Contents

Introduction

This document describes the configuration of Secure Sockets Layer (SSL) decryption on the FirePOWER Module using ASDM (On-Box Management).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Knowledge of ASA (Adaptive Security Appliance) firewall, ASDM (Adaptive Security Device Manager)
- Knowledge of FirePOWER appliance
- Knowledge of HTTPS/SSL protocol

Components Used

The information in this document is based on these software and hardware versions:

- ASA FirePOWER modules (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X)

running software version 6.0.0 and above
- ASA FirePOWER module (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) running software version 6.0.0 and above

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

> **Note**: Ensure that FirePOWER Module has a **Protect** license to configure this functionality. To verify the license, navigate to **Configuration > ASA FirePOWER Configuration > License**.

Background Information

Firepower Module decrypts and inspects inbound and outbound SSL connections which are redirected to it. Once the traffic is decrypted, tunneled applications such as facebook chat etc, are detected and controlled. The decrypted data is inspected for threats, URL filtering, file blocking, or malicious data.

Outbound SSL Decryption

The firepower module acts as the forward proxy for outbound SSL connections by intercepting outbound SSL requests and re-generating a certificate for the site which user wants to visit. The issuing authority (CA) is the Firepower Self-Signed certificate. If the firepower's certificate is not part of a hierarchy that exists or if it is not added to a client’s browser cache, the client receives a warning while it browses to a secure site. Decrypt-Resignmethod is used to perform outbound SSL decryption.

Inbound SSL Decryption

In the case of inbound traffic to an internal Web Server or device, the administrator imports a copy of the protected server’s certificate and the key. When the SSL server certificate is loaded on the firepower module, and SSL decryption policy is configured for the inbound traffic, the device then decrypts and inspects the traffic as it forwards the traffic. The module then detects malicious content, threats, malware flowing over this secure channel. Moreover, the Decrypt-Known Keymethod is used to perform inbound SSL decryption.

Configuration for SSL Decryption

There are two methods of SSL traffic decryption.

- Decrypt - Resign for Outbound SSL traffic
- Decrypt - Known for Inbound SSL traffic

Outbound SSL decryption (Decrypt - Resign)

Firepower module acts as MITM (man-in-the-middle) for any SSL negotiations for public SSL servers. It resigns the certificate of the public server with an intermediate CA certificate which is configured on the firepower module.

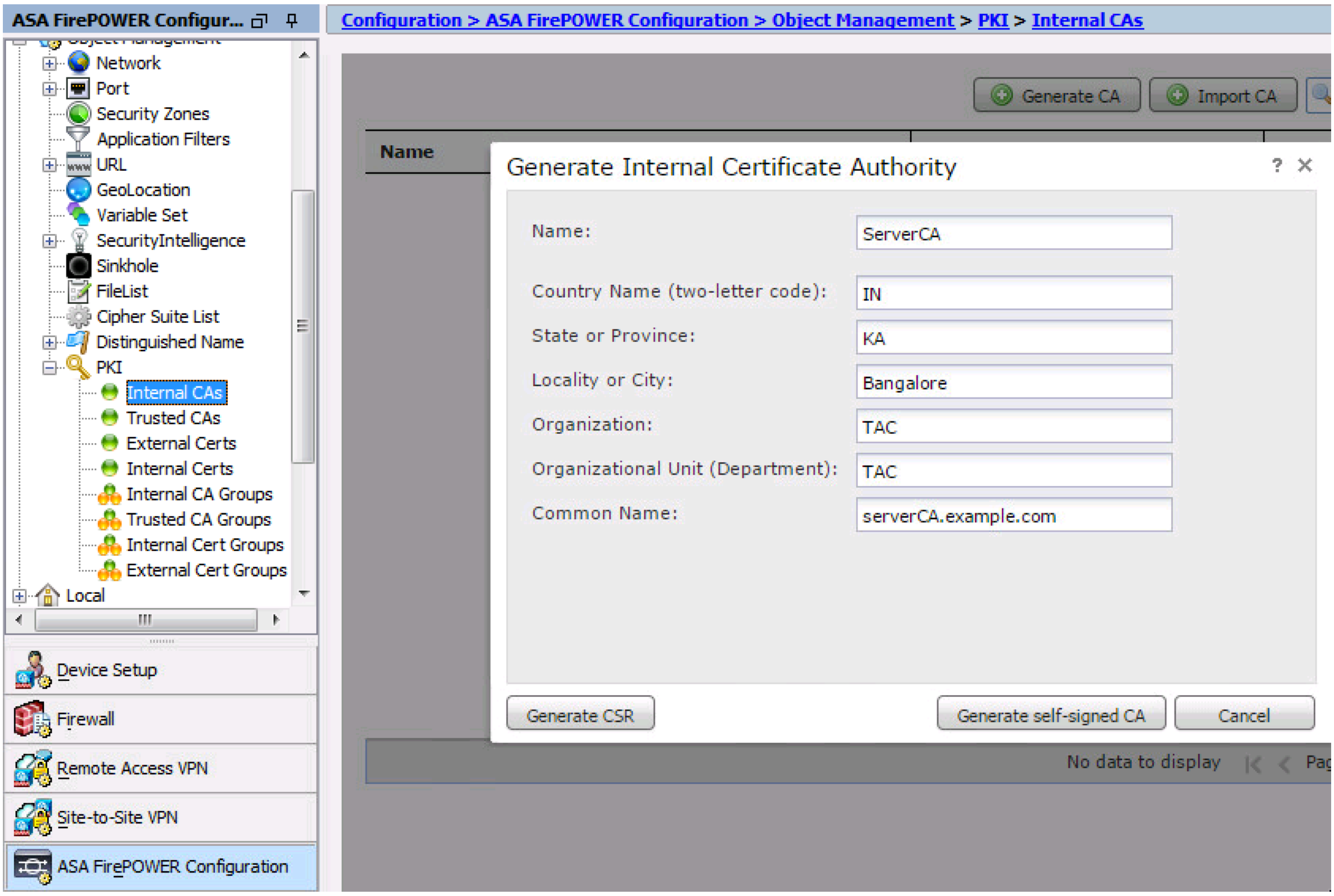
These are the three steps to configure the Outbound SSL Decryption.

Step 1. Configure the CA certificate.

Configure either a self-signed Certificate or an intermediate trusted CA certificate for certificate resign.

Configure the Self-Signed CA Certificate

In order to configure the Self-Signed CA Certificate, navigate to **Configuration > ASA Firepower Configuration > Object Management > PKI > Internal CAs** and click on **Generate CA**. The system prompts for the details of the CA certificate. As shown in the image, fill up the details as per your requirement.



Generate Internal Certificate Authority

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

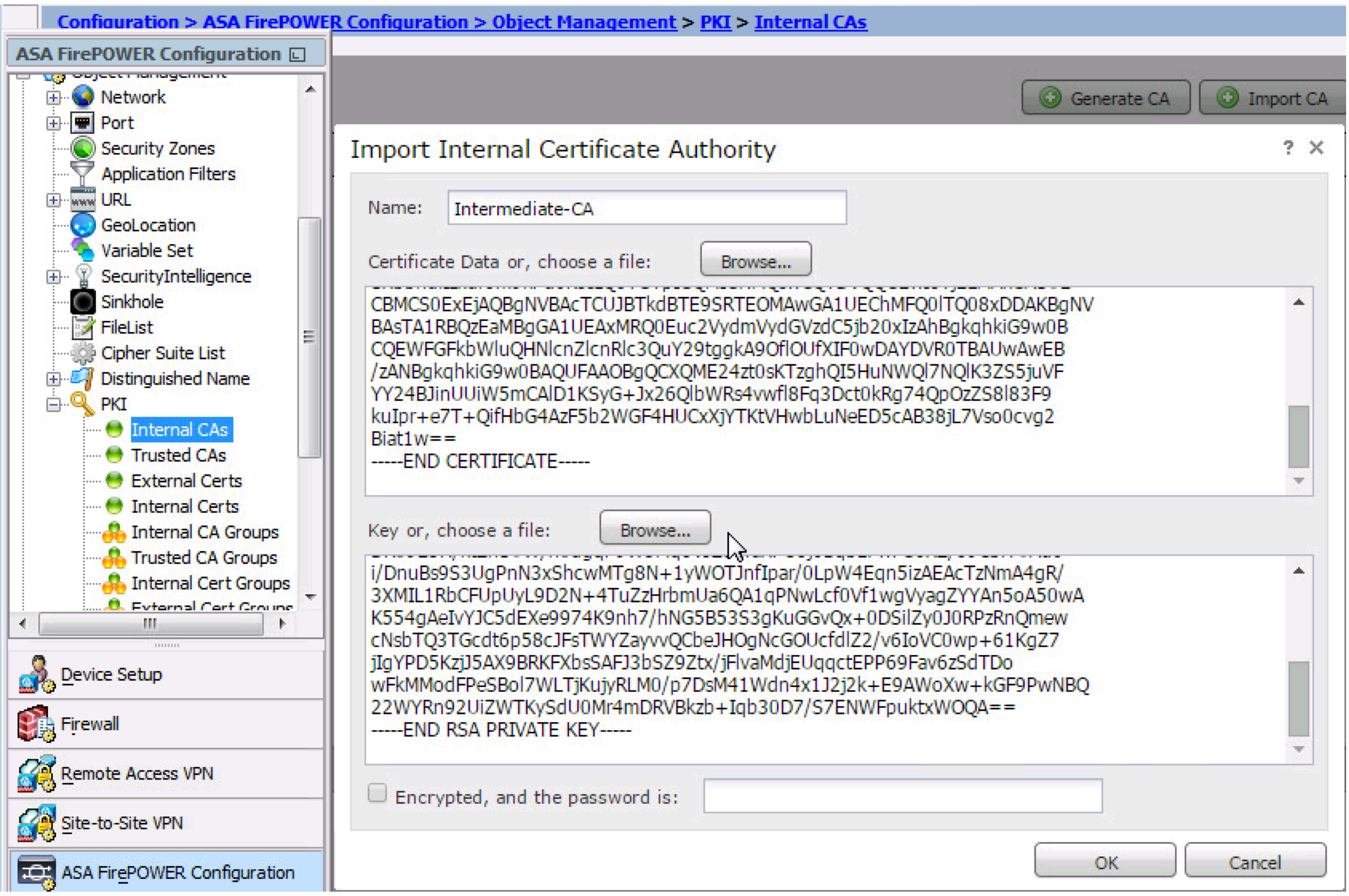
Click on **Generate self-signed CA** to generate the internal CA certificate. Then click on **Generate CSR** to generate the certificate-signing-request which is consequently shared with the CA server to sign.

