

Configurazione dell'accesso LAN locale per client protetto

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configurazione FMC](#)

[Configurazione client sicura](#)

[Verifica](#)

[Secure Client](#)

[CLI FTD](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare Cisco Secure Client per accedere alla LAN locale e mantenere una connessione sicura all'headend.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

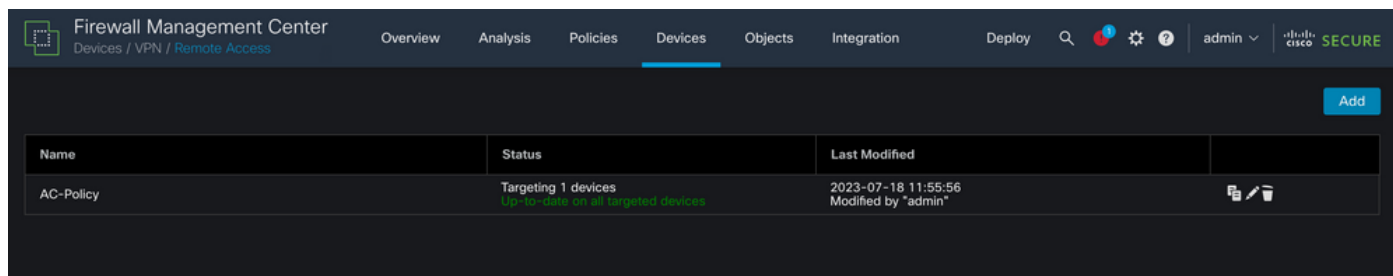
La configurazione descritta in questo documento consente a Cisco Secure Client di avere accesso completo alla LAN locale mantenendo una connessione sicura all'headend e alle risorse aziendali. Può essere utilizzato per consentire al client di stampare o accedere a un server di accesso alla rete (NAS, Network Access Server).

Configurazione

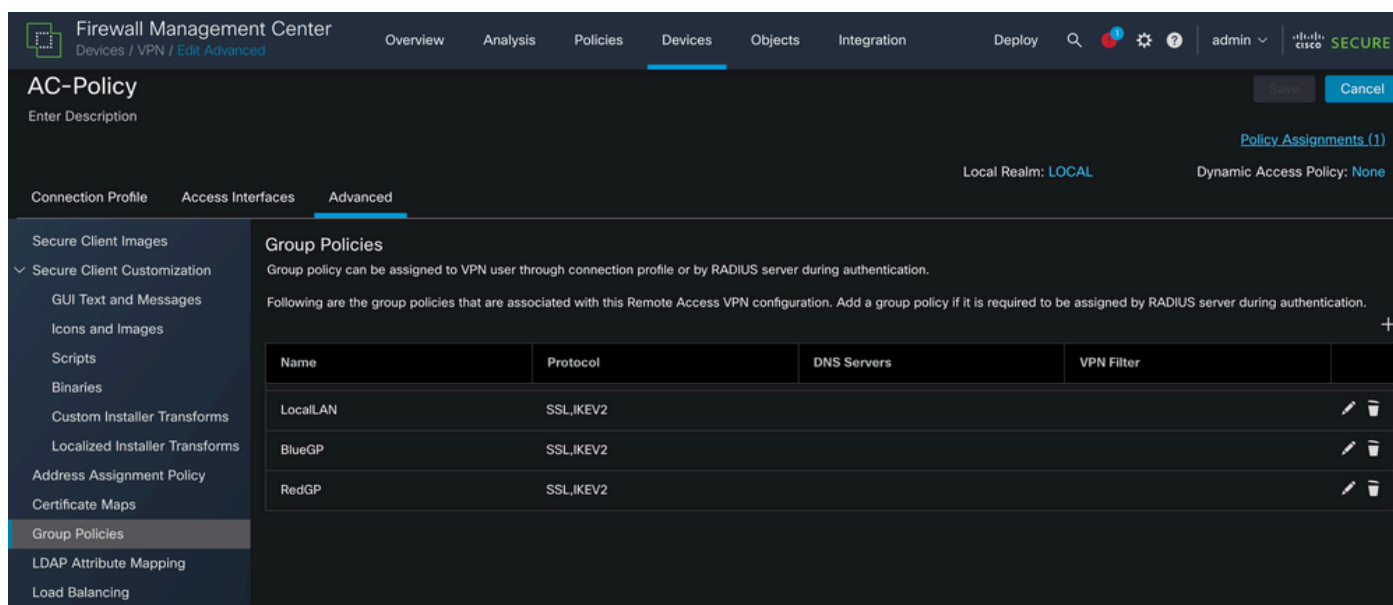
Configurazione FMC

In questo documento si presume che l'utente disponga già di una configurazione VPN ad accesso remoto funzionante.

