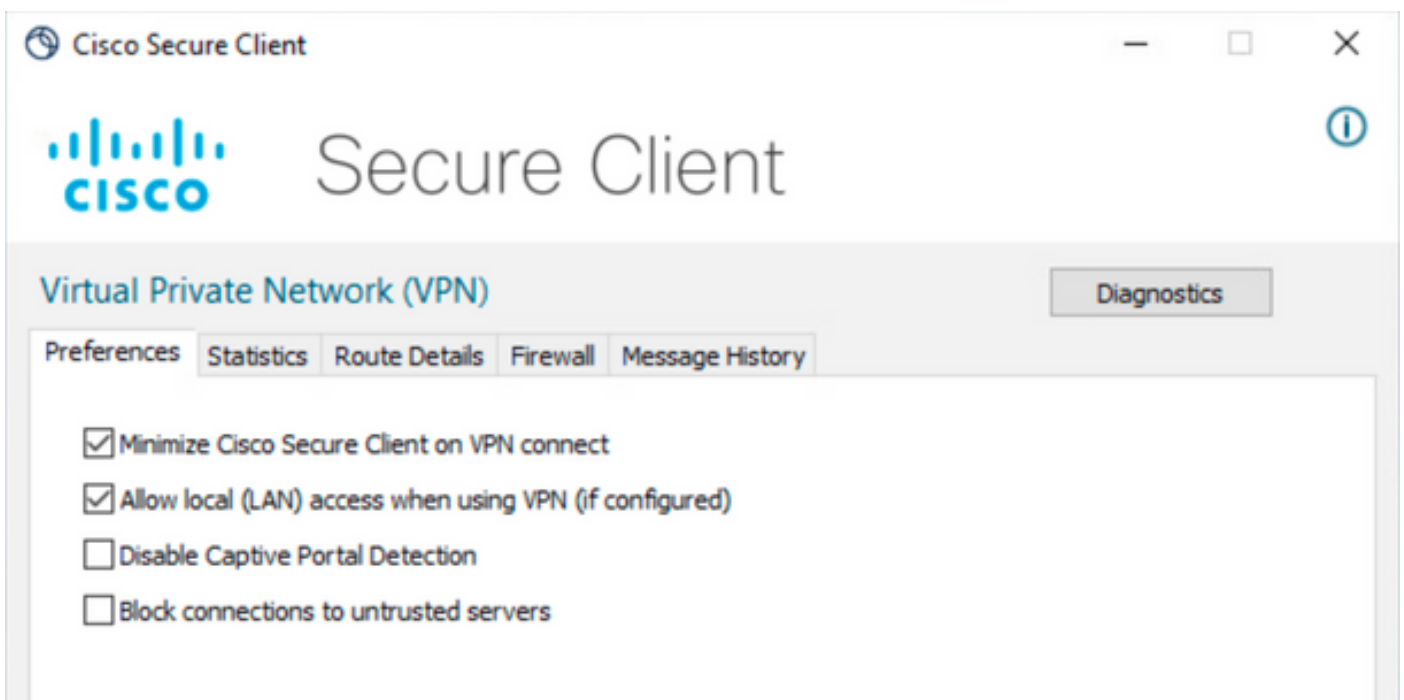
Klicken Sie auf die Schaltfläche Speichern, und stellen Sie die Änderungen bereit.

## Sichere Client-Konfiguration

Standardmäßig ist die Option Lokaler LAN-Zugriff auf Benutzersteuerbar eingestellt. Um die Option zu aktivieren, klicken Sie in der Secure Client-GUI auf das Zahnrad-Symbol.



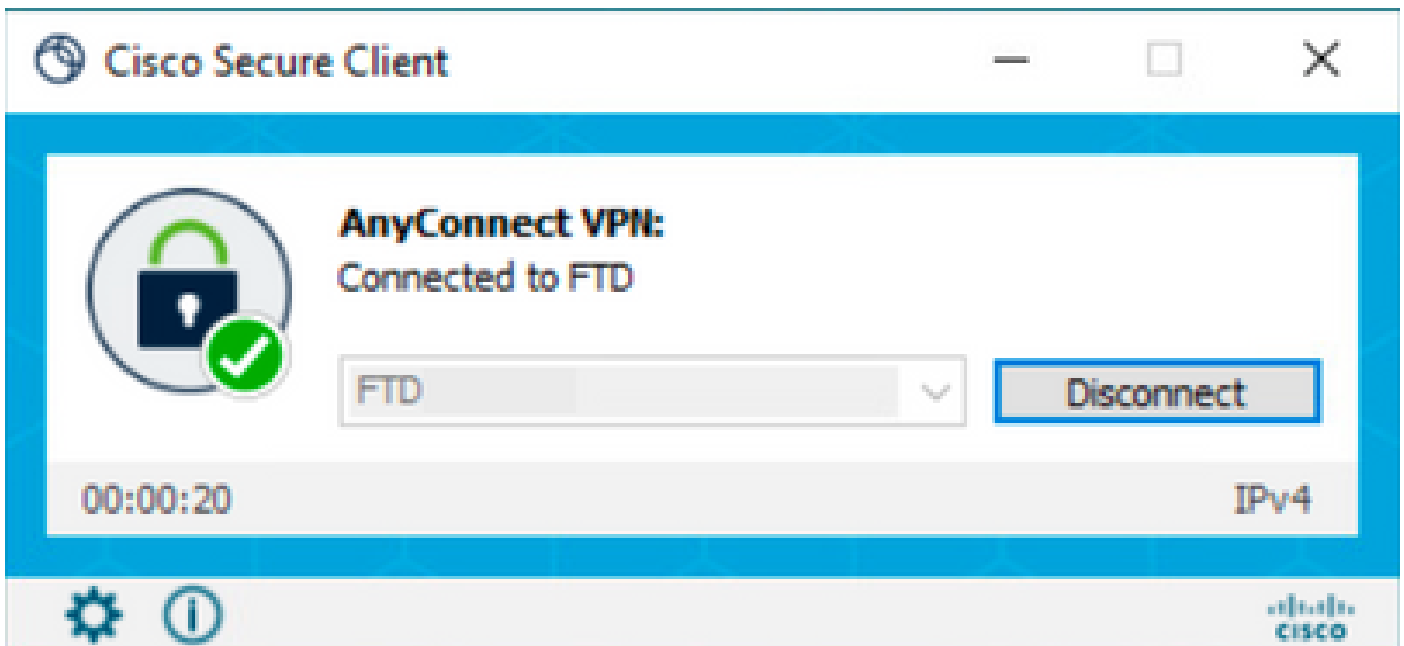
Navigieren Sie zu Preferences (Voreinstellungen), und stellen Sie sicher, dass die Option Allow local (LAN) access when using VPN (if configured) aktiviert ist.



