# Solucione problemas e colete informações básicas para a equipe de suporte do Secure Access

## Contents


Introdução

Pré-requisitos

- Requisitos
- Componentes Utilizados

Informações de Apoio

Localize a ID da Organização de Acesso Seguro

Ferramenta de Diagnóstico e Relatórios do Cisco Secure Client (DART)

Habilitar logs de depuração para os módulos ZTNA e SWG

- Habilitar logs de depuração para ZTNA
- Habilitar logs de depuração para SWG
- Habilitar logs de depuração para DUO

Coletar registros KDF para módulos ZTNA e SWG, DNS (Windows)

- Pré-requisitos

Capturas de Arquivo HTTP (HAR)

Capturas de pacotes

Saída de depuração de política

Comandos Comuns para Troubleshooting de Túnel de Site a Site

Comandos Comuns para Identificação e Solução de Problemas do Conector de Recursos

Carregar resultados para solicitação de serviço de suporte da Cisco

Informações Relacionadas


## Introdução

Este documento descreve as informações básicas que precisam ser coletadas ao trabalhar com a equipe de suporte do Cisco Secure Access

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso seguro da Cisco
- Cisco Secure Client

- Capturas de pacotes através do Wireshark e tcpdump

### Componentes Utilizados

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Informações de Apoio

Ao trabalhar com o Cisco Secure Access, você pode ter problemas para os quais precisa entrar em contato com a equipe de suporte da Cisco, ou gostaria de realizar uma investigação básica para o problema e tentar passar pelos logs e identificar o problema. Este artigo explica como coletar os logs básicos de solução de problemas relacionados ao Secure Access. observe que nem todas as etapas se aplicam a todos os cenários.

## Localize a ID da Organização de Acesso Seguro

Para que o Engenheiro da Cisco localize sua conta, forneça a ID da sua organização, que pode ser encontrada no URL depois que você estiver conectado ao Painel de Acesso Seguro.

Etapas para localizar a ID da Organização:

1. Faça login em sse.cisco.com
2. Se você tiver várias organizações, mude para a direita.
3. A ID da organização pode ser encontrada no URL neste padrão:
https://dashboard.sse.cisco.com/org/{7_digit_org_id}/overview

## Ferramenta de Diagnóstico e Relatórios do Cisco Secure Client (DART)

O Cisco Secure Client Diagnostic and Reporting Tool (DART) é uma ferramenta instalada com o pacote Secure Client, que ajuda a coletar informações importantes sobre o endpoint do usuário.

Exemplo de informações coletadas pelo pacote DART:

- Logs da ZTNA
- Logs de clientes seguros e informações de perfil
- Informações do sistema
- Outros registros de complementos ou plugins do Secure Client instalados no

Instruções para coletar DART:

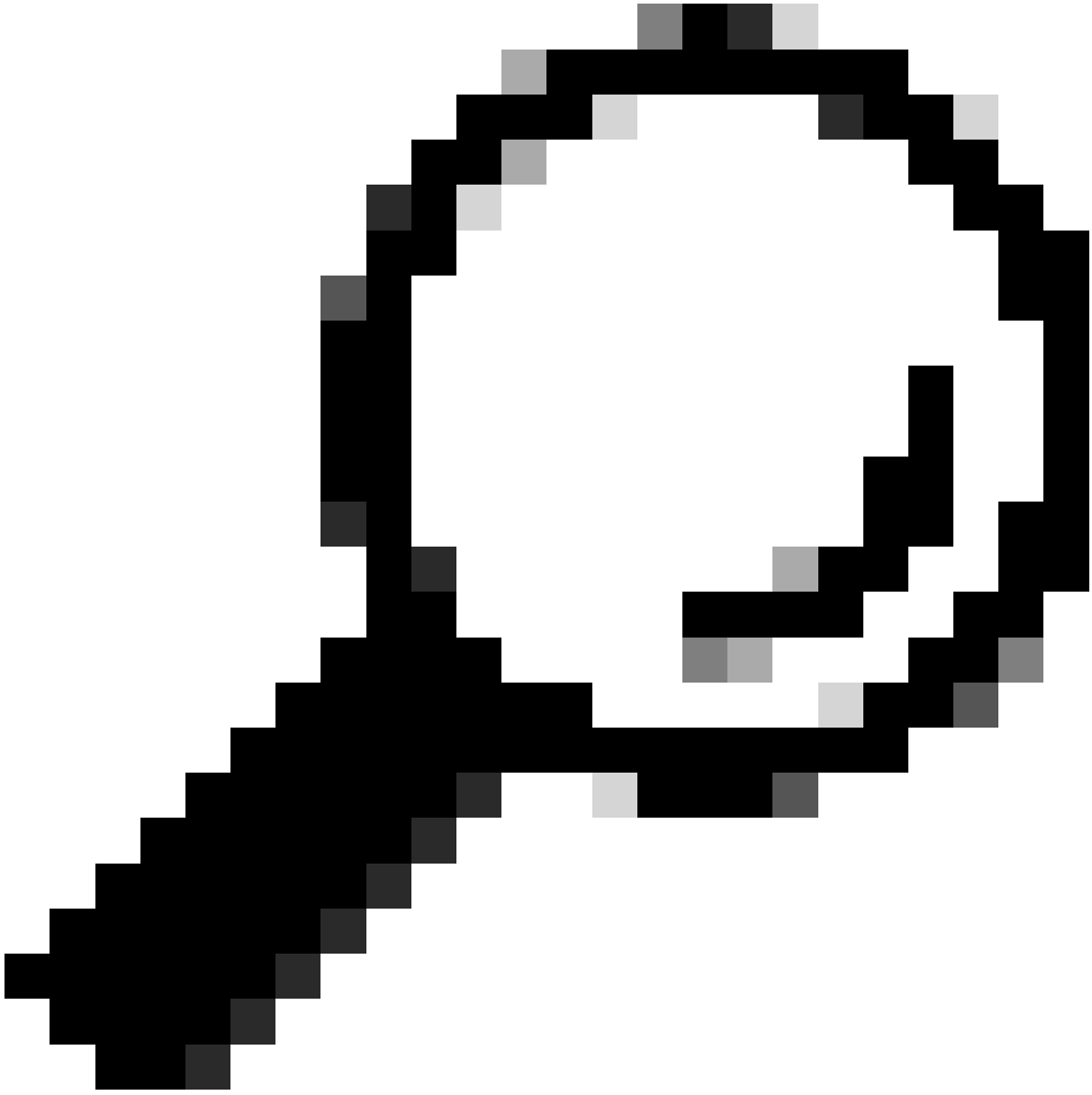
Etapa 1. Inicie o DART.

1. Para um computador Windows, inicie o Cisco Secure Client.
2. Para um computador Linux, escolha **Applications** > **Internet** > **Cisco DART**ou /opt/cisco/anyconnect/dart/dartui.
3. Para um computador Mac, escolhaApplications > Cisco > Cisco DART.

Etapa 2. Clique na guia Statistics (Estatísticas) e em Details (Detalhes).

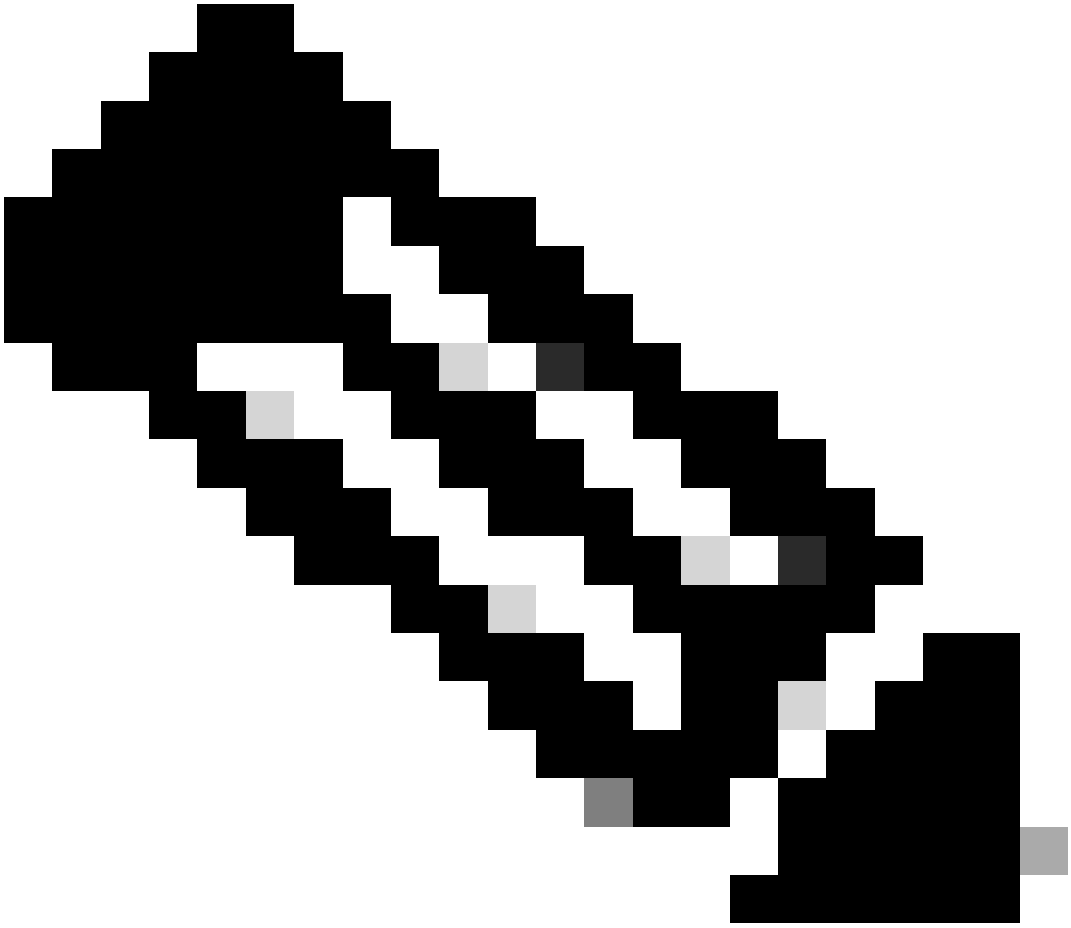
Etapa 3. Escolha Default ou Custom bundle creation.

---



Tip: O nome padrão do pacote é DARTBundle.zip, e ele é salvo no desktop local.

---



Note: Se você escolher Padrão, o DART começará a criar o pacote. Se você escolher Personalizar, continue os prompts do assistente para especificar logs, arquivos de preferência, informações de diagnóstico e outras personalizações.

## Habilitar logs de depuração para os módulos ZTNA e SWG

Em alguns dos cenários, a equipe de suporte exigiria a ativação de logs de nível de rastreamento ou depuração para identificar problemas mais complexos.

conclua as etapas fornecidas nesta seção para ativar depurações para cada um dos módulos.

### Habilitar logs de depuração para ZTNA

Etapa 1. Crie um arquivo json com o nome logconfig.json

Etapa 2. Insira este texto dentro do arquivo

```
{ "global": "DBG_TRACE" }
```

Etapa 3. Coloque o arquivo no diretório correto com base no sistema operacional

- Windows: C:\ProgramData\Cisco\Cisco Secure Client\ZTA
- MacOS: /opt/cisco/secureclient/zta

Etapa 4. Reinicie o módulo ZTNA ou o Cisco Secure Client para que os registros entrem em vigor.

### Habilitar logs de depuração para SWG

Etapa 1. Crie um arquivo json com o nome SWGConfigOverride.json

Etapa 2. Insira este texto dentro do arquivo

```
{"logLevel": "1"}□
```

Etapa 3. Coloque o arquivo no diretório correto com base no sistema operacional

- Windows: C:\ProgramData\Cisco\Cisco Seguro Client\Umbrella\SWG\
- MacOS: /opt/cisco/secureclient/umbrella/swg

Etapa 4. Reinicie o módulo SWG ou o Cisco Secure Client para que os registros tenham efeito.

### Habilitar logs de depuração para DUO

Habilitar logs KDF do DUO (Solução de Problemas de Postura, Problemas de Registro)

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Duo\Duo Device Health” /v verbose_logging_enabled /d 1 /f
```

Desabilitar logs KDF do DUO

```
reg add “HKEY_LOCAL_MACHINE\SOFTWARE\Duo\Duo Device Health” /v verbose_logging_enabled /d 0 /f
```

## Coletar registros KDF para módulos ZTNA e SWG, DNS (Windows)

Em alguns dos cenários, a equipe de suporte precisaria coletar logs do kdf para identificar problemas mais complexos.

conclua as etapas fornecidas nesta seção para configurar e coletar os logs do kdf.

### Pré-requisitos

A instalação do DebugView é necessária para coletar os logs corretamente. que pode ser instalado usando esta fonte: https://learn.microsoft.com/en-us/sysinternals/downloads/debugview

Habilitar Chave do Registro DNS

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\acsock" /v DebugFlags /d 0x20801FF /t reg
```

Habilitar chave de registro SWG

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\acsock" /v DebugFlags /d 0x70C01FF /t reg
```

Habilitar Chave do Registro ZTNA

```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -sdf 0x40018EF52
```

Desabilitar Todos os Sinalizadores

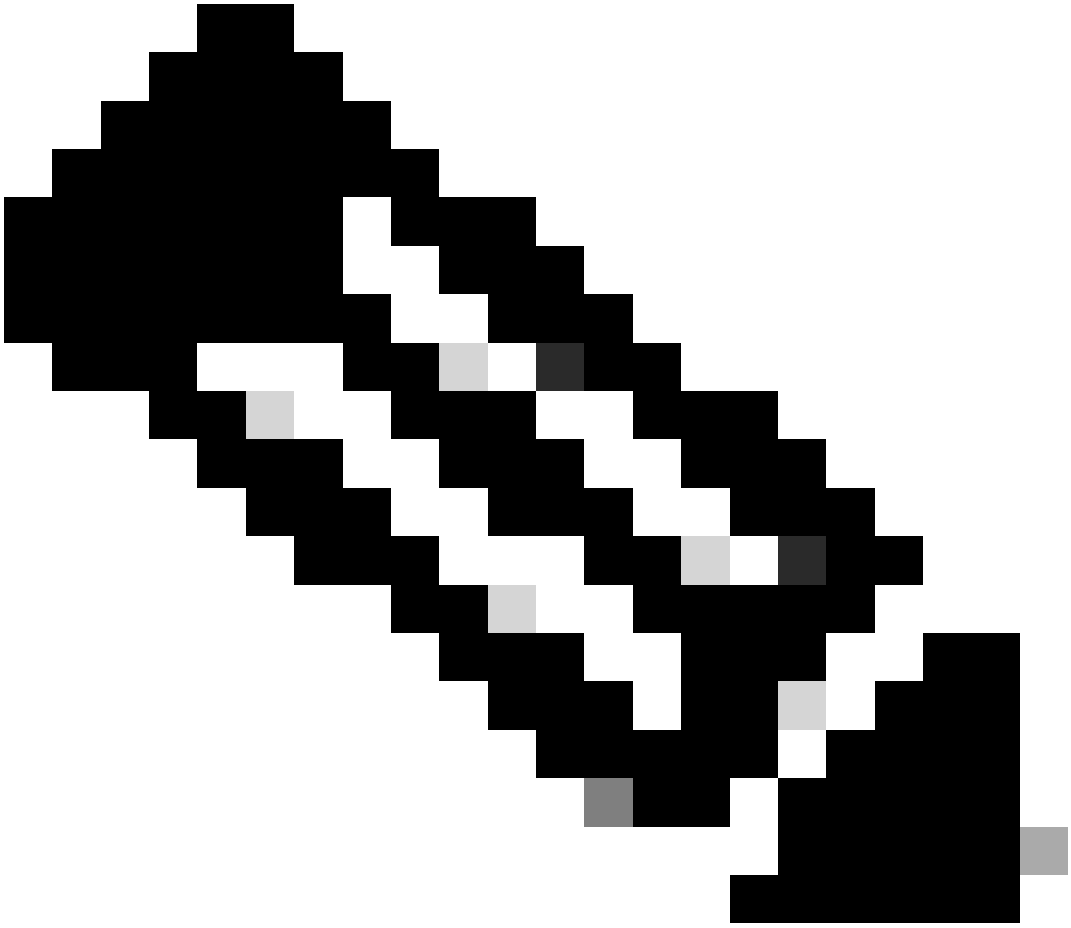
```
"%ProgramFiles(x86)%\Cisco\Cisco Secure Client\acsocktool.exe" -cdf
```

## Capturas de Arquivo HTTP (HAR)

HAR pode ser coletado de diferentes navegadores. ele fornece várias informações que incluem:

1. Versão descriptografada das solicitações HTTPS.
2. Informações internas sobre mensagens de erro, detalhes da solicitação e cabeçalhos.
3. Informações relativas ao calendário e aos atrasos
4. Outras informações diversas sobre solicitações baseadas no browser.

Para coletar capturas HAR, use as etapas descritas nesta fonte: https://toolbox.googleapps.com/apps/har_analyzer/



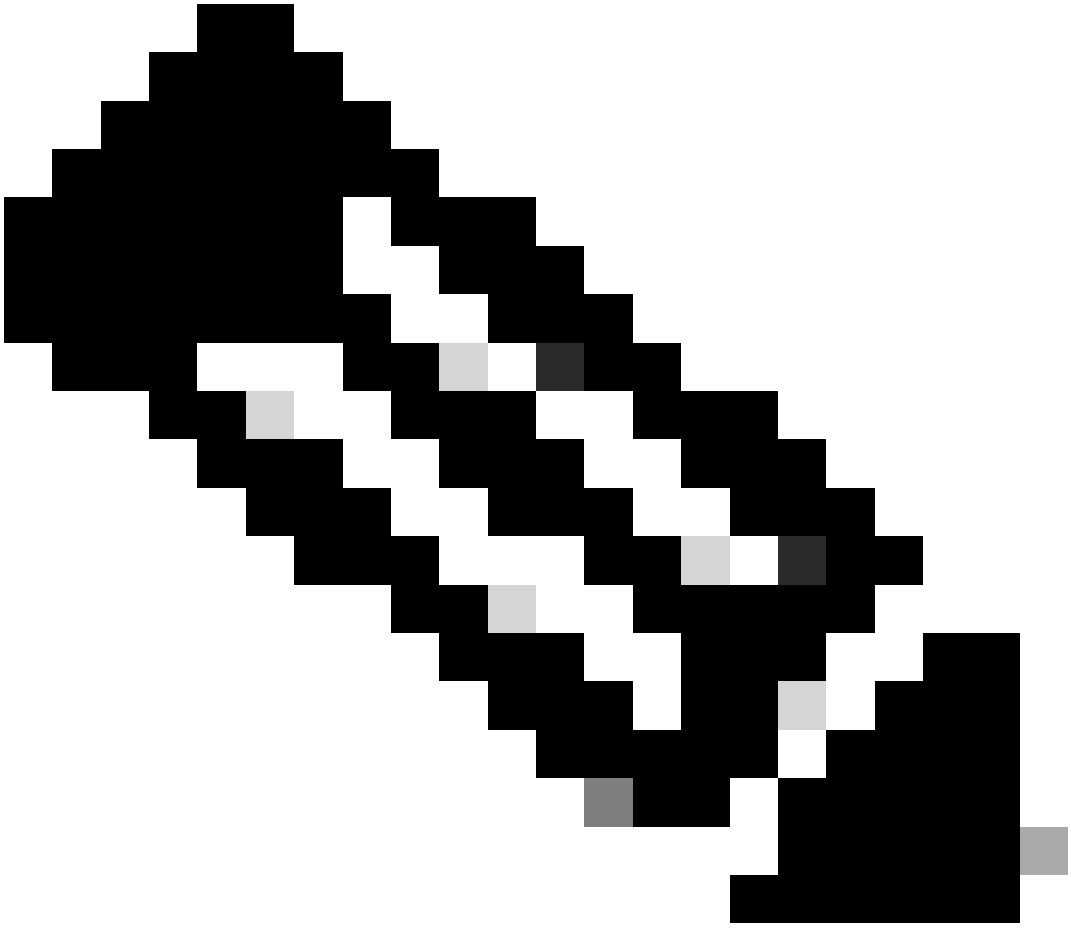
Note: Você precisa atualizar sua sessão do navegador para coletar os dados corretos

## Capturas de pacotes

As capturas de pacotes são úteis em um cenário em que um problema de desempenho ou uma perda de pacotes é detectada, ou uma interrupção total para a rede. As ferramentas mais comuns para coletar capturas sãowiresharke **tcpdump**. Ou um recurso interno para coletar formato de arquivos pcap dentro do próprio dispositivo, como um Cisco Firewall ou roteador.

Para coletar capturas de pacotes úteis em um endpoint, certifique-se de incluir:

1. Interface de loopback para capturar o tráfego enviado através de complementos do Secure Client.
2. Todas as outras interfaces envolvidas no caminho do pacote.
3. Aplique filtros mínimos ou nenhum filtro para garantir que todos os dados sejam coletados.



Note: Quando as capturas forem coletadas em um dispositivo de rede, certifique-se de filtrar a origem e o destino do tráfego e limitar as capturas somente a portas e serviços relacionados, para evitar qualquer desempenho causado por essa atividade.

## Saída de depuração de política

A saída de depuração de política é uma saída de diagnóstico enviada através do navegador do usuário ao ser protegida pelo Secure Access. que inclui informações críticas sobre a implantação.

1. ID da Organização
2. Tipo de implantação
3. Proxy conectado
4. Endereço IP público e privado
5. Outras informações relacionadas com a origem do tráfego.

Para executar os resultados do teste de política, faça login neste link a partir de um endpoint protegido: https://policy.test.sse.cisco.com/

Verifique se você confia no Certificado Raiz de Acesso Seguro se uma mensagem de erro de certificado for apresentada em seu navegador.

Para fazer download do certificado raiz de acesso seguro:

Navegue até Acesso seguro Dashboard > Secure > Settings > Certificate > (Internet Destinations tab)

# Comandos Comuns para Troubleshooting de Túnel de Site a Site

<#root>

```
# Tunnel Establishment


asa>show crypto ikev1 sa
asa>show crypto ikev2 sa
asa>show crypto ipsec sa
asa>show crypto session


#BGP Troubleshooting


asa>show running-config router bgp
asa>show bgp summary
asa>show ip bgp neighbors


#Routes Advertisements


asa>show bgp ipv4 unicast neighbors <sse-dc-ip> advertised-routes
asa>show bgp ipv4 unicast neighbors <sse-dc-ip> received-routes
asa>show bgp ipv4 unicast neighbors <sse-dc-ip> routes


#Debug BGP events


asa>debug ip bgp
asa>debug ip bgp events
asa>debug ip bgp updates
asa>debug ip routing


#Disable Debugs


asa>undebug all
```

# Comandos Comuns para Identificação e Solução de Problemas do Conector de Recursos

A lista fornecida fornece uma visão abrangente do conector de recursos e detalhes importantes

de solução de problemas para a equipe de suporte de acesso seguro

<#root>

```
#DNS and connectivity tests on the local IP address, gateway, Secure Access APIs

rc-cli> diagnostic

#Software version, VPN tunnel state, system health, sysctl settings, routes and iptables

rc-cli> techsupport

#Packet captures

rc-cli> tcpdump <host>
```

## Carregar resultados para solicitação de serviço de suporte da Cisco

Você pode carregar arquivos para o caso de suporte por meio destas etapas:

Etapa 1. Faça login no SCM.

Etapa 2. Para visualizar e editar o caso, clique no número do caso ou no título do caso na lista. A página Case Summary (Resumo do caso) é aberta.

Etapa 3. Clique em Add Files para escolher um arquivo e carregá-lo como um anexo ao caso. O sistema exibe a ferramenta Carregador de arquivo SCM.

Etapa 4. Na caixa de diálogo Escolher arquivos para upload, arraste os arquivos que você deseja carregar ou clique em inside para procurar arquivos para upload na máquina local.

Etapa 5. Adicione uma descrição e especifique uma categoria para todos os arquivos ou individualmente.

## Informações Relacionadas

- Suporte técnico e downloads da Cisco
- Documentação e Guia do Usuário do Secure Access
- Download do software Cisco Secure Client

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.