Per aggiungere la funzionalità di accesso LAN locale, selezionare Dispositivi > Accesso remoto e fare clic sul pulsante Modifica nella policy di accesso remoto appropriata.



Passare quindi a Avanzate > Criteri di gruppo.



Fare clic sul pulsante Modifica in Criteri di gruppo in cui si desidera configurare l'accesso LAN locale e passare alla scheda Tunneling ripartito.

The screenshot shows the 'Edit Group Policy' window with the 'Split Tunneling' section selected in the left-hand menu. The 'Name' field contains 'LocalLAN' and the 'Description' field is empty. The 'General' tab is active. The 'Split Tunneling' section includes the following settings:

- VPN Protocols**
- IP Address Pools**
- Banner**
- DNS/WINS**
- Split Tunneling** (selected)

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: [Empty dropdown] +

DNS Request Split Tunneling

DNS Requests: Send DNS requests as per split t

Domain List: [Empty text area]

Buttons: Cancel, Save

Nella sezione Tunneling ripartito IPv4, selezionare l'opzione Escludi reti specificate di seguito. In questo modo viene richiesta la selezione di un elenco degli accessi standard.

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

Fare clic sul pulsante + per creare un nuovo elenco degli accessi standard.

Edit Standard Access List Object



Name

LocalLAN-Access

▼ Entries (0)

Add

Sequence No

Action

Network

No records to display

Allow Overrides

Cancel

Save

Fare clic sul pulsante Aggiungi per creare una voce dell'elenco accessi standard. L'azione di questa voce deve essere impostata su Consenti.

Add Standard Access List Entry



Action:

Network:

Available Network

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

Selected Network

Fare clic sul pulsante + per aggiungere un nuovo oggetto di rete. Verificare che l'oggetto sia impostato come host nella sezione Rete e immettere 0.0.0.0 nella casella.

Edit Network Object



Name

Description

Network

Host Range Network FQDN

Allow Overrides

Cancel

Save

Fare clic sul pulsante Salva e selezionare il nuovo oggetto creato.

Add Standard Access List Entry



Action:

Network:

Available Network

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

Selected Network

LocalLAN

Fare clic sul pulsante Aggiungi per salvare la voce dell'elenco degli accessi standard.

Edit Standard Access List Object






Name

LocalLAN-Access

▼ Entries (1)

Add

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

Allow Overrides

Cancel

Save

Fare clic sul pulsante Salva per selezionare automaticamente il nuovo elenco degli accessi standard creato.

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:
LocalLAN-Access ▼ +

DNS Request Split Tunneling
DNS Requests:
Send DNS requests as per split t ▼

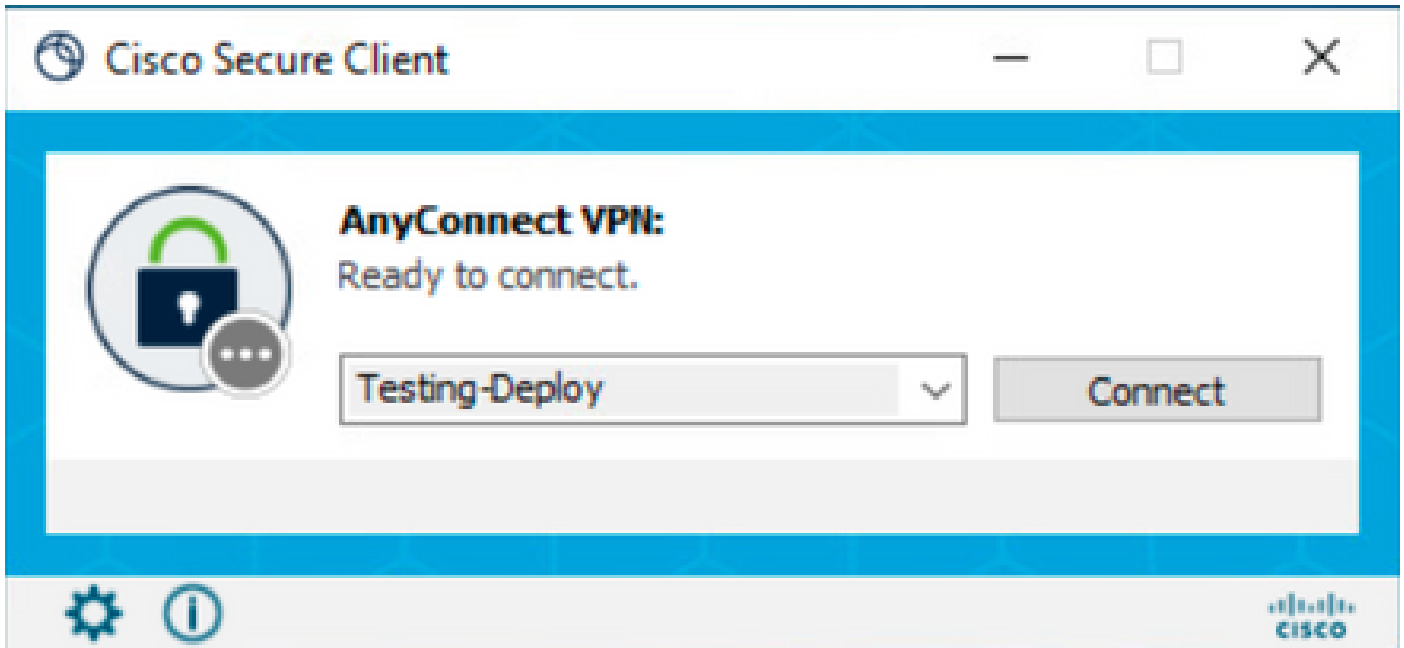
Domain List:

Cancel Save

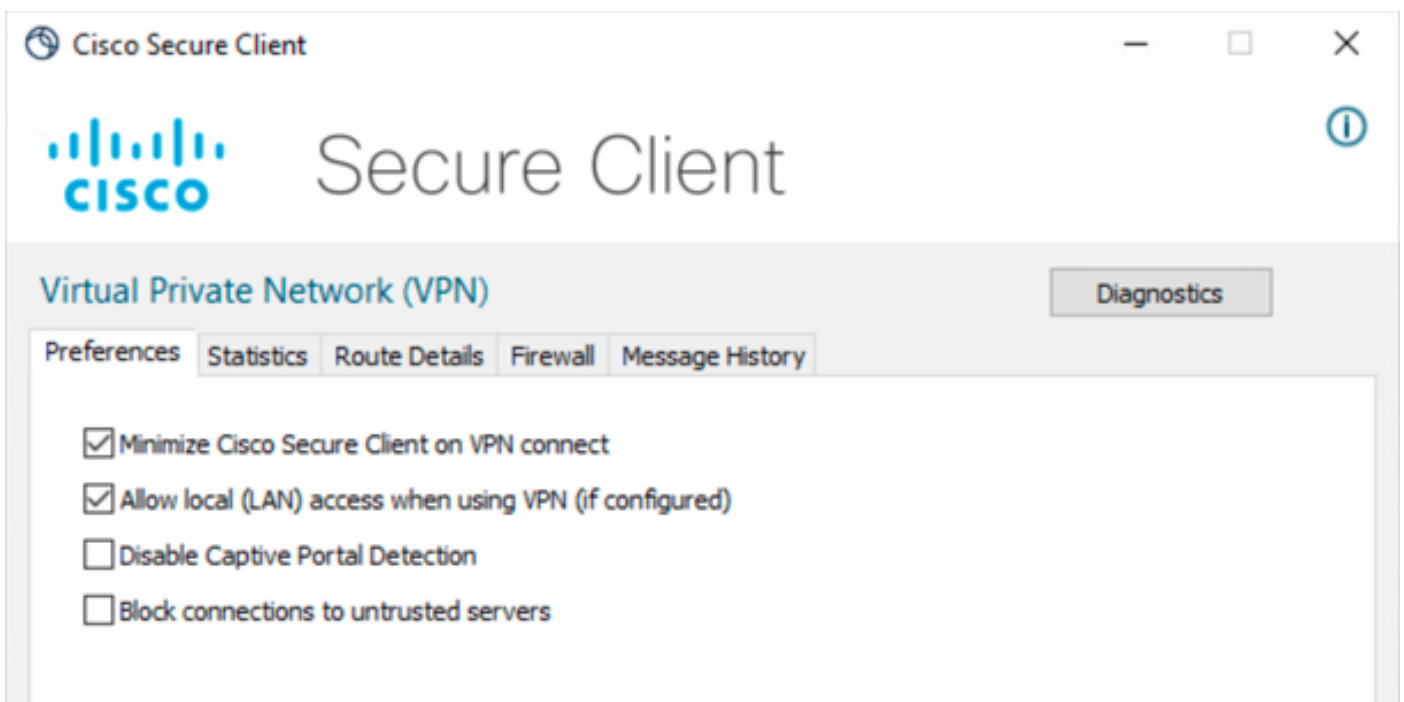
Fare clic sul pulsante Salva e distribuire le modifiche.

Configurazione client sicura

Per impostazione predefinita, l'opzione Accesso LAN locale è impostata su Controllabile dall'utente. Per abilitare l'opzione, fare clic sull'icona Gear nell'interfaccia utente Secure Client.



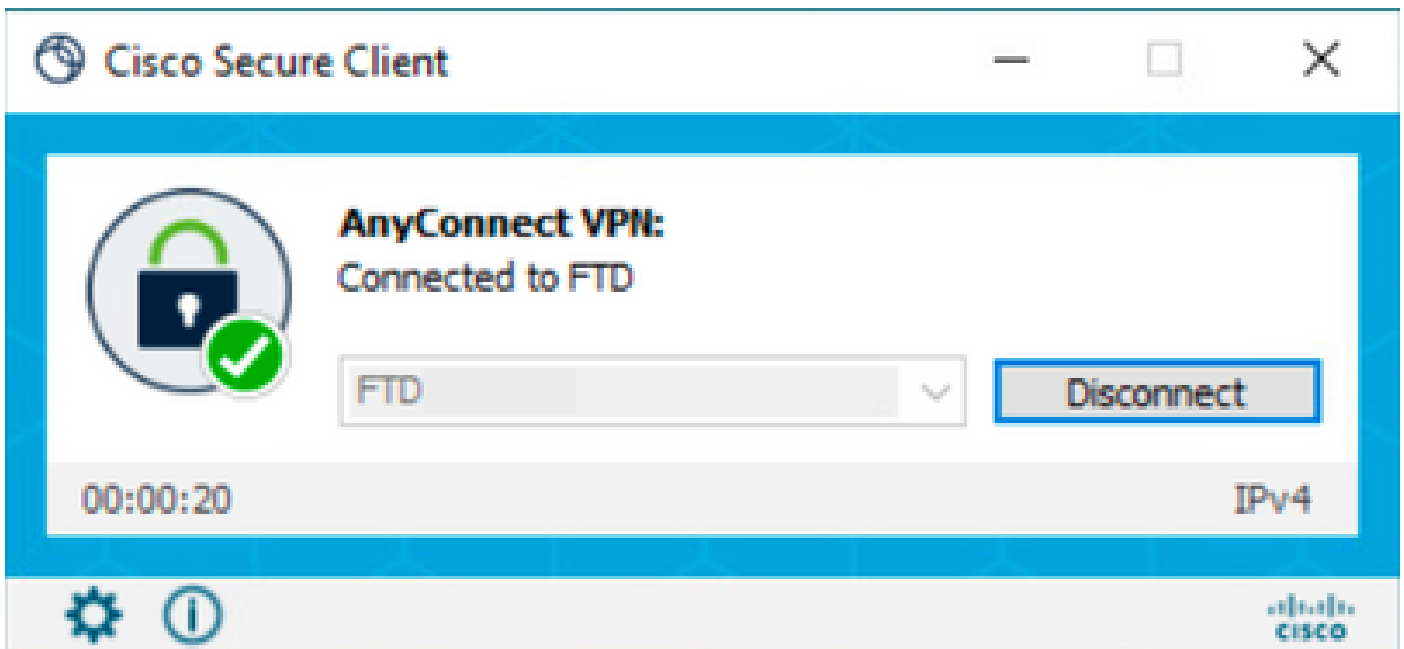
Passare a Preferenze e verificare che l'opzione Consenti accesso locale (LAN) quando si utilizza VPN (se configurata) sia abilitata.