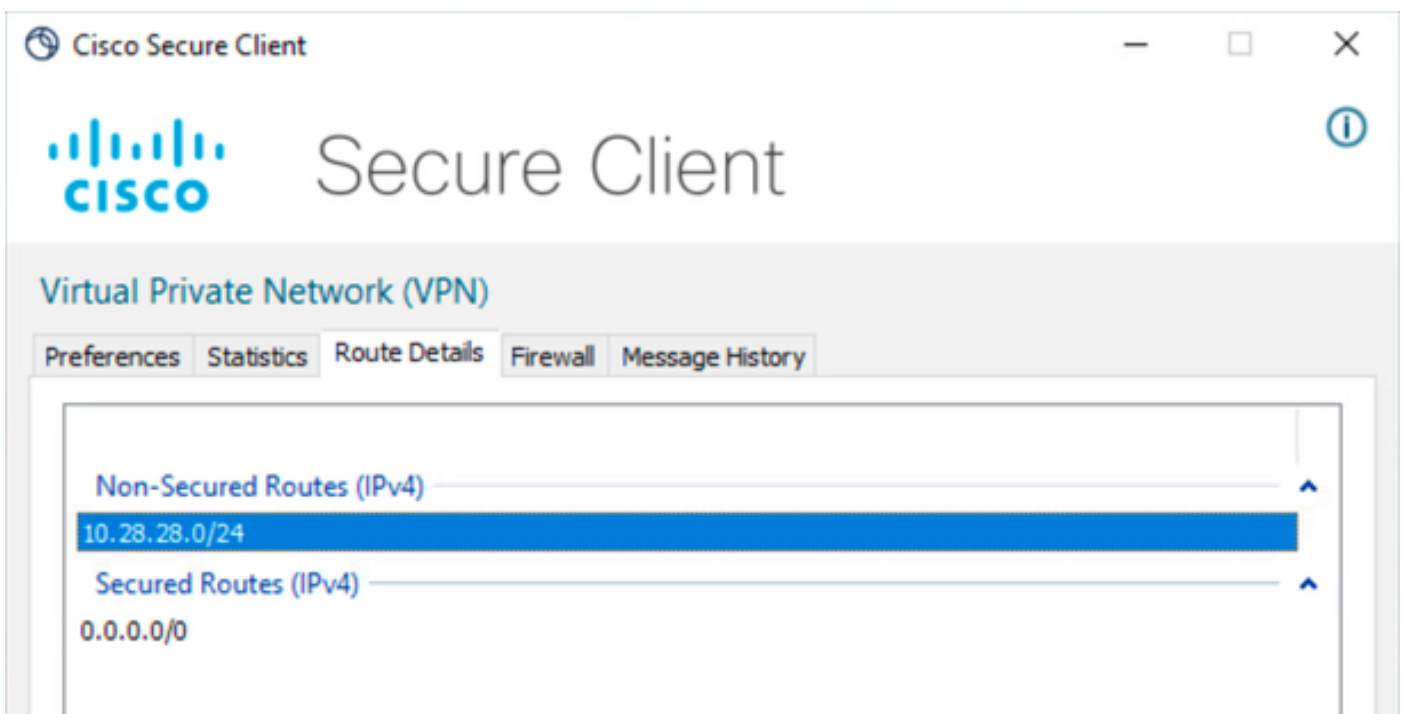
## Überprüfung

### Sicherer Client

Stellen Sie über den Secure Client eine Verbindung zum Headend her.



Klicken Sie auf das Zahnrad-Symbol, und navigieren Sie zu Route Details (Routendetails). Hier können Sie sehen, dass das lokale LAN automatisch erkannt und aus dem Tunnel ausgeschlossen wird.



## FTD-CLI

Um zu überprüfen, ob die Konfiguration erfolgreich angewendet wurde, können Sie die CLI des FTD verwenden.

```
<#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
```

## Fehlerbehebung

Um zu überprüfen, ob die Funktion für den lokalen LAN-Zugriff angewendet wurde, können Sie die folgenden Debug-Vorgänge aktivieren:

```
debug webvpn anyconnect 255
```

Dies ist ein Beispiel für eine erfolgreiche Debugausgabe:

<#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 successful, 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@BF38A398B90D09039C60B55929055D33AE31BA05'

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: MFkwEwYHKOZIZj0CAQYIKoZIZj0DAQcDQgAEkzG6nj9HDKz/zLa3Yz+QJDHOYwft6'

Setting Anyconnect STRAP rekey public key(len: 124): MFkwEwYHKOZIZj0CAQYIKoZIZj0DAQcDQgAEkzG6nj9HDKz/zLa3Yz+QJDHOYwft6

webvpn\_cstp\_parse\_request\_field()

...input: 'X-AnyConnect-STRAP-Verify: MEQCICzX1yDWLXQHn10hOXV+/OI1/O1LjBic/Nu/K2+N6E5GAiA5CLAF6Bt0tcxhj'

Processing CSTP header line: 'X-AnyConnect-STRAP-Verify: MEQCICzX1yDWLXQHn10hOXV+/OI1/O1LjBic/Nu/K2+N6E5GAiA5CLAF6Bt0tcxhj'

Setting Anyconnect STRAP client signature(len: 96): MEQCICzX1yDWLXQHn10hOXV+/OI1/O1LjBic/Nu/K2+N6E5GAiA5CLAF6Bt0tcxhj

webvpn\_cstp\_parse\_request\_field()

...input: 'X-DTLS-Master-Secret: 0224D83639071BBF29E2D77B15B762FE85BD50D1F0EF9758942B75DF9A97C709325C3E'

Processing CSTP header line: 'X-DTLS-Master-Secret: 0224D83639071BBF29E2D77B15B762FE85BD50D1F0EF9758942B75DF9A97C709325C3E'

webvpn\_cstp\_parse\_request\_field()

...input: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-RSA-AES128-GCM-SHA256'

Processing CSTP header line: 'X-DTLS-CipherSuite: DHE-RSA-AES256-GCM-SHA384:DHE-RSA-AES256-SHA256:DHE-RSA-AES128-GCM-SHA256'

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:ECDSA-AES256-GCM-SHA384:ECDSA-AES256-SHA384:ECDSA-RSA-AES256-SHA384'

```
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 assigned: 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) & 0xffff0(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(dtls_hdr) - 16(dtls_iv) = 1443
mod-mtu = 1443(mtu) & 0xffff0(complement) = 1440
dtls-mtu = 1440(mod-mtu) - 1(cstp) - 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
```

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.