

Solucionar problemas do Secure Access Roaming Module "Cloud Service Unavailable" ou "Unprotected" Status

Contents

[Introdução](#)

[Problema](#)

[O status de proteção DNS está desprotegido](#)

[O status da proteção da Web é Serviço em nuvem indisponível](#)

[Solução](#)

[Informações Relacionadas](#)

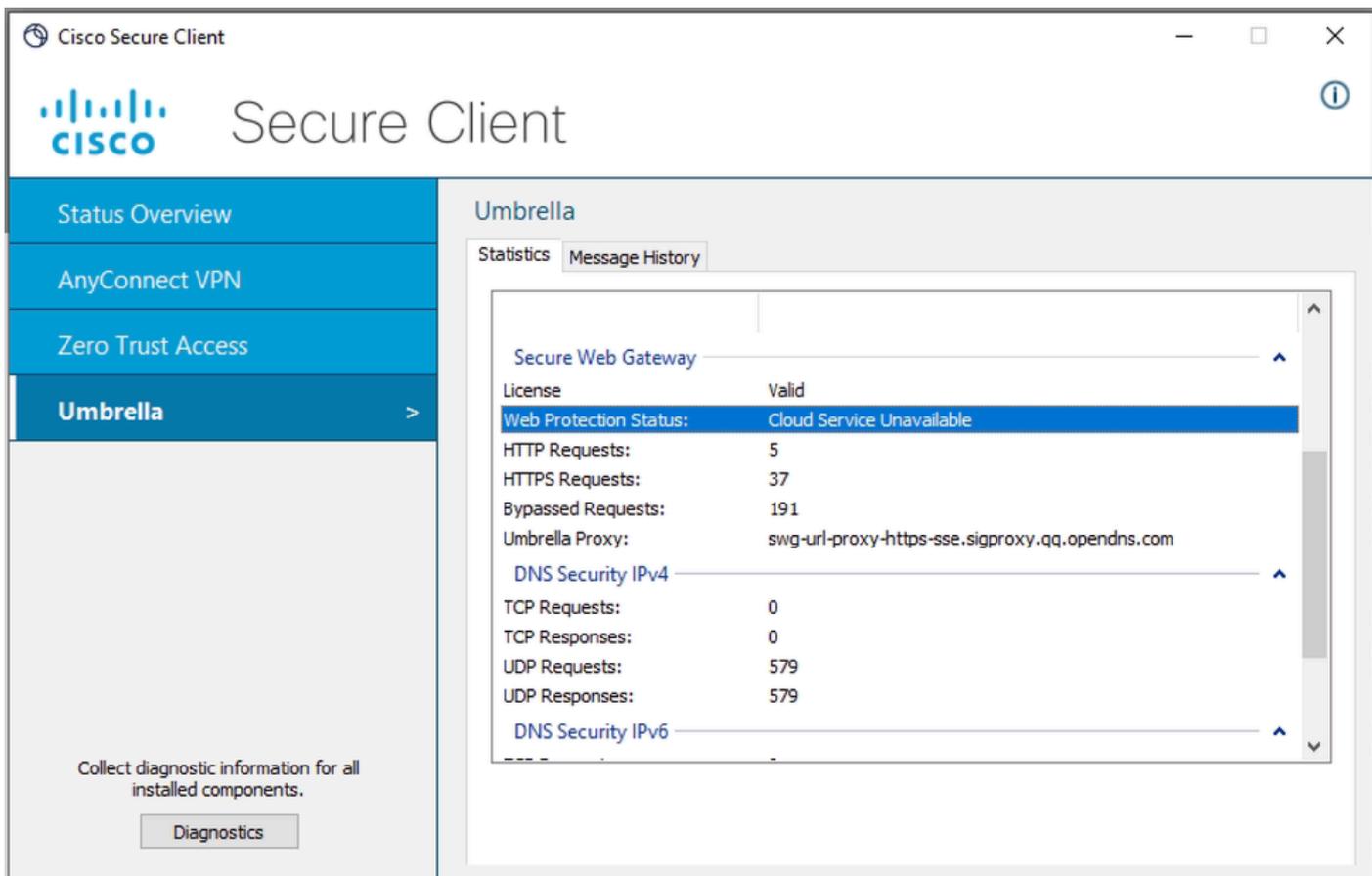
Introdução

Este documento descreve uma forma de investigar a causa raiz do status "Serviço em nuvem indisponível" ou "Desprotegido" no Módulo de roaming do cliente seguro.

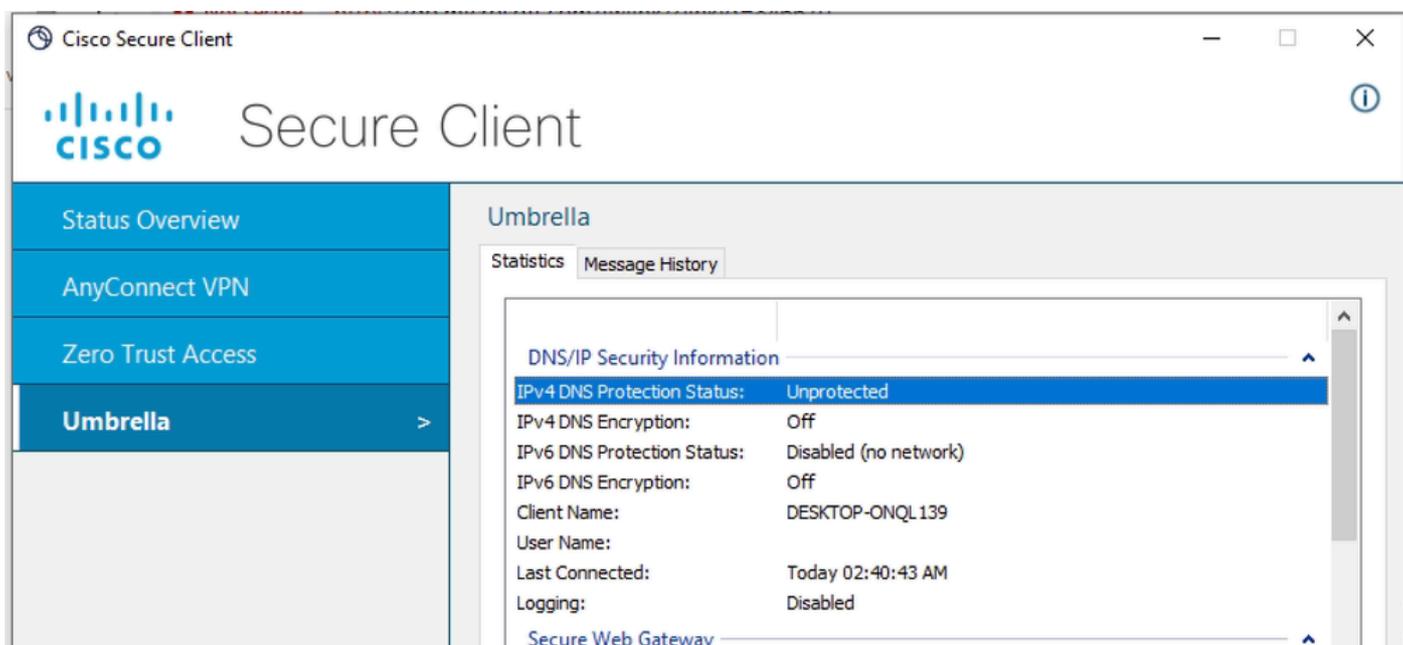
Problema

Quando um usuário inicia o módulo de roaming do cliente seguro e espera usar a proteção DNS e/ou Web, os estados errados podem ser vistos na interface de usuário do cliente seguro:

Serviço em nuvem indisponível para status de proteção da Web



Desprotegido para Status de Proteção DNS



A razão por trás desses erros é que o módulo de roaming não pode entrar em contato com seus serviços de nuvem devido a problemas de conectividade de rede.

Se esse problema não foi visto no PC cliente afetado no passado, isso significa que muito provavelmente a rede à qual o PC está conectado é restrita e não atende aos requisitos descritos na [Documentação do SSE](#)

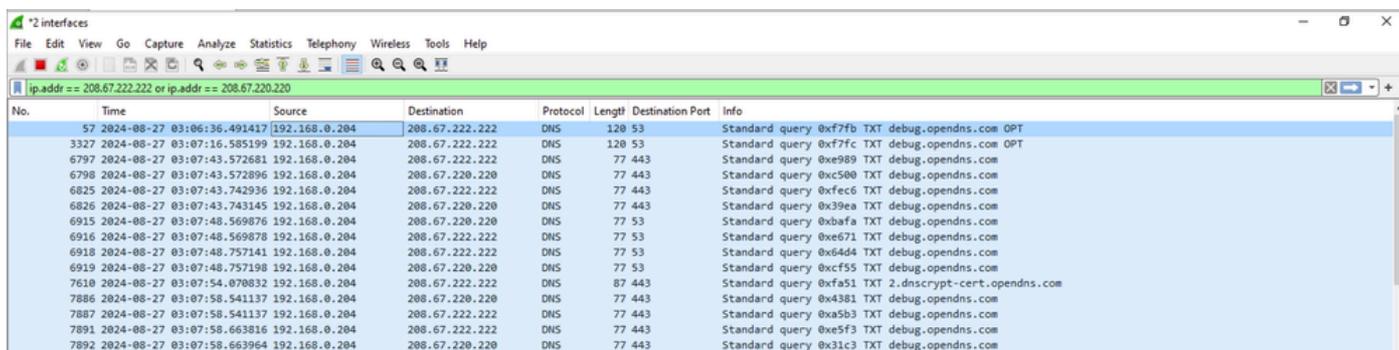
O status de proteção DNS está desprotegido

Quando você vir o estado DNS desprotegido, provavelmente o módulo de roaming não terá conectividade upstream com servidores OpenDNS (208.67.222.222 e 208.67.220.220). Você veria o arquivo de log no arquivo cscumbrellaplugin.txt, que faz parte do pacote DART.

```
2024-08-27 03:07:43 [8880] [DEBUG] < 12> Dns Protection IPv4 State Machine: checking reachability of pr
2024-08-27 03:07:43 [8880] [DEBUG] < 12> Dns Protection IPv4 State Machine: probing for OpenDNS resolve
2024-08-27 03:07:43 [8880] [DEBUG] < 13> Dns Protection IPv6 State Machine: rejected all candidate reso
2024-08-27 03:07:48 [8880] [DEBUG] < 12> Dns Protection IPv4 State Machine: checking reachability of pr
2024-08-27 03:07:48 [8880] [DEBUG] < 12> Dns Protection IPv4 State Machine: probing for OpenDNS resolve
2024-08-27 03:07:53 [8880] [DEBUG] < 12> Dns Protection IPv4 State Machine: rejected all candidate reso
```

Para verificar e confirmar novamente os problemas de conectividade, você pode coletar a captura do Wireshark na interface física de saída do PC (WiFi ou Ethernet) e usar o filtro de exibição para procurar apenas o tráfego destinado aos resolvedores do OpenDNS:

```
ip.addr == 208.67.222.222 or ip.addr == 208.67.220.220
```



No.	Time	Source	Destination	Protocol	Length	Destination Port	Info
57	2024-08-27 03:06:36.491417	192.168.0.204	208.67.222.222	DNS	120	53	Standard query 0xf7fb TXT debug.opendns.com OPT
3327	2024-08-27 03:07:16.585199	192.168.0.204	208.67.222.222	DNS	120	53	Standard query 0xf7fc TXT debug.opendns.com OPT
6797	2024-08-27 03:07:43.572681	192.168.0.204	208.67.222.222	DNS	77	443	Standard query 0xe989 TXT debug.opendns.com
6798	2024-08-27 03:07:43.572896	192.168.0.204	208.67.220.220	DNS	77	443	Standard query 0xc509 TXT debug.opendns.com
6825	2024-08-27 03:07:43.742936	192.168.0.204	208.67.222.222	DNS	77	443	Standard query 0xfec6 TXT debug.opendns.com
6826	2024-08-27 03:07:43.743145	192.168.0.204	208.67.220.220	DNS	77	443	Standard query 0x39ea TXT debug.opendns.com
6915	2024-08-27 03:07:48.569876	192.168.0.204	208.67.220.220	DNS	77	53	Standard query 0xbafa TXT debug.opendns.com
6916	2024-08-27 03:07:48.569878	192.168.0.204	208.67.222.222	DNS	77	53	Standard query 0xe671 TXT debug.opendns.com
6918	2024-08-27 03:07:48.757141	192.168.0.204	208.67.222.222	DNS	77	53	Standard query 0x64d4 TXT debug.opendns.com
6919	2024-08-27 03:07:48.757198	192.168.0.204	208.67.220.220	DNS	77	53	Standard query 0xc555 TXT debug.opendns.com
7610	2024-08-27 03:07:54.078032	192.168.0.204	208.67.222.222	DNS	87	443	Standard query 0xfa51 TXT 2.dnscrypt-cert.opendns.com
7886	2024-08-27 03:07:58.541137	192.168.0.204	208.67.220.220	DNS	77	443	Standard query 0x4381 TXT debug.opendns.com
7887	2024-08-27 03:07:58.541137	192.168.0.204	208.67.222.222	DNS	77	443	Standard query 0xa5b3 TXT debug.opendns.com
7891	2024-08-27 03:07:58.663816	192.168.0.204	208.67.222.222	DNS	77	443	Standard query 0xe5f3 TXT debug.opendns.com
7892	2024-08-27 03:07:58.663964	192.168.0.204	208.67.220.220	DNS	77	443	Standard query 0x31c3 TXT debug.opendns.com

Como você vê no snippet do Wireshark, é claro que o cliente continua retransmitindo consultas TXT DNS destinadas a 208.67.222.222 e 208.67.220.220 nas portas UDP 443 e 53, mas não recebe nenhuma resposta.

Pode haver vários motivos por trás de tal comportamento, muito provavelmente o dispositivo de firewall de perímetro está bloqueando o tráfego de DNS de saída para servidores OpenDNS ou permitindo apenas o tráfego para servidores DNS específicos.

O status da proteção da Web é Serviço em nuvem indisponível

Quando você vir o estado de proteção da Web Serviço Indisponível, provavelmente o Módulo de roaming não terá conectividade upstream com os servidores do Gateway da Web Seguro.

Se o PC não tiver conectividade IP com servidores SWG, você verá o arquivo de log no

Umbrella.txt, que faz parte do pacote DART.

Date : 08/27/2024
Time : 06:41:22
Type : Warning
Source : csc_swgagent

Description : WARN | Thread 27cc | TCP handshake to SWG Proxy URL was not successful. Since fail open p

Para investigar mais, colete a captura de pacotes para provar que o PC não tem conectividade com o servidor SWG.

Emita o comando no terminal para obter o endereço IP do SWG:

```
<#root>
```

```
C:\Users\admin>
```

```
nslookup swg-url-proxy-https-sse.sigproxy.qq.opendns.com
```

```
Server: ad.lab.local  
Address: 192.168.0.65
```

```
Non-authoritative answer:
```

```
Name: k8s-sigproxy-sigproxy-c8f482b42a-ddf1929ae349b3e5.elb.eu-west-2.amazonaws.com  
Address:
```

```
18.135.112.200
```

```
Aliases: swg-url-proxy-https-sse.sigproxy.qq.opendns.com  
swg-proxy_eu-west-2_1_1n.sigproxy.aws.umbrella.com
```

Para verificar e confirmar novamente os problemas de conectividade, você pode coletar a captura do Wireshark na interface física de saída do PC (WiFi ou Ethernet) e usar o filtro de exibição para procurar apenas o tráfego destinado ao servidor SWG (use o endereço IP obtido na etapa anterior)

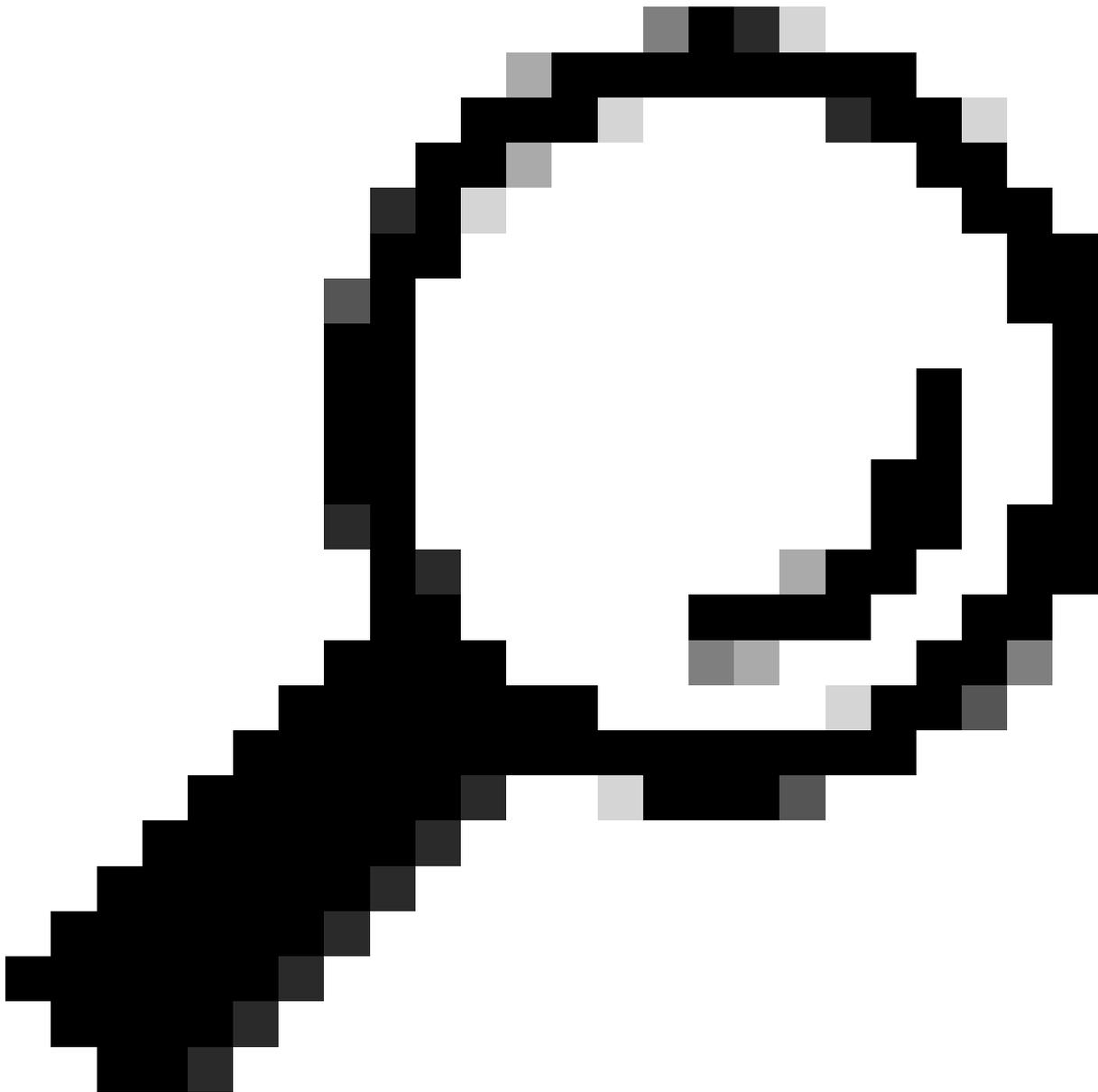
```
ip.addr == 18.135.112.200
```

No.	Time	Source	Destination	Protocol	Length	Destination Port	Info
7071	2024-08-27 06:41:19.812444	192.168.0.204	18.135.112.200	TCP	66		[TCP Port numbers reused] 56287 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7072	2024-08-27 06:41:19.812972	18.135.112.200	192.168.0.204	TCP	60		443 → 56287 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7128	2024-08-27 06:41:20.091970	192.168.0.204	18.135.112.200	TCP	66		56288 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7129	2024-08-27 06:41:20.092096	192.168.0.204	18.135.112.200	TCP	66		56289 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7130	2024-08-27 06:41:20.092255	18.135.112.200	192.168.0.204	TCP	60		443 → 56288 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7131	2024-08-27 06:41:20.092255	18.135.112.200	192.168.0.204	TCP	60		443 → 56289 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7205	2024-08-27 06:41:20.314423	192.168.0.204	18.135.112.200	TCP	66		[TCP Port numbers reused] 56287 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7206	2024-08-27 06:41:20.314819	18.135.112.200	192.168.0.204	TCP	60		443 → 56287 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7289	2024-08-27 06:41:20.603627	192.168.0.204	18.135.112.200	TCP	66		[TCP Port numbers reused] 56288 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7290	2024-08-27 06:41:20.603545	192.168.0.204	18.135.112.200	TCP	66		[TCP Port numbers reused] 56289 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7291	2024-08-27 06:41:20.604033	18.135.112.200	192.168.0.204	TCP	60		443 → 56288 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7292	2024-08-27 06:41:20.604033	18.135.112.200	192.168.0.204	TCP	60		443 → 56289 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
7434	2024-08-27 06:41:21.110571	192.168.0.204	18.135.112.200	TCP	66		[TCP Port numbers reused] 56288 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
7435	2024-08-27 06:41:21.110582	192.168.0.204	18.135.112.200	TCP	66		[TCP Port numbers reused] 56289 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM

Como você vê no snippet do Wireshark, é claro que o cliente continua retransmitindo pacotes TCP SYN destinados a 18.135.112.200, mas recebe TCP RST como resposta.

Neste cenário de laboratório específico, o firewall de perímetro estava bloqueando o tráfego para o endereço IP do SWG.

No cenário real, você pode ver apenas retransmissões TCP SYN, não TCP RST.



Dica: se o cliente não puder acessar os servidores SWG, ele, por padrão, entrará no estado fail open, onde o tráfego da Web está saindo através do Direct Internet Access (WiFi ou Ethernet). A proteção da Web não é aplicada no modo de falha/abertura.

Solução

Para identificar rapidamente se a rede subjacente está causando problemas, o usuário pode se conectar a qualquer outra rede aberta (hotspot, WiFi residencial) que não tenha nenhum firewall de perímetro.

Para corrigir o erro de conexão descrito, certifique-se de que o PC tenha conectividade upstream irrestrita, conforme descrito na [Documentação do SSE](#).

Problemas de Status de Proteção DNS:

- 208.67.222.222 porta TCP/UDP 53
- 208.67.220.220 Porta TCP/UDP 53

Para problemas de Status de proteção da Web, certifique-se de que o tráfego para Endereços IP de entrada seja permitido no firewall de perímetro - [Documentação SSE](#)

O intervalo específico de endereços IP de entrada depende da sua localização.

Informações Relacionadas

- [Guia do usuário do Secure Access](#)
- [Como coletar o pacote DART do Cisco Secure Client](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

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.