

# Konfigurieren von Domain Based Security Intelligence (DNS-Richtlinie) im FirePOWER-Modul mit ASDM (integriertes Management)

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Übersicht über Domänenlisten und Feeds](#)

[Von Cisco TALOS bereitgestellte Domänenlisten und Feeds](#)

[Benutzerdefinierte Domänenlisten und Feeds](#)

[DNS-Sicherheitsintelligenz konfigurieren](#)

[Schritt 1: Konfigurieren Sie einen benutzerdefinierten DNS-Feed/eine benutzerdefinierte Liste \(optional\).](#)

[Manuelles Hinzufügen von IP-Adressen zu Global-Blacklist und Global-Whitelist](#)

[Erstellen der benutzerdefinierten Liste von Blacklist-Domänen](#)

[Schritt 2: Konfigurieren eines Sinkhole-Objekts \(optional\)](#)

[Schritt 3: Konfigurieren der DNS-Richtlinie](#)

[Schritt 4: Konfigurieren Sie die Zugriffskontrollrichtlinie.](#)

[Schritt 5: Bereitstellung einer Zugriffskontrollrichtlinie.](#)

[Überprüfen](#)

[Ereignisüberwachung für DNS-Sicherheitsintelligenz](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## Einführung

In diesem Dokument wird beschrieben, wie Sie Domain Based Security Intelligence (SI) auf ASA mit FirePOWER-Modul mithilfe von ASDM (Adaptive Security Device Manager) konfigurieren.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Kenntnisse der ASA-Firewall (Adaptive Security Appliance)
- ASDM (Adaptive Security Device Manager)

- Fachwissen zum FirePOWER-Modul

**Hinweis:** Der Security Intelligence-Filter erfordert eine Schutzlizenz.

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- ASA FirePOWER-Module (ASA 5506X/5506H-X/5506W-X, ASA 5508-X, ASA 5516-X) mit Softwareversion 6.0.0 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

Das FirePOWER-System bietet die Möglichkeit, DNS-Datenverkehrsanforderungen abzufangen und nach dem schädlichen Domännennamen zu suchen. Wenn das FirePOWER-Modul eine schädliche Domäne findet, ergreift die FirePOWER geeignete Maßnahmen, um die Anforderung entsprechend der Konfiguration der DNS-Richtlinie zu mindern.

Neue Angriffsmethoden wurden entwickelt, um die IP-basierte Intelligenz zu verletzen und die Funktionen für den DNS-Lastenausgleich zu missbrauchen, um die tatsächliche IP-Adresse eines schädlichen Servers zu verbergen. Während die mit dem Angriff verbundenen IP-Adressen häufig ein- und austauscht, wird der Domänenname selten geändert.

FirePOWER bietet die Möglichkeit, die bösartige Anfrage an einen Tauchloch-Server umzuleiten, der ein Honeypot-Server sein kann, um Versuche zu erkennen, abzuwehren oder zu untersuchen, mehr über den Angriffsverkehr zu erfahren.

## Übersicht über Domänenlisten und Feeds

Domänenlisten und Feeds enthalten die Liste des schädlichen Domännennamens, der je nach Angriffstyp weiter in die verschiedenen Kategorien eingeteilt wird. In der Regel können Sie die Feeds in zwei Arten kategorisieren.

### Von Cisco TALOS bereitgestellte Domänenlisten und Feeds

**DNS-Angreifer:** Sammlung von Domännennamen, die kontinuierlich nach Schwachstellen suchen oder versuchen, andere Systeme auszunutzen.

**DNS-Bogon:** Sammlung von Domännennamen, die den Datenverkehr nicht zuweisen, aber erneut senden, auch bekannt als gefälschte IPs.

**DNS Bots:** Sammlung von Domännennamen, die aktiv als Teil eines Botnets verwendet werden und von einem bekannten Botnet-Controller gesteuert werden.

**DNS CnC:** Sammlung von Domännennamen, die als Steuerserver für ein bekanntes Botnet identifiziert werden.

**DNS-Exploit-Kit:** Auflistung von Domännennamen, die versuchen, andere Systeme auszunutzen.

**DNS-Malware:** Eine Sammlung von Domännennamen, die versuchen, Malware zu verbreiten, oder jeden, der sie besucht, aktiv angreift.

**DNS Open\_proxy:** Sammlung von Domännennamen, die Open Web Proxies ausführen und anonyme Internetbrowserdienste anbieten.

**DNS Open\_Relay:** Eine Sammlung von Domännennamen, die anonyme E-Mail-Relay-Dienste anbieten, die von Spam- und Phishing-Angreifern verwendet werden.

**DNS Phish (DNS-Phishing):** Sammlung von Domännennamen, die Endbenutzer aktiv dazu verleiten sollen, vertrauliche Informationen wie Benutzernamen und Kennwörter einzugeben.

**DNS Response:** Sammlung von Domännennamen, die wiederholt bei verdächtigem oder schädlichem Verhalten beobachtet werden.

**DNS Spam:** Sammlung von Domännennamen, die als Quelle für Spam-E-Mail-Nachrichten identifiziert werden.

**DNS Suspicious (DNS-verdächtig):** Sammlung von Domännennamen, die verdächtige Aktivitäten anzeigen und aktiv untersucht werden.

**DNS Tor\_exit\_node:** Sammlung von Domännennamen, die Exit Node Services für das Tor Anonymizer Netzwerk anbieten.

## **Benutzerdefinierte Domänenlisten und Feeds**

**Globale Blacklist für DNS:** Auflistung der benutzerdefinierten Liste von Domännennamen, die vom Administrator als schädlich identifiziert werden.

**Globale Whitelist für DNS:** Auflistung der benutzerdefinierten Liste von Domännennamen, die vom Administrator als authentisch identifiziert werden.

## **DNS-Sicherheitsintelligenz konfigurieren**

Es gibt mehrere Schritte, um die auf dem Domännennamen basierende Sicherheitsinformationen zu konfigurieren.

1. Konfigurieren Sie den benutzerdefinierten DNS-Feed/die benutzerdefinierte Liste (optional).

2. Konfigurieren des Sinkhole-Objekts (optional)
3. Konfigurieren der DNS-Richtlinie
4. Konfigurieren der Zugriffskontrollrichtlinie
5. Bereitstellung der Zugriffskontrollrichtlinie

## **Schritt 1: Konfigurieren Sie einen benutzerdefinierten DNS-Feed/eine benutzerdefinierte Liste (optional).**

Es gibt zwei vordefinierte Listen, in denen Sie die Domänen hinzufügen können. Sie erstellen Ihre eigenen Listen und Feeds für die Domänen, die Sie blockieren möchten.

- Globale Blacklist für DNS
- Globales Whitelist für DNS

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

Mit dem FirePOWER-Modul können Sie bestimmte Domänen zu Global-Blacklist hinzufügen, wenn Sie wissen, dass sie Teil einer böartigen Aktivität sind. Domänen können auch zu Global Whitelist hinzugefügt werden, wenn Sie den Datenverkehr zu bestimmten Domänen zulassen möchten, die von Blacklist-Domänen blockiert werden. Wenn Sie eine Domäne zu Global-Blacklist/Global-Whitelist hinzufügen, wird sie 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 Domänen zur Global-Blacklist/Global-Whitelist hinzufügen. Klicken Sie im DNS-Bereich auf **Bearbeiten**, und wählen Sie **Whitelist DNS Requests to Domain Now/Blacklist DNS Requests to Domain Now (Whitelist-DNS-Anfragen an Domänen) aus**, um die Domäne zur entsprechenden Liste hinzuzufügen, wie im Bild gezeigt.

Monitoring > ASA FirePOWER Monitoring > Real Time Eventing

Real Time Eventing

Connection Event ---- Allow Time: Fri 15/7/16 9:48:39 AM (IST) (start of the flow) [Close](#)

ASA FirePOWER firewall connection event

Reason:

**Event Details**

Initiator		Responder		Traffic	
Initiator IP	192.168.20.50	Responder IP	10.76.77.50	Ingress Security Zone	inside
Initiator Country and Continent	not available	Responder Country and Continent	not available	Egress Security Zone	outside
Source Port/ICMP Type	57317	Destination Port/ICMP Code	53	Ingress Interface	inside
User	Special Identities/No Authentication Required	URL	not available	Egress Interface	outside
<b>Transaction</b>		URL Category	not available	TCP Flags	0
Initiator Packets	1.0	URL Reputation	Risk unknown	NetBIOS Domain	not available
Responder Packets	0.0	HTTP Response	0	<b>DNS</b>	
Total Packets	1.0	<b>Application</b>		DNS Query	malicious.com
Initiator Bytes	73.0	Application	not available	Sinkhole	Whitelist DNS Requests to Domain Now Blacklist DNS Requests to Domain Now
Responder Bytes	0.0	Application Categories	not available	<a href="#">View more</a>	
Connection Bytes	73.0	Application Tag	not available	<b>SSL</b>	
<b>Policy</b>		Client Application	DNS	SSL Status	Unknown (Unknown)
Policy	Default Allow All Traffic	Client Version	not available	SSL Policy	not available
Firewall Policy Rule/SI Category	intrusion_detection	Client Categories	network protocols/services	SSL Rule	not available
Monitor Rules	not available	Client Tag	opens port	SSL Version	Unknown
<b>ISE Attributes</b>		Client Application	not available	SSL Cipher Suite	TLS_NULL_WITH_NULL_NULL
End Point Profile Name	not available	Web App Categories	not available	SSL Certificate Status	Not Checked
Security Group Tag Name	not available	Web App Tag	not available	<a href="#">View more</a>	
Location IP	::	Application Risk	not available		
		Application Business Relevance	not available		

Um zu überprüfen, ob Domänen der Global-Blacklist/Global-Whitelist hinzugefügt wurden, navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Object Management > SecurityIntelligence > DNS Lists and Feeds** und bearbeiten Sie **Global-Blacklist für DNS / Global Whitelist für DNS**. Sie können auch die Schaltfläche "Löschen" verwenden, um jede Domäne aus der Liste zu entfernen.

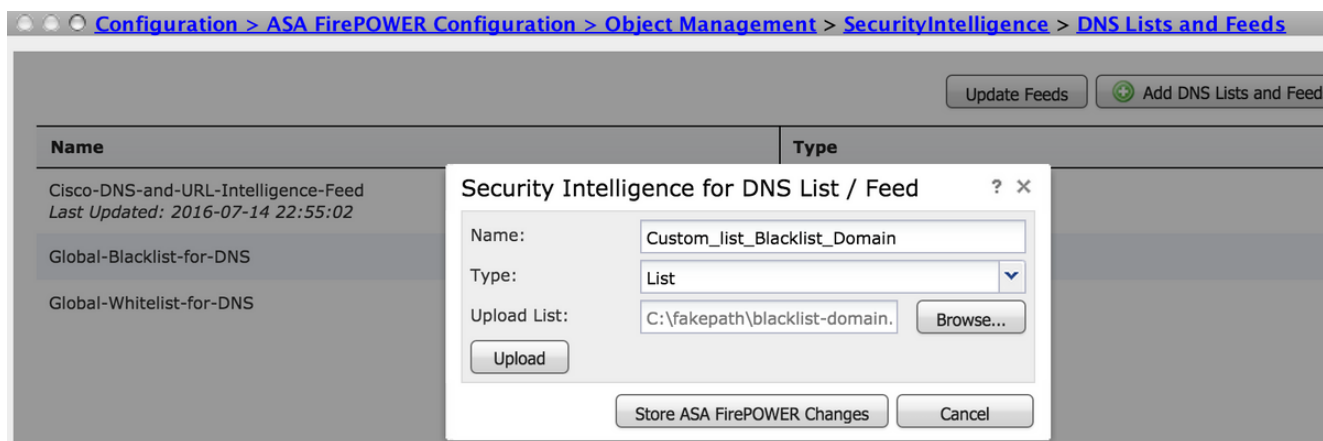
### Erstellen der benutzerdefinierten Liste von Blacklist-Domänen

FirePOWER ermöglicht Ihnen, eine benutzerdefinierte Domänenliste zu erstellen, die mit zwei verschiedenen Methoden zur Blacklist (Block) verwendet werden kann.

1. Sie können Domännennamen in eine Textdatei schreiben (eine Domäne pro Leitung) und die Datei auf das FirePOWER-Modul hochladen.

Um die Datei hochzuladen, navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > DNS Lists and Feeds**, und wählen Sie **Add DNS Lists and Feeds (DNS-Listen und -Feeds hinzufügen)**.

**Name:** Geben Sie den Namen der Liste Benutzerdefiniert 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 **Upload** aus, um die Datei hochzuladen.



Klicken Sie auf **ASA-FirePOWER-Änderungen speichern**, um die Änderungen zu speichern.

2. Sie können Domänen von Drittanbietern für die benutzerdefinierte Liste verwenden, für die das FirePOWER-Modul den Drittanbieter-Server anschließen kann, um die Domänenliste abzurufen.

Um dies zu konfigurieren, navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > DNS Lists and Feeds** und wählen dann **Add DNS Lists and Feeds (DNS-Listen und -Feeds hinzufügen)**.

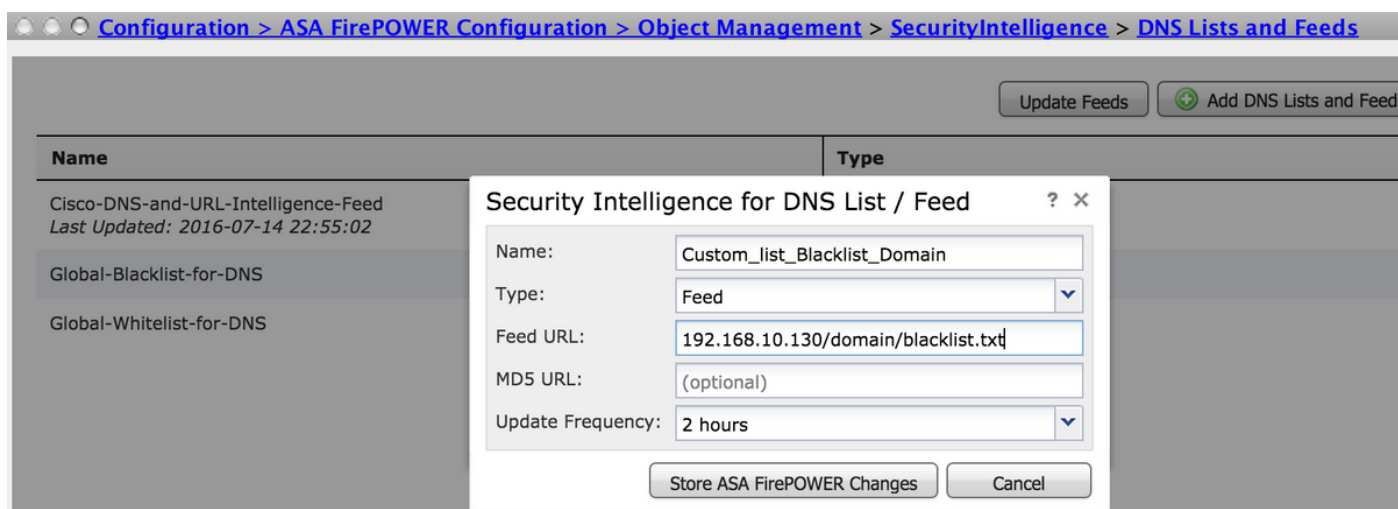
**Name:** Geben Sie den Namen des benutzerdefinierten Feeds an.

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

**Feed-URL:** Geben Sie die Server-URL an, zu der das FirePOWER-Modul eine Verbindung herstellen kann, 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 Modul eine Verbindung zum URL-Feed-Server herstellt.



Wählen Sie **ASA FirePOWER-Änderungen speichern** aus, um die Änderungen zu speichern.

## Schritt 2: Konfigurieren eines Sinkhole-Objekts (optional)

Sinkhole-IP-Adresse kann als Antwort auf eine schädliche DNS-Anfrage verwendet werden. Der Client-Computer erhält die IP-Adresse des sinkhole-Servers für schädliche Domänensuche, und das System versucht, eine Verbindung zum sinkhole-Server herzustellen. Daher kann das Tauchloch als Honeypot fungieren, um den Angriffsverkehr zu untersuchen. Das Tauchloch kann so konfiguriert werden, dass es einen Indicator of Compromise (IOC) auslöst.

Um den Sinkhole-Server hinzuzufügen, wählen Sie **Configuration > ASA FirePOWER Configuration > Object Management > Sinkhole** aus und klicken Sie auf die Option **Sinkhole** hinzufügen.

**Name:** Geben Sie den Namen des sinkhole-Servers an.

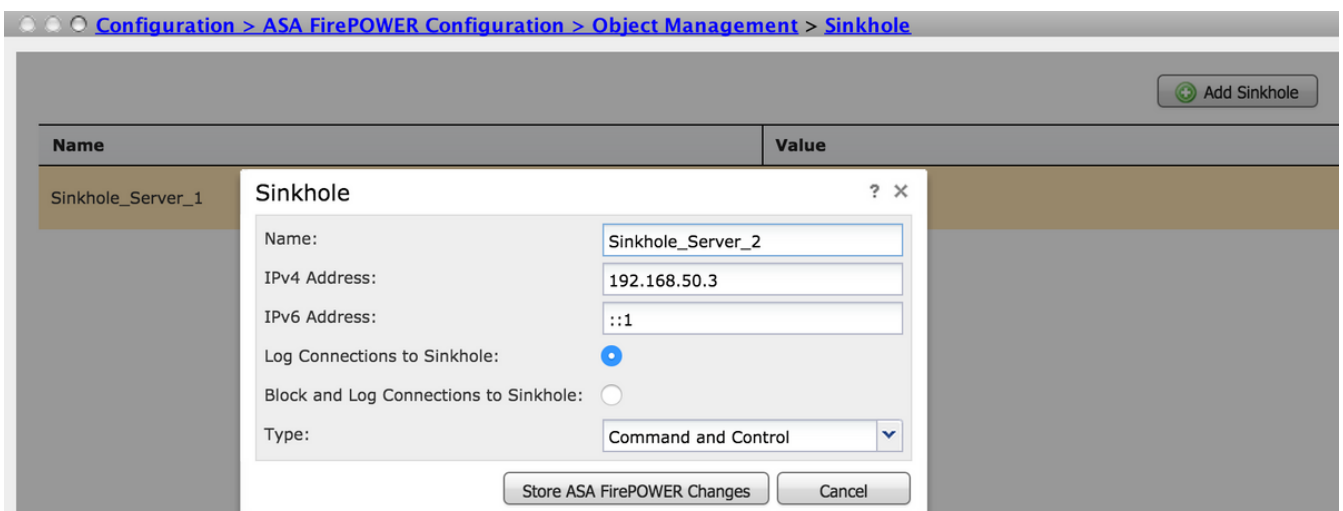
**IP-Adresse:** Geben Sie die IP-Adresse des sinkhole-Servers an.

**Protokollverbindungen zu Sinkhole:** Aktivieren Sie diese Option, um alle Verbindungen zwischen dem Endpunkt und dem sinkhole-Server zu protokollieren.

**Sperrern und Protokollieren von Verbindungen zum Sinkloch:** Aktivieren Sie diese Option, um die Verbindung zu blockieren, und melden Sie sich nur zu Beginn der Flow-Verbindung an. Wenn kein physischer sinkhole-Server vorhanden ist, können Sie eine beliebige IP-Adresse angeben und die Verbindungsereignisse sowie den IOC-Trigger anzeigen.

**Typ:** Geben Sie den Feed aus der Dropdown-Liste an, für den Sie den IOC-Typ (Indication of Compromise, Indications of Compromise) auswählen möchten. Es gibt drei Arten von Tauchloch-IOCs, die markiert werden können.

- Malware
- Command and Control
- Phishing



### Schritt 3: Konfigurieren der DNS-Richtlinie

DNS-Richtlinien müssen konfiguriert werden, um die Aktion für den DNS-Feed/die DNS-Liste festzulegen. Navigieren Sie zu **Konfiguration > ASA FirePOWER Configuration > Policies > DNS Policy**.

Die Standard-DNS-Richtlinie enthält zwei Standardregeln. Die erste Regel, **Global Whitelist für DNS**, enthält die benutzerdefinierte Liste der zulässigen Domäne (**Global-Whitelist-für-DNS**). Diese Regel wird am oberen Ende angezeigt, bevor das System versucht, eine Blacklist-Domäne zuzuordnen. Die zweite Regel, **Global Blacklist for DNS**, enthält die benutzerdefinierte Liste der blockierten Domäne (**Global-Blacklist-for-DNS**).

Sie können weitere Regeln hinzufügen, um die verschiedenen Aktionen für die **von Cisco TALOS bereitgestellten Domänenlisten und Feeds** zu definieren. Um eine neue Regel hinzuzufügen, wählen Sie **DNS-Regel hinzufügen aus**.

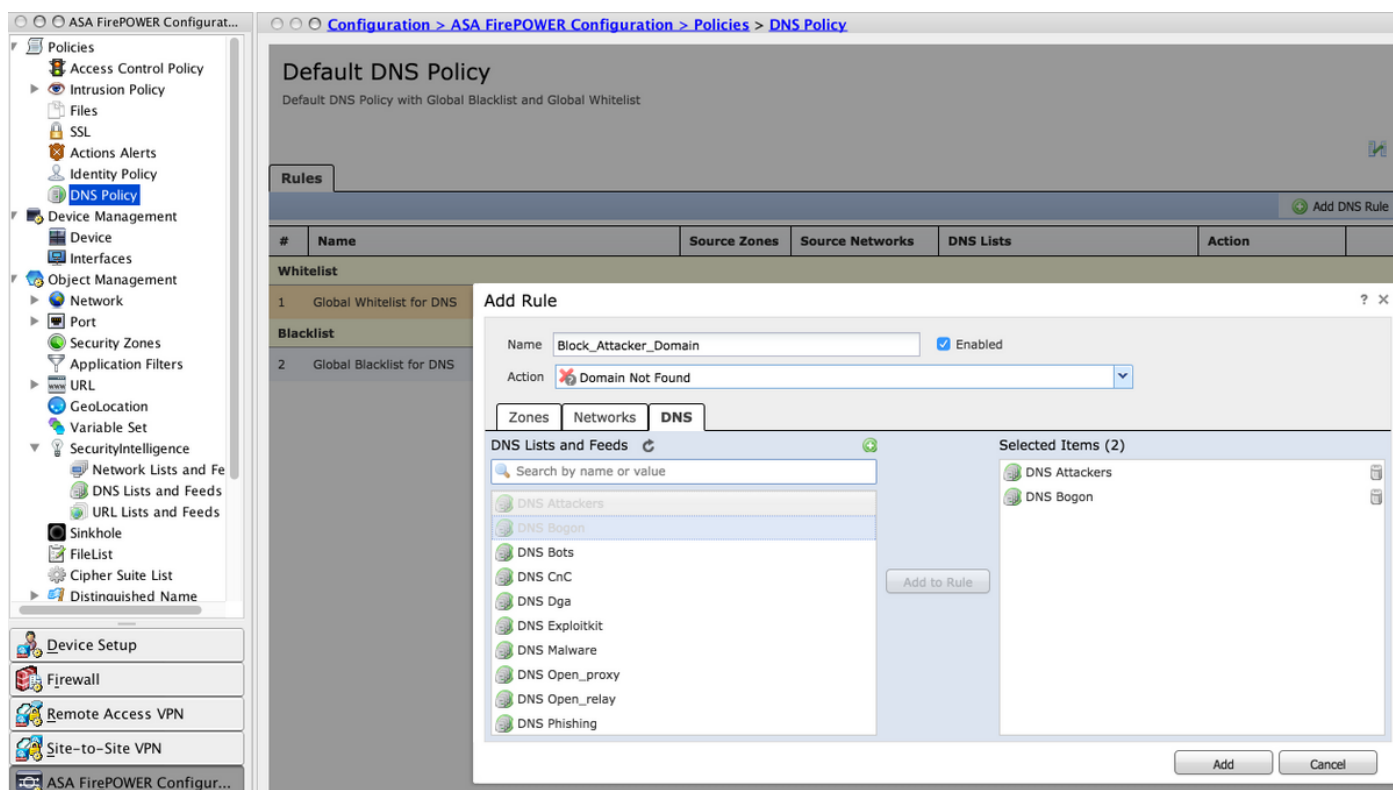
**Name:** Geben Sie den Regelnamen an.

**Aktion:** Geben Sie die Aktion an, die ausgelöst werden soll, wenn diese Regel übereinstimmt.

- **Whitelist:** Dies ermöglicht die DNS-Abfrage.
- **Überwachen:** Diese Aktion generiert das Ereignis für DNS-Abfragen, und der Datenverkehr stimmt weiterhin mit nachfolgenden Regeln überein.
- **Domain Not Found (Domäne nicht gefunden):** Diese Aktion sendet eine DNS-Antwort als Domain Not Found (Domain Not Found (nicht vorhandene Domäne)).
- **Verwerfen:** Diese Aktion blockiert und verwirft die DNS-Abfrage im Hintergrund.
- **Schraubenloch:** Bei dieser Aktion wird die IP-Adresse des Sinkhole-Servers als Antwort auf die DNS-Anforderung gesendet.

Geben Sie die **Zonen/Netzwerke** zum Definieren der Regelbedingungen an. Wählen Sie auf der Registerkarte DNS die **DNS-Listen und -Feeds aus** und wechseln Sie zur Option **Ausgewählte Artikel**, mit der Sie die konfigurierte Aktion anwenden können.

Sie können die verschiedenen DNS-Regeln für verschiedene DNS-Listen und -Feeds mit einer anderen Aktion konfigurieren, je nach den Anforderungen Ihres Unternehmens.



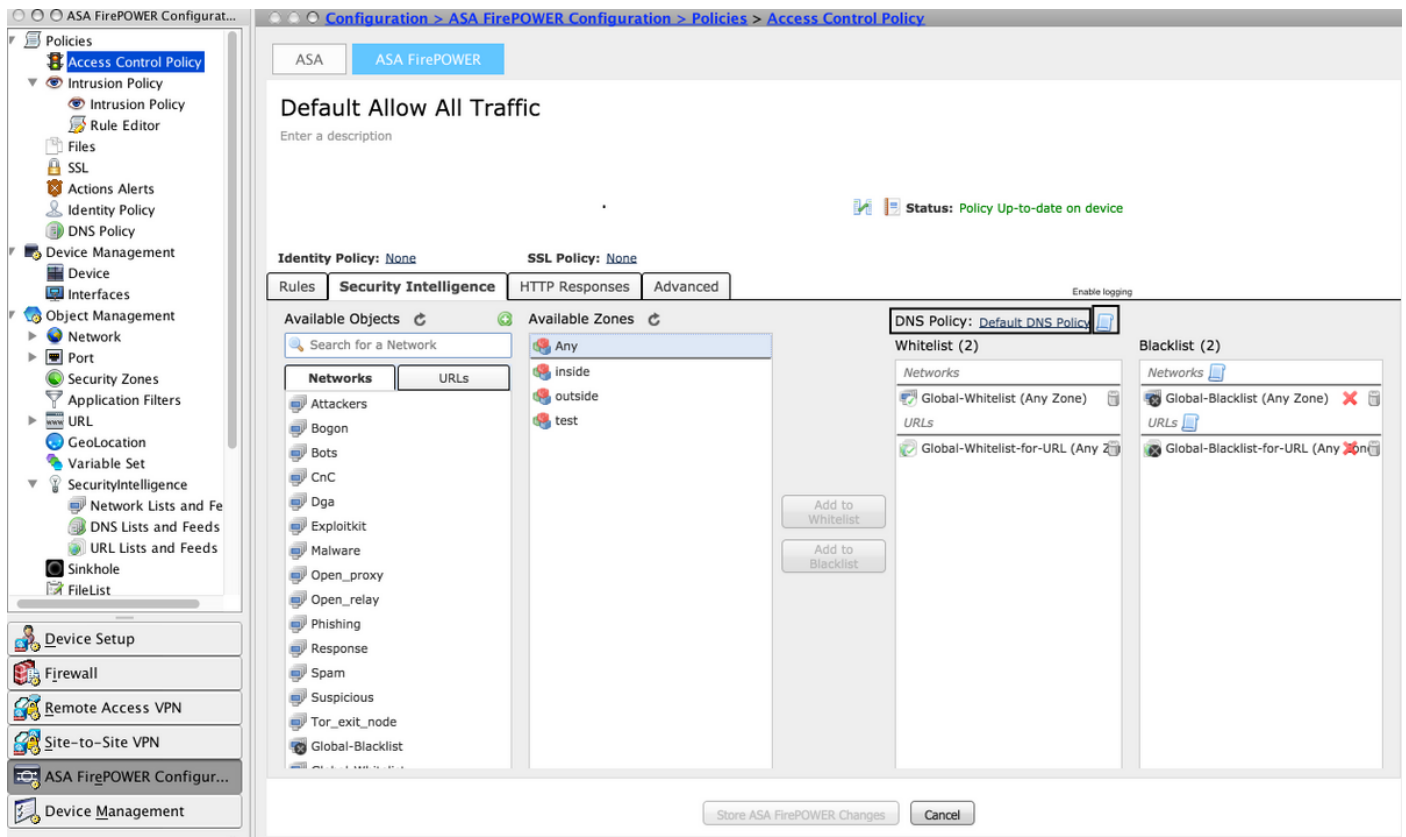


Klicken Sie auf die Option **Hinzufügen**, um die Regel hinzuzufügen.

#### Schritt 4: Konfigurieren Sie die Zugriffskontrollrichtlinie.

Um die DNS-basierten Sicherheitsinformationen zu konfigurieren, navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy (Konfiguration > ASA FirePOWER-Konfiguration > Richtlinien > Zugriffskontrollrichtlinie)**, wählen Sie die Registerkarte **Security Intelligence** aus.

Stellen Sie sicher, dass die DNS-Richtlinie konfiguriert ist. Optional können Sie die Protokolle aktivieren, wenn Sie auf das Protokollsymbol klicken, wie im Bild gezeigt.



Wählen Sie Option **Store ASA FirePOWER Changes**, um die AC-Richtlinienänderungen zu speichern.

#### Schritt 5: 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, klicken Sie auf **Deploy** und wählen Sie **Deploy FirePOWER Changes (FirePOWER-Änderungen bereitstellen)**. Wählen Sie anschließend **Deploy (Bereitstellen)** im Popup-Fenster aus, um die Änderungen bereitzustellen.

**Hinweis:** In Version 5.4.x müssen Sie auf "ASA FirePOWER Changes" klicken, um die Zugriffskontrollrichtlinie auf den Sensor anzuwenden.

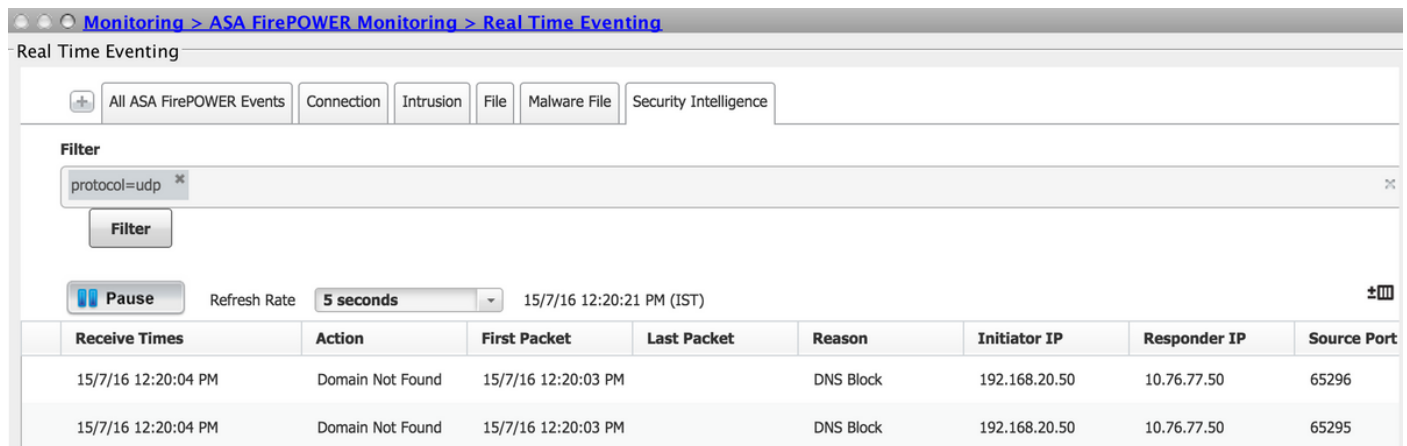
**Hinweis:** Navigieren Sie zu **Monitoring > ASA FirePOWER Monitoring > Task Status**. Stellen Sie sicher, dass die Aufgabe abgeschlossen ist, um die Konfigurationsänderungen zu bestätigen.

## Überprüfen

Konfiguration kann nur überprüft werden, wenn ein Ereignis ausgelöst wird. Dazu können Sie eine DNS-Abfrage auf einem Computer erzwingen. Seien Sie jedoch vorsichtig bei den Auswirkungen, wenn ein bekannter bössartiger Server ins Visier genommen wird. Nachdem Sie diese Abfrage generiert haben, können Sie das Ereignis im Abschnitt **Real Time Event (Echtzeit-Eventierung)** anzeigen.

## Ereignisüberwachung für DNS-Sicherheitsintelligenz

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:



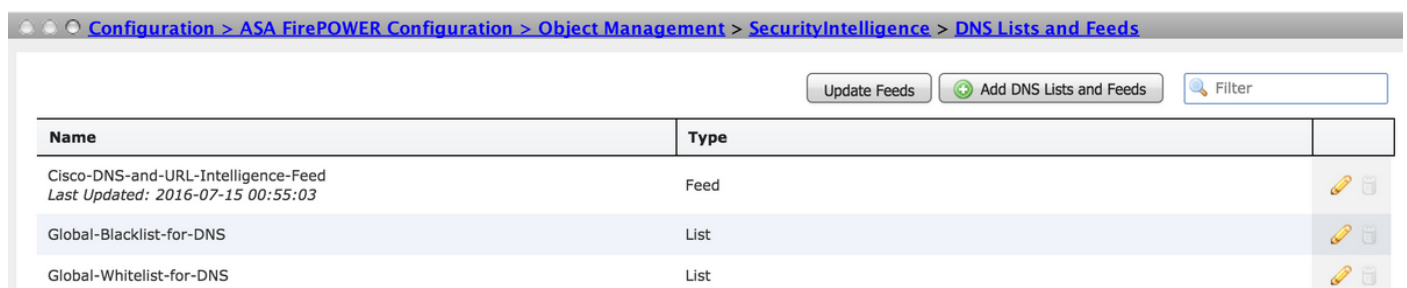
The screenshot shows the 'Real Time Eventing' interface with the 'Security Intelligence' tab selected. A filter 'protocol=udp' is applied. The table below displays two events:

Receive Times	Action	First Packet	Last Packet	Reason	Initiator IP	Responder IP	Source Port
15/7/16 12:20:04 PM	Domain Not Found	15/7/16 12:20:03 PM		DNS Block	192.168.20.50	10.76.77.50	65296
15/7/16 12:20:04 PM	Domain Not Found	15/7/16 12:20:03 PM		DNS Block	192.168.20.50	10.76.77.50	65295







## Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

Um sicherzustellen, dass die Sicherheitsinformations-Feeds auf dem neuesten Stand sind, navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Object Management > Security Intelligence > DNS Lists and Feeds**, und überprüfen Sie die Uhrzeit, zu der der Feed zuletzt aktualisiert wurde. Sie können **Edit** auswählen, um die Häufigkeit der Feed-Updates festzulegen.



The screenshot shows the 'DNS Lists and Feeds' configuration page. It includes buttons for 'Update Feeds', 'Add DNS Lists and Feeds', and a 'Filter' search box. The table below lists the configured feeds:

Name	Type	
Cisco-DNS-and-URL-Intelligence-Feed <i>Last Updated: 2016-07-15 00:55:03</i>	Feed	 
Global-Blacklist-for-DNS	List	 
Global-Whitelist-for-DNS	List	 

Stellen Sie sicher, dass die Bereitstellung der Zugriffskontrollrichtlinie erfolgreich abgeschlossen wurde.

Überwachen Sie die Registerkarte Security Intelligence Real Time Event, um festzustellen, ob der Datenverkehr blockiert wird.

## Zugehörige Informationen

- [Cisco ASA FirePOWER-Modul - Kurzreferenz](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)