

DNS طاشن لجس تال اخدا عا طخأ فاش كُتسأ رارق لا رطح عم اه حال صا و

تا يوت حم لا

ة ل أسم

ضارعالا هذه نم رثكأ وأ دحاو نع غالبإلا متي و

- (DNS شادحأ إلى هتي فصت تمت، Monitor > Activity Search) طاشن لا ي ف شحب لا رهظي
ة دعاق فشكي ال تنرتنإلا إلى لوصول دعاوق ةعجارم نكل، لاجمل "روطحم" = عارجإلا/ رارق لا
هعنمت اهنأ حضاو لا نم
- لوؤسم لا اب ظفحتي رطح ةهجو ةمئاق يأ ي ف دوجوم ريغ لاجم لا

ة ئي بل

- إلى دنتم لا اذه ي ف ةدراولا تامولعمل دنتمت
- Cisco نم (SSE) نم آلا لوصول ةباحسل يساسألا ماطن لا
- لوصول ةسسؤم إلى اهلي جست و لاوحت لا نامأ ةدحو رشن عم Cisco Secure Client 5.x
نم أ

راق

اهم ييقت مت يتي لا ةي وه لا نم ققحت لا 1. ةوطخ لا

- ال دب قفن وأ عقوم وأ ةكبش ةي وه شدحل رهظأ اذا. اهدض رارق لا دختا يتي لا ةي وه لا نم دكأت

دعاوق ةعومجم قباطي مالعئسالا نإف ،عقوئملا لوجئملا مدختسملا وأ رئويبمكلا نم اهئعجارم ئمئلا كئلئ نع ةفلئخم

- هنع ريراقت دادعإو زاهجلا ليجسئ نم ققحت ،ئيلوجئملا ئيمدختسملل ةبسنلاب يمحكم

— ةدوصقملا ةيوهلا قيبطئ مئئ شئحب رشنلا ةيلمع ئيحصئب مق :ةيوهلا قباطئ مدع ةعومجم طبض وأ ،ئيمدختسملا ةعومجم AD/ئيئعئ ءالصا وأ ،لوجئملا زاهجلا ليجسئب مق ئيحص ريء لكشب قباطئ ئئلا ةدعاقلا ئيئفئ نم الءب — ةكبشلا ةيوه دعاوق

نامأ ةئف ةقباطم نم ققحتلا: 2 ةوطخل

- ئئلا ئالاجملا ،ئلائئءالا ئيصئلا ،C2 ،ءراضلا جماربلا) نامأ ةئف لمئئ شءءلا ناك اذا ئاداعإ نم ئئأئ ةلئكلا نإف ،(كئذى لا امو ،ئيقفنلا DNS لاصئلا ،ئئئء اهضرع مئ لىا لىوئملا ةدعاق وأ ةءءولا ةمئاق ءائءئ ال — ةقباطملا دعاوقلا ةعومجملا نامألا لاجملا لىا ةراشلا
- ئف Cisco Telos ءاكئلا ةباب لىل هئئئصئو لاجملا ةيلءالا ةعمسلا نع شءب (ةعمسلا زكرم نع شءبلا) <https://talosintelligence.com/>
- بلمئ مئءقئب مقف ،ءئئص ريء Talos ئف ءضوملا ةعمسلا وأ ئئئصئلا ئئاك اذا <https://talosintelligence.com/> لالء نم ةرشابم Talos عم (ةلاء ءئف) ئئئصئ ةدعاق/ءازن رشن مئئ ،ئئئصئلا شئءءب Talos موقئ ناأ ءرءب .لاجملا مئئقئ ةدعاق مئئ ئئء لوصولل ئئفئئ نامضل ريءئلا

CNAME ةلسلس صءف: 3 ةوطخل

- لىل) ةلماكلا ئاباءلا ةلسلس صءفو ةافصملا ريء vantage ةطقن نم لاجملا لءب مق (`nslookup -debug <domain>` وأ `dig +noall +response <domain>` ،لائملا لئبس
- Talos ئئئصئ ءضو ةءءولا مئواق لباءم ةلسلسلا ئف CNAME فءه لك نم ققحت ائرهاظا ئئظن مالعئسالا لاجم لىل هرظء مئ رارق ءرشب روطءملا CNAME فءه موقئ

ةئلءفلا ةيوهلل لفسأ لىا لىلءأ نم ءهئلا مئئقئ ةدعاق: 4 ةوطخل

- ققءئو ،1 ةوطخل نم ةيوهك بئئرئلاب ئئرئئلا لىا لوصولل دعاوق عم لقئئلاب مق ،قئبئلا/لىوئملا/نامألا ئاداعإو ،ئئكمئلا ةلاءو ،ةلوءءو ،ةدعاق لكلا ةيوهلا قاطن نم

اهني مضتو ةيضا رتفال ةدعاقلا ىلإ الوصو

- (policy.test.sse.cisco.com/?=cisco.com - لاثملا لىبس ىلع) تاسايسلا ربتخم مدختسا
اهل اقباطم نمآلا لوصول ريراقت دعت يتلا ةدعاقلا ةفرعمل ةهجولا ةقيقدلا ةيولاب
ثدحلا ىلع ةامسملا ةدعاقلا اب اهت نراقمو

اثي دح اهضرع مت يتلا تالاجملا :ةصاخ ةلاح

(NSD) اثي دح اهضرع مت يتلا تالاجملا يه ثدحلا يف نامألا ةئف تناك اذا

:ةيلضفألا بسح ،ةجلالعمل تاراخي

اهلإ راشملا ةهجولاب حامسلا ةمئاق ىلإ هتفاضاب مقف ،لامعألل اساسح لاجملا ناك اذا
NSD نامألا ةلتك ىلع حامسلا لاخدإل ةيولوألا نوكت ؛قيبطتلل ةلباقلا ةدعاقلا ةطساوب
ةهجولا كلتل

QUIC و (DoH) رفشملا DNS لي طعت

مهاست يتلاو DNS ةقبط ةيؤري ف تاوچف ثودح يف رفشملا QUIC و DNS ببستي نأ نكمي
ضرعتسملا ربع اهلع مت يتلا تامالعتسال لصت ال :طاشنلا نع ثحبلا جئاتن كابري ف
امنبي ،(لمكلا لجلسلا نم ةدوقفم يهف يلاتلابو) "نمآلا لوصول تالوحم" ىلإ اقلطم DoH
ةروطحم ثادحأك اهسفن DoH رفوم تالاجم رهظت نأ نكمي

تالاجملا عامسأ ماطن لظي نأ ةرادملا ةياهنلا طاقن ىلع هذه لقنلا تايلمع لي طعت نمضي و
يلعفل ةياهنلا ةطقن كولس طاشنلا لجلس سكعي نأ وصحفلل الباق DNS

حفصتم لكل (DoH) HTTPS ربع DNS

Google Chrome

- .نمآلا DNS مادختسا ليغشت فاقياو chrome://settings/security ىلإ لقتنا :يودي

Microsoft Edge

- ن.م آال DNS مادختسإ ليغشت فاق يإو edge://settings/privacy إىل لقتنا :يودي

Mozilla Firefox

- يف ةكبشال تاداعإ وأ) HTTPS ربع DNS > نامألاو ةيصوصخال > تاداعإ > ةمئاقال :يودي HTTPS ربع DNS نيكمت ديدحت ءاغإل / فاق يإ ددحو (مدقأال تارادصإل)
- (use- Mozilla Canary لاجم إىل ع ةباجإل اب Umbrella/Secure Access تالوحم موقت :ةطحال م إىل ؛يضارتفا لكشب اديعب DoH ءاقبإل Firefox إىل ريش ةقيرطب (application-dns.net) مدختسمال لبق نم نيعمل DoH نيوكت نأل اهب ىصوم ةحيرصل GPO تاداعإ لازت إىل Mozilla kill-switch/canary تالاجم ةفاضإب مقت ال :ريدحت .يسنكلال ققحتال زواجتي اهنأ إىل ةحفصلال ةلتكل A لجس ةباجتسإ عم لماعتال متي — رطحال ةهجو ةمئاق هتيرت وأ DoH مادختساب طاقتحال اب Firefox مايقي ف ببستت نأ نكمي و ةحيرص

QUIC (HTTP/3)

ربع DNS) DoH3 و ةماعال بيولال رورم ةكرح نم الك لمحي عطتسي و UDP/443 ربع QUIC ضكري TCP. عقوت يتال شيتفتال تاراسم ازواجتم ،(HTTP/3

يذلاو ،TCP إىل ع مئاقال HTTP/1.1 وأ HTTP/2 إىل عوچرلل ةيوقال QUIC تاضرعتسم ليطعت :ةلمالكال ةيؤرلا ةيناكمإ ديعتسي

- طبض : (مدختسمال لبق نم ريغيغتلل لباقو لصاوتم ريغ) يودي :ةفاحال / موركلال ل.طعم إىل chrome://flags/#enable-quic / edge://flags/#enable-quic

- (و config:لوح) network.http.http3.enable = false ليضفتال تتبث Firefox: جم انرب policy/AutoConfig).

مالعإال مت يتال ةقباطم ال ةدعاقال ةقباطم نكمم ال ريغ نم لازي ال ،تاوطخال هذه دعب ،ناك اذا ثدح ريصدت مي دقتو Cisco TAC مادختساب ةلاح حتفب مقف ،نيوكتال عم ثدحال لوح اهنع ،ةقباطم ال ةدعاقال او ،تايوهال او ،ةينمزلال ةقطنمال عم ينمزلال عباطال) طاشنل نع ثحبال ةهجو ال ةلصلال تا ذدعاقولل ةشاشال تاطقل عم (لاجمال او ،لجسلال عونو ،تائفال او

ببسلال

لبيس إىل ع - نامأ دادعإ ةطساوب لاجمال رطح متي - (Talos Intelligence) نامأال ةئف ةقباطم لاصتا وأ DNS ريفشت وأ يلايحتالال ديصتال وأ مكحتالال رماوالأ وأ ةراضال جماربال لاثمال

Cisco Talos عمس ىلإ ادانتسا - اتيح اهضرع مت يتل تالاجملا وأ يقفنل DNS لكشب انه نيوكتب لوؤسملا ماق يوتحم ةدعاق وأ ةهجو ةمئاق يأةطساوب سيلو، اهفينصتو حضاو قباطت دوجو مدعل اعويش رثكأل ببسلا وه اذه .حيرص

ةيوه) اعقوتم ناك ام نع ةفلتخم ةيوه ىلإ مالعئسالا عاجرا مت - ةيوهلا ةبسن قباطت مدع ريغ زاهج وأ، ةفلتخم AD ةومجم/مدختم وأ، لوجتملا رتوي بمكلا نم الدب عقوملا/ةكبشلا نوكت ام ابلاغ - ةفلتخم ةدعاق ةقباطم تمت اذل، (ةكبشلا يوتسم ىلع جهن ىلإ عجري لجسم ةيضرارفا وأ ةمارص رثكأ

ةدعاق) وأ ةسايسلال يلىل عسوأ ةدعاق - ةيضرارفال ةدعاقلاو ةدعاقلا بيترت اضيأ نكمي؛ ةدوصقملا حامسلا ةدعاق لبق ةقباطتم (لفسألا يلىل لكلا طاقس/ريصقتلا ردصملا نمضتت ال يتل تايوهلا عم اهقطن وأ اهتلودج وأ ةدوصقملا ةدعاقلا ليطعت رثأتملا

اي نمض يطيغي، (example.com) يلىل لاجم ىلع رطح ةهجو ةمئاق يوتحت - ةهجو ةمئاق ثيروت لاجملا ليلىلحت متي يذال IP/CIDR ىلىل يوتحي وأ، (app.example.com) ةيضرارفال تالاجملا عيجم اذه رهظي ال هذو قيقذل FQDN نع مئاوقلا يلىل ثحبلا نإ .هيلي

ليلىلحت ةلسلس نكلو، هب حومسم هنع مالعئسالا مت يذال لاجملا - CNAME ةلسلس رطح مت (روظحم/فقوتم فيضم وأ Tracker وأ CDN ابلاغ) لاجم ىلىل CNAME ىلىل يوتحت تانايبلا هنع مالعئسالا مت يذال لاجملا لجسلا ضرعيو، ةلسلسلا ىلىل رارقلا قيبطت متي؛ هرطح روظحم لاجمك لصلأا يلىل

يلىل مكنحتلا) روظحم قيبطت ىلىل لاجملا يمتني - يوتحملا وأ قيبطتلا ةئف ةقباطم نع تافينصتلا فلتخت نأ نكمي؛ هئارقاب لوؤسملا مقى مل يوتحم ةئف وأ (قيبطتلا .لوهم/ليكو وأ تافلما ةكراشم هئأ ىلىل فنصم لمع ةادأ، لاثملا ليبس ىلىل) سدحلا

ارخؤم Talos فينصت وأ ةسايسلال رييغت مت - فينصتلا وأ ةسايسلال يلىل ريخألا رييغتلا دق ليىل ماعلا نم ازمل/جهنلا رشن وأ، رييغتلا نكي مل (ةقحالا خيراوتلا وأ) ةعجارملا ديق ثدحلا مالعئسالا تقو هلامكإ مت

ةلصلال يذ يوتحملا

- [Umbrella ل ةيلىلخادلا DNS مداوخ نيوكت](#)
- [Umbrella مادختساب HTTPS \(DoH\) ربع DNS نيوكت](#)
- [نمآلا لوصولا يلىل لاجملا ب مكنحت ةدحو ةفاضلا](#)
- [Cisco نم نمآلا لوصولا ةلتك ةحفص تامولعم](#)

- [Cisco نّم تالېزنتال او ښفلل م عدلا](#)

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