

# Konfigurieren der Intrusion Policy und Signature Configuration im FirePOWER-Modul (interne Verwaltung)

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfiguration](#)

[Schritt 1: Konfigurieren der Zugriffsrichtlinie](#)

[Schritt 1.1: Richtlinie für Sicherheitsrisiken erstellen](#)

[Schritt 1.2: Richtlinie für Sicherheitsrisiken ändern](#)

[Schritt 1.3: Basisrichtlinie ändern](#)

[Schritt 1.4: Signaturfilterung mit Option Filterleiste](#)

[Schritt 1.5: Konfigurieren des Regelstatus](#)

[Schritt 1.6: Ereignisfilter konfigurieren](#)

[Schritt 1.7: Konfigurieren des dynamischen Zustands](#)

[Schritt 2: Konfigurieren der Network Analysis Policy \(NAP\) und der Variablensätze \(optional\)](#)

[Schritt 3: Konfigurieren der Zugriffskontrolle zur Einbindung von Zugriffsrichtlinien/NAP/Variablensätzen](#)

[Schritt 4: Bereitstellung einer Zugriffskontrollrichtlinie](#)

[Schritt 5: Überwachung von Angriffsereignissen](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## Einführung

Dieses Dokument beschreibt die Funktionen des FirePOWER-Moduls Intrusion Prevention System (IPS)/Intrusion Detection System (IDS) und verschiedene Elemente der Intrusion Policy, die eine Erkennungsrichtlinie im FirePOWER-Modul bilden.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

\* Kenntnisse der ASA-Firewall (Adaptive Security Appliance), des Adaptive Security Device Manager (ASDM).

\* Informationen zur FirePOWER-Appliance.

## 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

FirePOWER IDS/IPS wurde entwickelt, um den Netzwerkverkehr zu untersuchen und schädliche Muster (oder Signaturen) zu identifizieren, die auf einen Netzwerk-/Systemangriff hinweisen. Das FirePOWER-Modul funktioniert im IDS-Modus, wenn die ASA-Service-Richtlinie speziell im Überwachungsmodus (Promiscuous) konfiguriert ist. Andernfalls funktioniert es im Inline-Modus.

FirePOWER IPS/IDS ist ein signaturbasiertes Erkennungsverfahren. FirePOWER-Modul im IDS-Modus generiert eine Warnmeldung, wenn die Signatur mit dem schädlichen Datenverkehr übereinstimmt, während das FirePOWER-Modul im IPS-Modus Warnmeldungen generiert und schädlichen Datenverkehr blockiert.

**Hinweis:** Stellen Sie sicher, dass das FirePOWER-Modul über eine **Protect**-Lizenz verfügen muss, um diese Funktion zu konfigurieren. Navigieren Sie zum Überprüfen der Lizenz zu **Configuration > ASA FirePOWER Configuration > License**.

## Konfiguration

### Schritt 1: Konfigurieren der Zugriffsrichtlinie

#### Schritt 1.1: Richtlinie für Sicherheitsrisiken erstellen

Melden Sie sich zum Konfigurieren der Intrusion Policy beim Adaptive Security Device Manager (ASDM) an, und führen Sie die folgenden Schritte aus:

Schritt 1: Navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy (Konfiguration > ASA FirePOWER-Konfiguration > Richtlinien für Sicherheitsrisiken > Intrusion Policy (Angriffsrichtlinie))**.

Schritt 2: Klicken Sie auf **Create Policy (Richtlinie erstellen)**.

Schritt 3: Geben Sie den **Namen** der Intrusion Policy ein.

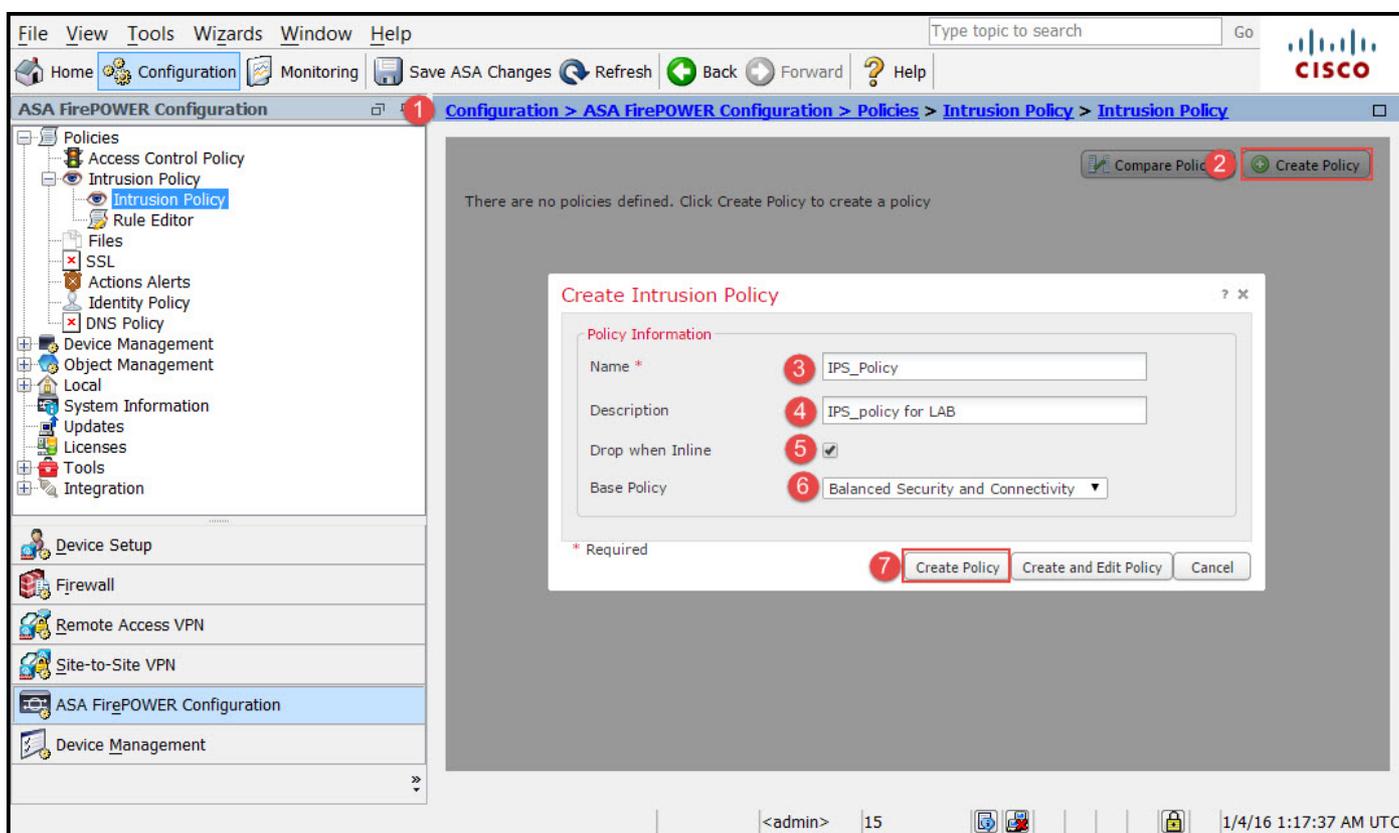
Schritt 4: Geben Sie die **Beschreibung** der Intrusion Policy (optional) ein.

Schritt 5: Geben Sie die Option **Drop when Inline** an.

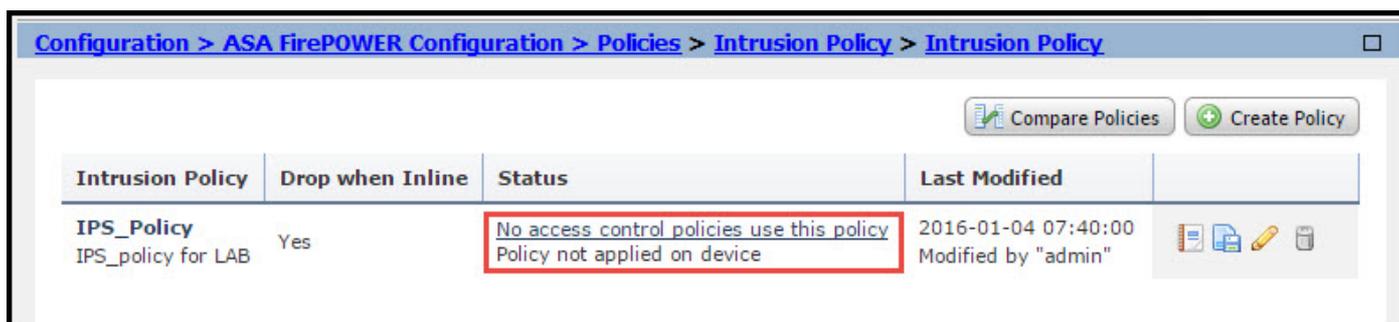
Schritt 6: Wählen Sie die **Basisrichtlinie** aus der Dropdown-Liste aus.

Schritt 7: Klicken Sie auf **Create Policy (Richtlinie erstellen)**, um die Erstellung von Intrusion Policy (Sicherheitsrichtlinie) abzuschließen.

**Tipp:** Wenn die Option Inline (Inline) in bestimmten Szenarien ausschlaggebend ist, wenn der Sensor im Inline-Modus konfiguriert ist und der Datenverkehr nicht unterbrochen werden muss, obwohl er mit einer Signatur übereinstimmt, die eine Drop-Aktion ausführt.

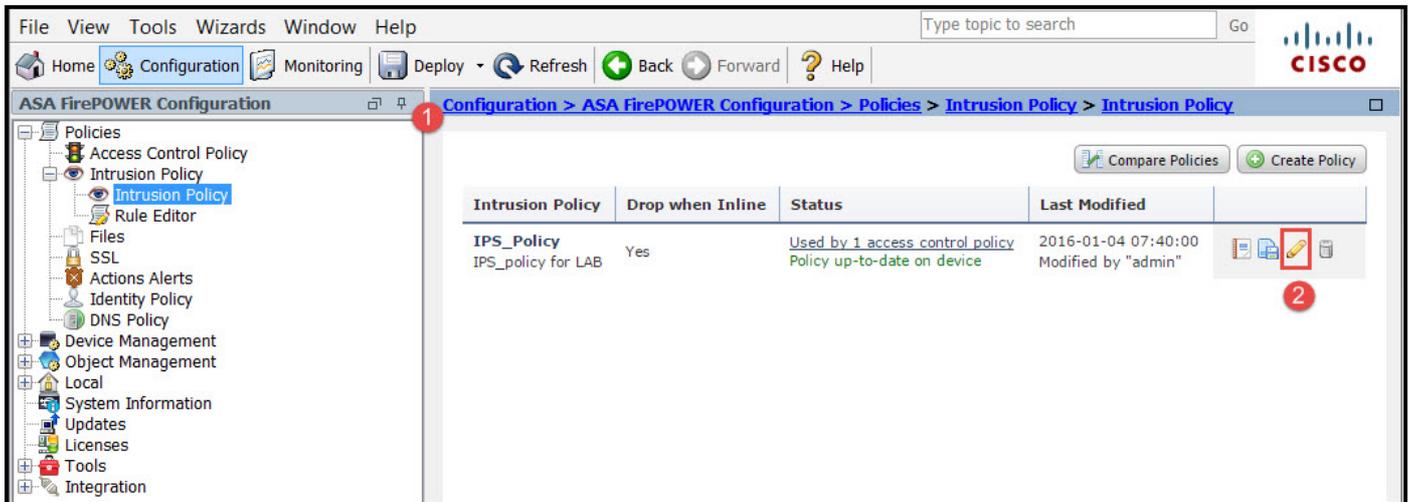


Sie können bemerken, dass die Richtlinie konfiguriert ist, sie jedoch nicht auf ein Gerät angewendet wird.



Schritt 1.2: Richtlinie für Sicherheitsrisiken ändern

Um die Intrusion Policy zu ändern, navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Policies > Intrusion Policy > Intrusion Policy (Konfiguration > ASA FirePOWER-Konfiguration > Richtlinien > Intrusion Policy (Angriffsrichtlinie))**, und wählen Sie die Option **Edit (Bearbeiten)** aus.



### Schritt 1.3: Basisrichtlinie ändern

Die Seite Intrusion Policy Management (Intrusion Policy-Management) bietet die Option, die Base-Richtlinie/-Drop zu ändern, wenn die Option Inline/Save and Discard (Inline/Speichern und Verwerfen) aktiviert ist.

Die Basisrichtlinie enthält einige vom System bereitgestellte Richtlinien, bei denen es sich um integrierte Richtlinien handelt.

1. Ausgewogene Sicherheit und Konnektivität: Diese Richtlinie bietet optimale Sicherheit und Konnektivität. Für diese Richtlinie sind etwa 7.500 Regeln aktiviert, von denen einige nur Ereignisse generieren, während andere Ereignisse generieren und den Datenverkehr verwerfen.
2. Sicherheit über Konnektivität: Wenn Sie Sicherheit bevorzugen, können Sie Sicherheit statt Konnektivitätsrichtlinie wählen, wodurch die Anzahl der aktivierten Regeln erhöht wird.
3. Konnektivität über Sicherheit: Wenn Ihre Präferenz eher Konnektivität als Sicherheit ist, können Sie Konnektivität statt Sicherheitsrichtlinien wählen, wodurch die Anzahl der aktivierten Regeln verringert wird.
4. Maximale Erkennung - Wählen Sie diese Richtlinie aus, um eine maximale Erkennung zu erhalten.
5. No Rule Active (Keine Regel aktiv): Mit dieser Option werden alle Regeln deaktiviert. Sie müssen die Regeln manuell aktivieren, basierend auf Ihren Sicherheitsrichtlinien.

The screenshot displays the 'Policy Information' configuration page. The left-hand navigation pane shows 'Policy Information' as the active section. The main content area is titled 'Policy Information' and includes a '< Back' link. The configuration details are as follows:

- Name:** IPS\_Policy
- Description:** IPS\_policy for LAB
- Drop when Inline:**
- Base Policy:** Balanced Security and Connectivity (with a 'Manage Base Policy' link)
- Policy Status:** The base policy is up to date (Rule Update 2015-10-01-001-vrt)
- Enabled Rules Summary:** This policy has 7591 enabled rules. 114 rules generate events, and 7477 rules drop and generate events. There are 'Manage Rules' and 'View' links for this summary.
- Preprocessor Note:** This policy contains enabled preprocessor rules. Please read the rule documentation to ensure the preprocessors have the correct settings for these rules.
- Buttons:** 'Commit Changes' and 'Discard Changes' buttons are located at the bottom of the page.

#### Schritt 1.4: Signaturfilterung mit Option Filterleiste

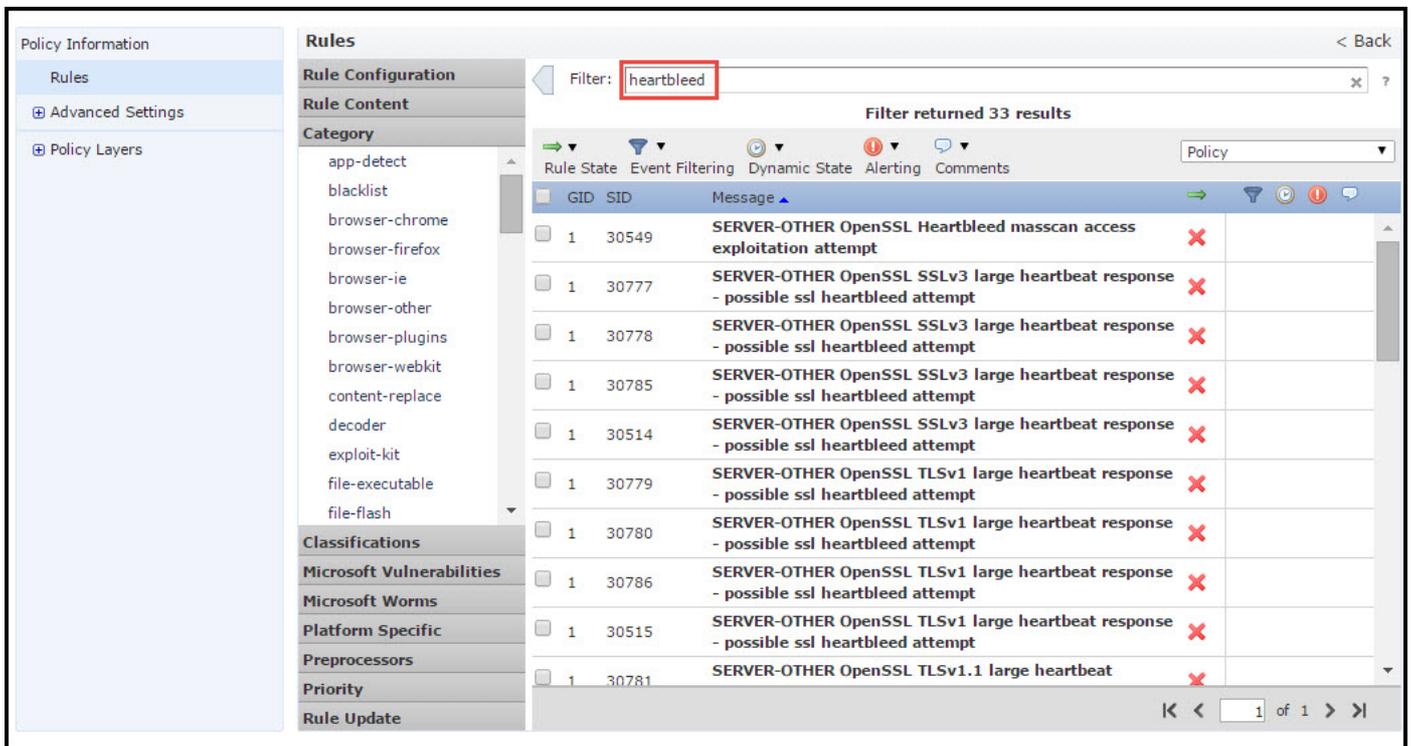
Navigieren Sie im Navigationsbereich zur Option **Regeln**, und die Seite Regelverwaltung wird angezeigt. Es gibt Tausende von Regeln in der Regeldatenbank. Die Filterleiste bietet eine gute Suchmaschinenoption, um die Regel effektiv zu durchsuchen.

Sie können ein beliebiges Schlüsselwort in die Filterleiste einfügen und das System erfasst die Ergebnisse für Sie. Wenn die Signatur für Heartbleed-Schwachstellen von Secure Sockets Layer (SSL) gesucht werden muss, können Sie Schlüsselwörter in der Filterleiste durchsuchen und die Signatur für die Heartbleed-Schwachstelle abrufen.

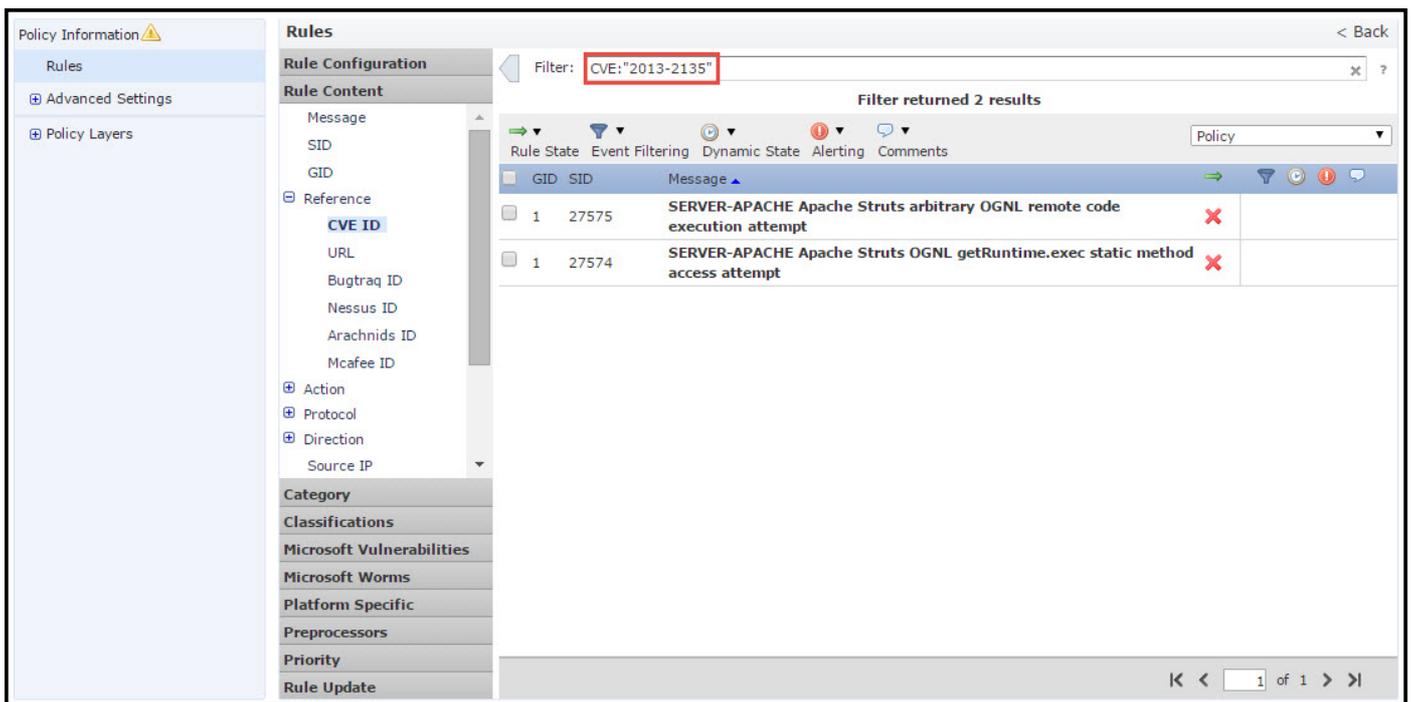
**Tipp:** Wenn in der Filterleiste mehrere Schlüsselwörter verwendet werden, kombiniert das System diese mit AND logic, um eine kombinierte Suche zu erstellen.

Sie können die Regeln auch mithilfe der Signature-ID (SID), Generator-ID (GID), Kategorie: DOS usw.

Regeln werden effektiv in verschiedene Kategorien unterteilt, z. B. nach Kategorie/Klassifizierung/Microsoft-Sicherheitslücken/Microsoft-Würmern/Plattformspezifisch. Eine solche Zuordnung von Regeln hilft dem Kunden, die richtige Signatur auf einfache Weise zu bekommen und hilft ihm, die Signaturen effektiv abzustimmen.



Sie können auch mit der CVE-Nummer nach den Regeln suchen, die diese abdecken. Sie können die Syntax **CVE: <cve-number>**.



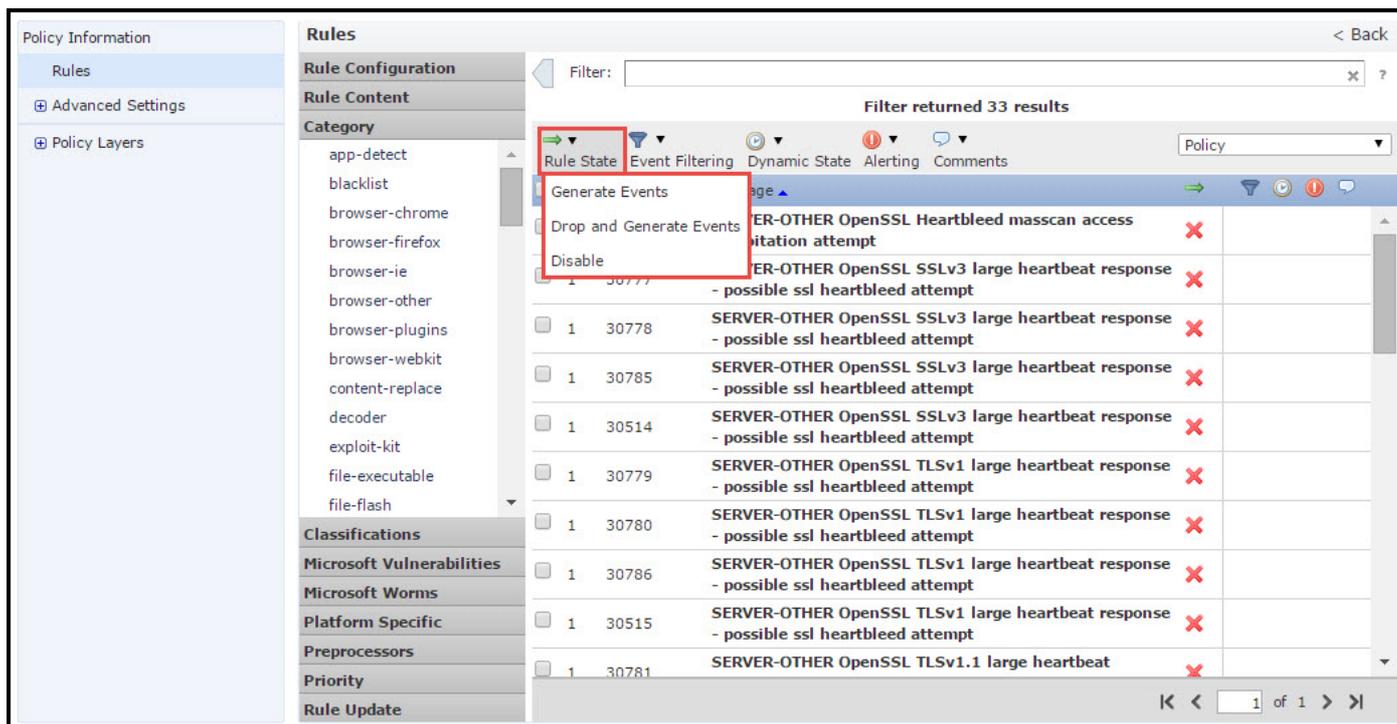
### Schritt 1.5: Konfigurieren des Regelstatus

Navigieren zu **Regeln** Option im Navigationsbereich und Seite "Regelverwaltung" wird angezeigt. Wählen Sie die Regeln aus, und wählen Sie die Option **Regelstatus**, um den Status der Regeln zu konfigurieren. Es gibt drei Zustände, die für eine Regel konfiguriert werden können:

- 1. Veranstaltungen generieren:** Diese Option generiert Ereignisse, wenn die Regel mit dem Datenverkehr übereinstimmt.
- 2. Drop and Generate Events (Ereignisse verwerfen und generieren):** Diese Option generiert

Ereignisse und Datenverkehr, wenn die Regel mit dem Datenverkehr übereinstimmt.

3. **Deaktivieren:** Diese Option deaktiviert die Regel.



### Schritt 1.6. Ereignisfilter konfigurieren

Die Wichtigkeit eines Angriffsereignisses kann von der Häufigkeit des Auftretens oder von der Quell- oder Ziel-IP-Adresse abhängen. In einigen Fällen ist Ihnen ein Ereignis möglicherweise erst dann wichtig, wenn es mehrfach aufgetreten ist. Sie sind beispielsweise möglicherweise nicht besorgt, wenn jemand versucht, sich bei einem Server anzumelden, bis er eine bestimmte Anzahl an Fehlern aufweist. In anderen Fällen müssen Sie möglicherweise nur einige wenige Regelschläge anzeigen, um zu überprüfen, ob ein weitverbreitetes Problem vorliegt.

Es gibt zwei Möglichkeiten, dies zu erreichen:

1. Ereignisgrenzwert.
2. Ereignisunterdrückung.

#### Ereignisgrenzwert

Sie können Grenzwerte festlegen, die abhängig von der Anzahl der Vorfälle festlegen, wie oft ein Ereignis angezeigt wird. Sie können Grenzwertverfahren pro Ereignis und pro Richtlinie konfigurieren.

Schritte zum Konfigurieren des Ereignisgrenzwerts:

Schritt 1: Wählen Sie die **Regel(en)** aus, für die Sie den Ereignisschwellenwert konfigurieren möchten.

Schritt 2: Klicken Sie auf **Ereignisfilterung**.

Schritt 3: Klicken Sie auf den **Schwellenwert**.

Schritt 4: Wählen Sie den **Typ** aus der Dropdown-Liste aus. (Limit oder Threshold oder Both).

Schritt 5: Wählen Sie im Dropdown-Feld **Track By** aus, wie Sie die Verfolgung durchführen möchten. (Quelle oder Ziel).

Schritt 6: Geben Sie die **Count** von Ereignissen ein, die den Schwellenwert erfüllen sollen.

Schritt 7: Geben Sie die **Sekunden** ein, die verstrichen werden soll, bevor die Zählung zurückgesetzt wird.

Schritt 8: Klicken Sie zum Abschließen auf **OK**.

The screenshot shows a network security management interface with a table of rules and a dialog box for configuring a threshold for a selected rule. The table has columns for Rule ID (GID), SID, and Rule Name. A red box highlights the 'Event Filtering' menu, and another red box highlights the 'Threshold' option. A red box highlights the selected rule (GID 1, SID 32846). The dialog box 'Set Threshold for 1 rule' has fields for Type (Limit), Track By (Source), Count (10), and Seconds (60). The OK button is highlighted with a red box.

GID	SID	Rule Name	State
1	280	360.cn SafeGuard local HTTP management	✗
1	280	360.cn Safeguard runtime outbound communication	→
1	328	Absolute Software Computrace outbound connection - 209.53.113.223	→
1	32846	APP-DETECT Absolute Software Computrace outbound connection - absolute.com	→
1	32847	APP-DETECT Absolute Software Computrace outbound connection - bh.namequery.com	→
1	32848	APP-DETECT Absolute Software Computrace outbound connection - namequery.nettrace.co.za	→
1	26286	APP-DETECT Absolute Software Computrace outbound connection - search.dnssearch.org	→
1	26287	APP-DETECT Absolute Software Computrace outbound connection - search.namequery.com	→

**Set Threshold for 1 rule**

4 Type: Limit  
5 Track By: Source  
6 Count: 10  
7 Seconds: 60  
8 OK

Nachdem ein Ereignisfilter zu einer Regel hinzugefügt wurde, sollten Sie ein Filtersymbol neben der Regelanzeige sehen können, das anzeigt, dass für diese Regel eine Ereignisfilterung aktiviert ist.

## Ereignisunterdrückung

Bestimmte Ereignisbenachrichtigungen können anhand der Quell-/Ziel-IP-Adresse oder anhand von Regel unterdrückt werden.

**Hinweis:** Wenn Sie eine Ereignisunterdrückung für eine Regel hinzufügen. Die Signaturüberprüfung funktioniert wie gewohnt, aber das System generiert keine Ereignisse, wenn der Datenverkehr mit der Signatur übereinstimmt. Wenn Sie eine bestimmte Quelle bzw. ein bestimmtes Ziel angeben, werden Ereignisse nicht nur für die spezifische Quelle bzw. das bestimmte Ziel für diese Regel angezeigt. Wenn Sie die vollständige Regel unterdrücken, generiert das System kein Ereignis für diese Regel.

Schritte zum Konfigurieren des Ereignisgrenzwerts:

Schritt 1: Wählen Sie die **Regel(en)** aus, für die Sie den Ereignisschwellenwert konfigurieren möchten.

Schritt 2: Klicken Sie auf **Ereignisfilterung**.

Schritt 3: Klicken Sie auf **Unterdrückung**.

Schritt 4: Wählen Sie **Suppression Type (Unterdrückungstyp)** aus der Dropdown-Liste aus. (Regel, Quelle oder Ziel).

Schritt 5: Klicken Sie zum Abschließen auf **OK**.

The screenshot displays a table of rules with columns for GID, SID, and Threshold. A red box highlights the 'Event Filtering' menu item (2) and the 'Suppression' option (3) in the dropdown menu. A red box highlights the selected rule (1) with GID 1 and SID 32846. Three dialog boxes, each titled 'Add Suppression for 1 rule', are overlaid on the interface. The first dialog shows 'Suppression Type' set to 'Rule' (4) and 'OK' (5) buttons. The second dialog shows 'Suppression Type' set to 'Source' (4) and 'OK' (5) buttons. The third dialog shows 'Suppression Type' set to 'Destination' (4) and 'OK' (5) buttons.

Nachdem der Ereignisfilter zu dieser Regel hinzugefügt wurde, sollten Sie ein Filtersymbol mit der Zählung "Zwei" neben der Regelanzeige sehen können, was zeigt, dass für diese Regel zwei Ereignisfilter aktiviert sind.

### Schritt 1.7: Konfigurieren des dynamischen Zustands

Es ist eine Funktion, mit der wir den Zustand einer Regel ändern können, wenn die angegebene Bedingung übereinstimmt.

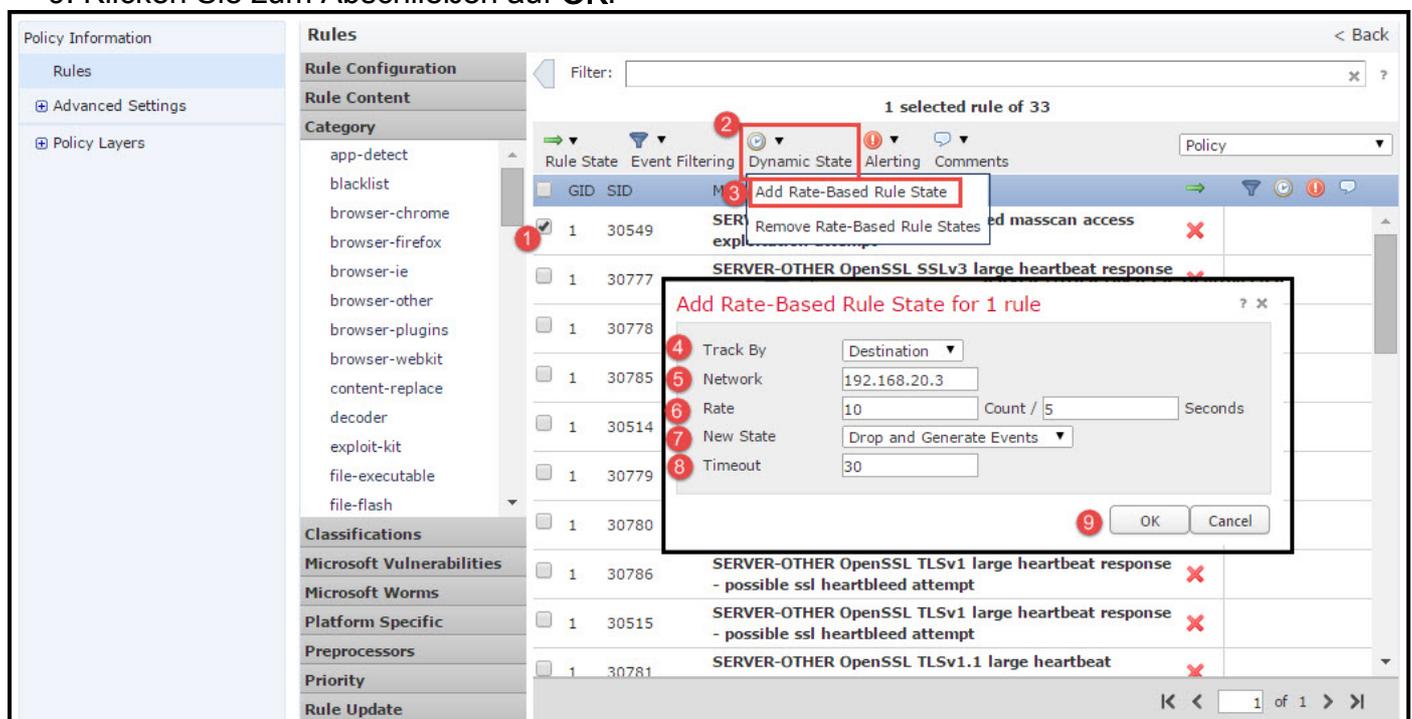
Nehmen wir an, Sie könnten ein Szenario eines Brute-Force-Angriffs erstellen, um das Kennwort

zu knacken. Wenn eine Signatur einen Versuch eines Kennwortfehlers feststellt und die Regelaktion darin besteht, ein Ereignis zu generieren. Das System generiert weiterhin eine Warnmeldung für den Versuch, ein Kennwort nicht zu versenden. In dieser Situation können Sie den **Dynamic-Zustand** verwenden, in dem eine Aktion von **Generate Events** in **Drop and Generate Events** geändert werden kann, um den Brute-Force-Angriff zu blockieren.

Navigieren zu **Regeln** im Navigationsbereich und auf der Seite Regelverwaltung angezeigt. Wählen Sie die Regel aus, für die Sie den dynamischen Zustand aktivieren möchten, und wählen Sie die Optionen **Dynamic State (Dynamischer Status) > Add a Rate-based Rule State (Status einer Ratenbasis-Regel hinzufügen)** aus.

So konfigurieren Sie den ratenbasierten Regelstatus:

1. Wählen Sie die **Regel(en)** aus, für die Sie den Ereignisschwellenwert konfigurieren möchten.
2. Klicken Sie auf den **Dynamic State**.
3. Klicken Sie auf den **Status Ratenbasierte Regel hinzufügen**.
4. Wählen Sie im Dropdown-Feld **Track By** aus, wie Sie den Regelstatus überwachen möchten. (**Regel oder Quelle oder Ziel**).
5. Geben Sie das **Netzwerk ein**. Sie können eine einzelne IP-Adresse, einen Adressblock, eine Variable oder eine kommasetrennte Liste angeben, die aus einer beliebigen Kombination dieser Listen besteht.
6. Geben Sie die **Anzahl** der Ereignisse und den Zeitstempel in Sekunden ein.
7. Wählen Sie den **Neuen Status aus**, den Sie für die Regel definieren möchten.
8. Geben Sie das **Timeout ein**, nach dem der Regelstatus zurückgesetzt wird.
9. Klicken Sie zum Abschließen auf **OK**.



## Schritt 2: Konfigurieren der Network Analysis Policy (NAP) und der Variablensätze (optional)

### Konfigurieren der Netzwerkanalyse-Richtlinie

Netzwerkzugriffsrichtlinien werden auch als Präprozessoren bezeichnet. Der Präprozessor

reassembliert das Paket und normalisiert den Datenverkehr. Es hilft bei der Identifizierung von Protokollanomalien auf der Netzwerkebene und der Transportschicht bei der Identifizierung ungeeigneter Headeroptionen.

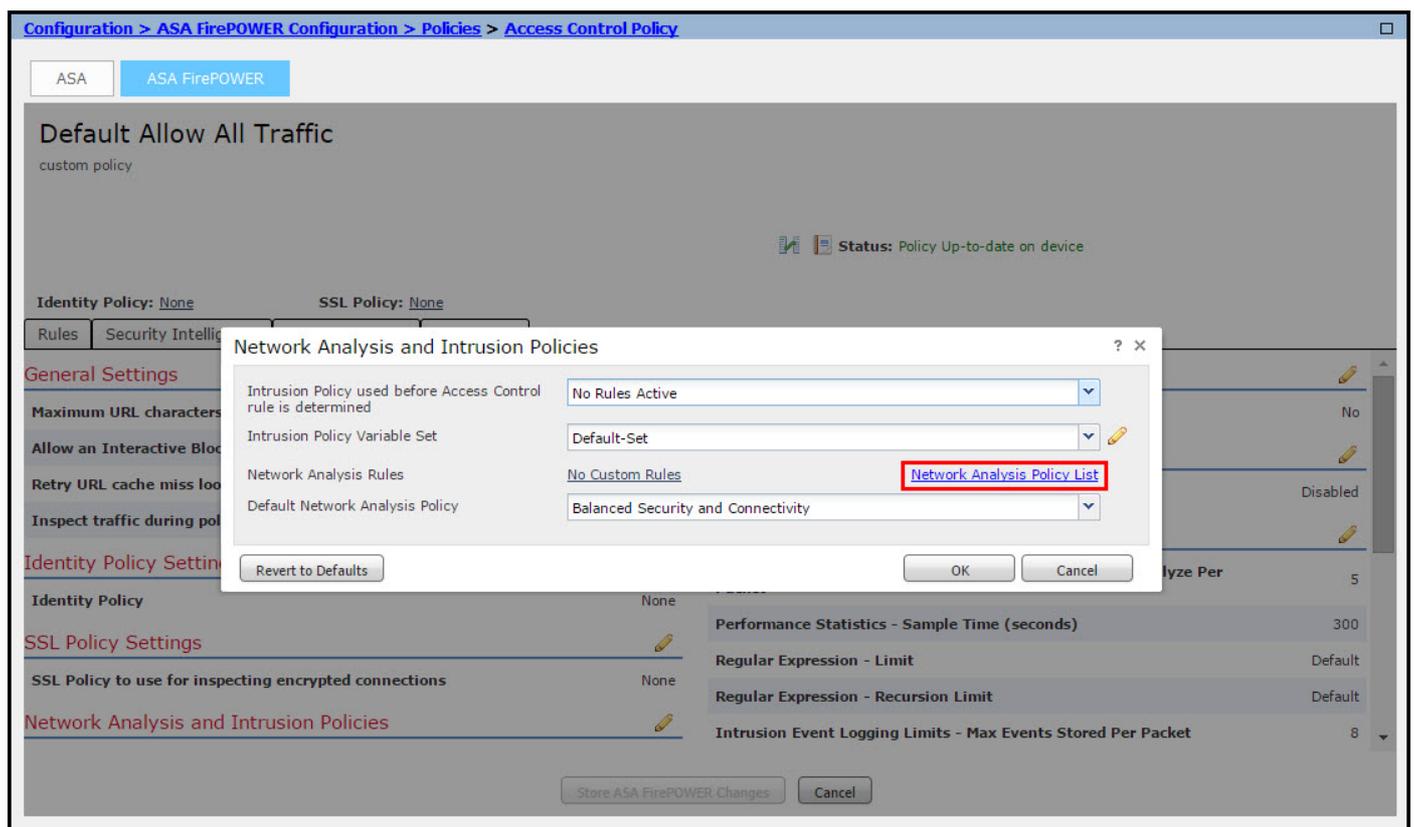
NAP defragmentiert IP-Datagramme, stellt Stateful Inspection, Streamreassemblierung und Validierung von Prüfsummen bereit. Der Präprozessor normalisiert den Datenverkehr, validiert und überprüft den Protokollstandard.

Jeder Präprozessor hat seine eigene GID-Nummer. Er stellt dar, welcher Präprozessor vom Paket ausgelöst wurde.

Navigieren Sie zum Konfigurieren von Richtlinien für die Netzwerkanalyse zu **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy > Advanced > Network Analysis and Intrusion Policy**.

Die Standard-Netzwerkanalyserichtlinie ist "Balanced Security and Connectivity" (Ausgewogene Sicherheit und Konnektivität), was die optimale empfohlene Richtlinie ist. Es gibt drei weitere systembereitgestellte NAP-Richtlinien, die aus der Dropdown-Liste ausgewählt werden können.

Wählen Sie die Option **Network Analysis Policy List** (Netzwerkanalyse-Richtlinienliste) aus, um eine benutzerdefinierte NAP-Richtlinie zu erstellen.



## Konfigurieren von Variablen

Variablensätze werden in Angriffsregeln verwendet, um die Quell- und Zieladressen und -ports zu identifizieren. Regeln sind effektiver, wenn Variablen Ihre Netzwerkumgebung genauer widerspiegeln. Variable spielt eine wichtige Rolle bei der Performance-Optimierung.

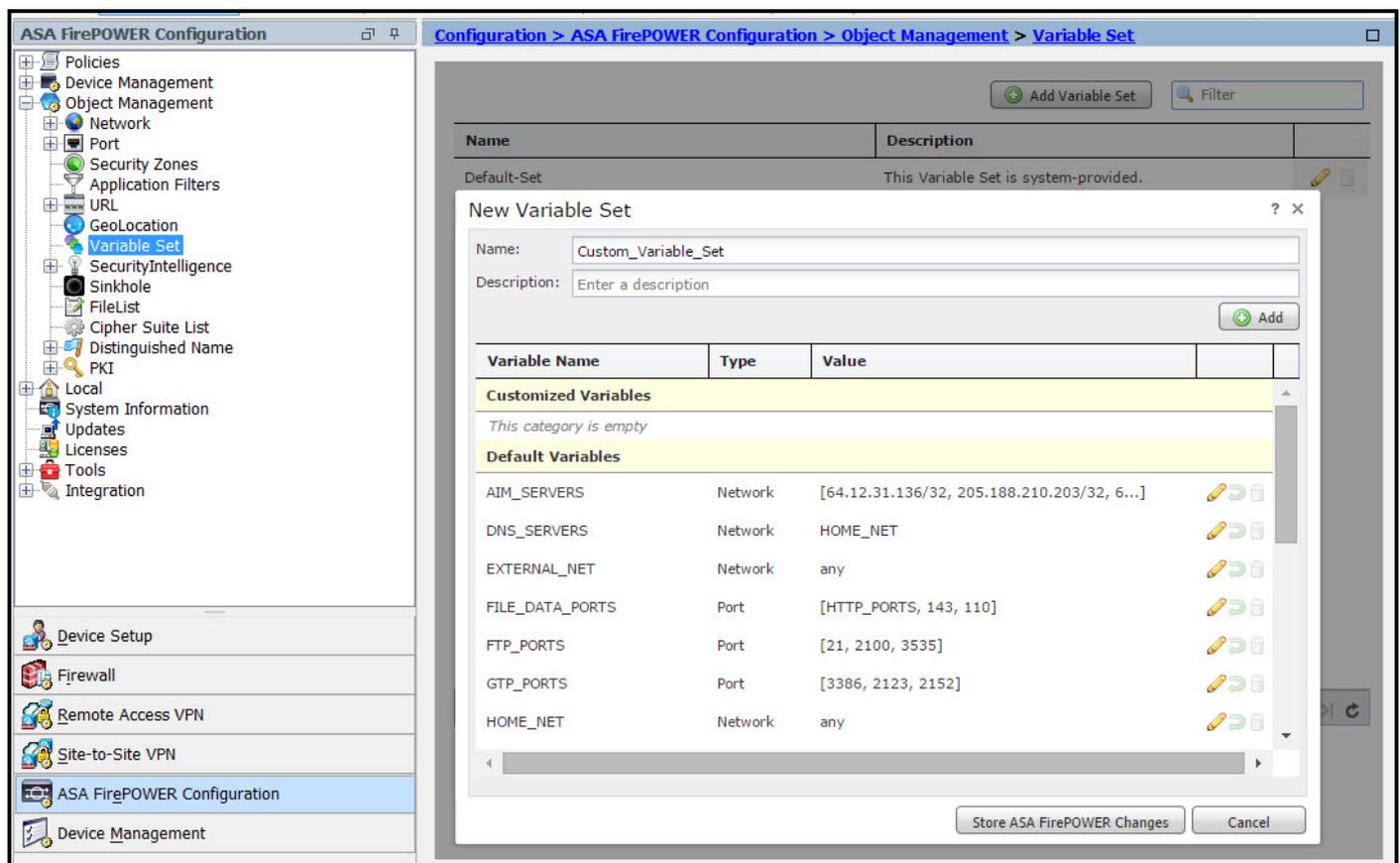
Die Variablensätze wurden bereits mit der Standardoption (Netzwerk/Port) konfiguriert. Fügen Sie neue Variablensätze hinzu, wenn Sie die Standardkonfiguration ändern möchten.

Um die Variablensätze zu konfigurieren, navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Object Management > Variable Set**. Wählen Sie die Option **Variablensatz hinzufügen**, um neue Variablensätze hinzuzufügen. Geben Sie den **Namen** der Variablensätze ein, und geben Sie die **Beschreibung** an.

Wenn eine benutzerdefinierte Anwendung an einem bestimmten Port funktioniert, definieren Sie die Portnummer im Feld Portnummer. Konfigurieren Sie den Netzwerkparameter.

**\$Home\_NET** legt das interne Netzwerk fest.

**\$External\_NET** gibt das externe Netzwerk an.



### Schritt 3: Konfigurieren der Zugriffskontrolle zur Einbindung von Intrusion Policy/NAP/Variable Sets

Navigieren Sie zu **Configuration > ASA FirePOWER Configuration > Policies > Access Control Policy**. Gehen Sie wie folgt vor:

1. Bearbeiten Sie die Zugriffsrichtlinien-Regel, der Sie die Richtlinie für Sicherheitsrisiken zuweisen möchten.
2. Wählen Sie die Registerkarte **Inspection** aus.
3. Wählen Sie die **Intrusion Policy** aus der Dropdown-Liste aus, und wählen Sie die **Variablensätze** aus der Dropdown-Liste aus.
4. Klicken Sie auf **Speichern**.

Standard Rules											
1	Access_Policy_Rule	any	<input checked="" type="checkbox"/> Allow   0  								

Editing Rule - Access\_Policy\_Rule

Name:   Enabled [Move](#)

Action:  **IPS:** IPS\_Policy **Variables:** Default-Set **Files:** no inspection **Logging:** no logging

Intrusion Policy:  Variable Set:

File Policy:

Da dieser Zugriffsrichtlinienregel eine Intrusion Policy hinzugefügt wird. Sie können das Schildsymbol in Golden Color sehen, das anzeigt, dass die Intrusion Policy aktiviert ist.

Identity Policy: None SSL Policy: None Status: Access Control policy out-of-date on device

Rules:

#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	Users	Applicat...	Src Ports	Dest Ports	URLs	Action					
<b>Administrator Rules</b>																
This category is empty																
<b>Standard Rules</b>																
1	Access_Policy_Rule	any	any	any	any	any	any	any	any	any	<input checked="" type="checkbox"/> Allow			0		
<b>Root Rules</b>																
This category is empty																
<b>Default Action</b>																
Intrusion Prevention: Balanced Security and Connectivity																

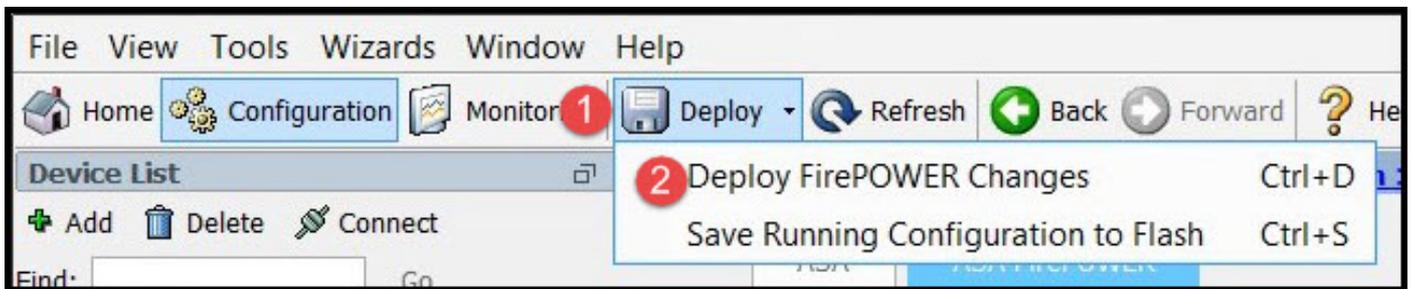
Displaying 1 - 1 of 1 rules | Page 1 of 1

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

## Schritt 4: Bereitstellung einer Zugriffskontrollrichtlinie

Jetzt müssen Sie die Zugriffskontrollrichtlinie bereitstellen. Bevor Sie die Richtlinie anwenden, wird auf dem Gerät die Meldung Access Control Policy (Zugriffskontrollrichtlinie) veraltet angezeigt. So stellen Sie die Änderungen am Sensor bereit:

1. Klicken Sie auf **Bereitstellen**.
2. Klicken Sie auf **FirePOWER-Änderungen bereitstellen**.
3. Klicken Sie im Popup-Fenster auf **Bereitstellen**.



**Hinweis:** In Version 5.4.x müssen Sie auf Apply ASA FirePOWER Changes 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 Konfigurationsänderung anzuwenden.

## Schritt 5: Überwachung von Angriffseignissen

Um die vom FirePOWER-Modul generierten Angriffseignisse anzuzeigen, navigieren Sie zu **Überwachung > ASA FirePOWER Monitoring > Real Time Event**

Monitoring > ASA FirePOWER Monitoring > Real Time Eventing

Real Time Eventing

Gaurav\_Connection\_Events ✕ All ASA FirePOWER Events Connection Intrusion File Malware File Security Intelligence

**Filter**

Rule Action=Block ✕ reason=Intrusion Block ✕

Pause Refresh Rate 5 seconds 1/10/16 6:13:42 PM (IST)

Receive Times	Action	Event Type	Inline Result	Reason
1/10/16 6:11:50 PM	Block	ASA FirePOWER Connection		Intrusion Block
1/10/16 6:09:52 PM	Block	ASA FirePOWER Connection		Intrusion Block
1/10/16 6:09:37 PM	Block	ASA FirePOWER Connection		Intrusion Block

## Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

## Fehlerbehebung

Schritt 1: Stellen Sie sicher, dass der Regelstatus ordnungsgemäß konfiguriert ist.

Schritt 2: Stellen Sie sicher, dass die richtigen IPS-Richtlinien in die Zugriffsregeln aufgenommen wurden.

Schritt 3: Stellen Sie sicher, dass die Gruppen "Variablen" korrekt konfiguriert sind. Wenn die Variablensätze nicht korrekt konfiguriert sind, stimmen die Signaturen nicht mit dem Datenverkehr überein.

Schritt 4: Stellen Sie sicher, dass die Bereitstellung der Zugriffskontrollrichtlinie erfolgreich abgeschlossen ist.

Schritt 5: Überwachen Sie die Verbindungsereignisse und Angriffsereignisse, um zu überprüfen, ob der Datenverkehrsfluss die richtige Regel trifft oder nicht.

## Zugehörige Informationen

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