

ىلع SAML عم ةعئاشلا لكاشملا فاشكتسا اهحالصا و FTD و ASA

تايوتحمل

[ةمدقملا](#)

[ةيساسالابلاطتلا](#)

[تابلطتلا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسا تامولعم](#)

[ةعئاشلا لكاشملا](#)

[نالكلا فرع م قباطت مدع: 1 ةلكشم](#)

[جرشلا](#)

[لجلا](#)

[حلاص ريغ ديكأتلا: 2 ةلكشملا](#)

[جرشلا](#)

[لجلا](#)

[عيقوتلا ققحتى ال: 3 ةلكشملا](#)

[جرشلا](#)

[لجلا](#)

[Confirmation Consumer Service لحيحص ريغ URL ناونع: 4 ةلكشملا](#)

[جرشلا](#)

[ةلثمألا](#)

[لجلا](#)

[حلاص ريغ ديكأتلا رومج: 5 ةلكشملا](#)

[جرشلا](#)

[لجلا](#)

[SAML نيوكت تاريغت نايرس مدع: 6 ةلكشملا](#)

[جرشلا](#)

[لجلا](#)

[ةومجم لاصتا تافيصوت نمض ايلخاد ني درشملا سفن مادختسا ةيفيك: 7 ةلكشملا
ةددعت م قافنا](#)

[جرشلا](#)

[لجلا](#)

[لوخدلا ليجست طاب ترا فيرعت فلم دادرستلا يف ةلكشم ببسب: 8 ةق، داصملا تالشف
يداحألا](#)

[جرشلا](#)

[لجلا](#)

[ةئجنتلا قباطت مدع ليخرت ةلاح: 9 ةلكشملا](#)

[تاريسفت](#)

[لجلا](#)

[اهحالصا و عا طخألا فاشكتسا نم دي زملا](#)

[ةلصتا اذ تامولعم](#)

مقدم

أطاح فاشكتسأءانثأهتفداصممتيتالاعويش رثكال لكاشملا دنتسملا اذه فصيا
Cisco ASA و FTD ؤزهجأىلع اءالصال SAML.

سساسال تابلطملا

تابلطملا

الالاعوضاوملاب ؤفرعم كيدل نوكت نأب Cisco يوصوت:

- SAML (IDp) ؤي وه رفوم نيوكت
- Cisco Secure ASA Firewall و FirePOWER Threat Defense (FTD) يءال لوخذل ليءست نئاك نيوكت
- Cisco Secure Client AnyConnect VPN

مءءتسملا تانوكملا

الالاءماربالاو ؤزهجال تاراءصالإلى تاسرامملا لضافألىل دنتسي:

- Cisco ASA 9.x
- Firepower 7.x / FMC 7.x ؤي ؤهء ءض عافءل اءارب

صاا ؤيلمم ؤئيب ي ؤءووملا ؤزهجال نم دنتسملا اذه ي ؤءراول تامولعملا عاشنإم
تناك اءا. (يضا رءافا) ءوسمم نيوكتب دنتسملا اذه ي ؤمءءتسملا ؤزهجال عيمءا ءب
رمأىل لمءءملا ريثأءلل كمهف نم ءكأءف، ليءشءل ءي قءكءبش.

سساسا تامولعم

ءقءاصملا تانايب لءابءل XML لىل دنتسي لمع راطإيه (نامال ءيكأء زييمء ؤغل) SAML
ءوزم و مءءتسملا نيب ؤءال نم ؤرئاء عاشنإىلع لمعي وهف. نامال تالاءم نيب ضيوفءل او
ءامء ؤءل ؤءاو ؤرم لوخذل ليءسءب مءءتسملل ءمسي امم (IDp) ؤي وهلا ءوزم و (SP) ؤمءءل
Cisco Secure Client Connections ل VPN ءعب نع لوصول ؤقءاصملا SAML مءءءسإن كممي
نامال ؤرئاء ي ؤي SP نايك وه FTD و ASA نوكي ءيء، ASA و FTD VPN HeadEnd.

