

Configuración del acceso LAN local para Secure Client

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[configuración de FMC](#)

[Configuración de Secure Client](#)

[Verificación](#)

[Cliente seguro](#)

[CLI FTD](#)

[Troubleshoot](#)

Introducción

Este documento describe cómo configurar Cisco Secure Client para acceder a la LAN local y aún así mantener una conexión segura con la cabecera.

Prerequisites

Requirements

Cisco recomienda que tenga conocimientos sobre estos temas:

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

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Appliance virtual Cisco Secure Firewall Management Center versión 7.3
- Appliance Virtual Cisco Firepower Threat Defense Versión 7.3
- Cisco Secure Client versión 5.0.02075

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

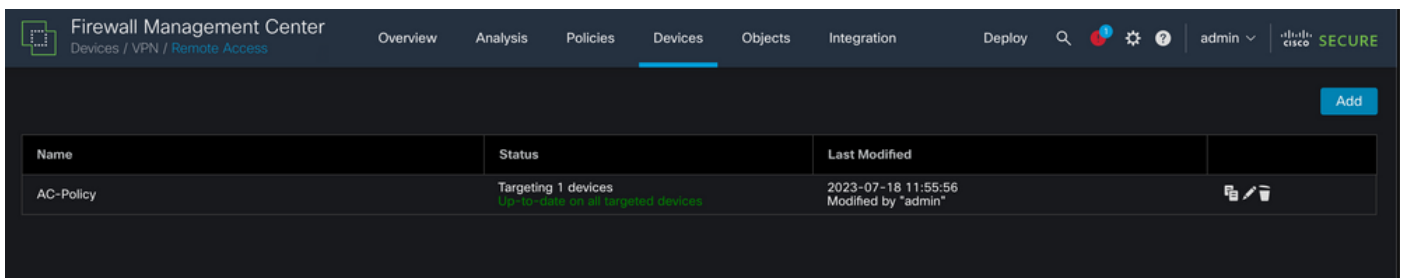
La configuración descrita en este documento permite que Cisco Secure Client tenga acceso completo a la LAN local mientras mantiene una conexión segura con la cabecera y los recursos corporativos. Esto se puede utilizar para permitir que el cliente imprima o acceda a un servidor de acceso a la red (NAS).

