

Configurazione di un criterio di ispezione SSL sul sistema Cisco FireSIGHT

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Componenti usati](#)

[Configurazioni](#)

[1. Decrittografa e abbandona](#)

[Opzione 1: Utilizzare il centro FireSIGHT come autorità di certificazione \(CA\) radice](#)

[Opzione 2: Apporre la firma del certificato a una CA interna](#)

[Opzione 3: Importa un certificato e una chiave CA](#)

[2. Decrittografare con chiave nota](#)

[Importazione del certificato noto \(alternativa alla decrittografia e alle dimissioni\)](#)

[Configurazioni aggiuntive](#)

[Verifica](#)

[Decrittografa - Abbandona](#)

[Decrittografa - Certificato noto](#)

[Risoluzione dei problemi](#)

[Numero 1: Alcuni siti Web potrebbero non caricare sul browser Chrome](#)

[Numero 2: Visualizzazione di un avviso/errore non attendibile in alcuni browser](#)

[Riferimenti](#)

[Discussioni correlate nella Cisco Support Community](#)

Introduzione

La funzione di ispezione SSL consente di bloccare il traffico crittografato senza ispezionarlo o di ispezionare il traffico crittografato o decrittografato con il controllo degli accessi. In questo documento viene descritta la procedura di configurazione per impostare un criterio di ispezione SSL sul sistema Cisco FireSIGHT.

Prerequisiti

Componenti usati

- Cisco FireSIGHT Management Center
- Appliance Cisco Firepower 7000 o 8000
- Software versione 5.4.1 o superiore

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Avviso: L'applicazione di criteri di ispezione SSL al dispositivo gestito può influire sulle prestazioni della rete.

Configurazioni

È possibile configurare un criterio di ispezione SSL per decrittografare il traffico nei modi seguenti:

1. Decrittografare e abbandonare:

- Opzione 1: utilizzare il centro FireSIGHT come autorità di certificazione (CA) radice oppure
- Opzione 2: Disporre di una CA interna per firmare il certificato oppure
- Opzione 3: Importa un certificato e una chiave CA

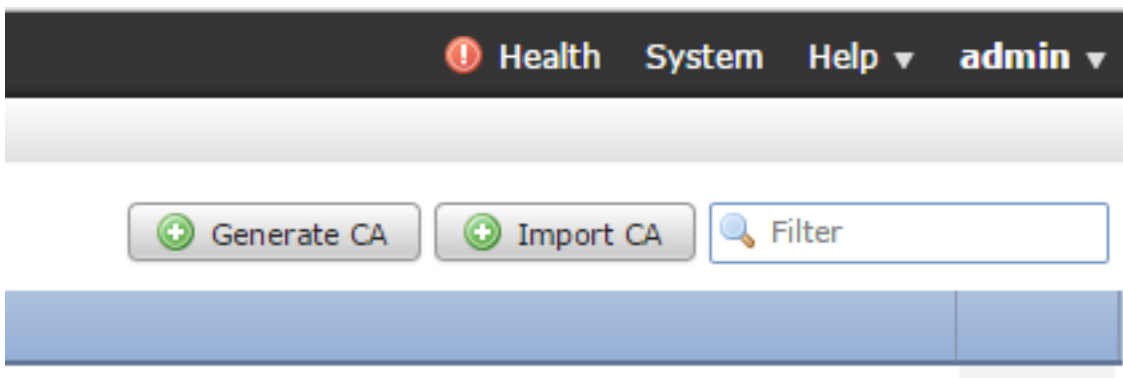
2. Decrittografare con certificato noto:

- Accedere al centro di gestione FireSIGHT, quindi selezionare **Oggetti**.
- Nella pagina **Oggetti** espandere **PKI** e selezionare **CA interne**.

1. Decrittografa e abbandona

Opzione 1: Utilizzare il centro FireSIGHT come autorità di certificazione (CA) radice

i. Fare clic su **Genera CA**.



ii. Inserire le informazioni pertinenti

Generate Internal Certificate Authority ? X

| | |
|-----------------------------------|---|
| Name: | <input type="text" value="InternalCA"/> |
| Country Name (two-letter code): | <input type="text" value="US"/> |
| State or Province: | <input type="text" value="MD"/> |
| Locality or City: | <input type="text" value="Columbia"/> |
| Organization: | <input type="text" value="Sourcefire"/> |
| Organizational Unit (Department): | <input type="text" value="TAC"/> |
| Common Name: | <input type="text" value="InternalCA"/> |

iii. Fare clic su **Genera CA autofirmata**.

Opzione 2: Apporre la firma del certificato a una CA interna

i. Fare clic su **Genera CA**.

! Health System Help admin

ii. Inserire le informazioni pertinenti.

Generate Internal Certificate Authority ? X

Name: InternalCA

Country Name (two-letter code): US

State or Province: MD

Locality or City: Columbia

Organization: Sourcefire

Organizational Unit (Department): TAC

Common Name: InternalCA

Generate CSR Generate self-signed CA Cancel

Nota: Potrebbe essere necessario contattare l'amministratore della CA per determinare se dispone di un modello per la richiesta di firma.

iii. Copiare l'intero certificato, inclusi —BEGIN CERTIFICATE REQUEST— e —END CERTIFICATE REQUEST— e quindi salvarlo in un file di testo con estensione .req.

Generate Internal Certificate Authority ? X

Subject:

- Common Name: InternalCA
- Organization: Sourcefire
- Organization Unit: TAC

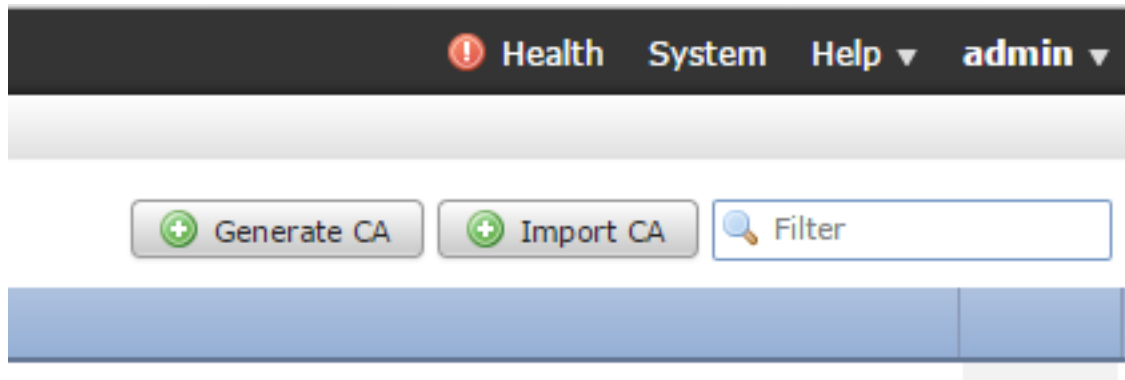
CSR:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIB4zCCAQAwCAQAwZTELMakGA1UEBhMCVVMxMzA1BjBjNVBAGMAk1EMREwDwYDVQQH
DAhDb2x1bWJpYTETMBEGA1UECgwKU291cmNlZmlyZTEMMAAoGA1UECwwDVFEFMRMw
EQYDVQQDDApJbnRlcm5hbENBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC5
XTQjxBMnyPNmGTVAXrqG7LhXPXzZ7lgF6MfKxwLh8rVwoejHhwbAUro8ju/R3Ig7
Ty1cwNpr4Bnbk9kDS9jDYqftFJzOu8UJ6wKcmxg2IUx80r9y1SKzSiRprJdSBaRc
LSHey3dI0K5SXNktTb8vBV97RYAfX4VDR7iVDKwxzQIDAQABoD4wPAYJKoZiHvcN
AQkOMS8wLTAdBgNVHQ4EFgQUih/JeYfJm2itIE3spLdPqzpTXGkwDAYDVR0TBAUw
AwER/zANBnkohkiG9w0BAQUFAAORoORlhzvWFeXilos25vxfvIto/W9Zu14DeV1m9
-----
```

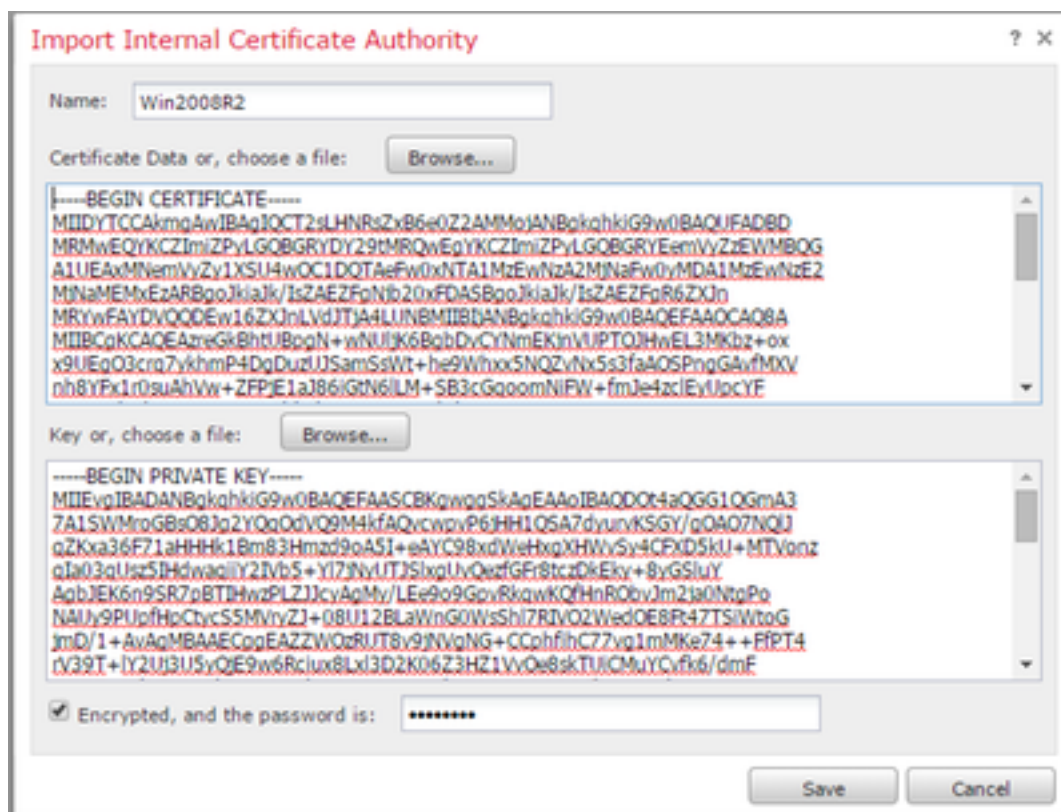
OK Cancel

Nota: L'amministratore della CA richiede un'altra estensione di file oltre a .req.

Opzione 3: Importa un certificato e una chiave CA



- i. Fare clic su **Importa CA**.
- ii. Individuare il certificato o incollarlo.
- iii. Selezionare o incollare nella chiave privata.
- iv. Selezionare la casella crittografata e immettere una password.



Nota: Se non è presente alcuna password, selezionare la casella crittografata e lasciarla vuota.

2. Decrittografare con chiave nota

Importazione del certificato noto (alternativa alla decrittografia e alle dimissioni)

- i. Nella pagina Oggetti a sinistra espandere PKI e selezionare Certificati interni.
- ii. Fare clic su **Aggiungi certificato interno**.
- iii. Individuare il certificato o incollarlo.
- iv. Selezionare o incollare nella chiave privata.
- v. Selezionare la casella **Encrypted** e immettere una password.

Add Known Internal Certificate ? X

Name:

Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIDODCCAIACCQDsfBhdDsHTDANBgkqhkiG9w0BAQUFADBeMQswCQYDVQOGEwJV
UzELMAkGA1UECawCTUQxETAPBgNVBAcMCENvbHVtYmhlMRMwEQYDVQQKDApTb3Vy
Y2VmaXJlMQwwCgYDVQQLDANUQUxMxDDAKBgNVBAMMA1RBOzAeFw0xNTA2MDQxNzA4
MDZaFw0xODAzMDQxNzA4MDZaMF4xCzAJBgNVBAYTAiVTMQswCQYDVQQIDAJNRDER
MASGA1UEBww1Q29sdW1laWEuExARBgNVBAoMCINvdXJlZmVzcmUxDDAKBgNVBAcM
A1RBOzEMMAoGA1UEAwwvDVEFDMIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAXAkHMrrPPyysIwkgwAH0ELtHmYQ3/i+MgMzmQiuAhrE3AZmh7t6BZQrwFgK
-----
```

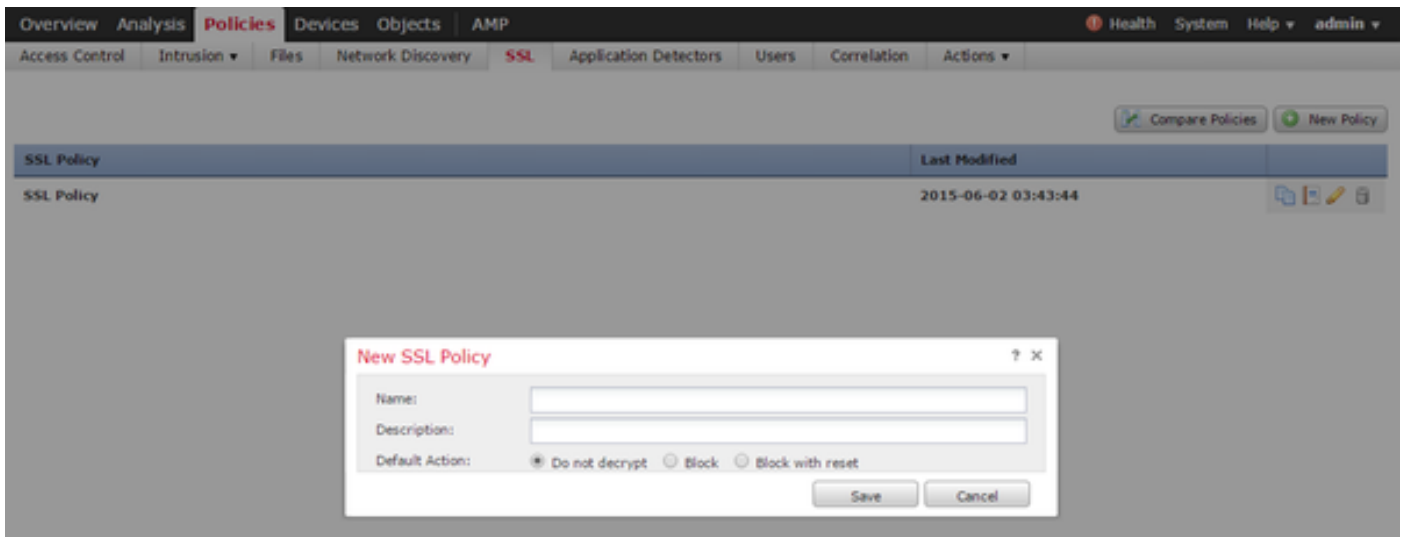
Key or, choose a file:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAXAkHMrrPPyysIwkgwAH0ELtHmYQ3/i+MgMzmQiuAhrE3AZm
h7t6BZQrwFgKeMX1KV7LuxXnsuJfpNk3Dp8fm33TMDQiuAZW6zpusjgOKS3yUs4E
wG5wcqMVe/baDT2B/XQt3BLUqLsL+TPipUgazrF3rOECvroPxDRQC/fz8AazQV
JfX8WVJt3SqYttzw41vU9qai2OuVaANrIBSiz+9NnwNTpVGvrvHx+IOl/e2ZARl1
FrtH/eN9+/p66tUSILV23rUKUKM0gkh8IPs2mu17Uppqv3uYW2OWVnQsz41CGzht
YonbuEUCpEtJdWctI/P2mIWECSumJN7hNfKQIDAQABAoIBACjSNHSDhYkDNWkq
Sm6ROZCOZTuaTeNFud15O1lfrFR13I5wqsMS8ArfWuj3rF6P4khWHBh+LDxc1UvP
-----
```

Encrypted, and the password is:

Nota: Se non è presente una password, lasciare vuota la casella **Encrypted**.

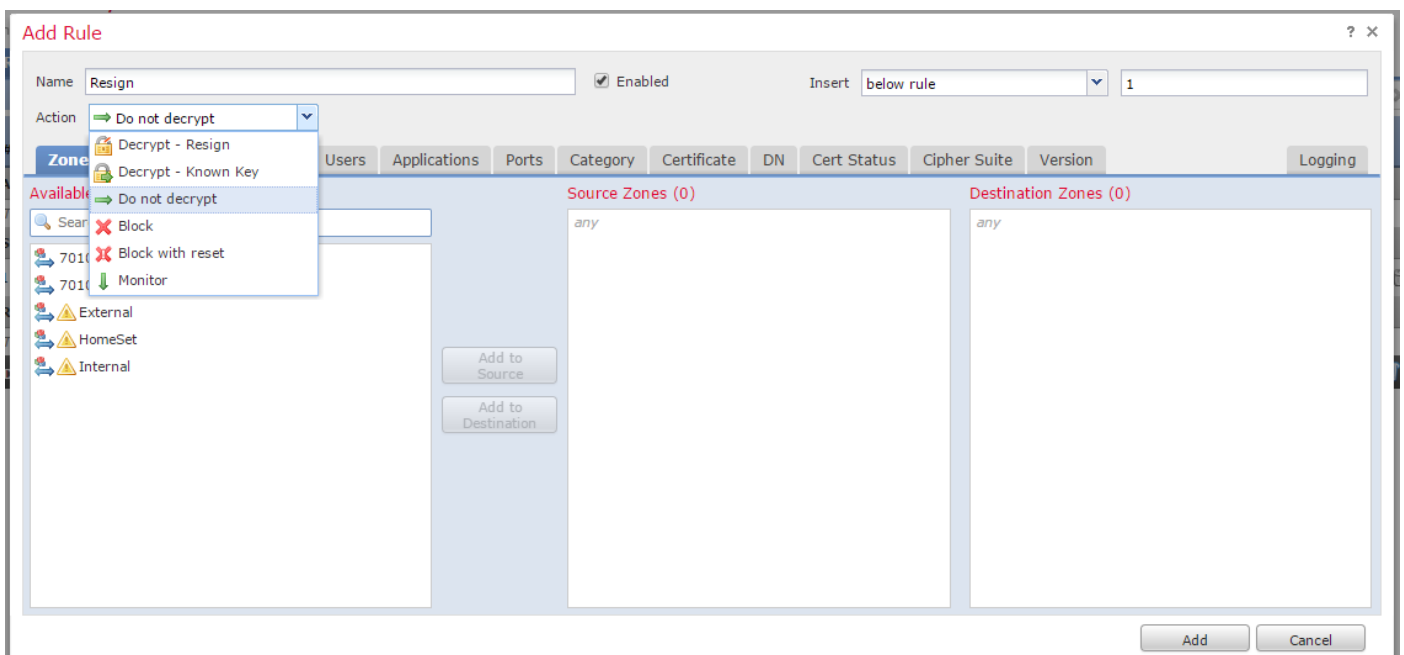
4. Passare a **Criteri > SSL** quindi fare clic su **Nuovo criterio**.



5. Fornire un nome e selezionare un'azione predefinita. Viene visualizzata la pagina dell'editor dei criteri SSL. La pagina dell'editor dei criteri SSL funziona come la pagina dell'editor dei criteri di controllo dell'accesso.

Nota: Se non si è certi dell'azione predefinita, non decrittografare è il punto di partenza consigliato.

6. Nella pagina Editor criteri SSL fare clic su **Aggiungi regola**. Nella finestra Aggiungi regola specificare un nome per la regola e immettere tutte le altre informazioni pertinenti.



Nella sezione seguente vengono descritte diverse opzioni della finestra **Aggiungi regola**:

Azione

Decrittografa - Abbandona

- Il sensore agisce come un Uomo nel Mezzo (MitM) e accetta la connessione con l'utente, quindi stabilisce una nuova connessione al server. Ad esempio: L'utente digita in <https://www.facebook.com> in un browser. Il traffico raggiunge il sensore, il sensore negozia con l'utente utilizzando il certificato CA selezionato e viene creato il tunnel SSL A. Allo stesso tempo il sensore si connette a <https://www.facebook.com> e crea il tunnel SSL B.

- Risultato finale: L'utente vede il certificato nella regola, non in Facebook.
- Questa azione richiede una CA interna. Selezionare Sostituisci chiave se si desidera sostituire la chiave. L'utente riceverà il certificato selezionato.

Nota: Non può essere utilizzato in modalità passiva.

Decrittografa - Chiave nota

- Il sensore ha la chiave che verrà utilizzata per decrittografare il traffico. Ad esempio: L'utente digita in <https://www.facebook.com> in un browser. Il traffico raggiunge il sensore, il sensore decripta il traffico, quindi lo controlla.
- Risultato finale: L'utente visualizza il certificato di Facebook
- Questa azione richiede un certificato interno. Questo viene aggiunto in **Oggetti > PKI > Certificati interni**.

Nota: L'organizzazione deve essere il proprietario del dominio e del certificato. Per l'esempio di facebook.com, l'unico modo possibile per fare in modo che l'utente finale veda il certificato di facebook sarebbe se tu possiedi effettivamente il dominio facebook.com (ossia la tua azienda è Facebook, Inc) e possiedi il certificato facebook.com firmato da una CA pubblica. È possibile decrittografare solo con chiavi note per i siti di proprietà dell'organizzazione.

Lo scopo principale della decrittografia della chiave nota è decrittografare il traffico diretto al server https per proteggere i server dagli attacchi esterni. Per ispezionare il traffico lato client verso siti https esterni, si utilizzerà il comando decrittografa rassegnazione in quanto non si è proprietari del server e si è interessati a controllare il traffico client nella rete che si connette a siti esterni crittografati.

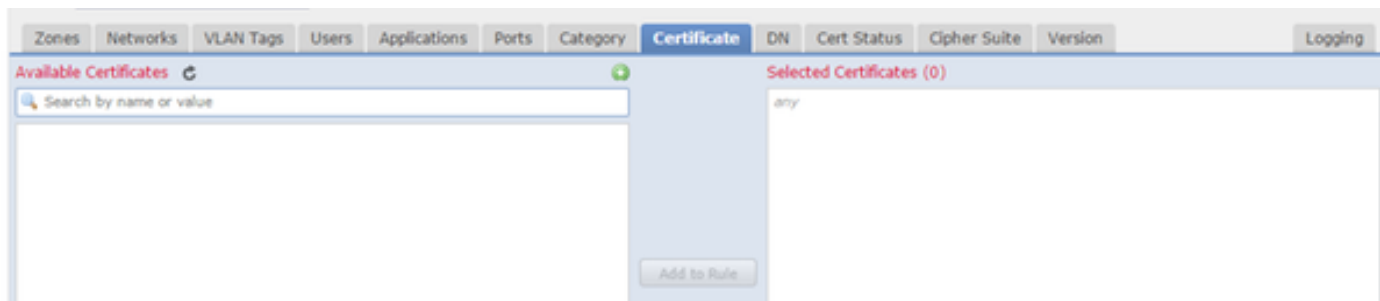
Nota: Affinché DHE ed ECDHE possano essere decriptati, è necessario essere in linea.

Non decrittografare

Il traffico ignora il criterio SSL e continua con il criterio di controllo dell'accesso.

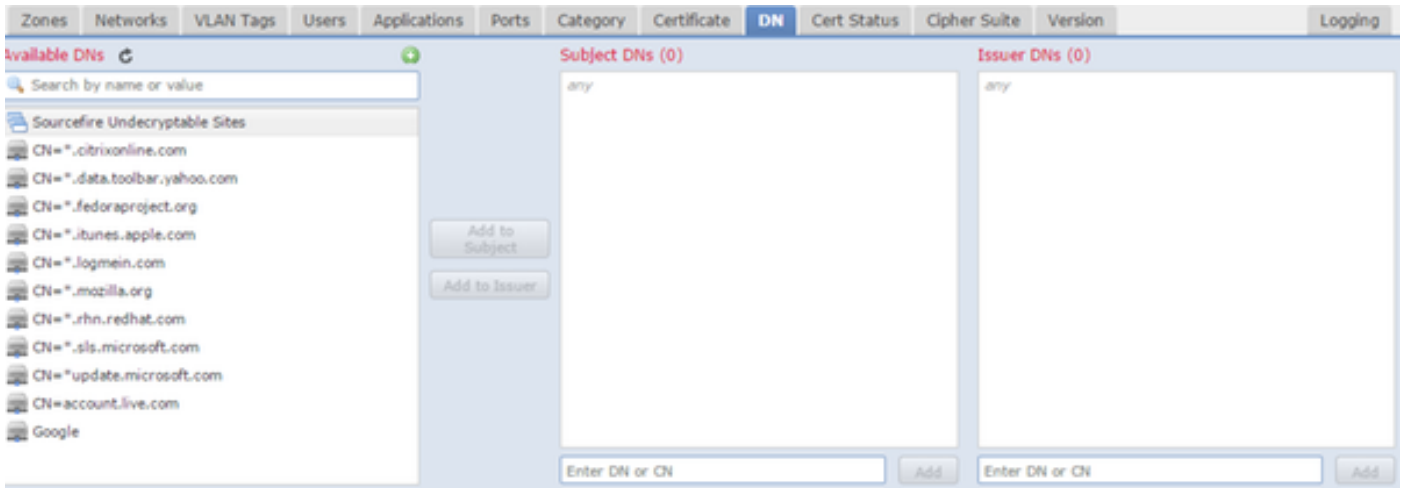
Certificato

La regola corrisponde al traffico SSL che utilizza questo particolare certificato.



DN

La regola corrisponde al traffico SSL utilizzando determinati nomi di dominio nei certificati.



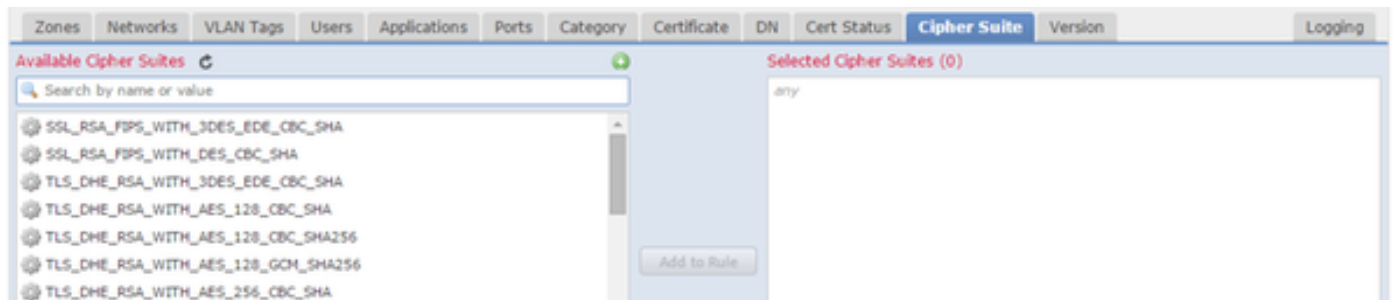
Stato certificato

La regola corrisponde al traffico SSL con questi stati del certificato.



Cipher Suite

La regola corrisponde al traffico SSL utilizzando queste suite di cifratura.



Version

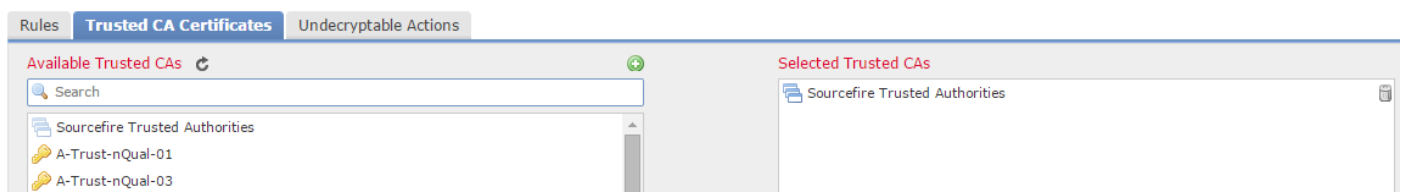
Le regole si applicano solo al traffico SSL con le versioni selezionate di SSL.

| Zones | Networks | VLAN Tags | Users | Applications | Ports | Category | Certificate | DN | Cert Status | Cipher Suite | Version |
|-------|----------|-----------|-------|--------------|-------|----------|-------------|----|-------------|--------------|-------------------------------------|
| | | | | | | | | | | | <input checked="" type="checkbox"/> |
| | | | | | | | | | | | <input checked="" type="checkbox"/> |
| | | | | | | | | | | | <input checked="" type="checkbox"/> |
| | | | | | | | | | | | <input checked="" type="checkbox"/> |

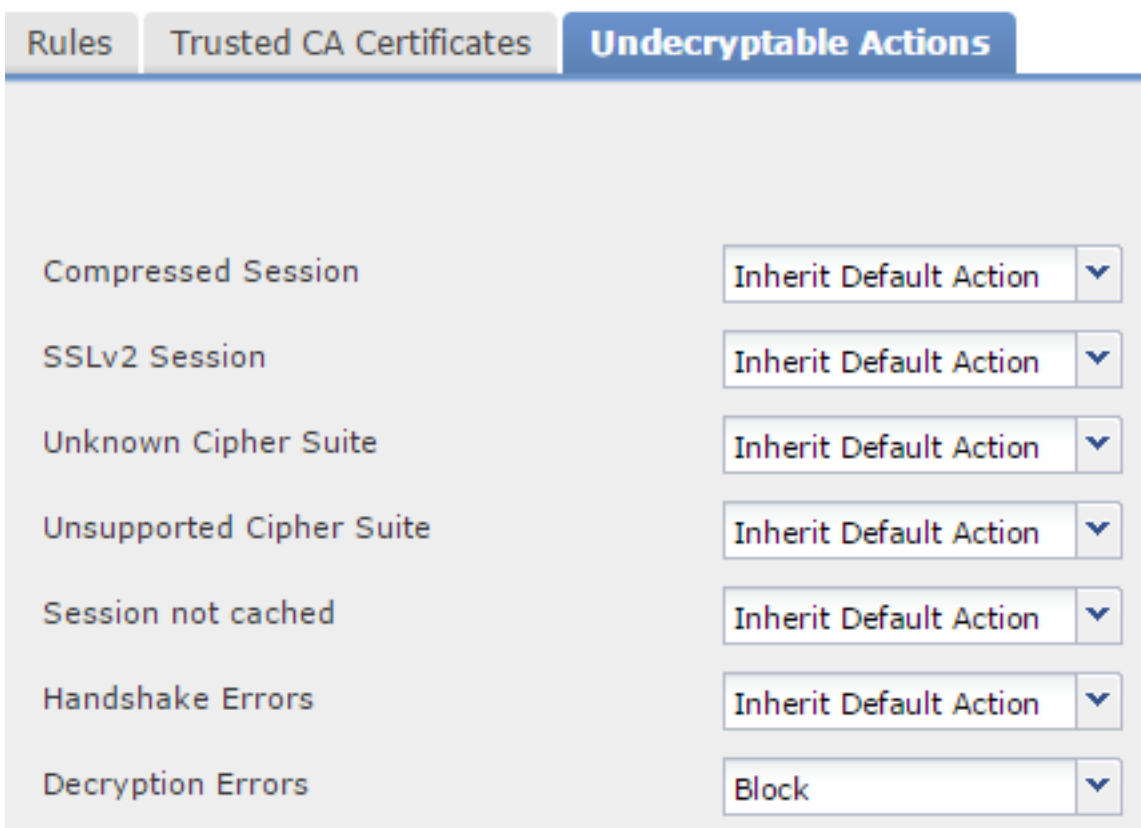
Registrazione

Abilitare la registrazione per visualizzare gli eventi di connessione per il traffico SSL.

7. Fare clic su **Certificato CA attendibile**. In questa posizione le CA attendibili vengono aggiunte al criterio.



8. Fare clic su **Azioni non decrittografabili**. Di seguito sono elencate le azioni per cui il sensore non è in grado di decrittografare il traffico. Le definizioni sono reperibili nella Guida in linea (**Guida > In linea**) di FireSIGHT Management Center.



- **Sessione compressa:** La sessione SSL applica un metodo di compressione dei dati.
- **Sessione SSLv2:** La sessione è crittografata con SSL versione 2. Il traffico può essere decrittografato se il messaggio di benvenuto del client è SSL 2.0 e la parte rimanente del traffico trasmesso è SSL 3.0.

- **Suite di crittografia sconosciuta:** Il sistema non riconosce la suite di cifratura.
- **Suite di crittografia non supportata:** Il sistema non supporta la decrittografia basata sulla suite di crittografia rilevata.
- **Sessione non memorizzata nella cache:** Per la sessione SSL è abilitato il riutilizzo della sessione, il client e il server hanno ristabilito la sessione con l'identificativo di sessione e il sistema non ha memorizzato nella cache tale identificativo di sessione.
- **Errori di handshake:** Errore durante la negoziazione dell'handshake SSL.
- **Errori di decrittografia:** Errore durante la decrittografia del traffico.

Nota: Per impostazione predefinita, queste azioni ereditano l'azione predefinita. Se l'azione predefinita è Blocca, è possibile che si verifichino problemi imprevisti

9. Salvare il criterio.

10. Passare a **Policy > Controllo accesso**. Modificare il criterio o creare un nuovo criterio di controllo dell'accesso.

11. Fare clic su **Avanzate** e modificare le **Impostazioni generali**.

The screenshot shows the 'TAC Access Control' configuration page in the 'Advanced' tab. A 'General Settings' dialog box is open, displaying the following configuration options:

| Setting | Value |
|---|-------------------------------------|
| Maximum URL characters to store in connection events | 1024 |
| Allow an Interactive Block to bypass blocking for (seconds) | 600 |
| SSL Policy to use for inspecting encrypted connections | SSL Policy |
| Inspect traffic during policy apply | <input checked="" type="checkbox"/> |

The dialog box also includes buttons for 'Revert to Defaults', 'OK', and 'Cancel'.

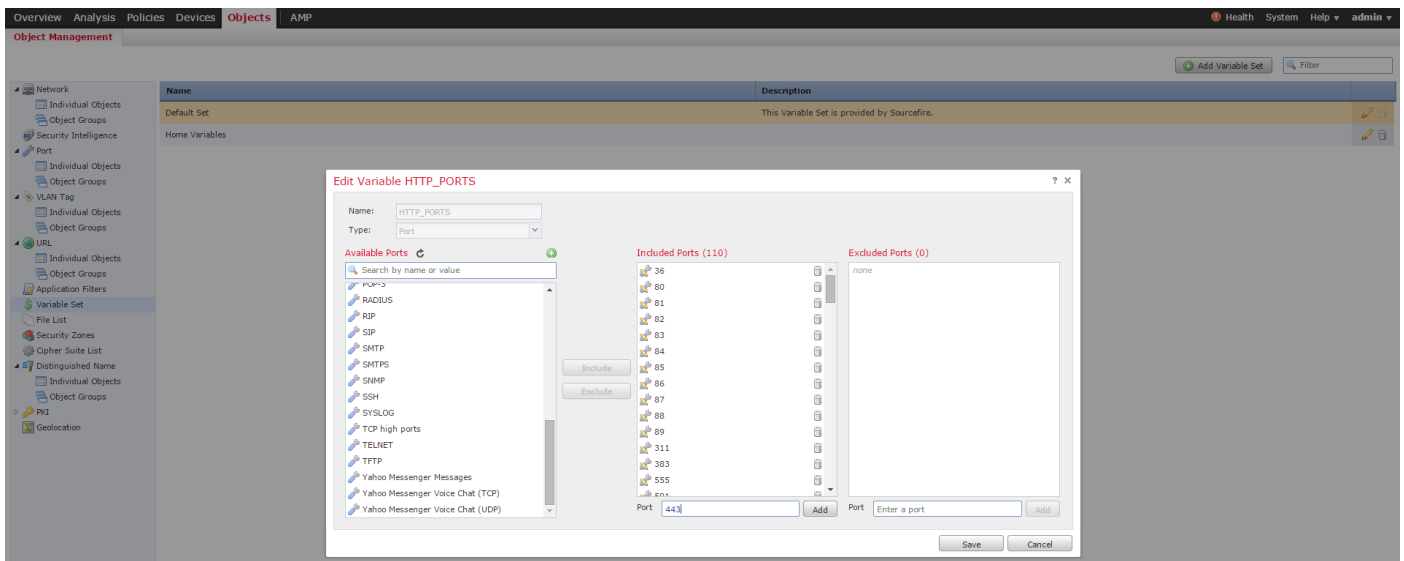
12. Dal menu a discesa, selezionare il **criterio SSL**.

13. Fare clic su **OK** per salvare.

Configurazioni aggiuntive

Ai fini di una corretta identificazione, è opportuno apportare le seguenti modifiche alle politiche in materia di intrusione:

i. La variabile \$HTTP_PORTS deve includere la porta 443 e qualsiasi altra porta con traffico https che verrà decrittografata dal criterio (**Oggetti > Gestione oggetti > Insieme di variabili > Modifica l'insieme di variabili**).



ii. Il criterio Analisi rete che controlla il traffico crittografato deve includere la porta 443 (e qualsiasi altra porta con traffico https che verrà decrittografata dal criterio) nel campo Porte delle impostazioni del preprocessore HTTP. In caso contrario, nessuna delle regole http con modificatori di contenuto http (ad esempio http_uri, http_header e così via) verrà attivata perché dipende dalle porte http definite e i buffer http in snort non verranno popolati per il traffico che non passa attraverso le porte specificate.

iii. (Facoltativo ma consigliato per un controllo migliore) Aggiungere le porte https alle impostazioni di **Configurazione flusso TCP** nel campo **Esegui riassetto flusso su entrambe le porte**.

iv. Riapplicare il criterio di controllo dell'accesso modificato durante un intervento di manutenzione pianificato.

Avviso: questo criterio modificato può causare problemi significativi di prestazioni. Il test deve essere eseguito al di fuori delle ore di produzione per ridurre il rischio di interruzioni o prestazioni della rete.

Verifica

Decrittografa - Abbandona

1. Aprire un browser Web.

Nota: nell'esempio riportato di seguito viene utilizzato il browser Firefox. Questo esempio potrebbe non funzionare in Chrome. Per ulteriori informazioni, vedere la sezione Risoluzione dei problemi.

2. Accedere a un sito Web SSL. Nell'esempio seguente viene utilizzato <https://www.google.com>, funzioneranno anche i siti web delle istituzioni finanziarie. Verrà visualizzata una delle seguenti pagine:

The screenshot shows a Firefox browser window with the address bar containing `https://www.google.com/?gws_rd=ssl`. A yellow warning icon is visible in the top left of the page content. The main heading reads "This Connection is Untrusted". Below it, the text states: "You have asked Firefox to connect securely to **www.google.com**, but we can't confirm that your connection is secure."

An "Add Security Exception" dialog box is open in the foreground. It contains the following information:

- Warning icon and text: "You are about to override how Firefox identifies this site. Legitimate banks, stores, and other public sites will not ask you to do this."
- Server section: "Location: `https://www.google.com/?gws_rd=ssl`" with a "Get Certificate" button.
- Certificate Status section: "This site attempts to identify itself with invalid information." with a "View..." button.
- Unknown Identity** section: "The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature."

Nota:La pagina precedente verrà visualizzata se il certificato stesso non è attendibile e il certificato CA di firma non è attendibile per il browser. Per informazioni su come il browser determina i certificati CA attendibili, vedere la sezione Autorità di certificazione attendibili riportata di seguito.

Google

Google Search I'm Feeling Lucky

Page Info - https://www.google.com/?gws_rd=ssl

General Media Permissions Security

Website Identity

Website: **www.google.com**
Owner: **This website does not supply ownership information.**
Verified by: **Sourcefire**

[View Certificate](#)

Privacy & History

| | | |
|---|-----------------------|--------------------------------------|
| Have I visited this website prior to today? | Yes, 277 times | |
| Is this website storing information (cookies) on my computer? | Yes | View Cookies |
| Have I saved any passwords for this website? | No | View Saved Passwords |

Technical Details

Nota: Se la pagina viene visualizzata, la firma del traffico è stata riapposta. Si noti la sezione **Verified by: Il Fuoco 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

Nota: Questo è un esame approfondito dello stesso certificato.

3. In Centro di gestione, andare in **Analisi > Connessioni > Eventi**.

4. A seconda del flusso di lavoro in uso, è possibile che venga visualizzata o meno l'opzione di decrittografia SSL. Fare clic su **Visualizzazione per tabella degli eventi di connessione**.



Connections with Application Details > Table View of Connection Events

No Search Constraints ([Edit Search](#))

| | | | | | |
|--------------|--------------------------|-----------------------|--------------------|---------------|---------------|
| Jump to... ▼ | <input type="checkbox"/> | ▼ <u>First Packet</u> | <u>Last Packet</u> | <u>Action</u> | <u>Reason</u> |
