

# Secure Access Roaming Module "؛مدخ"؛ ةلأحلا؛ "unprotected"؛ وأ؛ "ةرفوتم

## تايوتحمل

---

[ةمدقملا](#)

[ةلكشملا](#)

[فيمحمرغ DNS ةيامح ةلأح](#)

[ةرفوتم رغ ةباحسلا ةمدخ به بيولا ةيامح ةلأح](#)

[لأحلا](#)

[ةلص تاذا تامولعم](#)

---

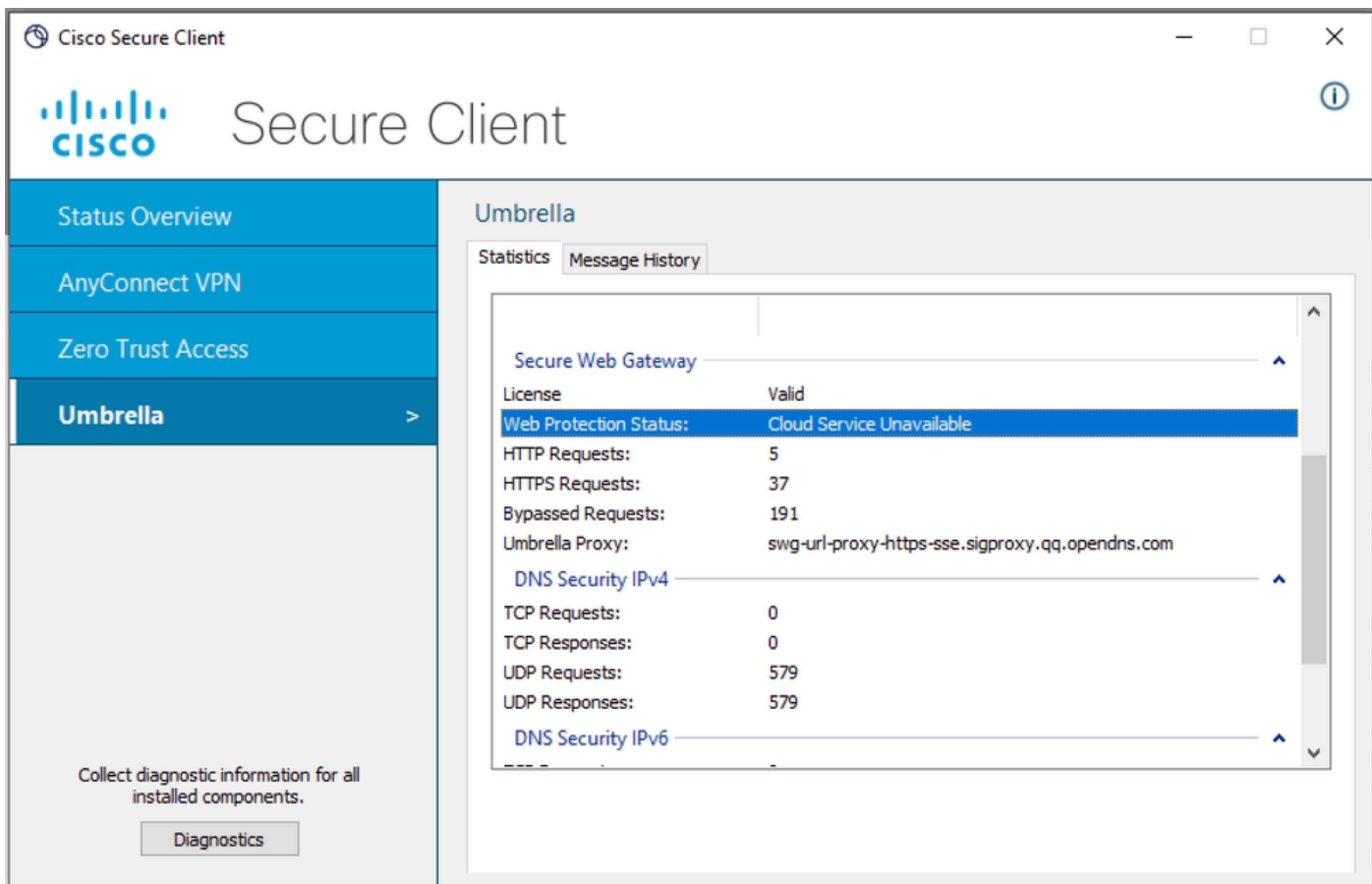
## ةمدقملا

رغ ةباحسلا ةمدخ" ةلأحلل يرذلجلا ببسلا في قيقحتلل ةقيرط دنتسملا اذه فصري  
نمآلا لي مءلاب ةصاخلا ةلأحلل ةيظمنلا ةدحوللا في "ةيحم رغ" وأ "ةرفوتم

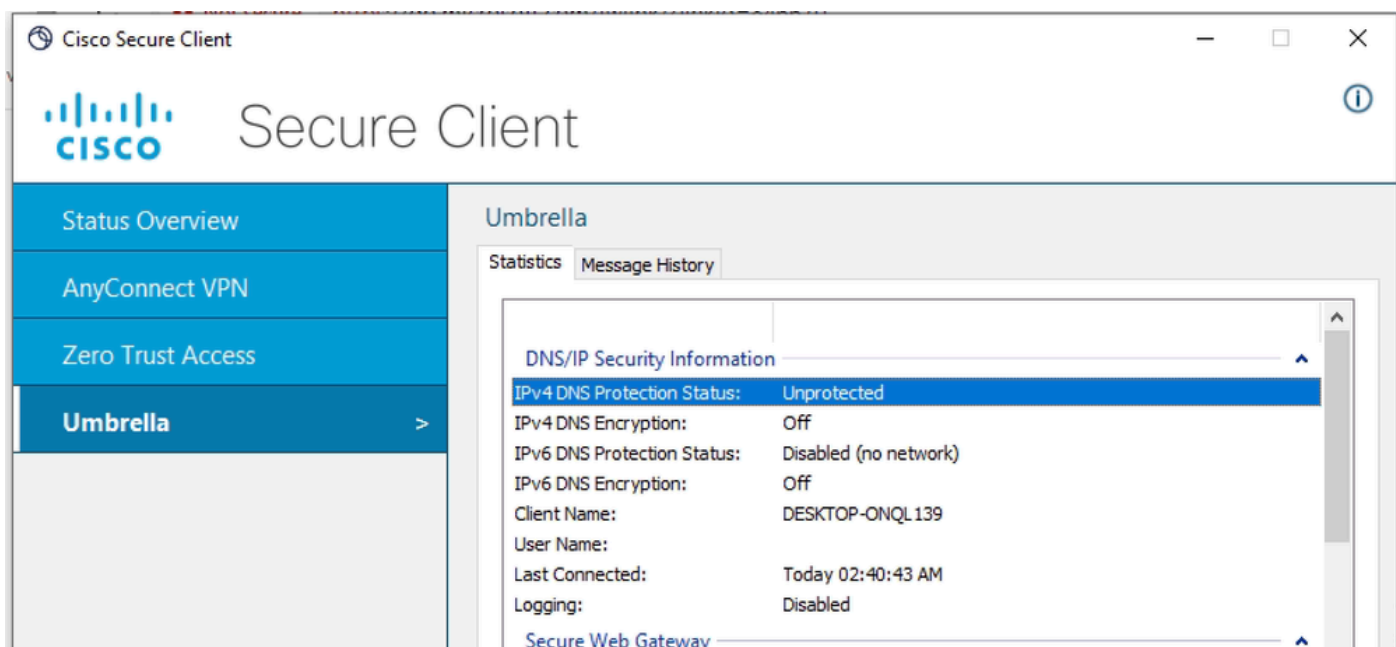
## ةلكشملا

عقوتيو Secure Client ب ةصاخلا ةلوجتملا ةيظمنلا ةدحوللا ليغشتب مدختسملا موقوي ام دنع  
لي مءلا مدختسم ةهجاو في ةئطاخلا ةلأحلل ةظالم نكمي، بيولا ةيامح وأ/و DNS مادختسا  
ةنمآلا:

بيولا ةيامح ةلأحلل ةرفوتم رغ ةباحسلا ةمدخ



DNS ةيامح ةلاجل يمحرم ريغ



ةباحسلا تامدخب لاصتالا ىلع لاوجتلا ةيطمنلا ةدجولا ةردق مدع وه ءاطخألا هذه ءارو ببسلا ةكبشلا لاصتا يف لكاشم ببسب اهب ةصاخلا

اذهف، يضا مال يف رثأتملا ليمعلا رتوي بمكلا زاهج ىلع ةلكشملا هذه ءطخال ممتي مل اذإ يف الوجج رألا ىلع ةديقم رتوي بمكلا زاهج اهب لصتي يتلا ةكبشلا نأ ينعي [SSE قئاثو](#) يف ءحضوملا تابلطتملاب

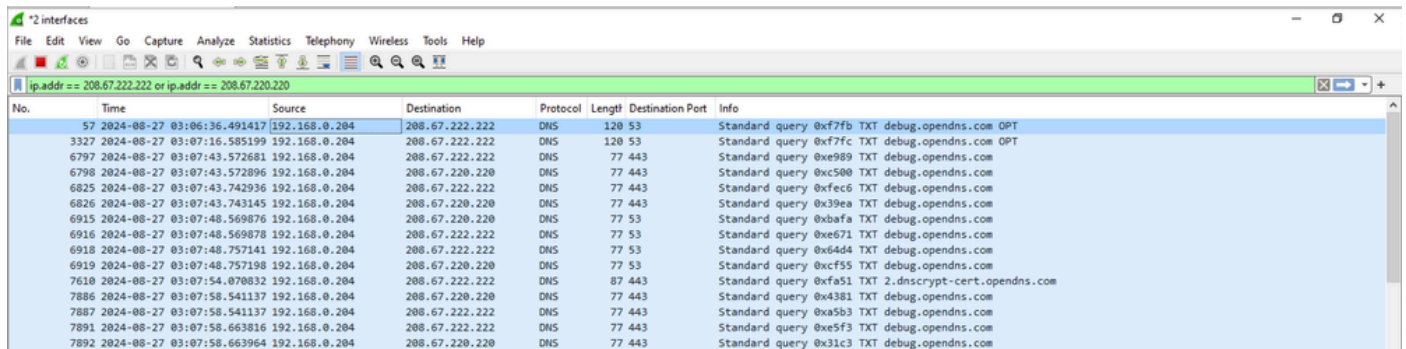
## ةيحمحم ريغ DNS ةيامح ةلأح

ىلع يوتحت ال ةلوجتم ال ةيظمن ال ةدحو ال نأ حجراأل نم ف، ةيحمحم ال ريغ DNS ةلأح ىرت ام دنع (208.67.222.222 و 208.67.220.220) OpenDNS م داوخل تانايب ال قفدت لاصتا DART. ةم زح نم عزج وه، cscUmbrellaplugin.txt فلم ي ف لوخدل لآس ىرتس

```
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
```

ةهجاو ىلع ك ال سأل طاقن ال ةيحمحم ك نكم ي، ىرخأ ةرم اءديكأت و لاصتا ال لكاشم نم ققحتل ةكرح نع طقف ثحب لل ضرع ال حشرم مادختسا و، (WiFi أو Ethernet) رتوي بيم كل ال ةيحمحم ةلأح ال رورم ال OpenDNS تال ي لآس ال ةهجوم ال رورم ال

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	208.67.220.220	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 03:07:43.742936	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 03:07:54.870832	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

DNS تام ال عتسا لاسرا لساوي لىم ال نأ حضاو ال نم، Wireshark نم ةصا صق ال ي ف ىرت ام ك ىقلى ال هنكلو، 53 و 443 ءانيم UDP ىلع 208.67.222.222 و 208.67.220.220 ىل ةهجوم ال TXT ةباجتسا ي

عنم ي طيحمحم ال ةيامح ال راج زا هج نأ حجراأل ىلع و، كولس ال اذه ءارو ةددم بابسأ كانه نوكت دق DNS م داوخل ال تانايب ال رورم ةكرح ل طقف حمسي و، OpenDNS م داوخل ال DNS رورم ةكرح ةني عم.

ةرفوتم ريغ ةباجس ال ةمدخ يه بيولا ةيامح ةلأح

حجراأل ىلع ةلوجتم ال ةيظمن ال ةدحو ال نإف، ةمدخل لل ةرفوتم ريغ بيولا ةيامح ةلأح ىرت ام دنع ةنم آل بيولا ةباجس م داوخل تانايب ال قفدت لاصتا ال ىلع يوتحت ال

Umbrella.txt فلم ي ف لآس ال ىرتس ف، SWG م داوخل IP لاصتا رتوي بيم كل ال ىدل نكي مل اذا

DART. ةمزمح نم اعزج دعوي يذلاو

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

مداخبل لاصتات نمضتتي ال رتوي بمكلا نأ تابثإل مزحلا طاقتللا عمجب مق، رثكأ قيقحتلل  
SWG.

ن: اوانع SWG لصحي نأ ةيئاهتنا يف رمألا تردصأ

<#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

جرخم ةهجاو ىلع كالسأل طاقتللا عيجمحت كنكمي، اهديكأتو لاصتاللا لكاشم نم قيقحتلل  
رورملا ةكرح نع طقف شحبلل ضرعلا حشرم مادختساو، (WiFi أو Ethernet) رتوي بمكلا لةي داملا  
(ةقباسلا ةوطخللا يف هيلع لوصحللا مت يذلا IP ناونع مادختسا) SWG مداخلىل ةهجوملا

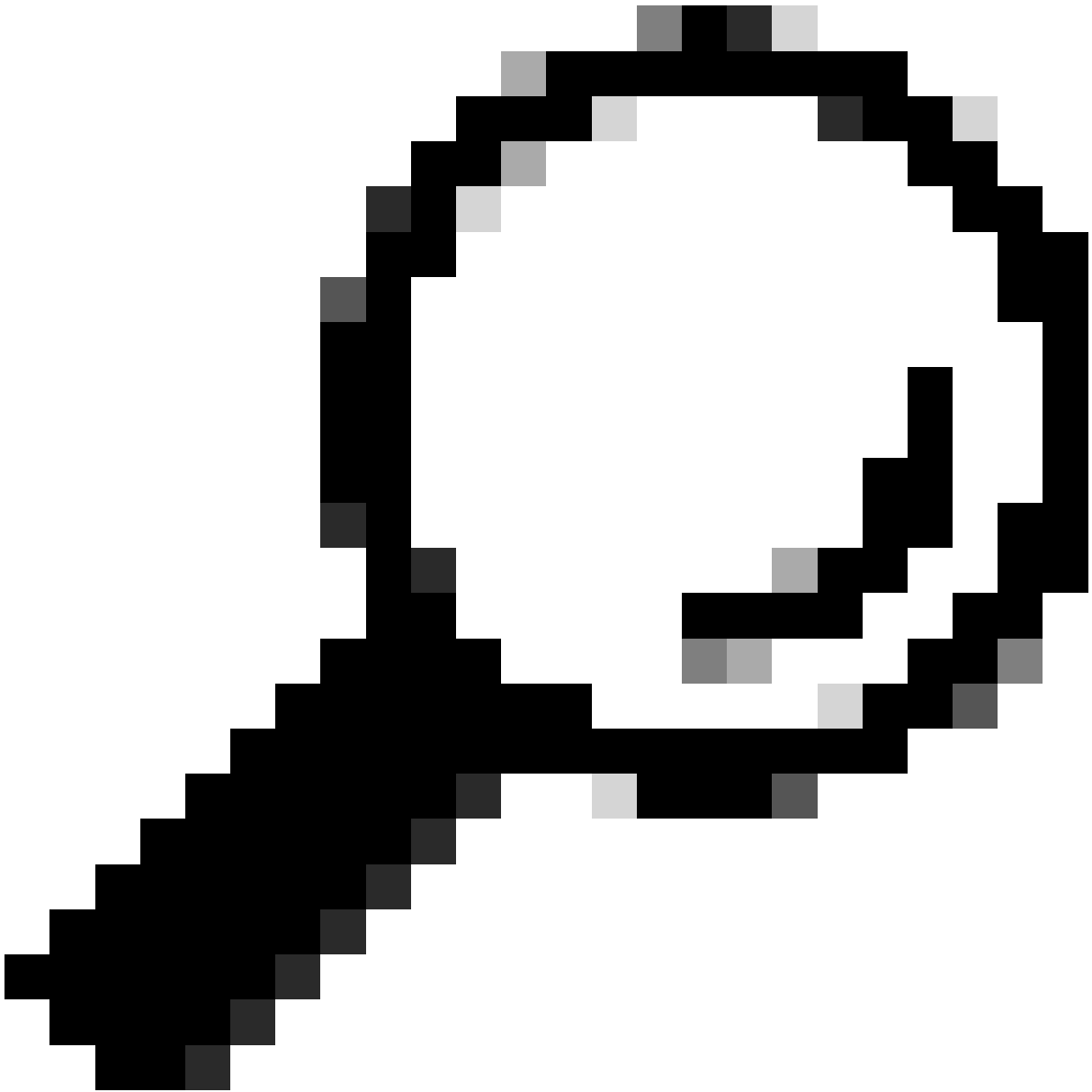
ip.addr == 18.135.112.200

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

لصاوي ليعمعلنا حضاولا نم، Wireshark، نمة ريغصلا ةيجمربلا ةملي لعتلا في ىرت امك ةباجتساك TCP RST ىقلى تي هنكلو، 18.135.112.200 ىلا ةهجوملا TCP SYN مزح لاسرا

ناونع ىلا تانايبلا رورم ةكرح عنمي قاطنلا ةيامح رادج ناك، اذه دحمل لمعمل ويرانيس في IP ل SWG.

TCP RST سىلو، طوق TCP SYN لاسرا ةداعا تاي لمعم ةدهاشم كنكمي، عقاول ويرانيس في



يضا رتفا لكش ب ه ن إ ف ، SWG م داوخ ىلإ لوصولا نم ليمعلا نكم تي مل اذا : حيملت  
ت نرتن إ لىلإ رشابملا لوصولا لال خ نم بي و رورم ة كرح جورخ دنع لش ف حتف ة ل ا ح ي ف  
ل. لش فل ا حتف عضو ي ف بي و ل ا ة ي ا م ح ق ي ب ط ت م ت ي ال . (ت ن ر ث ي إ و أ WiFi)

## لحل

نكم ي ، لكاشم ثودح ي ف ب بستت ة ي س ا س ا ل ا ة ك ب ش ل ا ن ا لىل ع ة ع ر س ب ف ر ع ت ل ا ل ج ا نم  
رادج ي ا لىل ع ي و ت ح ت ال (Hotstop ، Home WiFi) ى ر خ ا ة ح و ت ف م ة ك ب ش ي ا ب ل ا ص ت ا ل ا م د خ ت س م ل ل  
ط ي ح م ة ي ا م ح .

ديقم ريغ لاصتا هيدل رتوي ب م ك ل ا ن ا نم دك ا ت ل ا ء ا ج ر ل ا ، ح ض و م ل ا ل ا ص ت ا ل ا ا ط خ ح ا ل ص ا ل  
ل [SSE قئاثو](#) ي ف ح ض و م و ه ا م ك ل ي م ح ت ل ل

DNS ةيامح ةلاح لكاشم:

- 208.67.22.222 TCP/UDP 53 ذفنم لا
- 208.67.220.220 TCP/UDP 53 ذفنم لا

ىلا لوخدلل تانايبلا رورم ةكرحب حامسلا نم دكأت ،ببول ةيامح ةلاح لكاشم ل ةبسنلاب  
[SSE قئاثو](#) - طيحمل ةيامحلا رادج ىلع IP نيوانع

كعقوم ىلع ناوئع لخدم نم نيعم قاطن دم تعي.

## ةلص تاذا تاملعم

- [Secure Access مدختسم ليلد](#)
- [Cisco Secure Client نم DART ةمزح عي مجت ةيفيك](#)
- [Cisco Systems - تادنتس مل او ينقتلا معدلا](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت  
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او  
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب  
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لالحل وه  
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إلل دن تسمل