Configure the Intermediate CA Certificate

In order to configure the Intermediate CA Certificate which is signed by another third party CA, navigate to **Configuration > ASA Firepower Configuration > Object Management > PKI > Internal CAs** and click on **Import**.

Specify the Nameof the Certificate. Select **browse** and upload the certificate from the local machine or copy-paste the content of the certificate in the **Certificate Data** option. In order to specify the private key of the certificate, either browse the key file or copy-paste the key in the **Key** option.

If the key is encrypted, enable the check-box **Encrypted** and specify the password. Click **OK** to save the certificate content, as shown in the image:



Name: Intermediate-CA

Certificate Data or, choose a file:

```
CBMCS0ExEjAQBgNVBAcTCUJBTkdBTE9SRTEOMAwGA1UEChMFQ0lTQ08xDDAKBgNV
BAsTA1RBQzEaMBgGA1UEAxMRQ0Euc2VydmVydGVzdC5jb20xIzAhBgkqhkiG9w0B
CQEWFGFkbWluQHNlcnZlcnRlc3QuY29tggkA9OflOUfXIF0wDAYDVR0TBAUwAwEB
/zANBgkqhkiG9w0BAQUFAAOBgQCXQME24zt0sKTzghQI5HuNWQl7NQlK3ZS5juVF
YY24BJinUUiW5mCAlD1KSyG+Jx26QlbWRs4vwfl8Fq3Dct0kRg74QpOzZS8l83F9
kuIpr+e7T+QifHbG4AzF5b2WGF4HUCxXjYTKtVHwbLuNeED5cAB38jL7Vso0cvg2
Biat1w==
-----END CERTIFICATE-----
```

Key or, choose a file:

```
i/DnuBs9S3UgPnN3xShcwMTg8N+1yWOTJnfIpar/0LpW4Eqn5izAEAcTzNmA4gR/
3XMIL1RbCFUpUyL9D2N+4TuZzHrbmUa6QA1qPNwLcf0Vf1wgVyagZYYAn5oA50wA
K554gAeIvYJC5dEXe9974K9nh7/hNG5B53S3gKuGGvQx+0DSilZy0J0RPzRnQmew
cNsbTQ3TGcdt6p58cJFsTWYZayvvQCbeJHOgNcGOUcfdlZ2/v6IoVC0wp+61KgZ7
jIgYPD5KzjJ5AX9BRKFXbsSAFJ3bSZ9Ztx/jFlvaMdjEUqqctEPP69Fav6zSdTDo
wFkMModFPeSBol7WLTjKujyRLM0/p7DsM41Wdn4x1J2j2k+E9AWoXw+kGF9PwNBQ
22WYRn92UiZWTKySdU0Mr4mDRVBkzb+Iqb30D7/S7ENWFpuktxWOQA==
-----END RSA PRIVATE KEY-----
```

□ Encrypted, and the password is:

Step 2. Configure the SSL Policy.

SSL policy defines the decryption action and identifies the traffic on which Decrypt-Resign method of decryption is applied. Configure the multiple SSL rules based on your business requirement and organization security policy.

In order to configure the SSL policy, navigate to **Configure > ASA FirePOWER Configuration > Policies > SSL** and click **Add Rule**.

Name: Specify the name of the rule.

Action: Specify the action as **Decrypt - Resign** and choose the CA certificate from the drop-down list which is configured in the previous step.

Define conditions in the rule to match traffic as t

To generate the events of SSL decryption, enable the loggingat **logging** option, as shown in the image:

Click **Add** to add the SSL rule.

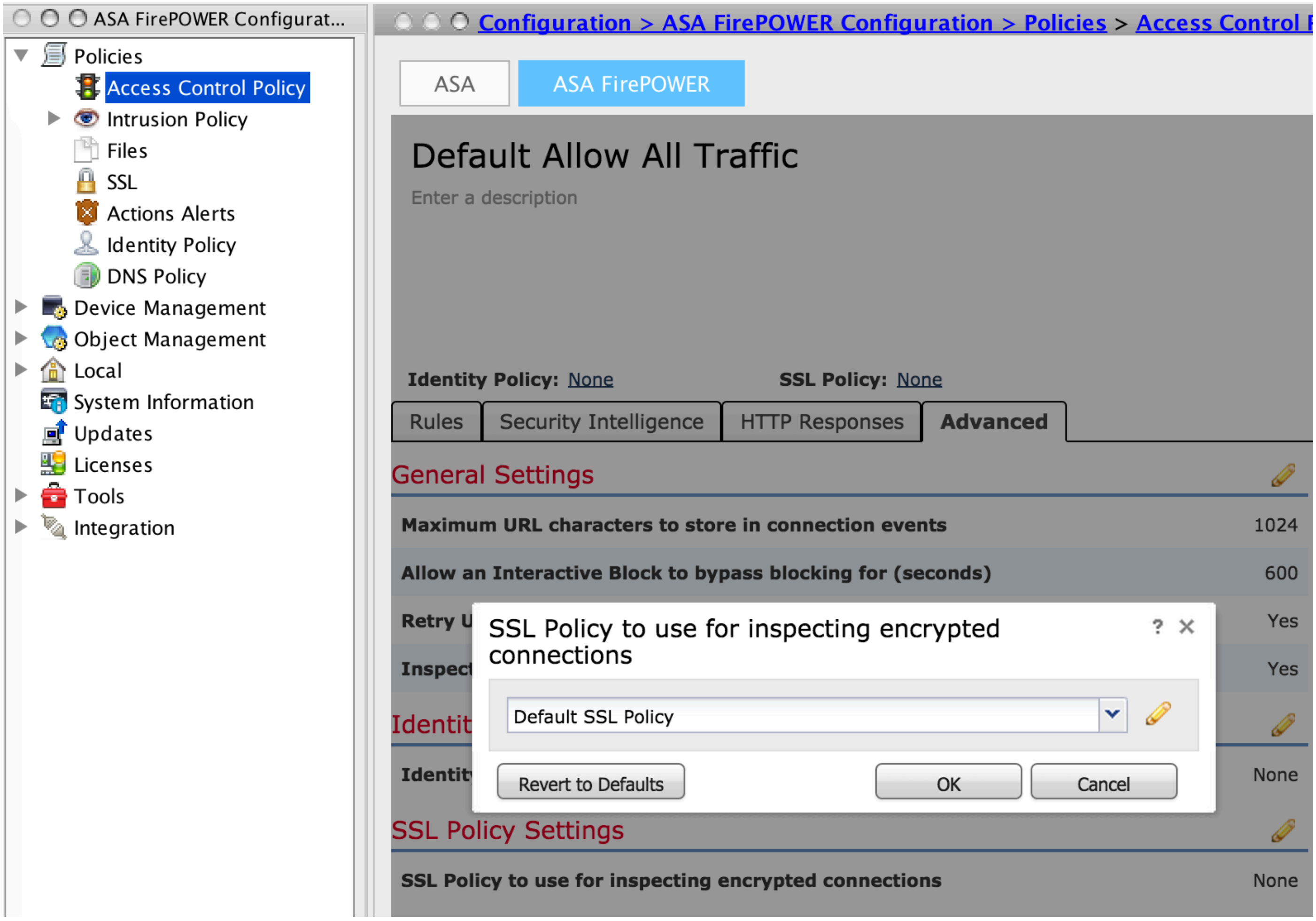
Click **Store ASA Firepower Changes** to save the configuration of SSL policy.

Step 3. Configure the Access Control Policy

Once you configure the SSL policy with appropriate rules, you must specify the SSL policy in the Access Control to implement the changes.

To configure the Access Control policy, navigate to **Configuration > ASA Firepower Configuation > Policies > Access Control.**

Either click **None** of the **SSL Policy** or navigate to **Advanced > SSL Policy Setting.** Specify the SSL policy from the drop-down list and click **OK** to save it, as shown in the image:



Default Allow All Traffic

Enter a description

Identity Policy: None SSL Policy: None

General Settings

Maximum URL characters to store in connection events 1024

Allow an Interactive Block to bypass blocking for (seconds) 600

Retry U Yes

Inspect Yes

Identit

Identit None

SSL Policy Settings

SSL Policy to use for inspecting encrypted connections None

SSL Policy to use for inspecting encrypted connections

Default SSL Policy

Click **Store ASA Firepower Changes** to save the configuration of SSL policy.

You must deploy the Access Control policy to the sensor. Before you apply the policy, there is an indication that **Access Control Policy out-of-date** on the module. To deploy the changes to the sensor, click **Deploy** and select **Deploy FirePOWER Changes option.** Verify the changes made and click **Deploy.**

> **Note**: In version 5.4.x, if you need to apply the access policy to the sensor, click **Apply ASA FirePOWER Changes.**

Note: Navigate to **Monitoring > ASA Firepower Monitoring > Task Status.** You then apply for cofiguration changes to ensure that the task is completed.

Inbound SSL Decryption (Decrypt - Known)

Inbound SSL Decryption (Decrypt-Known) method is used to decrypt the inbound SSL traffic for which you have configured server certificate and private key. You need to import the Server Certificate and Private key to the Firepower module. When SSL traffic hits the Firepower module, it decrypts the traffic and performs the inspection on decrypted traffic. After inspection, Firepower module re-encrypts the traffic and sends it to the server.

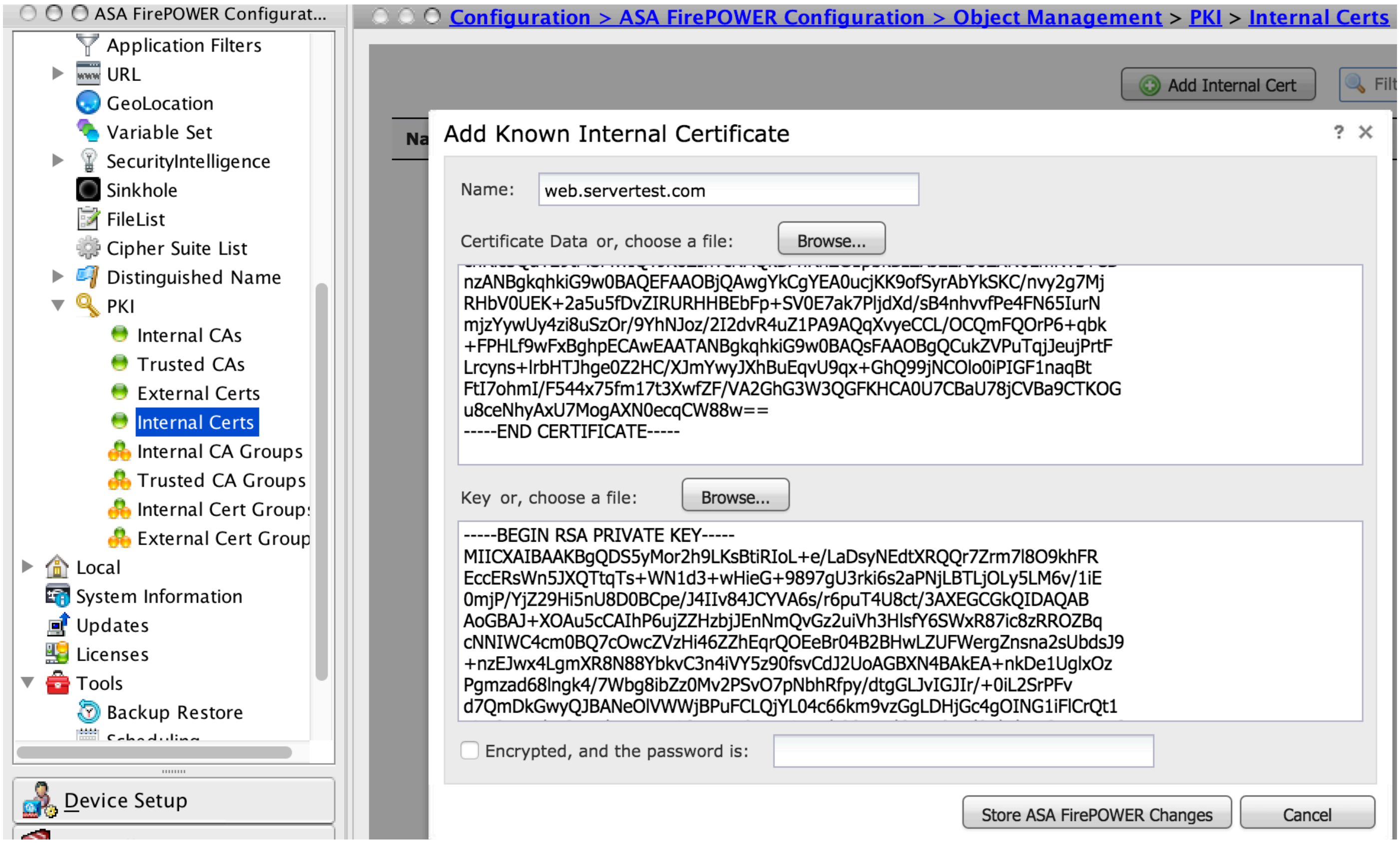
These are the four steps to configure the Outbound SSL Decryption:

Step 1.

In order to import the Server Certificate and Key, navigate to **Configuration > ASA Firepower Configuration > Object Management > PKI > Internal Certs** and click on **Add Internal Cert**.

As shown in the image, specify the Nameof the Certificate. Either select **browse** to select the certificate from the local machine or copy-paste the content of the certificate in the **Certificate Data**. In order to specify the private key of the certificate, either browse the key file or copy-paste the key in the option **Key**.

If the key is encrypted, then enable the checkbox **Encrypted** and specify the password, as shown in the image:



Add Known Internal Certificate

Name: web.servertest.com

Certificate Data or, choose a file:

```
nzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA0ucjKK9ofSyrAbYkSKC/nvy2g7Mj
RHbV0UEK+2a5u5fDvZIRURHHBEbFp+SV0E7ak7PljdXd/sB4nhvvfPe4FN65IurN
mjzYywUy4zi8uSzOr/9YhNJoz/2I2dvR4uZ1PA9AQqXvyeCCL/OCQmFQOrP6+qbk
+FPHLf9wFxBghpECAwEAATANBgkqhkiG9w0BAQsFAAOBgQCukZVPuTqjJeujPrtF
Lrcyns+lrbHTJhge0Z2HC/XJmYwyJXhBuEqvU9qx+GhQ99jNCOlo0iPIGF1naqBt
FtI7ohmI/F544x75fm17t3XwfZF/VA2GhG3W3QGFKHCA0U7CBaU78jCVBa9CTKOG
u8ceNhyAxU7MogAXN0ecqCW88w==
-----END CERTIFICATE-----
```

Key or, choose a file:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDS5yMor2h9LKsBtiRIoL+e/LaDsyNEdtXRQQr7Zrm7l8O9khFR
EccERsWn5JXQTtqTs+WN1d3+wHieG+9897gU3rki6s2aPNjLBTLjOLy5LM6v/1iE
0mjP/YjZ29Hi5nU8D0BCpe/J4IIv84JCYVA6s/r6puT4U8ct/3AXEGCGkQIDAQAB
AoGBAJ+XOAu5cCAIhP6ujZZHzbjJEnNmQvGz2uiVh3HlsfY6SWxR87ic8zRROZBq
cNNIWC4cm0BQ7cOwcZVzHi46ZZhEqrQOEeBr04B2BHwLZUFWergZnsna2sUbdsJ9
+nzEJwx4LgmXR8N88YbkvC3n4iVY5z90fsvCdJ2UoAGBXN4BAkEA+nkDe1UglxOz
Pgmzad68lngk4/7Wbg8ibZz0Mv2PSvO7pNbhRfpy/dtgGLJvIGJIr/+0iL2SrPFv
d7QmDkGwyQJBANeOlVWWjBPuFCLQjYL04c66km9vzGgLDHjGc4gOING1iFlCrQt1
```

☐ Encrypted, and the password is:

Click on **Store ASA FirePOWER Changes** to save the certificate content.

Step 2. Import the CA certificate (optional).

For server certificate signed by Internal intermediate or root CA certificate, you need to import the internal chain of CA certificates to the firepower module. After the import is carried out, firepower module is able to validate the server certificate.

To import the CA certificate, navigate to **Configuration > ASA Firepower Configuration > Object Management > Trusted CAs** and click **Add Trusted CA** to add the CA certificate.

Step 3. Configure the SSL Policy.

SSL policy defines the action and server details for which you wish to configure Decrypt-known method to decrypt the inbound traffic. If you have multiple internal servers, configure multiple SSL rules based on different servers and the traffic they handle .

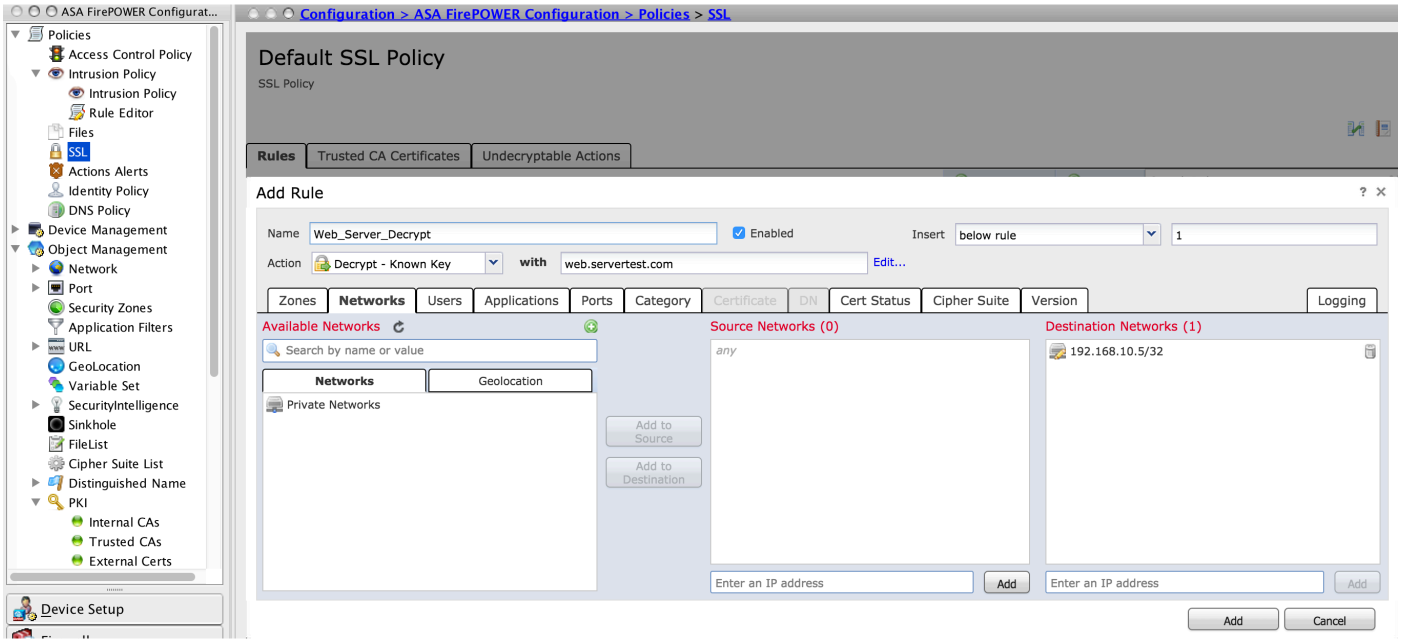
To configure the SSL policy, navigate to **Configure > ASA FirePOWER Configuration > Policies > SSL** and click on **Add Rule**.

Name: Specify the name of the rule.

Action: Specify the action as **Decrypt - known** and choose the CA certificate from the drop-down list which is configured in the previous step.

Define the condition to match this rules, as there are multiple options (network, application, ports etc.) specified to define the interesting traffic of the server for which you want to enable the SSL decryption. Specify the internal CA in **Selected Trusted CAs** in**Trusted CA certificate** tab**.**

To generate the events of SSL decryption, enable the loggingat **logging** option.



Name Web_Server_Decrypt ☑ Enabled Insert below rule 1

Action Decrypt - Known Key with web.servertest.com Edit...

Destination Networks (1): 192.168.10.5/32

Click **Add** to add the SSL rule.

And then click on **Store ASA Firepower Changes** to save the configuration of SSL policy.

Step 4. Configure the Access Control Policy.

Once you configure the SSL policy with appropriate rules, you must specify the SSL policy in the Access Control to implement the changes.

To configure the Access Control policy, navigate to **Configuration > ASA Firepower Configuation > Policies > Access Control.**

Either click the **None** option beside of **SSL Policy** or navigate to **Advanced > SSL Policy Setting**, specify the SSL policy from the drop-down list and click **OK** to save it.

Click **Store ASA Firepower Changes** to save the configuration of SSL policy.

You must deploy the Access Control policy. Before you apply the policy, you can see an indication Access Control Policy out-of-date on the module. To deploy the changes to the sensor, click **Deploy** and choose **Deploy FirePOWER Changes option.** Verify the changes made and click **Deploy** in the pop-up window.

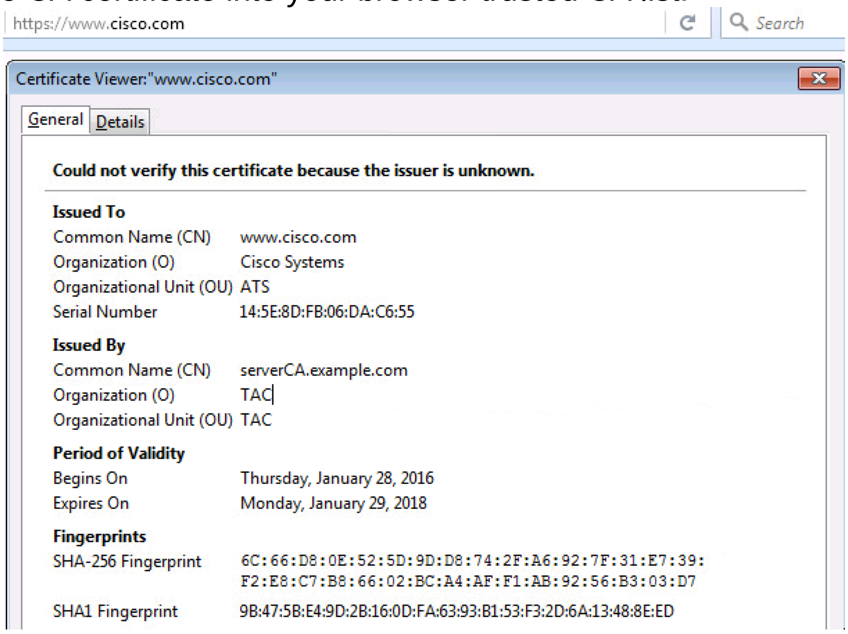
> **Note**: In version 5.4.x, if you need to apply the access policy to the sensor, click **Apply ASA FirePOWER C**.

> **Note**: Navigate to **Monitoring > ASA Firepower Monitoring > Task Status.** You then apply for cofiguration changes to ensure that the task is completed.

Verify

Use this section in order to confirm that your configuration works properly.

- For Outbound SSL connection, once you browse a public SSL website from the internal network, the system prompts an error message of the certificate. Check the certificate content and verify the CA information. The internal CA certificate you configured in the Firepower module appears. Accept the error message to browse the SSL certificate. To avoid the error message, add the CA certificate into your browser trusted CA list.



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

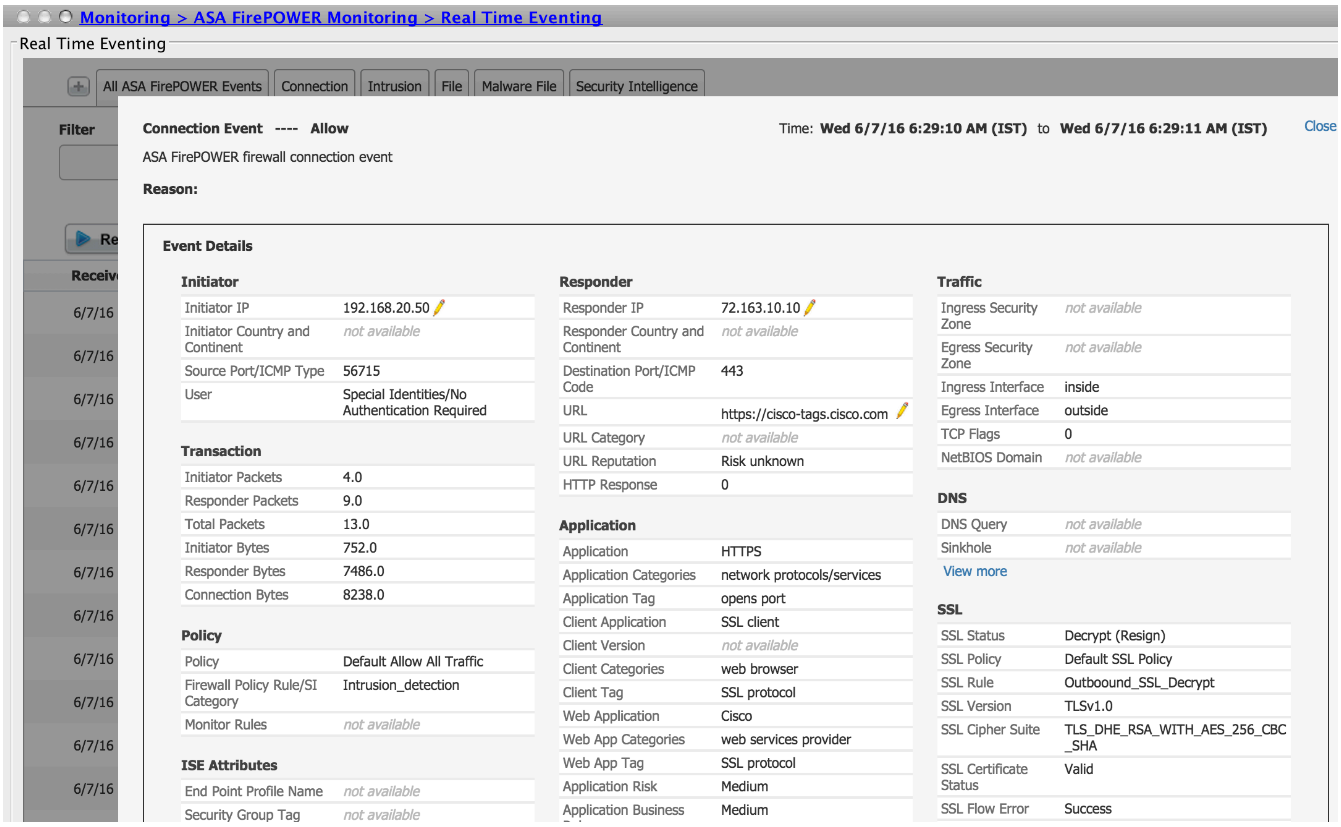
Period of Validity

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

- Check the connection events to verify which SSL policy and SSL rule is hitby the traffic. Navigate to **Monitoring > ASA FirePOWER Monitoring > Real-Time Eventing.**Select an event and click on **View Details**. Verify the SSL decryption statistics.



Connection Event ---- Allow

Time: **Wed 6/7/16 6:29:10 AM (IST)** to **Wed 6/7/16 6:29:11 AM (IST)**

ASA FirePOWER firewall connection event

Reason:

Event Details

Initiator

Initiator IP	192.168.20.50
Initiator Country and Continent	not available
Source Port/ICMP Type	56715
User	Special Identities/No Authentication Required

Transaction

Initiator Packets	4.0
Responder Packets	9.0
Total Packets	13.0
Initiator Bytes	752.0
Responder Bytes	7486.0
Connection Bytes	8238.0

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

Responder

Responder IP	72.163.10.10
Responder Country and Continent	not available
Destination Port/ICMP Code	443
URL	https://cisco-tags.cisco.com
URL Category	not available
URL Reputation	Risk unknown
HTTP Response	0

Application

Application	HTTPS
Application Categories	network protocols/services
Application Tag	opens port
Client Application	SSL client
Client Version	not available
Client Categories	web browser
Client Tag	SSL protocol
Web Application	Cisco
Web App Categories	web services provider
Web App Tag	SSL protocol
Application Risk	Medium
Application Business	Medium

Traffic

Ingress Security Zone	not available
Egress Security Zone	not available
Ingress Interface	inside
Egress Interface	outside
TCP Flags	0
NetBIOS Domain	not available

DNS

DNS Query	not available
Sinkhole	not available

View more

SSL

SSL Status	Decrypt (Resign)
SSL Policy	Default SSL Policy
SSL Rule	Outboound_SSL_Decrypt
SSL Version	TLSv1.0
SSL Cipher Suite	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
SSL Certificate Status	Valid
SSL Flow Error	Success

- Ensure that the Access Control Policy deployment completes successfully.
- Ensure that SSL policy is included in the Access Control Policy.
- Ensure that SSL policy contains appropriate rules for Inbound and Outbound direction.
- Ensure that SSL rules contain the proper condition to define the interesting traffic.
- Monitor the connection events to verify the SSL policy and SSL rule.
- Verify the SSL decryption status.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- **Technical Support & Documentation - Cisco Systems**