Configurar

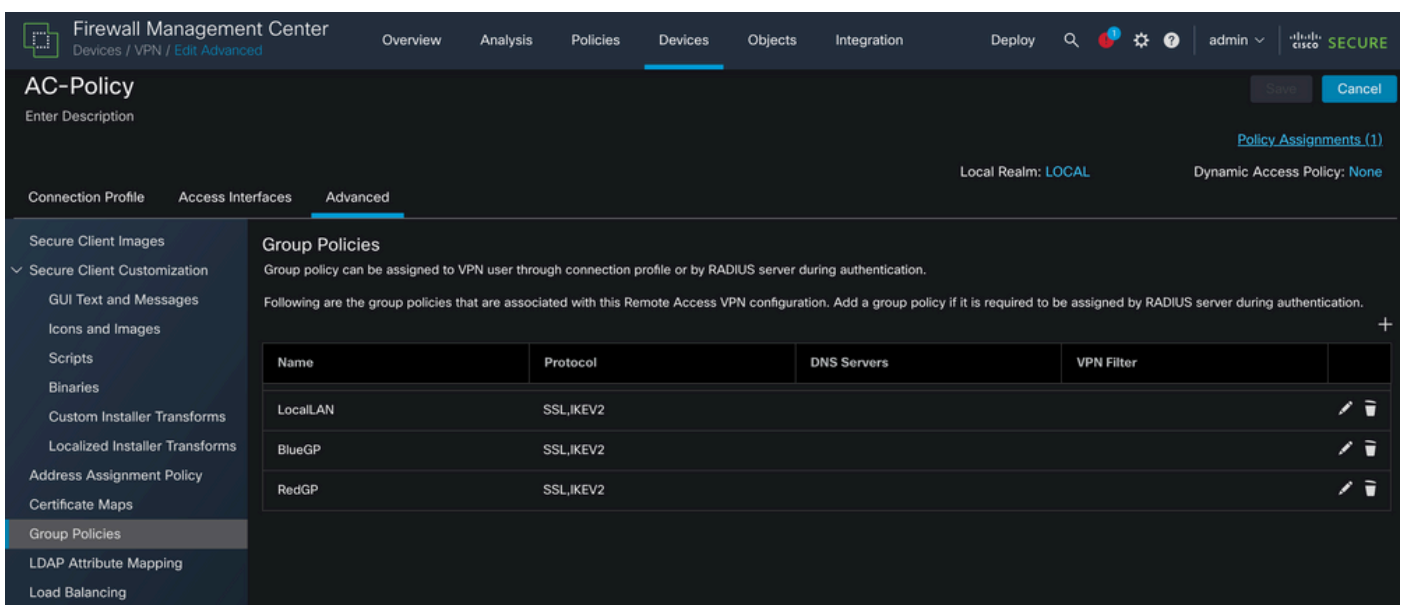
configuración de FMC

En este documento, se supone que ya tiene una configuración de VPN de acceso remoto en funcionamiento.

Para agregar la capacidad de acceso LAN local, navegue hasta Devices > Remote Access y haga clic en el botón Edit en la política de acceso remoto apropiada.



Luego, navegue hasta Avanzadas > Políticas de grupo.



Haga clic en el botón Edit de la Directiva de grupo en la que desea configurar el acceso LAN local y navegue hasta la pestaña Split Tunneling.

The screenshot shows the 'Edit Group Policy' window with the following configuration details:

- Name:** LocalLAN
- Description:** (Empty text box)
- Tabs:** General (selected), Secure Client, Advanced
- Left Navigation Menu:** VPN Protocols, IP Address Pools, Banner, DNS/WINS, Split Tunneling (highlighted)
- 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 menu with a plus sign)
- DNS Request Split Tunneling:**
 - DNS Requests:** Send DNS requests as per split t
 - Domain List:** (Empty text box)
- Buttons:** Cancel, Save

En la sección IPv4 Split Tunneling, seleccione la opción Excluir redes especificadas a continuación. Esto solicita una selección de lista de acceso estándar.

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

Haga clic en el botón + para crear una nueva lista de acceso estándar.

Edit Standard Access List Object



Name

LocalLAN-Access

▼ Entries (0)

Add

Sequence No

Action

Network

No records to display

Allow Overrides

Cancel

Save

Haga clic en el botón Add para crear una entrada de lista de acceso estándar. La Acción de esta entrada debe establecerse en Permitir.

Add Standard Access List Entry



Action:

Network:

Available Network

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

Selected Network

Haga clic en el botón + para agregar un nuevo objeto de red. Asegúrese de que este objeto esté configurado como Host en la sección Red e ingrese 0.0.0.0 en el cuadro.

Edit Network Object



Name

Description

Network

Host Range Network FQDN

Allow Overrides

Cancel

Save

Haga clic en el botón Save y seleccione el objeto recién creado.

Add Standard Access List Entry



Action:

▾

Network:

Available Network

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

Selected Network

LocalLAN

Haga clic en el botón Add para guardar la entrada Standard Access List.

Edit Standard Access List Object






Name

LocalLAN-Access

▼ Entries (1)

Add

Sequence No	Action	Network	
1	 Allow	LocalLAN	 

Allow Overrides

Cancel

Save

Haga clic en el botón Save y la lista de acceso estándar recién creada se seleccionará automáticamente.

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 ▼

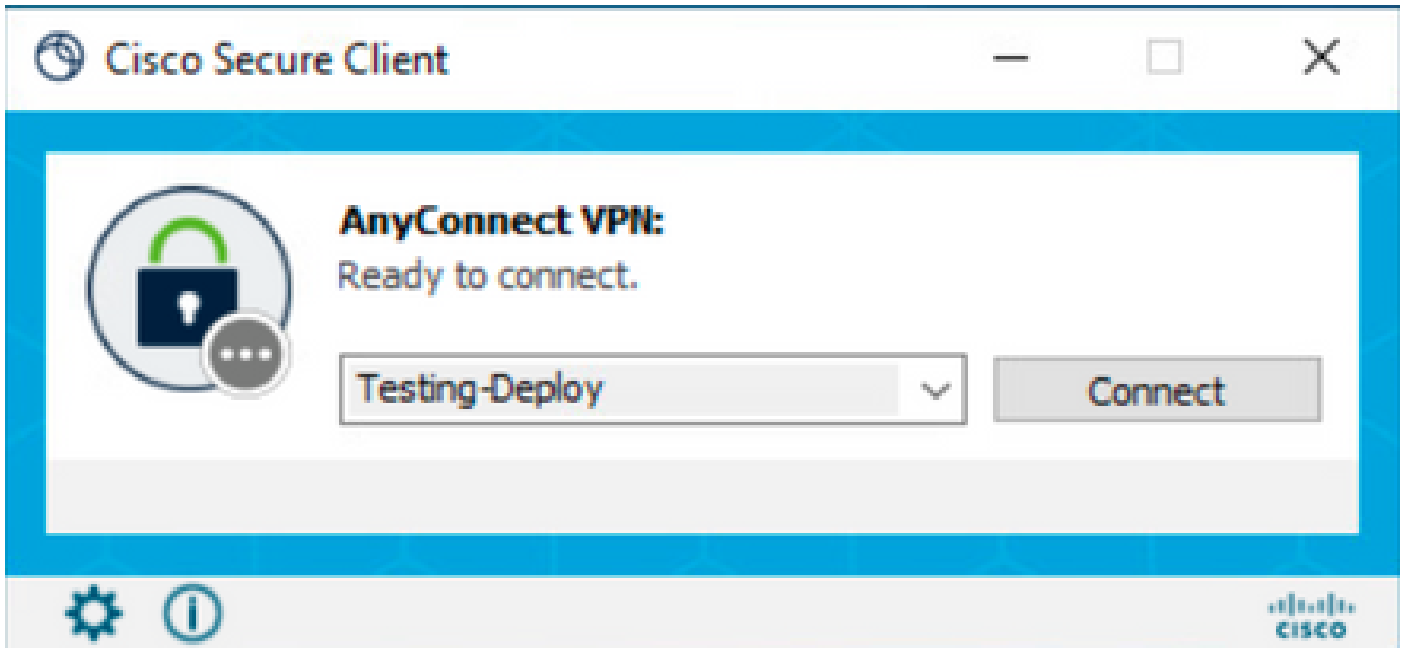
Domain List:

Cancel Save

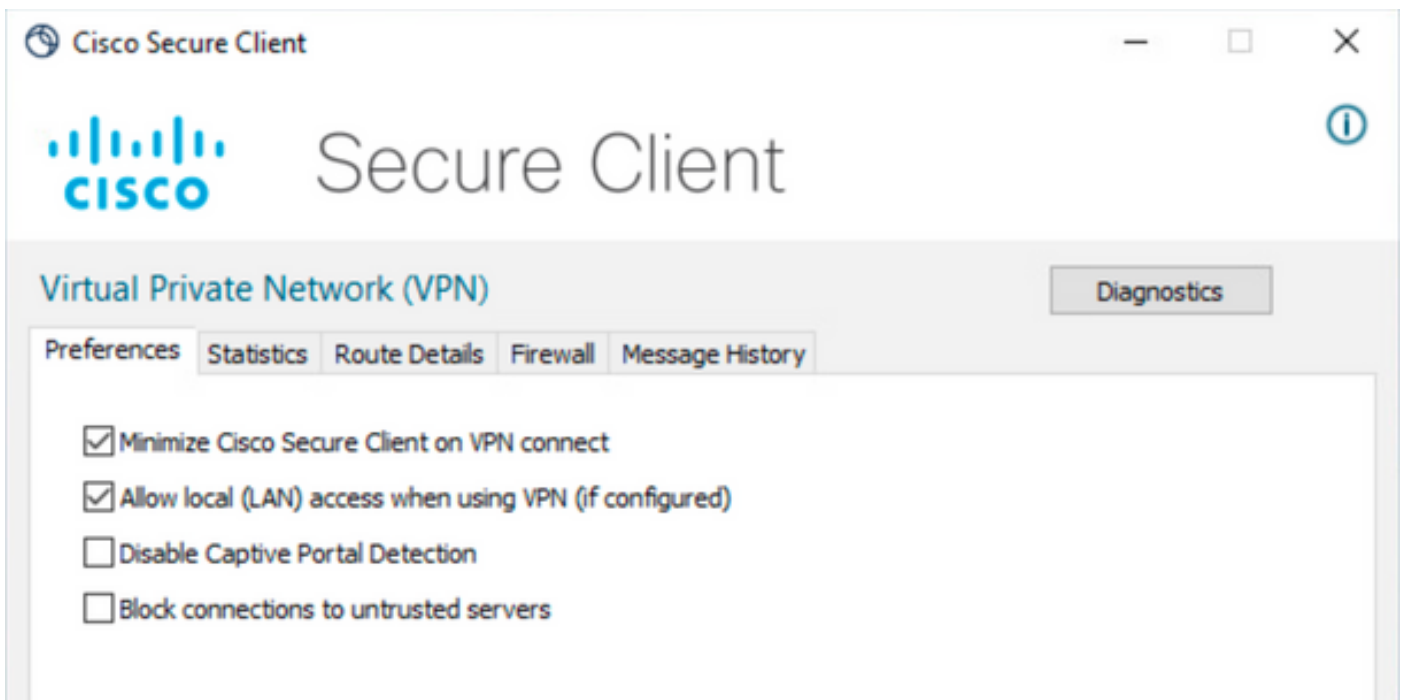
Haga clic en el botón Save e implemente los cambios.

Configuración de Secure Client

De forma predeterminada, la opción Local LAN Access (Acceso a LAN local) se establece en User Controllable. Para habilitar la opción, haga clic en el icono Engranaje en la GUI de Secure Client.



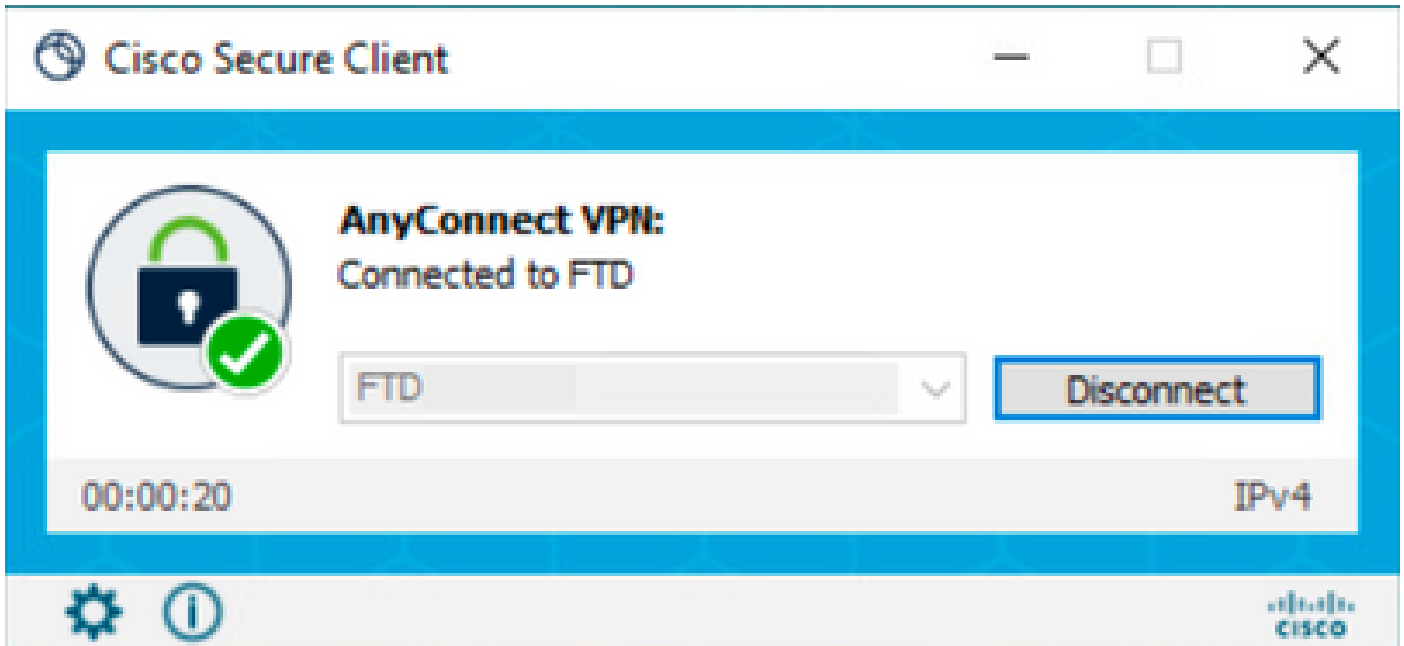
Navegue hasta Preferencias y asegúrese de que la opción Permitir acceso local (LAN) al utilizar VPN (si está configurada) esté habilitada.



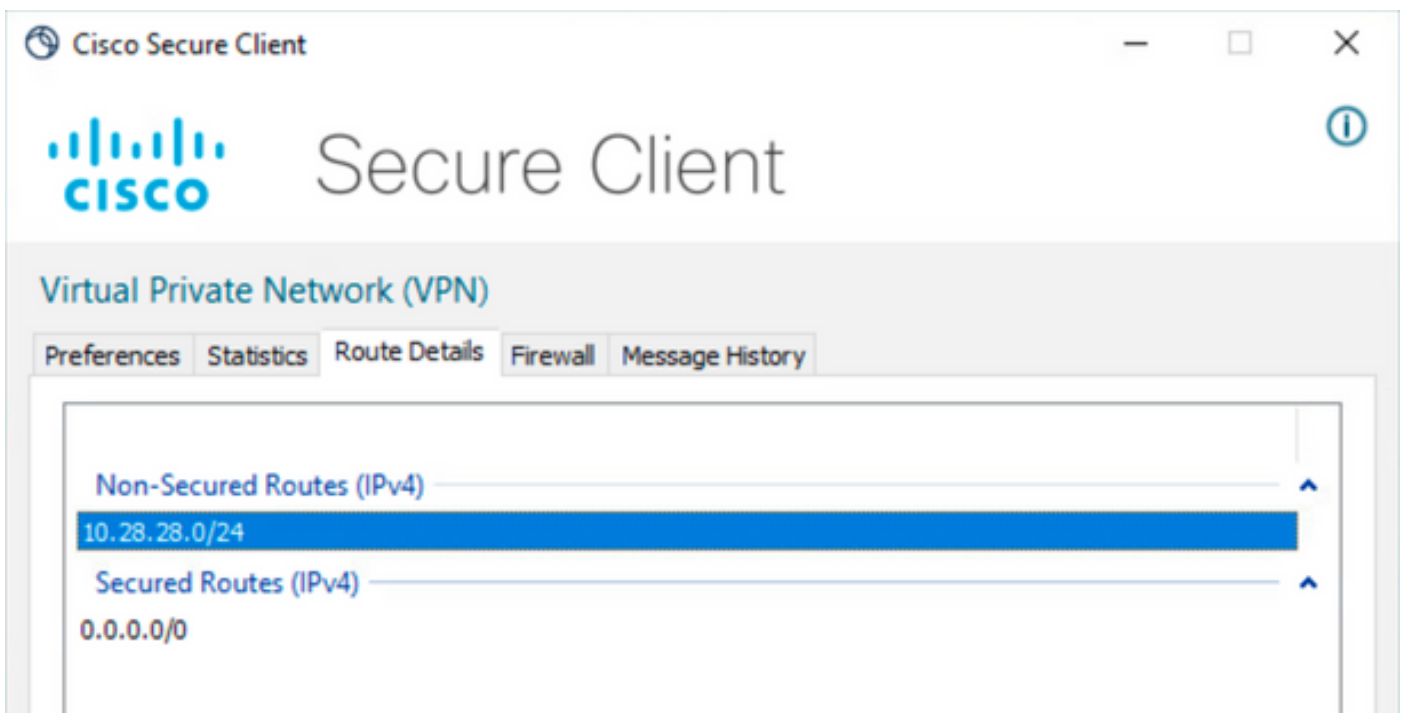
Verificación

Cliente seguro

Conéctese a la cabecera mediante Secure Client.



Haga clic en el icono del engranaje y desplácese hasta Detalles de ruta. Aquí puede ver que la LAN local se detecta automáticamente y se excluye del túnel.



CLI FTD

Para comprobar si la configuración se ha aplicado correctamente, puede utilizar la CLI del 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

Para verificar si se aplicó la función de acceso LAN local, puede habilitar estos debugs:

```
debug webvpn anyconnect 255
```

Este es un ejemplo de un resultado de debug exitoso:

```
<#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+/OI1/01LjBic/Nu/K2+N6E5GAiA5CLAF6Bt0tcxhj'
Processing CSTP header line: 'X-AnyConnect-STRAP-Verify: MEQCICzX1yDWLXQHn10hOXV+/OI1/01LjBic/Nu/K2+N6E5GAiA5CLAF6Bt0tcxhj'
Setting Anyconnect STRAP client signature(len: 96): MEQCICzX1yDWLXQHn10hOXV+/OI1/01LjBic/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-AES256-SHA256'
Processing CSTP header line: 'X-DTLS12-CipherSuite: ECDHE-RSA-AES256-GCM-SHA384:ECDSA-AES256-GCM-SHA384:ECDSA-AES256-SHA384:ECDSA-AES256-SHA256'
```

```
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) & 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(dtls_hdr) - 16(dtls_iv) = 1443
mod-mtu = 1443(mtu) & 0xfff0(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
```

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).