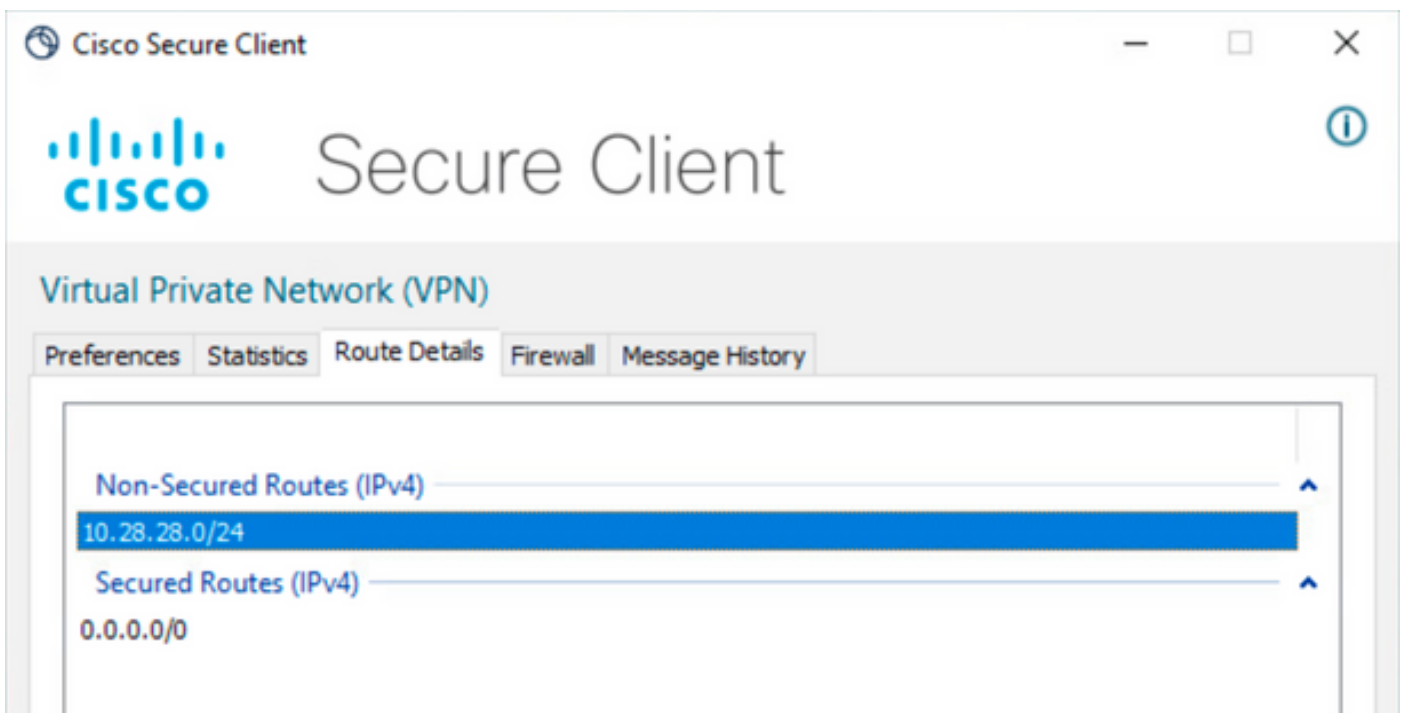
Verifica

Secure Client

Connettersi all'headend utilizzando Secure Client.



Fare clic sull'icona Ingranaggio e passare a Dettagli instradamento. Qui è possibile vedere che la LAN locale viene rilevata automaticamente ed esclusa dal tunnel.



CLI FTD

Per verificare se la configurazione è stata applicata correttamente, è possibile usare la CLI dell'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
```

Risoluzione dei problemi

Per verificare se la funzione di accesso LAN locale è stata applicata, è possibile abilitare i seguenti debug:

```
debug webvpn anyconnect 255
```

Questo è un esempio di output di debug riuscito:

<#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@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-AES128-GCM-SHA256'
```

```
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: lz'
Processing CSTL header line: 'X-DTLS-Accept-Encoding: lz'
webvpn_cstp_parse_request_field()
...input: 'X-DTLS-Header-Pad-Length: 0'
webvpn_cstp_parse_request_field()
...input: 'X-CSTP-Accept-Encoding: lz,deflate'
Processing CSTP header line: 'X-CSTP-Accept-Encoding: lz,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
```

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).