IP-adres is geblokkeerd of geblokkeerd door de Security Intelligence van Cisco FireSIGHT System

Inhoud

Inleiding

Met de Security Intelligence-functie kunt u het verkeer instellen dat uw netwerk kan verplaatsen op basis van het IP-adres van de bron of bestemming. Dit is vooral handig als u een zwarte lijst wilt maken van - of het verkeer naar en van - specifieke IP - adressen wilt ontkennen, voordat het verkeer wordt onderworpen aan analyse door toegangscontroleregels. Deze documenten beschrijft hoe u scenario's kunt omgaan wanneer een IP-adres geblokkeerd of op de zwarte lijst staat van een Cisco FireSIGHT System.

Voorwaarden

Vereisten

Cisco raadt u aan kennis te hebben over Cisco FireSIGHT Management Center.

Gebruikte componenten

De informatie in dit document is gebaseerd op deze hardware- en softwareversies:

- Cisco FireSIGHT Management Center
- Cisco FirePOWER-applicatie

- Cisco ASA met FirePOWER-module (SFR)
- Software, versie 5.2 of hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Verschil tussen inlichtingendiensten en inlichtingenlijsten

Er zijn twee manieren om de Security Intelligence-functie te gebruiken in een FireSIGHT-systeem:

Security Intelligence-feed

Een Security Intelligence-feed is een dynamische verzameling IP-adressen die door het Defense Center worden gedownload vanaf een HTTP- of HTTPS-server. Om u te helpen zwarte lijsten te bouwen, verstrekt Cisco de *Dienst van de Veiligheid*, die IP adressen vertegenwoordigt die door het Team van het Onderzoek van de Kwetsbaarheid (VRT) worden bepaald om een slechte reputatie te hebben.

Security Intelligence List

Een Security Intelligence lijst, contrasteerd met een feed, is een eenvoudige statische lijst van IP-adressen die u handmatig naar het FireSIGHT Management Center uploadt.

Legitiem IP-adres is geblokkeerd of geblokkeerd

Controleer of een IP-adres in het Security Intelligence-veld zit

Als een IP-adres wordt geblokkeerd door de zwarte lijst van de Security Intelligence Feed, kunt u de onderstaande stappen volgen om dit te controleren:

Stap 1: Toegang tot de CLI van het FirePOWER-apparaat of de servicemodule.

Stap 2: Start de volgende opdracht. Vervang **<**IP_Address**>** met het IP-adres dat u wilt zoeken:

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

Als u bijvoorbeeld naar IP-adres 198.51.100.1 wilt zoeken, voert u de volgende opdracht uit:

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

Als deze opdracht een overeenkomst retourneert naar het opgegeven IP-adres, duidt dit erop dat het IP-adres aanwezig is in de zwarte lijst met veiligheidsinformatie.

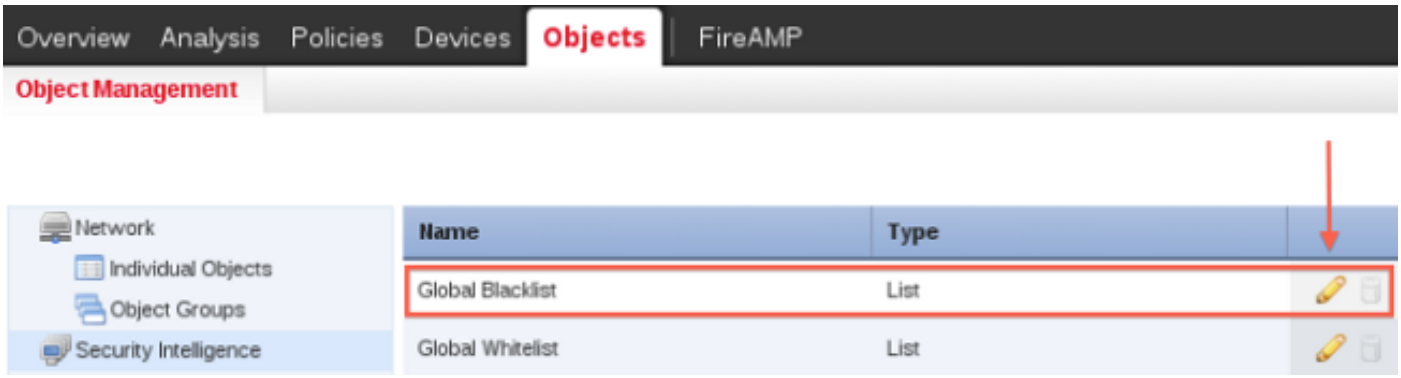
Controleer de Blacklist

Om een lijst van de IP-adressen te vinden die in de lijst kunnen worden opgenomen, volgt u de onderstaande stappen:

Stap 1: Toegang tot de webinterface van FireSIGHT Management Center.

Stap 2: Navigeer naar **objecten > Objectbeheer > Security Intelligence**.

Stap 3: Klik op het pictogram *potlood* om de **Global Blacklist** te openen of te bewerken. Er verschijnt een pop-upvenster met een lijst met IP-adressen.



Werken met een geblokkeerd of geblokkeerd IP-adres

Als een bepaald IP-adres is geblokkeerd of geblokkeerd door Security Intelligence Feed, kunt u een van de volgende opties overwegen om het toe te staan.

Optie 1: Security Intelligence Whitelists

U kunt een IP-adres bellen dat op de zwarte lijst staat van Security Intelligence. Een blanke staat boven zijn zwarte lijst. Het FireSIGHT-systeem evalueert het verkeer met een gefloten bron- of doeladres aan de hand van toegangscontroleregels, ook al is een IP-adres ook op de zwarte lijst geplaatst. Daarom kan je een whitelist gebruiken als een zwarte lijst nog handig is, maar te breed in omvang is en het verkeer dat je wilt inspecteren onjuist blokkeert.

Als een reputatieschade bijvoorbeeld ten onrechte de toegang tot een belangrijke hulpbron blokkeert maar in het algemeen nuttig is voor uw organisatie, kunt u de onjuist geclassificeerde IP adressen alleen lokaliseren, in plaats van het gehele feed-bestand van de zwarte lijst te verwijderen.

> **Voorzichtig:** Nadat u een verandering in een beleid van de Toegangscontrole aanbrengt, moet u het beleid op de beheerde apparaten opnieuw toepassen.

Optie 2: Security Intelligence Filter door security zone uitvoeren

Voor toegevoegde granulariteit, kunt u Beveiliging filteren op basis van of het bron- of doeladres in een verbinding in een bepaalde veiligheidszone ligt.

Om het bovenstaande blancovoorbeeld uit te breiden, kunt u de onjuist geclassificeerde IP-

adressen lokaliseren, maar dan het witte object beperken door gebruik te maken van een beveiligingszone die wordt gebruikt door degenen in uw organisatie die toegang moeten hebben tot die IP-adressen. Op die manier hebben alleen bedrijven die een zakelijke behoefte hebben toegang tot de gefloten IP-adressen. Als een ander voorbeeld, zou je een spamfeed van derden kunnen gebruiken om verkeer op een beveiligingszone van een e-mailserver te chanteren.

Optie 3: Monitor in plaats van Blacklist

Als u niet zeker weet of u een bepaald IP-adres of een reeks adressen wilt chanteren, kunt u een instelling "alleen-monitor" gebruiken, waarmee het systeem de corresponderende verbinding kan doorgeven aan toegangscontroleregels, maar ook de match aan de zwarte lijst logt. Merk op dat u de mondiale zwarte lijst niet kunt instellen voor alleen monitor

Neem een scenario in waarin u een derdenvoer wilt testen voordat u blokkering met dat voer uitvoert. Wanneer u de voeding alleen op de monitor instelt, kan het systeem toestaan dat verbindingen die geblokkeerd zouden zijn, verder door het systeem worden geanalyseerd, maar ook een register bijhouden van elk van deze verbindingen voor uw evaluatie.

Stappen om de Security Intelligence te configureren met de instelling "alleen monitor":

1. Klik op het tabblad **Security Intelligence** in een toegangsbeheerbeleid op het pictogram voor vastlegging. Het dialoogvenster zwarte lijst met opties verschijnt.
2. Selecteer het aanvinkvakje **Log Connections** om gebeurtenissen aan het begin van een verbinding te loggen wanneer het verkeer voldoet aan de voorwaarden van de Security Intelligence.
3. Specificeer waar u verbindingsgebeurtenissen wilt verzenden.
4. Klik op **OK** om de logopties in te stellen. Het tabblad Security Intelligence verschijnt opnieuw.
5. Klik op **Opslaan**. U moet het toegangscontrolebeleid toepassen om uw wijzigingen in werking te laten treden.

Optie 4: Contact opnemen met Cisco Technical Assistance Center

U kunt altijd contact opnemen met Cisco Technical Assistance Center, als:

- U hebt vragen met de bovenstaande opties 1, 2 of 3.
- U wilt verder onderzoek en analyse op een IP-adres dat door Security Intelligence op de zwarte lijst staat.
- U wilt uitleggen waarom het IP-adres is geblokkeerd door Security Intelligence.