Configurazione della decrittografia SSL sul modulo FirePOWER utilizzando ASDM (gestione integrata)

Sommario

Introduzione

In questo documento viene descritta la configurazione della decrittografia SSL (Secure Sockets Layer) sul modulo FirePOWER con ASDM (On-Box Management).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza del firewall ASA (Adaptive Security Appliance), ASDM (Adaptive Security Device Manager)
- Conoscenza dell'appliance FirePOWER
- Conoscenza del protocollo HTTPS/SSL

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Moduli ASA FirePOWER (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) con software versione 6.0.0 e successive
- Modulo ASA FirePOWER (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 5555-X) con software versione 6.0.0 e successive

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.

> **Nota:** Verificare che il modulo FirePOWER disponga di una licenza **Protect** per configurare questa funzionalità. Per verificare la licenza, selezionare **Configurazione > ASA FirePOWER Configuration > Licenza**.

Premesse

Il modulo Firepower decrittografa e controlla le connessioni SSL in entrata e in uscita a esso reindirizzate. Una volta che il traffico è decriptato, le applicazioni tunneling come Facebook chat ecc, vengono rilevate e controllate. I dati decrittografati vengono ispezionati alla ricerca di minacce, filtri URL, blocchi di file o dati dannosi.

Decrittografia SSL in uscita

Il modulo firepower funge da proxy di inoltro per le connessioni SSL in uscita intercettando le richieste SSL in uscita e rigenerando un certificato per il sito che l'utente desidera visitare. L'autorità emittente è il certificato autofirmato Firepower. Se il certificato di firepower non fa parte di una gerarchia esistente o se non viene aggiunto alla cache del browser di un client, il client riceve un avviso mentre accede a un sito protetto. Il metodo Decrypt-Resignmethod viene utilizzato per eseguire la decrittografia SSL in uscita.

Decrittografia SSL in ingresso

In caso di traffico in entrata verso un server Web o un dispositivo interno, l'amministratore importa una copia del certificato del server protetto e la chiave. Quando il certificato server SSL viene caricato sul modulo firepower e i criteri di decrittografia SSL sono configurati per il traffico in entrata, il dispositivo decrittografa e controlla il traffico mentre inoltra il traffico. Il modulo rileva quindi contenuti dannosi, minacce e malware che passano attraverso questo canale sicuro. Inoltre, il metodo Decrypt-Known Keymethod viene utilizzato per eseguire la decrittografia SSL in ingresso.

Configurazione per la decrittografia SSL

Esistono due metodi per decrittografare il traffico SSL.

- Decrittografa - Abbandona per traffico SSL in uscita
- Decrittografa - Noto per il traffico SSL in entrata

Decrittografia SSL in uscita (Decrittografia - Abbandona)

Il modulo Firepower agisce come MITM (man-in-the-middle) per qualsiasi negoziazione SSL per i server SSL pubblici. Rinuncia al certificato del server pubblico con un certificato CA intermedio configurato nel modulo firepower.

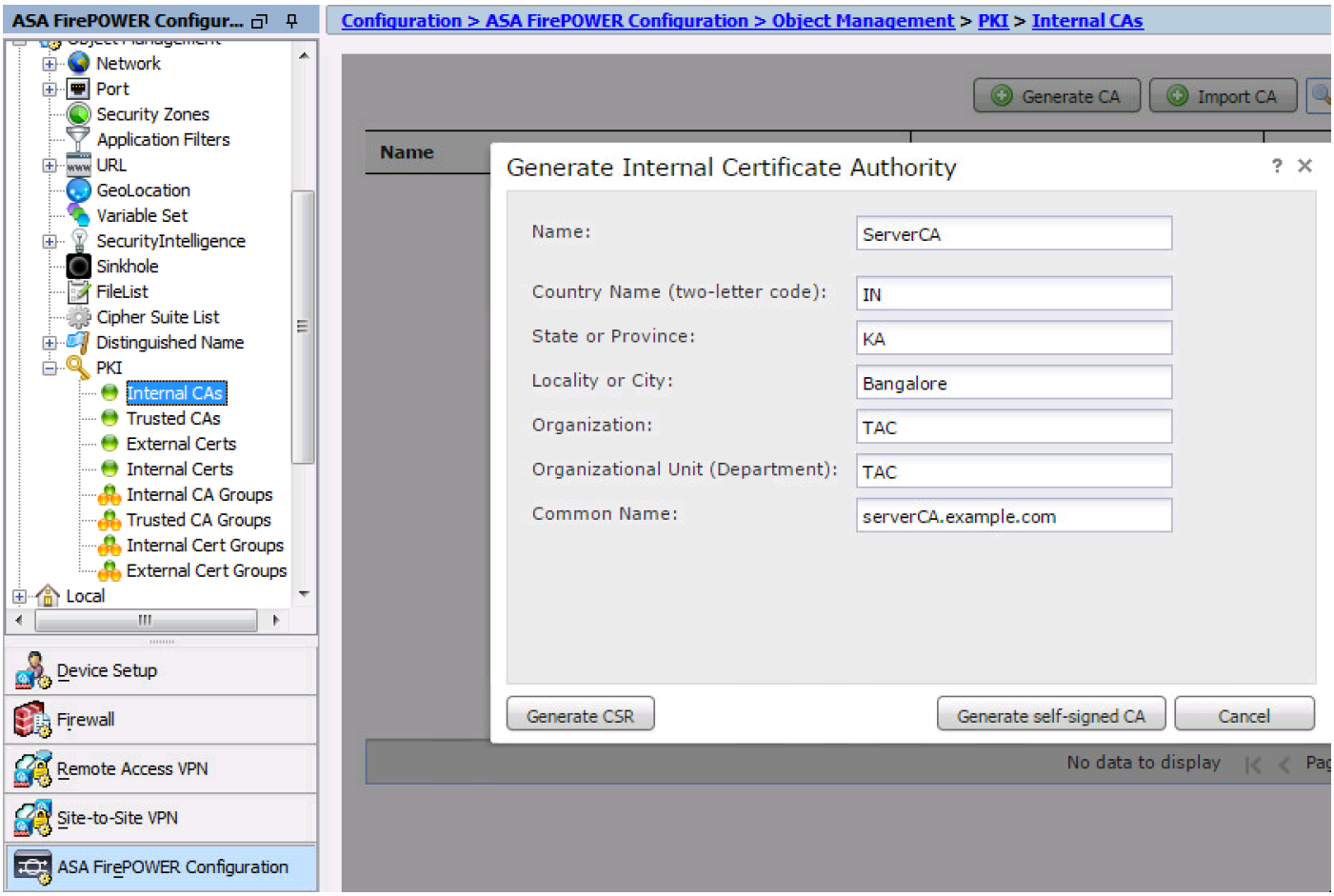
Di seguito vengono riportati i tre passaggi per configurare la decrittografia SSL in uscita.

Passaggio 1. Configurare il certificato CA.

Configurare un certificato autofirmato o un certificato intermedio di una CA attendibile per la revoca del certificato.

Configurare il certificato CA autofirmato

Per configurare il certificato CA autofirmato, selezionare **Configurazione > Configurazione ASA Firepower > Gestione oggetti > PKI > CA interne** e fare clic su **Genera CA**. Il sistema richiede i dettagli del certificato CA. Come mostrato nell'immagine, compilare i dettagli in base alle proprie esigenze.



Fare clic su **Genera CA autofirmata** per generare il certificato CA interno. Fare quindi clic su **Generate CSR** per generare la richiesta di firma del certificato, che viene quindi condivisa con il

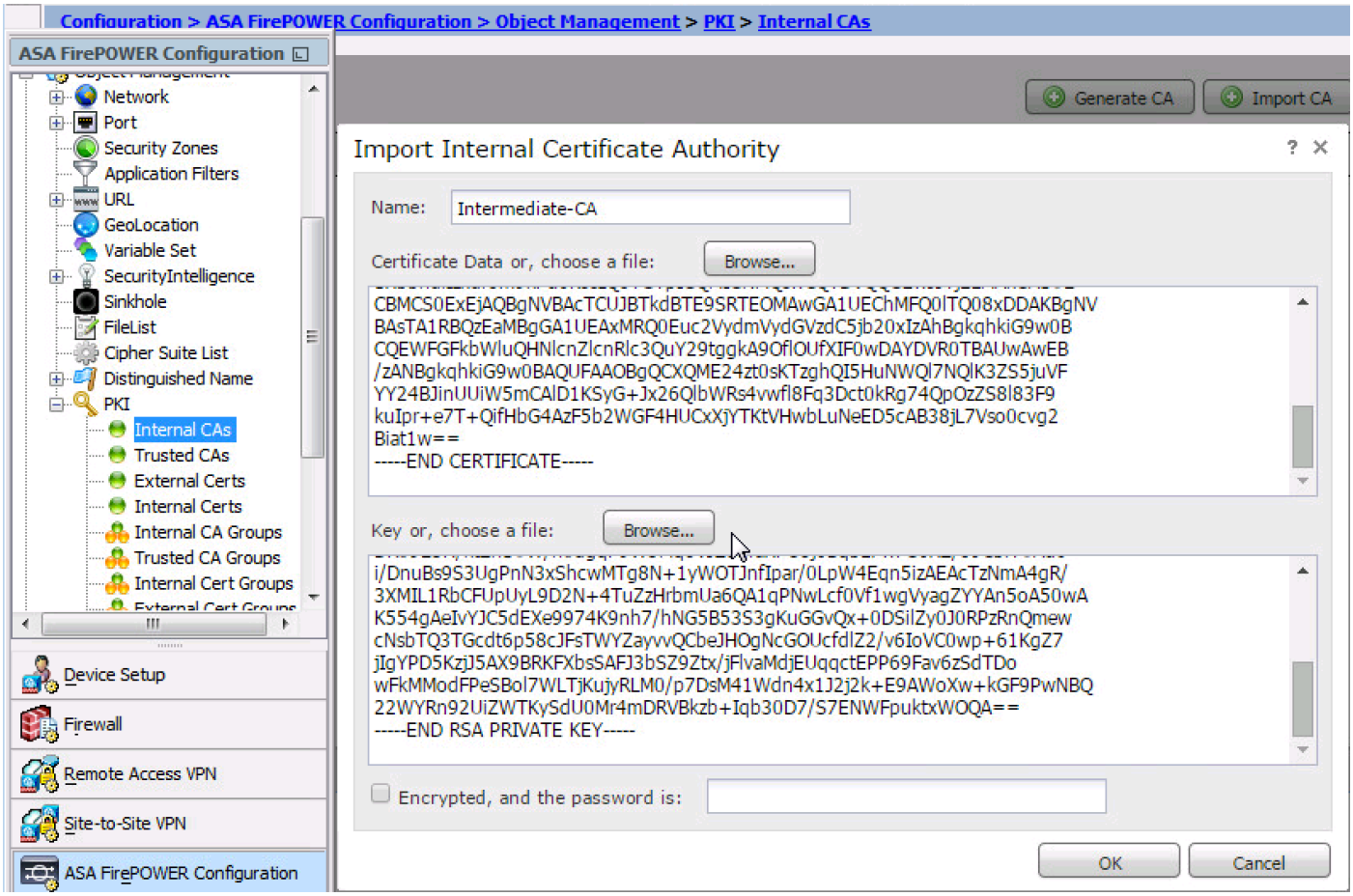
server CA per la firma.

Configurare il certificato CA intermedio

Per configurare il certificato CA intermedio firmato da un'altra CA di terze parti, selezionare **Configurazione > ASA Firepower Configuration > Object Management > PKI > CA interne** e fare clic su **Importa CA**.

Specificare il nome del certificato. Selezionare **Sfoglia** e carica il certificato dal computer locale oppure copiare e incollare il contenuto del certificato nell'opzione **Dati certificato**. Per specificare la chiave privata del certificato, sfogliare il file di chiave o copiare e incollare la chiave nell'opzione **Key**.

Se la chiave è crittografata, selezionare la casella di controllo **Crittografato** e specificare la password. Fare clic su **OK** per salvare il contenuto del certificato, come mostrato nell'immagine:



Passaggio 2. Configurare il criterio SSL.

Il criterio SSL definisce l'azione di decrittografia e identifica il traffico su cui viene applicato il metodo di decrittografia Decrypt-Resign. Configurare le regole SSL multiple in base ai requisiti aziendali e ai criteri di sicurezza dell'organizzazione.

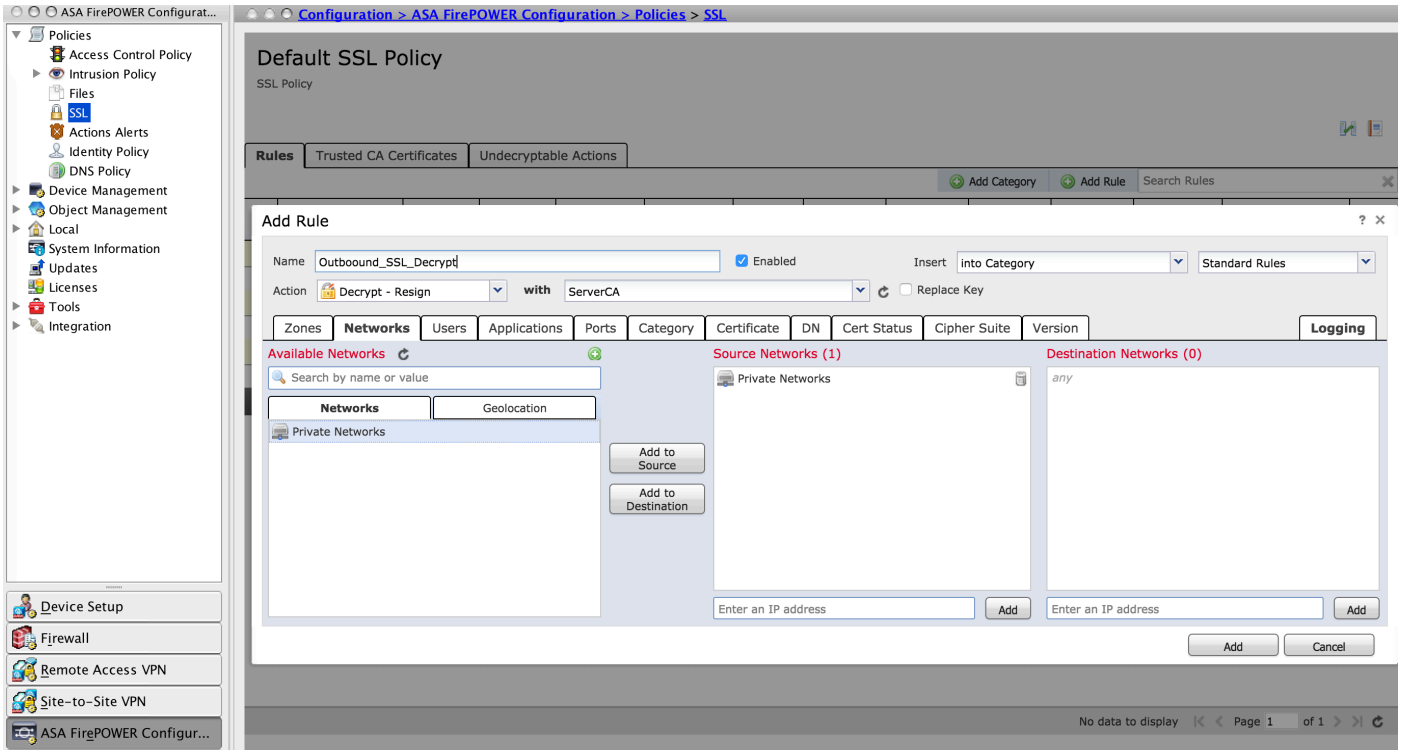
Per configurare il criterio SSL, selezionare **Configure > ASA FirePOWER Configuration > Policies > SSL** (Configurazione ASA FirePOWER > Criteri > SSL), quindi fare clic su **Add Rule** (Aggiungi regola).

