ةدحولا ىلع SSL ريفشت كف نيوكت ةرادإ) ASDM مادختساب FirePOWER ةيطمنلا (عبرملا لخاد

تايوتحملا

<u>ةمدقملا</u> <u>ةيساسألا تابلطتملا</u> <u>تابلطتملا</u> <u>ةمدختسملا تانوكملا</u> <u>ةىساساً تامولعم</u> <u>رداصلا SSL رىفشت كف</u> <u>دراولا SSL رىفشت كف</u> <u>SSL رىڧشت كڧ نىوكت</u> <u>(ةلاقتسالا - ريفشتلا كف) رداصلا SSL ريفشت كف</u> <u>. CA ةداەش نيوكتب مق .1 ةوطخلا</u> <u>. SSL جەن نىرەكتب مق .2 ةوطخلا</u> <u>لوصولا يف مكحتاا ةسايس نيوكت .3 ةوطخاا</u> <u>(فورعم - رىفش تلا كف) دراولا SSL رىفش ت كف</u> <u>مداخلا جاتفمو ةداەش داريتسا 1. ةوطخلا</u>. <u>(یرایتخا) CA ةداهش داریتسا .2 ةوطخلا).</u> <u>. SSL جەن نىوكتب مق .3 ةوطخلا</u> <u>لوصولا يف مكحتا ا ةسايس نيوكت .4 ةوطخاا.</u> <u>ةحصلا نم ققحتلا</u> <u>اهحالصاو ءاطخألا فاشكتسا</u> <u>ةلص تاذ تامولعم</u>

ەمدقملا

ةدحولا ىلع (SSL) ةنمآلاا ليصوتلا ذخآم ةقبط ريفشت كف نيوكت دنتسملا اذه فصي (عبرملا ةراداٍ) ASDM مادختساب FirePOWER ةيطمنلا

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- لباقلا نامألا ةزهجأ ريدم) ASDM و (ASA) فيكتلل لباقلا نامألا زاهج ةيامح رادج ةفرعم ِ (فيكتلل
- FirePOWER نامأ زاهج ةفرعم •
- HTTPS/SSL لوكوتورب ةفرغم •

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست

- اتادحول من ا تادحول ASA FirePOWER (ASA 5506X/5506H-X/5506W-X، ASA 5508-X، ASA د ASA ي المن ا تادحول ا ا
- أي المناه المحمن المحمن المعني المعني المحمن المعني المحمن المحمن المحمن المحمن المحمن المحمن المحمن المحمد ا المحمد المحمد

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألاا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ةرشابم كتكبش.

هدحو نأ نم دكأت :**ةظحالم** sirePOWER مذه نيوكتل Protect صيخرت ىلع يوتحت FirePOWER قدحو نأ نم دكأت : ح**نيوكتلا** ىلإ لقتنا ،صيخرتلا نم ققحتلل .ةفيظولا > ASA FirePOWER Configuration > License.

ةيساسأ تامولعم

متي يتلا ةرداصلاو ةدراولا SSL تالاصتإ ريفشت كفب Firepower ةيطمنلا ةدحولا موقت متي ،رورملا ةكرح ريفشت كف درجمب .تالاصتالا هذه صحف كلذكو ،اهيلإ اههيجوت ةداعإ .اهيف مكحتلاو كلذ ىلإ امو Facebook ىلع ةشدردلا لثم ةيقفنلا تاقيبطتلا فاشتكا رظح وأ URL ةيفصت وأ تاديدهتلا نع اثحب اهريفشت كف مت يتلا تانايبلا صحف متي رطح وأ URL ةيفصل التي الايبلا م

رداصلا SSL ريڧشت كڧ

قيطمنلا ةدحولا لمعت FirePOWER ميطنع قرداصلا SSL تالاصتا ميجوت قداعا ليكوك FirePOWER قيطمنلا قدحولا لمعت مدختسملا ديري يذلا عقوملل قدامش ءاشنا قداعاو قرداصلا SSL تابلط ضارتعا قدامش نكت مل اذا عيقوتلا قيتاذ FirePOWER قدامش يه (CA) قردصملا قطلسلا .مترايز نيزختلا قركاذ ىلا امتفاضا متت مل اذا وأ دوجوم يلكيه لسلست نم اءزج FirePOWER عقوم ىلا ضارعتسالا ءانثأ اريذحت ليمعلا ملتسي ،ليمعلاب صاخلا ضرعتسمللا تقوملا .رداصل SSL ريفش لي مادختسا متي .نم

