Die IP-Adresse wird durch die Sicherheitsintelligenz eines Cisco FireSIGHT-Systems blockiert oder Blacklist

Inhalt

Einführung

Mithilfe der Funktion "Sicherheitsinformationsfunktion" können Sie den Datenverkehr, der das Netzwerk durchläuft, anhand der Quell- oder Ziel-IP-Adresse angeben. Dies ist besonders nützlich, wenn Sie Datenverkehr an und von bestimmten IP-Adressen blockieren möchten, bevor der Datenverkehr anhand von Zugriffskontrollregeln analysiert wird. In diesen Dokumenten wird beschrieben, wie Sie Szenarien behandeln, in denen eine IP-Adresse von einem Cisco FireSIGHT-System blockiert oder in Blacklists gesetzt wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über das Cisco FireSIGHT Management Center verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Hardware- und Softwareversionen:

- Cisco FireSIGHT Management Center
- Cisco FirePOWER-Appliance

- Cisco ASA mit FirePOWER (SFR)-Modul
- Softwareversion 5.2 oder 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.

Unterschied zwischen Intelligence Feed und Intelligence List

Es gibt zwei Möglichkeiten, die Sicherheitsintelligenz-Funktion in einem FireSIGHT-System zu verwenden:

Sicherheitsinformations-Feed

Ein Sicherheitsinformations-Feed ist eine dynamische Sammlung von IP-Adressen, die das Defense Center von einem HTTP- oder HTTPS-Server herunterlädt. Um Ihnen bei der Erstellung von Blacklists zu helfen, stellt Cisco den *Security Intelligence Feed bereit*, der IP-Adressen darstellt, die vom Vulnerability Research Team (VRT) als schlecht bekannt eingestuft wurden.

Sicherheitsinformationsliste

Eine Sicherheitsinformationsliste ist im Gegensatz zu einem Feed eine einfache statische Liste von IP-Adressen, die Sie manuell in das FireSIGHT Management Center hochladen.

Legitime IP-Adresse wird blockiert oder Blacklist

Überprüfen Sie, ob sich eine IP-Adresse im Sicherheitsinformations-Feed befindet

Wenn eine IP-Adresse von der Blacklist des Security Intelligence Feed blockiert wird, können Sie die folgenden Schritte ausführen, um Folgendes zu überprüfen:

Schritt 1: Greifen Sie auf die CLI der FirePOWER-Appliance oder des Dienstmoduls zu.

Schritt 2: Führen Sie den folgenden Befehl aus. Ersetzen Sie <IP_Address> durch die IP-Adresse, nach der Sie suchen möchten:

```
admin@Firepower:~$ grep
```

Wenn Sie beispielsweise nach der IP-Adresse 198.51.100.1 suchen möchten, führen Sie den folgenden Befehl aus:

```
admin@Firepower:~$ grep 198.51.100.1 /var/sf/iprep_download/*.blf
```

Wenn dieser Befehl eine Übereinstimmung mit der von Ihnen angegebenen IP-Adresse zurückgibt, wird darauf hingewiesen, dass die IP-Adresse in der Blacklist der Sicherheitsinformations-Feed aufgeführt ist.

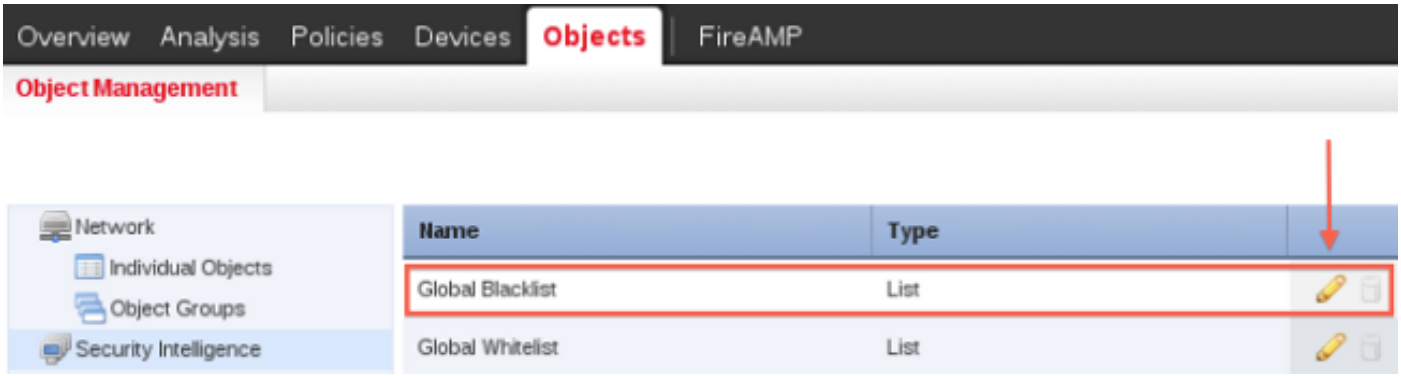
Blacklist überprüfen

Führen Sie die folgenden Schritte aus, um eine Liste der IP-Adressen zu finden, die möglicherweise in Blacklists gesetzt werden:

Schritt 1: Zugriff auf die Webschnittstelle des FireSIGHT Management Center.

Schritt 2: Navigieren Sie zu **Objekte > Objektverwaltung > Sicherheitsintelligenz**.

Schritt 3: Klicken Sie auf das *Bleistiftsymbol*, um die **globale Blacklist** zu öffnen oder zu bearbeiten. Ein Popup-Fenster mit einer Liste von IP-Adressen wird angezeigt.



Arbeiten mit einer blockierten oder Blacklist-IP-Adresse

Wenn eine bestimmte IP-Adresse durch den Sicherheitsinformations-Feed blockiert oder blockiert wird, können Sie eine der folgenden Optionen in Betracht ziehen, um sie zuzulassen.

Option 1: Whitelists zu Sicherheitsinformationen

Sie können eine Whitelist für eine IP-Adresse erstellen, die von Security Intelligence auf Blacklists gesetzt wird. Eine Whitelist überschreibt seine Blacklist. Das FireSIGHT-System evaluiert Datenverkehr mit einer Whitelist-IP-Adresse oder Ziel-IP-Adresse unter Verwendung von Zugriffskontrollregeln, selbst wenn eine IP-Adresse ebenfalls in Blacklists gesetzt ist. Aus diesem Grund können Sie eine Whitelist verwenden, wenn eine Blacklist noch nützlich ist, aber zu weit gefasst ist und Datenverkehr, den Sie überprüfen möchten, falsch blockiert.

Wenn z. B. ein seriöser Feed den Zugriff auf eine wichtige Ressource nicht korrekt blockiert, aber für Ihr Unternehmen insgesamt nützlich ist, können Sie die falsch klassifizierten IP-Adressen nur Whitelist anlegen, anstatt den gesamten Feed aus der Blacklist zu entfernen.

> **Vorsicht**: Nachdem Sie Änderungen an einer Zugriffskontrollrichtlinie vorgenommen haben, müssen Sie die Richtlinie erneut auf die verwalteten Geräte anwenden.

Option 2: Durchsetzen von Security Intelligence-Filtern nach Sicherheitszone

Um eine größere Detailgenauigkeit zu erreichen, können Sie die Sicherheitsintelligenzfilterung basierend darauf erzwingen, ob sich die Quell- oder Ziel-IP-Adresse einer Verbindung in einer bestimmten Sicherheitszone befindet.

Um das obige Whitelist-Beispiel zu erweitern, können Sie die falsch klassifizierten IP-Adressen Whitelist-Listen erstellen, das Whitelist-Objekt jedoch mithilfe einer Sicherheitszone einschränken, die von Personen in Ihrer Organisation verwendet wird, die auf diese IP-Adressen zugreifen müssen. Auf diese Weise können nur diejenigen mit Geschäftsanforderungen auf die Whitelist-IP-Adressen zugreifen. Als weiteres Beispiel könnten Sie einen Spam-Feed eines Drittanbieters verwenden, um Datenverkehr auf Blacklists in einer Sicherheitszone für einen E-Mail-Server zu leiten.

Option 3: Überwachen statt Blacklist

Wenn Sie nicht sicher sind, ob Sie eine bestimmte IP-Adresse oder einen Adresssatz Blacklist erstellen möchten, können Sie eine "Monitor-only"-Einstellung verwenden, mit der das System die passende Verbindung zu Zugriffskontrollregeln übergeben kann, aber auch die Übereinstimmung mit der Blacklist protokolliert. Beachten Sie, dass Sie die globale Blacklist nicht auf "Überwachen" festlegen können.

Denken Sie an ein Szenario, in dem Sie einen Drittanbieter-Feed testen möchten, bevor Sie die Blockierung mithilfe dieses Feeds implementieren. Wenn Sie den Feed auf Monitor-only einstellen, ermöglicht das System, dass Verbindungen, die vom System blockiert worden wären, weiter analysiert werden, aber auch einen Datensatz jeder dieser Verbindungen für Ihre Bewertung protokolliert.

Schritte zur Konfiguration der Sicherheitsintelligenz mit der Einstellung "nur überwachen":

1. Klicken Sie auf der Registerkarte **Sicherheitsinformationen** einer Zugriffskontrollrichtlinie auf das Protokollierungssymbol. Das Dialogfeld Blacklist-Optionen wird angezeigt.
2. Aktivieren Sie das Kontrollkästchen **Log Connections (Protokollverbindungen)**, um Ereignisse zu Beginn der Verbindung zu protokollieren, wenn der Datenverkehr die Sicherheitsrichtlinienerfordernisse erfüllt.
3. Geben Sie an, wohin Verbindungsereignisse gesendet werden sollen.
4. Klicken Sie auf **OK**, um die Protokollierungsoptionen festzulegen. Die Registerkarte "Sicherheitsintelligenz" wird erneut angezeigt.
5. Klicken Sie auf **Speichern**. Sie müssen die Zugriffskontrollrichtlinie anwenden, damit Ihre Änderungen wirksam werden.

Option 4: Cisco Technical Assistance Center kontaktieren

Sie können sich jederzeit an das Cisco Technical Assistance Center wenden, wenn:

- Sie haben Fragen zu den oben genannten Optionen 1, 2 oder 3.
- Sie benötigen weitere Untersuchungen und Analysen zu einer IP-Adresse, die von Security Intelligence auf Blacklists gesetzt wird.
- Sie benötigen eine Erklärung, warum die IP-Adresse von Security Intelligence als Blacklist aufgeführt wird.