Überprüfung einer benutzerdefinierten SID-Liste von FirePOWER-Sensoren mithilfe der CLI und der FMC-GUI

Einführung

In diesem Dokument wird beschrieben, wie Sie mithilfe der CLI und der FMC-GUI eine benutzerdefinierte SID-Liste von FirePOWER Threat Defense (FTD)- oder FirePOWER-Modulen erhalten. SID-Informationen finden Sie in der FMC-GUI, wenn Sie zu *Objects > Intrusion Rules* (Objekte *> Intrusion Rules)* navigieren. In einigen Fällen ist es erforderlich, eine Liste der verfügbaren SIDs über die CLI abzurufen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie die folgenden Themen kennen:

- Cisco FirePOWER Threat Defense (FTD)
- Cisco ASA mit FirePOWER Services
- Cisco FirePOWER Management Center (FMC)
- Linux-Grundkenntnisse

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der folgenden Softwareversion:

- FirePOWER Management Center 6.6.0
- Firepower Threat Defense 6.4.0.9
- FirePOWER-Modul 6.2.3.2

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

Eine *Intrusion-Regel* ist eine Reihe von Schlüsselwörtern und Argumenten, die das System verwendet, um Versuche zu erkennen, Schwachstellen in Ihrem Netzwerk auszunutzen. Während das System den Netzwerkverkehr analysiert, vergleicht es Pakete mit den in den einzelnen Regeln festgelegten Bedingungen. Wenn die Paketdaten mit allen in einer Regel angegebenen Bedingungen übereinstimmen, wird die Regel ausgelöst. Wenn eine Regel eine Warnregel ist, wird ein Intrusion-Ereignis generiert. Wenn es sich um eine Pass-Regel handelt, wird der Datenverkehr ignoriert. Bei einer Drop-Regel in einer Inline-Bereitstellung verwirft das System das Paket und generiert ein Ereignis. Sie können Intrusion Events über die FirePOWER Management

Center-Webkonsole anzeigen und auswerten.

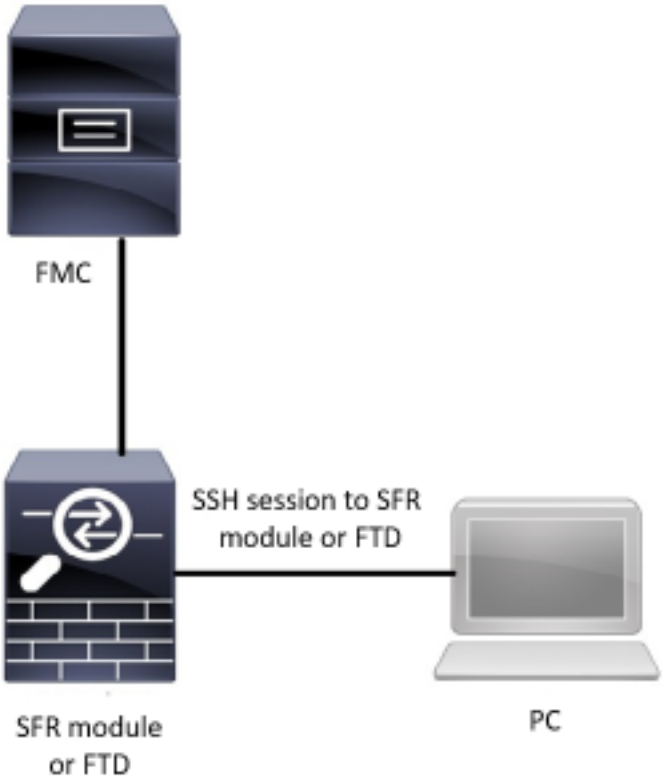
Das FirePOWER-System bietet zwei Arten von Intrusion-Regeln: ***gemeinsam genutzte Objektregeln*** und ***Standardtextregeln***. Die Cisco Talos Security Intelligence and Research Group (Talos) kann gemeinsam genutzte Objektregeln verwenden, um Angriffe auf Schwachstellen auf eine Weise zu erkennen, die mit herkömmlichen Standardtextregeln nicht möglich ist. Es ist nicht möglich, Regeln für freigegebene Objekte zu erstellen. Wenn Intrusion-Regeln auf eigene Faust geschrieben werden, muss eine Standardtextregel erstellt werden. Benutzerdefinierte Standardtextregeln zur Anpassung der zu erwartenden Ereignistypen. Durch das Schreiben von Regeln und das Angeben der Ereignismeldung der Regel können Sie Datenverkehr, der Angriffe und Richtlinienumgehungen anzeigt, leichter identifizieren.

Wenn Sie eine benutzerdefinierte Standardtextregel in einer benutzerdefinierten Zugriffsrichtlinie aktivieren, sollten Sie bedenken, dass bei einigen Regelschlüsselwörtern und -argumenten zunächst der Datenverkehr dekodiert oder vorverarbeitet werden muss.

Eine ***benutzerdefinierte lokale Regel*** auf einem FirePOWER-System ist eine benutzerdefinierte Snort-Regel, die Sie in einem ASCII-Textdateiformat von einem lokalen Computer importieren. Mit einem FirePOWER-System können Sie lokale Regeln über die Webschnittstelle importieren. Die Schritte zum Importieren lokaler Regeln sind sehr einfach. Um jedoch eine optimale lokale Regel zu schreiben, müssen Benutzer mit Snort- und Netzwerkprotokollen vertraut sein.

> **Warnung**: Stellen Sie sicher, dass Sie eine kontrollierte Netzwerkumgebung verwenden, um alle von Ihnen erstellten Zugriffsregeln zu testen, bevor Sie die Regeln in einer Produktionsumgebung verwenden. Unzureichend geschriebene Intrusion Rules können die Leistung des Systems ernsthaft beeinträchtigen

Netzwerkdiagramm

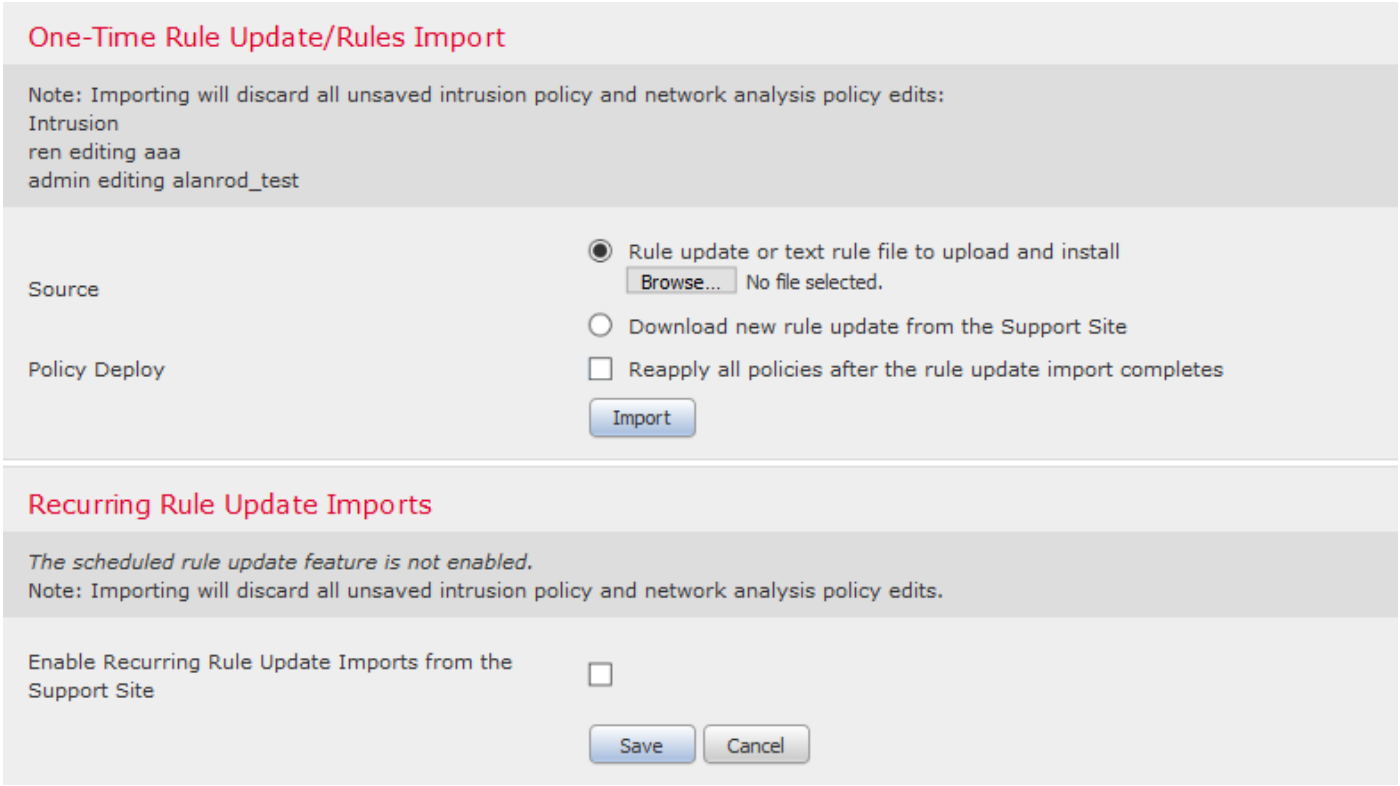


Konfigurieren

Lokale Regeln importieren

Bevor Sie beginnen, müssen Sie sicherstellen, dass die in der benutzerdefinierten Datei aufgeführten Regeln keine Sonderzeichen enthalten. Der Regelimporteur verlangt, dass alle benutzerdefinierten Regeln mit ASCII- oder UTF-8-Codierung importiert werden. In der folgenden Prozedur wird erläutert, wie lokale Standardtextregeln aus einem lokalen Computer importiert werden.

Schritt 1: Öffnen Sie die Registerkarte **Regeln importieren**, indem Sie **auf Objekte > Zugriffsregeln > Regeln importieren klicken.** Die Seite **Regelaktualisierungen** wird wie in der Abbildung unten angezeigt:



Schritt 2: Wählen Sie **Regelupdate oder Textregeldatei zum Hochladen und Installieren aus** und klicken Sie auf **Durchsuchen**, um die benutzerdefinierte Regeldatei auszuwählen.

> **Hinweis**: Alle hochgeladenen Regeln werden in der Kategorie **lokale Regeln** gespeichert.

Schritt 3: Klicken Sie auf **Importieren**. Die Regeldatei wird importiert

> **Hinweis**: Die FirePOWER-Systeme verwenden den neuen Regelsatz nicht für die Prüfung. Um eine lokale Regel zu aktivieren, müssen Sie diese in der Intrusion Policy aktivieren und anschließend die Richtlinie anwenden.

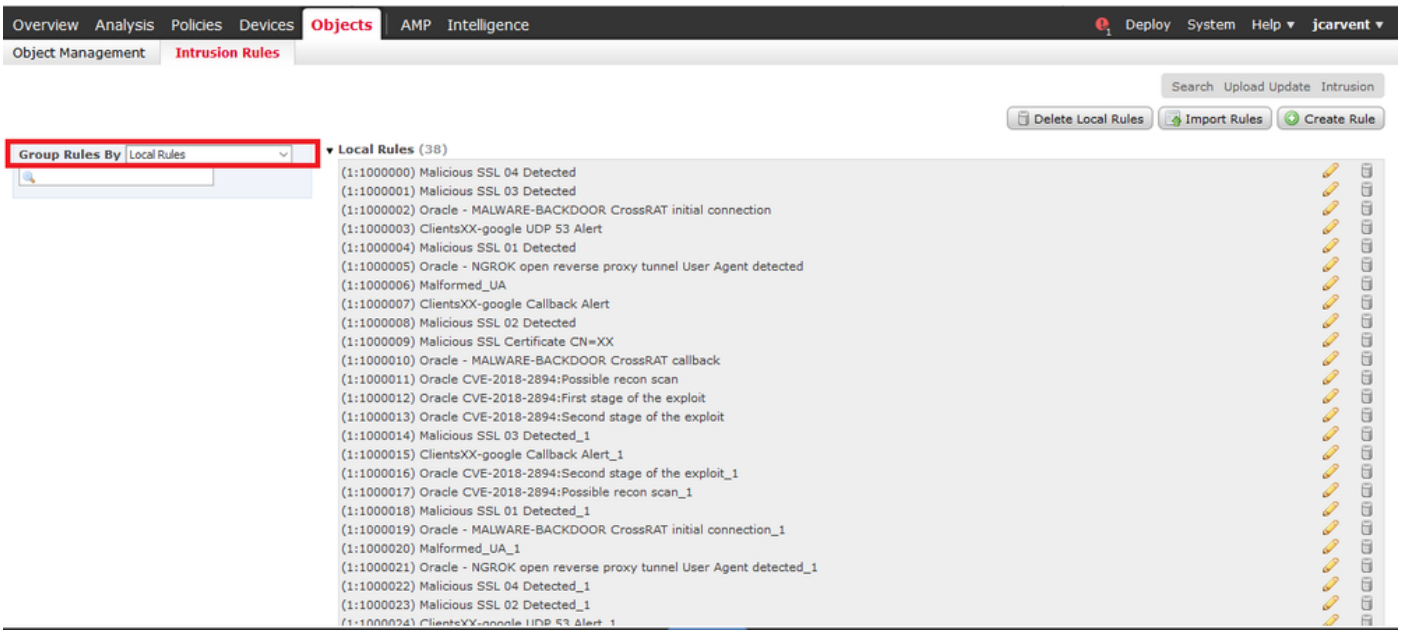
Überprüfen

Von der FMC-GUI

1. Lokale Regeln anzeigen, die von der FMC-GUI importiert wurden

Schritt 1: Navigieren Sie zu **Objekte > Angriffsregeln**

Schritt 2: Wählen Sie **Lokale Regeln** aus **Gruppenregeln**



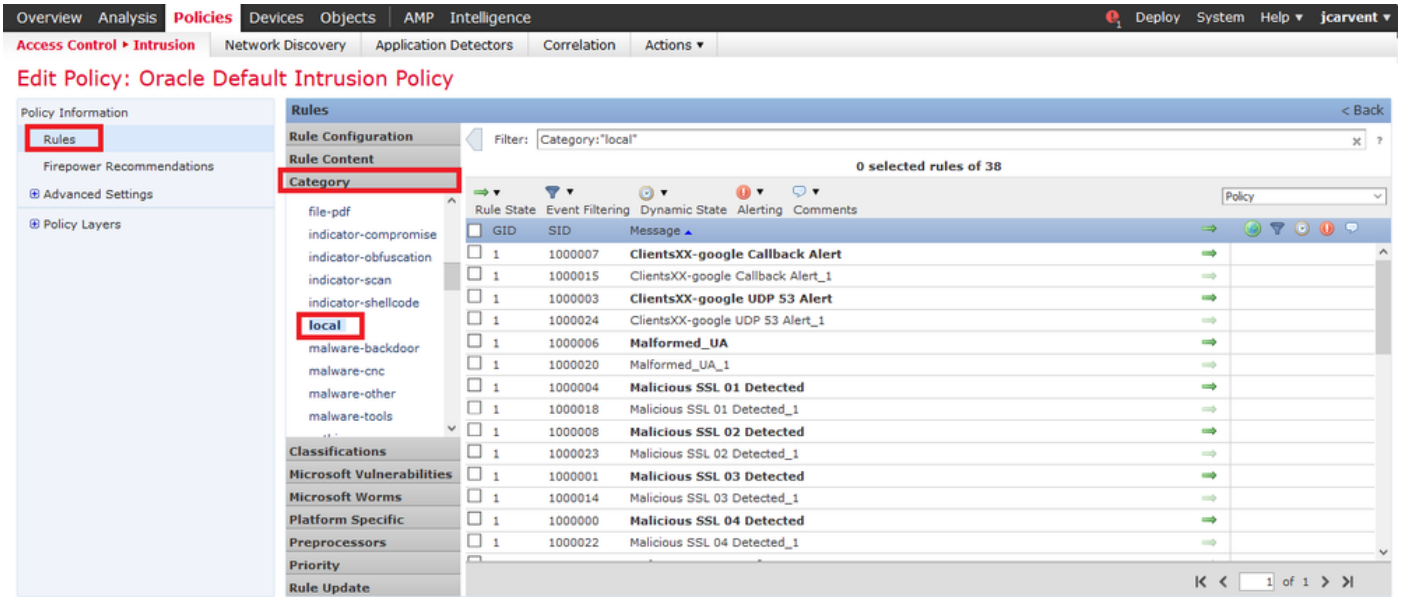
Standardmäßig legt das FirePOWER-System die lokalen Regeln in einem deaktivierten Zustand fest. Diese lokalen Regeln müssen manuell den Zustand lokaler Regeln festlegen, bevor Sie diese in Ihrer Richtlinie für Sicherheitsrisiken verwenden können.

2. Aktivieren einer lokalen Regel aus der Richtlinie für Sicherheitsrisiken

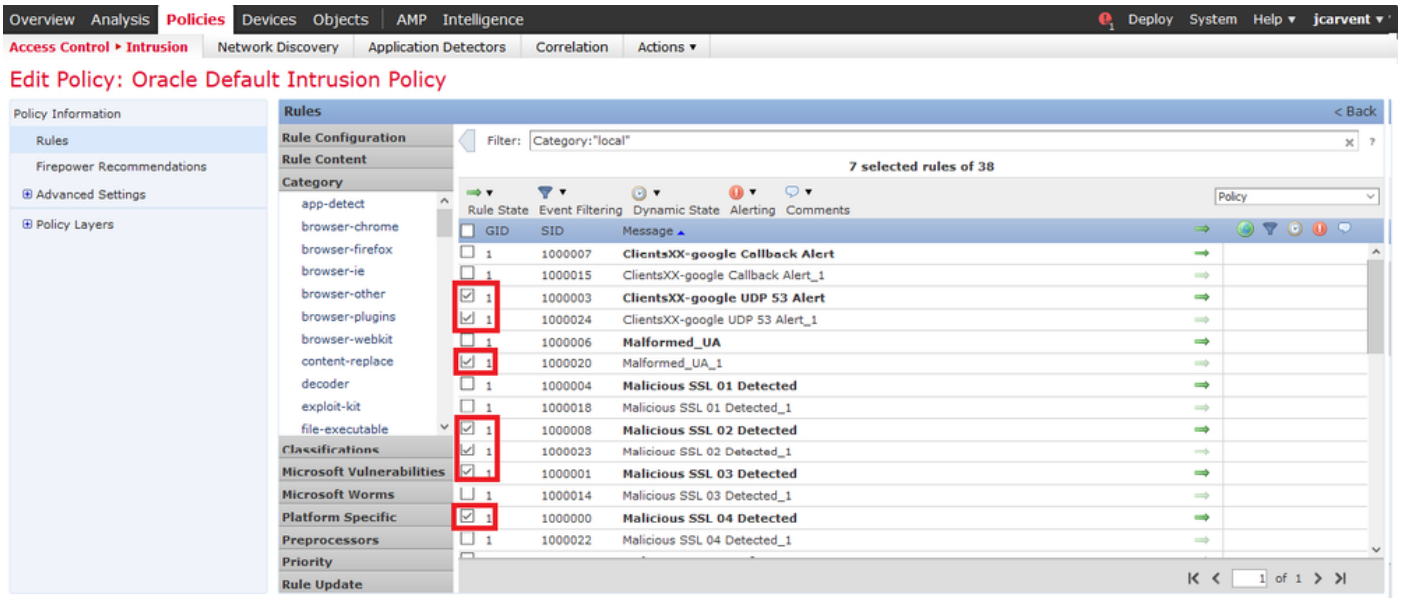
Schritt 1: Navigieren Sie zur Seite Richtlinien-Editor unter **Richtlinien > Sicherheitsrisiken > Angriffsrichtlinien.**

Schritt 2: Wählen Sie **Regeln** im linken Bereich aus.

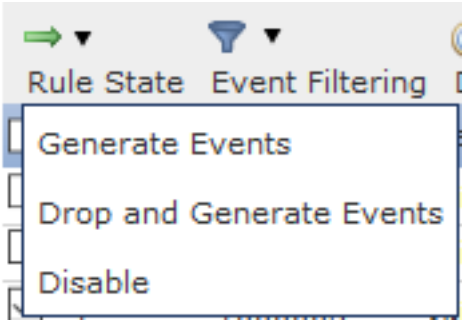
Schritt 3: Wählen Sie unter der **Kategorie** die Option **Lokal aus.** Wenn verfügbar, sollten alle lokalen Regeln angezeigt werden:



Schritt 4: Wählen Sie die gewünschten lokalen Regeln aus:



Schritt 5: Nachdem Sie die gewünschten lokalen Regeln ausgewählt haben, wählen Sie einen Status aus dem **Regelstatus aus.**



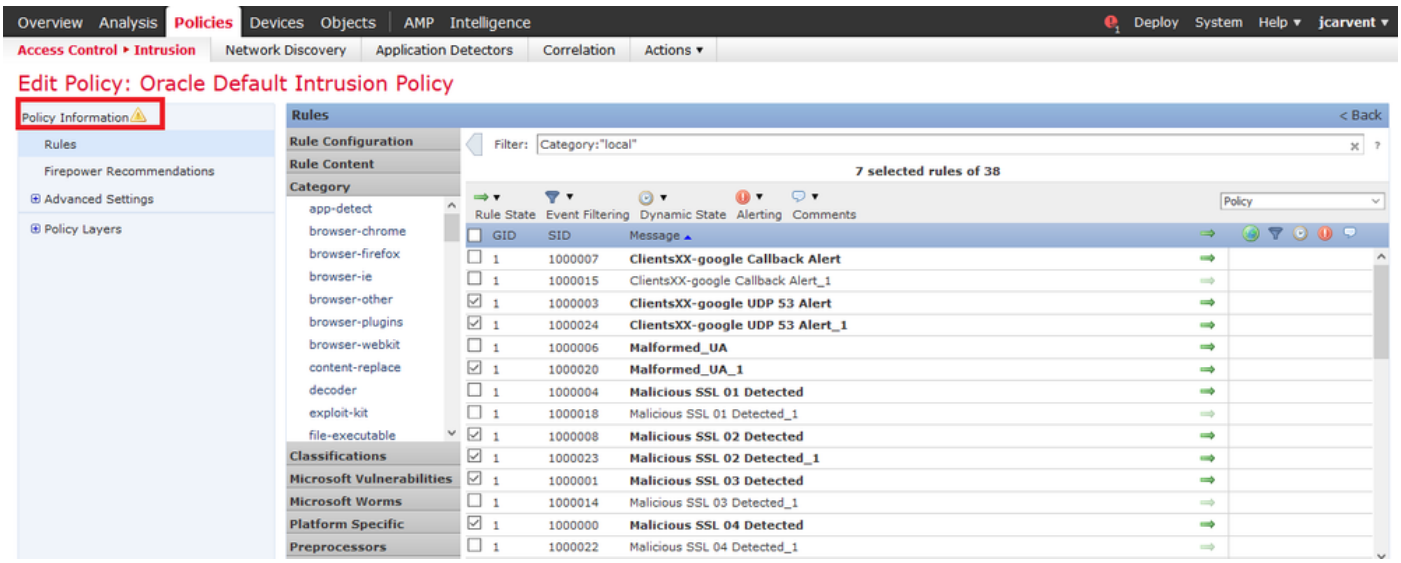
Folgende Optionen sind verfügbar:

- **Veranstaltungen generieren:** Aktivieren der Regel und Generieren eines Ereignisses

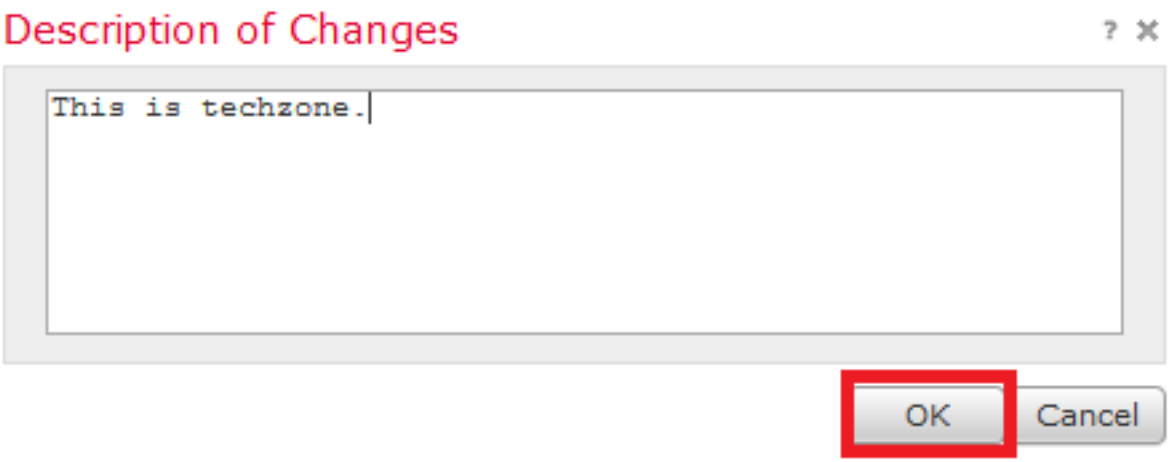
- **Verwerfen und Generieren von Ereignissen:** Aktivieren Sie die Regel, löschen Sie den Datenverkehr, und generieren Sie ein Ereignis.

- **Deaktivieren:** Keine Regel aktivieren, keine Ereignisse

Schritt 6: Wenn Sie den Regelstatus ausgewählt haben, klicken Sie auf Option **"Richtlinieninformationen"** im linken Bereich



Schritt 7: Wählen Sie die Schaltfläche **Änderungen bestätigen**, und geben Sie eine kurze Beschreibung der Änderungen an. Klicken Sie später auf **OK**. Die Intrusion Policy wird validiert.



> **Hinweis**: Die Richtlinienvalidierung schlägt fehl, wenn Sie eine importierte lokale Regel aktivieren, die das veraltete Grenzwert-Schlüsselwort in Kombination mit dem Intrusion Event Dreging Feature in einer Intrusion Policy verwendet.

Schritt 8: Bereitstellung der Änderungen

Von FTD oder SFR-Modul-CLI

1. Anzeigen der lokalen Regeln, die aus der CLI des FTD- oder SFR-Moduls importiert wurden

Schritt 1: Einrichten einer SSH- oder CLI-Sitzung über Ihr SFR-Modul oder FTD

Schritt 2: Zum Expertenmodus wechseln

```
> expert
admin@firepower:~$
```

Schritt 3: Administratorrechte erhalten

```
admin@firepower:~$ sudo su -
```

Schritt 4: Geben Sie Ihr Kennwort ein.

```
admin@firepower:~$ sudo su -
Password:
root@firepower:~#
```

Schritt 5: Navigieren Sie zu **/ngfw/var/sf/detect_engines/UUID/intrusion/**

```
root@firepower:/home/admin# cd /ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-
2369c038cbc9/intrusion/
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
```

> **Hinweis**: Wenn Sie das SFR-Modul verwenden, verwenden Sie nicht /ngfw/var/sf/detect_engines/*/intrusion path. Eingeschränkte Verwendung **/var/sf/detect_engines/*/intrusion**

Schritt 6: Stellen Sie den folgenden Befehl vor

```
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
```

Ein funktionierendes Beispiel ist das nachfolgende Bild:

```
root@firepower:/ngfw/var/sf/detection_engines/70f28390-f73d-11de-acfc-2369c038cbc9/intrusion#
grep -Eo "sid:*([0-9]{1,8})" */*local.rules
sid:1000008
sid:1000023
sid:1000007
sid:1000035
sid:1000004
sid:1000000
...
```

Hier wird die vom FTD- oder SFR-Modul aktivierte Kunden-SID-Liste aufgeführt.

Fehlerbehebung

Schritt 1: Stellen Sie sicher, dass die SSH-Sitzung für das SFR-Modul oder FTD erstellt wurde, von FMC Detection_engines an nicht aufgeführt ist.

Schritt 2: Der Befehl grep -Eo "sid:*([0-9]{1,8})" */*local.rules funktioniert nur unter Intrusion Directory. Der Befehl kann nicht in einem anderen Verzeichnis verwendet werden.

Schritt 3: Verwenden Sie den Befehl grep -Eo "sid:*([0-9]{1,8})" */*.rules, um eine vollständige SID-Liste aller Kategorien zu erhalten.

Best Practices für das Importieren lokaler Angriffsregeln

Beachten Sie beim Importieren einer lokalen Regeldatei die folgenden Richtlinien:

- Der Regelimporteur fordert, dass alle benutzerdefinierten Regeln in eine Nur-Text-Datei importiert werden, die in ASCII oder UTF-8 codiert ist.
- Der Name der Textdatei kann alphanumerische Zeichen, Leerzeichen und keine anderen Sonderzeichen als Unterstrich (_), Punkt (.) und Bindestrich (-) enthalten.
- Das System importiert lokale Regeln, denen ein einzelnes Pfund-Zeichen (#) vorangestellt ist, die jedoch als gelöscht gekennzeichnet sind
- Das System importiert lokale Regeln, denen ein einzelnes Pfund vorangestellt ist (#), und importiert keine lokalen Regeln, denen zwei Pfund vorangestellt sind (##)
- Regeln dürfen keine Escapezeichen enthalten.
- Beim Importieren einer lokalen Regel müssen Sie keine Generator-ID (GID) angeben. Wenn dies der Fall ist, geben Sie für eine Standardtextregel nur die GID 1 an.
- Wenn Sie eine Regel zum ersten Mal importieren, müssen Sie *nicht* Geben Sie ein Snort-ID (SID) oder Revisionsnummer. Dadurch werden Kollisionen mit SIDs anderer Regeln, einschließlich gelöschter Regeln, vermieden. Das System weist der Regel automatisch die nächste verfügbare benutzerdefinierte Regel SID von 100000 oder höher und eine Revisionsnummer von 1 zu.
- Wenn Sie Regeln mit SIDs importieren müssen, müssen die SIDs eindeutige Nummern zwischen 1.000.000 und 9.999.999 sein.
- In einer Bereitstellung mit mehreren Domänen weist das System importierten Regeln aus einem gemeinsamen Pool, der von allen Domänen auf dem FirePOWER Management Center. Wenn mehrere Administratoren gleichzeitig lokale Regeln importieren, können SIDs innerhalb einer einzelnen Domäne als nicht sequenziell erscheinen, da das System die dazugehörigen Nummern in der Sequenz einer anderen Domäne zugewiesen hat
- Beim Importieren einer aktualisierten Version einer lokalen Regel, die Sie zuvor importiert haben, oder bei der Wiedereinsetzung einer lokalen Regel, die Sie gelöscht haben, ***müssen*** Sie die vom System zugewiesene SID und eine Revisionsnummer hinzufügen, die größer ist als die aktuelle Revisionsnummer. Sie können die Versionsnummer einer aktuellen oder gelöschten Regel bestimmen, indem Sie die Regel bearbeiten

  Hinweis: Beim Löschen einer lokalen Regel erhöht das System automatisch die Revisionsnummer. Dies ist ein Gerät, mit dem Sie lokale Regeln wieder einrichten können. Alle gelöschten lokalen Regeln werden von der Kategorie für lokale Regeln in die Kategorie für gelöschte Regeln verschoben.

- Importieren lokaler Regeln in das primäre FirePOWER Management Center in einem Hochverfügbarkeitspaar, um Probleme mit der SID-Nummerierung zu vermeiden
- Der Import schlägt fehl, wenn eine Regel Folgendes enthält:Eine SID ist größer als 2147483647.Eine Liste von Quell- oder Zielports mit mehr als 64 Zeichen
- Die Richtlinienvalidierung schlägt fehl, wenn Sie eine importierte lokale Regel aktivieren, die das veraltete ***Grenzwert-Schlüsselwort*** in Kombination mit dem Intrusion Event Dreding-Feature in einer Intrusion Policy verwendet.
- Alle importierten lokalen Regeln werden automatisch in der lokalen Regelkategorie gespeichert
- Das System legt immer lokale Regeln fest, die Sie in den deaktivierten Regelstatus importieren. Sie müssen den Status lokaler Regeln manuell festlegen, bevor Sie diese in Ihrer Richtlinie für Sicherheitsrisiken verwenden können.

Zugehörige Informationen

Nachstehend finden Sie Referenzdokumente für die SNORT SID:

Regeln für Sicherheitsrisiken aktualisieren

https://www.cisco.com/c/en/us/td/docs/security/firepower/60/configuration/guide/fpmc-config-guide-v60/System_Software_Updates.html#ID-2259-00000356

Editor für Intrusion Rules

https://www.cisco.com/c/en/us/td/docs/security/firepower/660/configuration/guide/fpmc-config-guide-v66/the_intrusion_rules_editor.html