

Configurazione della blacklist IP durante l'uso di Cisco Security Intelligence tramite ASDM (gestione integrata)

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Panoramica sui feed di Security Intelligence](#)

[Aggiungi manualmente indirizzi IP alla lista nera globale e alla lista bianca globale](#)

[Creare l'elenco personalizzato dell'indirizzo IP della blacklist](#)

[Configurare la Security Intelligence](#)

[Distribuisce criteri di controllo di accesso](#)

[Monitoraggio degli eventi di Security Intelligence](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive la reputazione di Cisco Security Intelligence/indirizzo IP e la configurazione della blacklist IP (blocco) durante l'uso di feed personalizzati/automatici di indirizzi IP di bassa reputazione.

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

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

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 5.4.1 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.

Premesse

Cisco Security Intelligence comprende diverse raccolte di indirizzi IP aggiornate regolarmente che sono ritenute di scarsa reputazione dal team Cisco TALOS. Il team Cisco TALOS determina la bassa reputazione se una qualsiasi attività dannosa proviene da quegli indirizzi IP come spam, malware, attacchi di phishing, ecc.

Il feed di Cisco IP Security Intelligence tiene traccia del database di aggressori, bogon, bot, CnC, Dga, ExploitKit, malware, Open_proxy, Open_relay, phishing, Response, Spam, Suspicious. Il modulo Firepower non fornisce l'opzione per creare il feed personalizzato di un indirizzo IP di bassa reputazione.

Panoramica sui feed di Security Intelligence

Di seguito sono disponibili ulteriori informazioni sul tipo di raccolte di indirizzi IP che possono essere classificate come categorie diverse in Security Intelligence.

Attaccanti: Raccolta di indirizzi IP che analizzano continuamente le vulnerabilità o tentano di sfruttare altri sistemi.

Malware: Raccolta di indirizzi IP che tentano di propagare malware o che attaccano attivamente chiunque li visiti.

Phishing: Raccolta di host che tentano attivamente di indurre gli utenti finali a immettere informazioni riservate, come nomi utente e password.

Posta indesiderata: Raccolta di host identificati come origine dell'invio di messaggi di posta indesiderata.

Bot: Raccolta di host che partecipano attivamente come parte di una botnet e sono controllati da un controller di rete di bot noto.

CnC: Insieme di host identificati come server di controllo per una rete Botnet nota.

OpenProxy: Raccolta di host noti per eseguire proxy Web aperti e offrire servizi di esplorazione Web anonimi.

OpenRelay: Raccolta di host noti per offrire servizi di inoltro di e-mail anonimi utilizzati da autori di spam e phishing.

TorExitNode: Raccolta di host noti per offrire servizi di uscita dal nodo per la rete Tor Anonymizer.

Bogone: Raccolta di indirizzi IP non allocati che stanno inviando traffico.

Sospetto: Raccolta di indirizzi IP che mostrano attività sospette e sono sotto indagine attiva.

Risposta: Raccolta di indirizzi IP che sono stati ripetutamente osservati coinvolti nel comportamento sospetto o dannoso.

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

Il modulo Firepower consente di aggiungere determinati indirizzi IP alla lista nera globale quando si è a conoscenza che fanno parte di attività dannose. È inoltre possibile aggiungere indirizzi IP alla lista bianca globale se si desidera consentire il traffico verso determinati indirizzi IP bloccati da indirizzi IP della lista nera. Se si aggiunge un indirizzo IP alla lista nera globale/lista bianca globale, questa viene applicata immediatamente senza che sia necessario applicare il criterio.

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)**.

È possibile aggiungere l'indirizzo IP di origine o di destinazione alla lista nera globale. Fare clic sul pulsante **Edit** (Modifica) e selezionare **Whitelist Now/Blacklist Now** (Lista nera ora) per aggiungere l'indirizzo IP all'elenco corrispondente, come mostrato nell'immagine.

Monitoring > ASA FirePOWER Monitoring > Real Time Eventing

Real Time Eventing

+ All ASA FirePOWER Events Connection Intrusion File Malware File Security Intelligence

Filter
Rule Action=Allow *

Pause Refresh Rate 5 seconds 1/25/16 9:11:25 AM (IST)

Receive Times	Action	First Packet	Last Packet	Reason
1/25/16 9:09:50 AM	Allow	1/25/16 9:09:48 AM	1/25/16 9:09:49 AM	
1/25/16 9:07:36 AM	Allow	1/25/16 9:07:03 AM	1/25/16 9:07:03 AM	
1/25/16 9:07:07 AM	Allow	1/25/16 9:07:06 AM	1/25/16 9:07:06 AM	

Monitoring > ASA FirePOWER Monitoring > Real Time Eventing

Real Time Eventing

Initiator		Responder	
Initiator IP	192.168.20.3	Responder IP	10.106.44.55
Initiator Country and Continent	not available	Responder Country and Continent	not available
Source Port/ICMP Type	60297	Destination Port/ICMP	49153

Per verificare che l'indirizzo IP di origine o di destinazione sia stato aggiunto alla lista nera globale/lista bianca globale, selezionare **Configurazione > ASA Firepower Configuration > Object Management > Security Intelligence > Network Lists and Feeds** (Configurazione > ASA Firepower Configuration > Object Management > Security Intelligence > Elenchi e feed di rete) e modificare **Global-Blacklist/lista bianca globale**. È inoltre possibile utilizzare il pulsante Elimina per rimuovere qualsiasi indirizzo IP dall'elenco.

Creare l'elenco personalizzato dell'indirizzo IP della blacklist

Firepower consente di creare un elenco personalizzato di indirizzi di rete/IP da utilizzare nella lista nera (blocco). A tale scopo, è possibile procedere in tre modi:

- È possibile scrivere gli indirizzi IP in un file di testo (un indirizzo IP per riga) e caricare il file in Firepower Module. Per caricare il file, selezionare **Configurazione > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds** (Configurazione > ASA FirePOWER Configuration > Object Management > Security Intelligence > Elenchi e feed di rete), quindi fare clic su **Aggiungi elenchi e feed di rete**
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 l'opzione **Upload** per caricare il file.
- È possibile utilizzare qualsiasi database IP di terze parti per l'elenco personalizzato per il quale il modulo Firepower contatta il server di terze parti per recuperare l'elenco di indirizzi IP. Per configurare questa impostazione, selezionare **Configurazione > ASA FirePOWER**

Configuration > Object Management > Security Intelligence > Network Lists and Feeds, quindi fare clic su **Add Network Lists and Feeds**

Nome: Specificare il nome del feed personalizzato.

Tipo: Selezionare l'opzione **Feed** dall'elenco a discesa.

URL feed: Specificare l'URL del server a cui il modulo Firepower deve 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 sistema si connette al server feed URL.

The image contains two screenshots of the ASA FirePOWER configuration interface, specifically the 'Network Lists and Feeds' section. Both screenshots show a breadcrumb trail: Configuration > ASA FirePOWER Configuration > Object Management > SecurityIntelligence > Network Lists and Feeds. At the top right of each screenshot are buttons for 'Update Feeds' and 'Add Network Lists and Feeds'. On the left, there is a table with the following entries:

Name
Cisco-Intelligence-Feed <i>Last Updated: 2016-01-22 05:56:</i>
Custom_Feed
Global-Blacklist
Global-Whitelist

The first screenshot shows the 'Security Intelligence for Network List / Feed' dialog box with the following fields:

- Name: Custom_Feed
- Type: List
- Upload List: C:\fakepath\Custom_IP_Feed. (with a 'Browse...' button)
- Buttons: Upload, Store ASA FirePOWER Changes, Cancel

The second screenshot shows the same dialog box but with the 'Feed' type selected and additional fields:

- Name: Custom_Network_Feed
- Type: Feed
- Feed URL: http://192.168.30.1/blacklist-IP.txt
- MD5 URL: (optional)
- Update Frequency: 30 minutes
- Buttons: Store ASA FirePOWER Changes, Cancel

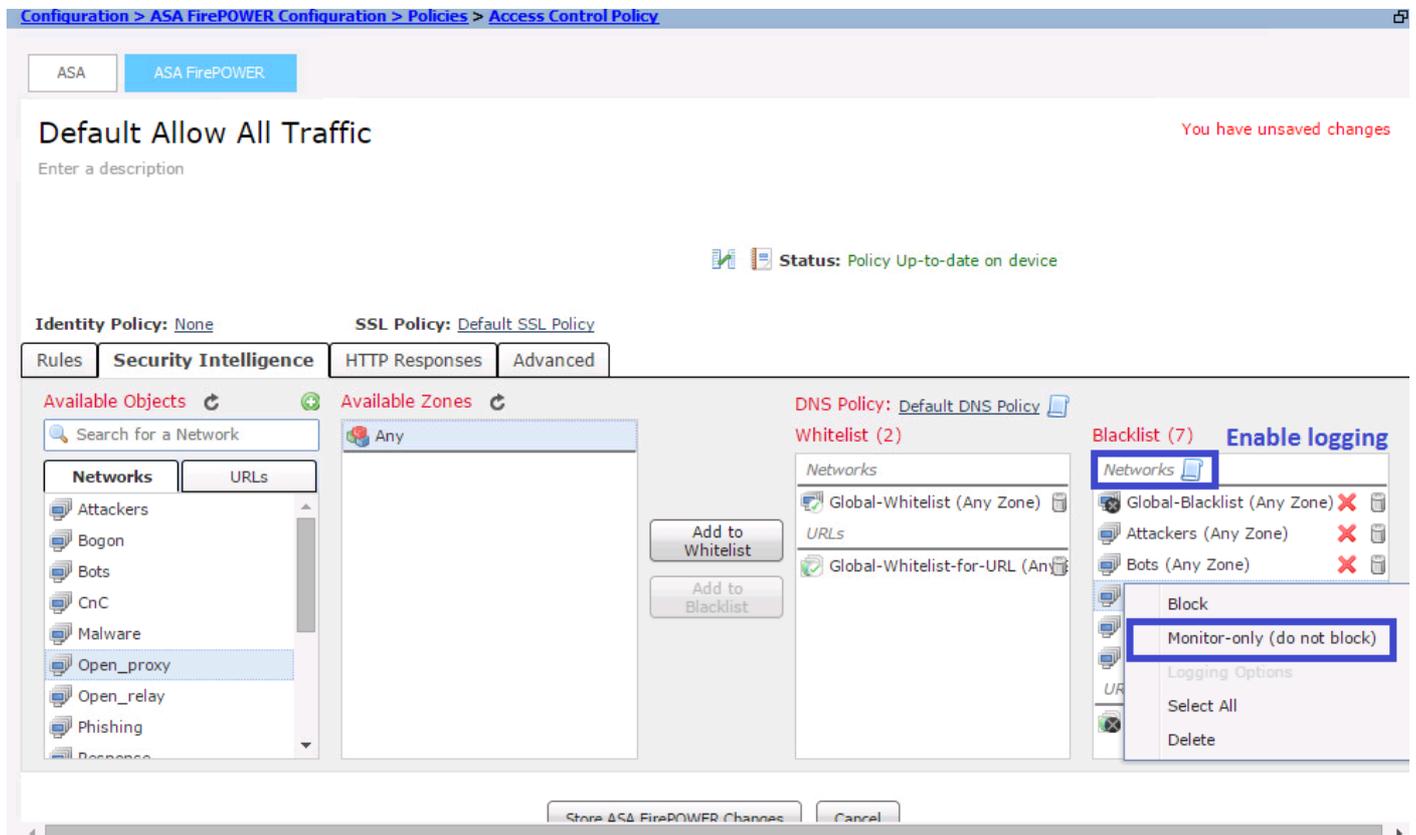
Configurare la Security Intelligence

Per configurare Security Intelligence, selezionare **Configurazione > ASA Firepower Configuration > Policy > Access Control Policy**, quindi selezionare la scheda **Security Intelligence**.

Scegliere il feed dalla colonna Network Available Object, spostarsi nella **colonna Whitelist/Blacklist** per consentire/bloccare la connessione all'indirizzo IP dannoso.

È possibile fare clic sull'icona e attivare la registrazione come specificato nell'immagine.

Se si desidera semplicemente generare l'evento per connessioni IP dannose invece di bloccare la connessione, quindi fare clic con il pulsante destro del mouse sul feed, scegliere **Monitor-only (non bloccare)**, come mostrato nell'immagine:

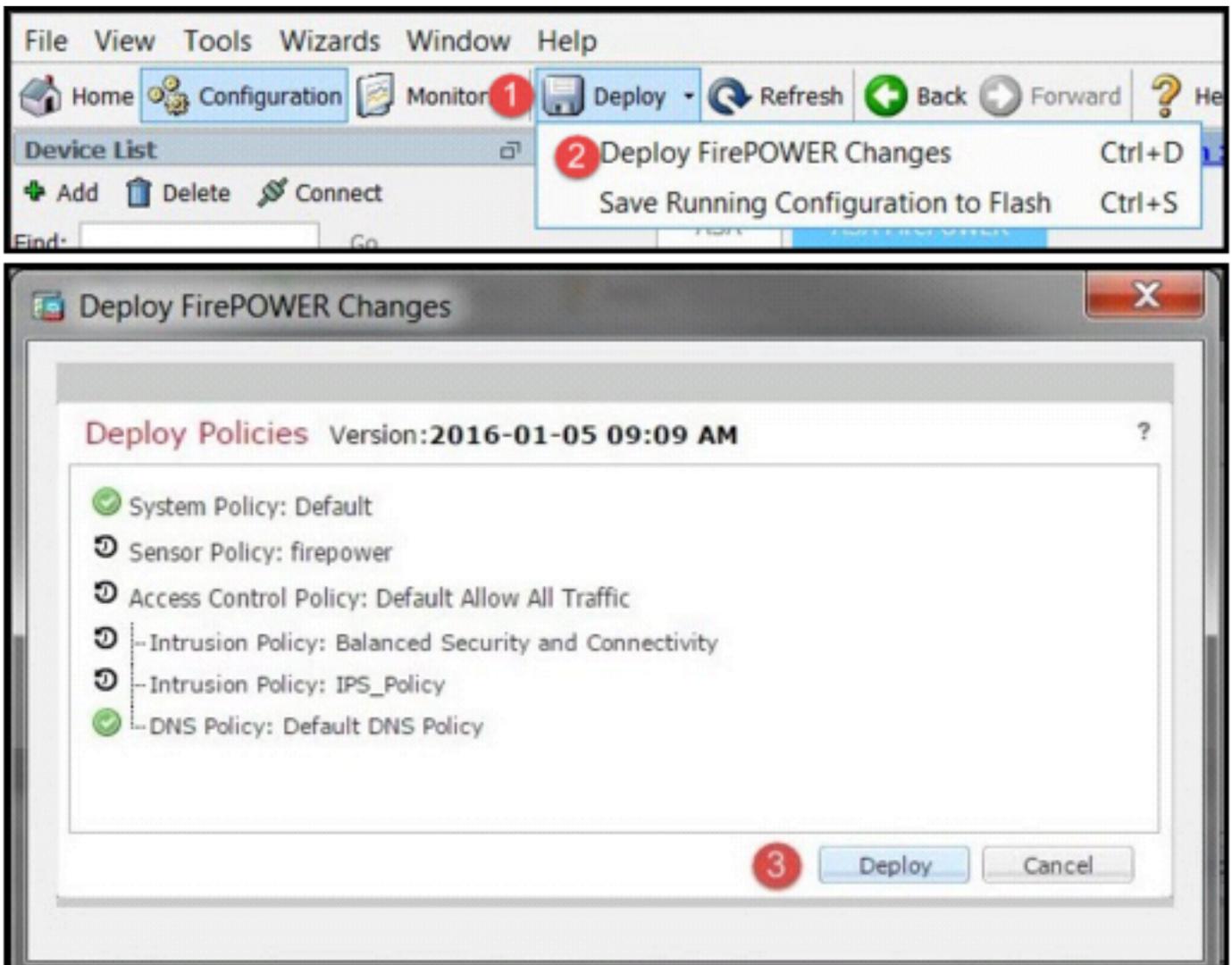


Scegliere l'opzione Store ASA Firepower Changes per salvare le modifiche ai criteri CA.

Distribuisci 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 implementare le modifiche al sensore, cFare clic su **Deploy** e 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 applicare le modifiche alla configurazione, verificare che il task sia stato completato.

Monitoraggio degli eventi di Security Intelligence

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**. Verranno visualizzati gli eventi come mostrato nell'immagine:

Monitoring > ASA FirePOWER Monitoring > Real Time Eventing

Real Time Eventing

All FirePOWER Events Connection Intrusion File Malware File Security Intelligence

Filter

Enter filter criteria

Pause Refresh Rate 5 seconds 2/9/16 1:03:31 PM (IST)

Receive Times	Action	First Packet	Last Packet	Reason	Initiator IP	Responder IP
2/9/16 1:01:48 PM	Block	2/9/16 1:01:47 PM		IP Block	192.168.20.3	184.26.162.43

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

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

Configuration > ASA FirePOWER Configuration > Object Management > SecurityIntelligence > Network Lists and Feeds

Update Feeds Add Network Lists and Feeds Filter

Name	Type	
Cisco-Intelligence-Feed Last Updated: 2016-02-08 10:03:14	Feed	 
Custom_Feed	Feed	 
Global-Blacklist	List	 
Global-Whitelist	List	 

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

Monitorare le funzionalità di sicurezza per verificare se il traffico è bloccato.

Informazioni correlate

- [Guida introduttiva al modulo Cisco ASA FirePOWER](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)