Konfigurieren von IP-Blacklisting unter Verwendung von Cisco Security Intelligence über ASDM (integriertes Management)

Inhalt

Einführung

Dieses Dokument beschreibt die Reputation von Cisco Security Intelligence/IP-Adressen und die Konfiguration von IP-Blacklisting (Blockierung) unter Verwendung benutzerdefinierter/automatischer Feeds mit IP-Adressen mit niedriger Reputation.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnis der ASA-Firewall (Adaptive Security Appliance), ASDM (Adaptive Security Device Manager)
- Fachkenntnis der FirePOWER-Appliance

Hinweis: Für die Filterung von Sicherheitsinformationen ist eine Schutzlizenz erforderlich.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASA FirePOWER-Module (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) mit Softwareversion 5.4.1 und höher
- ASA FirePOWER-Modul (ASA 5515-X, ASA 5525-X, ASA 5545-X, ASA 555-X) mit Softwareversion 6.0.0 und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

Cisco Security Intelligence besteht aus mehreren regelmäßig aktualisierten Auflistungen von IP-Adressen, die vom Cisco TALOS-Team als schlecht bekannt eingestuft werden. Das Cisco TALOS-Team ermittelt die geringe Reputation, wenn schädliche Aktivitäten von IP-Adressen wie Spam, Malware, Phishing-Angriffe usw. ausgehen.

Cisco IP Security Intelligence Feed verfolgt die Datenbank von Angreifern, Bogon, Bots, CnC, DGA, ExploitKit, Malware, Open_Proxy, Open_Relay, Phishing, Response, Spam, Verdächtig. Das FirePOWER-Modul bietet die Möglichkeit, einen benutzerdefinierten Feed mit IP-Adresse in niedriger Reputation zu erstellen.

Übersicht über Security Intelligence Feed

Im Folgenden finden Sie einige weitere Informationen über den Typ der IP-Adresserfassungen, die in den Sicherheitsinformationen als unterschiedliche Kategorien klassifiziert werden können.

Angreifer: Eine Sammlung von IP-Adressen, die ständig nach Schwachstellen durchsucht werden oder versuchen, andere Systeme auszunutzen.

Malware: Eine Sammlung von IP-Adressen, die versuchen, Malware zu verbreiten, oder aktiv jeden angreifen, der sie besucht.

Phishing: Sammlung von Hosts, die Benutzer aktiv dazu verleiten sollen, vertrauliche Informationen wie Benutzernamen und Kennwörter einzugeben.

Spam: Sammlung von Hosts, die als Quelle für das Senden von Spam-E-Mail-Nachrichten identifiziert wurden.

Bots: Eine Auflistung von Hosts, die aktiv als Teil eines Botnets beteiligt sind und von einem bekannten Botnet-Controller gesteuert werden.

CnC: Sammlung von Hosts, die als die Kontrollserver für ein bekanntes Botnet identifiziert wurden.

OpenProxy: Eine Auflistung von Hosts, die bekannte Open Web Proxies ausführen und anonyme Webbrowserdienste anbieten.

OpenRelay: Eine Sammlung von Hosts, die bekannte anonyme E-Mail-Weiterleitungsdienste anbieten, die von Spam- und Phishing-Angreifern verwendet werden.

TorExitNode: Sammlung von Hosts, die bekanntermaßen Exit Node Services für das Tor Anonymizer Netzwerk anbieten.

Bogon: Sammlung von IP-Adressen, die nicht zugewiesen sind, aber Datenverkehr senden.

Verdächtig: Erfassung von IP-Adressen, die verdächtige Aktivitäten anzeigen und aktiv untersucht werden.

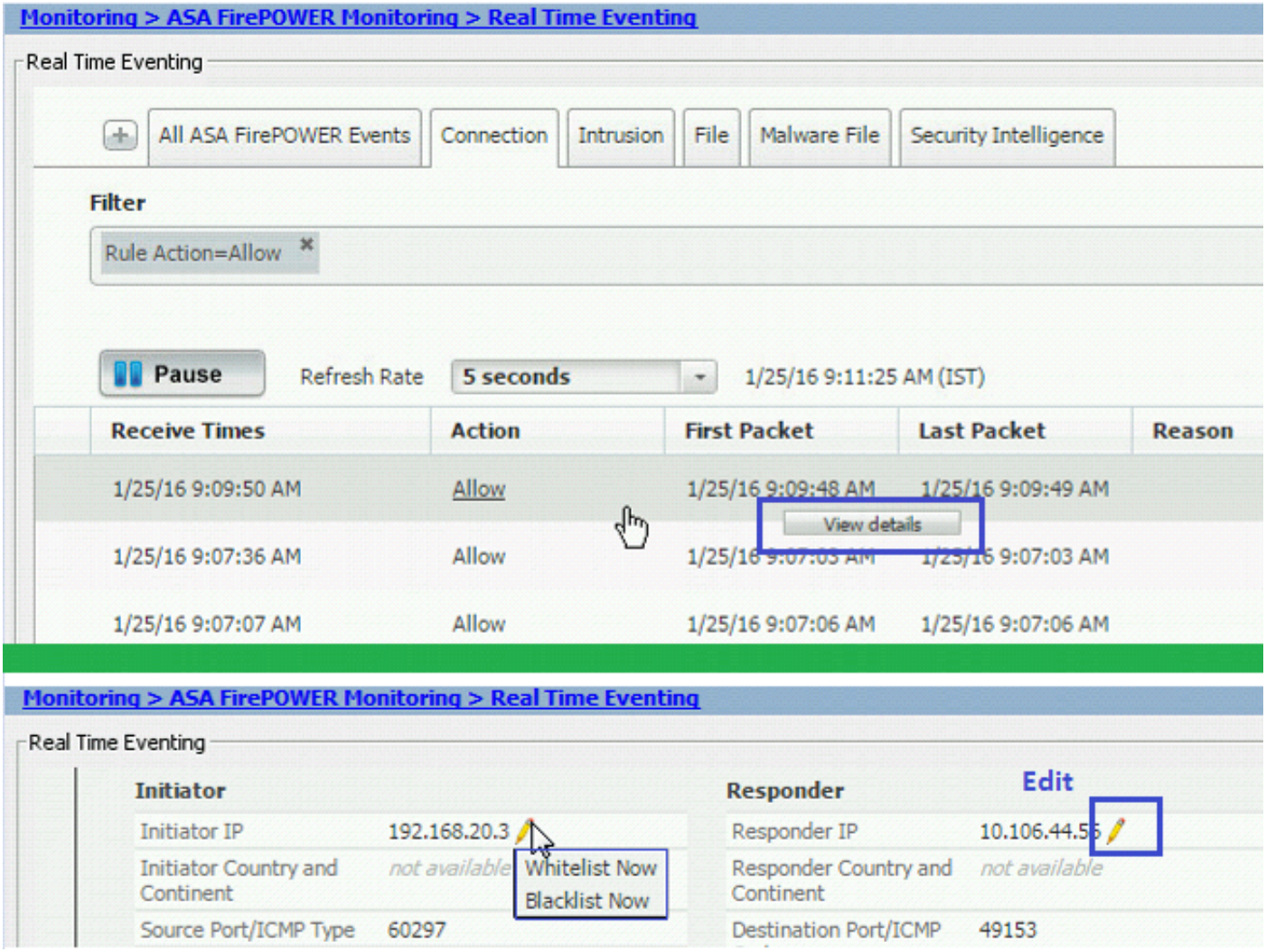
Antwort: Sammlung von IP-Adressen, die wiederholt bei verdächtigem oder schädlichem Verhalten beobachtet wurden.

Manuelles Hinzufügen von IP-Adressen zu Global-Blacklist und Global-Whitelist

Mit dem FirePOWER-Modul können Sie Global-Blacklist bestimmte IP-Adressen hinzufügen, wenn Sie wissen, dass diese Teil einer bösartigen Aktivität sind. IP-Adressen können auch Global-Whitelist hinzugefügt werden, wenn Sie den Datenverkehr an bestimmte IP-Adressen zulassen möchten, die von Blacklist-IP-Adressen blockiert werden. Wenn Sie Global-Blacklist/Global-Whitelist eine IP-Adresse hinzufügen, wird diese sofort wirksam, ohne dass die Richtlinie angewendet werden muss.

Um die IP-Adresse Global-Blacklist/Global-Whitelist hinzuzufügen, navigieren Sie zu **Monitoring > ASA FirePOWER Monitoring > Real Time Event**, bewegen Sie die Maus über Verbindungsereignisse, und wählen Sie **Details anzeigen aus**.

Sie können der Global-Blacklist/Global-Whitelist entweder die Quell- oder Ziel-IP-Adresse hinzufügen. Klicken Sie auf die Schaltfläche **Bearbeiten** und wählen Sie **Whitelist Now/Blacklist Now**, um die IP-Adresse der entsprechenden Liste hinzuzufügen, wie im Bild gezeigt.



Um zu überprüfen, ob die Quell- oder Ziel-IP-Adresse der Global-Blacklist/Global-Whitelist hinzugefügt wurde, navigieren Sie zu **Configuration > ASA Firepower Configuration > Object Management > Security Intelligence > Network Lists and Feeds** und bearbeiten Sie **Global-Blacklist/Global Whitelist**. Sie können auch die Schaltfläche Löschen verwenden, um alle IP-Adressen aus der Liste zu entfernen.

Erstellen der benutzerdefinierten Liste der Blacklist-IP-Adresse

Mit FirePOWER können Sie eine benutzerdefinierte Netzwerk-/IP-Adressenliste erstellen, die in Blacklists (Blockierungen) verwendet werden kann. Sie haben drei Möglichkeiten:

1. Sie können die IP-Adressen in eine Textdatei schreiben (eine IP-Adresse pro Leitung) und die Datei in das FirePOWER-Modul hochladen. Um die Datei hochzuladen, navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds** und klicken Sie dann auf **Add Network Lists and Feeds (Netzwerklisten und -Feeds hinzufügen).** **Name:** Geben Sie den Namen der benutzerdefinierten Liste an. **Typ:** Wählen Sie **List** aus der Dropdown-Liste aus. **Upload-Liste:** Wählen Sie **Durchsuchen**, um die Textdatei in Ihrem System zu suchen. Wählen Sie die Option **Hochladen** aus, um die Datei hochzuladen.
2. Sie können eine beliebige IP-Datenbank eines Drittanbieters für die benutzerdefinierte Liste verwenden, für die das FirePOWER-Modul den Drittanbieter-Server kontaktiert, um die IP-Adressliste abzurufen. Um dies zu konfigurieren, navigieren Sie zu **Configuration > ASA**

FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds und klicken Sie dann auf **Add Network Lists and Feeds (Netzwerklisten und -Feeds hinzufügen).**

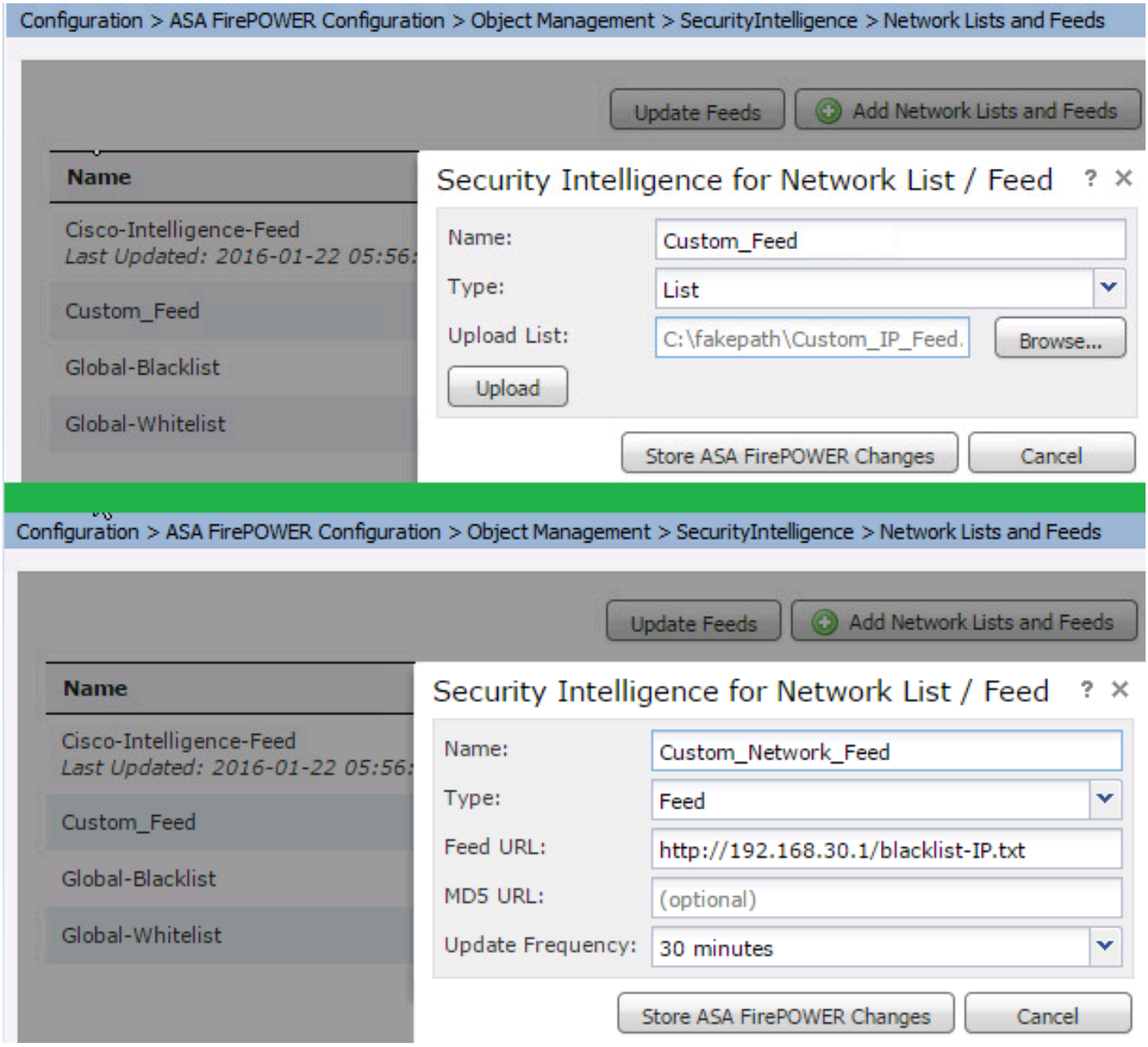
Name: Geben Sie den Namen des benutzerdefinierten Feeds an.

Typ: Wählen Sie Option **Feed** aus der Dropdown-Liste aus.

Feed-URL: Geben Sie die URL des Servers an, zu dem das FirePOWER-Modul eine Verbindung herstellen soll, und laden Sie den Feed herunter.

MD5-URL: Geben Sie den Hashwert an, um den URL-Pfad für den Feed zu validieren.

Aktualisierungshäufigkeit: Geben Sie das Zeitintervall an, in dem das System eine Verbindung zum URL-Feed-Server herstellt.



Konfigurieren der Sicherheitsintelligenz

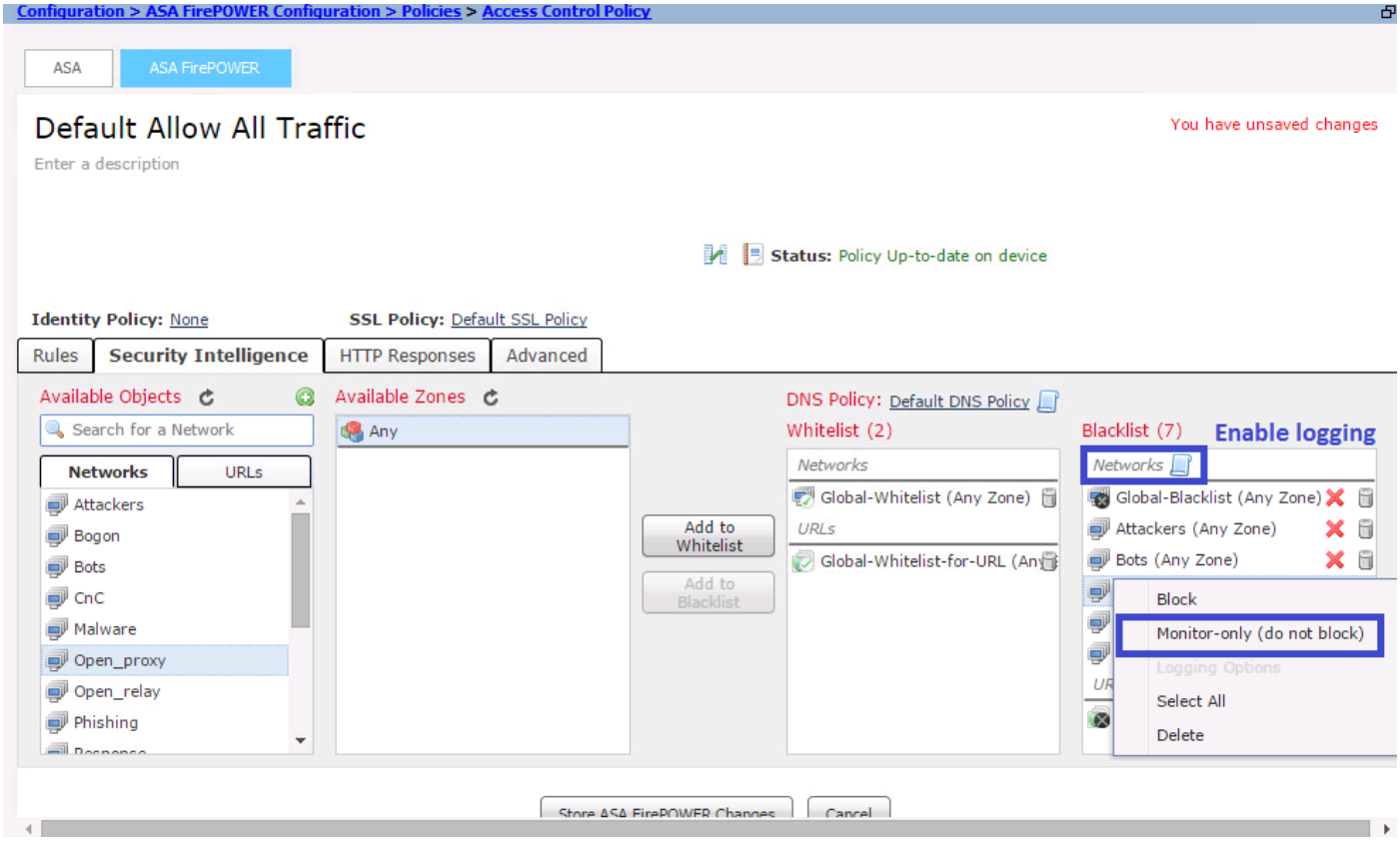
Navigieren Sie zum Konfigurieren von Sicherheitsinformationen zu **Configuration > ASA**

FirePOWER Configuration > Policies > Access Control Policy (Konfiguration > ASA FirePOWER-Konfiguration > Richtlinien > Zugriffskontrollrichtlinie), und wählen Sie die Registerkarte **Security Intelligence aus**.

Wählen Sie den Feed aus dem Network Available Object (Netzwerk verfügbar) aus, und wechseln Sie zur **Whitelist/Blacklist-**Spalte, um die Verbindung zur schädlichen IP-Adresse zuzulassen/zu blockieren.

Sie können auf das Symbol klicken und die Protokollierung aktivieren, wie im Bild angegeben.

Wenn Sie das Ereignis nur für schädliche IP-Verbindungen generieren möchten, statt die Verbindung zu blockieren, klicken Sie mit der rechten Maustaste auf den Feed, und wählen Sie **Monitor-only (Nur Monitor) (nicht blockieren)** aus, wie im Bild gezeigt:

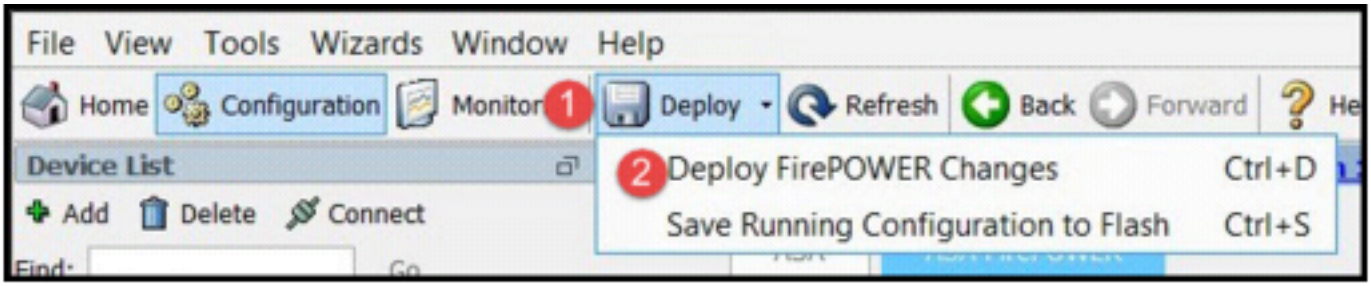


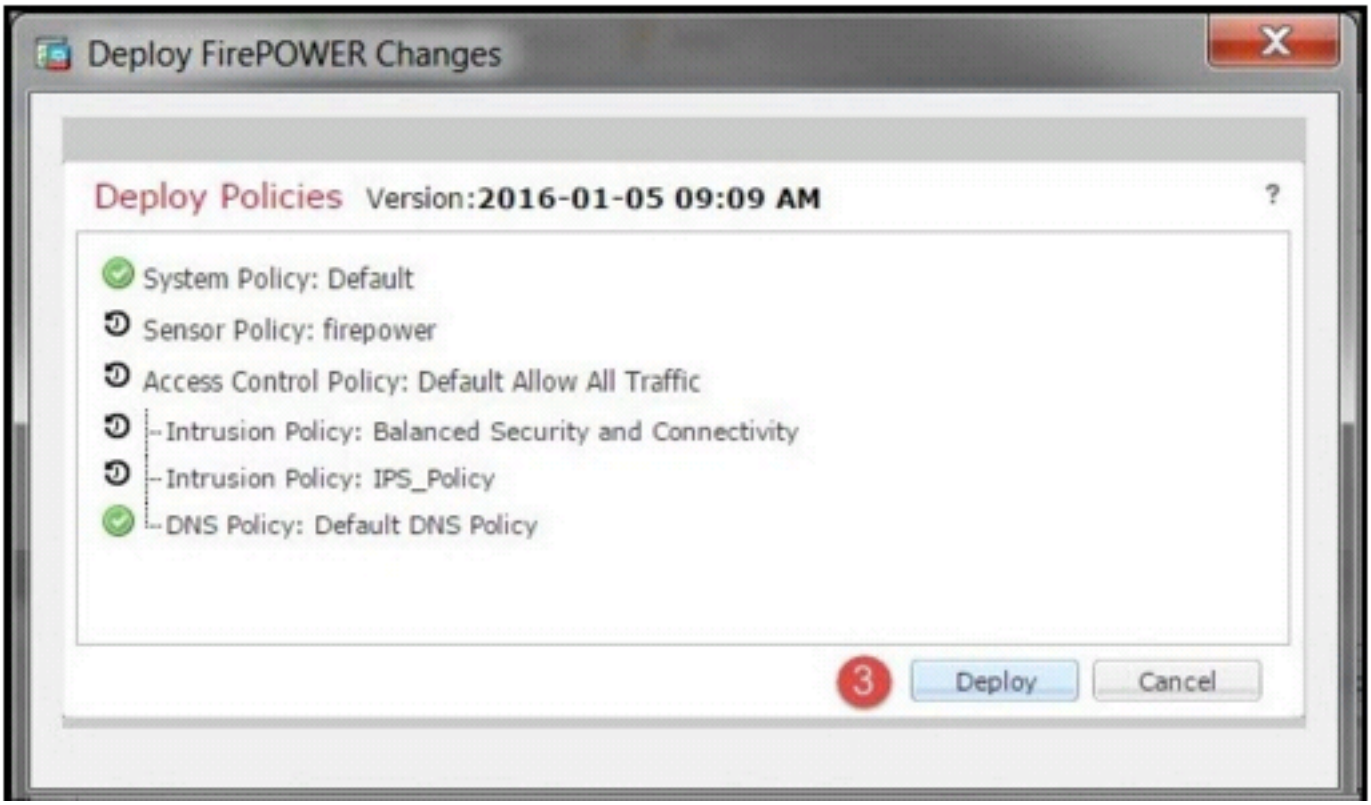
Wählen Sie Option Store ASA FirePOWER Changes, um die Änderungen an AC-Richtlinien zu speichern.

Bereitstellung einer Zugriffskontrollrichtlinie

Damit die Änderungen wirksam werden, müssen Sie die Zugriffskontrollrichtlinie bereitstellen. Bevor Sie die Richtlinie anwenden, sehen Sie einen Hinweis darauf, dass die Zugriffskontrollrichtlinie auf dem Gerät veraltet ist.

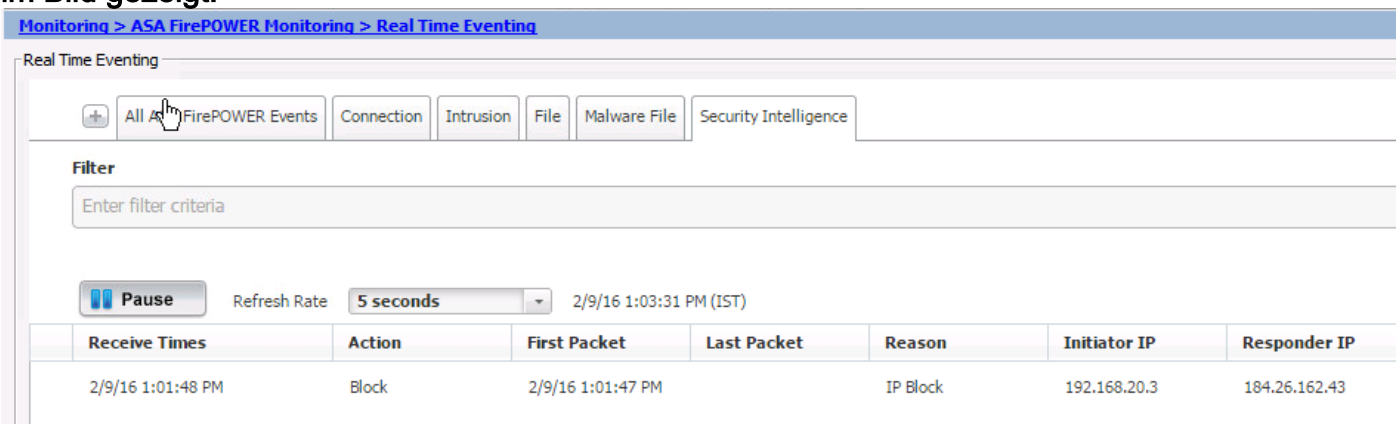
Um die Änderungen am Sensor bereitzustellen, cKlicken Sie auf **Deploy** und wählen Sie **Deploy FirePOWER Changes aus.** Wählen Sie anschließend **Deploy** im Popup-Fenster aus, um die Änderungen bereitzustellen.





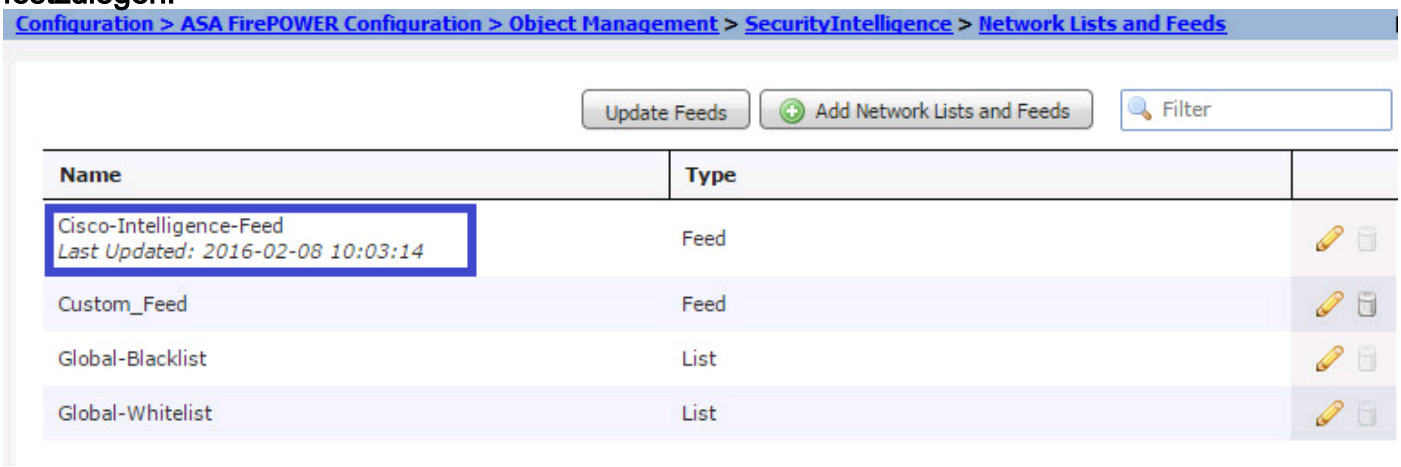
Hinweis: In Version 5.4.x müssen Sie auf **ASA FirePOWER-Änderungen anwenden klicken, um die Zugriffsrichtlinie auf den Sensor anzuwenden.**

Hinweis: Navigieren Sie zu **Monitoring > ASA FirePOWER Monitoring > Task Status.** Stellen Sie sicher, dass die Aufgabe abgeschlossen sein muss, um die Konfigurationsänderungen anzuwenden.## Ereignisüberwachung durch Security Intelligence Um die Sicherheitsintelligenz des FirePOWER-Moduls anzuzeigen, navigieren Sie zu Monitoring > ASA FirePOWER Monitoring > Real Time Event. Wählen Sie die Registerkarte Sicherheitsintelligenz aus. Es werden die Ereignisse angezeigt, wie im Bild gezeigt:



Überprüfen Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.## Fehlerbehebung Um sicherzustellen, dass die Sicherheitsinformations-Feeds

auf dem neuesten Stand sind, navigieren Sie zu Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > Network Lists and Feeds und überprüfen Sie die Uhrzeit, zu der der Feed zuletzt aktualisiert wurde. Sie können die Schaltfläche Bearbeiten auswählen, um die Häufigkeit der Feed-Updates festzulegen.



Stellen Sie sicher, dass die Bereitstellung der Zugriffskontrollrichtlinie erfolgreich abgeschlossen wurde. Überwachen Sie die Sicherheitsinformationen, um festzustellen, ob der Datenverkehr blockiert wird oder nicht.

Zugehörige Informationen

- Cisco ASA FirePOWER-Modul - Kurzreferenz
- Technischer Support und Dokumentation - Cisco Systems