دراولا SSL ريڧشت كڧ

نم ةخسن داريتساب لوؤسملا موقي ،زاهج وأ يلخاد بيو مداخ ىلإ ةدراولا رورملا ةكرح ةلاح يف ،ةيطمنلا FirePOWER قدحو ىلع SSL مداخ قداهش ليمحت دنع .حاتفملاو يمحملا مداخلا قداهش ريفشت كفب كلذ دعب زاهجلا موقي ،قدراولا رورملا ةكرحل SSL ريفشت كف قسايس نيوكتو فاشتكاب ةيطمنلا قدحولا موقت مث نمو .رورملا قكرح هيجوت قداعإ ءانثأ اهصحفو رورملا قكرح ،كلذ ىلع قوالع .قنمآلا قانقلا هذه ربع ققفدتملا قراضلا جماربلاو تاديدهتاو تايوتحملا متي

SSL ريڧشت كڧ نيوكت

.SSL رورم ةكرح ريفشت كفل ناتقيرط كانه

- ةرداصلا SSL رورم ةكرحل اهتلاقتسإ ميدقت ريفشتلا كف •
- ةدراولا SSL رورم ةكرحل فورعم ريفشتلا كف •

(ةلاقتسالا - ريفشتلا كف) رداصلا SSL ريفشت كف

ةدحو لمعت SSL مداوخل SSL تاضوافم يأل (ليخدلا) MITM ةدحوك FirePOWER قدحو لمعت ةيطمنلا ةدحولا يلع اهنيوكت مت يتلا ةطيسولا CA قداهش عم ماعلا مداخلا قداهش FirePOWER.

رداصلا SSL ريفشت كف نيوكتل ثالثلا تاوطخلا يه هذه.

.CA ةداەش نيوكتب مق .1 ةوطخلا

ةداهشلا ةلاقتسال ةطيسو ةقث قدصم عجرم ةداهش وأ ايتاذ ةعقوم ةداهش امإ نيوكتب مق.

ايتاذ ةعقوملا CA ةداەش نيوكت

CSR ءاشنا ىلع رقنا مث .ةيلخادلا CA ةداەش ءاشنال **عيقوتلا يتاذ CA ءاشنا** ىلع رقنا .ەعيقوتل CA مداخ عم يلاتلاب ەتكراشم متت يذلا ةداەشلا عيقوت بلط ءاشنال

ةطيسولا CA ةداەش نيوكت

ASA < نيوكت ىلإ لقتنا ،رخآ قدصم عجرم لبق نم ةعقوملا ةطيسولا CA ةداهش نيوكتل

. CA د**اريتسإ** ىلع رقناو **يلخاد PKI > CAs نئاكلا ةرادإ < CA**

ةداەشلا ىوتحم خسن وأ يلحملا زاەجلا نم ةداەشلا ليمحتو **ضارعتساٍ** ددح .ةداەشلا مسا ددح فلم ضارعتساب امإ مق ،ةداەشلل صاخلا حاتفملا ديدحتل .**ةداەشلا تانايب** رايخ يف **حاتفمل**ا رايخ يف حاتفملا خسنب مق وأ حاتفملا.

ىلع رقنا **.رورملا ةملك ددحو** رايتخالاا ةناخ **ريفشت** نيكمتب مق ،حاتفملا ريفشت مت اذإ ةروصلا يف حضوم وه امك ،ةداهشلا ىوتحم ظفحل **قفاوم:**

| Configuration > ASA FirePOWE | R Configuration > Object Management > PKI > Internal CAs | |
|---|--|-----------|
| ASA FirePOWER Configuration 🗉 | | |
| Network | Generate CA | Import CA |
| Dort Port | | <u> </u> |
| Security Zones | Import Internal Certificate Authority | ? × |
| | Name: Intermediate-CA | |
| Variable Set | Certificate Data or, choose a file: Browse | |
| ····································· | CBMCS0ExEjAQBgNVBAcTCUJBTkdBTE9SRTEOMAwGA1UEChMFQ0ITQ08xDDAKBgNV BAsTA1RBQzEaMBgGA1UEAxMRQ0Euc2VydmVydGVzdC5jb20xIzAhBgkqhkiG9w0B CQEWFGFkbWluQHNlcnZlcnRlc3QuY29tggkA9OflOUfXIF0wDAYDVR0TBAUwAwEB /zANBgkqhkiG9w0BAQUFAAOBgQCXQME24zt0sKTzghQI5HuNWQl7NQlK3ZS5juVF | ^ |
| PKI Internal CAs Trusted CAs External Certs | YY24BJinUUiW5mCAlD1KSyG+Jx26QlbWRs4vwfl8Fq3Dct0kRg74QpOzZS8l83F9 kuIpr+e7T+QifHbG4AzF5b2WGF4HUCxXjYTKtVHwbLuNeED5cAB38jL7Vso0cvg2 Biat1w== END CERTIFICATE | |
| | Key or, choose a file: Browse | |
| Internal Cert Groups Evternal Cert Groups III | i/DnuBs9S3UgPnN3xShcwMTg8N+1yWOTJnfIpar/0LpW4Eqn5izAEAcTzNmA4gR/ 3XMIL1RbCFUpUyL9D2N+4TuZzHrbmUa6QA1qPNwLcf0Vf1wgVyagZYYAn5oA50wA K554gAeIvYJC5dEXe9974K9nh7/hNG5B53S3gKuGGvQx+0DSilZy0J0RPzRnQmew cNsbTQ3TGcdt6p58cJFsTWYZayvvQCbeJHOgNcGOUcfdlZ2/v6IoVC0wp+61KgZ7 | - |
| Device Setup | jIgYPD5KzjJ5AX9BRKFXbsSAFJ3bSZ9Ztx/jFlvaMdjEUqqctEPP69Fav6zSdTDo wFkMModFPeSBol7WLTjKujyRLM0/p7DsM41Wdn4x1J2j2k+E9AWoXw+kGF9PwNBQ | |
| Firewall | 22WYRn92UiZWTKySdU0Mr4mDRVBkzb+Iqb30D7/S7ENWFpuktxWOQA==END RSA PRIVATE KEY | |
| Remote Access VPN | Encounted and the pressured is: | |
| Site-to-Site VPN | | |
| ASA FirePOWER Configuration | ОК | Cancel |

.SSL جەن نيوكتب مق .2 ةوطخلا

كف ةقيرط قيبطت متي يتلا رورملا ةكرح ددحيو ريفشتلا كف ءارجإ SSL جهن ددحي تابلطتم ىلإ ادانتسا ةددعتملا SSL دعاوق نيوكتب مق .اهيلع ةضاعتسالا-ريفشتلا .ةسسؤملا نامأ جەنو لـمعلا

ةسايس نيوكتل SSL، الس**ايسلا > ASA FirePOWER Configuration > نيوكتل > SSL**. SSL **مدعاق ةفاضإ** قوف رقناو

ةدعاقلا مسا ددح **:مسالا**.

مت يتلا ةلدسنملا ةمئاقلا نم CA ةداهش رتخاو **ليقتسأ - ريفشت كفك** ءارجإلا ددح **:ءارجإلاا** ةقباسلا ةوطخلا يف اهنيوكت.

،ةقطنملا) ةددعتم تارايخ دوجول ارظن رورملا ةكرح ةقباطمل ةدعاقلا يف طورشلا ديدحتب مق اهريفشت كف مزلي يتلاا رورملا ةكرح ديدحتل ةددحم ،(خلاٍ ،نيمدختسملا ،ةكبشلا.

:ةروصلا يف حضوم وه امك ،**لوخدلا** ليجست رايخ نيكمتب مق ،SSL ريفشت كف ثادحاً ءاشنإل

| O O ASA FirePOWER Configurat | ○ ○ ○ ○ Configuration > | ASA FirePOWER C | nfiguration > | Policies > S | <u>SL</u> | | | | | | |
|------------------------------|-------------------------|--------------------|---------------|--------------|---------------|----------|-------------|--------------|--------------|------------------------------------|------------|
| V Dolicies | | | | | | _ | | | _ | | |
| Access Control Policy | Default SSL Po | olicy | | | | | | | | | |
| Intrusion Policy | | Jiney | | | | | | | | | |
| 🖻 Files | SSL Policy | | | | | | | | | | |
| 🔒 SSL | | | | | | | | | | | |
| 🔯 Actions Alerts | | | | | | | | | | | |
| & Identity Policy | Rules Trusted CA Ce | rtificates Undecry | table Actions | | | | | | | | |
| DNS Policy | L | | | | | | | 0 | <u> </u> | Count Dates | |
| 🕨 📕 Device Management | | | | | | | | Add Catego | ry 😳 Add Rul | e Search Rules | X |
| 🕨 🧒 Object Management | Laura 1 | | | | | | | | | | |
| 🕨 🏠 Local | Add Rule | | | | | | | | | | ? X |
| 🔄 System Information | | | | | | | | | | | |
| 📑 Updates | Name Outboound_SSI | Decrypt | | | Enabled | d | Ir | into Categor | γ | Standard Rules | ~ |
| 🔛 Licenses | Action G Decrypt - R | esian 🔽 w | ith ServerCA | | | | V & 🗆 F | teplace Key | | | |
| 🕨 🧰 Tools | | | | | | | | | | | |
| 🕨 🍇 Integration | Zones Network | s Users Applica | ions Ports | Category | Certificate | DN | Cert Status | Cipher Suite | Version | | Logging |
| | Available Networks | | 0 | | Source Netw | orks (1) | | | Destination | Networks (0) | |
| | Caserth bu some and | - | | | | | | | | | |
| | Search by hame or v | alue | | | Private Ne | etworks | | | dily | | |
| | Networks | Geolocati | on | | | | | | | | |
| | Private Networks | | | | | | | | | | |
| | | | | Add to | | | | | | | |
| | | | | Source | | | | | | | |
| | | | | Add to | | | | | | | |
| | | | De | estination | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| A Device Setup | | | | | Enter an IP a | ddress | | Add | Enter an IP | address | Add |
| Firewall | | | | | | | | | | Add | Cancel |
| Remote Access VPN | | | | | | | | | | | |
| | | | | | | | | | | | |
| Site-to-Site VPN | | | | | | | | | | | |
| ASA FirePOWER Configur | | | | | | | | | No data | a to display 🔣 🔇 Page 1 | of 1 🔉 🔊 🖒 |

