Configuratie van een SSL-inspectiebeleid in Cisco FireSIGHT System

Inhoud

Inleiding

Met de SSL-inspectie kunt u versleuteld verkeer blokkeren zonder het te inspecteren of versleutelen met toegangscontrole. Dit document beschrijft de configuratiestappen om een SSL-inspectiebeleid in het Cisco FireSIGHT System te zetten.

Voorwaarden

Gebruikte componenten

- Cisco FireSIGHT Management Center
- Cisco Firepower 7000 of 8000 applicaties
- Software, versie 5.4.1 of 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.

Waarschuwing: Als u een SSL inspectiebeleid op uw beheerd apparaat toepast, kan het netwerkprestaties beïnvloeden.

Configuraties

U kunt een SSL inspectiebeleid configureren om verkeer op de volgende manieren te decrypteren:

1. Ontcijferen en ontslag:

- Optie 1: Gebruik het FireSIGHT Center als basiscertificeringsinstantie (CA), of
- Optie 2: Zorg voor een intern CA-teken van uw certificaat, of
- Optie 3: Een CA-certificaat en -toets importeren

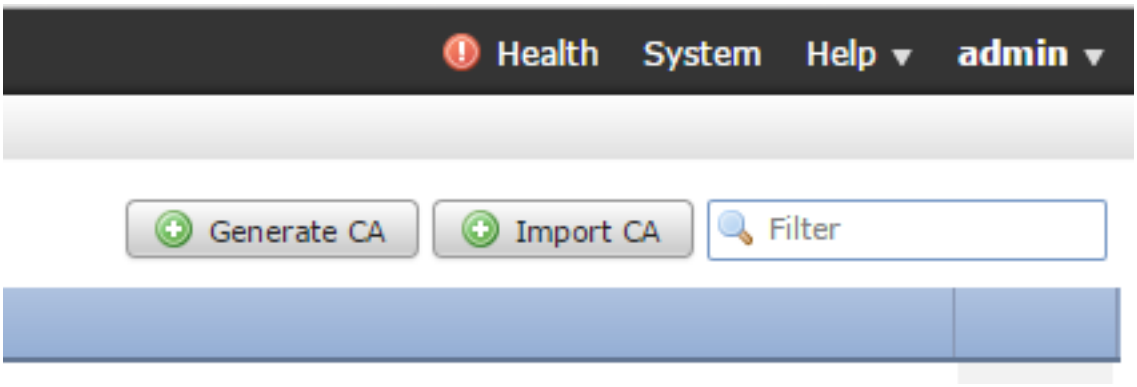
2. Ontsleutelen van bekende fouten:

- Log in op FireSIGHT Management Center en navigeer vervolgens naar **Exemplaar**.
- Vul de **PKI** uit op de pagina **Objects** en selecteer **Interne CAs**.

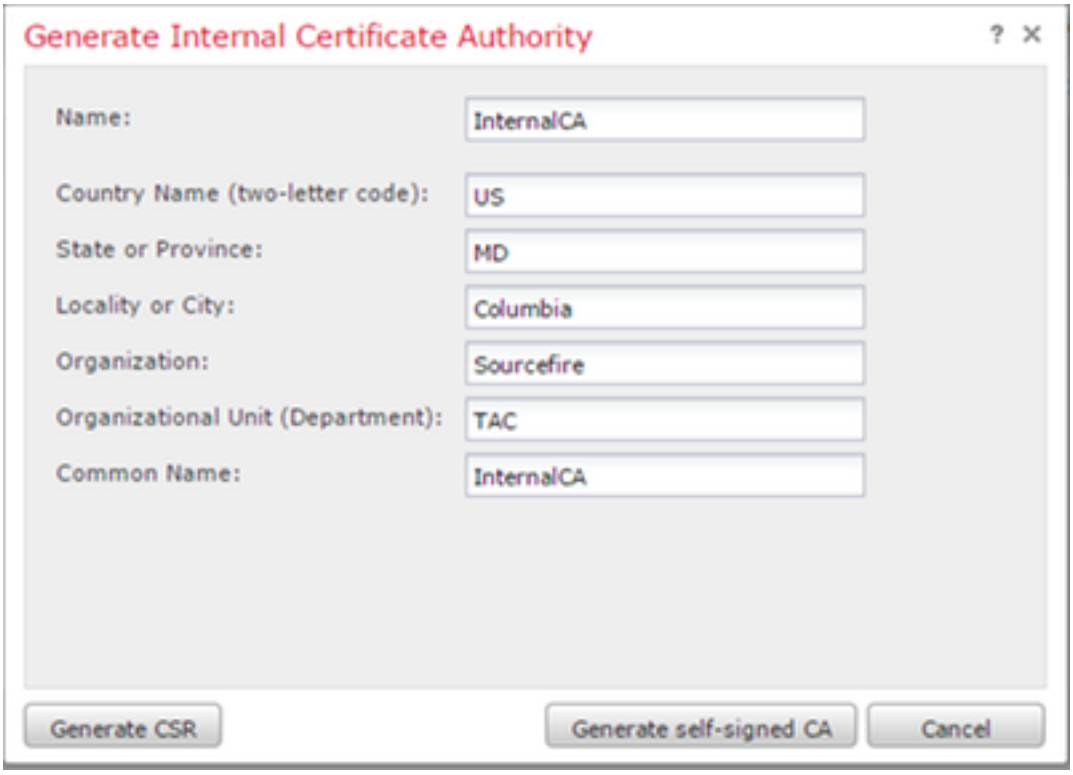
1. Ontcijferen en ontslag

Optie 1: Gebruik het FireSIGHT Center als basiscertificeringsinstantie (CA)

i. Klik op **Generate CA**.



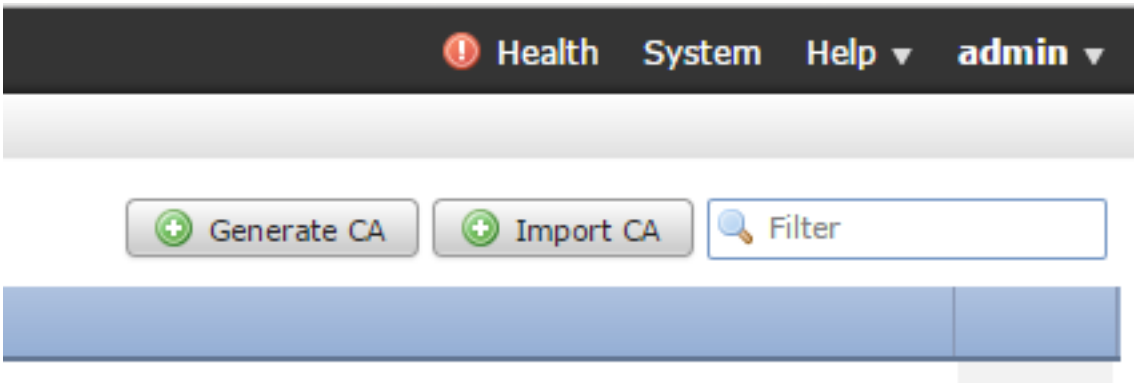
ii. Vul de relevante informatie in



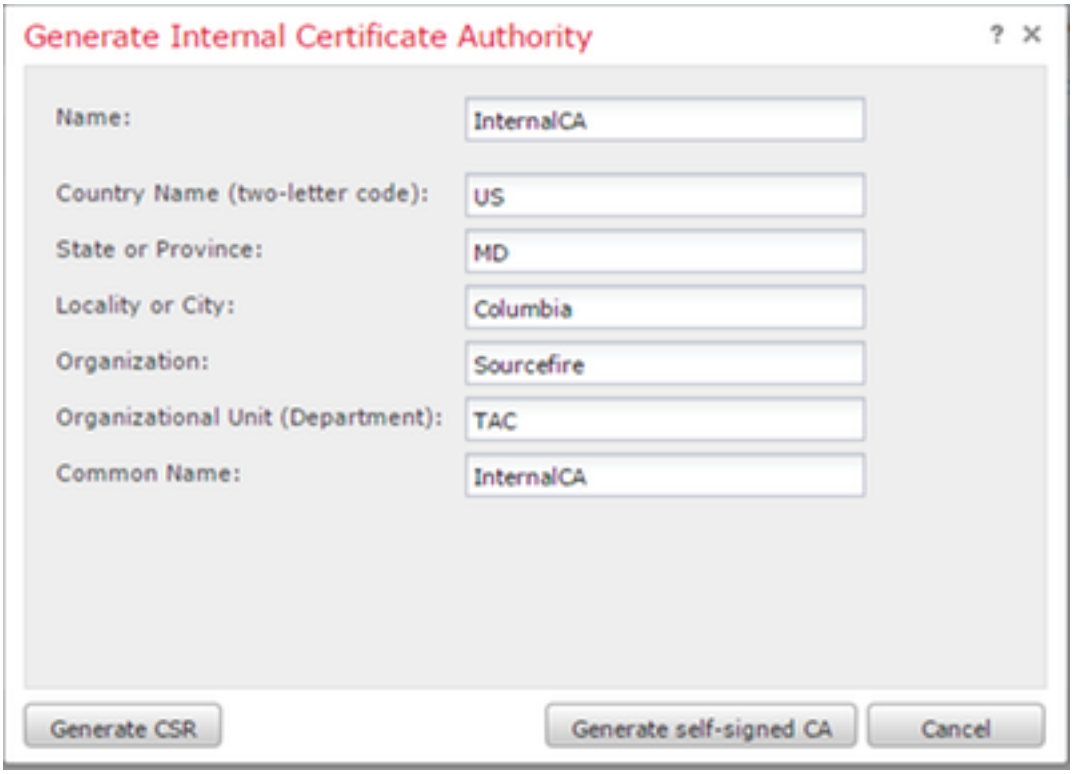
iii. Klik op **Generate zelfgetekende CA**.

Optie 2: Zorg voor een intern CA-teken voor uw certificaat

i. Klik op **Generate CA**.

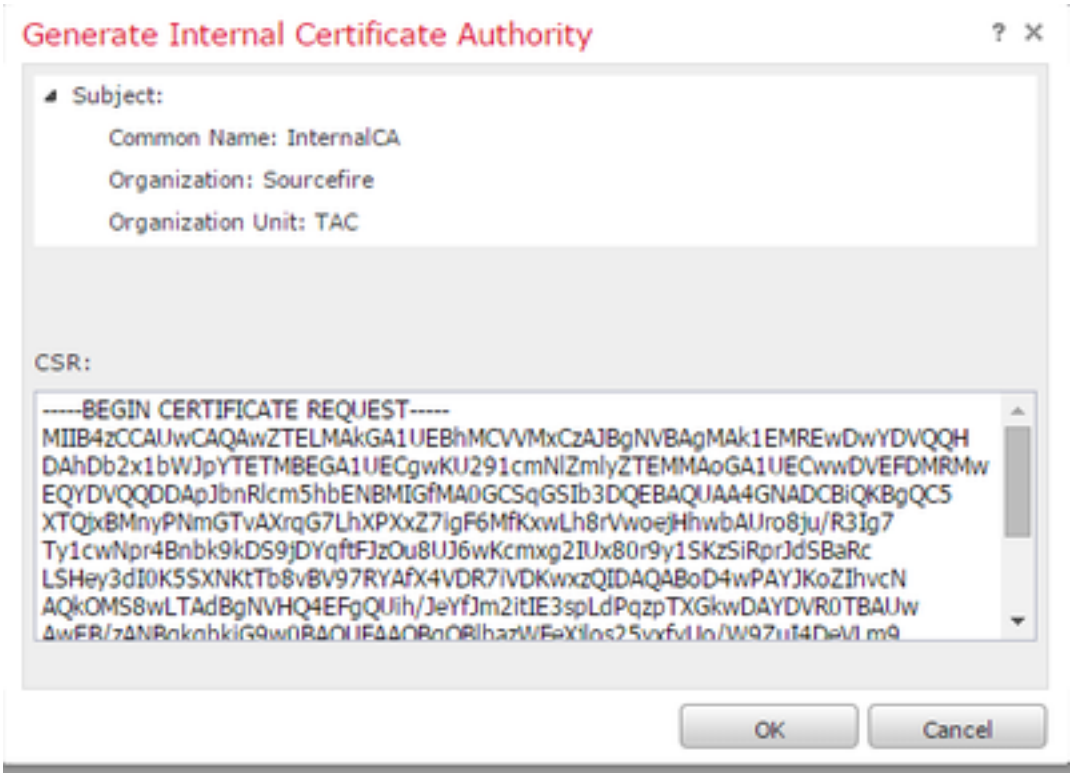


ii. Vul de desbetreffende informatie in.



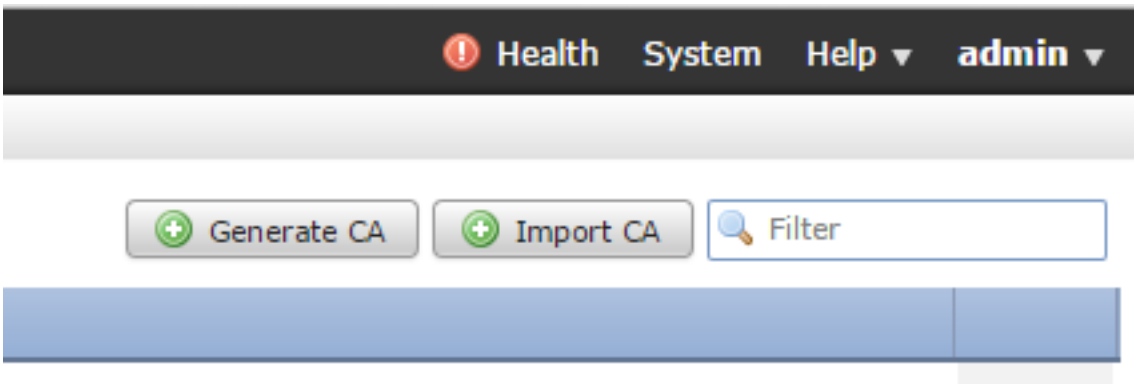
Opmerking: Het kan nodig zijn om contact op te nemen met de CA-beheerder om te bepalen of deze een sjabloon heeft voor de tekenaanvraag.

iii. Kopieer het gehele certificaat inclusief het —BEGIN CERTIFICAAT VERZOEK— en —END CERTIFICAAT VERZOEK— en bewaar het vervolgens in een tekstbestand met de extensie .req.



Opmerking: Uw CA-beheerder vraagt om een andere bestandsextensie dan .req.

Optie 3: Een CA-certificaat en -toets importeren

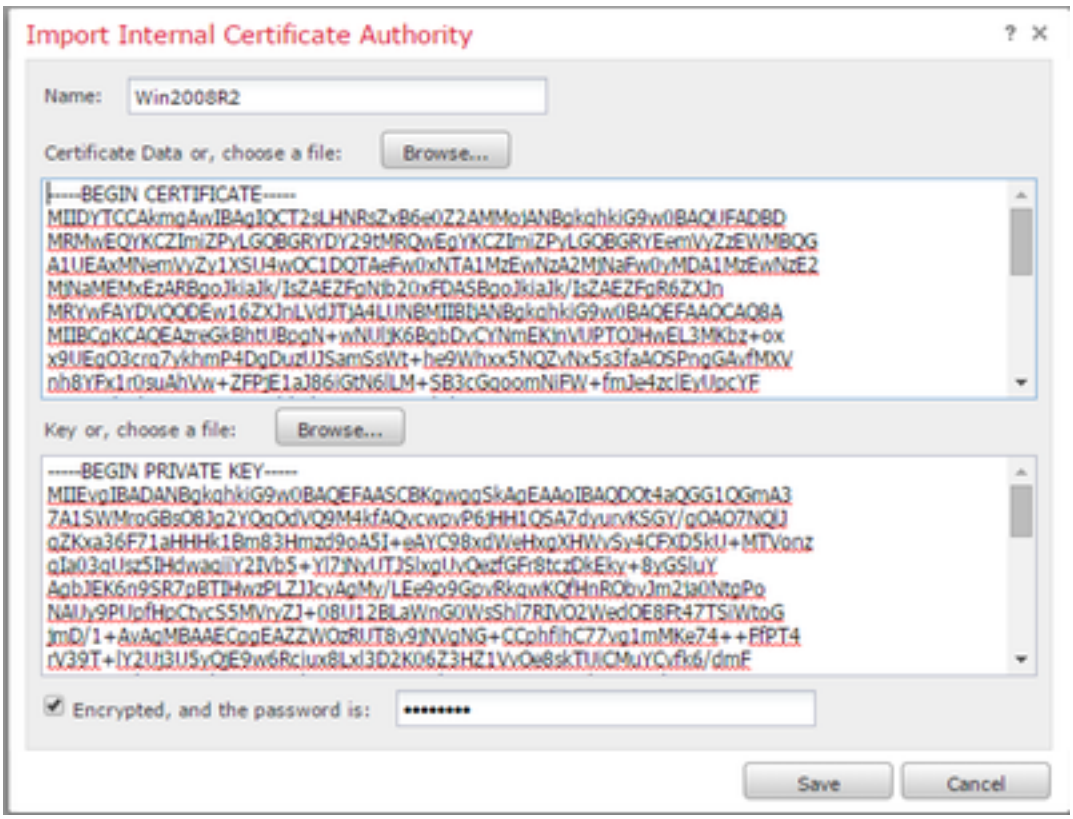


i. Klik op **CA importeren**.

ii. Bladeren naar of plakken in het certificaat.

iii. Bladeren naar of plakken in de privé-toets.

iv. Controleer het gecodeerde vakje en type in een wachtwoord.



Opmerking: Als er geen wachtwoord is, controleert u het gecodeerde vakje en laat u het leeg.

2. Ontcijferen met bekende sleutel

Bekend certificaat importeren (Alternatief voor decryptie en ontslag)

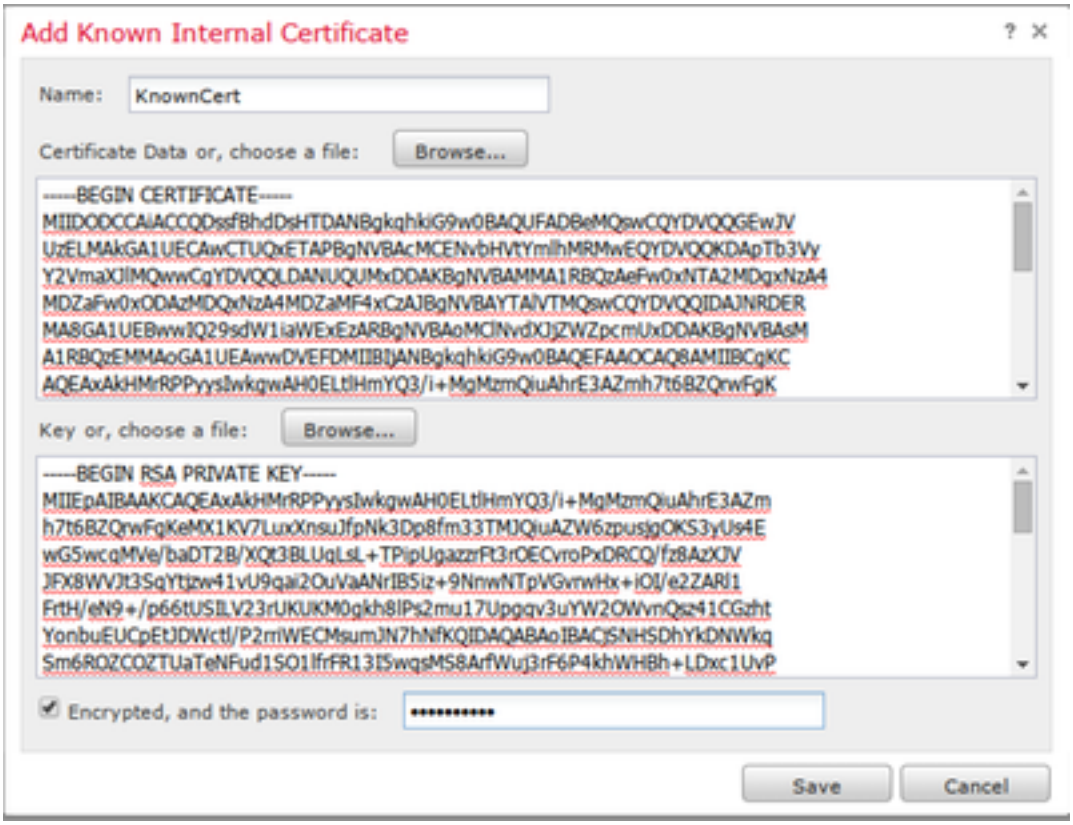
i. Vul PKI uit in de pagina Objects aan de linkerkant en selecteer Interne Certs.

ii. Klik op **Interne** waarschuwing **toevoegen**.

iii. Bladeren naar of plakken in het certificaat.

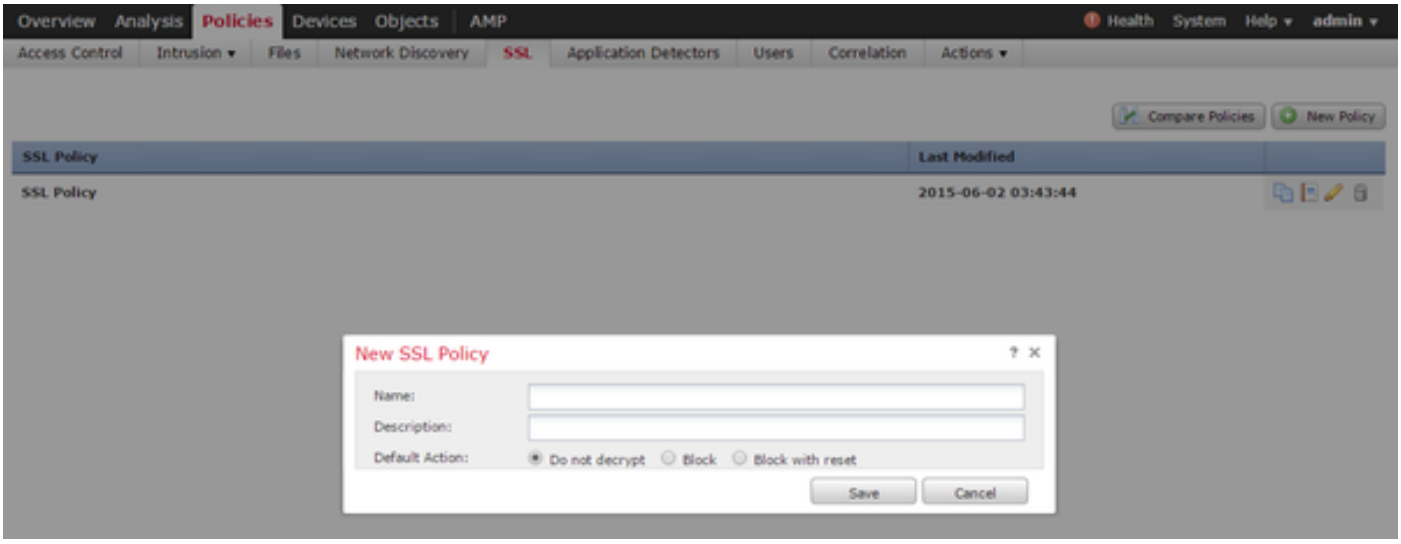
iv. Bladeren naar of plakken in de privé-toets.

v. Controleer het vakje **Encrypted** en voer een wachtwoord in.



Opmerking: Als er geen wachtwoord is, laat het vakje **Encrypted** leeg.

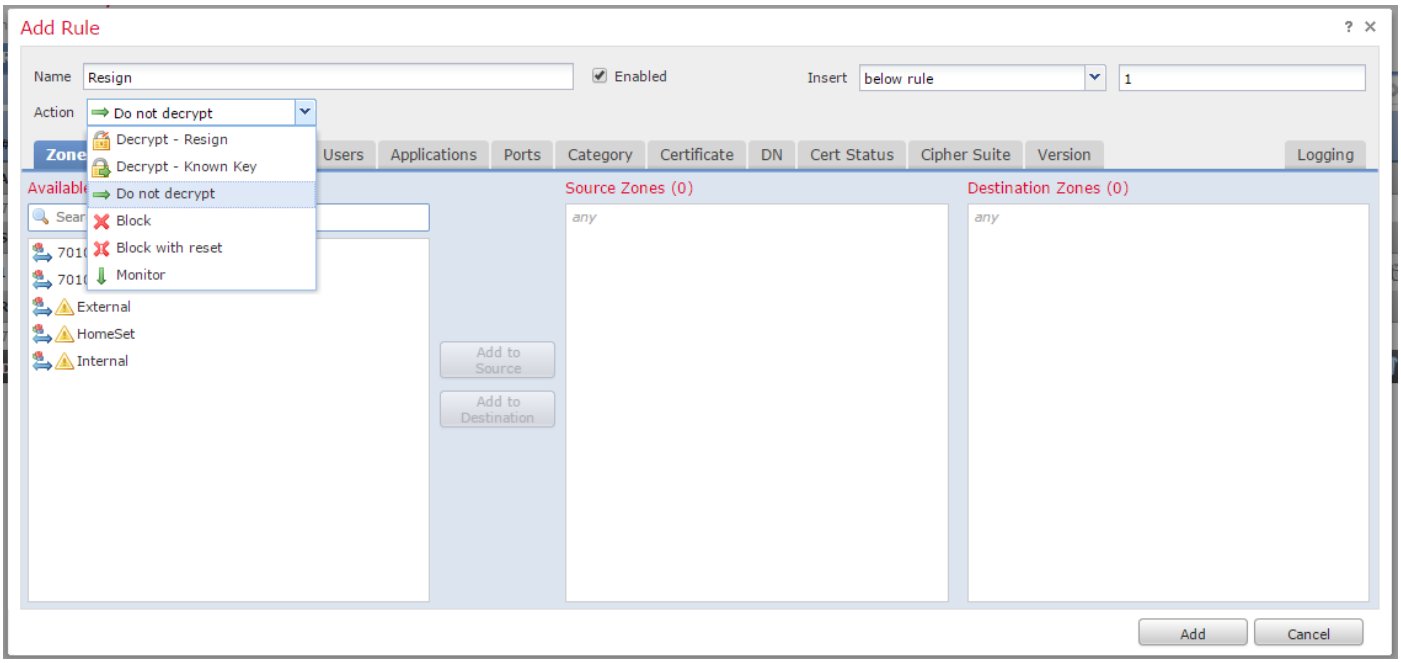
4. Navigeer naar **beleid > SSL** en klik vervolgens op **Nieuw beleid**.



5. Typ een naam en selecteer een **Standaardactie**. De SSL beleideditor pagina verschijnt. De SSL beleideditor pagina werkt hetzelfde als de hoofdpagina van de Access Control Policy.

> **Opmerking:** Als u niet zeker weet over de **Default Action**, is decrypt **niet** het aanbevolen startpunt.

6. Klik op de pagina SSL-beleidseditor op **Regel toevoegen**. Typ in het venster Regel toevoegen een naam voor de regel en vul alle andere relevante informatie in.



In het volgende gedeelte worden verschillende opties beschreven in het venster **Toevoegen regel**:

Handeling

decryptie - ontslag

- De sensor werkt als een Man in het Midden (MitM) en accepteert de verbinding met de gebruiker en maakt vervolgens een nieuwe verbinding met de server. Bijvoorbeeld: Gebruikerstypen in https://www.facebook.com in een browser. Het verkeer bereikt de sensor, de sensor onderhandelt met de gebruiker met het geselecteerde CA certificaat en SSL tunnel A is gebouwd. Tegelijkertijd verbindt de sensor zich met https://www.facebook.com en maakt hij SSL-tunnel B.
- Eindresultaat: De gebruiker ziet het certificaat in de regel, niet in de regel.

- Voor deze actie is een interne CA nodig. Selecteer Vervangen als u wilt dat de toets wordt vervangen. De gebruiker ontvangt het geselecteerde certificaat.

  Opmerking: Dit kan niet in passieve modus worden gebruikt.

Decryptie - bekende sleutel

- De sensor heeft de sleutel die gebruikt zal worden om het verkeer te decrypteren. Bijvoorbeeld: Gebruikerstypen in https://www.facebook.com in een browser. Het verkeer bereikt de sensor, de sensor ontsleutelt het verkeer en inspecteert het verkeer.
- Eindresultaat: Zie het certificaat van het Faceboek
- Voor deze actie is een intern certificaat vereist. Dit wordt toegevoegd in **Objects** > **PKI** >**Interne Certs**.

  Opmerking: Uw organisatie moet eigenaar zijn van het domein en het certificaat. Bijvoorbeeld facebook.com de enige mogelijke manier om de eindgebruiker het certificaat van facebook te laten zien is als je het domein facebook.com (d.w.z. je bedrijf is Facebook, Inc.) bezitten en het facebook.com certificaat bezitten, ondertekend door een publiek CA. U kunt alleen decrypteren met bekende sleutels voor sites die uw organisatie bezit.

Het belangrijkste doel van de decrypt bekende sleutel is om verkeersgeleiding naar uw https server te decrypteren om uw servers tegen externe aanvallen te beschermen. Voor het inspecteren van client zijverkeer naar externe https-sites gebruikt u decrypt resignatuur omdat u de server niet bezit en u bent geïnteresseerd in het inspecteren van client verkeer in uw netwerk dat aansluit op externe gecodeerde sites.

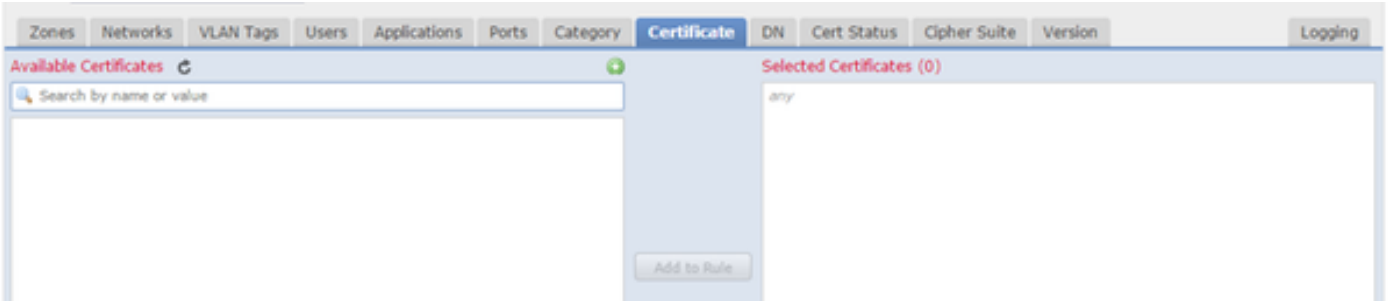
Opmerking: Voor DHE en ECDHE om te decrypteren moeten we in de rij staan.

Niet decrypteren

Het verkeer passeert het SSL beleid en blijft het beleid van de Toegangscontrole voortzetten.

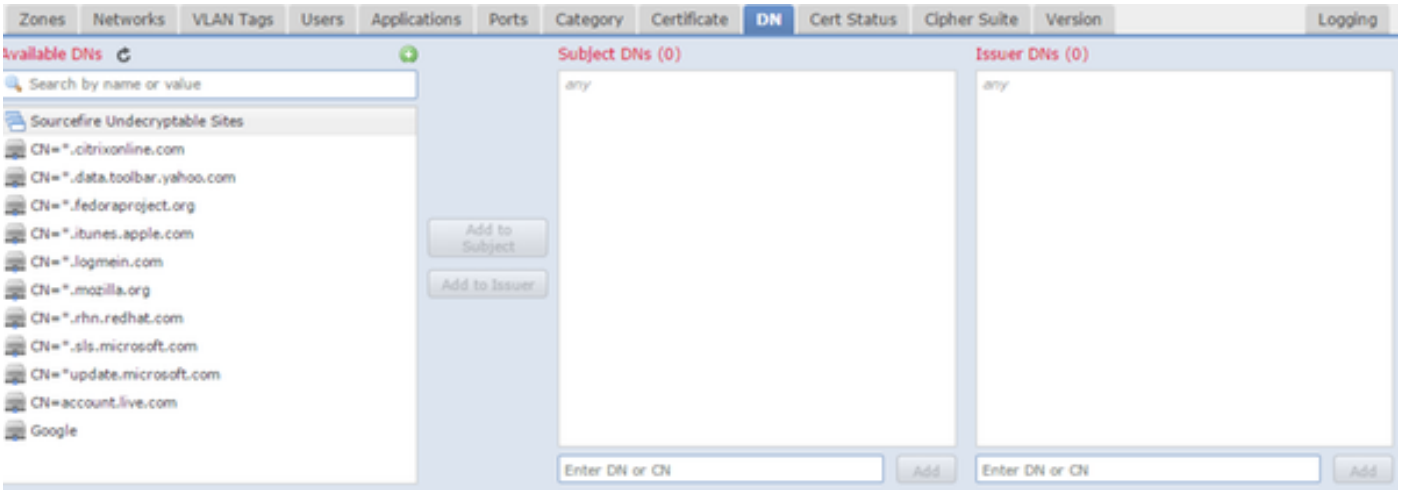
Certificaat

De regel past SSL verkeer met dit specifieke certificaat aan.



DN

De regel past SSL verkeer toe die bepaalde Namen van het Domein in de certificaten gebruikt.

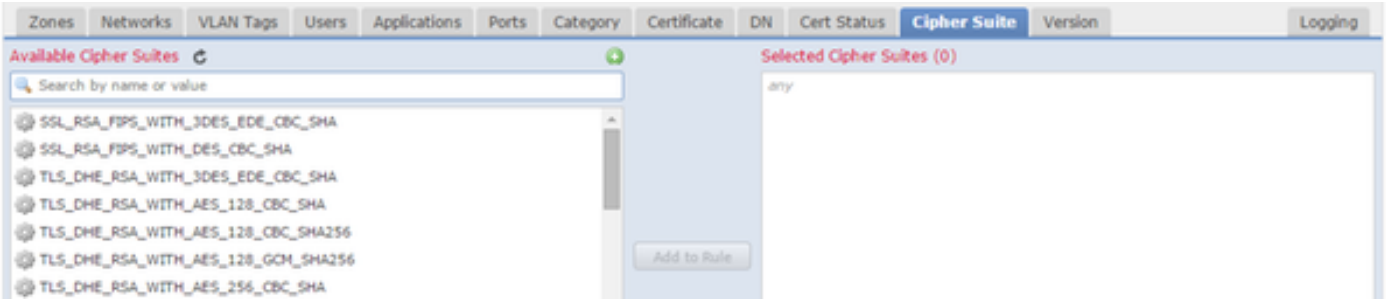


Status weergeven

De regel past SSL verkeer met deze status van het certificaat aan.

Computer Suite

De regel past SSL verkeer toe met deze Klanten van het Kind.



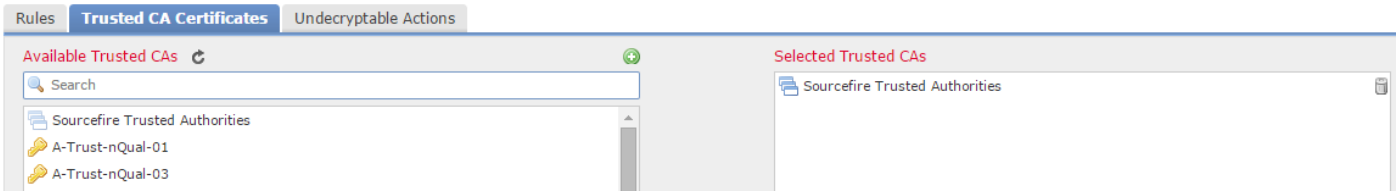
Versie

De regels zijn alleen van toepassing op SSL-verkeer met de geselecteerde versies van SSL.

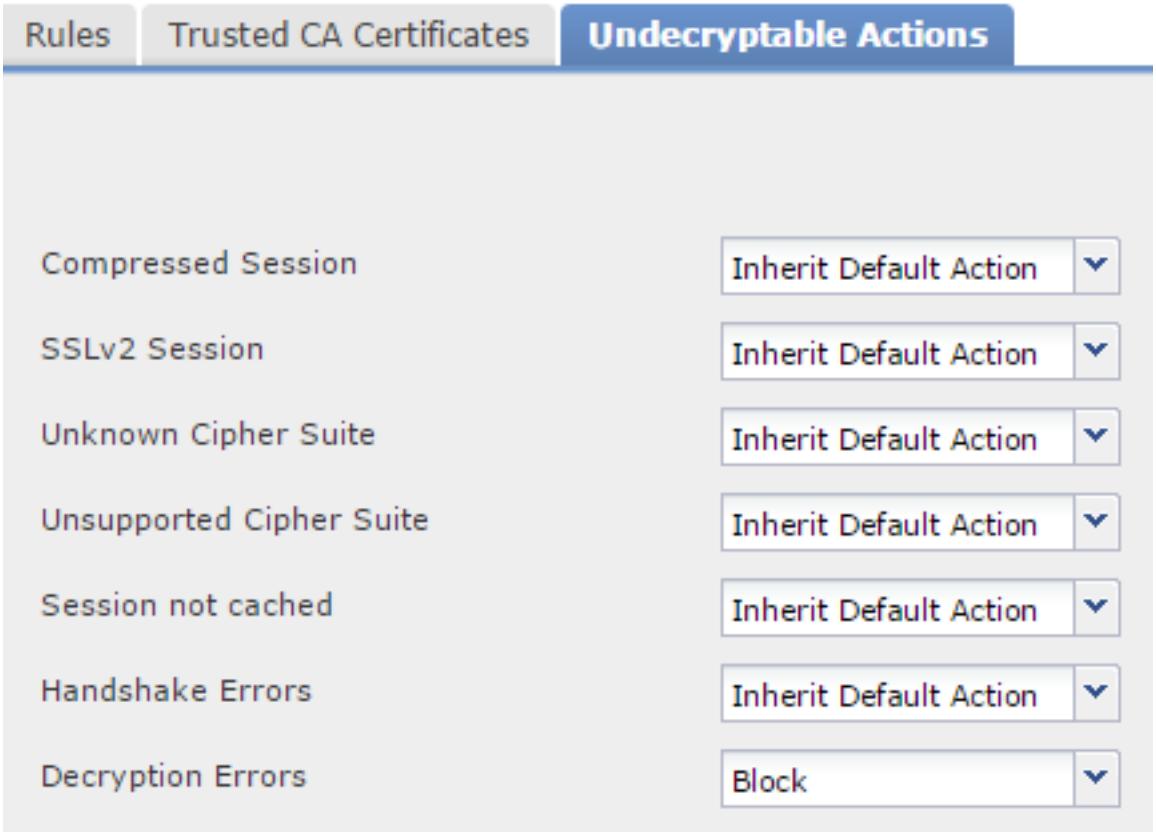
Vastlegging

Schakel loggen in om verbindingsgebeurtenissen voor het SSL-verkeer te zien.

7. Klik op **Vertrouwd CA-certificaat**. Dit is waar Trusted CA aan het beleid wordt toegevoegd.



8. Klik op **ondecrypteerbare acties**. Hier zijn de acties waarvoor de sensor het verkeer niet kan decrypteren. U vindt de definities van de online hulp (**Help > Online**) van het FireSIGHT Management Center.



- **Samengeperste sessie**: De SSL sessie past een gegevenscompressiemethode toe.
- **SSLv2-sessie**: De sessie is versleuteld met SSL versie 2. Merk op dat verkeer decrypteerbaar is als het bericht van de client is SSL 2.0 en de rest van het overgedragen verkeer SSL 3.0 is.
- **Onbekende Cipher Suite**: Het systeem herkent de zoekreeks niet.
- **Niet-ondersteunde coderingssysteem**: Het systeem ondersteunt geen decryptie op basis van

de gedetecteerde algoritme suite.

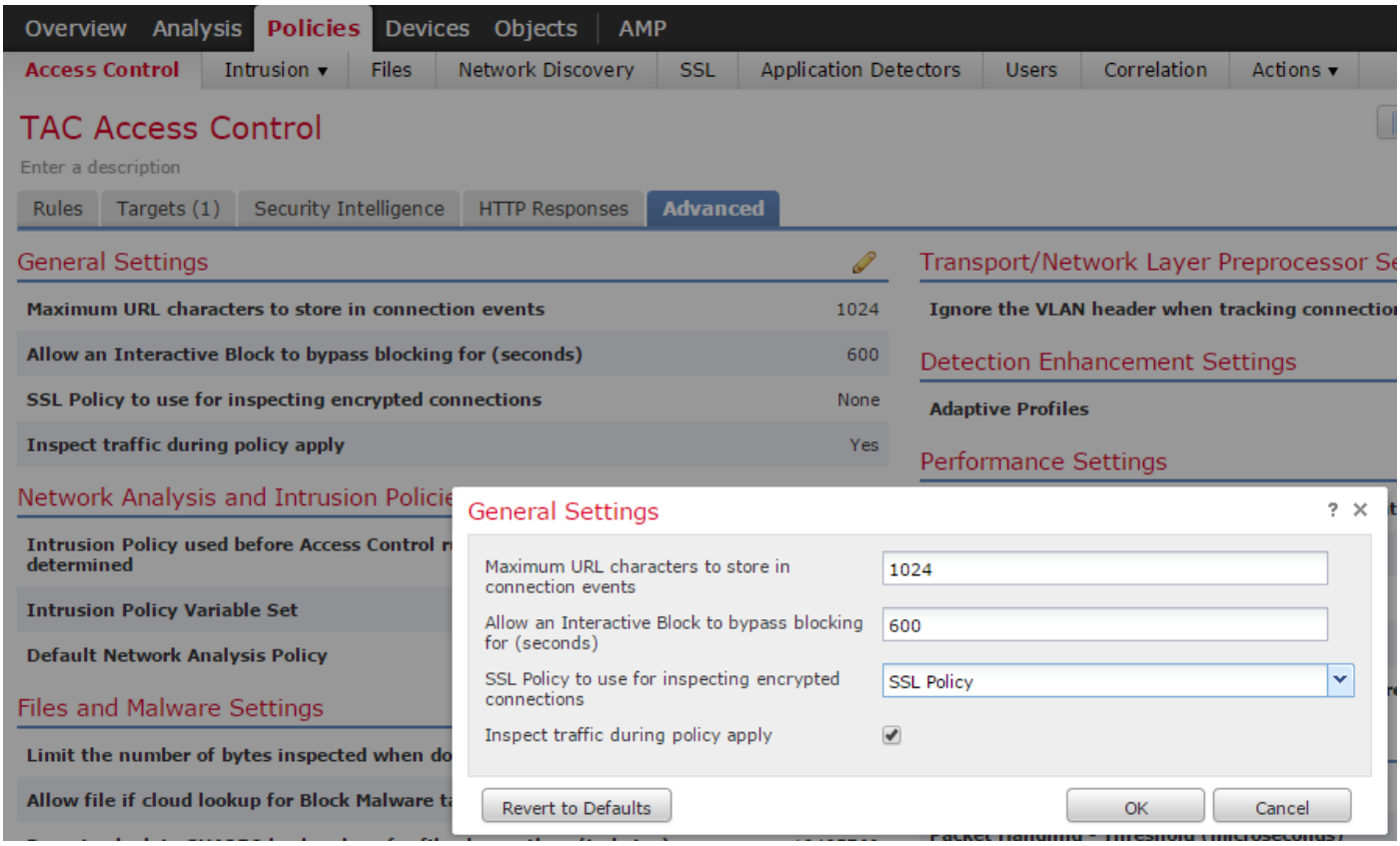
- **Session niet gecached**: De SSL sessie heeft hergebruik van sessie mogelijk gemaakt, de client en server herstelde de sessie met de sessie identificator, en het systeem heeft die sessie identificator niet in het geheugen gegrift.
- **Handdruk**: Een fout is opgetreden tijdens de SSL-handdruk tijdens de onderhandeling.
- **Versleuteling van fouten**: Een fout is opgetreden tijdens verkeersdecryptie.

Opmerking: Standaard erven deze de Standaardactie. Als uw standaardopdracht blokkeert, kunt u onverwachte problemen krijgen

9. Bespaar het beleid.

10. Navigeer naar **beleid > Toegangsbeheer**. Bewerk uw beleid of maak een nieuw toegangscontrolebeleid.

1. Klik op **Geavanceerd** en bevestig de **algemene instellingen**.



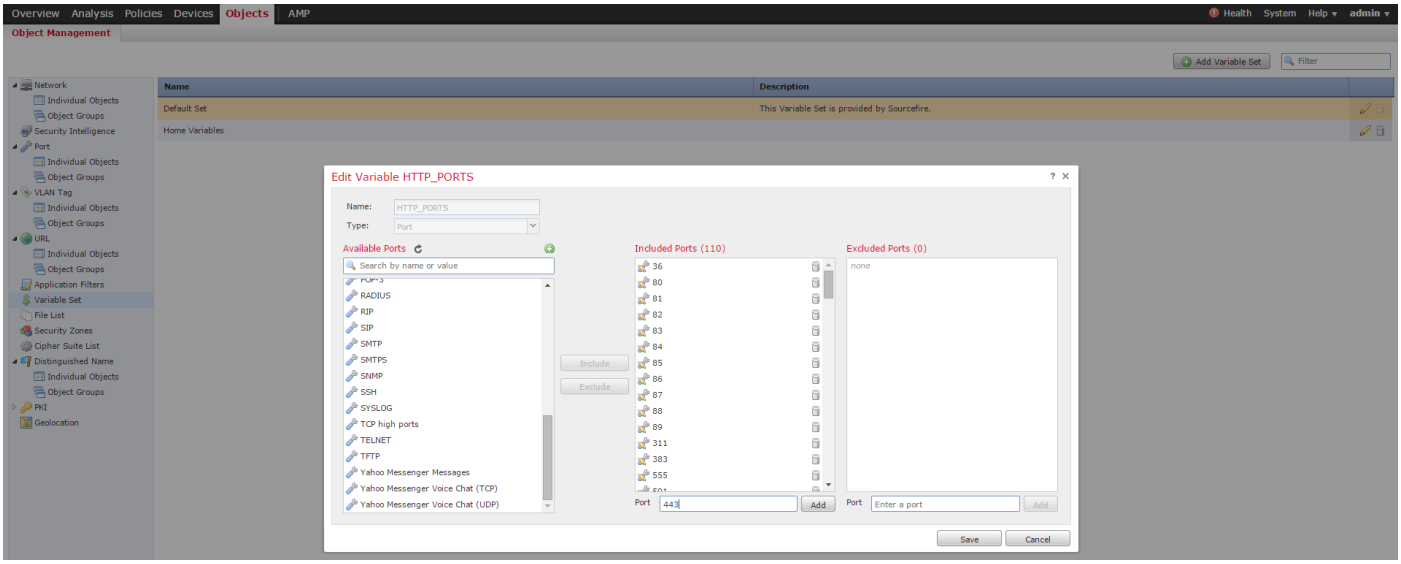
12. Selecteer in het uitrolmenu uw **SSL-beleid**.

13. Klik op **OK** om op te slaan.

Aanvullende configuraties

Het inbraakbeleid moet voor een goede identificatie de volgende wijzigingen ondergaan:

i. Uw variabele $HTTP_PORTS moet poort 443 en andere poorten met https-verkeer omvatten die door uw beleid zullen worden gedecrypteerd (**Objecten > Objectbeheer > Variable Set > Bewerken de variabele set).**



ii. Het beleid voor netwerkanalyse dat het gecodeerde verkeer inspecteert moet poort 443 (en alle andere poorten met https-verkeer die door uw beleid zullen worden gedecrypteerd) hebben die in het veld havens van de HTTP preprocessor instellingen zijn opgenomen, anders zal geen van de http regels met http content modificatoren (d.w.z. http_uri, http_header, etc.) veroorzaken omdat dit afhankelijk is van de http poorten en http buffers in snort zullen niet worden ingevuld voor verkeer dat niet over de aangegeven poorten gaat.

iii. (Optioneel maar aanbevolen voor een betere inspectie) Voeg uw https-poorten toe aan de instellingen van **TCP-stream** in het **veld** Stream **Reassembleren uitvoeren op beide poorten**.

iv. Pas het herziene Access Control-beleid opnieuw toe tijdens een gepland onderhoudsvenster.

> **Waarschuwing:** dit gewijzigde beleid kan belangrijke prestatiekwesties veroorzaken. Dit moet buiten de productieuren worden getest om het risico op netwerkstoringen of -prestaties te verminderen.

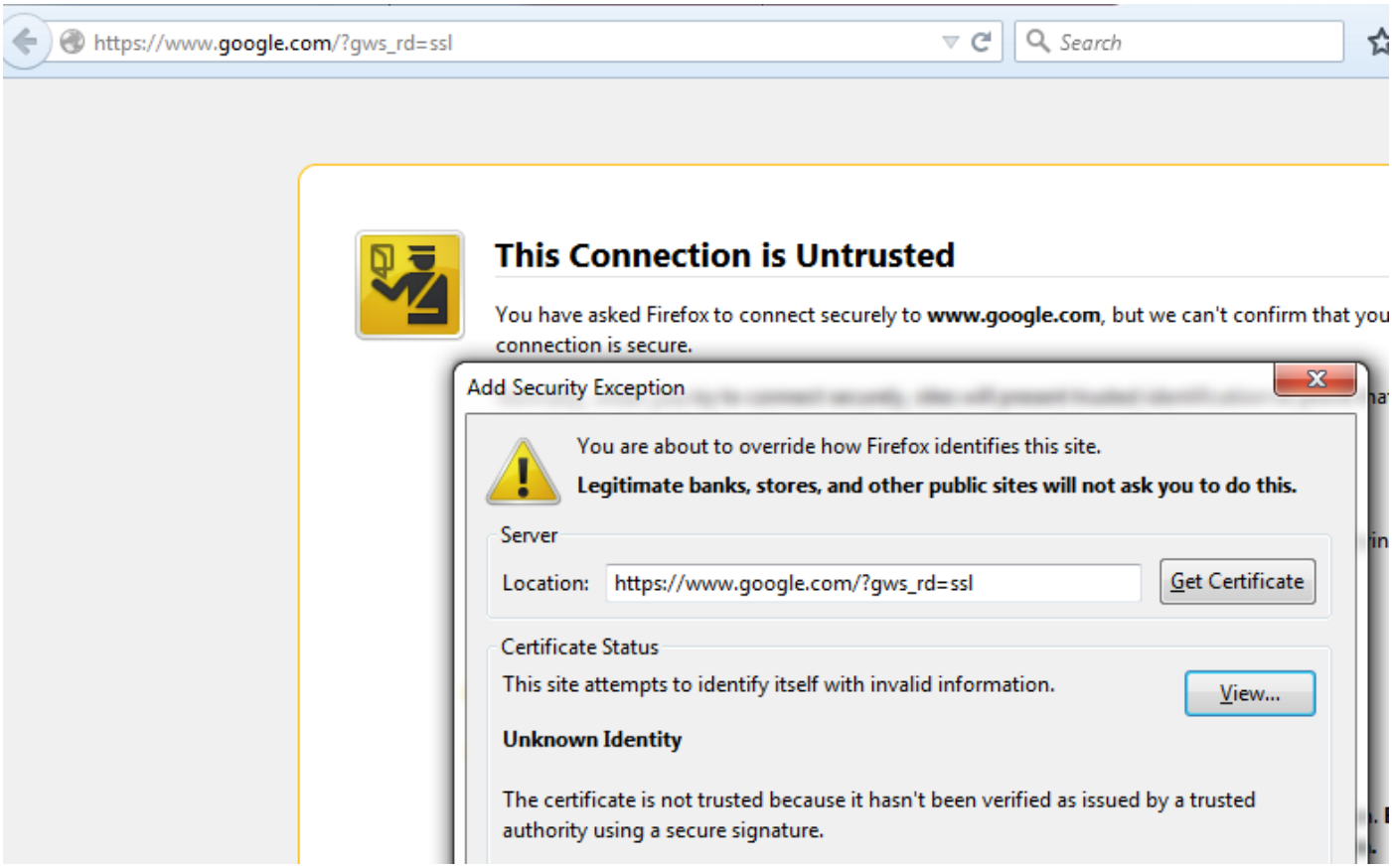
Verificatie

decryptie - ontslag

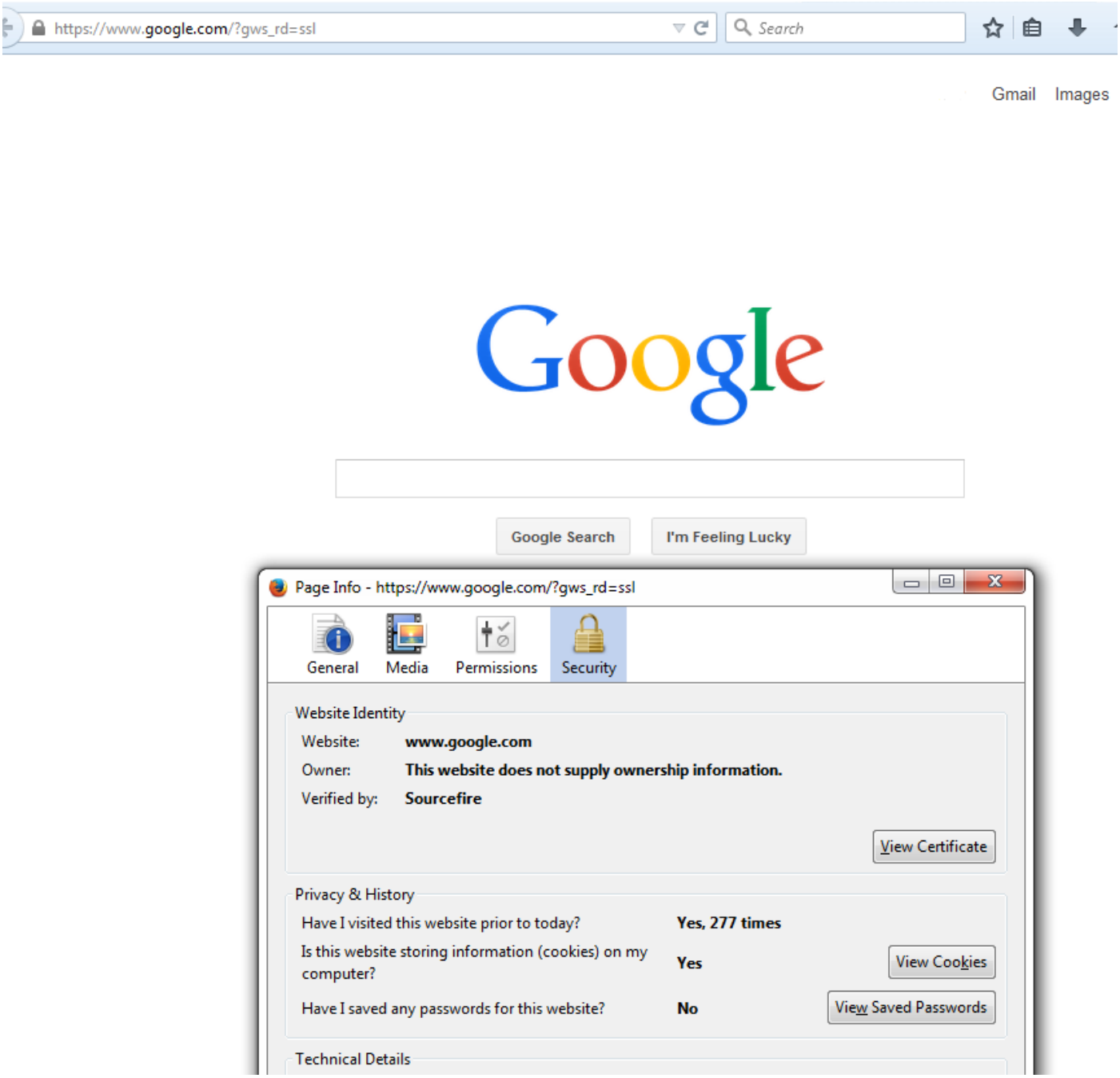
1. Open een webbrowser.

> **Opmerking:** De browser Firefox wordt in het onderstaande voorbeeld gebruikt. Dit voorbeeld werkt misschien niet in Chrome. Zie het gedeelte Problemen oplossen voor meer informatie.

2. Blader naar een SSL-website. In het onderstaande voorbeeld https://www.google.com wordt gebruikt, zullen ook de websites van financiële instellingen werken. U ziet een van de volgende pagina's:



Opmerking:U ziet de bovenstaande pagina als het certificaat zelf niet wordt vertrouwd en het ondertekenende CA-certificaat niet wordt vertrouwd door uw browser. Om te weten te komen hoe browser vertrouwde CA certificaten bepaalt zie de sectie van de Trusted certificaatautoriteiten hieronder.



Opmerking: Als deze pagina wordt gezien, hebt u het verkeer opnieuw getekend. Noteer het gedeelte **Geverifieerd door: Sourcefire**.

Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	www.google.com
Organization (O)	Google Inc
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	13:E3:D5:7D:4E:5F:8F:E7

Issued By

Common Name (CN)	Sourcefire TAC
Organization (O)	Sourcefire
Organizational Unit (OU)	Tac

Period of Validity

Begins On	5/6/2015
Expires On	8/3/2015

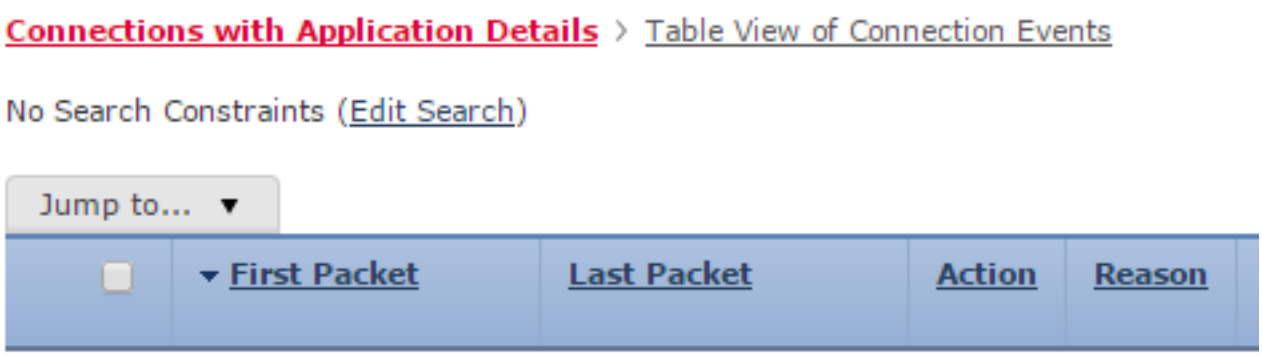
Fingerprints

SHA-256 Fingerprint	20:00:CB:25:13:8B:1F:89:4D:4A:CF:C5:E2:21:38:92: 06:66:00:2E:B7:83:27:72:98:EA:B1:6A:10:B3:67:A1
SHA1 Fingerprint	1B:C2:30:D9:66:84:DB:97:CF:A9:5E:5F:29:DA:4C:3F:13:E9:DE:5D

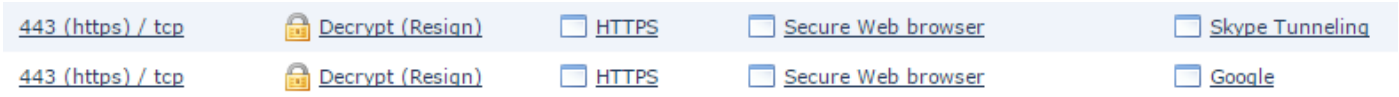
Opmerking: Dit is een close-up kijk naar hetzelfde certificaat.

3. Ga in het Management Center naar **Analyse > Connecties > Evenementen**.

4. Afhankelijk van uw werkschema kan of mag u SSL-decryptie optie al dan niet zien. Klik op **Tabelweergave van verbindingsgebeurtenissen**.



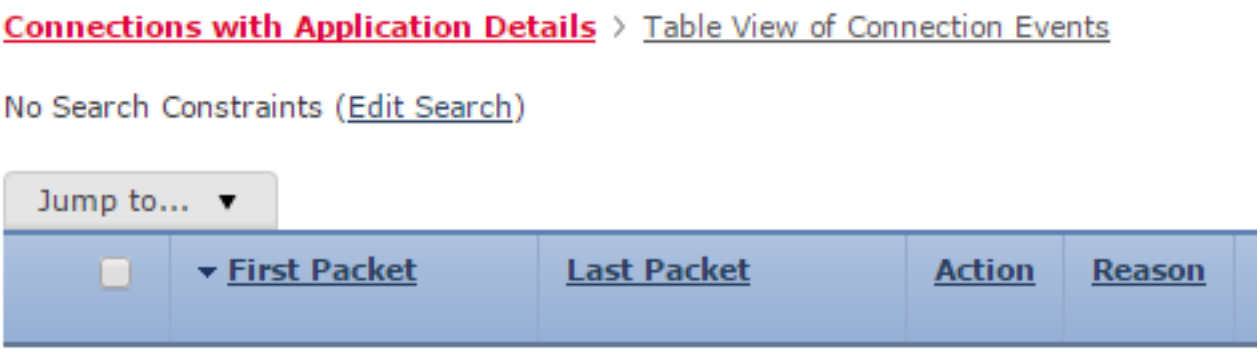
5. Scrolt naar rechts en zoek de SSL-status. U dient opties zoals hieronder te zien:



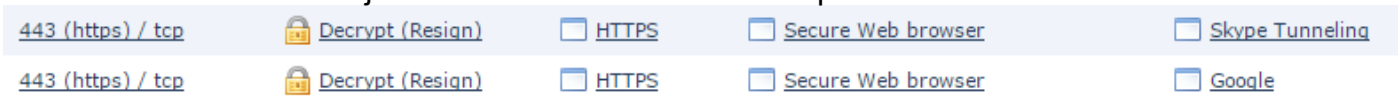
decryptie - bekend certificaat

1. Navigeer in het FireSIGHT Management Center naar **Analyse > Connecties > evenementen**.

2. Afhankelijk van uw werkschema, kunt u de SSL decrypt optie al dan niet zien. Klik op **Tabelweergave van verbindingsgebeurtenissen**.



3. Scrolt naar rechts en kijk naar de SSL-status. U dient opties zoals hieronder te zien:



Probleemoplossing

Vraag 1: Sommige websites laden mogelijk niet op de browser Chrome

Voorbeeld

www.google.com kan niet laden met een decrypt - Aftreden met Chrome.

reden

De browser Google Chrome kan frauduleuze certificaten voor Google-eigenschappen detecteren om aanvallen van mensen in het midden te voorkomen. Als de browser Chrome (client) probeert verbinding te maken met een google.com domein (server) en een certificaat wordt teruggegeven dat geen geldig Google certificaat is, ontkent de browser de verbinding.

Oplossing

Als u dit ervaart, voeg een **Do not Decrypt** regel toe voor DN=*.google.com, *.gmail.com, *.youtube.com. Maak de browser cache en geschiedenis los.

Onderdeel 2: Een onvertrouwde waarschuwing/fout in bepaalde browsers verkrijgen

Voorbeeld

Wanneer u een verbinding maakt met een site via Internet Explorer en Chrome, ontvangt u geen veiligheidswaarschuwing, maar wanneer u een browser Firefox gebruikt, moet u de verbinding vertrouwen telkens wanneer u de browser sluit en heropent.

reden

De lijst van vertrouwde CA's is afhankelijk van de browser. Wanneer u een certificaat vertrouwt, creëert dit niet voor alle browsers en het vertrouwde bericht blijft doorgaans alleen bestaan terwijl de browser geopend is. Zodra het certificaat is gesloten, worden alle certificaten die vertrouwd waren, afgedrukt en moet u de volgende keer dat u de browser opent en de site bezoekt, de site opnieuw toevoegen aan de lijst met vertrouwde certificaten.

Oplossing

In dit scenario gebruiken zowel IE als Chrome de lijst van vertrouwde CA's in het besturingssysteem, maar Firefox handhaaft zijn eigen lijst. Het CA cert werd geïmporteerd in de OS-winkel maar werd niet geïmporteerd in de Firefox-browser. Om de veiligheidswaarschuwing in Firefox te vermijden moet u de CA cert in de browser importeren als een vertrouwde CA.

Trusted certificaatautoriteiten

Wanneer een SSL-verbinding wordt gemaakt, controleert de browser eerst of dit certificaat wordt vertrouwd (d.w.z. u hebt vóór en handmatig aan de browser gevraagd om dit certificaat te vertrouwen). Als het certificaat niet wordt vertrouwd aan de browser, dan controleert u het certificaat van de certificaatinstantie (CA) dat het certificaat voor deze site heeft geverifieerd. Als het CA certificaat door de browser wordt vertrouwd, beschouwt het het als een betrouwbaar certificaat en staat het de verbinding toe. Als het CA-certificaat niet wordt vertrouwd, geeft de browser een beveiligingswaarschuwing weer en dwingt u het certificaat handmatig toe te voegen als een betrouwbaar certificaat.

De lijst van vertrouwde CA's in een browser is volledig afhankelijk van de implementatie van de makelaar en elke browser kan de vertrouwde lijst anders bevolken dan andere browsers. In het algemeen zijn er 2 manieren waarop de huidige browsers een lijst van vertrouwde CA's bevolken:

1. Ze gebruiken de lijst van vertrouwde CA's die het besturingssysteem beheerst
2. Ze verzenden een lijst met vertrouwde CA's met de software en het is ingebouwd in de browser.

Voor de meest gebruikelijke browsers worden de vertrouwde CA's als volgt ingevuld:

- **Google Chrome**: De vertrouwde CA-lijst van het besturingssysteem
- **Firefox**: Hiermee blijft de eigen vertrouwde CA-lijst behouden
- **Internet Explorer**: De vertrouwde CA-lijst van het besturingssysteem
- **Safari**: De vertrouwde CA-lijst van het besturingssysteem

Het is belangrijk om het verschil te weten, omdat het gedrag dat op de cliënt wordt gezien, hiervan afhangt. Om bijvoorbeeld een vertrouwde CA voor Chrome en IE toe te voegen, moet u het CA-certificaat importeren naar de vertrouwde CA-winkel van het besturingssysteem. Als u het CA-certificaat importeert naar de vertrouwde CA-winkel van het besturingssysteem, krijgt u geen

waarschuwing meer bij de aansluiting op sites met een certificaat dat door dit CA is ondertekend. In de browser Firefox moet u het CA certificaat handmatig importeren in de vertrouwde CA winkel in de browser zelf. Nadat u dit hebt gedaan, krijgt u geen veiligheidswaarschuwing meer wanneer u verbinding maakt met sites die door die CA zijn geverifieerd.

Referenties

- Aan de slag met SSL-regels