Configuratie van de SSL decryptie op FirePOWER Module die ASDM (On-Box Management) gebruikt

Inhoud

Inleiding

Dit document beschrijft de configuratie van Secure Socket Layer (SSL) decryptie op FirePOWER Module met behulp van ASDM (On-Box Management).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Kennis van ASA (adaptieve security applicatie) firewall, ASDM (adaptieve security applicatie Manager)
- Kennis van FirePOWER-apparaat
- Kennis van HTTPS/SSL-protocol

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- ASA FirePOWER-modules (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) met software versie 6.0.0 en hoger
- ASA FirePOWER-module (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) met software versie 6.0.0 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

> Opmerking: Zorg ervoor dat FirePOWER Module een **Protect** licentie heeft om deze functionaliteit te configureren. Om de licentie te controleren dient u te navigeren naar **Configuration > ASA FirePOWER Configuration > Licentie**.

Achtergrondinformatie

Firepower Module decrypteert en inspecteert inkomende en uitgaande SSL verbindingen die naar deze worden omgeleid. Zodra het verkeer is gedecrypteerd, worden de getunnelde toepassingen zoals Facebookchat etc. gedetecteerd en gecontroleerd. De gecodeerde gegevens worden geïnspecteerd op bedreigingen, URL-filtering, bestandblokkering of kwaadaardige gegevens.

Uitgaande SSL-decryptie

De vuurkrachtmodule fungeert als de voorwaartse proxy voor uitgaande SSL-verbindingen door het onderscheppen van uitgaande SSL-verzoeken en het opnieuw genereren van een certificaat voor de site die de gebruiker wil bezoeken. De instantie van afgifte (CA) is het certificaat van zelfondertekening van vuurkracht. Als het certificaat van de vuurkracht geen deel uitmaakt van een hiërarchie die bestaat of als het niet wordt toegevoegd aan de browser cache van een klant, ontvangt de klant een waarschuwing terwijl hij doorbladert naar een beveiligde site. Decrypt-Resignatiemethode wordt gebruikt om uitgaande SSL decryptie uit te voeren.

Inbound SSL-decryptie

In het geval van inkomend verkeer naar een interne server of apparaat van het Web importeert de beheerder een kopie van het certificaat van de beschermde server en de sleutel. Wanneer het SSL servercertificaat op de vuurkrachtmodule wordt geladen, en het SSL decryptiebeleid wordt gevormd voor het inkomende verkeer, decrypteert het apparaat dan en inspecteert het verkeer wanneer het het verkeer door het verkeer leidt. De module detecteert dan kwaadaardige inhoud, bedreigingen, kwiek die over dit veilige kanaal stroomt. Bovendien wordt de Decrypt-Known Keymethode gebruikt om inkomende SSL decryptie uit te voeren.

Configuratie voor SSL-decryptie

Er zijn twee methoden van SSL-verkeersdecryptie.

- Decrypteren - Aftreden voor Uitgaand SSL verkeer
- Decrypteren - gekend voor Inbound SSL verkeer

Uitgaande SSL-decryptie (decrypt - Afgifte)

Firepower module fungeert als MITM (man-in-the-middle) voor SSL-onderhandelingen voor openbare SSL-servers. Het wijst het certificaat van de openbare server met een middelgroot CA certificaat af dat op de vuurkrachtmodule is ingesteld.

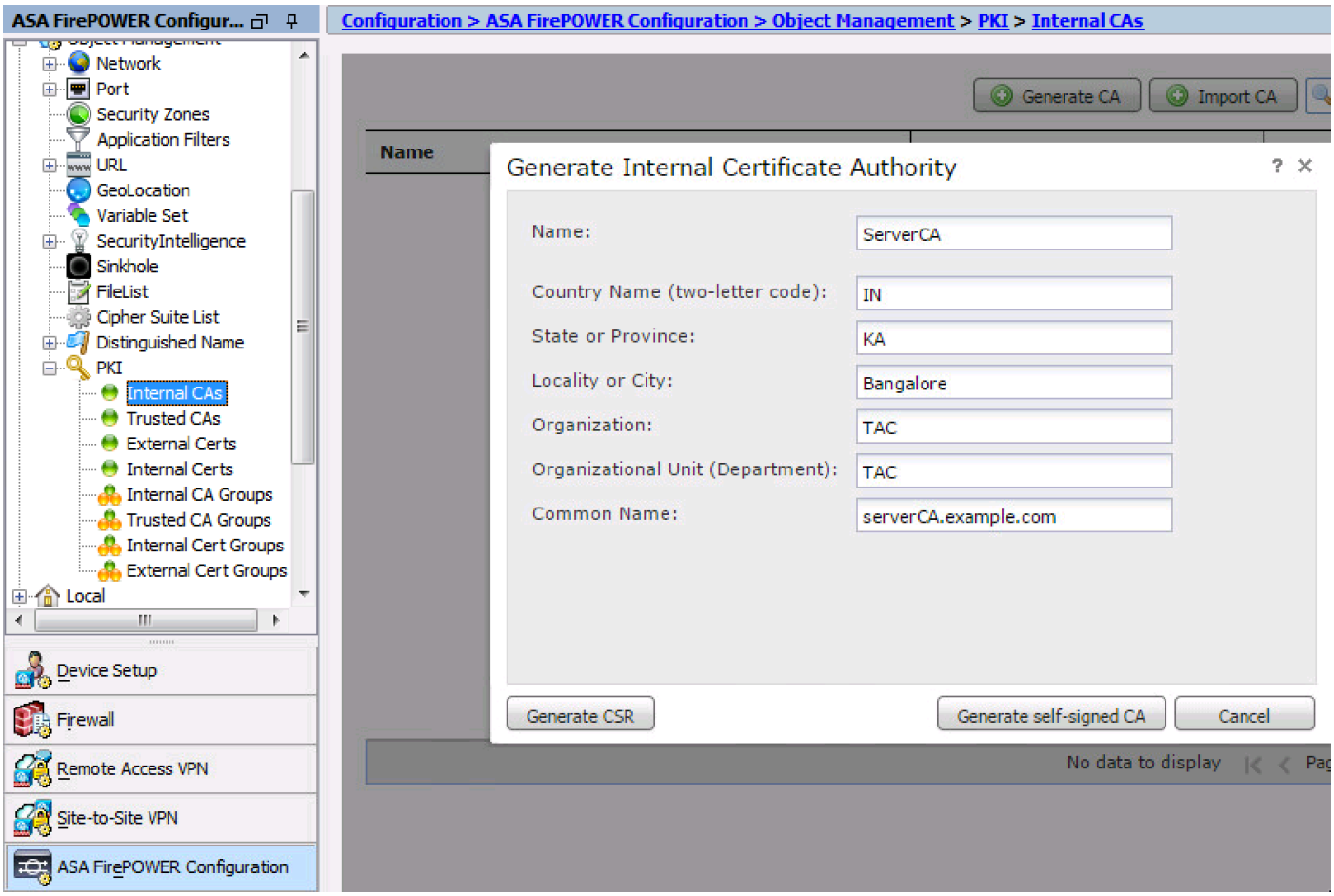
Dit zijn de drie stappen om de uitgaande SSL-decryptie te configureren.

Stap 1. Configuratie van het CA-certificaat.

Configureer een zelfgetekend certificaat of een middelmatig betrouwbaar CA-certificaat voor ontslag.

Het zelf-ondertekende CA-certificaat configureren

Om het CA-certificaat met eigen handtekening te configureren **navigeer** naar **Configuration > ASA Firepower Configuration > Objectbeheer > PKI > Interne CA's** en klik op **Generate CA**. Het systeem vraagt om informatie over het CA-certificaat. Zoals in de afbeelding wordt aangegeven, vult u de gegevens in zoals vereist.



Klik op **Generate zelfgetekende CA** om het interne CA certificaat te genereren. Klik vervolgens op **Generate CSR** om het certificaat-teken-verzoek te genereren dat dientengevolge met de CA

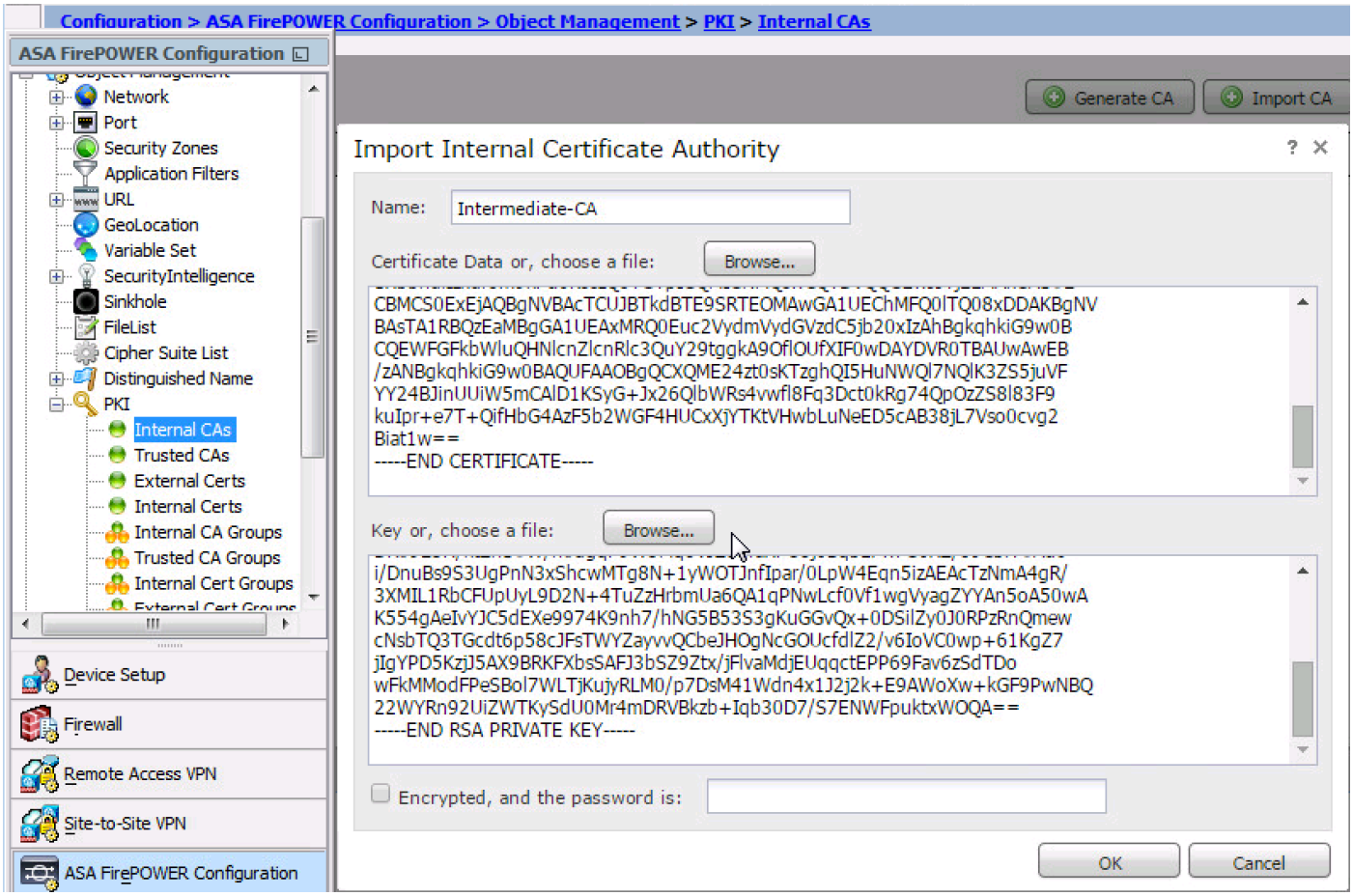
server wordt gedeeld om te tekenen.

Het middelste CA-certificaat configureren

Om het Intermediate CA Certificaat te configureren dat door een andere derde CA wordt ondertekend, navigeer naar **Configuratie > ASA Firepower Configuration > Objectbeheer > PKI > Interne CA's** en klik op **Importeren CA**.

Specificeer de naam van het certificaat. Selecteer de optie Bladeren en uploaden het certificaat vanuit de lokale machine of kopieer de inhoud van het certificaat in de optie **certificaatgegevens**. Om de privétoets van het certificaat te specificeren, bladert u door het sleutelbestand of kopieert u de toets in de optie **Key**.

Als de toets is versleuteld, stelt u het vakje **Encrypted** in en specificeert u het wachtwoord. Klik op **OK** om de certificaatinhoud op te slaan, zoals in de afbeelding wordt weergegeven:



Stap 2. Het SSL-beleid configureren.

SSL-beleid definieert de decryptie-actie en identificeert het verkeer waarop de decryptie-afgiftemethode wordt toegepast. Configureer de meerdere SSL-regels op basis van uw zakelijke vereisten en het beveiligingsbeleid van de organisatie.

Om het SSL beleid te configureren **navigeer** om **> ASA FirePOWER Configuration > Policy > SSL** te **configureren** en op **Add Rule** te klikken.

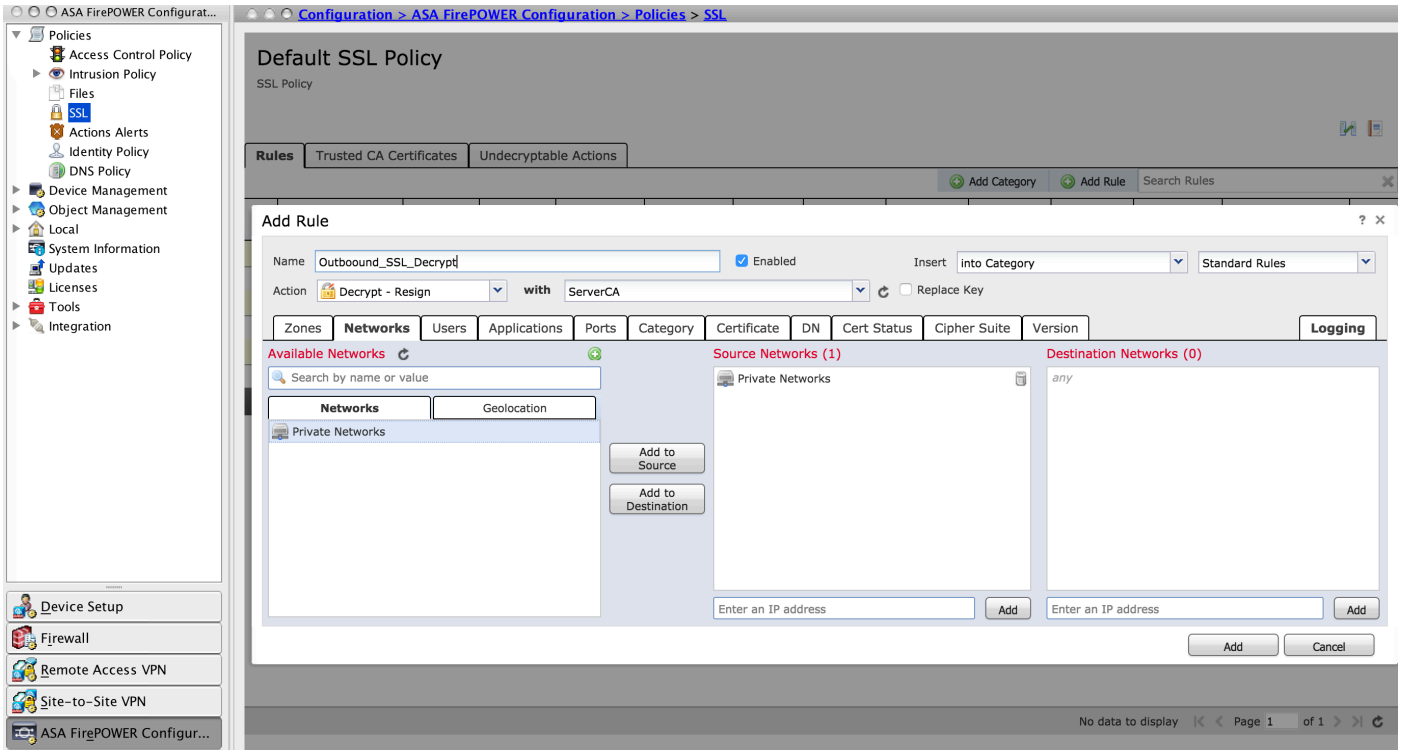
Naam: Specificeer de naam van de regel.

Actie: Specificeer de actie als **decrypt - ontvang** en kies het CA certificaat van de vervolgkeuzelijst

die in de vorige stap is ingesteld.

Bepaal de voorwaarden in de regel om verkeer aan te passen zoals er meerdere opties zijn (zone, netwerk, gebruikers enz.), gespecificeerd om het verkeer te definiëren dat moet worden gedecrypteerd.

Om de gebeurtenissen van SSL decryptie te genereren, schakelt u de logingat **logging** optie in zoals in de afbeelding:



Klik op **Add** om de SSL-regel toe te voegen.

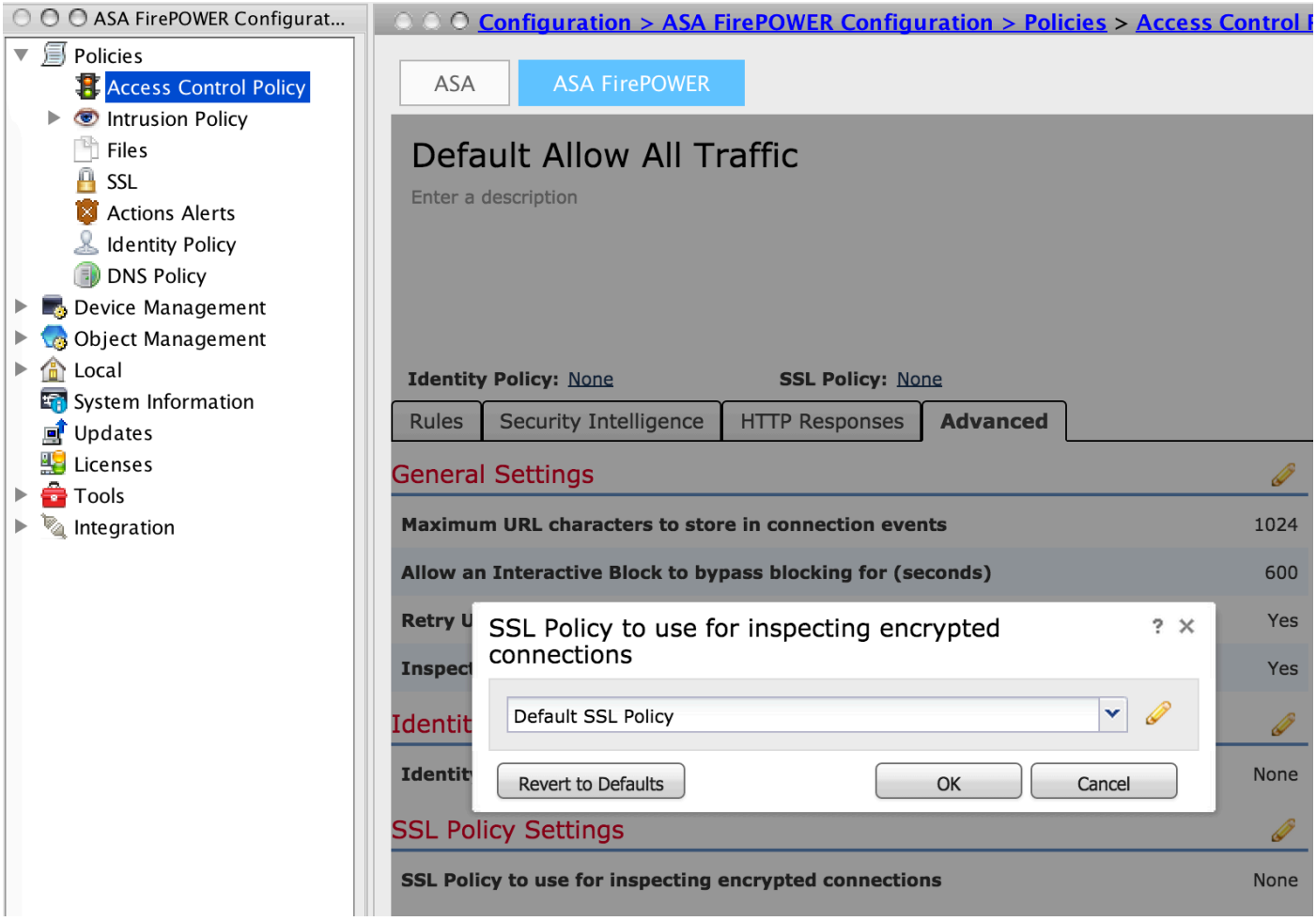
Klik op **Store ASA Firepower Wijzigingen** om de configuratie van SSL beleid op te slaan.

Stap 3. Het beleid voor toegangscontrole configureren

Zodra u het SSL beleid met de juiste regels vormt, moet u het SSL beleid in het Toegangsbeheer specificeren om de veranderingen uit te voeren.

Om het beleid voor toegangscontrole te configureren **navigeer** naar **Configuratie > ASA Firepower Configuration > Policy > Access Control.**

Klik of op **Geen** van het **SSL Beleid** of navigeer naar **Geavanceerd > SSL Policy Setting.** Specificeer het SSL-beleid in de vervolgkeuzelijst en klik op **OK** om het op te slaan, zoals in de afbeelding:



Klik **ASA FireSIGHT-wijzigingen opslaan** om de configuratie van SSL beleid op te slaan.

Je moet het toegangscontrolemiddel op de sensor zetten. Voordat u het beleid toepast, is er een indicatie dat **Access Control Policy verouderd is** op de module. Om de wijzigingen in de sensor in te stellen, klikt u op **Importeren** en selecteert u **optie FirePOWER Wijzigingen implementeren.** Controleer de aangebrachte wijzigingen en klik op **Importeren.**

> Opmerking: In versie 5.4.x, als u het toegangsbeleid op de sensor moet toepassen, klik op **ASA FirePOWER Wijzigingen toepassen.**

> Opmerking: Navigeer naar **bewaking > ASA FirePOWER Monitoring > Taakstatus.** U dient vervolgens wijzigingen in de configuratie in om er zeker van te zijn dat de taak is voltooid.

Inbound SSL-decryptie (decrypt - bekend)

De inkomende SSL Decryptie (Decrypt-Known) methode wordt gebruikt om het inkomende SSL verkeer te decrypteren waarvoor u het servercertificaat en de privé sleutel hebt gevormd. U moet het servercertificaat en de privétoets naar de FirePOWER-module importeren. Wanneer SSL-verkeer de Firepower module raakt, ontsleutelt het het verkeer en voert het de inspectie uit op gedecrypteerd verkeer. Na inspectie, herversleutelt de Firepower module het verkeer en verstuurt het naar de server.

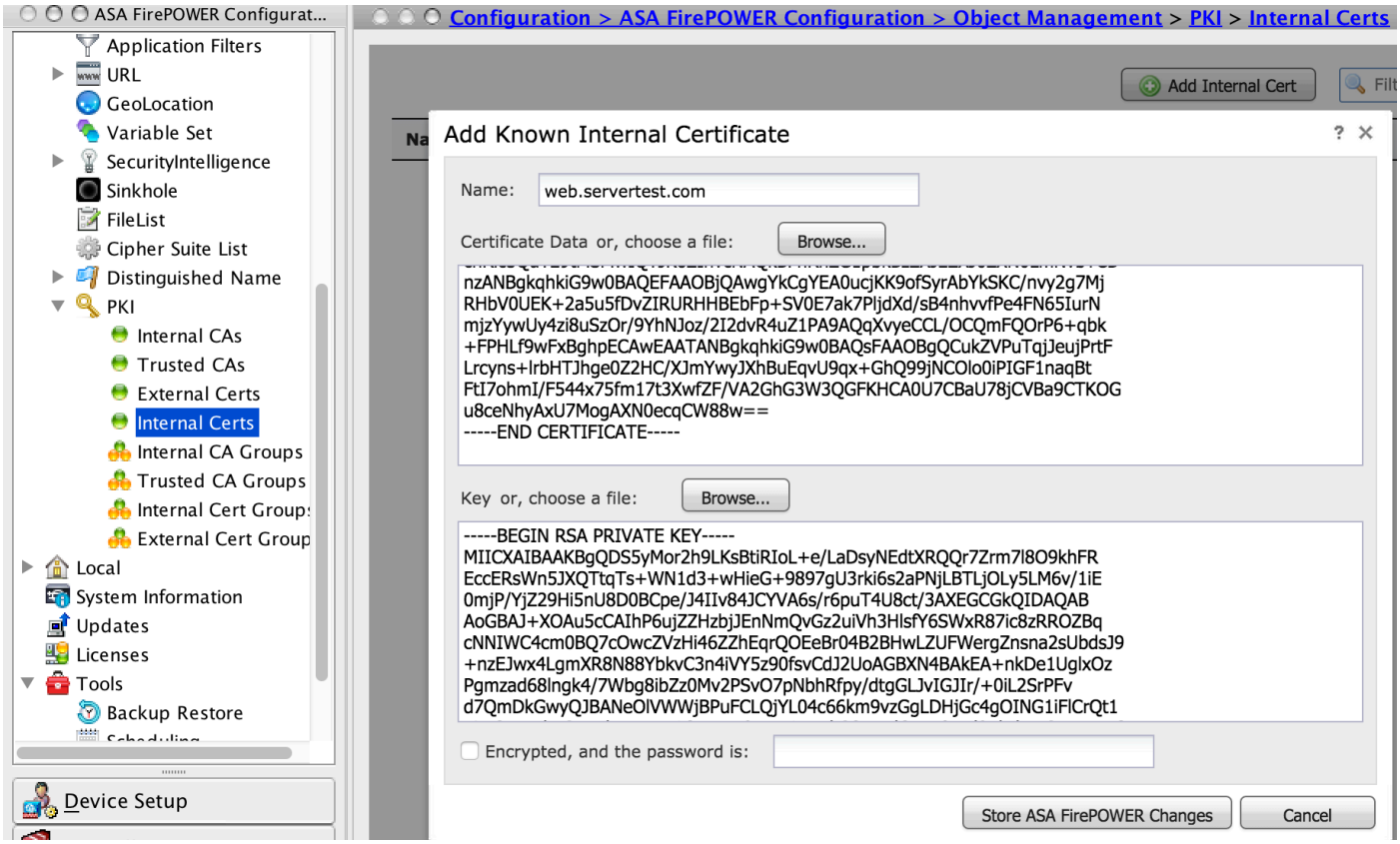
Dit zijn de vier stappen om de uitgaande SSL-decryptie te configureren:

Stap 1. Importeer het servercertificaat en de -toets.

Als u het servercertificaat en de -toets wilt importeren, navigeer dan naar **configuratie > ASA Firepower Configuration > Objectbeheer > PKI > Interne Certs** en klik op **Add Internal Cert**.

Specificeer zoals in de afbeelding de naam van het certificaat. Selecteer ofwel browsen om het certificaat uit de lokale machine te selecteren of kopieer de inhoud van het certificaat in de **certificaatgegevens**. Om de privétoets van het certificaat te specificeren, bladert u door het sleutelbestand of kopieert u de toets in de optie-**toets**.

Als de toets is versleuteld, schakelt u het **versleutelde** keuzevakje in en specificeert u het wachtwoord, zoals in de afbeelding:



Klik op **Store ASA FirePOWER Wijzigingen** om de certificaatinhoud op te slaan.

Stap 2. Importeer het CA-certificaat (optioneel).

Voor een servercertificaat dat is getekend door een interne tussenpersoon of een basiscertificaat, moet u de interne keten CA-certificaten importeren naar de vuurkrachtmodule. Nadat de invoer is uitgevoerd, kan de vuurkrachtmodule het servercertificaat valideren.

Als u het CA-certificaat wilt importeren, navigeer dan naar **Configuratie > ASA Firepower Configuration > Objectbeheer > Trusted CA's** en klik op **Add Trusted CA** om het CA-certificaat toe te voegen.

Stap 3. Het SSL-beleid configureren.

SSL beleid definieert de actie- en serverdetails waarvoor u de decrypt-bekende methode wilt configureren om het inkomende verkeer te decrypteren. Als u meerdere interne servers hebt, moet u meerdere SSL-regels configureren op basis van verschillende servers en het verkeer dat zij verwerken.

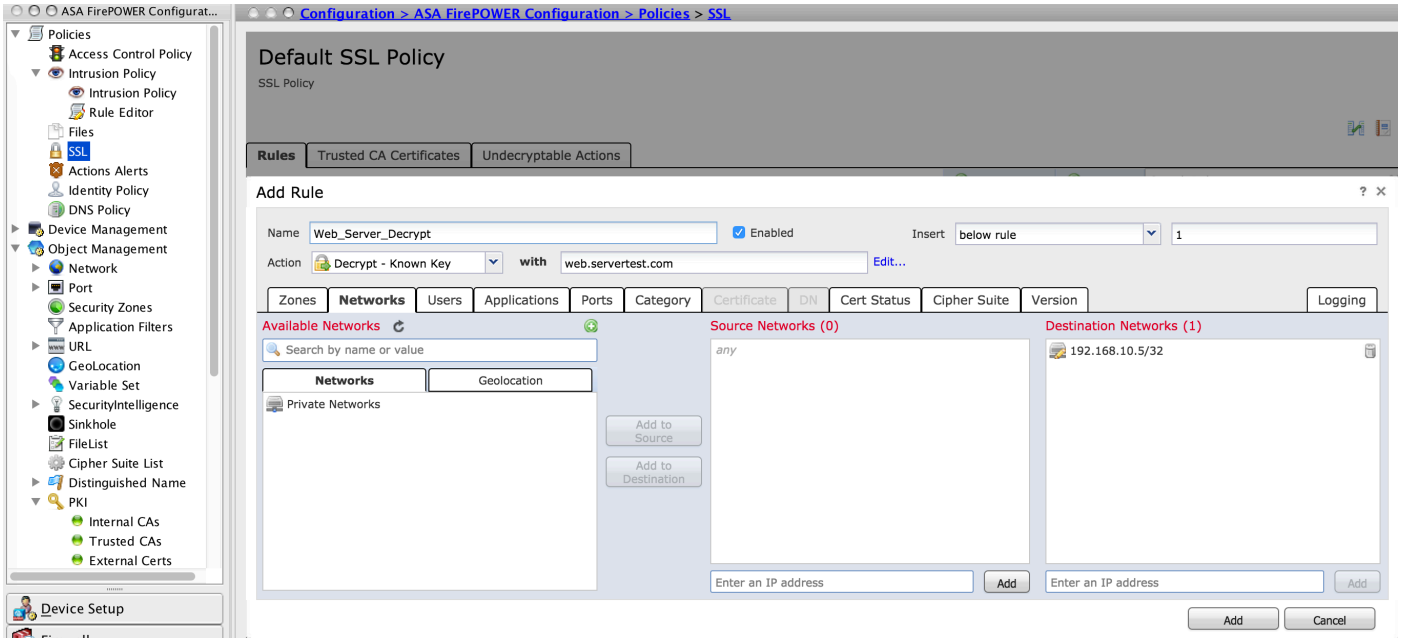
Om het SSL beleid te configureren **navigeer** om **> ASA FirePOWER Configuration > Policy > SSL** te **configureren** en op **Add Rule** te klikken.

Naam: Specificeer de naam van de regel.

Actie: Specificeer de actie als **Decrypt - bekend** en kies het CA certificaat uit de vervolgkeuzelijst die in de vorige stap is ingesteld.

Defineer de voorwaarde om deze regels aan te passen, aangezien er meerdere opties (netwerk, toepassing, poorten enz.) zijn gespecificeerd om het interessante verkeer van de server te definiëren waarvoor u de SSL decryptie wilt inschakelen. Specificeer de interne CA in **Geselecteerde Trusted CAs in** tabblad **Trusted CA certificaat.**

Om de gebeurtenissen van SSL decryptie te genereren, schakelt u de logingat **logging** optie in.



Klik op **Add** om de SSL-regel toe te voegen.

Klik vervolgens op **Store ASA Firepower Wijzigingen** om de configuratie van SSL beleid op te slaan.

Stap 4. Configureer het toegangscontrolebeleid.

Zodra u het SSL beleid met de juiste regels vormt, moet u het SSL beleid in het Toegangsbeheer specificeren om de veranderingen uit te voeren.

Om het beleid voor toegangscontrole te configureren **navigeer** naar **Configuratie > ASA Firepower Configuration > Policy > Access Control.**

Klik op de optie **Geen** naast **SSL Policy** of navigeer naar **Advanced > SSL Policy Setting**, specificeer het SSL-beleid in de vervolgkeuzelijst en klik op **OK** om het op te slaan.

Klik **ASA FireSIGHT-wijzigingen opslaan** om de configuratie van SSL beleid op te slaan.

U moet het beleid voor toegangscontrole implementeren. Voordat u het beleid toepast, kunt u een indicatie Toegangsbeleid op de module zien. Om de veranderingen in de sensor in te zetten, klikt u op **Uitvoeren** en kiest u **optie FirePOWER Veranderingen implementeren.** Controleer de aangebrachte wijzigingen en klik op In het pop-upvenster **implementeren**.

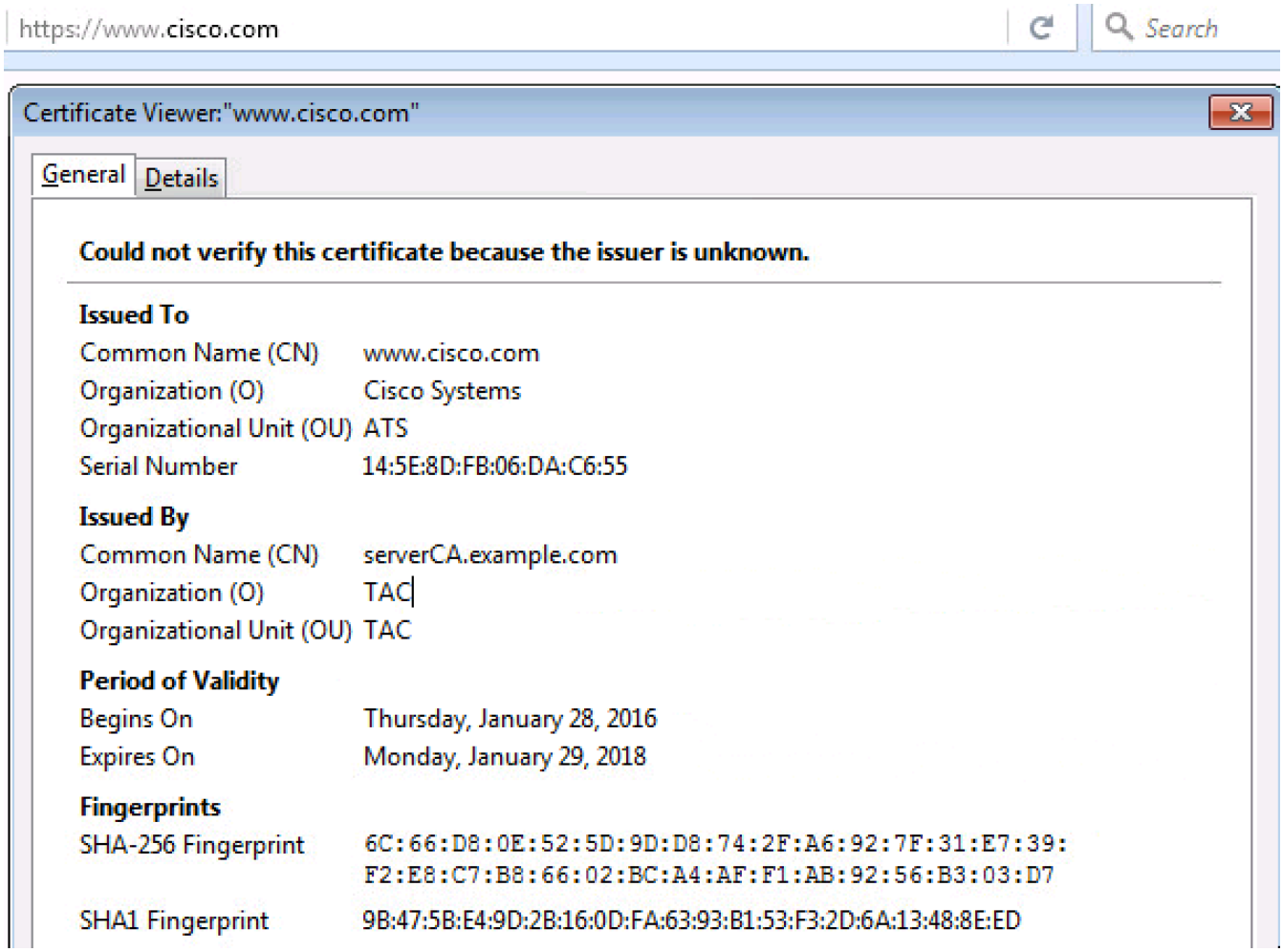
> Opmerking: In versie 5.4.x, als u het toegangsbeleid op de sensor moet toepassen, klik op **ASA FirePOWER Wijzigingen toepassen**.

> Opmerking: Navigeer naar **bewaking > ASA FirePOWER Monitoring > Taakstatus.** U dient vervolgens wijzigingen in de configuratie in om er zeker van te zijn dat de taak is voltooid.

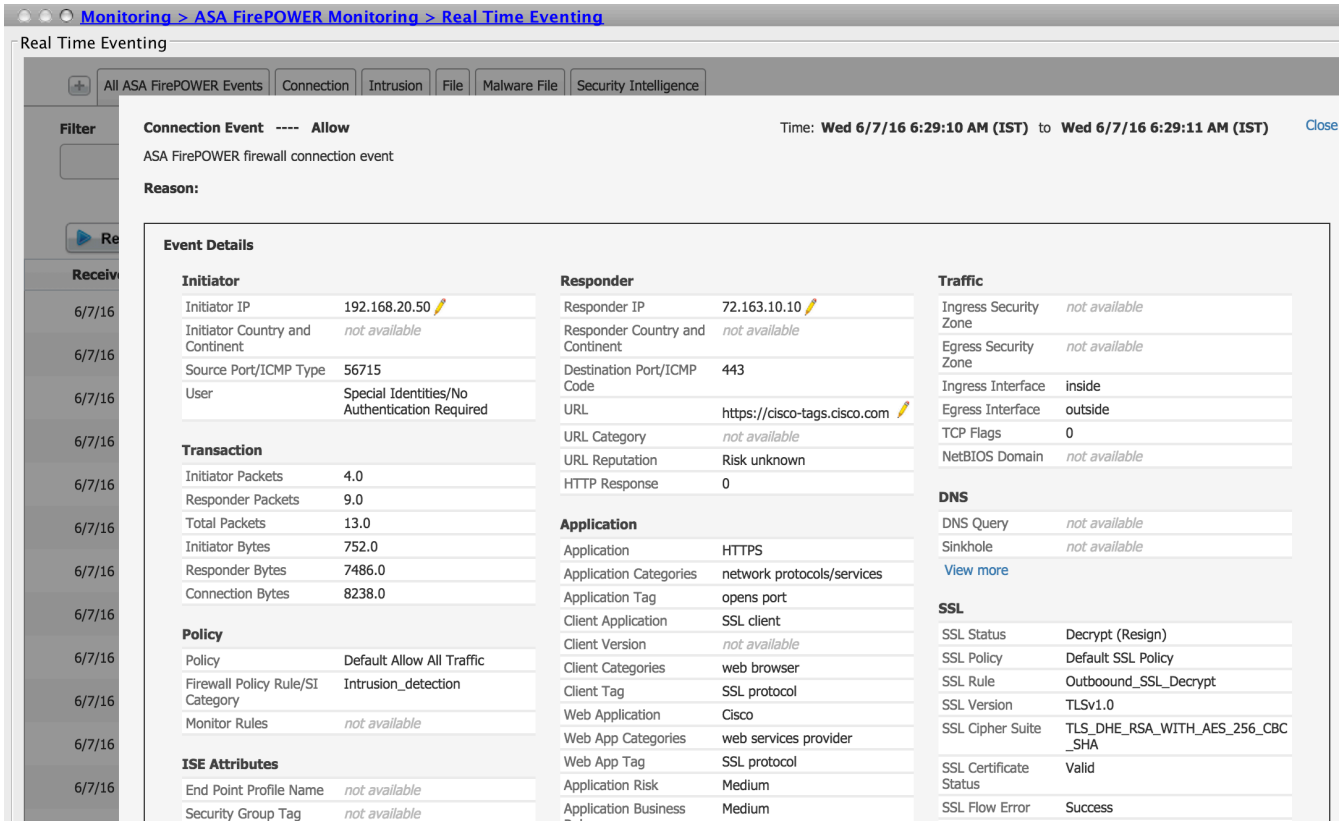
Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

- Voor een uitgaande SSL-verbinding maakt het systeem, nadat u door een openbare SSL-website van het interne netwerk bladert, een foutmelding van het certificaat. Controleer de certificaatinhoud en controleer de CA-informatie. Het interne CA-certificaat dat u in de FirePOWER-module hebt ingesteld, wordt weergegeven. Neem de foutmelding in om door het SSL-certificaat te bladeren. Om de foutmelding te voorkomen, voegt u het CA-certificaat toe aan de vertrouwde CA-lijst van uw browser.



- Controleer de verbindingsgebeurtenissen om te verifiëren welk SSL beleid en SSL regel door het verkeer zijn verbonden. Navigeer naar **bewaking > ASA FirePOWER-bewaking > Real-Time Eventing.**Selecteer een gebeurtenis en klik op **View Details**. Controleer de SSL-decryptie statistieken.



- Zorg ervoor dat de implementatie van het toegangsbeheerbeleid is voltooid.
- Zorg ervoor dat het SSL-beleid in het toegangsbeleid is opgenomen.
- Zorg ervoor dat SSL-beleid passende regels voor inkomende en uitgaande richting bevat.
- Zorg ervoor dat SSL-regels de juiste voorwaarde bevatten om het interessante verkeer te definiëren.
- Controleer de verbindingsgebeurtenissen om het SSL beleid en de SSL regel te verifiëren.
- Controleer de SSL-decryptie status.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- [Technische ondersteuning en documentatie – Cisco Systems]