.SSL ةدعاق ةفاضإل **ةفاضإ** قوف رقنا

.SSL جەن نيوكت ظفحل **ASA ل FirePOWER تارىيغت نيزخت** قوف رقنا

لوصولا يف مكحتلا ةسايس نيوكت .3 ةوطخلا

جەن نيوكت درجمب SSL "لوصولا يف مكحتلا" يف SSL جەن ديدحت بجي ،ةبسانملا دعاوقلاب. تارييغتلا ذيفنتل.

نيوكتل ا الماني العن العن العن الموصول ا يف مكحتل ا مايس نيوكتل ASA Firepower Configuration > الوصول ا يف مكحتل ا < تاسايسل.

ددح .SSL جەن دادع**ا < مدقتم** ىلإ لاقتنالا وأ SSL جەن نم **ءيش ال** قوف رقنلاب موقت نأ امإ قروصلا يف حضوم وہ امك ،اەظفحل **قفاوم قوف رقناو ةلدسنملا ةمئاقلا نم SSL ةسايس**:

| O O ASA FirePOWER Configurat | O O O Configuration > ASA FirePOWER Configuration > Policies > Access | Control |
|------------------------------|---|---------|
| ▼ | | |
| Access Control Policy | ASA ASA FirePOWER | |
| ▶ 💿 Intrusion Policy | | _ |
| Files | Default Allow All Traffic | |
| 🔒 SSL | | |
| 🔋 Actions Alerts | Enter a description | |
| 💄 Identity Policy | | |
| DNS Policy | | |
| 🕨 📕 Device Management | | |
| 🕨 🧑 Object Management | | |
| 🕨 🏠 Local | Identity Policy: None SSL Policy: None | |
| 🔄 System Information | | |
| 📑 Updates | Rules Security Intelligence HTTP Responses Advanced | |
| Licenses | General Settings | Ø |
| Tools | | |
| 🕨 🍡 Integration | Maximum URL characters to store in connection events | 1024 |
| | Allow an Interactive Block to bypass blocking for (seconds) | 600 |
| | | Ves |
| | sonnections | 103 |
| | Inspect | Yes |
| | Default SSL Policy | |
| | | |
| | Identit Revert to Defaults OK Cancel | None |
| | SSL Policy Settings | Ø |
| | SSL Policy to use for inspecting encrypted connections | None |
| | | |

جەن نيوكت ظفحل ASA FirePOWER تارىيغت نيزخت رقنا SSL.

نأ ىلإ ةراشإ كانه ،جەنلا قيبطت لبق .رعشتسملا ىلإ لوصولا يف مكحتلا جەن رشن بجي ىلع اەۋارچا مت يتلا تارييغتلا رشنل .ةيطمنلا ةدحولا ىلع **ميدق لوصولا يف مكحتلا جەن** تارييغتلا نم ققحت .**FirePOWER تارييغت رشن رايخ** ددحو **رشن** قوف رقنا ،راعشتسالا ةادأ .ر**شن** قوف رقناو اەۋارچا مت يتلا

ىلع لوصولا ةسايس قيبطت ىلإ ةجاحب تنك اذإ ،5.4.x رادصإلا يف :**قظحالم** مارييغت قيبطت قوف رقنا ،رعشتسمل

موقت مث **.ةمەملا ةلاح < ASA FirePOWER ةبقارم < ةبقارملا** ىلا لقتنا :**ةظحالم** ةمەملا لامكا نامضل نيوكتلا تارىيغت قىبطتب.

(فورعم - ريفشتلا كف) دراولا SSL ريفشت كف

ةكرح ريفشت كفل (ريفشتلا كف فورعملا) دراولا SSL ريفشت كف بولسأ مادختسا متي داريتسا ىل جاتحت .اەل صاخلا حاتفملاو مداخلا ةداەش نيوكتب تمق يتلا ةدراولا SSL رورم SSL رورم ةكرح لصت امدنع .FirePOWER ةيطمنلا ةدحولا ىل صاخلا حاتفملاو مداخلا ةداەش ىلع صحفلا ءارچاب موقتو رورملا ةكرح ريفشت كفت اەنإف ،ةيطمنلا اتومنلا اتحو ىل قداع با اور مان الارمان الارمان الارمان الارمان الارمان الارمان الارمان الارمان الارمان قدر وىل الارمان الارم الارمان مالارمان الارمان الالارمان الارمان الارمان الارمان الارمان الارمان الارمان ال رداصلا SSL ريفشت كف نيوكتل عبرألاا تاوطخلا يه هذه:

مداخلا حاتفمو ةداەش داريتسإ .1 ةوطخلا.

ق**رادا < ASA Firepower Configuration < نيوكتلا** ىلإ لقتنا ،حاتفملاو مداخلا ةداەش داريتسال قوف رقناو **ةيلخادا تاداەشلا < PKI < نئاكلا**.

نم ةداهشلا ديدحتل **حفصت** ددحت نأ امإ .ةداهشلا مسا نييعتب مق ،ةروصلا يف حضوم وه امك حاتفملا ديدحتل .**صيخرتلا تانايب** يف ةداهشلا ىوتحم خسنب موقت نأ وأ يلحملا زاهجلا رايخلا **حاتفم** يف حاتفملا خسنب مق وأ حاتفملا فلم ضارعتساب امإ مق ،ةداهشلل صاخلا

امك ،رورملا ةملك ددحو **ةرفشم** رايتخالاا ةناخ نيكمتب مق ذئدنعف ،حاتفملا ريفشت مت اذإ ةروصلا يف حضوم وه:

| 🔿 🔘 🔿 ASA FirePOWER Configurat | O O Configuration > ASA FirePOWER Configuration > Object Management > PKI > Internal Certs |
|--------------------------------|--|
| Application Filters | |
| ► WWW URL | Add Internal Cert |
| 😡 GeoLocation | |
| 🌯 Variable Set | Na Add Known Internal Certificate ? X |
| SecurityIntelligence | |
| Sinkhole | Name: web.servertest.com |
| 📝 FileList | |
| 🌼 Cipher Suite List | Certificate Data or, choose a file: Browse |
| 🕨 🍯 Distinguished Name | nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA0ucjKK9ofSyrAbYkSKC/nvy2g7Mj |
| 🔻 🔦 РКІ | RHbV0UEK+2a5u5fDvZIRURHHBEbFp+SV0E7ak7PljdXd/sB4nhvvfPe4FN65IurN |
| 😝 Internal CAs | mjzYywUy4zi8uSzOr/9YhNJoz/212dvR4uZ1PA9AQqXvyeCCL/OCQmFQOrP6+qbk +EPHI f9wEy8abaECAwE&AT&NBakabkiC9w0B&OsE&&OBaOCuk7VPuTaiJeui9rtE |
| 🖶 Trusted CAs | Lrcyns+lrbHTJhge0Z2HC/XJmYwyJXhBuEqvU9qx+GhQ99jNCOlo0iPIGF1naqBt |
| 🖶 External Certs | FtI7ohmI/F544x75fm17t3XwfZF/VA2GhG3W3QGFKHCA0U7CBaU78jCVBa9CTKOG |
| 😁 Internal Certs | u8ceNnyAxU/MogAXNuecqLw88w== |
| 👶 Internal CA Groups | |
| 🚜 Trusted CA Groups | |
| 🐥 Internal Cert Group: | Key or, choose a file: Browse |
| 👶 External Cert Group | BEGIN RSA PRIVATE KEY |
| 🕨 🏠 Local | MIICXAIBAAKBgQDS5yMor2h9LKsBtiRIoL+e/LaDsyNEdtXRQQr7Zrm7l8O9khFR |
| 🔄 System Information | 0mjP/YjZ29Hi5nU8D0BCpe/J4IIv84JCYVA6s/r6puT4U8ct/3AXEGCGkQIDAQAB |
| 📑 Updates | AoGBAJ+XOAu5cCAIhP6ujZZHzbjJEnNmQvGz2uiVh3HlsfY6SWxR87ic8zRROZBq |
| 🔛 Licenses | <pre>cnniwc4cmu8Q/c0wc2vzHi462zhEqrQ0EeBr04BzBHwL20FwergZnsna2s0bdsJ9 +nzFlwx4LamXR8N88YbkvC3n4iVY5z90fsvCd12LloAGBXN4BAkEA+nkDe1LloIxOz</pre> |
| 🔻 💼 Tools | Pgmzad68lngk4/7Wbg8ibZz0Mv2PSvO7pNbhRfpy/dtgGLJvIGJIr/+0iL2SrPFv |
| 🗑 Backup Restore | d7QmDkGwyQJBANeOlVWWjBPuFCLQjYL04c66km9vzGgLDHjGc4gOING1iFlCrQt1 |
| Cebadulina | Encrypted, and the password is: |
| | |
| A Device Setup | |
| | |
| | |

.ةداەشلا ىوتحم ظفحل **نيزختلل FirePOWER تارىيغت** ىلع رقنا

(يرايتخإ) CA ةداەش داريتسإ .2 ةوطخلا.

داريتسإ ىلإ جاتحت ،رذجلا وأ ةطيسولا ةيلخادلا CA ةداەش لبق نم ةعقوملا مداخلا ةداەشل ،داريتسالا ذيفنت دعب Firepower قيطمنلا ةدحولا ىلإ CA تاداەشل ةيلخادلا ةلسلسلا مداخلا ةداەش نم ققحتلا ىلع ةرداق Firepower قيطمنلا ةدحولا حبصت.

نى ال الق تنا ،CA ةداەش داريت سال ASA Firepower Configuration > ال الق تنا ،CA قراد CA من ال حال من ال >CA من ا قداەش قفاضإل **ەب قوثوم CA قفاض ا**قوف رقناو **ەب قوثوم**

.SSL جەن نيوكتب مق .3 ةوطخلا

كفل فورعملا بولسألا نيوكت يف بغرت يتلا مداخلا ليصافتو ءارجإلاا SSL جهن ددحي SSL دعاوق نيوكتب مقف ،ةددعتم ةيلخاد مداوخ كيدل ناك اذا اهل ةدراولا رورملا ةكرح ريفشت . اهعم لماعتت يتلا تانايبلا رورم ةكرحو ةفلتخم مداوخ ىلإ ادانتسا ةددعتم

ةسايس نيوكتل SSL، القتنا SSL، **نيوكتل > ASA FirePOWER Configuration > تاسايسلا >** SSL **ةدعاق ةفاضإ** قوف رقناو

ةدعاقلا مسا ددح **:مسالا**.

يتلا ةلدسنملا ةمئاقلا نم CA ةداهش رتخاو **فورعم - ريفشتلا كف** مساب ءارجإلا ددح **:ءارجإلا** ةقباسلا ةوطخلا يف اهنيوكت مت.

،قيبطتلا، ،ةكبشلا) تارايخلا نم ديدعلا دوجول ارظن ،دعاوقلا هذه ةقباطمل طرشلا ددح يتلا مداخلاب ةصاخلا مامتهالل ةريثملا تانايبلا رورم ةكرح ديدحتل ةددحملا (خلإ ،ذفانملا **يف ددحم ةقث قدصم** يف يلخادلا قدصملا عجرملا ددح .اهل SSL ريفشت كف نيكمت ديرت مالع

ل**وخدلا ليجست** رايخ نيكمتب مق ،SSL ريفشت كف ثادحأ ءاشنإل.

| ○ ○ ○ ASA FirePOWER Configurat | ○ ○ ○ ○ Configuration > | ASA FirePOWER Confi | guration > Policies | > <u>SSL</u> | | | |
|--------------------------------|-------------------------|------------------------|---------------------|---------------------|-------------------------|------------------------|------------|
| V Policies | | | | | | | |
| Access Control Policy | Default SSL Po | licy | | | | | |
| S Intrusion Policy | SSL Policy | | | | | | |
| Pule Editor | | | | | | | |
| Files | | | | | | | |
| | Bulas Trustad CA Cor | tificator Undecryptab | la Actions | | | | |
| X Actions Alerts | Rules Trusted CA Cer | tilicates officeryptab | le Actions | | 2 | | |
| 🔔 Identity Policy | Add Rule | | | | | | ? × |
| DNS Policy | | | | | | | |
| 🕨 📑 Device Management | Name Web_Server_Decr | rypt | | Enabled | Insert below r | ule 💙 : | 1 |
| 🔻 🈡 Object Management | Action Decrypt - Know | wo Koy | web convertest com | | Edit | | |
| Network | Decivit - Kilo | will Key | web.servertest.com | | | | |
| Port Security Zenes | Zones Networks | Users Applications | Ports Category | Certificate DN | Cert Status Cipher Suit | e Version | Logging |
| Application Filters | Available Networks | | @ | Source Networks (C |))) | Destination Networks | (1) |
| ► WARE | Search by name or val | 114 | | | •) | = 102 168 10 E/22 | |
| GeoLocation | Search by name of van | | | any | | 2192.108.10.3/32 | |
| 🤏 Variable Set | Networks | Geolocation | | | | | |
| SecurityIntelligence | Private Networks | | | | | | |
| Sinkhole | | | Add to | | | | |
| FileList | | | | | | | |
| Cipher Suite List | | | Add to | | | | |
| Distinguished Name | | | | | | | |
| PKI Internal CAs | | | | | | | |
| Trusted CAs | | | | | | | |
| External Certs | | | | | | | |
| | | | | Enter an IP address | | dd Enter an IP address | Add |
| A Device Setup | | | | L | | | |
| | | | | | | | Add Cancel |

.SSL ةدعاق ةفاضإل **ةفاضإ** قوف رقنا

.SSL جەن نيوكت ظفحل Store ASA FirePOWER تارىيغت قوف رقنا مث

لوصولا يف مكحتلا ةسايس نيوكت .4 ةوطخلا.

جەن نيوكت درجمب SSL "لوصولا يف مكحتلا" يف SSL جەن ديدحت بجي ،ةبسانملا دعاوقلاب. تارىيغتلا ذيفنتل.

نيوكتل ا المان > ASA Firepower Configuration > المان الم

امإ **SSL، جەن دادعا < ةمدقتم تارايخ** ىلا لقتنا وأ **SSL ةسايس** راوجب **الب** رايخلا قوف رقنت نأ امإ. اەظفحل **قفاوم** قوف رقناو ةلدسنملا ةمئاقلا نم SSL ةسايس ددجو.

.SSL جەن نيوكت ظفحل ASA FirePOWER تارىيغت نيزخت رقنا

جەن نأ ىلإ ةراشإ ةدەاشم كنكمي ،جەنلا قيبطت لبق .لوصولاب مكحتلا جەن رشن بجي

ةادأ ىلع اهؤارجإ مت يتلا تارييغتلا رشنل .ةيطمنلا ةدحولا ىلع ميدق لوصولا يف مكحتلا تارييغتلا نم ققحت .FirePOWE<mark>R تارييغت رايخ رشن</mark> رتخاو **رشن** قوف رقنا ،راعشتسالا قثبنملا راطإلا يف **رشن قوف رقناو اهؤارجإ مت يتلا**

ىلع لوصولاا ةسايس قيبطت ىلإ ةجاحب تنك اذإ ،5.4.x رادصإلا يف :**ةظحالم** مارييغت قيبطت قوف رقنا ،رعشتسملا

موقت مث **.ةمەملا ةلاح < ASA FirePOWER ةبقارم < ةبقارملا** ىلإ لقتنا :**ةظحالم** .قمەملا لامكإ نامضل نيوكتلا تارىيغت قىبطتب

ةحصلا نم ققحتلا

حيحص لكشب نيوكتلا لمع ديكأتل مسقلا اذه مدختسا.

• بلطي ،ةيلخادلا ةكبشلا نم ماع SSL بيو عقوم ضارعتسإ درجمب ،رداصلا SSL لاصتال عجرملا تامولعم نم ققحتو ةداهشلا ىوتحم نم ققحت .ةداهشلا نم أطخ ةلاسر ماظنلا ةيطمنلا قدحولا يف اهنيوكتب تمق يتلا ةيلخادلا CA ةداهش رهظت .قدصملا مق ،أطخلا ةلاسر بنجتل .SSL قداهش ضارعتسال أطخلا قلاسر لوبق .FirePOWER مق ،أطخلا قداهش قفاضإب

| ficate Viewer:"www.cisc | o.com" |
|-------------------------|--|
| neral <u>D</u> etails | |
| Could not verify this c | ertificate because the issuer is unknown. |
| Issued To | |
| Common Name (CN) | www.cisco.com |
| Organization (O) | Cisco Systems |
| Organizational Unit (Ol | J) ATS |
| Serial Number | 14:5E:8D:FB:06:DA:C6:55 |
| Issued By | |
| Common Name (CN) | serverCA.example.com |
| Organization (O) | TAC |
| Organizational Unit (Ol | J) TAC |
| Period of Validity | |
| Begins On | Thursday, January 28, 2016 |
| Expires On | Monday, January 29, 2018 |
| Fingerprints | |
| SHA-256 Fingerprint | 6C:66:D8:0E:52:5D:9D:D8:74:2F:A6:92:7F:31:E7:39: |
| SHA-250 Hingerphilic | |

.رورملا ةكرح ىلع دمتعت يتلا SSL ةدعاقو SSL جەن نم ققحتلل لاصتالا ثادحاً نم ققحت •

اثدح ددج **.يلعفلا تقولا يف حيحصت < ASA FirePOWER ةبقارم < <mark>ةبقارملا</mark> ىلإ لقتنا ريفشت كف تايئاصحإ نم ققحت .ليصافتلا ضرع** قوف رقناو

| | A FirePOWER Events Connecti | on Intrusion File Malwa | re File Security Intelligence | | | |
|--------|---|---------------------------|------------------------------------|--------------------------------|-------------------------|-----------------------------|
| ilter | Connection Event Allo ASA FirePOWER firewall connec Reason: | DW tion event | | Time: Wed 6/7/16 6: | 29:10 AM (IST) to | Wed 6/7/16 6:29:11 AM (IST) |
| 🕨 Re | Event Details | | | | | |
| Receiv | Initiator | | Responder | | Traffic | |
| 6/7/16 | Initiator IP | 192.168.20.50 🥖 | Responder IP | 72.163.10.10 🥖 | Ingress Security | not available |
| 6/7/16 | Initiator Country and Continent | not available | Responder Country and Continent | not available | Zone Egress Security | not available |
| 0,7,10 | Source Port/ICMP Type | 56715 | Destination Port/ICMP | 443 | Zone | te et de |
| 6/7/16 | User | Special Identities/No | LIPI | | Egross Interface | Inside |
| | | Authentication Required | | https://cisco-tags.cisco.com / | TCP Flags | 0 |
| 6/7/16 | Transaction | | URL Category | not available | NetBIOS Domain | not available |
| CITUC | Initiator Packets | 4.0 | UKL Reputation | | Netbros Domain | not ortanolo |
| 6///16 | Responder Packets | 9.0 | HTTP Response | U | DNS | |
| 6/7/16 | Total Packets | 13.0 | Application | | DNS Query | not available |
| 0,7,10 | Initiator Bytes | 752.0 | Application | HTTPS | Sinkhole | not available |
| 6/7/16 | Responder Bytes | 7486.0 | Application Categories | network protocols/services | View more | |
| | Connection Bytes | 8238.0 | Application Tag | opens port | | |
| 6/7/16 | | | Client Application | SSL client | SSL | |
| | Policy | | Client Version | not available | SSL Status | Decrypt (Resign) |
| 6/7/16 | Policy | Default Allow All Traffic | Client Categories | web browser | SSL Policy | Default SSL Policy |
| | Firewall Policy Rule/SI | Intrusion_detection | Client Tag | SSL protocol | SSL Rule | Outboound_SSL_Decrypt |
| 6/7/16 | Category | | Web Application | Cisco | SSL Version | TLSv1.0 |
| 6/7/16 | Monitor Rules | not available | Web App Categories | web services provider | SSL Cipher Suite | TLS_DHE_RSA_WITH_AES_256_CB |
| 0/7/10 | ISE Attributes | | Web App Tag | SSL protocol | SSI Certificate | Valid |
| 6/7/16 | End Point Profile Name | not available | Application Risk | Medium | Status | Talla |
| | | | Application Business | Medium | SSI Flow Error | Success |

- حاجنب "لوصولاب مكحتلا جەن" رشن لامتكا نم دكأت.
- لوصولا يف مكحتلا جهن يف SSL ةسايس نيمضت نم دكأت.
- رداصلاو دراولا هاجتالل ةبسانملا دعاوقلا ىلع يوتحي SSL جەن نأ نم دكأت.
- .ةديفملا رورملا ةكرح ديدحتل بسانملا طرشلا ىلع يوتحت SSL دعاوق نأ نم دكأت.
- جەن نم ققحتال لاصتالا ثادحأ قبقارم SSL.
- .SSL ريڧشت كڧ ةلاح نم ققحت •

اهحالصإو ءاطخألا فاشكتسا

نيوكتلا اذهل اهحالصإو ءاطخألا فاشكتسال ةددحم تامولعم أَيلاح رفوتت ال.

ةلص تاذ تامولعم

- <u>Cisco Systems - تادنتسملاو ينقتلا معدلا</u>

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما