# 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.

<u>File View Tools Wizards Window H</u> elp		Type topic to search	Go
🚮 Home 🦓 Configuration 🔯 Monitoring 🔲 Save ASA Changes	s 🔇 Refresh 🔇 Back 🕥 Forward 🢡 Help	5	CISCO
ASA FirePOWER Configuration 🛛 🕤 🚺 Configuration	n > ASA FirePOWER Configuration > Policies	> Intrusion Policy > Intrusion Policy	
Policies     Access Control Policy     Intrusion Policy     Files     SSL     Accions Alerts	o policies defined. Click Create Policy to create a polic	V Compare Polic	Create Policy
Identity Policy	Create Intrusion Policy	?	×
Dis Folicy     Dougle Management     Object Management     Local     System Information	Policy Information Name * Bescription Besc	LAB	
Conses     Consess     Consesses     Con	Drop when Inline 5	urity and Connectivity	
A Device Setup	* Required		
🗊 Firewall		Create Policy Create and Edit Policy Cance	
Remote Access VPN			
Site-to-Site VPN			
ASA FirePOWER Configuration			
Device Management			
» •			Hile
	<admin> 15</admin>	🔂 🌌 🛛 🔒 1	/4/16 1:17:37 AM UTC

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

niguration 2 AS	A HIEFOWER Coning		Compare Policies	s) 💿 Create Policy
Intrusion Policy	Drop when Inline	Status	Last Modified	
IPS_Policy IPS_policy for LAB	Yes	<u>No access control policies use this policy</u> Policy not applied on device	2016-01-04 07:40:00 Modified by "admin"	🖪 🕞 🥒 🖯

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.

File View Tools Wizards Window Help			Type topic to	search	Go ululu
Thome Configuration Monitoring Deplo	y • C Refresh	Back Forward	Кар		cisco
ASA FirePOWER Configuration 🗗 🖣 🚾	onfiguration > ASA	FirePOWER Configu	ration > Policies > Intrusion	Policy > Intrusion Polic	ay □
□ □ Policies □ □ ■ Access Control Policy □ □ ■ Intrusion Policy				Compare Policies	Create Policy
Sule Editor	Intrusion Policy	Drop when Inline	Status	Last Modified	
Files     SSL     SSL     Jentity Policy     DNS Policy     Object Management     Ccal     Ccal     System Information     Updates     Licenses     Licenses     Tools     Integration	IPS_policy IPS_policy for LAB	Yes	<u>Used by 1 access control policy</u> Policy up-to-date on device	2016-01-04 07:40:00 Modified by "admin"	2

#### 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.

- 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.

Policy Information 🖄	Policy Information	< Back			
Rules ⊕ Advanced Settings	Name IPS_Policy				
⊕ Policy Layers	Drop when Inline  Base Policy Balanced Security and Connectivity Manage Bas				
	<ul> <li>The base policy is up to date (Rule Update 2015</li> <li>This policy has 7591 enabled rules</li> <li>⇒ 114 rules generate events</li> <li>X 7477 rules drop and generate events</li> </ul>	i-10-01-001-vrt) Manage Rules View View			
	This policy contains enabled preprocessor rules. Please the preprocessors have the correct settings for these r Commit Changes Disca	e read the rule documentation to ensure rules ard Changes			

#### 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.

Policy Information	Rules		< Back
Rules	Rule Configuration	Filter: heartbleed	× ?
⊕ Advanced Settings	Rule Content	Filter returned 33 results	
④ Policy Layers	Category app-detect	Rule State Event Filtering Dynamic State Alerting Comments	Policy
	browser-chrome browser-firefox	GID SID     Message ▲       □     1     30549       SERVER-OTHER OpenSSL Heartbleed masscan access exploitation attempt	× vouv
	browser-ie browser-other browser-plugins browser-webkit content-replace	1         30777           SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	×
		1         30778         SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	×
		1         30785         SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	×
	decoder exploit-kit	1         30514         SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	×
	file-executable	1         30779         SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	×
	file-flash Classifications	1         30780         SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	×
	Microsoft Vulnerabilities Microsoft Worms	SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	×
	Platform Specific	1     30515       SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	×
	Preprocessors	SERVER-OTHER OpenSSL TLSv1.1 large heartbeat	¥
	Rule Update	к	< 1 of 1 > >

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

Policy Information 🛆	Rules		< Back
Rules	Rule Configuration	Filter: CVE:"2013-2135"	× ?
⊕ Advanced Settings	Rule Content	Filter returned 2 results	
⊕ Policy Layers	Message A	⇔ ▼ ▼ ▼	Policy T
	GID	GID SID Message 🔺	⇒ 🔻 🕑 🕕 🖓
	Reference     CVE ID	1 27575     SERVER-APACHE Apache Struts arbitrary OGNL remote code     execution attempt	×
	URL Buotrag ID	1 27574     SERVER-APACHE Apache Struts OGNL getRuntime.exec static metho access attempt	<sup>d</sup> 🗙
	Nessus ID Arachnids ID Mcafee ID Action Protocol Direction Source IP		
	Category		
	Classifications		
	Microsoft Vulnerabilities		
	Microsoft Worms		
	Platform Specific		
	Preprocessors		
	Priority		/
	Rule Update	K	

#### 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.

Policy Information	Rules		< Back
Rules	Rule Configuration	Filter:	× ?
⊕ Advanced Settings	Rule Content	Filter returned 33 results	
	Category app-detect	Rule State Event Filtering Dynamic State Alerting Comments	Policy
	browser-chrome browser-firefox	Generate Events     age ▲       Image: Drop and Generate Events     Image: Exercise Comparison of the comparison of	×
	browser-ie browser-other	Disable FR-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	* ×
	browser-plugins	1         30778         SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	* ×
	content-replace	1         30785         SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	* 🗙
	decoder exploit-kit	I         30514         SERVER-OTHER OpenSSL SSLv3 large heartbeat response - possible ssl heartbleed attempt	<sup>a</sup> ×
	file-executable	1         30779         SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	* ×
	Classifications	1         30780         SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	*
	Microsoft Vulnerabilities	1 30786     SERVER-OTHER OpenSSL TLSv1 large heartbeat response     presible of heartbland attempt	* ×
	Microsoft Worms Platform Specific	SERVER-OTHER OpenSSL TLSv1 large heartbeat response possible ssl heartbleed attempt	× ×
	Preprocessors	SERVER-OTHER OpenSSL TLSv1.1 large heartbeat	×
	Priority Rule Update	M	< 1 of 1 > >

#### 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.

GID	SIL Th	reshold 3				$\Rightarrow$	7	0	0	ç
1	280 Su	ppression	T 360.cn SafeG ess attempt	iuard local HTTP i	management	×				
1	28t Rer	move Thresholds	360.cn Safegua	rd runtime outboun	d communication	$\Rightarrow$				
1	32E Rer	move Suppressions 209.53.113	Absolute Softwa	re Computrace out	oound connection -					
1	32846	APP-DETEC absolute.co	r Absolute Softwa m	re Computrace out	oound connection -	⇒				ſ
1	32847	APP-DETEC bh.namequ	F Absolute Softwa ery.com	Set Threshold	d for 1 rule		?	×		
1	32848	APP-DETEC namequery.	r Absolute Softwa nettrace.co.za	4 Type	Limit	•				
1	26286	APP-DETEC search.dns	F Absolute Softwa search.org	Count	10					
1	26287	APP-DETEC search.nam	F Absolute Softwa equery.com	7 Seconds	60		7			

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.

⇒ ▼ 2 💎 ▼ Rule State Event Filte	ering Dynami	00 ▼ G c State Alerting C	⊃ ▼ Comments	Polic	У			•
GID SID Threshol	d			⇒	7	•	9	
🗌 1 🚺 Suppress	sion	T 360.cn SafeGua ess attempt	ard local HTTP mana	gement 🗙				
1 280 Remove 1 Remove 9	Thresholds Suppressions	360.cn Safeguard on	runtime outbound	$\Rightarrow$				
1 32845	APP-DETECT connection -	Absolute Software 209.53.113.223	Computrace outbound	$\Rightarrow$				
1 32846	APP-DETECT connection -	Absolute Software absolute.com	Computrace outbound	⇒	•			
Add Suppression Suppression Type 1 20207 1 32849	A Rule	Software uery.cor Software y.nettrai Software ssearch. Software search.namequery Absolute Software search.us.namequ	Add Suppression Type Network Add Suppression Type Network	n for 1 rule Source 5 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	▼ ▼	? X Cancel	:	

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-base 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 kommagetrennte 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.

Policy Information	Rules		< Back
Rules	Rule Configuration	Filter:	x 7
Advanced Settings	Rule Content	1 selected rule of 33	
Policy Layers	Category app-detect	→ ▼ ▼ <sup>2</sup> <sup>3</sup> <sup>3</sup> <sup>3</sup> <sup>3</sup> <sup>4</sup> <sup>3</sup> <sup>3</sup> <sup>4</sup> <sup>3</sup> <sup>4</sup> <sup>3</sup> <sup>4</sup> <sup>3</sup> <sup>4</sup> <sup>3</sup> <sup>4</sup> <sup>4</sup> <sup>4</sup> <sup>4</sup> <sup>4</sup> <sup>4</sup> <sup>4</sup> <sup>4</sup>	Policy V
	blacklist browser-chrome	GID SID M3 Add Rate-Based Rule State SER Remove Rate-Based Rule States ed masscan access	→ <b>▼</b> ⊙ <b>0 </b>
	browser-firefox browser-ie	SERVER-OTHER OpenSSL SSLv3 large heartbeat response	<u>~</u>
	browser-other browser-plugins	Add Rate-Based Rule State for 1 rule	? X
	content-replace	1         30785         5         Network         192.168.20.3           6         Rate         10         Count / 5	Seconds
	exploit-kit	1     30514     7     New State     Drop and Generate Events ▼       1     20770     8     Timeout     30	·
	file-flash  Classifications	ОК 9 ОК	Cancel
	Microsoft Vulnerabilities Microsoft Worms	SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	×
	Platform Specific	1         30515         SERVER-OTHER OpenSSL TLSv1 large heartbeat response - possible ssl heartbleed attempt	×
	Priority	SERVER-OTHER OpenSSL TLSv1.1 large heartbeat	× · · · · · · · · · · · · · · · · · · ·
	Rule Update	K	< 1 of 1 > >

# 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.

Configuration > ASA FireP	POWER Configuration > Policies > Access	S Control Policy			
ASA ASA FirePOV	WER				
				_	
Default Allow Al	ll Traffic				
custom policy					
			M 📃 Status: Policy Up-to-date on device		
Identity Policy: None	SSL Policy: None				
Rules Security Intellig	Network Analysis and Intrusion Pol	icies	? ×		
General Settings	Intrusion Policy used before Access Control	No Rules Active		ø	
Maximum URL characters	rule is determined			No	
Allow an Interactive Bloc	Intrusion Policy Variable Set	Default-Set	<b>_</b>	<i>a</i>	
Retry URL cache miss loo	Network Analysis Rules	No Custom Rules	Network Analysis Policy List	Disabled	
Inspect traffic during pol	Default Network Analysis Policy	Balanced Security	and Connectivity	li li	
Identity Policy Settine	Pavart to Defaults			Ø	
Identity Policy	(Reverted behavits)	None		5	
CCL Dolioy Cottings		A	Performance Statistics - Sample Time (seconds)	300	
SSL Policy Settings			Regular Expression - Limit	Default	
SSL Policy to use for inspe	cting encrypted connections	None	Regular Expression - Recursion Limit	Default	
Network Analysis and I	Intrusion Policies	Ø	Intrusion Event Logging Limits - Max Events Stored Per Packet	8	-
			ER-Changes Cancel		

#### 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.

ASA FirePOWER Configuration	Configuration > ASA FirePOW	ER Configurati	ion > Object Management > <u>Variable Set</u>		
Policies     Solution     Policies     Solution     Solution	Name		Add Variable Set	Filter	
Security Zones	Default Cat		This Variable Cat is sustain annuided		R
Application Filters	Naw Variable Set		This Variable Set is system-provided.	6 2 ¥	
GeoLocation	New variable Sec				
Variable Set     E:      SecurityIntelligence	Name: Custom_Variab	le_Set			
Sinkhole	Description: Enter a descrip	tion			
Cipher Suite List				💿 Add	
⊕ - I Distinguished Name ⊕ - ♀ PKI	Variable Name	Туре	Value		
Local	Customized Variables	24			
Updates	This category is empty				
Licenses	Default Variables				
Integration	AIM_SERVERS	Network	[64.12.31.136/32, 205.188.210.203/32, 6]	Ø76	
	DNS_SERVERS	Network	HOME_NET	/>B	
	EXTERNAL_NET	Network	any	<b>23</b> 6	
	FILE_DATA_PORTS	Port	[HTTP_PORTS, 143, 110]	@ <b>2</b> 6	
Bevice Setup	FTP_PORTS	Port	[21, 2100, 3535]	@ <b>&gt;</b> 6	
Firewall	GTP_PORTS	Port	[3386, 2123, 2152]	@>6	
Remote Access VPN	HOME_NET	Network	any	Ø28 _	> C
Site-to-Site VPN					
ASA FirePOWER Configuration					
Device Management			Store ASA FirePOWER Char	iges Cancel	

# 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	any	any	any ai	ny any	any	any	any	🖋 Allow	0000	Ø 8
Root Rules										1	
Editing Rule - Access_	Policy_R	ule									? ×
					1949						
Name Access_Policy_Rule					Enabled		Move				
Action			▼ IP9	5: IPS_Policy	Variables: D	efault-Set	Files: no i	inspection Lo	gging: no la	gging	
Zones Networks 🔺	Users	Applicatio	ns Port	s 🔺 URLs	🔺 ISE At	tributes	2	Inspection	Logging	Comment	ts
Intrusion Policy				(833)	1	Variable	Set		9		
IPS_Policy					× 🖉	Default	Set				
3											
File Policy											
None										*	
											_
								4	Save	Cancel	

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

									🖌 📑 Sta	tus: Access Cont	trol policy out-	of-date on devic	e
Ide	ntity Policy: None	0	SSL Policy: N	lone							0		
Ru	les Security Ir	telligence	HTTP Responses	Advanced									
								🕜 Add Ca	tegory 📀 A	dd Rule Search	Rules		×
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	Users	Applicat	Src Ports	Dest Ports	URLs	Action	Ç 🔒 🔊 🤍	
Adn	ninistrator Rules					2	25)			20			
This	category is empty												
Sta	ndard Rules												
1	Access_Policy_Rul	any	any	any	any	any	any	any	any	any	Allow	0 [] (] 🤍	0
Roo	t Rules										/	1	
This	category is empty												
Def	ault Action							Intrusion P	revention: Balan	iced Security and	d Connectivity	*	\$ 📕
									Displaying	1 - 1 of 1 rules	< < Page	e 1 of 1 >	> c
					Store	ASA FirePOW	ER Changes	Cancel					

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.

File View Tools Wizards Window	Help	
Home 🍓 Configuration 🔯 Monitor	Deploy - 🐼 Refresh 🔇 Back 🚫 Forward	? He
Device List	2 Deploy FirePOWER Changes Ctrl	I+D
🕈 Add 📋 Delete 🚿 Connect	Save Running Configuration to Flash Ctrl	I+S
Find: Go	1071 FORTHOLOWER	

Deploy FirePOWER Changes	
Deploy Policies Version:2016-01-05 09:09 AM	?
<ul> <li>System Policy: Default</li> <li>Sensor Policy: firepower</li> <li>Access Control Policy: Default Allow All Traffic</li> <li>Intrusion Policy: Balanced Security and Connectivity</li> <li>Intrusion Policy: IPS_Policy</li> <li>DNS Policy: Default DNS Policy</li> </ul>	
3 Deploy Can	el

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 Angriffsereignissen

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

Seventing					
Gaurav_Connection_Ever	All ASA FirePOWER Event	Connection Ir	ntrusion	ile Malware File	Security Intelligen
ilter Rule Action=Block * reason	=Intrusion Block ×				
<b>Pause</b> Refresh R Receive Times	ate 5 seconds ~ Action Ev	1/10/16 6:13:42 ent Type	PM (IST)	Inline Result	Reason
Pause Refresh R Receive Times 1/10/16 6:11:50 PM	ate <b>5 seconds</b> Action     Ev       Block     AS	1/10/16 6:13:42 ent Type A FirePOWER Conne	PM (IST) ection	Inline Result	Reason Intrusion Block
Pause         Refresh R           Receive Times         1/10/16 6:11:50 PM           1/10/16 6:09:52 PM         1/10/16 6:09:52 PM	ate <mark>5 seconds ~</mark> Action Ev Block AS Block AS	1/10/16 6:13:42 ent Type A FirePOWER Conne A FirePOWER Conne	PM (IST) ection ection	Inline Result	Reason 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