يراءل ASA/FTD و IDp لىلع نيوكءل نم ققءءل قيرط نع SAML لكاشم مظعم لءن كممي
نم ءيزملا ءيءصءل ي طعي، ءضا و ريغ ببسل اهي نوكي يءل تالاءل ي. اءامءءسإ
debug webVPN saml 255 رمل نم لىلءل اذه ي ؤلءمال رهظء و ءوصل.

ءنكمملا لولءل او ؤفورعملا SAML لكاشم ل اعيرس اعءرم نوكي نأ وه دنتسملا اذه نم ضرغل.

ءئاشل لكاشملا:

نايكال فرعم قءاباء مءء: 1 ؤلءشملا

حشرل

قبطاطي ال ةيامل رادل WebVPN نيوك ت نمض [entityID] saml idp رمأل نأ ماع لكشب ينعي
لاثلما في حضوم وه امك IdP's فيرعت تانايب في هيلع روثعل مت يذل IdP نايك فرع م عم

ءاطأل احيصت لاثم:

Sep 05 23:54:02 [SAML] consume_assertion: The identifier of a provider is unknown to #LassoServer. To r

IDP: ع قوم نم

<#root>

<EntityDescriptor ID="

_7e53f3f3-7c79-444a-b42d-d60ae13f0948

" entityID="

<https://sts.example.net/69c69fff-03f6-4c9c-be73-9ed4f5f894c/>

">

ASA/FTD: نم

<#root>

saml idp

<https://sts.example.net/69c69fff-03f6-4c9c-be73-9ed4f5f894>

>>>> The entity ID is missing characters at the end

لحل

فرع م [saml idp] رمأل رييغت ب مقو IdP فيرعت تانايب فلمب صاأل نايك الفرع م نم ققحت
(/). ةيسكع ةلئام ةطرش فرأ يأ لكذي في امب ،امامت اذه ةقبطامل [نايكال

حل اص ريغ ديكتال: 2 ةلكشمل

حشرل

نأ ثيح IdP نم مدقمال ديكتال ةحص نم ققحتال لىل رداق ريغ ةيامل رادل نأ ينعي اذهو
ديكتال ةحص قاطن چراخ ةيامل رادل ةعاس

ءاطخأل احيصت لاثم

<#root>

[SAML] consume_assertion: assertion is expired or not valid

لاثم:

<#root>

[SAML]

NotBefore:2022-06-21T09:52:10.759Z NotOnOrAfter:2022-06-21T10:57:10.759Z

timeout: 0 >>>> Validity of the saml assertion provided by the IDP
Jun 21 15:20:46 [SAML] consume_assertion: assertion is expired or not valid

<#root>

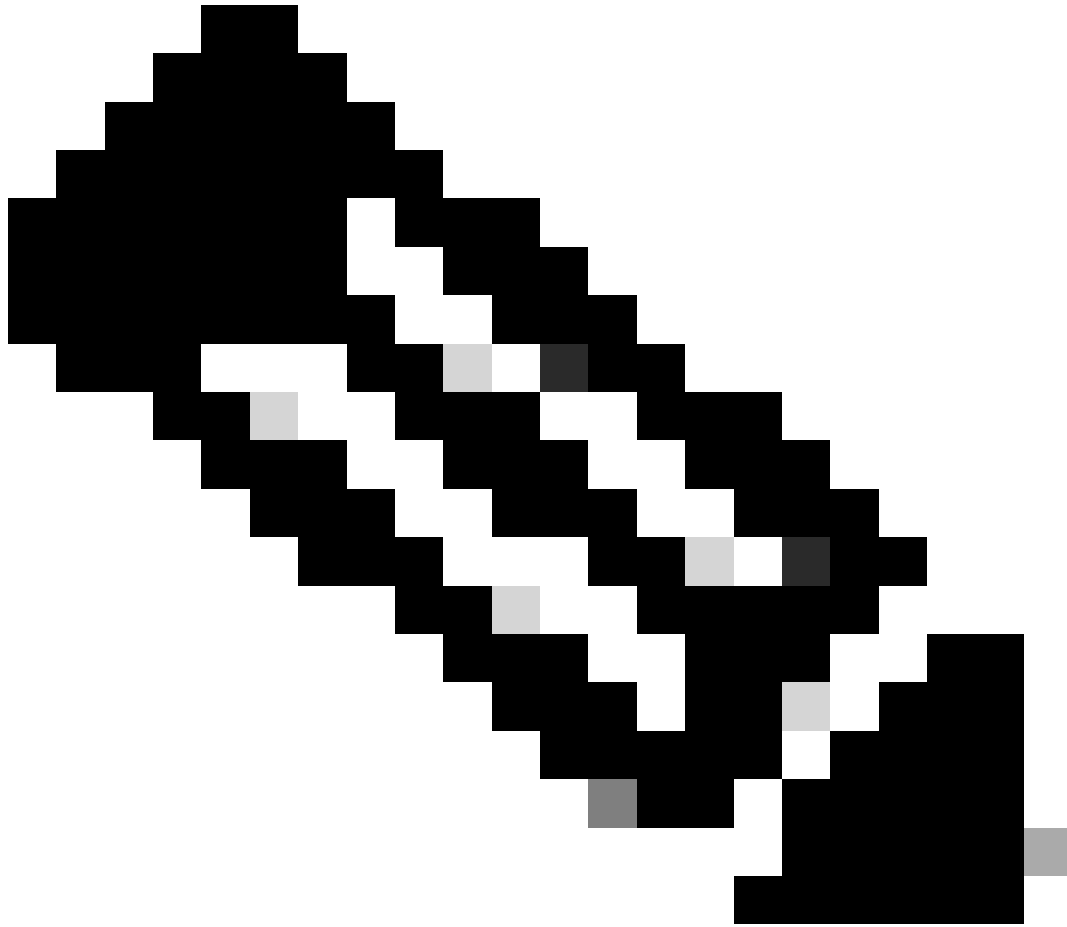
firepower#

show clock

15:26:49.240 UTC Tue Jun 21 2022

>>>> Current time on the firewall

اذة ةالصلل راطل اراخ ةيامحل رادج لىل ع تقولل او، UTC، 10:57:10.759 لىل 09:52:10.759 UTC نىب طقف حللص دىكأتل نأ لىرن نأ اننكمى، لاثم لىف



قسننم اليملاعلا تي قوتلا يف هه ديكأتلا يف ةنيبملا ةيصالصلا ةرتفو :ةطحالما
يف تقولا لوحهنا ةفلتخم ةنمز ةقطنم يف ةيصالصلا رادج ةعاس نيوكت مت اذا
ةصالصلا نم ققحتلا لبق UTC.

لحل

نأ نم ققحتو NTP مداخل مادختساب وأ ايودي ةيصالصلا رادج ىلع حيصالصلا تقولا نيوكتب مق
يف ةيصالصلا رادج نيوكت مت اذا UTC. يف ديكأتلا ةحص نمض عقي ةيصالصلا رادجل يلالصلا تقولا
ىلا تقولا ليوت نم دكأتف ،(UTC) قسننم اليملاعلا تي قوتلا نع ةفلتخم ةنمز ةقطنم
ديكأتلا ةحص نم ققحتلا لبق UTC.

عقوتلا ققحتي ال 3: ةلكشمال

حرشال

بباسب IdP نم همالتسا مت يذلا SAML ديكأت عي قوت نم ققحتلا يف ةيصالصلا رادج لشف دنع

رمأل مادختساب ةيامل رادل WebVPN نيوكت نمض اهنويوكت مت ةحيحص ريغ IdP ةداهش trustPoint idp <trustPoint>.

ءاطأل احيحصت لاثم

<#root>

[Lasso] func=xmlSecOpenSSLEvpSignatureVerify:file=evp_signatures.c:line=372:obj=rsa-sha256:subj=unknown
signature does not verify

لحل

تحت ديدج TrustPoint نييعتو ةيامل رادل يلع اهتيبثتو IdP نم ةداهش ليزنن ب مق فيرعت تانايب في IdP عيقوت ةداهش يلع ةداع روثعل نكمي. ةيامل رادل WebVPN نيوكت اهزيمرت كف مت يتل SAML ةباجتسا و IdP.

Confirmation Consumer Service ل احيحص ريغ URL: 4 ةلكشم

حرش

(ةيوهل ديكاأل ءالمعل ةمدخ URL) درلل احيحص ريغ URL مادختساب IDp نيوكت مت

ةلثمأل

ءاطأل احيحصت لاثم

لاخدإ مدختسملل نكمي. ةيلوأل ةقداصمل بلط لاسرا دعب ءاطأ احيحصت يا ضرع متي ال ءاطأ احيحصت يا ةعابط مدعو لاصتال لشف دعب نكلو دامتعال تانايب

IDP: عقوم نم

Reply URL (Assertion Consumer Service URL) * ⓘ

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

Index Default

https://ac-vpn.local/+CSCOE+/saml/sp/acs?tgname=ac-saml ✓

SP: و FW فيرعت تانايب نم

<#root>

<AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP
"https://ac-vpn.local/+CSCOE+/saml/sp/acs?tgname=acvpn"

/>

قبطاي ال IDp ىلع "ةيوهال ديكتل لىلهتسمال ةمدخ URL" نأ ةظحالمنكمي، لاثمال ي في SP. فيرعت تانايب ىلع عقومال

لحال

تانايب في حضوم وه امك IDp ىلع ةيوهال ديكتل ءالمعال ةمدخل URL ناونع ريغيغت م ق show saml metadata رمال مادختساب SP فيرعت تانايب ىلع لوصحال نكمي. SP فيرعت <tunnel-group-name>.

حلاص ريغ ديكتل روهمج: 5 ةلكشمال

حशल

أطخال قفنال ةعومجم لثم، SAML ةباجتسا في ءحيحص ريغ ءهجو IdP لسري امدنع

ءاطخال ءحيصت لاثم:

<#root>

[SAML] consume_assertion: assertion audience is invalid

SAML: عبتت نم

<#root>

<samlp:Response ID="_36585f72-f813-471b-b4fd-3663fd24ffe8"
Version="2.0"
IssueInstant="2022-06-21T11:36:26.664Z"
Destination=

["https://ac-vpn.local/+CSCOE+/saml/sp/acs?tname=acvpn1](https://ac-vpn.local/+CSCOE+/saml/sp/acs?tname=acvpn1)

"

Recipient="<https://ac-vpn.local/+CSCOE+/saml/sp/acs?>

tname=acvpn1

"

<AudienceRestriction> <Audience>

<https://ac-vpn.local/saml/sp/metadata/acvpn>

Audience>

AudienceRestriction>

SP: وأية مالح راج فيرعت تانايب نم

<#root>

<AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP
Location="<https://ac-vpn.local/+CSCOE+/saml/sp/acs?tgname=acvpn>"
>

الحل

قباطي نأ بجي SAML ةباجتسا يف ملتسمو ةهجو IDP ىلج دوجومل نيوكتلل احيصت ب مق
show saml فيرعت تانايب جارخا يف SP/أية مالح راج فيرعت تانايب يف حضوم وه امك عقومل
<tunnel-group-name>.

SAML نيوكت تاريخي غت نايرس مدع 6: ةلكشمل

حشال

saml identity-provider <idp-
entity-id> رمال ةلازا حرتقي، WebVPN نمض SAML نيوكت عم لي دعت يا دعب
قفنل ةعومجم نمض هتفاضل ةداعاو <idp-
entity-id>.

الحل

قفنل ةعومجم تحت هتفاضل ةداعاو <idp-
entity-id> saml identity-provider رمال ةلازاب مق

تافي صوت نمض ايلخاد ني درشمل س فن مادختسا ةيفيك 7: ةلكشمل
ةددعتم قافنا ةعومجم/الاصتات

حشال

عبتا، ةددعتم قافنا ةعومجم ل هس فن IdP SSO قيبطت مادختسا SAML ةقداصم نيوكتل
هاندأ نيوكتل تاوطخ

لحل

تارادصل او 7.0 FMC/FTD وأ FDM Managed FTD وأ، مدقأل تارادصل او 9.16 ASA ل 1 رايل
مدقأل:

- قفن لاصتات/ةعومجم فيرعت فلم لكل دحاو، IdP ىلج ةلص فنم SSO تارادصل عاشنإ
- IDP لبق نم مدختسمل يضارتفال CN مادختساب CSR عاشنإ مق

- جي.جراخ/ي.لخاد ق.دصم ع.جرم نم CSR ع.قوت
- اهم ادخستسا متيس يتل تاقي ببطتال ىلع ةعقومال ةيولهال ةداهش سفن تي بشتب مق ل.لاصتا فيرعت تافلم وأ ةلصفنم قافنأ تاعومجمل

دعب اميفو 7.1 FTD/FMC وأ دعب اميفو 9.17.1 ASA ل 2 رايخل

- فيرعت فلم لكل قي ببطت عقاوب، IdP ىلع ةلصفنم SSO تاقي ببطت عاشنإ قافنأ ةعومجمل/لاصتا
- FTD وأ ASA ىلع اهلي محتو قي ببطت لك نم تاداهشال لي زنت
- ةعومجمل لكل فيرعت فلم لكل IdP قي ببطت عم قفاوتي يذال TrustPoint نيي عتت مق ل.لاصتا/قفن

فيرعت فلم دادرتسا في ةلكشم ببسب ةقداصملا تلشف 8: ةلكشملا يداحألا لوخدلا ليحست طابترا

حرشلا

كلذ في امب، ةددعتم بابسأل لي ماعلا زاهج ىلع Secure Client جم انرب ىلع كلذ ةظحالم نكميو رصالحالا لاثملا لي بس ىلع

- جذوم نلل يلاحلا تقولا ديكاتال ةي حالص زواجتت ال
- حيحص ريغ لكشب ديكاتال لك لهتسملا ةمدخل URL ناو نع وأ ناياكل فرعم فيرعت مت ىلع IDP.

لحل

- ةددجم عا طخأ نع ثحباو FW ىلع عا طخألا حيحصت لي غشتب مق
- ىلع هنيوكت مت يذال ديكاتال لك لهتسملا ةمدخل URL ناو نع و ناياكل فرعم نم ققحت FW نم اهيلع لوصالحا مت يتل فيرعتل تانايب لباقم IDP.

ةئزجتال قباطت مدع ليحرت ةلاح 9: ةلكشملا

تاريست

- دروملا ىلى ىرخأ ةرم مدختسملل IdP هي جوت ةداعإ نم ضرغل RelayState ةملعمل مدخت RelayState تامولعم قباطت نأ بجي. ةحجانل SAML ةقداصم دعب بولطملا ي لصلأا ةقداصملا بلطل URL ناو نع ةياهن في RelayState تامولعم عم ديكاتال ىلع
- تاريغتل لبسب اضيا ثدحي نأ نكمي نكلو MitM موجه ىلع ارشؤم اذه نوكي نأ نكمي IdP بناج ىلع RelayState

ءا طخألا حيحصت لاثم

[SAML] relay-state hash mismatch.

الحل

- Cisco نم ءاطخأل احيحصت فرع م ي ف لصف م وه امك تباث رادصإ ىلإ لاقتنال [CSCwf85757](#)
- RelayState تامولعم رييغت ب IdP مايق مدع نم ققحت

اهحالصإو ءاطخأل افاشكتسا نم ديزملا

جارخإل عم قبس م لكشب اھحالصإو SAML ءاطخأ افاشكتسا تايلمع مظعم ءارجا نكمي امن ي ب نأ نكمي تاقوا كانه نأ ال، vpn بيولا ةكبشب ءاطخأ احيحصت نم طقف جتانل تالكشملا يدحا ببس ديدحت ي ف ءديفم ءافاضإل ءاطخأل احيحصت تايلمع اهي ف نوكت

<#root>

firepower#

debug webvpn saml 255

firepower#

debug webvpn 255

firepower#

debug webvpn session 255

firepower#

debug webvpn request 255

ةلص تاذا تامولعم

- [Cisco نم تاليزنت لاوي نفل م عدلإ](#)
- [ASA نيوكت ةلدأ](#)
- [FMC/FDM نيوكت ةلدأ](#)

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