|--------------|--------------------------|-----------------------|--------------------|---------------|---------------|

5. Scorrere verso destra e cercare lo stato SSL. Le opzioni visualizzate sono simili a quelle

riportate di seguito:

| | | | | |
|-----------------------------------|--|--|---|--|
| 443 (https) / tcp |  Decrypt (Resign) | <input type="checkbox"/> HTTPS | <input type="checkbox"/> Secure Web browser | <input type="checkbox"/> Skype Tunneling |
| 443 (https) / tcp |  Decrypt (Resign) | <input type="checkbox"/> HTTPS | <input type="checkbox"/> Secure Web browser | <input type="checkbox"/> Google |

Decrittografa - Certificato noto



1. Nel centro di gestione FireSIGHT, passare ad **Analisi > Connessioni > Eventi**.
2. A seconda del flusso di lavoro, è possibile che l'opzione di decrittografia SSL sia disponibile o meno. Fare clic su **Visualizzazione per tabella degli eventi di connessione**.

[Connections with Application Details](#) > [Table View of Connection Events](#)

No Search Constraints ([Edit Search](#))

| | | | | | |
|--------------|--------------------------|--------------------------------|-----------------------------|------------------------|------------------------|
| Jump to... ▼ | <input type="checkbox"/> | ▼ First Packet | Last Packet | Action | Reason |
|--------------|--------------------------|--------------------------------|-----------------------------|------------------------|------------------------|

3. Scorrere verso destra e cercare lo stato SSL. Le opzioni visualizzate sono simili a quelle riportate di seguito:

| | | | | |
|-----------------------------------|--|--|---|--|
| 443 (https) / tcp |  Decrypt (Resign) | <input type="checkbox"/> HTTPS | <input type="checkbox"/> Secure Web browser | <input type="checkbox"/> Skype Tunneling |
| 443 (https) / tcp |  Decrypt (Resign) | <input type="checkbox"/> HTTPS | <input type="checkbox"/> Secure Web browser | <input type="checkbox"/> Google |

Risoluzione dei problemi

Numero 1: Alcuni siti Web potrebbero non caricare sul browser Chrome

Esempio

www.google.com non può caricare con un Decrypt - Abbandona utilizzando Chrome.

Motivo

Il browser Google Chrome è in grado di rilevare certificati fraudolenti per proprietà google al fine di prevenire attacchi man-in-the-middle. Se il browser Chrome (client) tenta di connettersi a un dominio google.com (server) e viene restituito un certificato che non è un certificato google valido, il browser negherà la connessione.

Soluzione

Se si verifica questo problema, aggiungere una regola **Non decrittografare** per DN=*.google.com,

*.gmail.com, *.youtube.com. Quindi cancellare la cache e la cronologia del browser.

Numero 2: Visualizzazione di un avviso/errore non attendibile in alcuni browser

Esempio

Quando ci si connette a un sito utilizzando Internet Explorer e Chrome, non si riceve alcun avviso di protezione, tuttavia quando si utilizza il browser Firefox, è necessario considerare attendibile la connessione ogni volta che si chiude e si riapre il browser.

Motivo

L'elenco delle CA attendibili dipende dal browser. Quando si considera attendibile un certificato, questo non viene propagato tra i browser e la voce attendibile in genere rimane disponibile solo quando il browser è aperto, quindi, una volta chiuso, tutti i certificati considerati attendibili verranno eliminati e la volta successiva che si apre il browser e si visita il sito sarà necessario aggiungerlo di nuovo all'elenco dei certificati attendibili.

Soluzione

In questo scenario sia IE che Chrome utilizzano l'elenco di CA attendibili nel sistema operativo, ma Firefox mantiene il proprio elenco. Il certificato CA è stato quindi importato nell'archivio del sistema operativo ma non nel browser Firefox. Per evitare di ricevere l'avviso di protezione in Firefox, è necessario importare il certificato CA nel browser come CA attendibile.

Autorità di certificazione attendibili

Quando viene stabilita una connessione SSL, il browser verifica innanzitutto se il certificato è attendibile, ovvero se l'utente ha già visitato il sito e gli ha chiesto manualmente di considerare attendibile il certificato. Se il certificato non è considerato attendibile, il browser controlla il certificato dell'Autorità di certificazione (CA) che ha verificato il certificato per questo sito. Se il certificato CA è considerato attendibile dal browser, lo considera attendibile e consente la connessione. Se il certificato CA non è attendibile, nel browser viene visualizzato un avviso di protezione e viene forzata l'aggiunta manuale del certificato come attendibile.

L'elenco delle CA attendibili in un browser dipende completamente dall'implementazione del browser e ogni browser può compilarlo in modo diverso rispetto agli altri browser. In generale, esistono due modi in cui i browser correnti compilano un elenco di CA attendibili:

1. Utilizzano l'elenco di CA attendibili considerate attendibili dal sistema operativo
2. Contengono un elenco di CA attendibili con il software e sono incorporate nel browser.

Per i browser più comuni, le CA attendibili vengono popolate come segue:

- **Google Chrome:** Elenco di CA attendibili del sistema operativo
- **Firefox:** Gestisce il proprio elenco di CA attendibili
- **Internet Explorer:** Elenco di CA attendibili del sistema operativo
- **Safari:** Elenco di CA attendibili del sistema operativo

È importante conoscere la differenza perché il comportamento visualizzato sul client varia in base a questo. Ad esempio, per aggiungere una CA attendibile per Chrome e IE è necessario importare il certificato CA nell'archivio CA attendibile del sistema operativo. Se si importa il certificato CA nell'archivio delle CA attendibili del sistema operativo, non verrà più visualizzato alcun avviso

quando ci si connette a siti con un certificato firmato da questa CA. Nel browser Firefox è necessario importare manualmente il certificato CA nell'archivio delle CA attendibili nel browser stesso. In questo modo non verrà più visualizzato un avviso di protezione quando ci si connette a siti verificati da tale autorità di certificazione.

Riferimenti

- [Introduzione alle regole SSL](#)