Nome: specificare il nome della regola.

Azione: specificare l'azione come **Decrittografa - Abbandona** e scegliere il certificato CA dall'elenco a discesa configurato nel passaggio precedente.

Definire le condizioni nella regola per far corrispondere il traffico in quanto sono disponibili più opzioni (zona, rete, utenti e così via), specificate per definire il traffico da decrittografare.

Per generare gli eventi di decrittografia SSL, abilitare l'opzione di **registrazione** all'**accesso**, come mostrato nell'immagine:



Fare clic su **Add** per aggiungere la regola SSL.

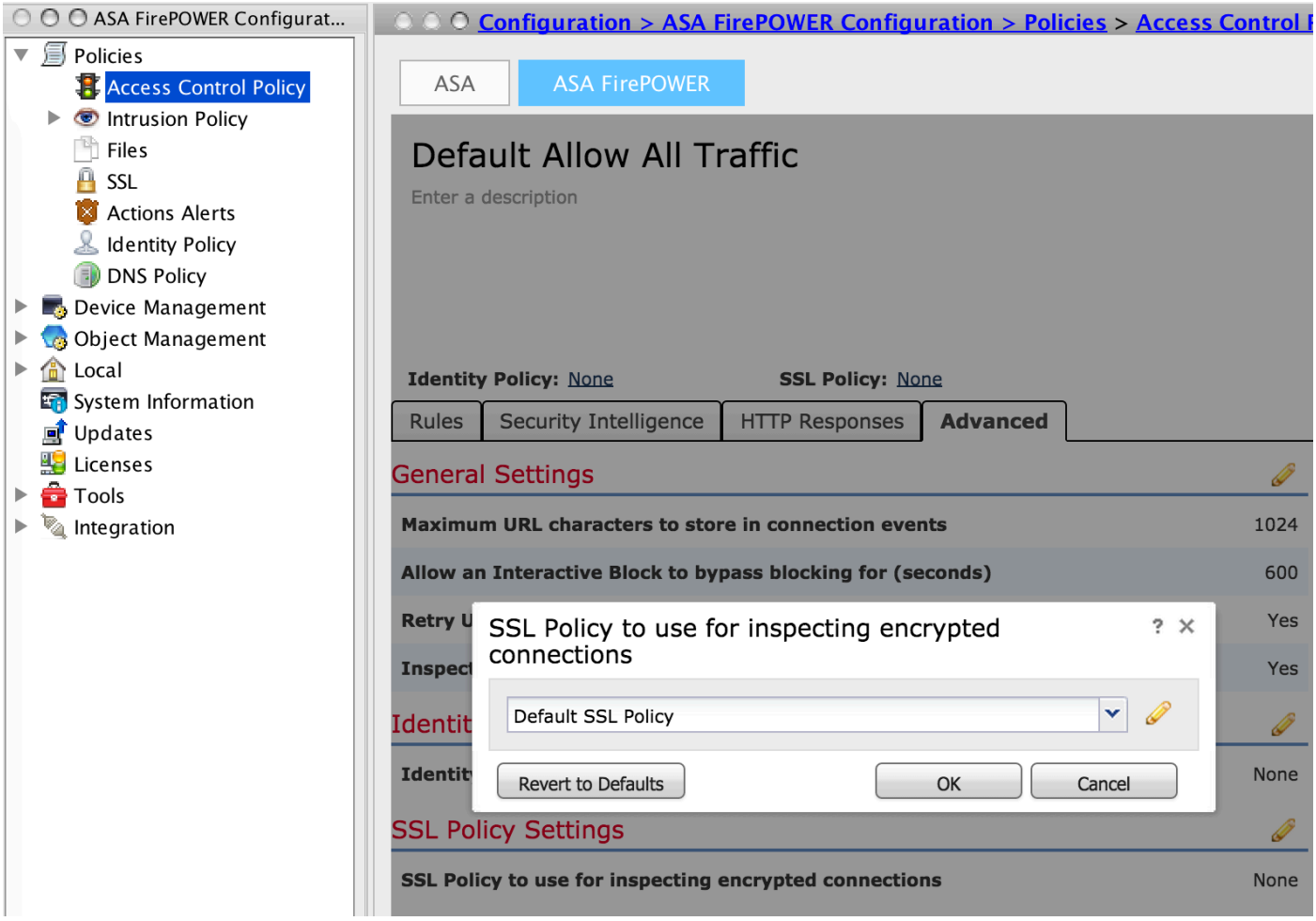
Fare clic su **Store ASA Firepower Changes** per salvare la configurazione del criterio SSL.

Passaggio 3. Configurare i criteri di controllo di accesso

Dopo aver configurato il criterio SSL con le regole appropriate, è necessario specificare il criterio SSL nel controllo di accesso per implementare le modifiche.

Per configurare il criterio di controllo dell'accesso, selezionare **Configurazione > Configurazione di ASA Firepower > Criteri > Controllo dell'accesso.**

Fare clic su **None** (Nessun criterio **SSL**) oppure selezionare **Advanced (Avanzate) > SSL Policy Setting (Impostazione criterio SSL). Specificare il criterio SSL dall'elenco a discesa e fare clic su OK** per salvarlo, come mostrato nell'immagine:



Clic **Archivia modifiche ASA Firepower** per salvare la configurazione del criterio SSL.

Ènecessario distribuire i criteri di controllo di accesso al sensore. Prima di applicare il criterio, è possibile che i **criteri di controllo di accesso non siano aggiornati** sul modulo. Per distribuire le modifiche al sensore, fare clic su **Distribuisci** e selezionare l'opzione **Distribuisci modifiche FirePOWER. Verificare le modifiche apportate e fare clic su Distribuisci.**

> **Nota:** Nella versione 5.4.x, se è necessario applicare la policy di accesso al sensore, fare clic su **Apply ASA FirePOWER Changes** (Applica modifiche FirePOWER ASA).

> **Nota:** Selezionare **Monitoraggio > Monitoraggio di ASA Firepower > Stato task.** È quindi necessario richiedere le modifiche alla configurazione per assicurarsi che l'attività sia stata completata.

Decrittografia SSL in ingresso (decrittografia - nota)

Il metodo Decrittografia SSL in entrata (Decrypt-Known) viene utilizzato per decrittografare il traffico SSL in entrata per il quale sono stati configurati il certificato server e la chiave privata. È necessario importare il certificato del server e la chiave privata nel modulo Firepower. Quando il traffico SSL colpisce il modulo Firepower, lo decrittografa ed esegue l'ispezione sul traffico decrittografato. Dopo l'ispezione, il modulo Firepower crittografa nuovamente il traffico e lo invia al server.

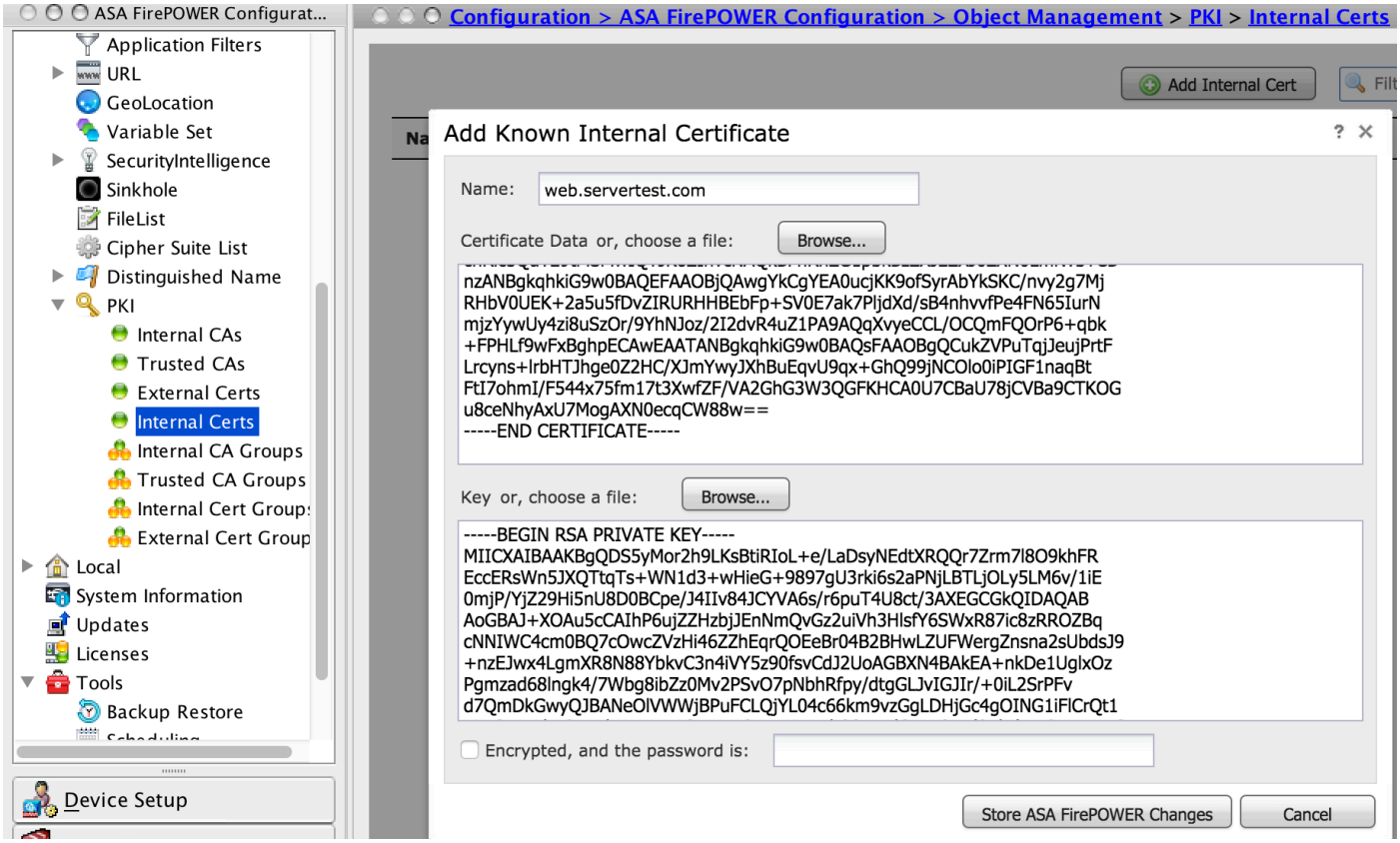
Di seguito vengono riportati i quattro passaggi per configurare la decrittografia SSL in uscita:

Passaggio 1. Importare il certificato e la chiave del server.

Per importare il certificato e la chiave del server, selezionare **Configurazione > ASA Firepower Configuration > Object Management > PKI > Internal Certs** (Configurazione > ASA Firepower > Gestione oggetti > PKI > Certificati interni), quindi fare clic su **Add Internal Cert** (Aggiungi certificato interno).

Come illustrato nell'immagine, specificare il nome del certificato. Selezionare **Sfoglia** per selezionare il certificato dal computer locale oppure copiare e incollare il contenuto del certificato nei **dati** del **certificato**. Per specificare la chiave privata del certificato, sfogliare il file di chiave o copiare e incollare la chiave nell'opzione **Chiave**.

Se la chiave è crittografata, selezionare la casella di controllo **Encrypted** e specificare la password, come mostrato nell'immagine:



Fare clic su **Store ASA FirePOWER Changes** per salvare il contenuto del certificato.

Passaggio 2. Importare il certificato CA (facoltativo).

Per i certificati server firmati da un certificato CA intermedio interno o radice, è necessario importare la catena interna di certificati CA nel modulo firepower. Al termine dell'importazione, il modulo firepower è in grado di convalidare il certificato del server.

Per importare il certificato CA, selezionare **Configurazione > Configurazione ASA Firepower > Gestione oggetti > CA attendibili** e fare clic su **Aggiungi CA attendibile** per aggiungere il certificato CA.

Passaggio 3. Configurare il criterio SSL.

Il criterio SSL definisce l'azione e i dettagli del server per cui si desidera configurare il metodo Decrypt-known per decrittografare il traffico in entrata. Se si dispone di più server interni, configurare più regole SSL in base a server diversi e al traffico che gestiscono.

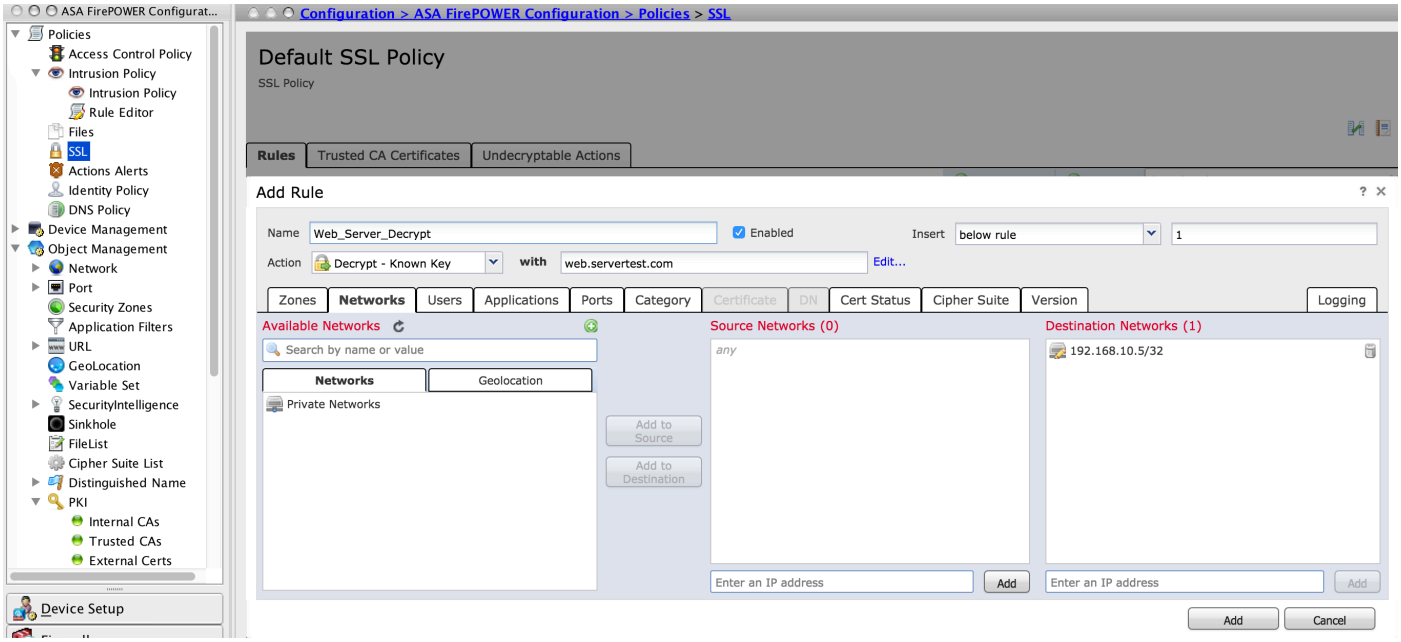
Per configurare il criterio SSL, selezionare **Configura > Configurazione ASA FirePOWER > Criteri > SSL** e fare clic su **Aggiungi regola**.

Nome: specificare il nome della regola.

Azione: specificare l'azione come **Decrittografa - nota** e scegliere il certificato CA dall'elenco a discesa configurato nel passaggio precedente.

Definire la condizione in modo che corrisponda a queste regole, poiché sono disponibili più opzioni (rete, applicazione, porte e così via) specificate per definire il traffico interessante del server per il quale si desidera abilitare la decrittografia SSL. Specificare la CA interna nella scheda **CA attendibili selezionate nella** scheda **Certificato CA attendibili.**

Per generare gli eventi di decrittografia SSL, abilitare l'opzione di **registrazione** all'**accesso**.



Fare clic su **Add** per aggiungere la regola SSL.

E quindi fare clic su **Store ASA Firepower Changes** per salvare la configurazione del criterio SSL.

Passaggio 4. Configurare i criteri di controllo di accesso.

Dopo aver configurato il criterio SSL con le regole appropriate, è necessario specificare il criterio SSL nel controllo di accesso per implementare le modifiche.

Per configurare il criterio di controllo dell'accesso, selezionare **Configurazione > Configurazione di ASA Firepower > Criteri > Controllo dell'accesso.**

Fare clic sull'opzione **None** accanto a **SSL Policy** (Criterio SSL) oppure selezionare **Advanced (Avanzate) > SSL Policy Setting** (Impostazione criterio SSL), specificare il criterio SSL dall'elenco

a discesa e fare clic su **OK** per salvarlo.

Clic **Archivia modifiche ASA Firepower** per salvare la configurazione del criterio SSL.

Ènecessario distribuire i criteri di controllo di accesso. Prima di applicare il criterio, è possibile visualizzare un'indicazione relativa ai criteri di controllo di accesso non aggiornata nel modulo. Per distribuire le modifiche al sensore, fare clic su **Distribuisci** e scegliere l'**opzione Distribuisci modifiche FirePOWER. Verificare le modifiche apportate e fare clic su Distribuisci** nella finestra popup.

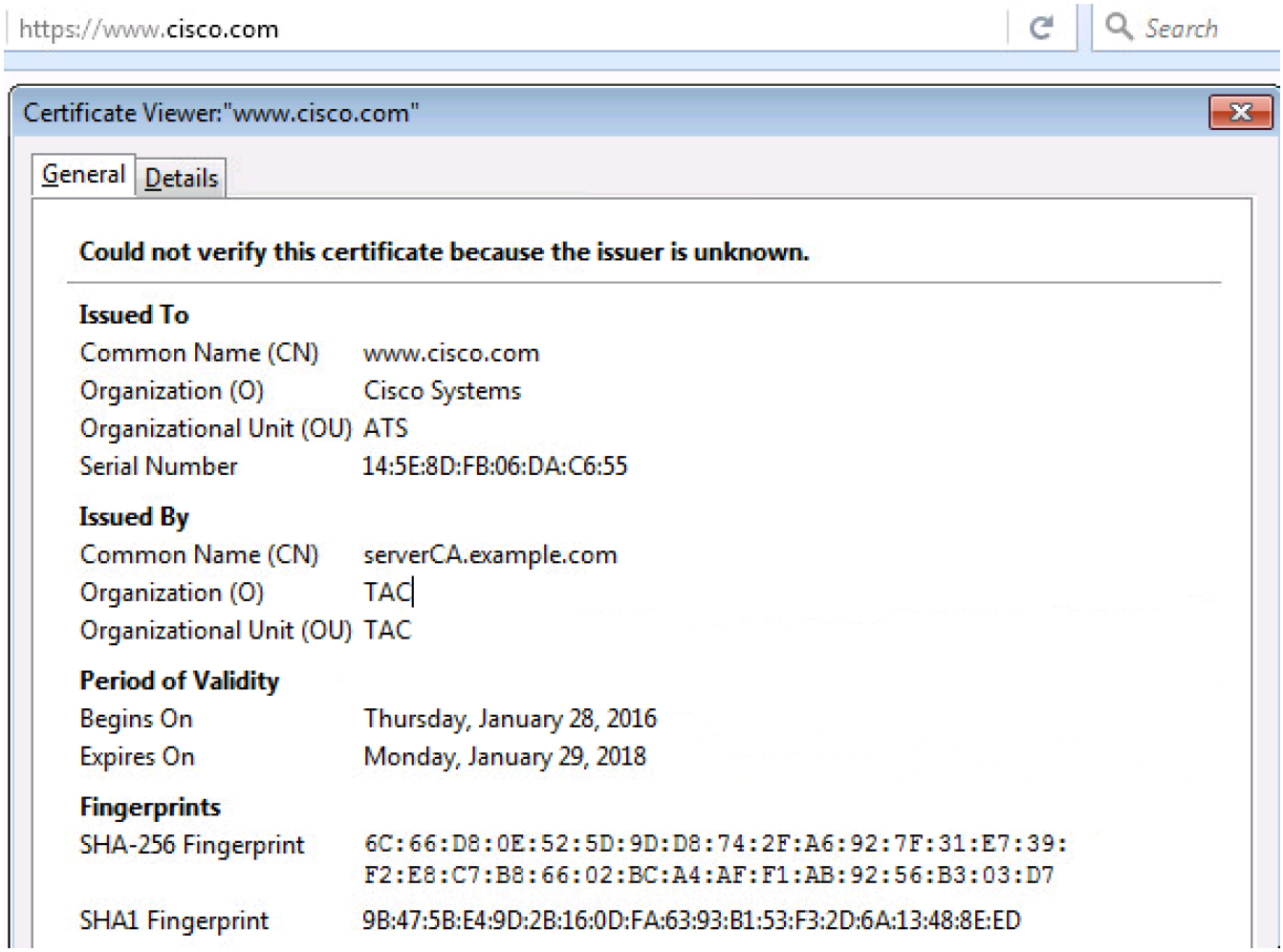
> **Nota:** Nella versione 5.4.x, se è necessario applicare la policy di accesso al sensore, fare clic su **Apply ASA FirePOWER Changes** (Applica modifiche FirePOWER ASA).

> **Nota:** Selezionare **Monitoraggio > Monitoraggio di ASA Firepower > Stato task.** È quindi necessario richiedere le modifiche alla configurazione per assicurarsi che l'attività sia stata completata.

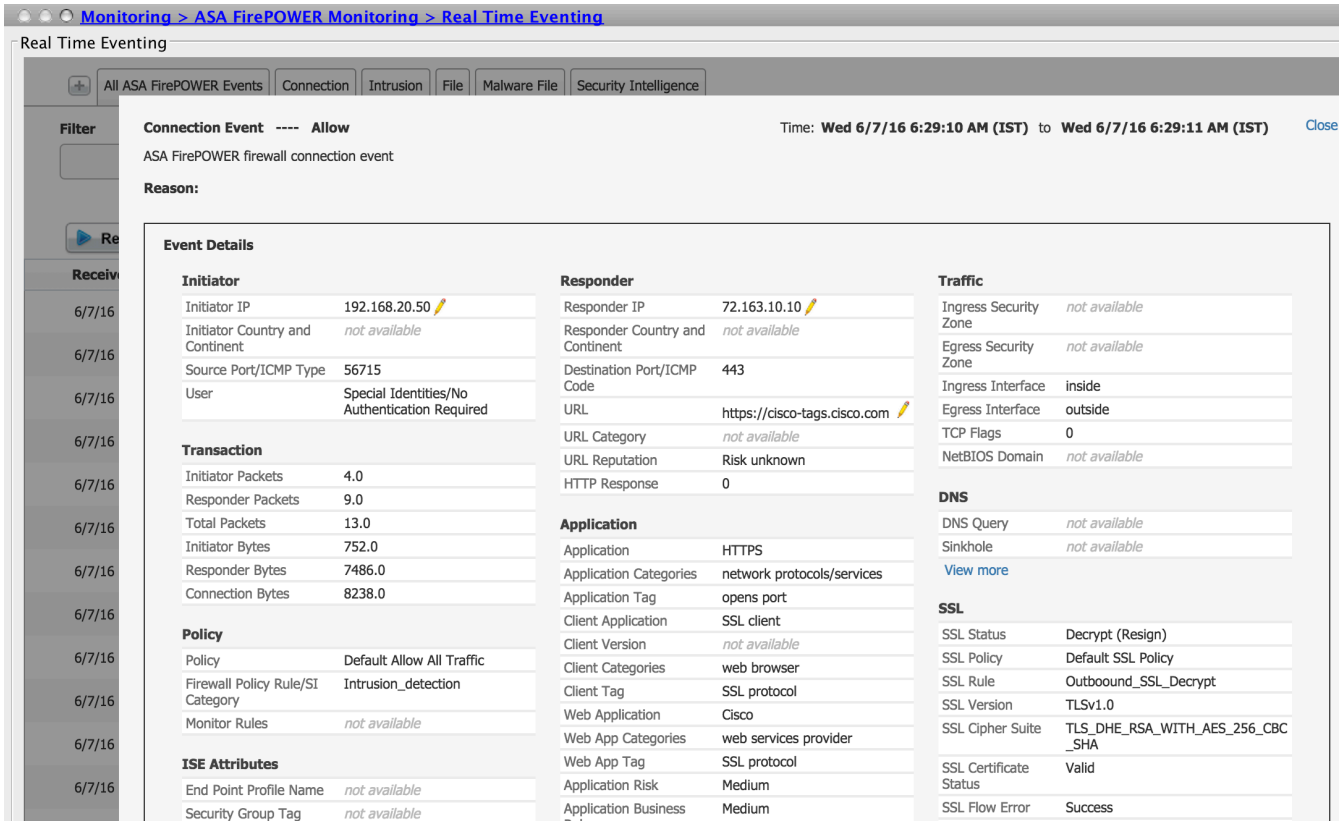
Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

- Per la connessione SSL in uscita, dopo aver esplorato un sito Web SSL pubblico dalla rete interna, il sistema visualizza un messaggio di errore del certificato. Controllare il contenuto del certificato e verificare le informazioni sulla CA. Viene visualizzato il certificato CA interno configurato nel modulo Firepower. Accettare il messaggio di errore per sfogliare il certificato SSL. Per evitare la visualizzazione del messaggio di errore, aggiungere il certificato CA all'elenco delle CA attendibili del browser.



- Controllare gli eventi di connessione per verificare quali criteri SSL e la regola SSL sono interessati dal traffico. Selezionare **Monitoraggio > ASA FirePOWER Monitoring > Real-Time Eventing.** Selezionare un evento e fare clic su **Visualizza dettagli**. Verificare le statistiche di decrittografia SSL.



- Verificare che la distribuzione dei criteri di controllo di accesso venga completata correttamente.
- Verificare che i criteri SSL siano inclusi nei criteri di controllo di accesso.
- Verificare che i criteri SSL contengano regole appropriate per la direzione in entrata e in uscita.
- Verificare che le regole SSL contengano la condizione corretta per definire il traffico di interesse.
- Monitorare gli eventi di connessione per verificare il criterio SSL e la regola SSL.
- Verificare lo stato di decrittografia SSL.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems