Configurazione dell'intelligence di sicurezza basata su dominio (criteri DNS) nel modulo FirePOWER con ASDM (gestione integrata)

Sommario

Introduzione

In questo documento viene descritto come configurare la funzionalità SI (Domain Based Security Intelligence) su un'appliance ASA con il modulo FirePOWER utilizzando Adaptive Security Device Manager (ASDM).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenza del firewall ASA (Adaptive Security Appliance)
- ASDM (Adaptive Security Device Manager)

- Knowledge Base del modulo FirePOWER

Nota: Il filtro di Security Intelligence richiede una licenza di Protection.

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

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

Premesse

Il sistema Firepower consente di intercettare le richieste di traffico DNS e cercare il nome di dominio dannoso. Se il modulo Firepower rileva un dominio dannoso, Firepower adotta le misure appropriate per ridurre la richiesta in base alla configurazione dei criteri DNS.

Nuovi metodi di attacco progettati per violare l'intelligence basata su IP, abusare delle funzionalità di bilanciamento del carico DNS per nascondere l'indirizzo IP effettivo di un server dannoso. Mentre gli indirizzi IP associati all'attacco vengono scambiati frequentemente dentro e fuori, il nome di dominio viene raramente modificato.

Firepower consente di reindirizzare la richiesta dannosa a un server sinkhole che può essere un server honeypot per rilevare, deviare o studiare i tentativi di sapere di più sul traffico di attacco.

Cenni preliminari su elenchi di domini e feed

Elenchi di domini e feed contiene l'elenco dei nomi di dominio dannosi, ulteriormente classificati nelle varie categorie in base al tipo di attacco. In genere, è possibile suddividere i feed in due tipi.

Elenchi di domini e feed forniti da Cisco TALOS

Attacker DNS: raccolta di nomi di dominio che analizzano continuamente le vulnerabilità o cercano di sfruttare altri sistemi.

DNS Bogon: insieme di nomi di dominio che non allocano ma rinviano il traffico, noti anche come IP falsi.

Bot DNS: insieme di nomi di dominio che partecipano attivamente come parte di una botnet e sono controllati da un controller botnet noto.

CnC DNS: insieme di nomi di dominio identificati come server di controllo per una rete Botnet nota.

Exploit kit DNS: Raccolta di nomi di dominio che tentano di sfruttare altri sistemi.

Malware DNS: raccolta di nomi di dominio che tentano di propagare malware o che attaccano attivamente chiunque li visiti.

DNS Open_proxy: raccolta di nomi di dominio che eseguono Open Web Proxies e offrono servizi di esplorazione Web anonimi.

DNS Open_relay: raccolta di nomi di dominio che offrono servizi di inoltro e-mail anonimi utilizzati da autori di spam e phishing.

Phishing DNS: raccolta di nomi di dominio che tentano attivamente di ingannare gli utenti finali affinché immettano informazioni riservate, ad esempio nomi utente e password.

Risposta DNS: raccolta di nomi di dominio osservati ripetutamente in modalità sospetta o dannosa.

Spam DNS: raccolta di nomi di dominio identificati come origine per l'invio di messaggi di posta indesiderata.

DNS sospetto: raccolta di nomi di dominio che mostrano attività sospette e sono sotto indagine attiva.

Tor_exit_node DNS: raccolta di nomi di dominio che offrono servizi di uscita dei nodi per la rete Tor Anonymizer.

Elenchi di domini e feed personalizzati

Blacklist globale per DNS: Raccolta dell'elenco personalizzato di nomi di dominio identificati come dannosi dall'amministratore.

White list globale per DNS: Raccolta dell'elenco personalizzato di nomi di dominio identificati come autentici dall'amministratore.

Configurare l'intelligence di sicurezza DNS

Per configurare le funzionalità di sicurezza intelligenti basate sul nome di dominio, è necessario eseguire più passaggi.

1. Configura feed/elenco DNS personalizzato (facoltativo)
2. Configurazione dell'oggetto Sinkhole (facoltativo)
3. Configurare i criteri DNS

4. Configurare i criteri di controllo di accesso
5. Distribuire i criteri di controllo di accesso

Passaggio 1. Configurare feed/elenchi DNS personalizzati (facoltativo).

Sono disponibili due elenchi predefiniti che consentono di aggiungere i domini. È possibile creare elenchi e feed personalizzati per i domini che si desidera bloccare.

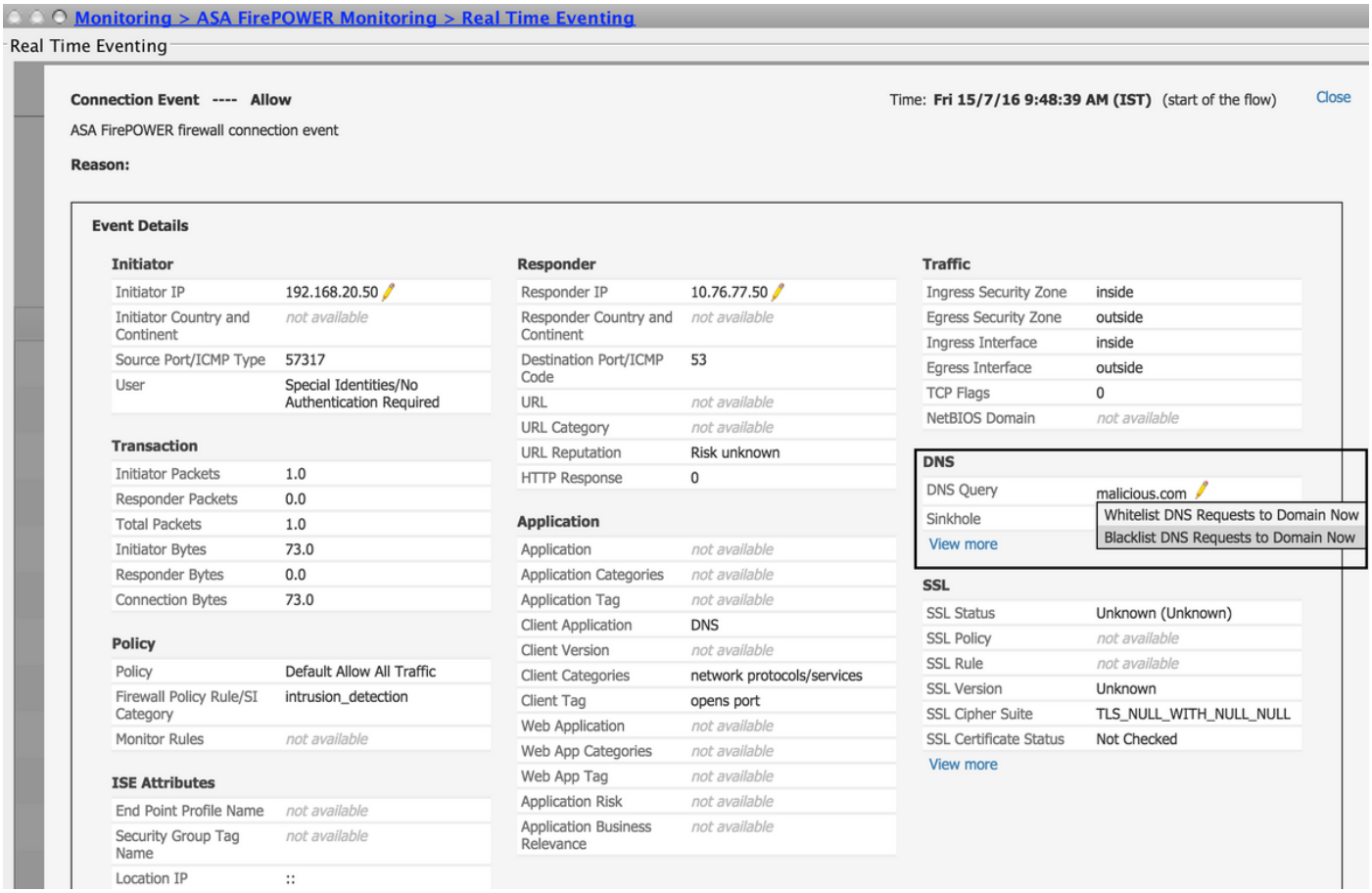
- Blacklist globale per DNS
- Whitelist globale per DNS

Aggiungi manualmente indirizzi IP alla lista nera globale e alla lista bianca globale

Il modulo Firepower consente di aggiungere determinati domini alla lista nera globale quando si è a conoscenza che fanno parte di attività dannose. È possibile aggiungere domini alla lista bianca globale anche se si desidera consentire il traffico verso alcuni domini bloccati da domini della lista nera. Se si aggiunge un dominio a Global-Blacklist/Global-Whitelist, questa viene applicata immediatamente senza che sia necessario applicarla.

Per aggiungere l'indirizzo IP alla lista nera globale, selezionare **Monitoraggio > ASA FirePOWER Monitoring > Real Time Eventing** (Monitoraggio FirePOWER ASA > Eventi in tempo reale), spostare il mouse sugli eventi di connessione e selezionare **View Details (Visualizza dettagli)**.

Èpossibile aggiungere domini alla lista nera globale/lista bianca globale. Fare clic su **Modifica** su DNS e selezionare **Whitelist DNS Requests to Domain Now/Blacklist DNS Requests to Domain Now** per aggiungere il dominio all'elenco corrispondente, come mostrato nell'immagine.



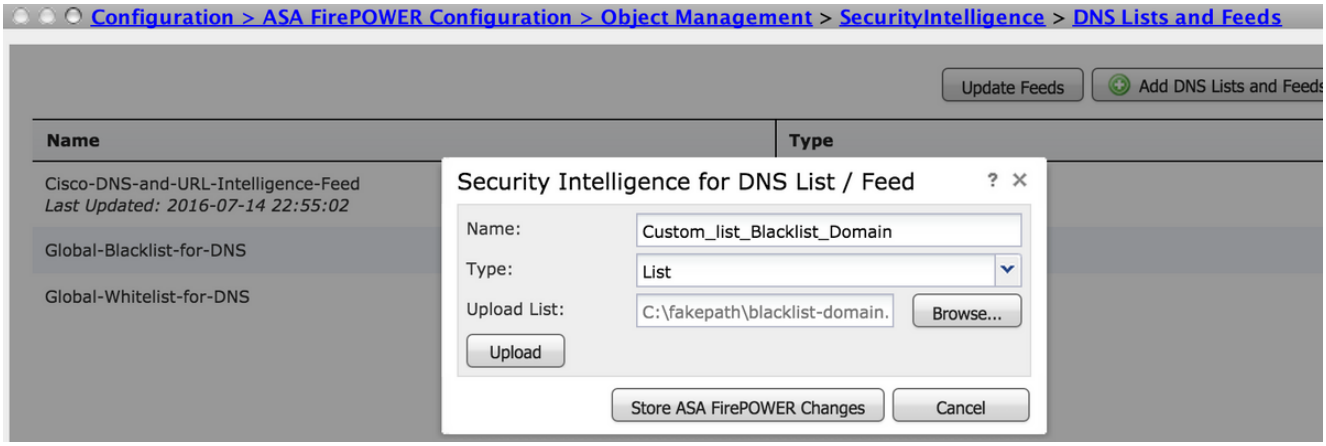
Per verificare che i domini siano stati aggiunti alla lista nera globale/lista bianca globale, selezionare **Configurazione > ASA FirePOWER Configuration > Object Management > SecurityIntelligence > DNS Lists and Feeds** e modificare **Global-Blacklist for DNS / Global Whitelist for DNS**. È inoltre possibile utilizzare il pulsante Elimina per rimuovere qualsiasi dominio dall'elenco.

Creare l'elenco personalizzato dei domini della blacklist

Firepower consente di creare un elenco di domini personalizzato da utilizzare per creare una blacklist (blocco) con due metodi diversi.

1. Èpossibile scrivere i nomi di dominio in un file di testo (un dominio per riga) e caricare il file nel modulo FirePOWER.

   Per caricare il file, selezionare **Configurazione > ASA FirePOWER Configuration > Object Management > SecurityIntelligence > DNS Lists and Feeds**, quindi selezionare **Add DNS Lists and Feeds** **Nome:** Specificare il nome dell'elenco Personalizzato. **Tipo:** **Selezionare Elenco** dall'elenco a discesa. **Elenco di caricamento:** Scegliere **Sfoglia** per individuare il file di testo nel sistema. Selezionare **Upload** per caricare il file.



   Fare clic su **Store ASA FirePOWER Changes** per salvare le modifiche.

2. Èpossibile utilizzare qualsiasi dominio di terze parti per l'elenco personalizzato per il quale il modulo Firepower può connettere il server di terze parti per recuperare l'elenco dei domini.

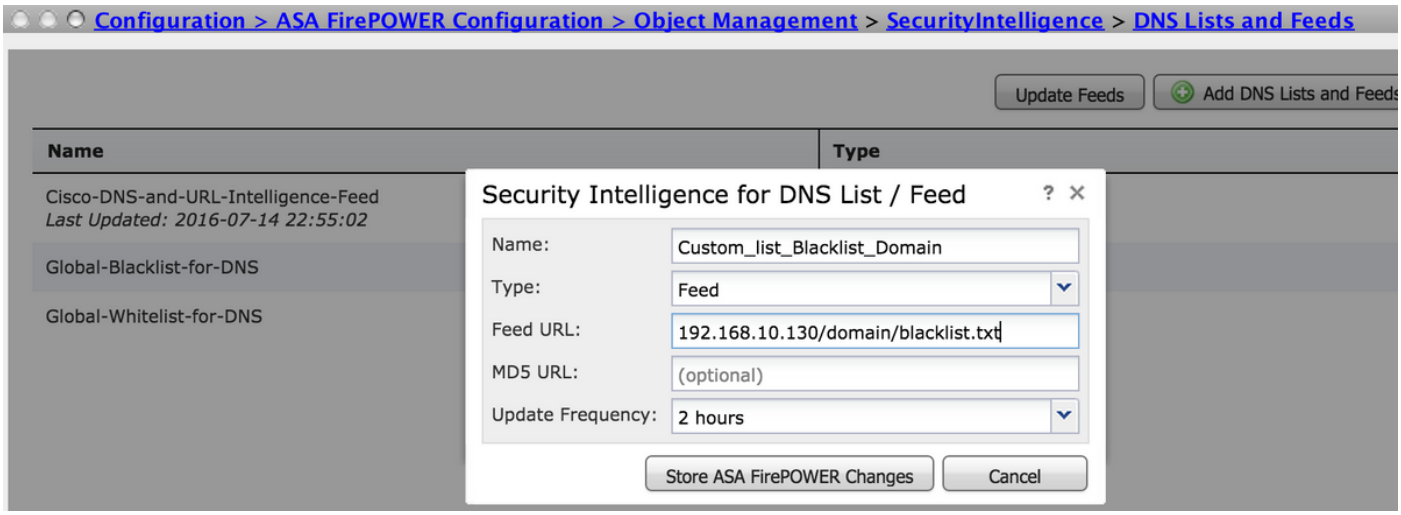
   Per configurare questa impostazione, selezionare **Configurazione > ASA FirePOWER Configuration > Object Management > Security Intelligence > DNS Lists and Feeds** e quindi selezionare **Add DNS Lists and Feeds**
   Nome: Specificare il nome del feed personalizzato.

   Tipo: Selezionare Feed dall'elenco a discesa.

   URL feed: Specificare l'URL del server a cui il modulo FirePOWER può connettersi e scaricare il feed.

   URL MD5: Specificare il valore hash per convalidare il percorso URL feed.

Frequenza aggiornamento: Specificare l'intervallo di tempo durante il quale il modulo si connette al server feed URL.



Selezionare **Store ASA FirePOWER Changes** per salvare le modifiche.

Passaggio 2. Configurare Un Oggetto Sinkhole (facoltativo).

L'indirizzo IP Sinkhole può essere utilizzato come risposta a una richiesta DNS dannosa. Il computer client ottiene l'indirizzo IP del server sinkhole per la ricerca di domini dannosi e,n il computer finale tenta di connettersi al server sinkhole. Quindi, il sinkhole può fungere da Honeypot per indagare sul traffico di attacco. Il sinkhole può essere configurato per attivare un indicatore di compromesso (IOC).

Per aggiungere il server sinkhole, selezionare **Configurazione > ASA FirePOWER Configuration > Object Management > Sinkhole** e fare clic sull'opzione **Add Sinkhole**.

Nome: Specificare il nome del server sinkhole.

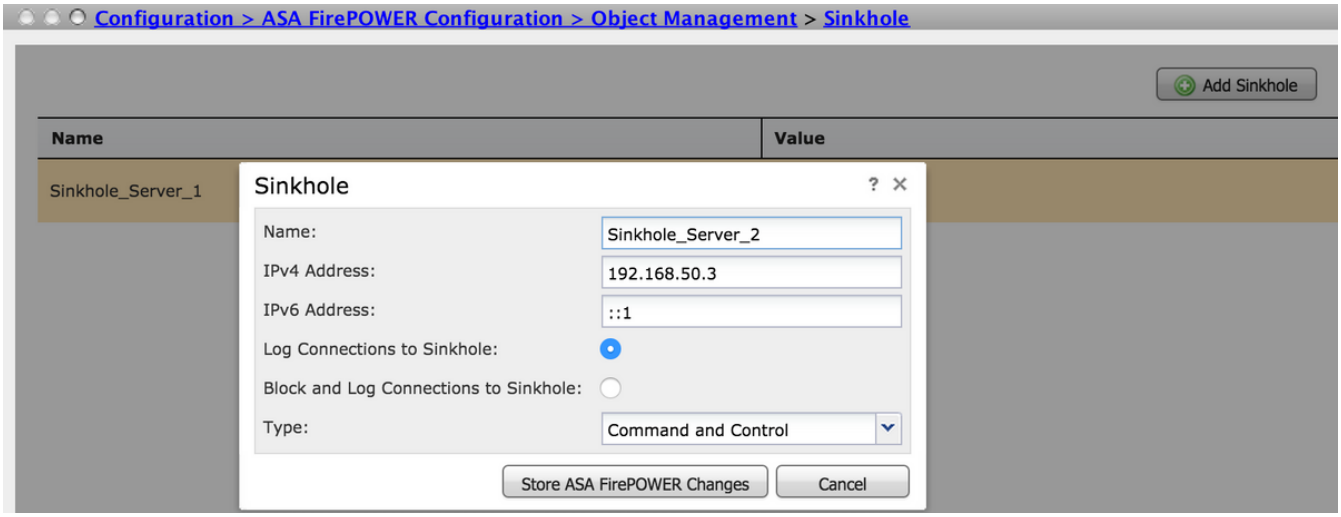
Indirizzo IP: Specificare l'indirizzo IP del server sinkhole.

Registra connessioni a Sinkhole: Abilitare questa opzione per registrare tutte le connessioni tra l'endpoint e il server sinkhole.

Blocca e registra connessioni a Sinkhole: Abilitare questa opzione per bloccare la connessione e registrare solo all'inizio della connessione di flusso. Se non è presente alcun server sinkhole fisico, è possibile specificare qualsiasi indirizzo IP e visualizzare gli eventi di connessione e il trigger IOC.

Tipo: Specificare il Feed dall'elenco a discesa per il quale si desidera selezionare il tipo di IOC (Indication of Compromise) associato agli eventi sinkhole. Ci sono tre tipi di IOC sinkhole che possono essere contrassegnati.

- Malware
- Comando e controllo
- Phishing



Passaggio 3. Configurare i criteri DNS.

Ènecessario configurare i criteri DNS per decidere l'azione per il feed/elenco DNS. Selezionare **Configurazione > Configurazione ASA FirePOWER > Criteri > Criteri DNS.**

Il criterio DNS predefinito contiene due regole predefinite. La prima regola, **Global Whitelist for DNS**, contiene l'elenco personalizzato del dominio consentito (**Global-Whitelist-for-DNS**). Questa regola è nella parte superiore da applicare prima che il sistema tenti di trovare una corrispondenza con qualsiasi dominio della lista nera. La seconda regola, **Elenco nero globale per DNS**, contiene l'elenco personalizzato del dominio bloccato (**Elenco nero globale per DNS**).

Èpossibile aggiungere altre regole per definire le varie azioni per gli **elenchi di domini e i feed forniti da Cisco TALOS**. Per aggiungere una nuova regola, selezionare **Aggiungi regola DNS.**

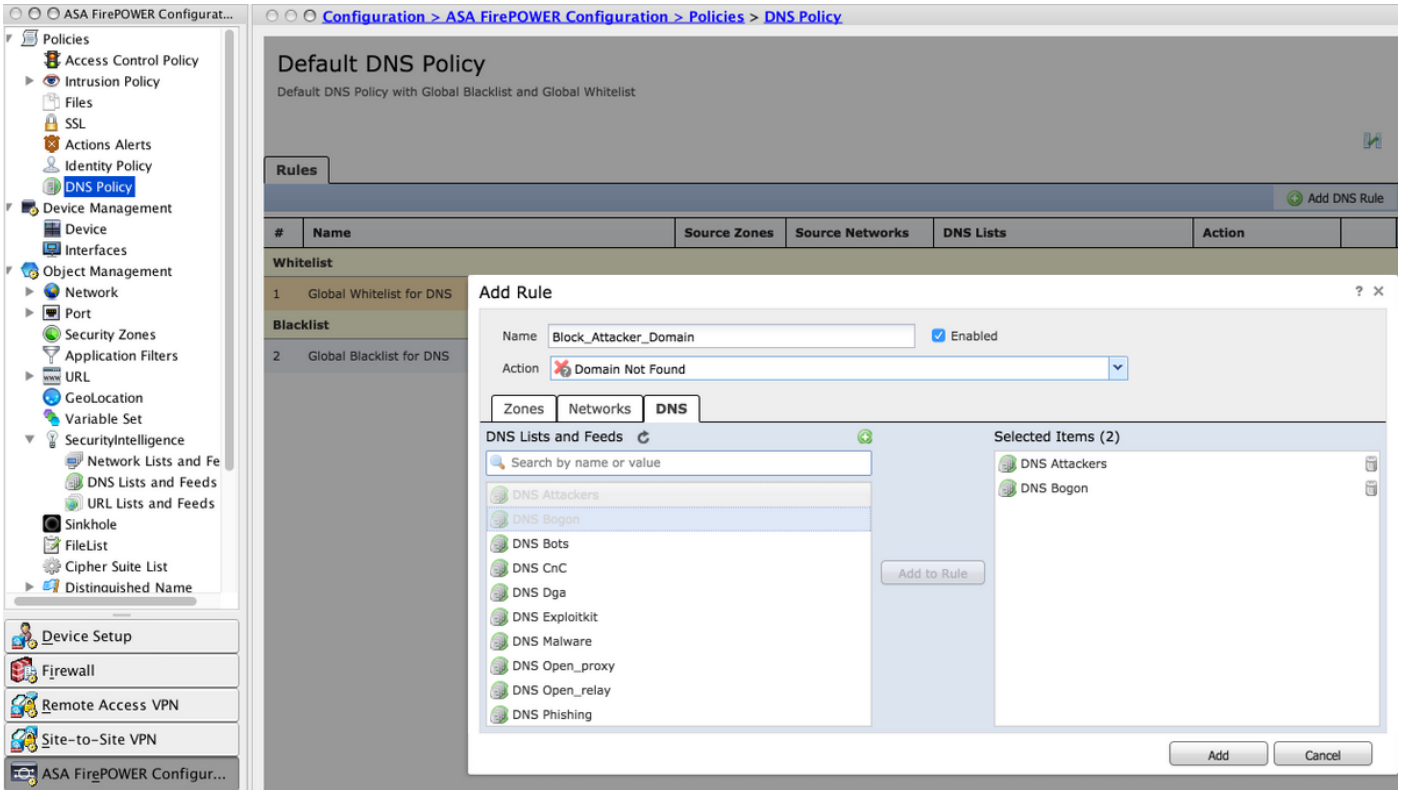
Nome: specificare il nome della regola.

Azione: Specificare l'azione da attivare quando la regola corrisponde.

- **Whitelist** In questo modo viene consentita la query DNS.
- **Monitor:** Questa azione genera l'evento per la query DNS e il traffico continua a corrispondere alle regole successive.
- **Dominio non trovato:** questa azione invia la risposta DNS come Dominio non trovato (Dominio inesistente).
- **Drop:** Questa azione blocca ed elimina automaticamente la query DNS.
- **Sinkhole** Questa azione invia l'indirizzo IP del server Sinkhole come risposta alla richiesta DNS.

Specificare le **zone/rete** per definire le condizioni della regola. Nella scheda DNS, scegliere l'opzione **Elenchi e feed DNS** e passare a **Elementi selezionati**, in cui è possibile applicare l'azione configurata.

Èpossibile configurare più regole DNS per diversi elenchi e feed DNS con un'azione diversa in base alle esigenze dell'organizzazione.

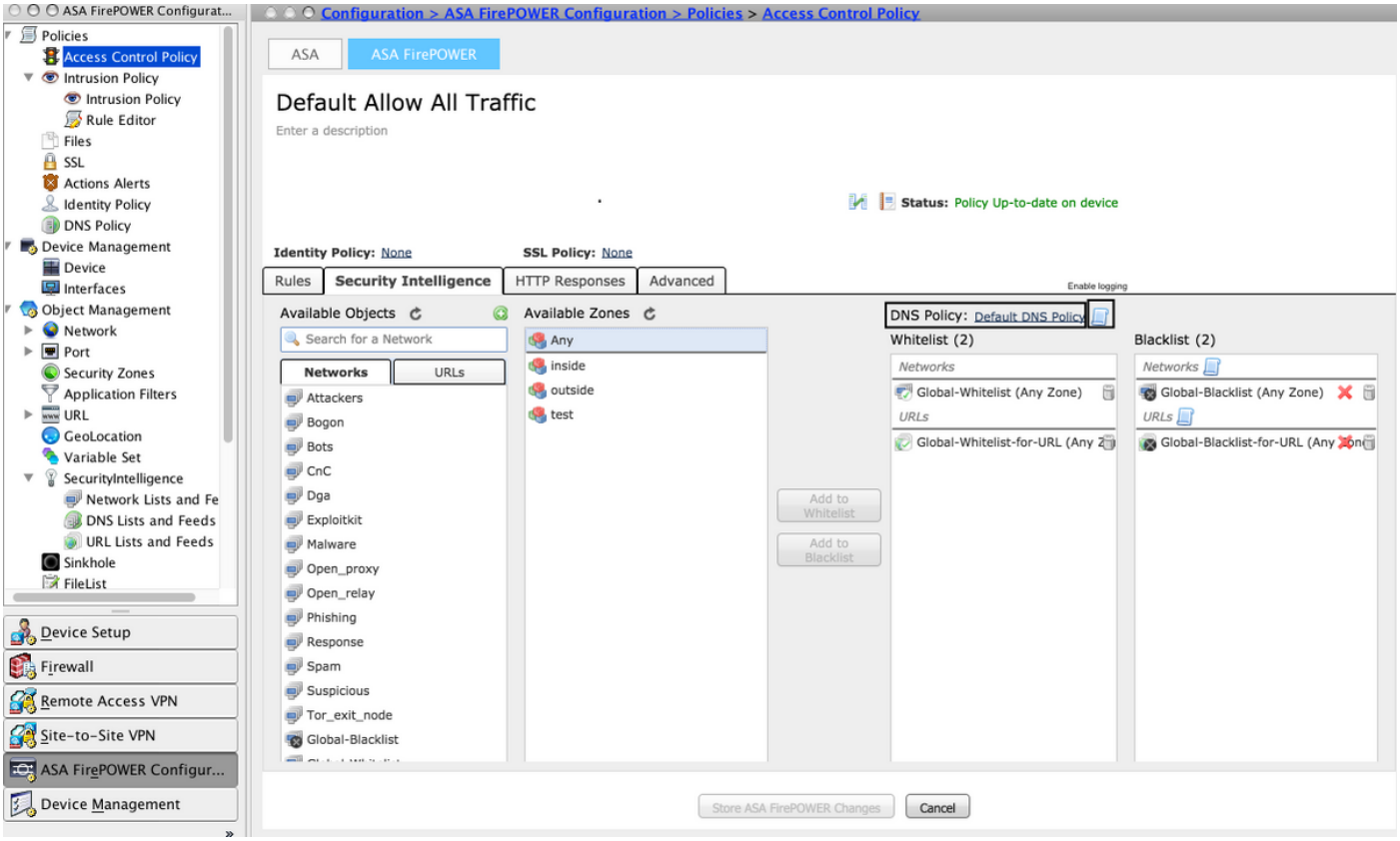


Fare clic sull'opzione **Add** (Aggiungi) per aggiungere la regola.

Passaggio 4. Configurare i criteri di controllo di accesso.

Per configurare l'intelligence di sicurezza basata su DNS, selezionare **Configurazione > Configurazione di ASA Firepower > Criteri > Criteri di controllo di accesso,** quindi selezionare la scheda **Intelligence di sicurezza**.

Verificare che il criterio DNS sia configurato e, facoltativamente, è possibile abilitare i registri facendo clic sull'icona dei registri come mostrato nell'immagine.



Scegliere l'opzione **Store ASA Firepower Changes** per salvare le modifiche ai criteri CA.

Passaggio 5. Distribuire i criteri di controllo di accesso.

Per rendere effettive le modifiche, è necessario distribuire i criteri di controllo di accesso. Prima di applicare il criterio, verificare se il criterio di controllo dell'accesso è obsoleto nel dispositivo.

Per distribuire le modifiche al sensore, fare clic su **Deploy**, scegliere **Deploy FirePOWER Changes** quindi selezionare **Deploy** nella finestra popup per distribuire le modifiche.

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

> **Nota:** Passare a **Monitoraggio > Monitoraggio ASA Firepower > Stato task. Per** confermare le modifiche alla configurazione, verificare che il task sia stato completato.

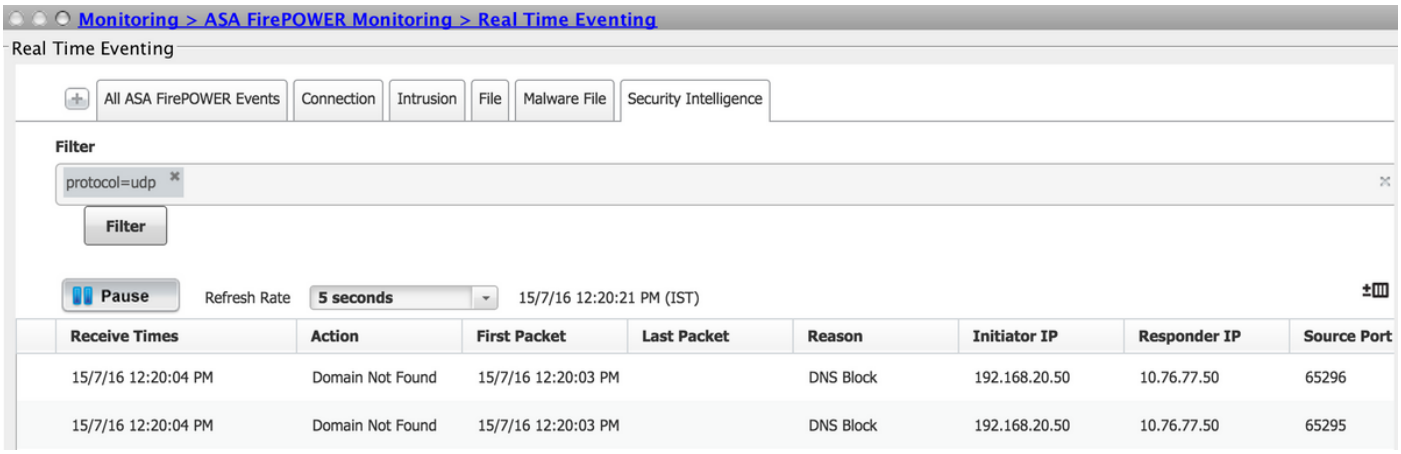
Verifica

Èpossibile verificare la configurazione solo se viene attivato un evento. A tale scopo, è possibile forzare una query DNS in un computer. È tuttavia necessario prestare attenzione alle ripercussioni derivanti dalla scelta di un server dannoso. Dopo aver generato questa query, è possibile visualizzare l'evento nella sezione **Eventi in tempo reale**.

Monitoraggio eventi di Security Intelligence DNS

Per visualizzare l'intelligence di sicurezza del modulo Firepower, selezionare **Monitoraggio > ASA**

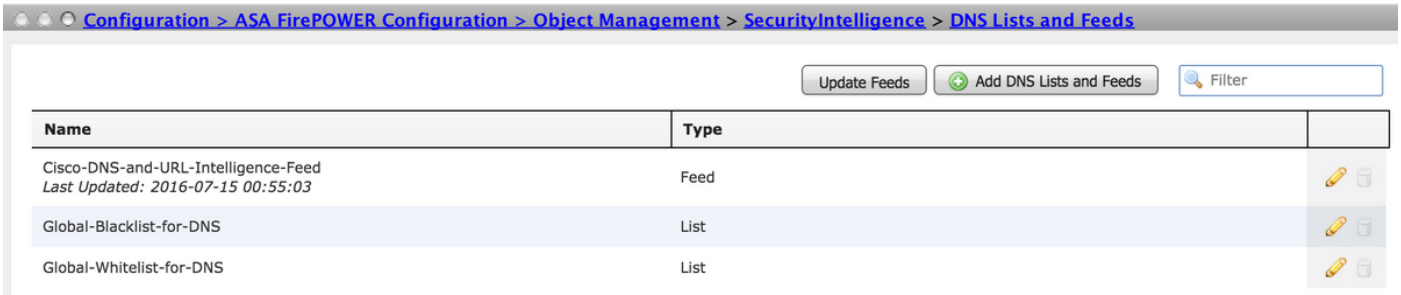
Firepower Monitoring > Real Time Eventing (Monitoraggio ASA Firepower > Eventi in tempo reale). Selezionare la scheda **Security Intelligence**. In questo modo vengono visualizzati gli eventi come mostrato nell'immagine:



Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Per verificare che i feed di Security Intelligence siano aggiornati, selezionare **Configurazione > ASA FirePOWER Configuration > Object Management > Security Intelligence > DNS Lists and Feeds** e controllare l'ora dell'ultimo aggiornamento dei feed. È possibile scegliere **Modifica** per impostare la frequenza di aggiornamento dei feed.



Verificare che la distribuzione dei criteri di controllo di accesso sia stata completata correttamente.

Controllare la scheda Eventi in tempo reale di Security Intelligence per verificare se il traffico è bloccato o meno.

Informazioni correlate

- Guida introduttiva al modulo Cisco ASA FirePOWER
- Documentazione e supporto tecnico – Cisco Systems