

SWG ةيظمنلا ةدحولل ي في ةيجراخلل تالاجملل نمآلل ليملل

تايوتحملل

[ةمدقملا](#)

[فماع قرظن](#)

[ةقيظللل مذهب لمعت اذامل](#)

[اذه يينمهي اذامل](#)

[اهحلصلل ةيظمنلا هذه عاطخأ فاشك تسأ ييننكمي فيك](#)

[KDF لفس تالخدملا](#)

ةمدقملا

(SWG) بيولخدم نمأي (AnyConnect اقباس) (CSC) نوبز نمأي cisco لا فيك ةقيثو اذه فصي
اذه نم تاريثأتلا بناج ىلإ ناليم ةمئاق يجراخلل لاجم لكشي لا ةيظمن ةدحو



2023 ماع ي في Cisco AnyConnect ل يضارثف ال رمة الة نة Cisco تنلعة: عظهال م Cisco Umbrella عالمة نم ديدع ال ديفتسي. 2024 ماع ي في Umbrella لوجتم ال لمع الو برقأ ي في ليحرت ال ادبل ك عيجشت متي و، نم آل Cisco لي مع ال ليحرت ال نم لعف ال باب فراعمة ال دةقاة لاقم ي في ديزم ال أرقا. لصفأ ل اوجتة برة جت ال لع لوصحلل نمم تقو Umbrella؟ طمة ن ال دةحول م ادختساب Cisco Secure Client تي بثة ي ن نكمي فيك: هذه

ةماع ةرطن

اتلك ي في، كلذ عمو. IP نيوانعو تالاجم ال نم الك ةلظم ال [ةيجراخ ال Cisco تالاجم ةمئاق](#) لبقت ال ادانتسا طقف انثتس ال رارق قي بطة طمة ن ال CSC SWG دةحول نممي، ني تالاجم ال IP. ناو نع

رورم ةكرح فيرعتل طمة ن ال SWG دةحو اهم دختست تي تال ال آل نوكت، لاع يوتسم ال لع يلي امك ةيجراخ ال تالاجم ال ةمئاق ي في تالاجم ال ال تاناي ال

- تاللمع ديدحتل ل لمع ال زاهج نم DNS ثحب تاللمع ةبقارم ب SWG طمة ن ال دةحول موقت ةيجراخ ال تالاجم ال ةمئاق ي في تالاجم ال نع ثحب ال

- ةيلحم DNS تقوؤم نيزخت ةركاذ ىلإ اهل ةقبطاطم ال IP نيوانعو تالاجمل هذه ةفاضل متت
- لاجمل لثامي IP ىلإ ةهجوم رورم ةكرح يأل ىلع SWG زواجتب رارقلا قيبطت كلذ دعب متي و لاجمل ىلإ رارقلا دنتسي ال .يلحمل DNS تقوؤملا نيزختلا ةركاذ نمض يجرالخ HTTP. بلط نمض مدختسملا

ةقيرطال هذه لمعت اذامل

ىلع طقف يوتحت امناف ،وحنلا اذه ىلع ،3/Layer4 ةقبطاطم ي ف ةيطمنل CSC SWG ةدحو لمعت تاعومجم 5 وذل لاصلتال لىصافت نيزخت يتل TCP/IP سوؤر ي ف ةيؤر ةيناكل ةكرح زواجت دعاوق سيسيأت امنكمي يتلاو (DestinationIP:Port، SourceIP:Port and Protocol) اهب ةصاخلا رورملا

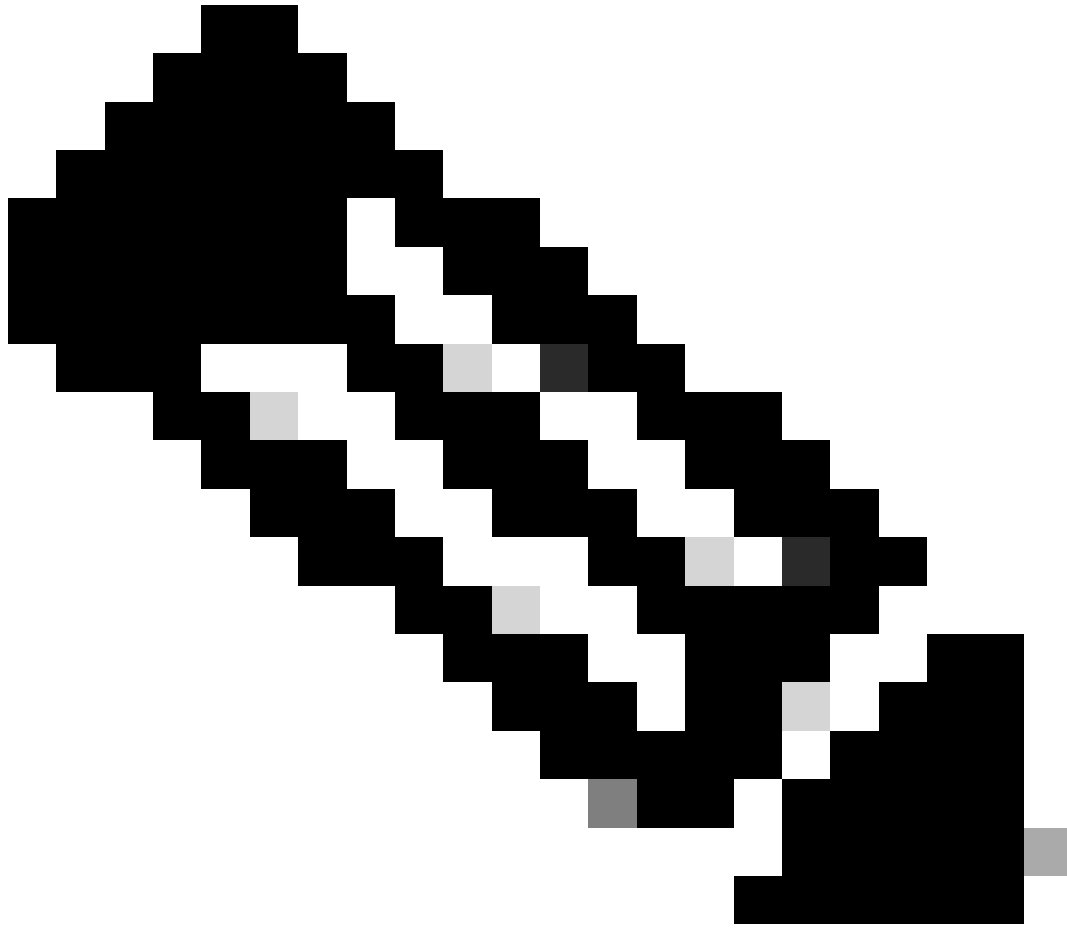
ةمجرتل ةقيرط CSC SWG بلطتي ،لاجمل ىلإ ةدنتسمل تازواجتلل ةبسنلاب ،كلذل تانايبلا رورم ةكرحل اهتقبطاطم كلذ دعب نكمي يتلاو IP نيوانع ىلإ ةمئاقلا ي ف تالاجمل شحب تايلمع نم DNS ل تقوؤملا نيزختلا ةركاذ عاشناب موقت ،ةياغل هذهل .ليمعل زاهج ىلع IP ناونع درسب DNS ل تقوؤملا نيزختلا ةركاذ موقت ،ليمعل نم اهل اسرا مت يتلا DNS ةيجرالخال تالاجمل ةمئاق ي ف ةدوجوملا تالاجملل قبطاطملا

اهضارتعا مت يتلا تانايبلا رورم ةكرح ىلع SWG زواجتب رارقلا قيبطت كلذ دعب متي .هذه IP نيوانع ىلإ ةهجوملا (80/443 يضايرتفا لكشب)

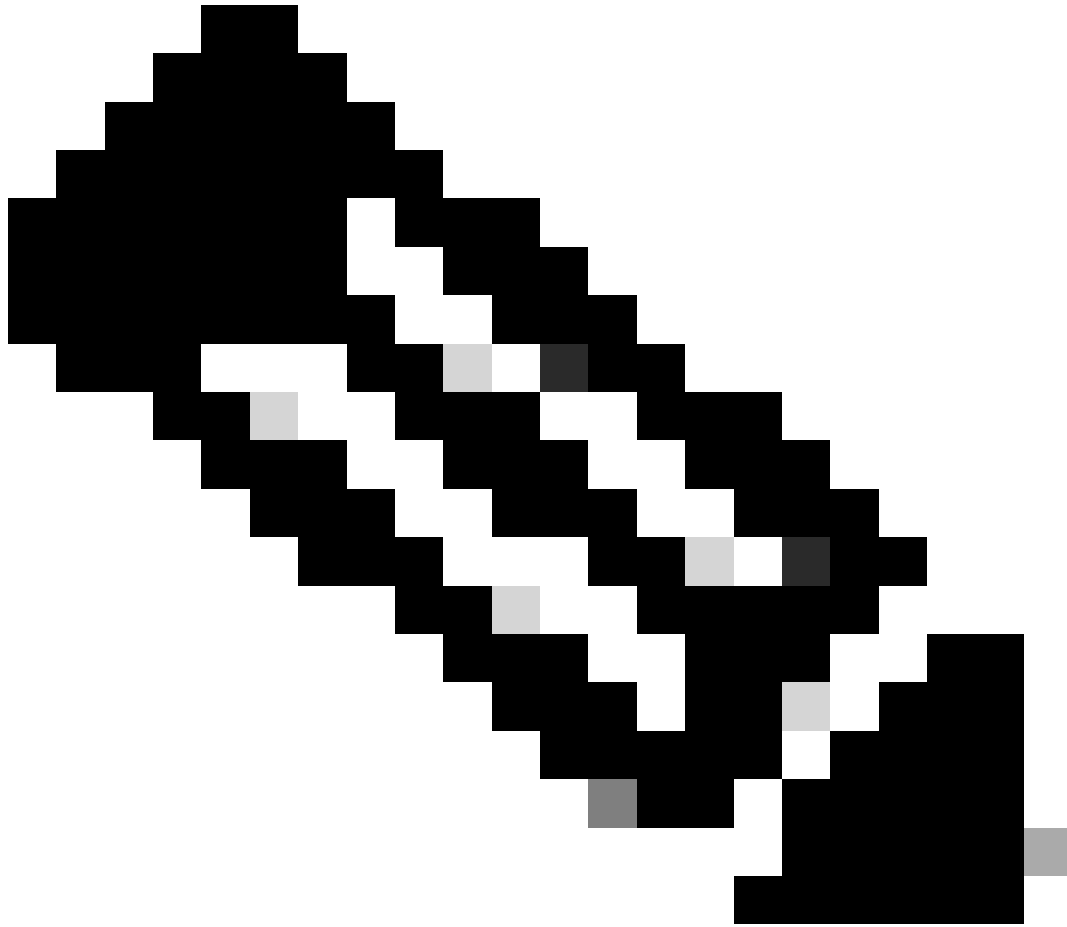
اذه ينمهي اذامل

اذه اهببسي دق يتلا ةكرتشملا اياضقلا نم ددع كانهو

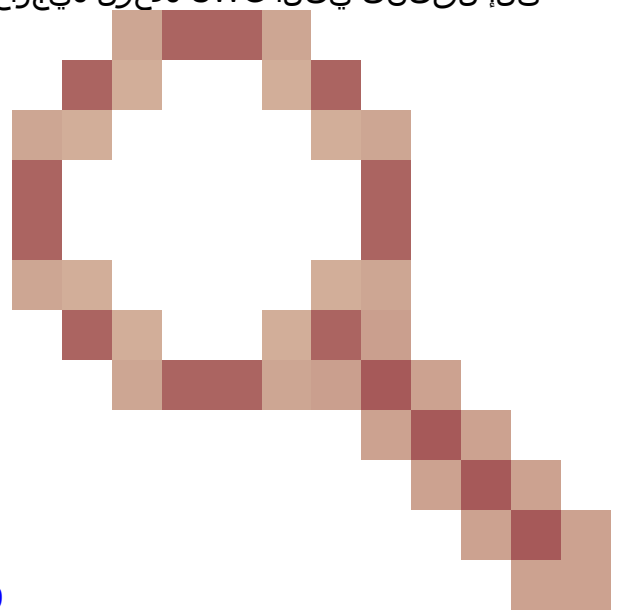
1. ةكرح زواجت اضيأ متي ،IP ىلع فاطملا ةياهن ي ف دمتعي فافتلالا رارق نا ضارثفاب .
ناهنع جتني امم Cisco Umbrella، نم IP هسفنلا ي ف كرتشت يتلا ىرخال تالاجمل رورم ةسايس هيدل سيلو ةرشابم ليمعل نم عقوتم ريغ رورم ةكرح ليچست ليمعل بقاري طاشنلا نع شحبلا ي ف ةرهاظ وأ ةقبطاطم SWG.
2. وه امك) لاجملل DNS نع شحبلا ةيؤر نم ببس يأل ةيطمنل SWG ةدحو نكمت مل اذإ
ةركاذ ىلإ IP ةفاضل متت نلف ،(لاجملل يلحم فيضم لاخدا كانه ،كلذ ي ف لاجل ىلإ عقوتم ريغ لكشب تانايبلا رورم ةكرح لاسرا متي يلاتلابو ،تقوؤملا نيزختلا SWG.



ثحب ءارجإ مت اذإ . طقف DNS UDP ثحب تاي لمع KDF لي غشت جمان رب بقاري : ةطحال م
متي نلوت قؤم لاني زختلا ةركاذى لىإ IP ةفاضإ متت نلف ، ببس يأل TCP ربع DNS
Cisco نم ءاطخألان ع ثحب لىإ في اذه رشن متي . يجرالخال لاجم لاقى ببط



ىلا لقتنت يتال SWG ةدحول ةيجراخلا تالاجملا عم ةلكشم انحلصأ دقل :ةظالم



Umbrella ءنح DNS ربع TCP ([CSCwe48679](#))
(Cisco Secure Client 5.1.4.74 (MR4) ف (Windows و MacOS))

اهال صاوي لمعل هذه عا طخا فاشكتسا يننكمي فيك

ىل تال اذ اة فاضا و DNS، ثح تاي لمع بقارت ي تال اة طمنن ال SWG ة دحو ة لمع عابتا نكمي في IPs ل ة هجوم ال رورم ال ة كرح ىل ع فافتال ال ة لمع قي بطت و DNS، ل تقوؤم ال نيزختال ة كذا ة رت فل طق ه نكمي و احاتم KDF لي جست نو كي نا كلذ بلطتي KDF تال جس تال جس ال عاستا ببسب اهال صا و عا طخا ل فاشكتسا انا ثا ة ري صق

KDF لجس تال خدم لاثم

DNS ل تقوؤم ال نيزختال ة كذا ىل اة فاضا ممت لاجم نع DNS ثح

```
00000283 11.60169029 acsock 11:34:57.9474385 (CDnsCachePluginImp::notify_recv): acquired safe buffer fo
00000284 11.60171318 acsock 11:34:57.9474385 (CDnsCacheMgr::AddResponseToCache): add to cache (www.club
00000285 11.60171986 acsock 11:34:57.9474385 (CDnsCacheMgr::addToCacheByAddr): Added entry to cache by
00000286 11.60172462 acsock 11:34:57.9474385 (CDnsCacheMgr::addToCacheByAddr): Added entry to cache by
00000287 11.60172939 acsock 11:34:57.9474385 (CDnsCacheMgr::addToCacheByAddr): Added entry to cache by
00000288 11.60173225 acsock 11:34:57.9474385 (CDnsCacheMgr::addToCache): Added entry (www.club386.com,
00000289 11.60173607 acsock 11:34:57.9474385 (CDnsCacheMgr::AddResponseToCache): add to cache (www.club
```

ربع لسري بل طال، ة ج راخ ال تال اجم ال ة مئاق ىل ع سيل لاجم ال، HTTPS لاصتا ة طحال ممت
SWG:

```
00000840 10.69207287 acsock 12:13:50.0741618 (CNvmPlugin::notify_bind): called
00000841 10.69207764 acsock 12:13:50.0741618 (CNvmPlugin::notify_bind): nvm: cookie 0x0000000000000000:
00000842 10.69208336 acsock 12:13:50.0741618 (CSocketScanSafePluginImp::notify_bind): websec cookie FFF
00000843 10.69208908 acsock 12:13:50.0741618 (COpenDnsPluginImp::notify_bind): opendns cookie FFFFD30F9
00000844 10.69209576 acsock 12:13:50.0741618 (CNvmPlugin::notify_send): nvm: cookie 0000000000000000: p
00000845 10.69211483 acsock 12:13:50.0741618 (CDnsCacheMgr::GetAllDomainNamesByIpAddr): lookupAll by ad
00000846 10.69221306 acsock 12:13:50.0741618 (CSocketMultiplexor::notify_stream_v4): recv: protocol 6,
00000847 10.69222069 acsock 12:13:50.0741618 (CNvmPlugin::notify_recv): nvm: cookie 0000000000000000: p
```

ءار ا قي بطت ممت، تقوؤم ال نيزختال ة كذا في دوجوم IP ل ل اذ ا، HTTPS لاصتا ة طحال ممت
زواج:

```
00003163 9.63360023 acsock 15:33:48.7197706 (CNvmPlugin::notify_bind): called
00003164 9.63360405 acsock 15:33:48.7197706 (CNvmPlugin::notify_bind): nvm: cookie 0x0000000000000000:
00003165 9.63360882 acsock 15:33:48.7197706 (CSocketScanSafePluginImp::notify_bind): websec cookie FFFF
00003166 9.63361359 acsock 15:33:48.7197706 (COpenDnsPluginImp::notify_bind): opendns cookie FFFF8C02C8
00003167 9.63364792 acsock 15:33:48.7197706 (CNvmPlugin::notify_connect): called
00003168 9.63365269 acsock 15:33:48.7197706 (CNvmPlugin::notify_connect): nvm: cookie 0x0000000000000000:
00003169 9.63366127 acsock 15:33:48.7197706 (CSocketScanSafePluginImp::notify_connect): websec cookie F
00003170 9.63367081 acsock 15:33:48.7197706 (CDnsCacheMgr::GetAllDomainNamesByIpAddr): lookupAll by add
00003171 9.63367558 acsock 15:33:48.7197706 (CDnsCacheMgr::GetAllDomainNamesByIpAddr): lookupAll by add
00003172 9.63370323 acsock 15:33:48.7197706 (CSocketScanSafePluginImp::getFQDN_check_domain_exception):
00003173 9.63370800 acsock 15:33:48.7197706 (CSocketScanSafePluginImp::evaluate_rules): domain name fou
00003174 9.63371372 acsock 15:33:48.7197706 (CSocketScanSafePluginImp::notify_connect): cookie FFFF8C02
```


ةمچرتل هذه ل و ح

ةيلآل ا تاي ن ق ت ل ا ن م ة و م ج م ا د خ ت س ا ب د ن ت س م ل ا ا ذ ه Cisco ت م چ ر ت م ل ا ع ل ا ا ح ن ا ع م ج ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل ا و ا م ك ة ق ي ق د ن و ك ت ن ل ة ي ل آ ة م چ ر ت ل ض ف ا ن ا ة ط ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب Cisco ي ل خ ت . ف ر ت ح م م چ ر ت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة م چ ر ت ل ا ع م ل ا ح ل ا و ه ي ل ا ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا م چ ر ت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا