

ةدحوللا ىلع SSL ريفشت ك ف نيوكت ةرادا ASDM مادختساب FirePOWER ةيطمنلا (عبرملا لخاد)

تايوتحمل

[ةمدقملا](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[ةمدختسملا تانوكملا](#)

[ةيساسأ تامولعم](#)

[رداصللا SSL ريفشت ك ف](#)

[دراولا SSL ريفشت ك ف](#)

[SSL ريفشت ك ف نيوكت](#)

[\(ةلاقسالا - ريفشتلا ك ف\) رداصللا SSL ريفشت ك ف](#)

[CA. ةداهش نيوكتب مق. 1. ةوطخلا](#)

[SSL. جهن نيوكتب مق. 2. ةوطخلا](#)

[لوصوللا يف مكحتلا ةسايس نيوكت. 3. ةوطخلا](#)

[\(فورعم - ريفشتلا ك ف\) دراولا SSL ريفشت ك ف](#)

[مداخلالات فمو ةداهش داريتسا. 1. ةوطخلا](#)

[\(يرايخا\) CA ةداهش داريتسا. 2. ةوطخلا](#)

[SSL. جهن نيوكتب مق. 3. ةوطخلا](#)

[لوصوللا يف مكحتلا ةسايس نيوكت. 4. ةوطخلا](#)

[قحصللا نم ققحتلا](#)

[اهجالص او ءاطخألا فاشكتسا](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

ةدحوللا ىلع (SSL) ةنمألا ليصوتلا ذخأم ةقبط ريفشت ك ف نيوكت دننتمسلا اذه فصوي
(عبرملا ةرادا) ASDM مادختساب FirePOWER ةيطمنلا.

ةيساسألا تابلطتملا

تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كيديل نوكت ناب Cisco يصوص:

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

- رداصل ال SSL رورم ة كرحل اهتلاق تساميدقت - ريفشتلا ك ف
- ة دراوال SSL رورم ة كرحل فورعم - ريفشتلا ك ف

ة لاق تسالال - ريفشتلا ك ف) رداصل ال SSL ريفشت ك ف

ملتسي . ةماع ال SSL مداوخل SSL تاضوافم يأل (لليخدلا) MITM ةدحوك FirePOWER ةدحو لمعت ةيطمنل ةدحو لا يلع اهنويوكت مت يتلل ةطيسولل CA ةداهش عم ماع ال مداوخل ةداهش FirePOWER.

رداصل ال SSL ريفشت ك ف نيويوكتل ثالثل تاوطلال يه هذه

CA ةداهش نيويوكتب مق 1. ةوطلال

ةداهش ال ة لاق تسالال ةطيسو ةوكت ق دصم عجرم ةداهش وأ ايتاذ ةعقوم ةداهش ام نيويوكتب مق

ايتاذ ةعقوم ال CA ةداهش نيويوكت

راد | > ASA Firepower Configuration > نيويوكتل ال ل لقتنا ، ايتاذ ةعقوم ال CA ةداهش نيويوكتل عجرم ال ةداهش ليصافات ماظنل بلطي . CA ءاشن | يلع رقناو ةديلخدل PKI > CAs > نئال ال ك. تابلطتم بسح ليصافات ال الما ، ةروصلال ي ف حضوم وه امك . ق دصم ال

The screenshot shows the ASA FirePOWER Configuration interface. The left sidebar displays the 'Object Management' tree with 'Internal CAs' selected under 'PKI'. The main window shows the 'Generate Internal Certificate Authority' dialog box with the following fields:

- Name: ServerCA
- Country Name (two-letter code): IN
- State or Province: KA
- Locality or City: Bangalore
- Organization: TAC
- Organizational Unit (Department): TAC
- Common Name: serverCA.example.com

Buttons at the bottom include 'Generate CSR', 'Generate self-signed CA', and 'Cancel'. The background shows the configuration tree and a 'No data to display' message.

CSR ءاشن | يلع رقنا م ث . ةديلخدل CA ةداهش ءاشن | عيقوتل ايتاذ CA ءاشن | يلع رقنا ءاشن | عيقوتل CA مداوخل عم يلاتلاب هتكراشم مت يذل ةداهش ال عيقوت بلط ءاشن |

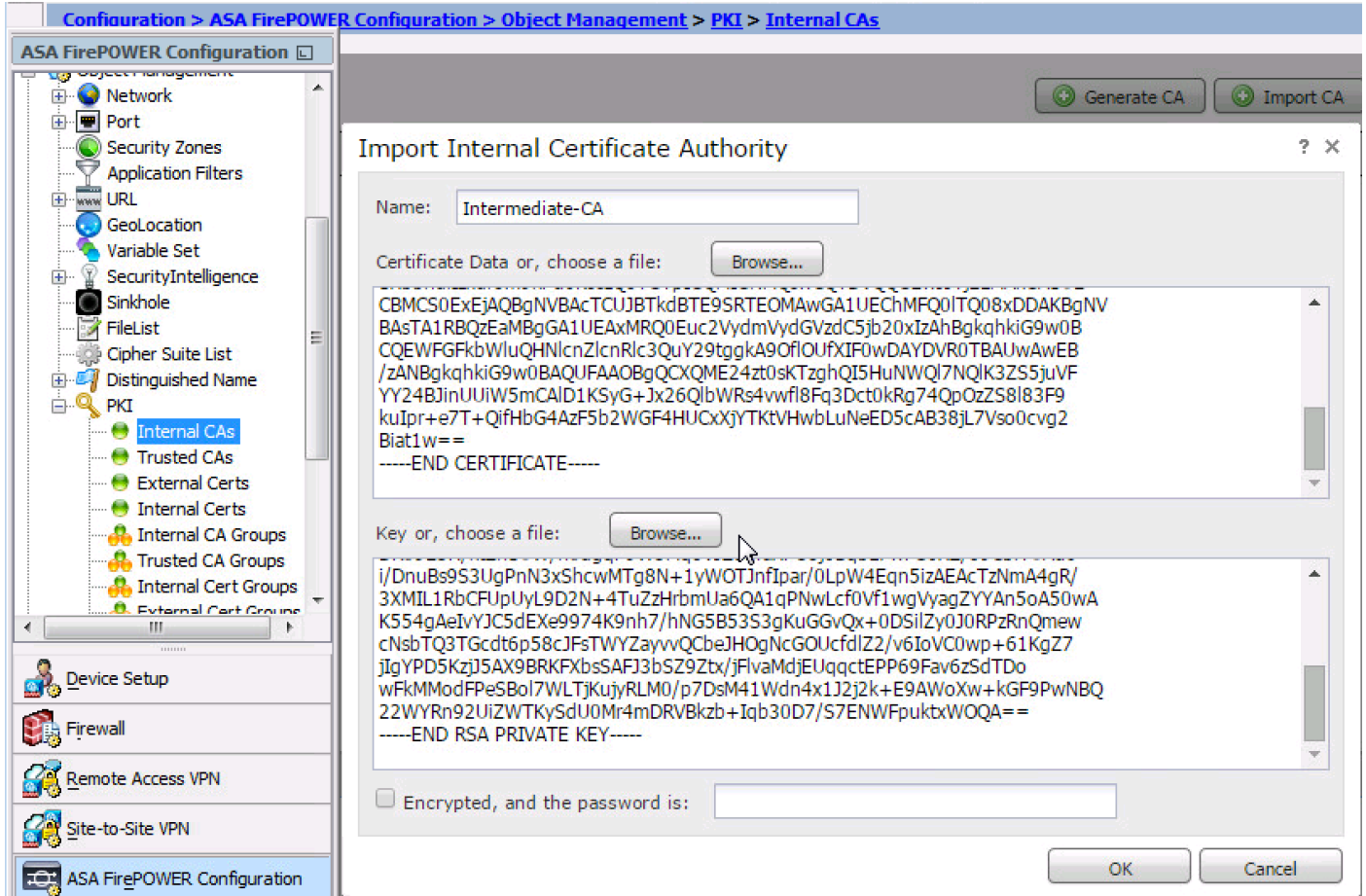
ةطيسولل CA ةداهش نيويوكت

ASA > نيويوكتل ال ل لقتنا ، رخآ ق دصم عجرم لبق نم ةعقوم ال ةطيسولل CA ةداهش نيويوكتل

CA داري تسي لى لى رى قى ن او ي لى خاد CAs > PKI > نئىلك لى اءاردا > Firepower Configuration

ءءاهش لى لى و تى ح م خ س ن و ا ي لى ح م لى ز ا ه ج لى ن م ءءاهش لى لى م ح ت و ض ا ر ع ت س لى د د ح . ءءاهش لى م س ا د د ح ف ل م ض ا ر ع ت س ا ب ا م ا م ق ، ءءاهش لى لى ص ا خ لى ح ا ت ف م لى د ي د ح ت ل . ءءاهش لى ت ا ن ا ي ب ر ا ي خ ي ف ح ا ت ف م لى ر ا ي خ ي ف ح ا ت ف م لى خ س ن ب م ق و ا ح ا ت ف م لى .

لى لى ر ق ن ا . ر و ر م لى ء م ل ك د د ح و ر ا ي ت خ ا ل ا ء ن ا خ ر ي ف ف ش ت ن ي ك م ت ب م ق ، ح ا ت ف م لى ر ي ف ف ش ت م ت ا ذ ا ء ر و و ص ل لى ي ف ح و م و ه ا م ك ، ءءاهش لى لى و تى ح م ط ف ح ل ق ف ا و م :



SSL ءه ن ن ي و ك ت ب م ق 2 ء و ط خ ل ا

ك ف ء ق ي ر ط ق ي ب ط ت م ت ي ي ت ل ا ر و ر م ل ا ء ك ر ح د د ح و ر ي ف ف ش ت ل ا ك ف ا ر ج لى SSL ءه ن د د ح ي ت ا ب ل ط ت م لى ا د ا ن ت س ا ء ء ء ع ت م ل ا SSL ء ع ا و ق ن ي و ك ت ب م ق . ا ه ي لى ء ض ا ع ت س ا ل ا ر ي ف ف ش ت ل ا ء س س و م ل ا ن ا م ا ءه ن و ل م ل ا

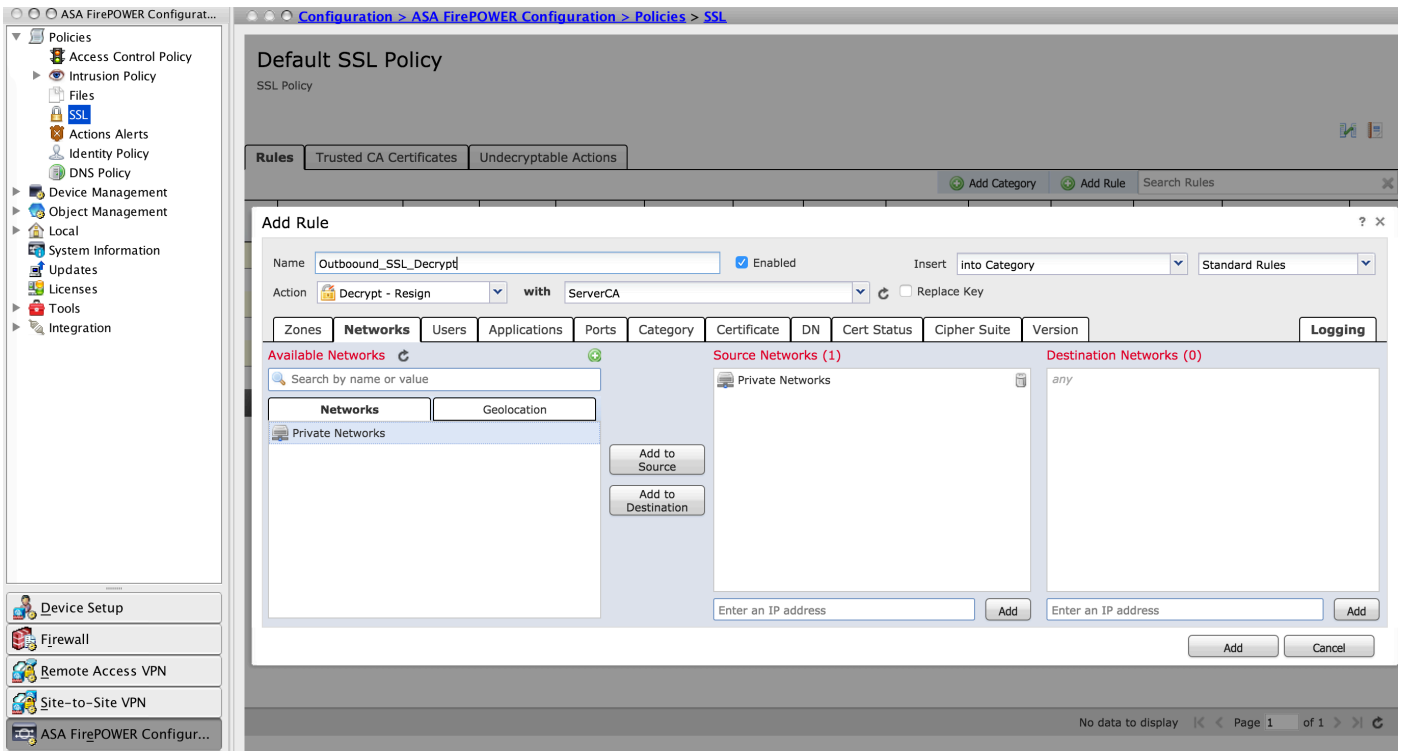
> ت ا س ا ي س ل ل ا > ASA FirePOWER Configuration > ن ي و ك ت ل لى لى لى ق ت ن ا ، SSL ء س ا ي س ن ي و ك ت ل ء ء ع ا ق ء ف ا ض لى ق و ف ر ق ن ا و SSL .

ءءء ا ق ل م س ا د د ح : م س ا ل ا .

م ت ي ت ل ا ء ل ء س ن م ل ا ء م ئ ا ق ل لى ن م CA ءءاهش ر ن خ ا و لى ق ت س ا - ر ي ف ف ش ت ك ف ك ا ر ج ل ا د د ح : ا ر ج ل ا ء . ء ق ب ا س ل ل ا ء و ط خ ل ا ي ف ا ه ن ي و ك ت .

ء ق ط ن م ل ا ، ء ء ء ع ت م ت ا ر ا ي خ ء و ج و ل ا ر ط ن ر و ر م ل ا ء ك ر ح ء ق ب ا ط م ل ء ء ع ا ق ل لى ي ف ط و ر ش ل لى د ي د ح ت ب م ق . ا ه ر ي ف ف ش ت ك ف م ز ل ي ي ت ل ا ر و ر م ل ا ء ك ر ح د ي د ح ت ل ء ء ء م ، (خ ل) ، ن ي م ء خ ت س م ل ا ، ء ك ب ش ل ل ا .

ء ر و و ص ل لى ي ف ح و م و ه ا م ك ، ل و خ ء ل لى ء س ت ر ا ي خ ن ي ك م ت ب م ق ، SSL ر ي ف ف ش ت ك ف ش ا ء ح ا ء ا ش ن ل ا



SSL. ةدعاق ةفاضل ةفاضل قوف رقنا

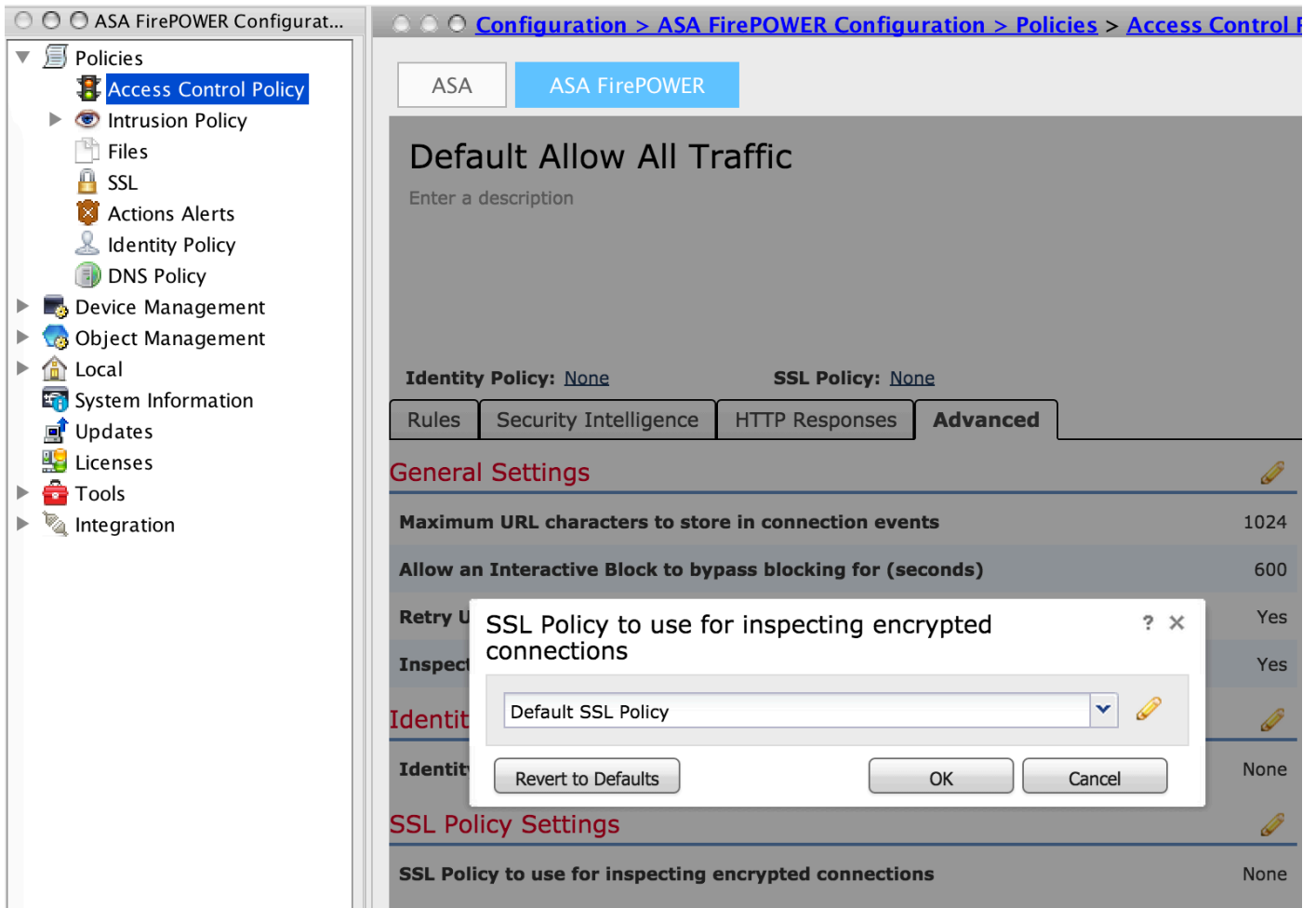
SSL. جهن نيوكت ظفحل ASA ج FirePOWER تاريغت نيخت قوف رقنا

لوصول في مكحتل ةسايس نيوكت. 3 ةوطخل

"لوصول في مكحتل" في SSL جهن ديدحت بجي، ةبسانم لدع او قلاب SSL جهن نيوكت درجم بتاريغتال ذيفنتل.

ASA Firepower Configuration > نيوكتال للاقنتنا، لوصول في مكحتل ةسايس نيوكتال لوصول في مكحتل > تاسايسال.

دح. SSL جهن دادع | > مدقتم للاقنتنال و SSL جهن نم عيش ال قوف رقنلاب موقت نأ ام | ةروصل في حضورم وه امك، اهظحل قفاوم قوف رقناو ةلدسنم ل ةمئاقال نم SSL ةسايس:



SSL جهن ني وكت ظفحل ASA FirePOWER تاريغت ني زخت رقنا

نأ إلى قرأش إكانه، جهنلا قي ببط لبق. رعشت سمل إلى لوصول في مكحتلا جهن رشن بجي
 إلى اهؤارج متي تاريغتلا رشنل. ةيظمنلا ةدحول إلى ع مي دق لوصول في مكحتلا جهن
 تاريغتلا نم ققحت. FirePOWER تاريغت رشن راخي دحو رشن قوف رقنا، راعشت سالا ةادا
 رشن قوف رقنا واهؤارج متي تاريغتلا

إلى لوصول ةسايس قي ببط إلى ةجاحب تنك اذا، 5.4.x رادصل إلى في: ةظحال م
 ASA FirePOWER تاريغت قي ببط قوف رقنا، رعشت سمل

موقت م. ةمهمل ةلاح > ASA FirePOWER ةبقارم > ةبقارملا إلى لقتنا: ةظحال م
 ةمهمل لامك إ نامضل ني وكتلا تاريغت قي ببط

فورعم - ريفشتلا كف) دراو ال SSL ريفشت كف

ةكرح ريفشت كفل (ريفشتلا كف فورعمل) دراو ال SSL ريفشت كف بولسأ مادختسا متي
 داريتسا إلى جاتحت. اهل صاخلا حاتفملا و مدخالل ةداهش ني وكتب تمق يتلا ةدراو ال SSL رورم
 SSL رورم ةكرح لصت ام دنع. FirePOWER ةيظمنلا ةدحول إلى صاخلا حاتفملا و مدخالل ةداهش
 إلى صخفلا ءارجاب موقت و رورملا ةكرح ريفشت كفت اهنا ف، ةيظمنلا FirePOWER ةدحو إلى
 ةداعاب Firepower ةيظمنلا ةدحول موقت، صخفلا دعب. اهري فشت كفت متي تاريغتلا رورملا ةكرح
 مداخل إلى اهل اسرا و رورملا ةكرح ريفشت

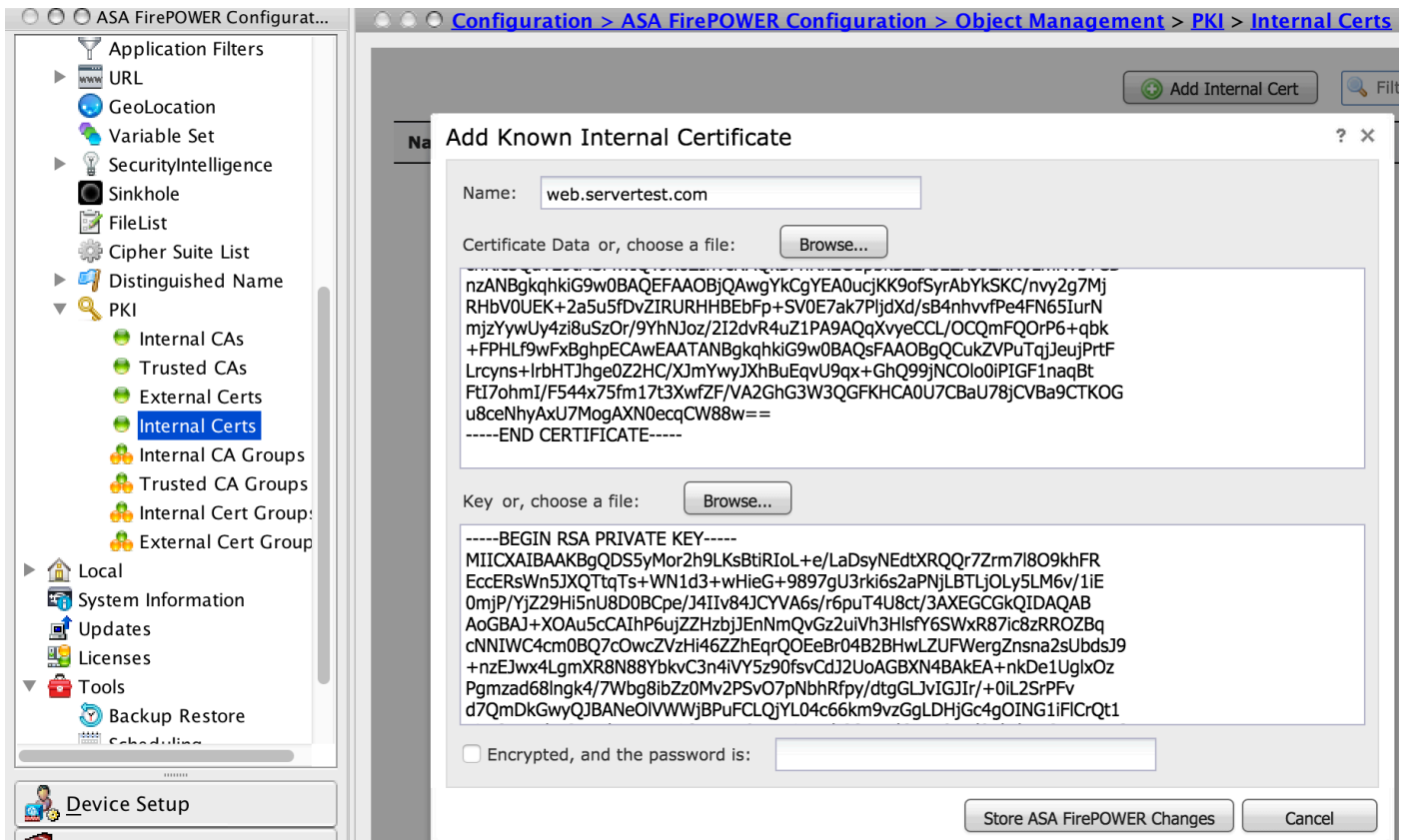
رداصل ال SSL ري فشت ك ف نيوكتل ع برأل تاوطلخ ال يه هه

مداخل حاتم و عدهاش داريت سا 1. ووطخل

قراذ > ASA Firepower Configuration > نيوكتل ال ل ل قتنا ، حاتم فملاو مداخل عدهاش داريت سا ال
ةي ل خاد عدهاش ة فاضا قوف ر قناو ةي ل خاد ال تاداهش ال > PKI > نئال ال

نم عدهاش ال دي دحتل ح ف ص ت دحت نأ ام . عدهاش ال مسا ني عت ب مق ، ةروصل ال ي ف ح ص وم وه امك
حاتم فملا دي دحتل . ص ي خرتل ال تانا ي ب ي ف عدهاش ال يوت ح م خ س ن ب موقت نأ و ا ي ل ح م ال زا ه ج ل
راي خ ل حاتم فم ي ف حاتم فم ال خ س ن ب مق و ا حاتم فم ال ف ل م ضارعت سا ب ام مق ، عدهاش ال صاخ ال

امك ، رورم ال ةم لك ددحو ةرف شم راي خ ال ةنا خ ني ك م ت ب مق ذئ دن ع ف ، حاتم فم ال ري فشت م ت ا ذ ا
ةروصل ال ي ف ح ص وم وه



ةدهاش ال يوت ح م ظ ف ح ل ني خ ت ل ل FirePOWER تاري ي غ ت ي ل ع ر قنا

مداخل (ي راي خ ت ا) CA عدهاش داريت سا 2. ووطخل

داريت سا ال ا ج ا ح ت ، ر ذ ج ل و ا ة ط ي س و ل ا ةي ل خ ا د ل ا CA عدهاش ل ب ق ن م ة ع ق و م ل ا م د ا خ ل ا عدهاش ل
داريت سا ال ذ ي ف ن ت د ع ب . Firepower ةي ط م ن ل ا ة د ح و ل ا ال ا CA تاداهش ل ةي ل خ ا د ل ا ة ل س ل س ل ا
م . م د ا خ ل ا عدهاش ن م ق ق ح ت ل ا ال ع ر د ا ق Firepower ةي ط م ن ل ا ة د ح و ل ا ح ب ص ت

CA > نئال ال قراذ > ASA Firepower Configuration > نيوكتل ال ل ل قتنا ، CA عدهاش داريت سا ال
CA . عدهاش ة فاضا ل ه ب ق و ت و م CA ة فاضا قوف ر قناو ه ب ق و ت و م

SSL جهن نيوكتل مق 3. ووطخل

ك ف ل ف و ر ع م ل ا ب و ل س ا ل ا ني و ك ت ي ف ب غ ر ت ي ت ل ا م د ا خ ل ا ل ي ص ا ف ت و ء ا ر ج ا ل ا SSL جهن د د ح ي
SSL د ع ا و ق ني و ك ت ب مق ف ، ة د د ع ت م ةي ل خ ا د م د ا و خ ك ي د ل ن ا ك ا ذ ا . ا ه ل ة د ر ا و ل ر و ر م ل ا ة ك ر ح ري ف ش ت

اهم لماعتت يتل تانايبلا رورم ةكرحو ةفلتخم مداوخ ىل اذانتسا ةددعتم .

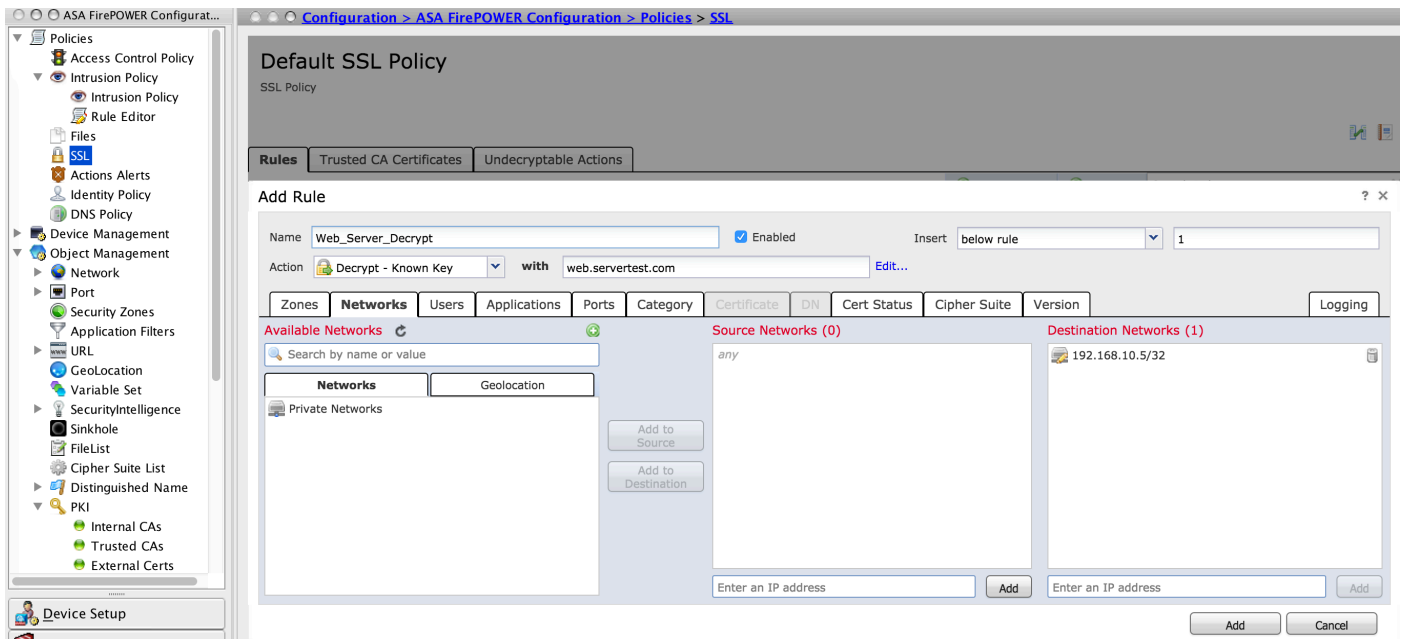
تاسايسلا > ASA FirePOWER Configuration > نيوكتل ىل لقتنا ، SSL ةسايس نيوكتل
ةدعا ةفاضل قوف رقنا و SSL .

ةدعا قلا مسا دح : مسالا .

يتل ةلدسنملا ةمئاقلا نم CA ةداهش رتخاو فورعم - ريفشتلا كف مساب ءارجالا دح : ءارجالا
ةقبا سلا ةوطخلال يف اهنوكت مت

قيبطتلا ، ةكبشلا) تارايلال نم ديدعلا دوجول ارظن ، دعاوقلا هذه ةقبا طمل طرشلال دح
يتل مداخلال ءاصلا ءرئامتهال ءرئامتهال تانايبلا رورم ةكرحو ديدحتلا ءدحملال (خل) ، ذفانملا
يف ددحم ةقت قوصم يف يلخادلا قوصملا ءجرملا دح . اهلا SSL ريفشت كف نيكمت ديرت
هب قوئوملا قوصملا ءجرملا ءداهش بيوت ءمالع

لوخلال ليجست رايخ نيكمتب مق ، SSL ريفشت كف ءادح ءاشنلا



SSL ةدعا ةفاضل قوف رقنا

SSL جهن نيوكت ظفحل ASA FirePOWER Store تاريغت قوف رقنا مئ

لوصلال يف مكحتلا ةسايس نيوكت .4 ةوطخلال

"لوصلال يف مكحتلا" يف SSL جهن ديدحت بجي ، ءبسانملا دعاوقلا اب SSL جهن نيوكت درجم
تاريغتلا ذيفنتل

نيوكتل ىل لقتنا ، لوصلال يف مكحتلا ةسايس نيوكتل > ASA Firepower Configuration >
لوصلال يف مكحتلا > تاسايسلا

SSL جهن دادع > ءمدقتم تارايلال ىل لقتنا و SSL ةسايس راجب ال رايخلال قوف رقنت نأ ام
اهظحل قفاوم قوف رقنا و ءلدسنملا ةمئاقلا نم SSL ةسايس ددحو

SSL جهن نيوكت ظفحل ASA FirePOWER تاريغت نيخت رقنا

جهن نأ ىل ءراش ءداهش كنكمي ، جهنلا قيبطت لبق . لوصلال مكحتلا جهن رشن بجي

ةادأ ىلع اهؤارج مت يتل تاريخيغتلارشنل. ةيظمنلا ةدحوللا ىلع ميديق لوصوللا يف مكحتلا تاريخيغتللا نم ققحت. FirePOWER تاريخيغت راخ رشن رتخا ورشن قوف رقنا، راعشتسالا قثبمنلا راطاللا يف رشن قوف رقنا وهؤارج مت يتلا

ىلع لوصوللا ةسايس قيبطتلا ةجاحب تنك اذا 5.4.x رادصاللا يف: ةظالم ASA FirePOWER تاريخيغت قيبطت قوف رقنا، راعشتسالا

موقت مت. ةمهمللا ةلاح > ASA FirePOWER ةبقارم > ةبقارملا ىللا لقتنا: ةظالم ةمهمللا لامك نامضل نيوكتلا تاريخيغت قيبطت

ةحصللا نم ققحتلا

جحص لكشب نيوكتلا لمع ديكأتل مسقلا اذه مدختسا

- بلطي، ةيلخادلا ةكبشللا نم ماع SSL بيوع قوم ضارعتسا درجمب، رداصلا SSL لاصتال عجرملا تامولعم نم ققحتو ةداهشلا ىوتحم نم ققحت. ةداهشلا نم أطخ ةلاسر ماطنلا ةيظمنلا ةدحوللا يف اهنيوكتب تمق يتلا ةيلخادلا CA ةداهش رهظت. قدصملا مق، أطخللا ةلاسر بنجتل. SSL ةداهش ضارعتسالا أطخللا ةلاسر لوبق. FirePOWER. ضرعتسملا اب اهيلع قدصملا عجرملا ةمئاق ىللا CA ةداهش ةفاضاب

https://www.cisco.com

Search

Certificate Viewer: "www.cisco.com"

General Details

Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	www.cisco.com
Organization (O)	Cisco Systems
Organizational Unit (OU)	ATS
Serial Number	14:5E:8D:FB:06:DA:C6:55

Issued By

Common Name (CN)	serverCA.example.com
Organization (O)	TAC
Organizational Unit (OU)	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: F2:E8:C7:B8:66:02:BC:A4:AF:F1:AB:92:56:B3:03:D7
SHA1 Fingerprint	9B:47:5B:E4:9D:2B:16:0D:FA:63:93:B1:53:F3:2D:6A:13:48:8E:ED

- رورملا ةكرح ىلع دمتعت يتلا SSL ةدعاقو SSL جهن نم ققحتلل لاصتالا شادح نم ققحت

اشرح ددح .يلعفل تقولا يف حيحصت > ASA FirePOWER > ةبقارم > ةبقارملا ىلا لقتنا
 SSL. ريفشت كف تايناصح نم ققحت .لصافتلا ضرع قوف روناو

Monitoring > ASA FirePOWER Monitoring > Real Time Eventing

Real Time Eventing

All ASA FirePOWER Events | Connection | Intrusion | File | Malware File | Security Intelligence

Filter: Connection Event --- Allow Time: Wed 6/7/16 6:29:10 AM (IST) to Wed 6/7/16 6:29:11 AM (IST) Close

Reason: ASA FirePOWER firewall connection event

Event Details

Initiator	Responder	Traffic
Initiator IP: 192.168.20.50	Responder IP: 72.163.10.10	Ingress Security Zone: not available
Initiator Country and Continent: not available	Responder Country and Continent: not available	Egress Security Zone: not available
Source Port/ICMP Type: 56715	Destination Port/ICMP Code: 443	Ingress Interface: inside
User: Special Identities/No Authentication Required	URL: https://cisco-tags.cisco.com	Egress Interface: outside
	URL Category: not available	TCP Flags: 0
	URL Reputation: Risk unknown	NetBIOS Domain: not available
	HTTP Response: 0	
Transaction	Application	DNS
Initiator Packets: 4.0	Application: HTTPS	DNS Query: not available
Responder Packets: 9.0	Application Categories: network protocols/services	Sinkhole: not available
Total Packets: 13.0	Application Tag: opens port	View more
Initiator Bytes: 752.0	Client Application: SSL client	SSL
Responder Bytes: 7486.0	Client Version: not available	SSL Status: Decrypt (Resign)
Connection Bytes: 8238.0	Client Categories: web browser	SSL Policy: Default SSL Policy
	Client Tag: SSL protocol	SSL Rule: Outbound_SSL_Decrypt
	Web Application: Cisco	SSL Version: TLSv1.0
	Web App Categories: web services provider	SSL Cipher Suite: TLS_DHE_RSA_WITH_AES_256_CBC_SHA
	Web App Tag: SSL protocol	SSL Certificate Status: Valid
	Application Risk: Medium	SSL Flow Error: Success
	Application Business: Medium	
Policy		
Policy: Default Allow All Traffic		
Firewall Policy Rule/SI Category: Intrusion_detection		
Monitor Rules: not available		
ISE Attributes		
End Point Profile Name: not available		
Security Group Tag: not available		

- حاجنب "لوصولاب مكحتلال جهن" رشن لامتك نم دكأت .
- لوصولا يف مكحتلال جهن يف SSL ةسايس ني مضت نم دكأت .
- رداصل او دراوالا هاجتال ل ةبسانملا دعاوقلا ىلع يوتحي SSL جهن نأ نم دكأت .
- ةديفملا رورملا ةكرح ديدحتل بسانملا طرشللا ىلع يوتحت SSL دعاوق نأ نم دكأت .
- SSL ةدعاوق SSL جهن نم ققحتلل لاصتالا اذحأ ةبقارم .
- SSL ريفشت كف ةلاح نم ققحت .

اهحالص او ءاطخال فاشكتسا

نويوكتلا اذهل اهلص او ءاطخال فاشكتسال ةددحم تامولعم ايلاح رفوتت ال

ةلص تاذا تامولعم

- [Cisco Systems - تادنتس مل او يبقنقتلا 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 لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل