Konfiguration einer SSL-Überprüfungsrichtlinie für das Cisco FireSIGHT-System

Inhalt

Einführung

Mit der SSL-Überprüfungsfunktion können Sie verschlüsselten Datenverkehr blockieren, ohne ihn zu überprüfen, oder verschlüsselten oder entschlüsselten Datenverkehr mit Zugriffskontrolle überprüfen. In diesem Dokument werden die Konfigurationsschritte zum Einrichten einer SSL-Überprüfungsrichtlinie für das Cisco FireSIGHT-System beschrieben.

Voraussetzungen

Verwendete Komponenten

- Cisco FireSIGHT Management Center
- Cisco FirePOWER-Appliances der Serien 7000 oder 8000
- Softwareversion 5.4.1 oder höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die

mögliche Auswirkung jedes möglichen Befehls verstehen.

> **Warnung:** Wenn Sie eine SSL-Überprüfungsrichtlinie auf Ihrem verwalteten Gerät anwenden, kann dies die Netzwerkleistung beeinträchtigen.

Konfigurationen

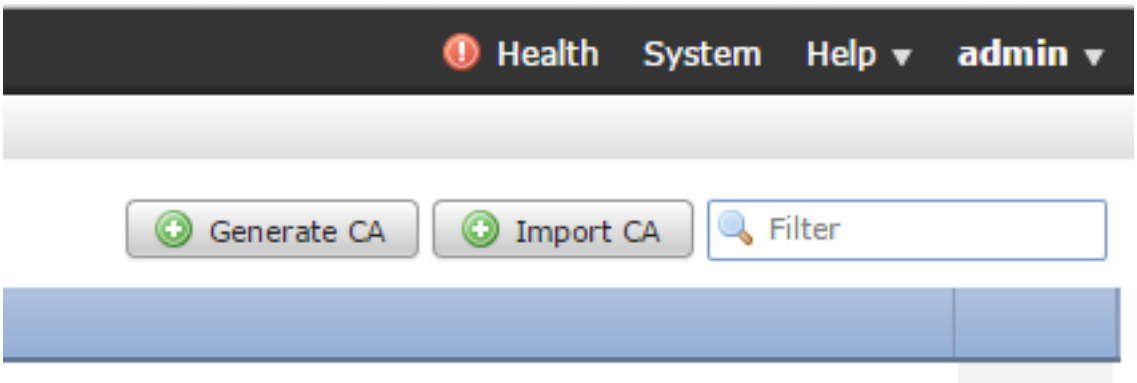
Sie können eine SSL-Überprüfungsrichtlinie folgendermaßen konfigurieren, um Datenverkehr zu entschlüsseln:

1. Entschlüsseln und Rückzeichnen:
   - Option 1: Verwenden Sie das FireSIGHT Center als Stammzertifizierungsstelle (Certificate Authority, CA), oder
   - Option 2: eine interne Zertifizierungsstelle haben, die Ihr Zertifikat signiert, oder
   - Option 3: Importieren eines Zertifizierungsstellenzertifikats und -schlüssels
2. Entschlüsseln mit einem bekannten Zertifikat:
   - Melden Sie sich beim FireSIGHT Management Center an, und navigieren Sie dann zu **Objects**.
   - Erweitern Sie auf der Seite **Objekte** die **PKI**, und wählen Sie **Interne CAs aus**.

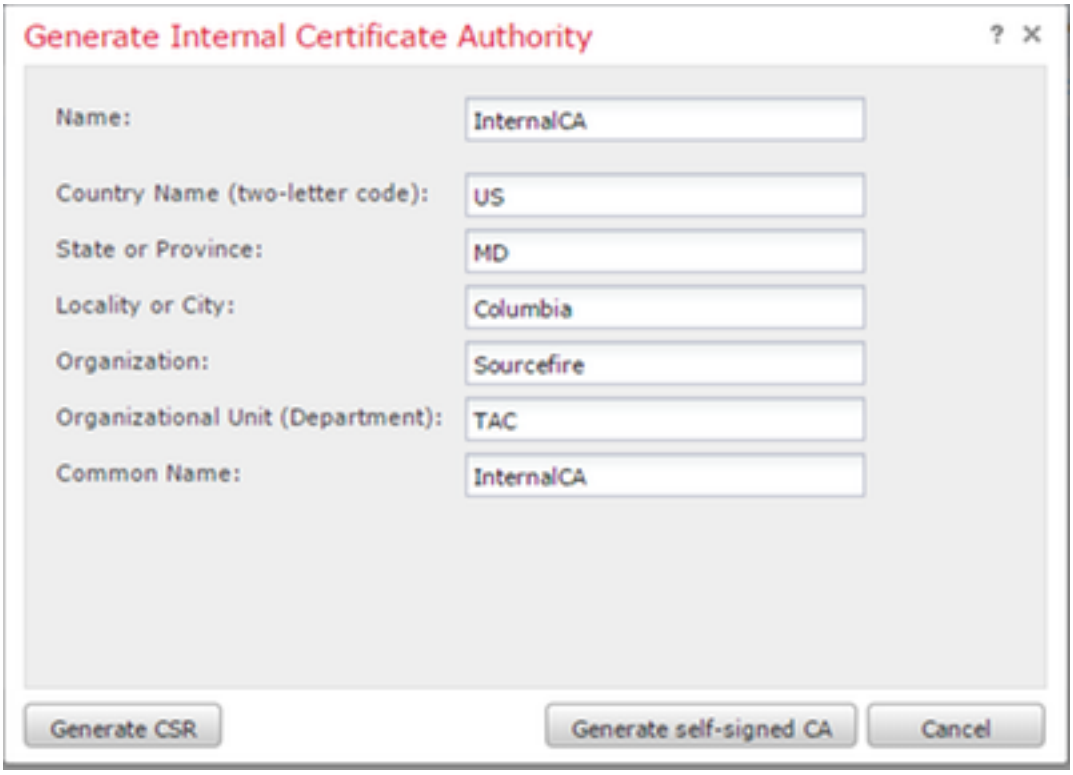
1. Entschlüsseln und Rückzeichnen

Option 1: Verwenden des FireSIGHT Center als Stammzertifizierungsstelle (Certificate Authority, CA)

i. Klicken Sie auf **CA generieren**.



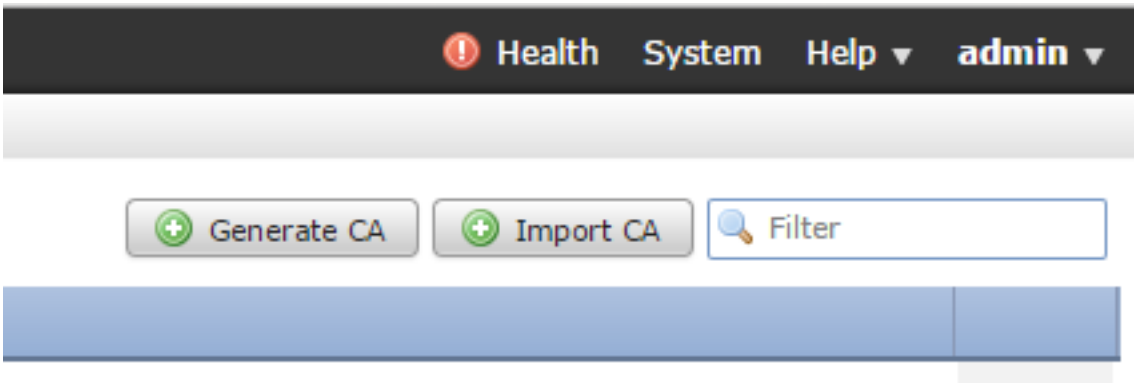
ii) Geben Sie die relevanten Informationen ein.



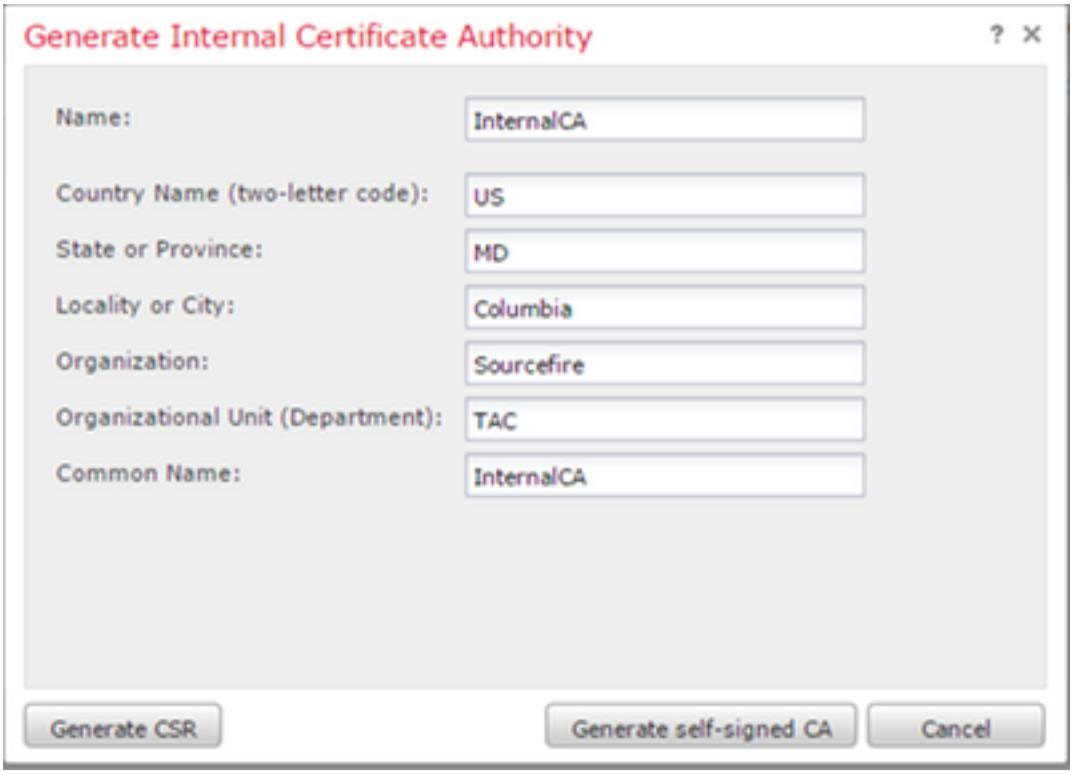
iii) Klicken Sie auf **Eigensignierte CA generieren**.

Option 2: Signieren Sie Ihr Zertifikat mit einer internen Zertifizierungsstelle.

i. Klicken Sie auf **CA generieren**.

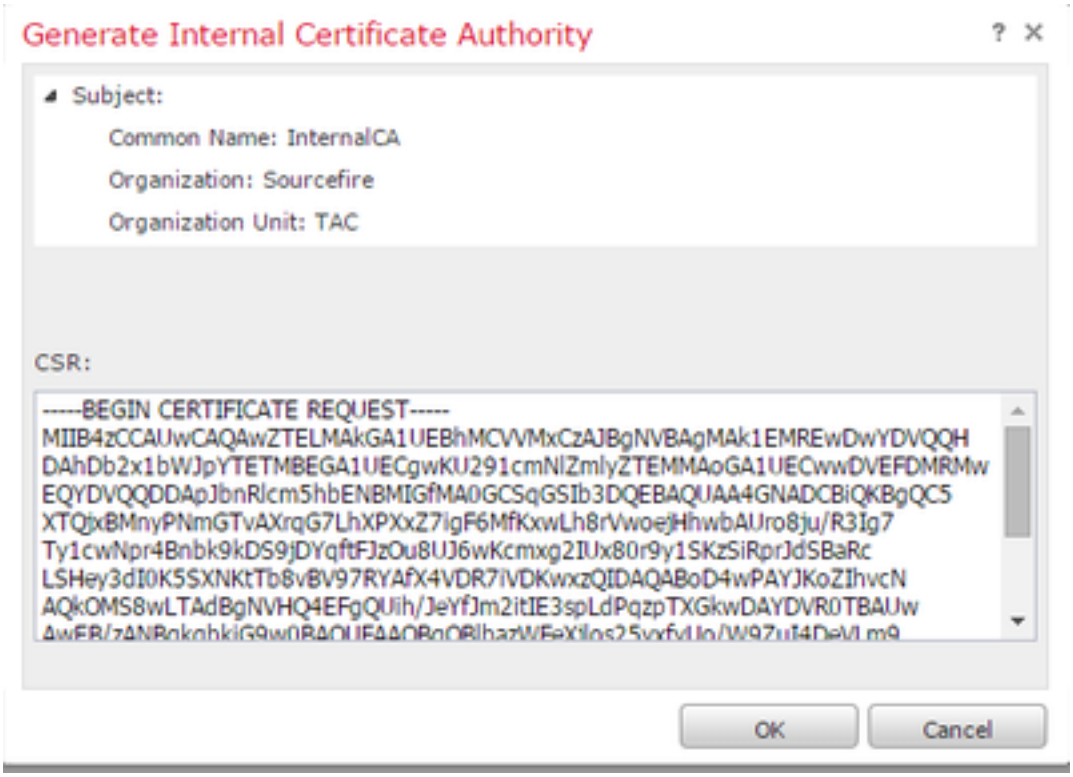


ii) Geben Sie die relevanten Informationen ein.



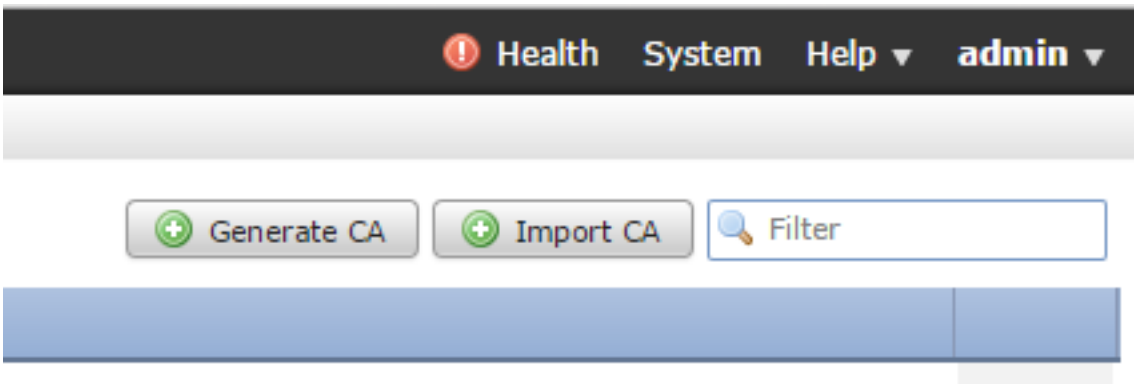
Hinweis: Wenden Sie sich an den Administrator der Zertifizierungsstelle, um festzustellen, ob eine Vorlage für die Signierungsanfrage vorhanden ist.

iii) Kopieren Sie das gesamte Zertifikat einschließlich der - BEGIN CERTIFICATE REQUEST - und —END CERTIFICATE REQUEST - und speichern Sie es dann in einer Textdatei mit der Erweiterung .req.



Hinweis: Ihr CA-Administrator bittet um eine weitere Dateierweiterung neben .req.

Option 3: Importieren eines Zertifizierungsstellenzertifikats und -schlüssels

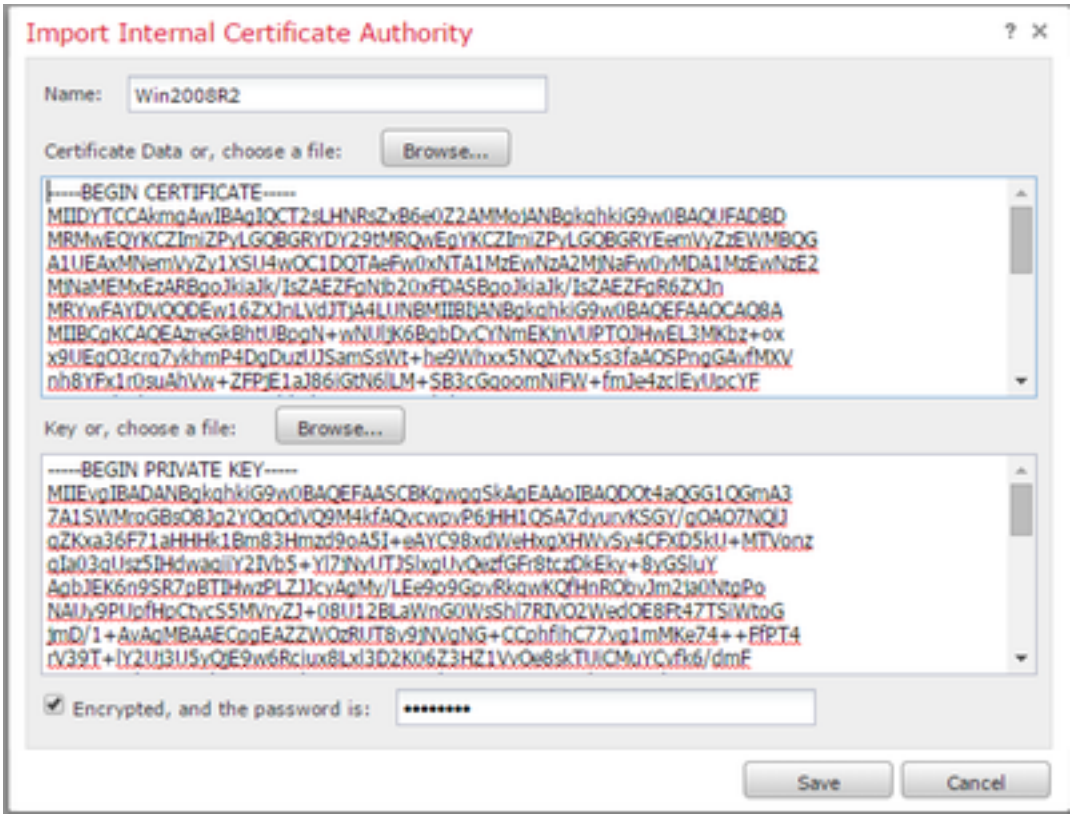


i. Klicken Sie auf **CA importieren**.

ii) Suchen Sie das Zertifikat, oder fügen Sie es ein.

iii) Navigieren Sie zum privaten Schlüssel, oder fügen Sie ihn ein.

iv) Aktivieren Sie das verschlüsselte Feld, und geben Sie ein Kennwort ein.



Hinweis: Wenn kein Kennwort vorhanden ist, aktivieren Sie das verschlüsselte Feld, und lassen Sie es leer.

2. Entschlüsseln mit einem bekannten Schlüssel

Importieren eines bekannten Zertifikats (Alternative zum Entschlüsseln und Zurücksetzen)

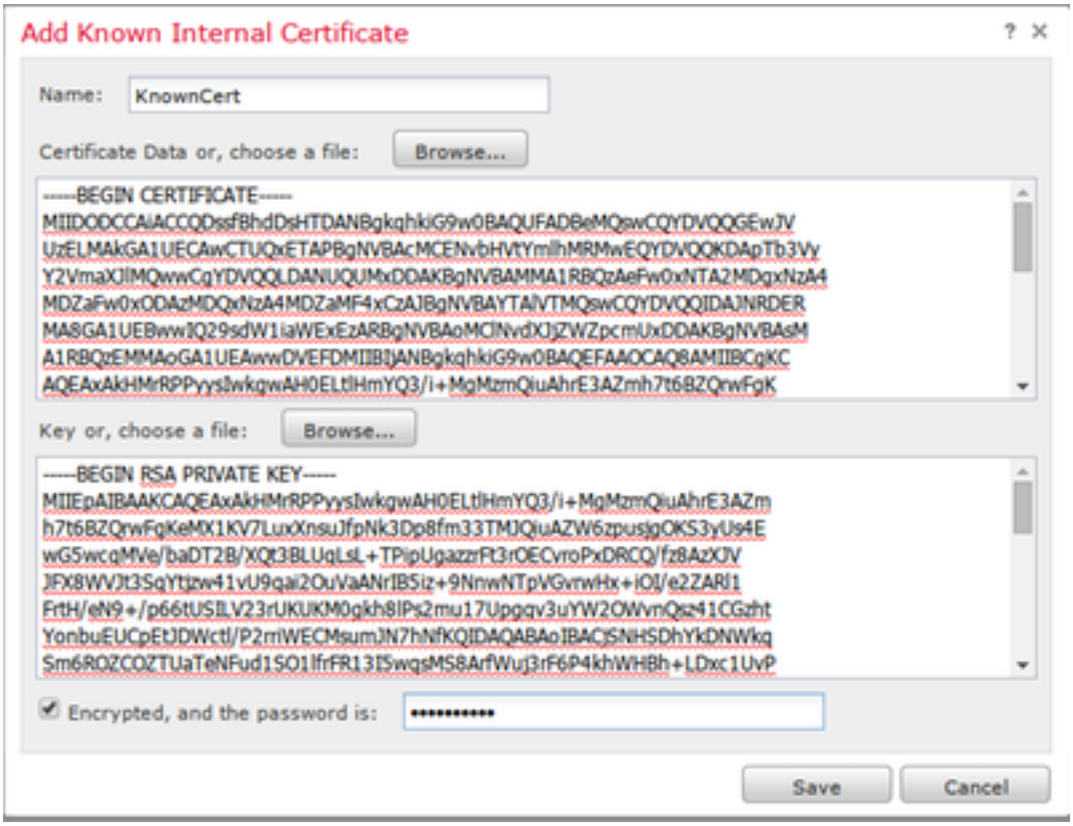
i. Erweitern Sie auf der Seite Objekte auf der linken Seite PKI, und wählen Sie Interne Zertifikate aus.

ii) Klicken Sie auf **Internes Zertifikat hinzufügen**.

iii) Suchen Sie das Zertifikat, oder fügen Sie es ein.

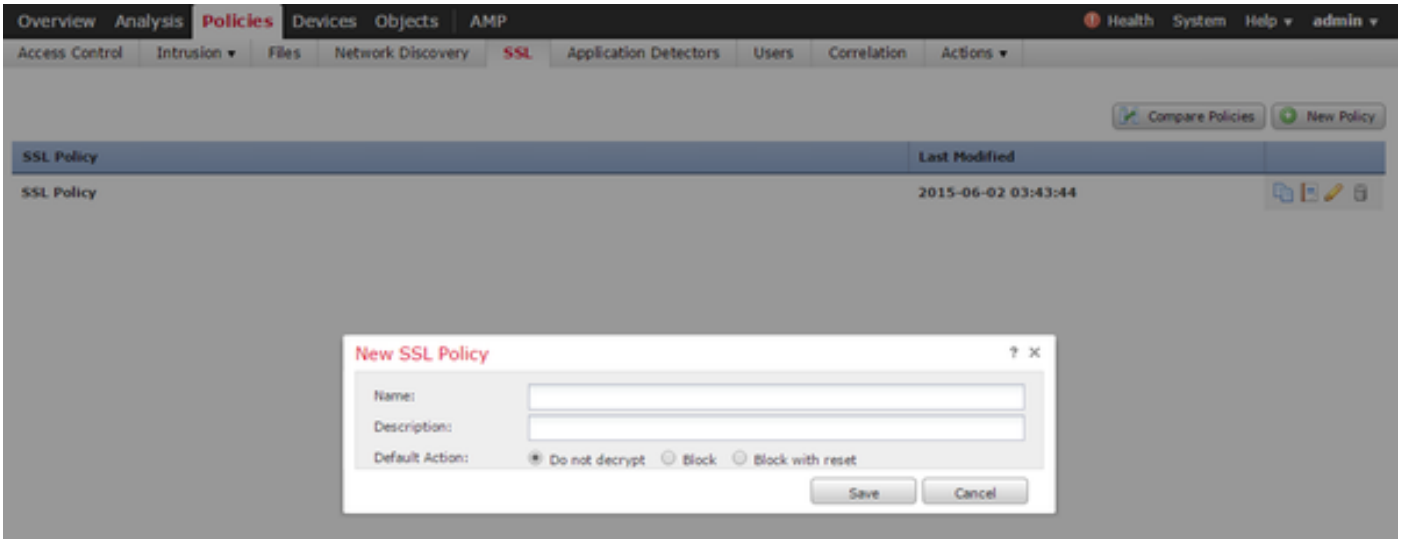
iv) Navigieren Sie zum privaten Schlüssel, oder fügen Sie ihn ein.

v. Aktivieren Sie das Feld **Verschlüsselt**, und geben Sie ein Kennwort ein.



Hinweis: Wenn kein Kennwort vorhanden ist, lassen Sie das Feld **Verschlüsselt** leer.

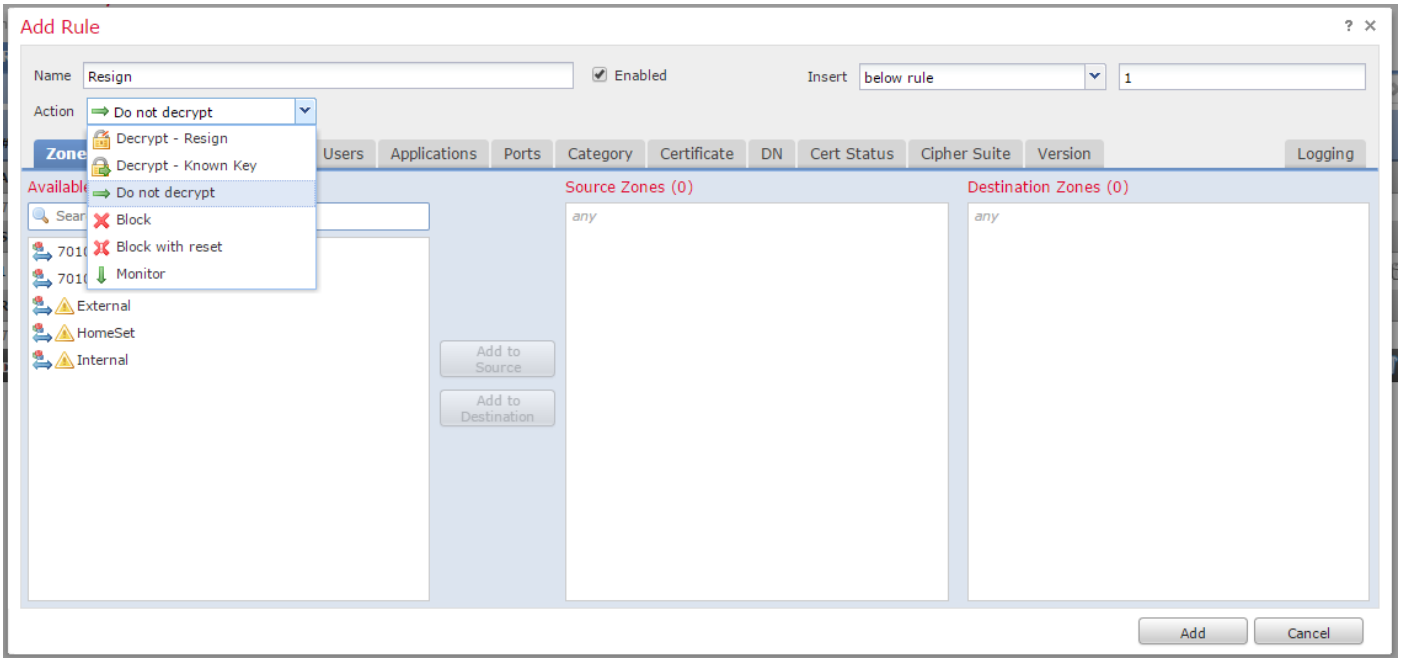
4. Navigieren Sie zu **Richtlinien > SSL,** und klicken Sie dann auf **Neue Richtlinie**.



5. Geben Sie einen Namen ein, und wählen Sie eine **Standardaktion aus**. Die Seite mit dem SSL Policy Editor wird angezeigt. Die Seite des SSL Policy Editor entspricht der Seite des Access Control Policy-Editors.

> **Hinweis:** Wenn Sie sich über die **Standardaktion** nicht sicher sind, **entschlüsseln Sie nicht** den empfohlenen Ausgangspunkt.

6. Klicken Sie auf der Seite des SSL-Policy-Editors auf **Regel hinzufügen**. Geben Sie im Fenster Regel hinzufügen einen Namen für die Regel ein, und füllen Sie alle anderen relevanten Informationen aus.



Im folgenden Abschnitt werden verschiedene Optionen im Fenster **Regel hinzufügen** beschrieben:

Aktion

Entschlüsseln - Zurücksetzen

- Der Sensor agiert als Man in the Middle (MitM) und akzeptiert die Verbindung mit dem Benutzer, stellt dann eine neue Verbindung zum Server her. Beispiele: Benutzertypen in https://www.facebook.com in einem Browser. Der Datenverkehr

erreicht den Sensor, der Sensor verhandelt dann mit dem Benutzer über das ausgewählte CA-Zertifikat und der SSL-Tunnel A wird erstellt. Gleichzeitig stellt der Sensor eine Verbindung zu https://www.facebook.com her und erstellt SSL-Tunnel B.
- Endergebnis: Benutzer sehen das Zertifikat in der Regel, nicht in Facebook's.
- Für diese Aktion ist eine interne CA erforderlich. Wählen Sie Schlüssel ersetzen, wenn der Schlüssel ersetzt werden soll. Der Benutzer erhält das ausgewählte Zertifikat.

Hinweis: Dies kann nicht im passiven Modus verwendet werden.

Entschlüsseln - Bekannter Schlüssel

- Der Sensor verfügt über den Schlüssel, der zum Entschlüsseln des Datenverkehrs verwendet wird. Beispiele: Benutzertypen in https://www.facebook.com in einem Browser. Der Datenverkehr erreicht den Sensor, der Sensor entschlüsselt den Datenverkehr und überprüft anschließend den Datenverkehr.
- Endergebnis: Benutzer sieht das Facebook-Zertifikat
- Für diese Aktion ist ein internes Zertifikat erforderlich. Dies wird unter **Objekte** > **PKI** > **Interne Zertifikate** hinzugefügt.

Hinweis: Ihre Organisation muss der Eigentümer der Domäne und des Zertifikats sein. Zum Beispiel von facebook.com wäre die einzige Möglichkeit, den Endbenutzer zu sehen, Facebook's Zertifikat wäre, wenn Sie tatsächlich Eigentümer der Domain facebook.com (d.h. Ihr Unternehmen ist Facebook, Inc) und haben Eigentümer des facebook.com Zertifikat signiert von einer öffentlichen CA. Sie können nur mit bekannten Schlüsseln für Sites entschlüsseln, die im Besitz Ihres Unternehmens sind.

Der Hauptzweck der Entschlüsselung eines bekannten Schlüssels besteht in der Entschlüsselung des Datenverkehrs zu Ihrem HTTPS-Server, um Ihre Server vor externen Angriffen zu schützen. Für die Überprüfung des clientseitigen Datenverkehrs zu externen HTTPS-Sites verwenden Sie die Rückmeldung entschlüsseln, da Sie nicht Eigentümer des Servers sind. Sie sind daran interessiert, den Client-Datenverkehr in Ihrem Netzwerk zu überprüfen, der mit externen verschlüsselten Sites verbunden ist.

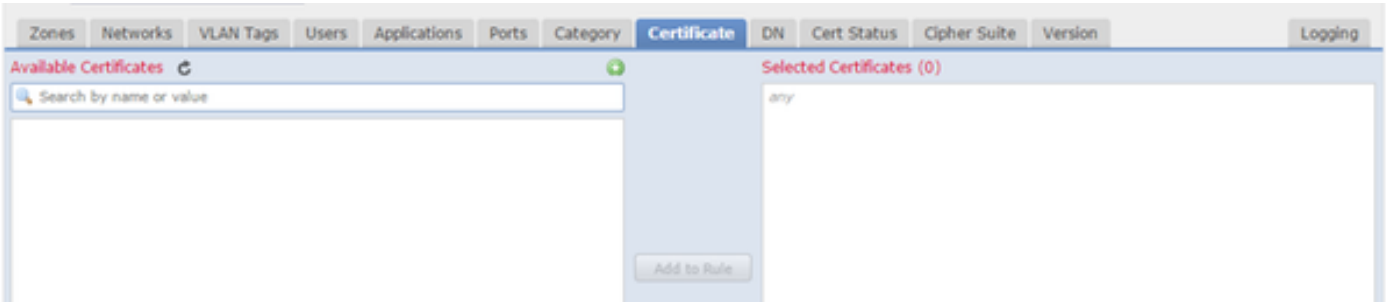
Hinweis: Damit DHE und ECDHE entschlüsseln können, müssen wir in-line sein.

Nicht entschlüsseln

Der Datenverkehr umgeht die SSL-Richtlinie und setzt die Zugriffskontrollrichtlinie fort.

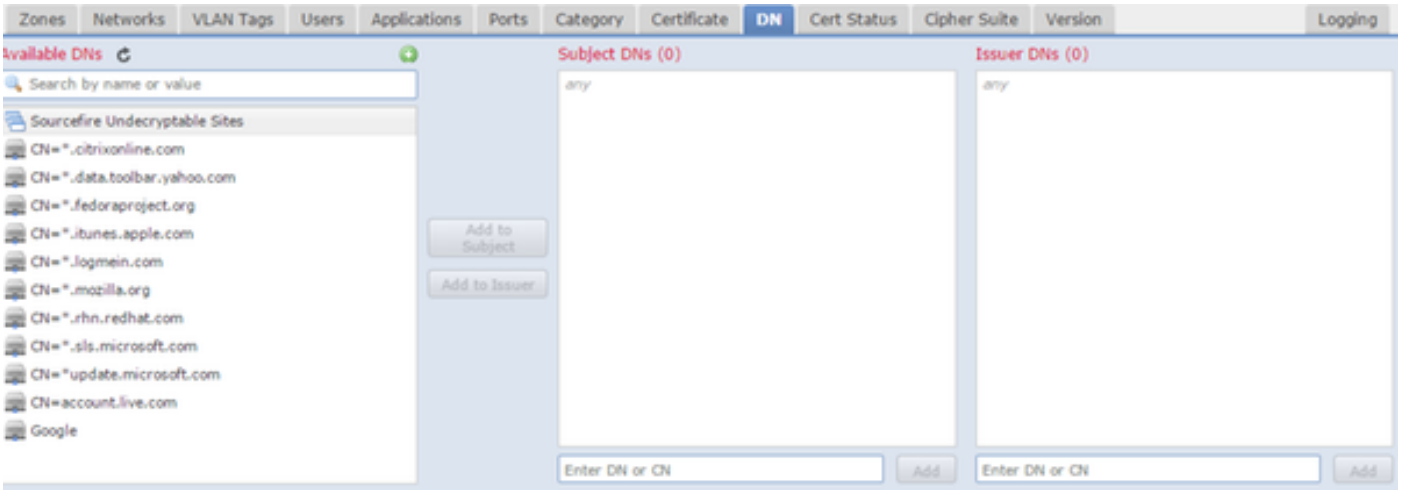
Zertifikat

Regel gleicht SSL-Datenverkehr mit diesem speziellen Zertifikat ab.



DN

Regel gleicht SSL-Datenverkehr mithilfe bestimmter Domänennamen in den Zertifikaten ab.

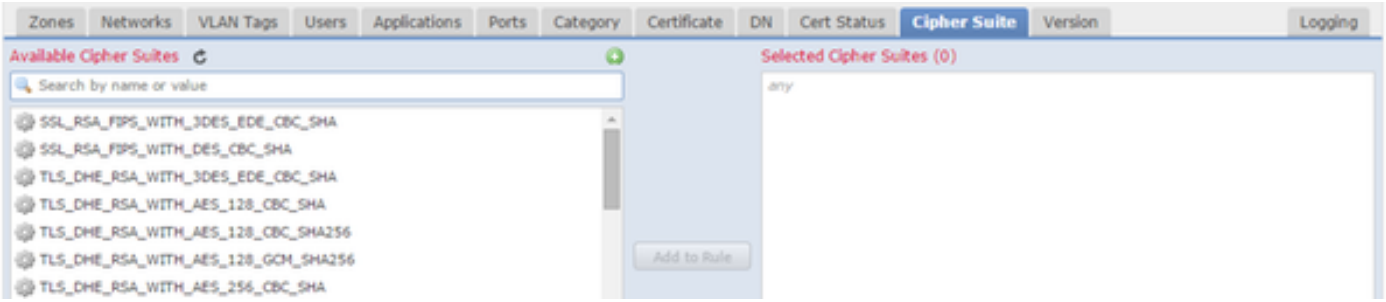


Zertifizierungsstatus

Regel gleicht SSL-Datenverkehr mit diesen Zertifikatsstatus ab.

Cipher Suite

Regel gleicht SSL-Datenverkehr mit diesen Cipher-Suites ab.



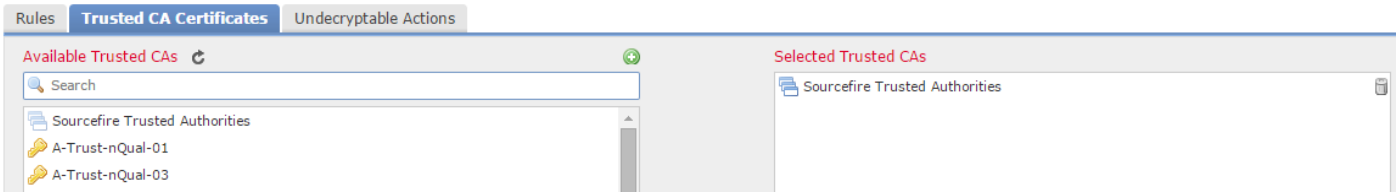
Version

Regeln gelten nur für SSL-Datenverkehr mit den ausgewählten SSL-Versionen.

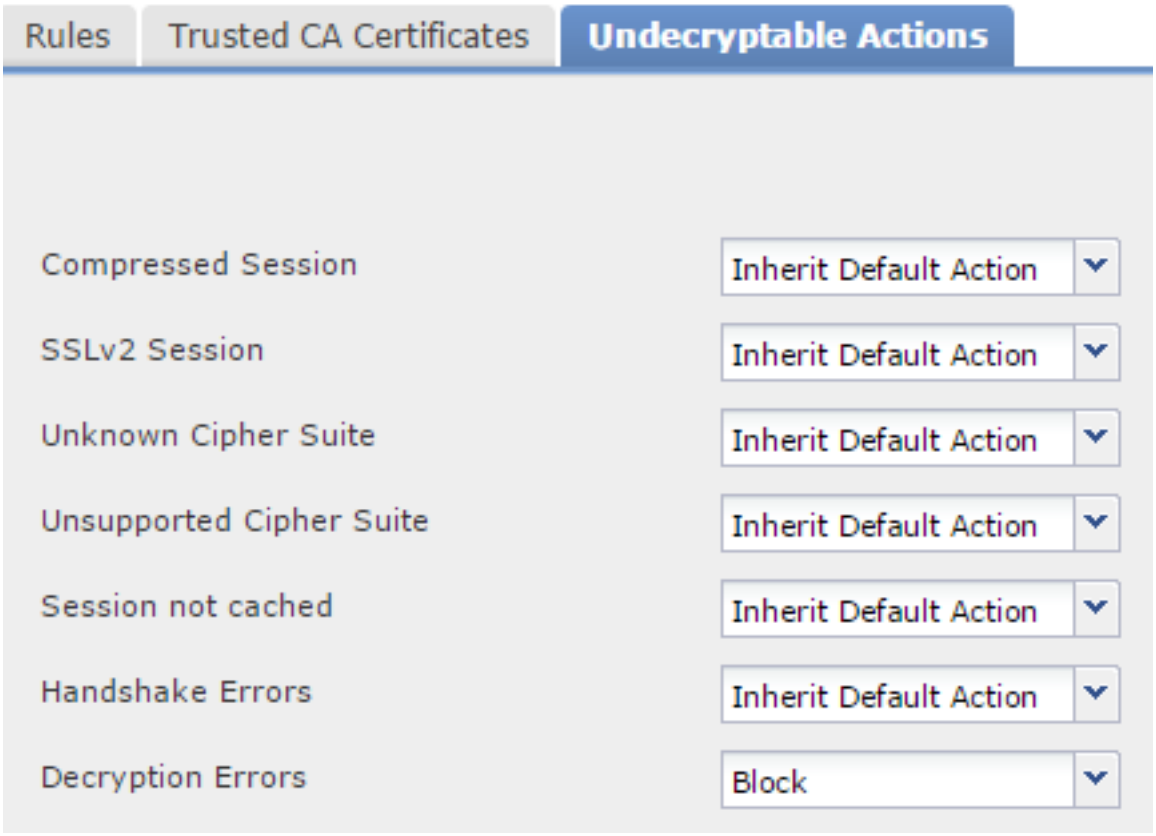
Protokollieren

Aktivieren Sie die Protokollierung, um Verbindungsereignisse für den SSL-Datenverkehr anzuzeigen.

7. Klicken Sie auf **Vertrauenswürdiges CA-Zertifikat**. Hier wird die vertrauenswürdige CA der Richtlinie hinzugefügt.



8. Klicken Sie auf **Unentschlüsselbare Aktionen**. Hier sind die Aktionen, für die der Sensor den Datenverkehr nicht entschlüsseln kann. Die Definitionen finden Sie in der Online-Hilfe (**Hilfe > Online**) des FireSIGHT Management Center.



- **Komprimierte Sitzung**: Die SSL-Sitzung wendet eine Datenkomprimierungsmethode an.
- **SSLv2-Sitzung**: Die Sitzung wird mit SSL Version 2 verschlüsselt. Beachten Sie, dass Datenverkehr entschlüsselt werden kann, wenn die Client-Hello-Nachricht SSL 2.0 und der

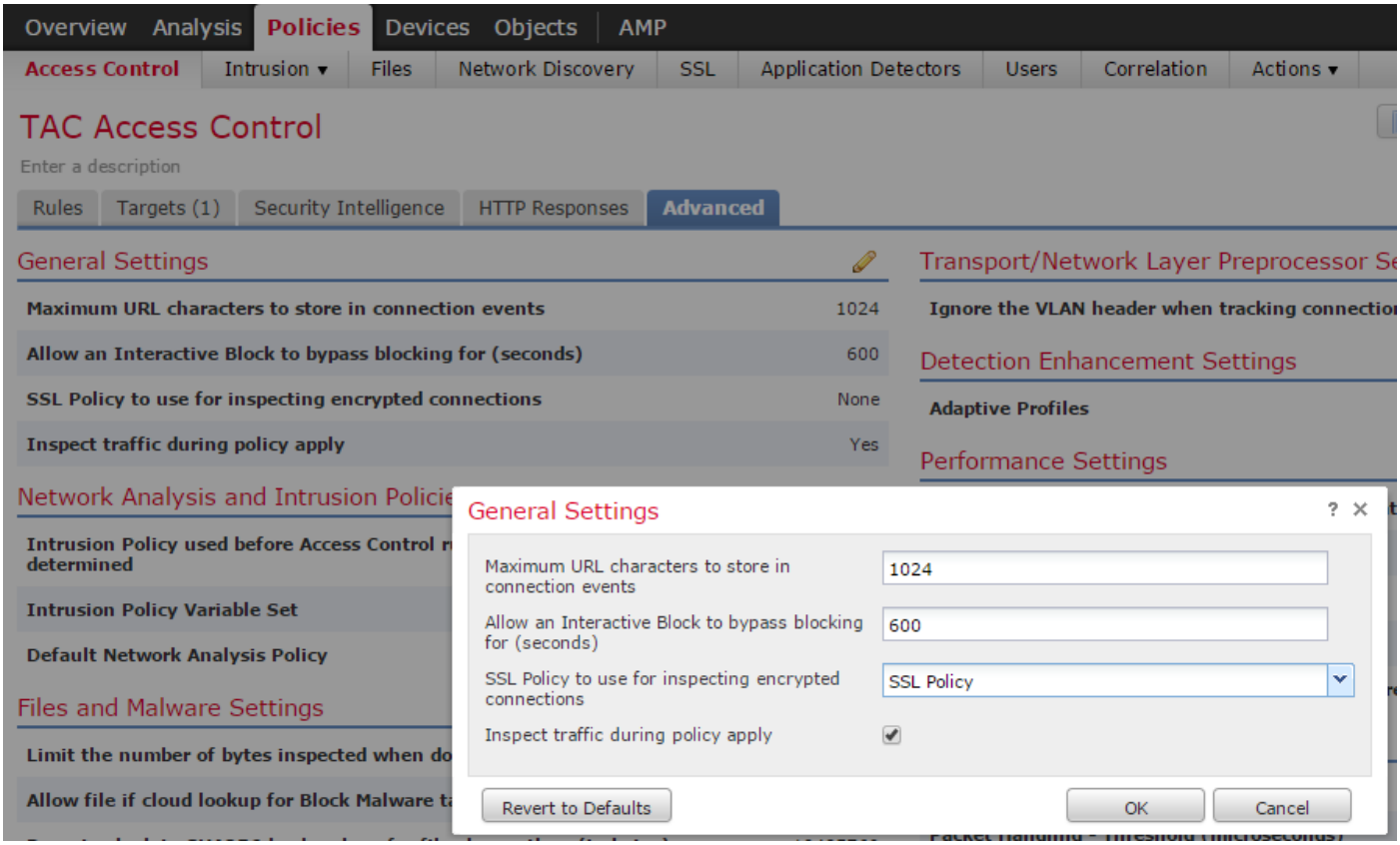
Rest des übertragenen Datenverkehrs SSL 3.0 ist.
- **Unbekannte Cipher Suite**: Das System erkennt die Verschlüsselungssuite nicht.
- **Nicht unterstützte Cipher Suite**: Das System unterstützt die Entschlüsselung auf der Grundlage der erkannten Verschlüsselungssuite nicht.
- **Sitzung nicht zwischengespeichert**: Bei der SSL-Sitzung ist die Sitzungswiederverwendung aktiviert, der Client und der Server haben die Sitzung mit der Sitzungskennung wiederhergestellt, und das System hat die Sitzungskennung nicht zwischengespeichert.
- **Handshake-Fehler**: Bei der SSL-Handshake-Aushandlung ist ein Fehler aufgetreten.
- **Entschlüsselungsfehler**: Bei der Entschlüsselung des Datenverkehrs ist ein Fehler aufgetreten.

Hinweis: Standardmäßig erben diese die Standardaktion. Wenn die Standardaktion "Blockieren" lautet, treten möglicherweise unerwartete Probleme auf.

9. Speichern Sie die Richtlinie.

10. Navigieren Sie zu **Richtlinien > Zugriffskontrolle**. Bearbeiten Sie Ihre Richtlinie, oder erstellen Sie eine neue Zugriffskontrollrichtlinie.

11. Klicken Sie auf **Erweitert**, und bearbeiten Sie die **allgemeinen Einstellungen**.



12. Wählen Sie aus dem Dropdown-Menü Ihre **SSL-Richtlinie aus**.

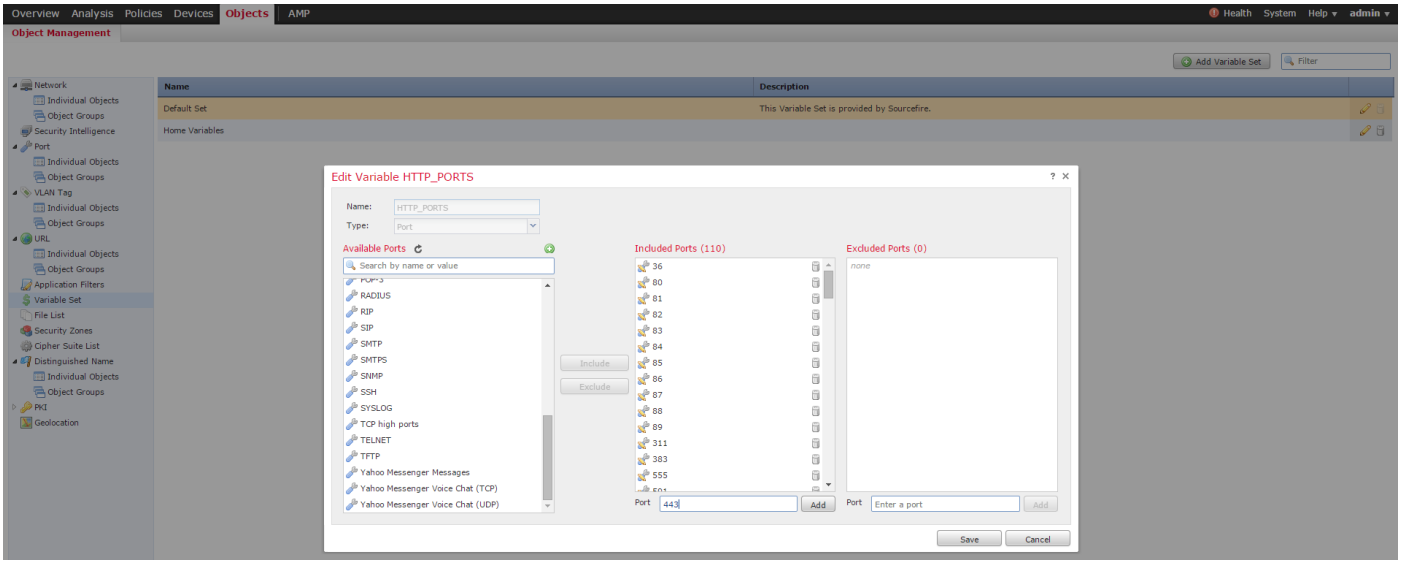
13. Klicken Sie zum Speichern auf **OK**.

Zusätzliche Konfigurationen

Folgende Änderungen sollten an den Intrusion-Policies vorgenommen werden, damit eine

ordnungsgemäße Identifizierung gewährleistet ist:

i. Ihre $HTTP_PORTS-Variable sollte Port 443 und alle anderen Ports mit HTTPS-Datenverkehr enthalten, die von Ihrer Richtlinie entschlüsselt werden (**Objekte > Objektverwaltung > Variablensatz > Variablensatz bearbeiten).**



ii) Die Network Analysis-Richtlinie, die den verschlüsselten Datenverkehr prüft, muss Port 443 (und alle anderen Ports mit HTTPS-Datenverkehr, die von Ihrer Richtlinie entschlüsselt werden) im Port-Feld der HTTP-Präprozessoreinstellungen enthalten. Andernfalls werden keine der HTTP-Regeln mit HTTP-Inhaltsmodifizierern (z. B. http_uri, http_header usw.) ausgelöst, da dies von den HTTP-Ports abhängt. und die HTTP-Puffer in snort werden nicht für Datenverkehr gefüllt, der nicht über die angegebenen Ports läuft.

iii) (Optional, aber für eine bessere Überprüfung empfohlen) Fügen Sie Ihre https-Ports den Einstellungen für die **TCP-Stream-Konfiguration** im Feld **Perform Stream Reassembly (Reassemblierung des Perform-Streams auf beiden Ports) hinzu**.

iv) Überarbeitete Zugriffskontrollrichtlinie während eines geplanten Wartungsfensters erneut anwenden.

> **Warnung:** Diese geänderte Richtlinie kann erhebliche Leistungsprobleme verursachen. Dies sollte außerhalb der Produktionszeiten getestet werden, um das Risiko von Netzwerkausfällen oder -leistung zu reduzieren.

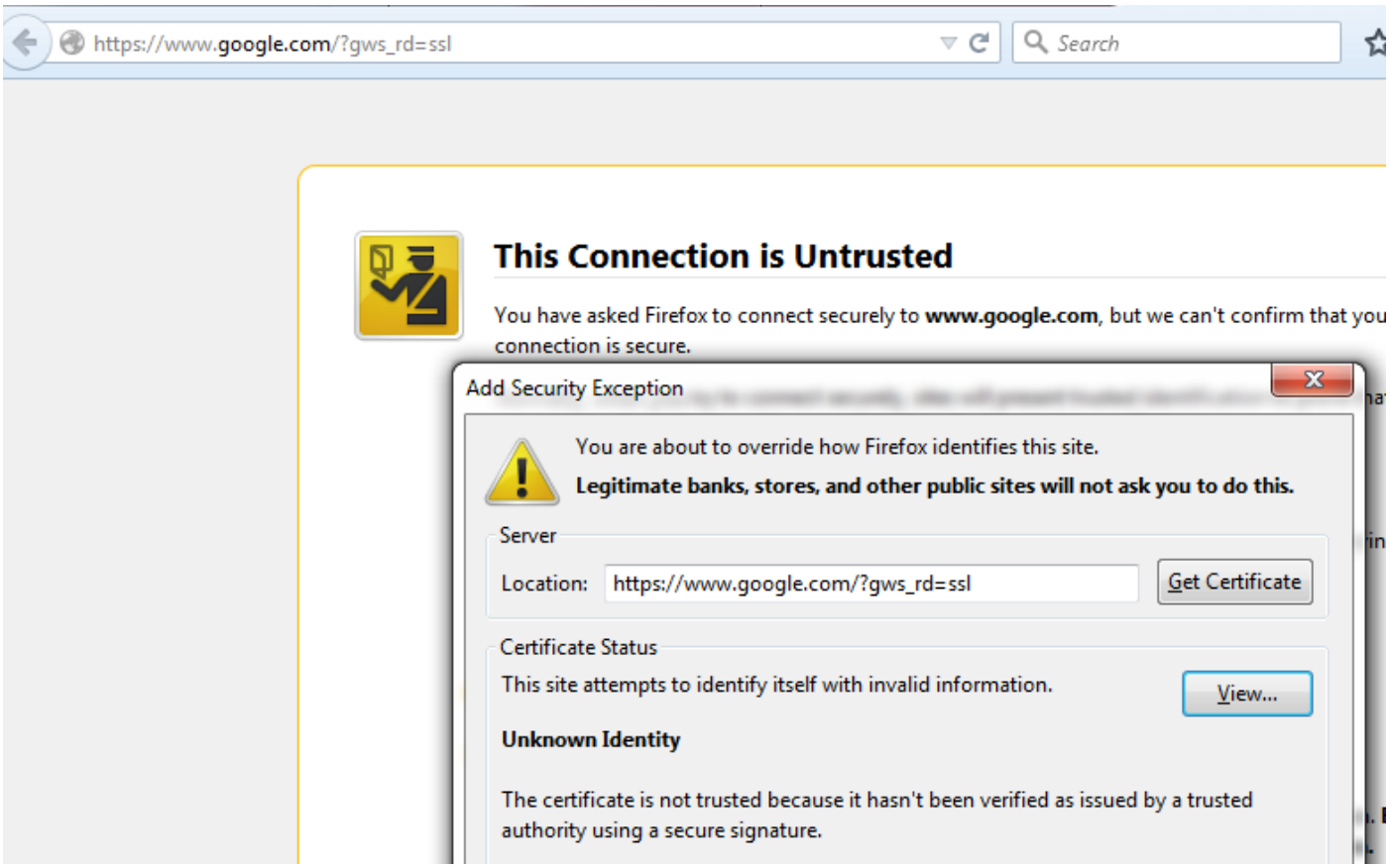
Überprüfung

Entschlüsseln - Zurücksetzen

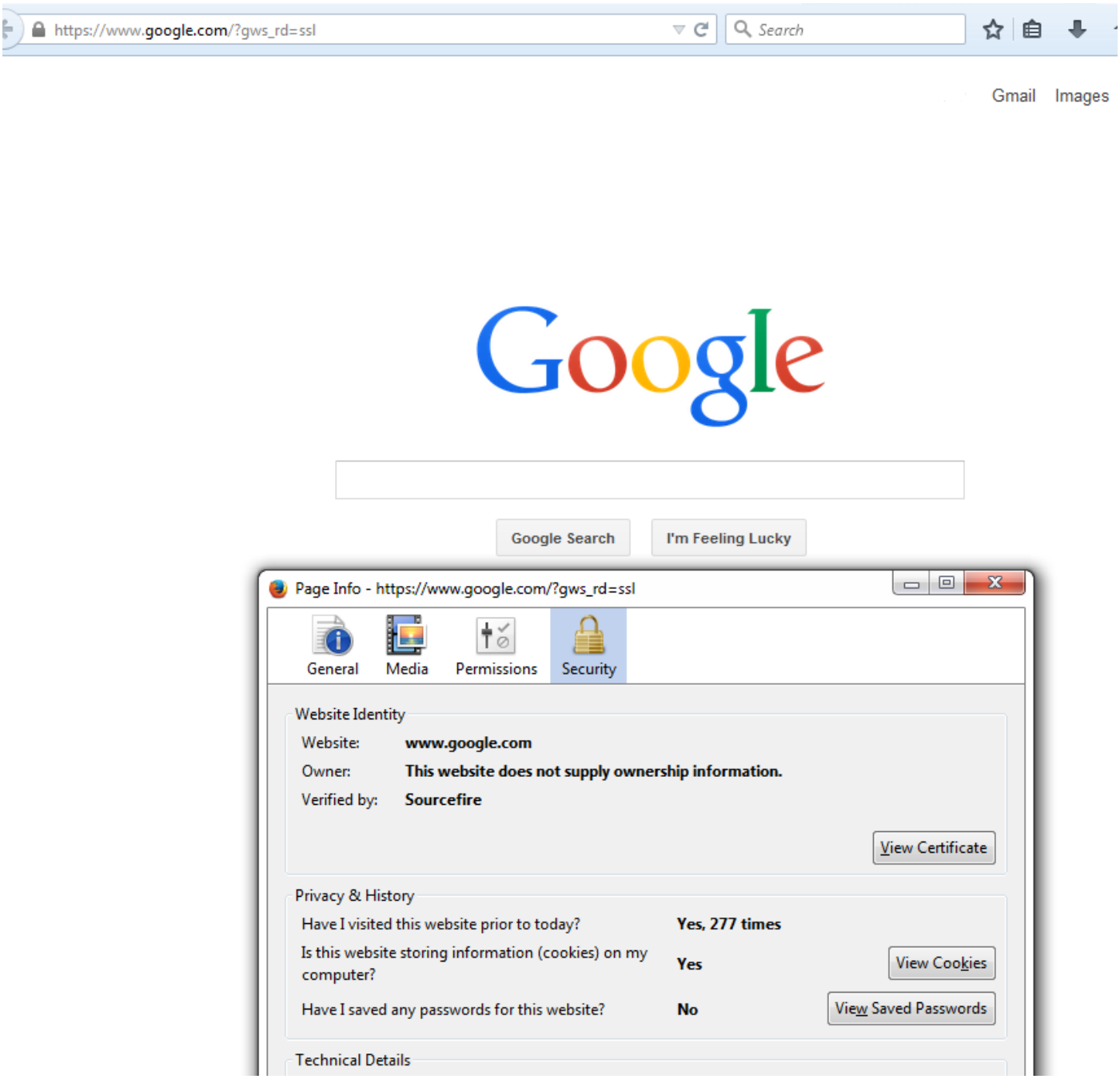
1. Öffnen Sie einen Webbrowser.

> **Hinweis:** Im Beispiel unten wird der Firefox-Browser verwendet. Dieses Beispiel funktioniert möglicherweise nicht in Chrome. Weitere Informationen finden Sie im Abschnitt Fehlerbehebung.

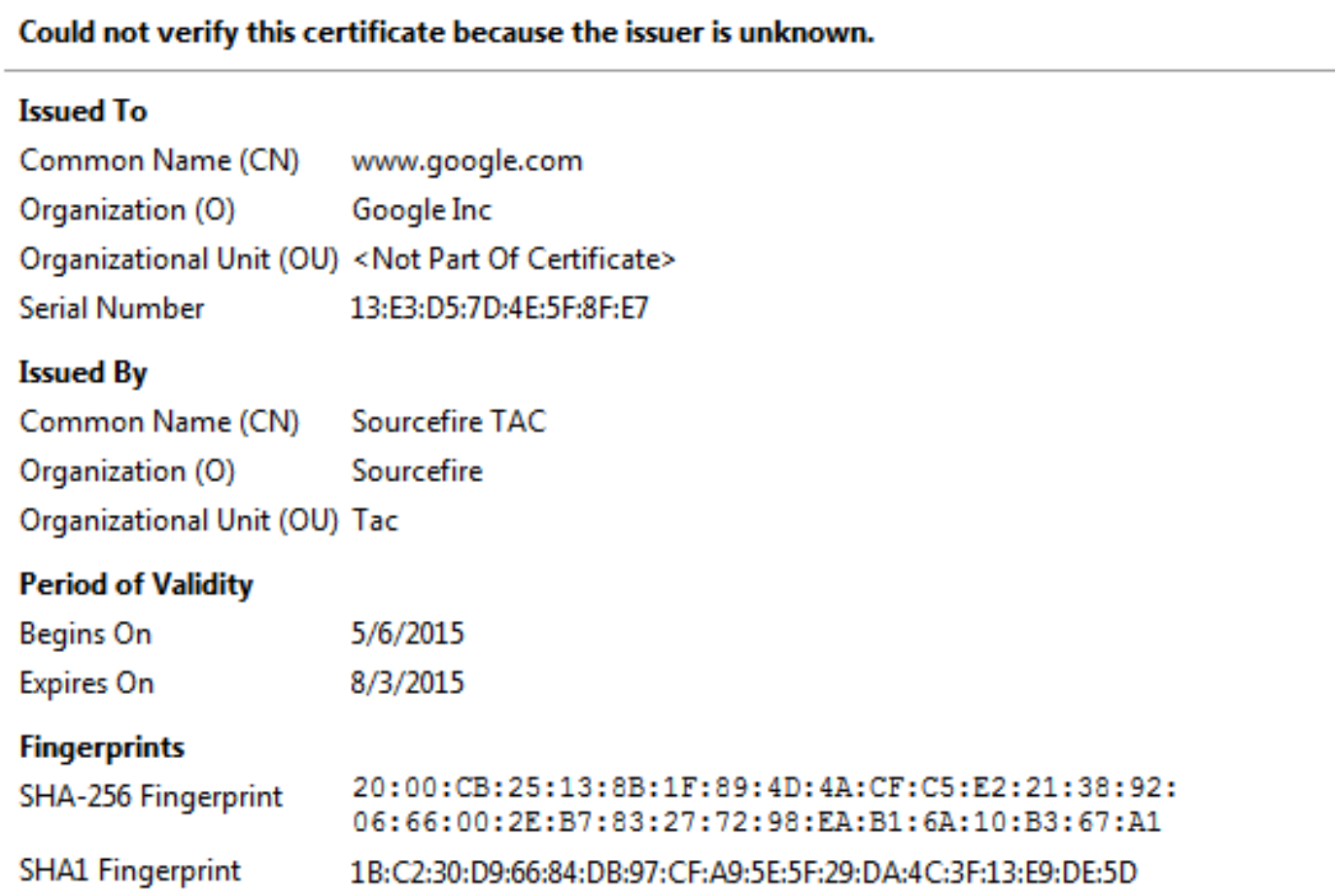
2. Navigieren Sie zu einer SSL-Website. Im Beispiel unten wird https://www.google.com verwendet, die Websites der Finanzinstitute wird auch funktionieren. Sie sehen eine der folgenden Seiten:



Hinweis: Die obige Seite wird angezeigt, wenn das Zertifikat selbst nicht vertrauenswürdig ist und das signierende Zertifizierungsstellenzertifikat von Ihrem Browser nicht als vertrauenswürdig eingestuft wird. Wie der Browser vertrauenswürdige Zertifizierungsstellenzertifikate auswählt, erfahren Sie im Abschnitt Vertrauenswürdige Zertifizierungsstellen weiter unten.



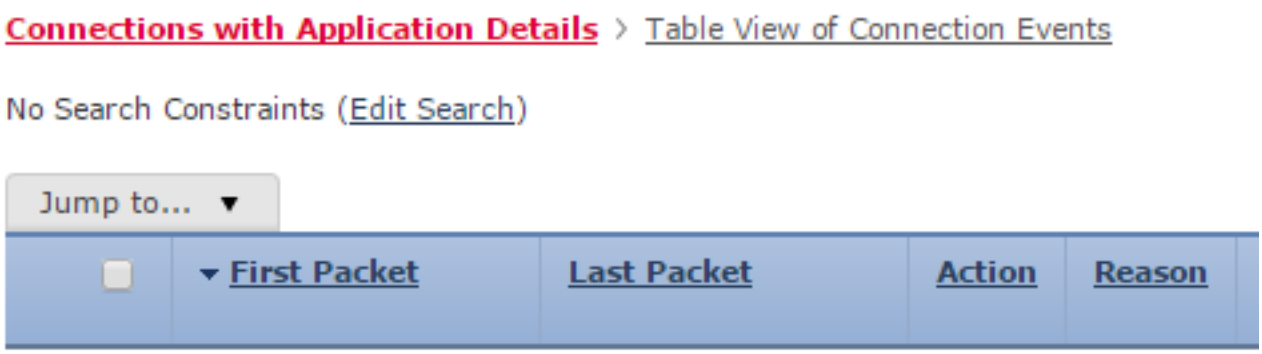
Hinweis: Wenn diese Seite angezeigt wird, haben Sie den Datenverkehr erfolgreich neu signiert. Beachten Sie den Abschnitt **Verified by: Sourcefire**.



Hinweis: Dies ist ein genauerer Blick auf dasselbe Zertifikat.

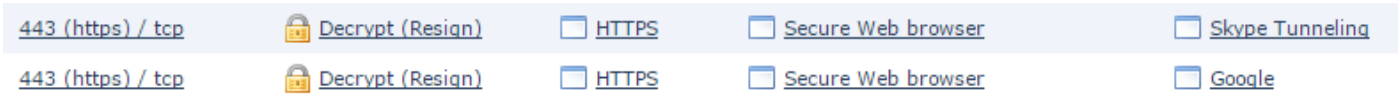
3. Gehen Sie im Management Center zu **Analysis > Connections > Events**.

4. Abhängig von Ihrem Workflow wird möglicherweise die Option SSL-Entschlüsselung angezeigt. Klicken Sie auf **Tabellenansicht von Verbindungsereignissen**.



5. Navigieren Sie nach rechts, und suchen Sie nach dem SSL-Status. Folgende Optionen sind

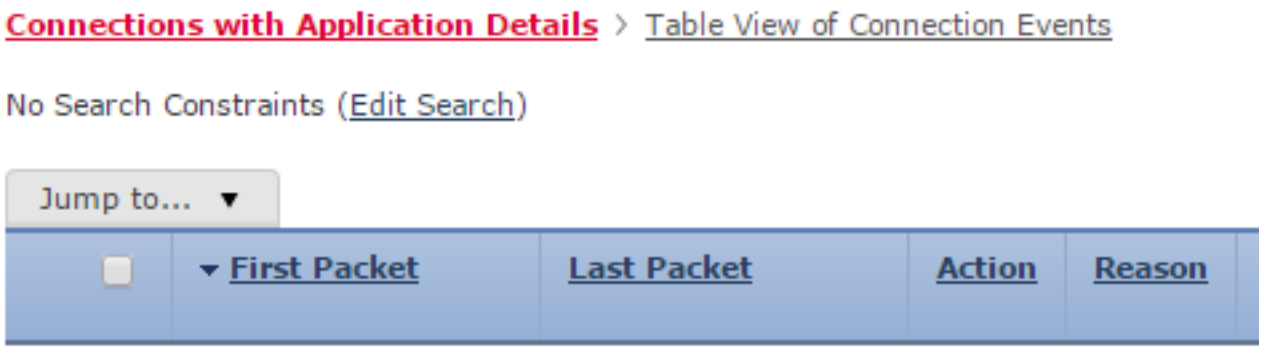
ähnlich:



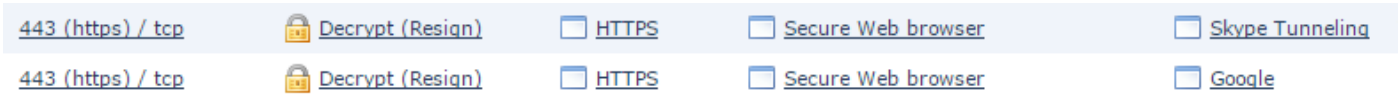
Entschlüsseln - Bekanntes Zertifikat

1. Navigieren Sie im FireSIGHT Management Center zu **Analysis > Connections > Events**.

2. Je nach Workflow wird die Option SSL-Entschlüsselung möglicherweise nicht angezeigt. Klicken Sie auf **Tabellenansicht von Verbindungsereignissen**.



3. Navigieren Sie nach rechts, und suchen Sie nach dem SSL-Status. Folgende Optionen sind ähnlich:



Fehlerbehebung

Ausgabe 1: Einige Websites werden möglicherweise nicht im Chrome-Browser geladen

Beispiel

www.google.com lädt möglicherweise nicht mit einer Entschlüsselung - Resign using Chrome.

Grund

Der Google Chrome-Browser ist in der Lage, betrügerische Zertifikate für Google-Eigenschaften zu erkennen, um Man-in-the-Middle-Angriffe zu verhindern. Wenn der Chrome-Browser (Client) versucht, eine Verbindung zu einer google.com-Domäne (Server) und ein Zertifikat zurückgegeben wird, das kein gültiges Google-Zertifikat ist, verweigert der Browser die Verbindung.

Lösung

Wenn dies auftritt, fügen Sie eine **Do Not Decrypt-**Regel für DN=*.google.com, *.gmail.com, *.youtube.com hinzu. Löschen Sie anschließend den Browser-Cache und den Browserverlauf.

Ausgabe 2: Abrufen einer nicht vertrauenswürdigen Warnung/eines nicht vertrauenswürdigen Fehlers in einigen Browsern

Beispiel

Wenn Sie mit Internet Explorer und Chrome eine Verbindung zu einer Website herstellen, erhalten Sie keine Sicherheitswarnung. Wenn Sie jedoch den Firefox-Browser verwenden, müssen Sie der Verbindung bei jedem Schließen und erneuten Öffnen des Browsers vertrauen.

Grund

Die Liste der vertrauenswürdigen CAs hängt vom Browser ab. Wenn Sie einem Zertifikat vertrauen, wird es nicht über alle Browser verteilt, und der vertrauenswürdige Eintrag wird in der Regel nur bei geöffnetem Browser beibehalten. Wenn der Browser geschlossen ist, werden alle vertrauenswürdigen Zertifikate gelöscht, und beim nächsten Öffnen des Browsers und beim nächsten Besuch der Site müssen Sie das Zertifikat erneut zur Liste der vertrauenswürdigen Zertifikate hinzufügen.

Lösung

In diesem Szenario verwenden sowohl IE als auch Chrome die Liste der vertrauenswürdigen CAs im Betriebssystem, Firefox pflegt jedoch eine eigene Liste. Das CA-Zertifikat wurde also in den OS-Store importiert, aber nicht in den Firefox-Browser importiert. Um die Sicherheitswarnung in Firefox zu vermeiden, müssen Sie das CA-Zertifikat als vertrauenswürdige CA in den Browser importieren.

Vertrauenswürdige Zertifizierungsstellen

Wenn eine SSL-Verbindung hergestellt wird, prüft der Browser zuerst, ob dieses Zertifikat vertrauenswürdig ist (d.h. Sie waren vor dieser Site und haben dem Browser manuell mitgeteilt, dass er diesem Zertifikat vertrauen soll). Wenn das Zertifikat nicht vertrauenswürdig ist, überprüft der Browser das Zertifikat der Zertifizierungsstelle (Certificate Authority, CA), das das Zertifikat für diese Site verifiziert hat. Wenn das Zertifizierungsstellenzertifikat vom Browser als vertrauenswürdig eingestuft wird, wird es als vertrauenswürdiges Zertifikat betrachtet und die Verbindung zugelassen. Wenn das Zertifizierungsstellenzertifikat nicht vertrauenswürdig ist, zeigt der Browser eine Sicherheitswarnung an und zwingt Sie, das Zertifikat manuell als vertrauenswürdiges Zertifikat hinzuzufügen.

Die Liste der vertrauenswürdigen CAs in einem Browser ist vollständig von der Implementierung des Browsers abhängig, und jeder Browser kann seine vertrauenswürdige Liste anders als andere Browser ausfüllen. Im Allgemeinen gibt es zwei Möglichkeiten, wie aktuelle Browser eine Liste vertrauenswürdiger CAs ausfüllen:

1. Sie verwenden die Liste der vertrauenswürdigen CAs, denen das Betriebssystem vertraut.
2. Sie liefern eine Liste der vertrauenswürdigen CAs zusammen mit der Software und ist in den Browser integriert.

Für die gängigsten Browser werden die vertrauenswürdigen CAs wie folgt aufgefüllt:

- **Google Chrome**: Vertrauenswürdige CA-Liste des Betriebssystems
- **Firefox**: Behält seine eigene vertrauenswürdige CA-Liste bei
- **Internet Explorer**: Vertrauenswürdige CA-Liste des Betriebssystems
- **Safari**: Vertrauenswürdige CA-Liste des Betriebssystems

Es ist wichtig, den Unterschied zu kennen, da das Verhalten, das auf dem Client gesehen wird, je nach dem variieren wird. Um beispielsweise eine vertrauenswürdige CA für Chrome und IE hinzuzufügen, müssen Sie das CA-Zertifikat in den vertrauenswürdigen CA-Speicher des Betriebssystems importieren. Wenn Sie das Zertifizierungsstellenzertifikat in den vertrauenswürdigen Zertifizierungsstellenspeicher des Betriebssystems importieren, wird keine Warnung mehr angezeigt, wenn Sie eine Verbindung zu Standorten herstellen, für die ein von dieser Zertifizierungsstelle signiertes Zertifikat vorliegt. Im Firefox-Browser müssen Sie das CA-Zertifikat manuell in den vertrauenswürdigen CA-Speicher im Browser selbst importieren. Danach erhalten Sie keine Sicherheitswarnung mehr, wenn Sie eine Verbindung zu Sites herstellen, die von dieser CA überprüft wurden.

Referenzen

- Erste Schritte mit SSL-Regeln