

Risolvere i problemi relativi allo stato "Cloud Service Unavailable" o "Unprotected"

Sommario

[Introduzione](#)

[Problema](#)

[Stato protezione DNS non protetto](#)

[Lo stato della protezione Web è Servizio cloud non disponibile](#)

[Soluzione](#)

[Informazioni correlate](#)

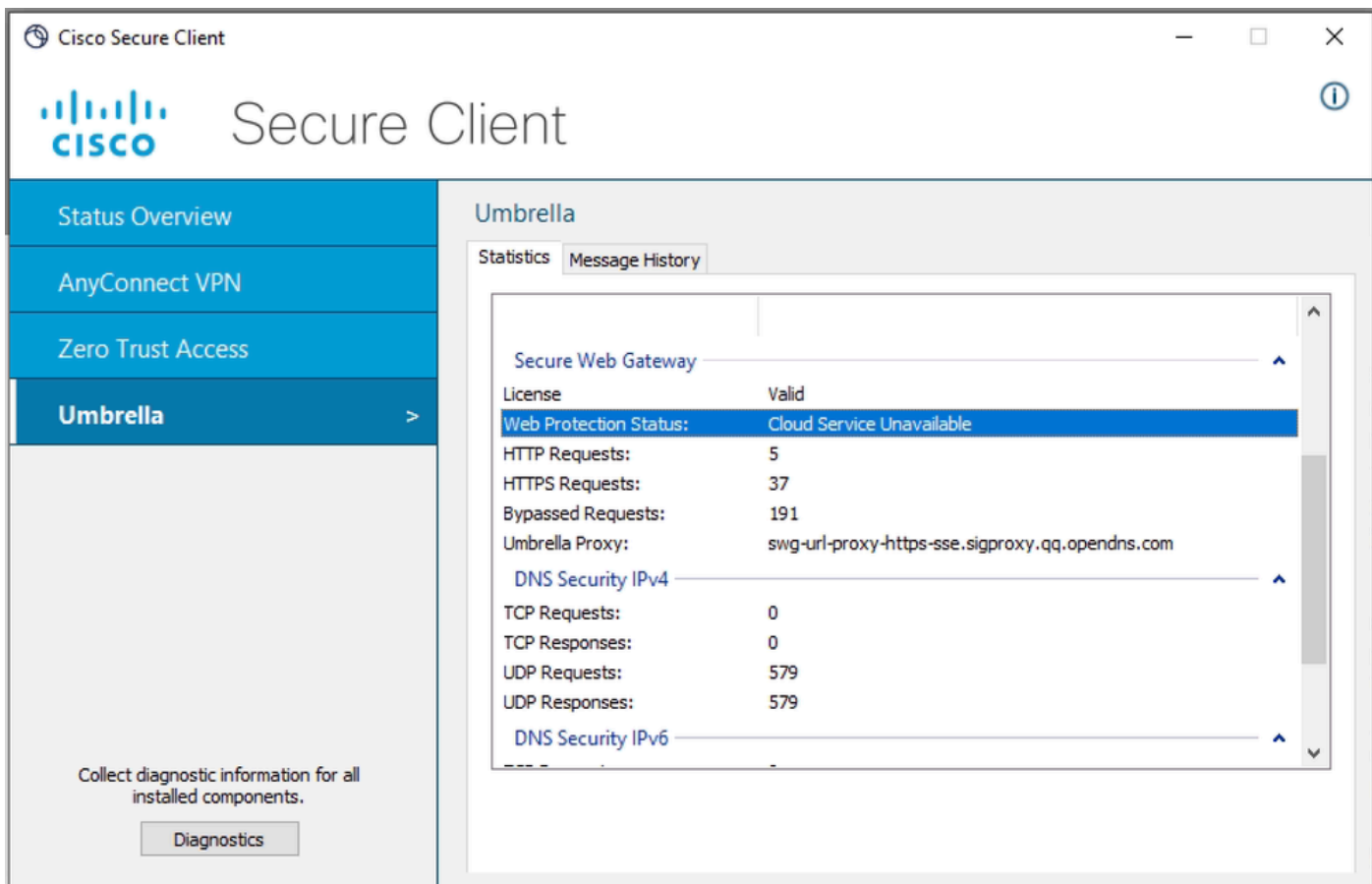
Introduzione

In questo documento viene descritto come analizzare la causa principale dello stato "Servizio cloud non disponibile" o "Non protetto" nel modulo roaming di Secure Client.

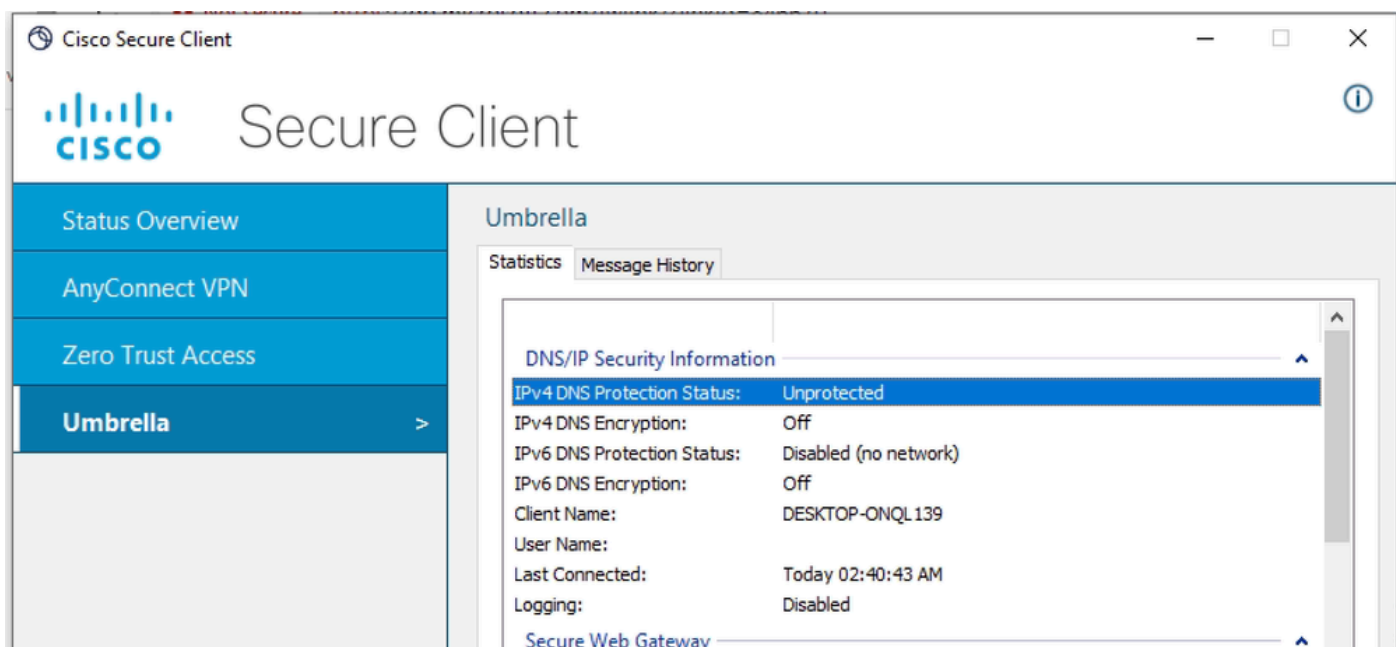
Problema

Quando un utente avvia il modulo Roaming di Secure Client e prevede di utilizzare la protezione DNS e/o Web, nell'interfaccia utente Secure Client possono essere visualizzati stati errati:

Servizio cloud non disponibile per stato protezione Web



Non protetto per stato protezione DNS



La causa di questi errori è che il modulo Roaming non è in grado di contattare i servizi cloud a causa di problemi di connettività di rete.

Se in passato questo problema non è stato rilevato sul PC client interessato, significa che molto probabilmente la rete a cui è connesso il PC è soggetta a restrizioni e non soddisfa i requisiti indicati nella [documentazione SSE](#)

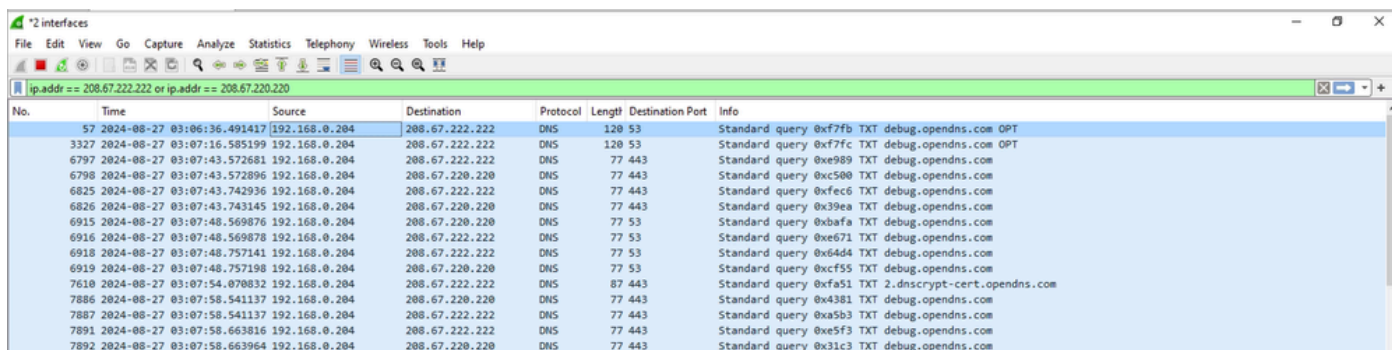
Stato protezione DNS non protetto

Quando viene visualizzato lo stato DNS non protetto, molto probabilmente il modulo Roaming non dispone di connettività upstream ai server OpenDNS (208.67.222.222 e 208.67.220.220). Viene visualizzato il file log in cscumbrellaplugin.txt, che fa parte del bundle 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
```

Per verificare e confermare i problemi di connettività, è possibile raccogliere wireshark capture sull'interfaccia fisica in uscita del PC (WiFi o Ethernet) e utilizzare il filtro di visualizzazione per cercare solo il traffico destinato ai resolver 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 0xc500 TXT debug.opendns.com
6825	2024-08-27 03:07:43.743293	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 0xcf55 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

Come si vede nello snippet di Wireshark, è chiaro che il client continua a trasmettere query TXT DNS destinate a 208.67.222.222 e 208.67.220.220 sulle porte UDP 443 e 53, ma non riceve alcuna risposta.

Questo comportamento può essere dovuto a diversi motivi: molto probabilmente il firewall perimetrale blocca il traffico DNS in uscita verso i server OpenDNS o consente il traffico solo verso determinati server DNS.

Lo stato della protezione Web è Servizio cloud non disponibile

Quando viene visualizzato lo stato di protezione Web Servizio non disponibile, è molto probabile che il modulo Roaming non disponga di connettività upstream ai server gateway Web protetti.

Se il PC non dispone di connettività IP ai server SWG, è possibile visualizzare il file di log in

Umbrella.txt, che fa parte del bundle 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

Per approfondire l'analisi, raccogliete l'acquisizione dei pacchetti per dimostrare che il PC non è connesso al server SWG.

Per ottenere l'indirizzo IP SWG, usare il comando nel terminale:

```
<#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
```

Per verificare e confermare i problemi di connettività, è possibile raccogliere wireshark capture sull'interfaccia fisica in uscita del PC (WiFi o Ethernet) e utilizzare il filtro di visualizzazione per cercare solo il traffico destinato al server SWG (utilizzare l'indirizzo IP ottenuto nel passaggio precedente)

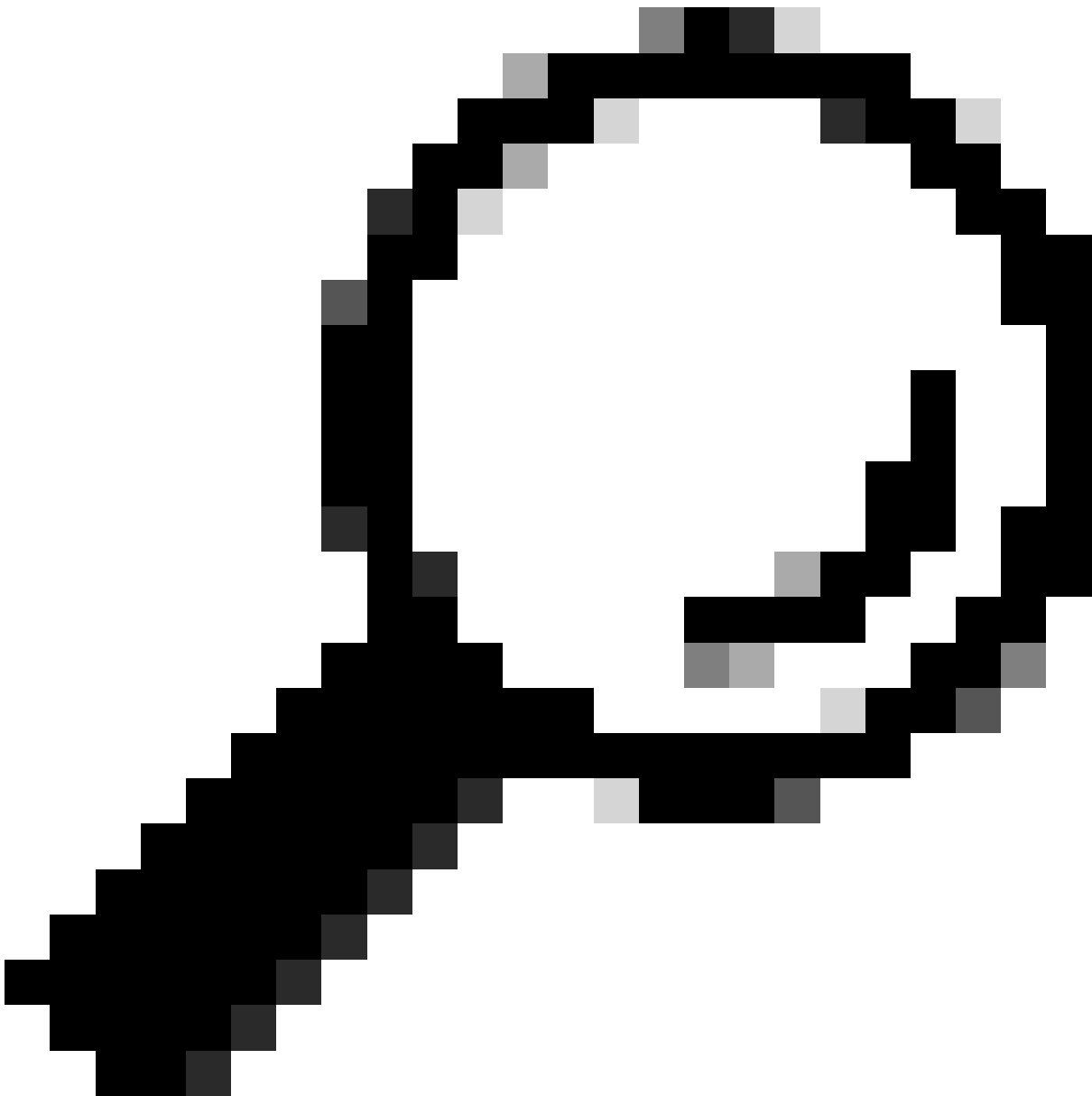
```
ip.addr == 18.135.112.200
```

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

Come si vede nello snippet di Wireshark, è chiaro che il client continua a trasmettere i pacchetti TCP SYN destinati alla versione 18.135.112.200, ma riceve come risposta il pacchetto TCP RST.

In questo scenario di laboratorio specifico, il firewall perimetrale stava bloccando il traffico verso l'indirizzo IP SWG.

Nello scenario reale, è possibile visualizzare solo le ritrasmissioni TCP SYN, non TCP RST.



Suggerimento: se il client non è in grado di raggiungere i server SWG, per impostazione predefinita entra nello stato fail-open in cui il traffico Web sta uscendo attraverso Direct Internet Access (WiFi o Ethernet). La protezione Web non viene applicata in modalità di apertura con errori.

Soluzione

Per identificare rapidamente che la rete sottostante sta causando problemi, l'utente può connettersi a qualsiasi altra rete aperta (hotspot, WiFi domestico) che non abbia alcun firewall perimetrale.

Per correggere l'errore di connessione descritto, verificare che il PC disponga di connettività upstream senza restrizioni, come indicato nella [documentazione SSE](#).

Problemi di stato della protezione DNS:

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

Per problemi di stato della protezione Web, verificare che il traffico diretto agli indirizzi IP in ingresso sia consentito nel firewall perimetrale - [Documentazione SSE](#)

L'intervallo specifico di indirizzi IP in ingresso dipende dalla località.

Informazioni correlate

- [Guida per l'utente di Secure Access](#)
- [Come raccogliere il bundle DART da Cisco Secure Client](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

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).