

Problemen oplossen en URL-rubriek in CSF verifiëren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Verwante producten](#)

[Achtergrondinformatie](#)

[architectuur](#)

[Stap 1: Zoek de URL-categorie op in FMC](#)

[Stap 2: Instellingen voor integratie van URL-filtering bekijken](#)

[Stap 3: Bevestig de URL-categorie op het apparaat met behulp van System Support Trace](#)

[Stap 4: Los het rubrieknummer op in een rubrieknaam](#)

[Verifiëren](#)

[Knop Geschil](#)

[Problemen oplossen](#)

Inleiding

In dit document wordt beschreven hoe u URL-categorietoewijzingen op Secure Firewall en FMC kunt verifiëren om ervoor te zorgen dat het apparaat dezelfde URL-classificatie gebruikt.

Voorwaarden

U moet de URL-filterlicentie voor het apparaat hebben ingeschakeld, de integratie van Cloud Services in een gezonde staat en een toegangsbeheerbeleid dat URL-filtering omvat en is geïmplementeerd nadat de URL-voorwaarde is geconfigureerd.

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower Management Center (FMC) URL-filtering en opzoeken van rubrieken
- Verkeersinspectie en beleidsevaluatie van Cisco Secure Firewall (CSF)
- URL-categorisatie en reputatiegedrag, gebaseerd op Talos beginnend met CSF versie 6.5

Gebruikte componenten

Dit document beschrijft de functionaliteit die beschikbaar is in Cisco Secure Firewall en FMC versie 6.5 en hoger. De voorbeelden in deze handleiding gebruiken versie 7.6.5.

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 zorgen dat u de potentiële impact van elke opdracht begrijpt.

Verwante producten

Dit document kan ook worden gebruikt met deze producten en versies:

- Secure Firewall Management Center (FMC)
- Cisco Secure Firewall (CSF)
- URL-filtering en integratie van cloudservices

Achtergrondinformatie

URL-filtering is gebaseerd op een categoriedatabase die wordt geëvalueerd tijdens verkeersinspectie. De FMC slaat de URL-categoriegegevens op voor een bestemming en het apparaat voert een runtime lookup uit wanneer het verkeer wordt geïnspecteerd. Wanneer er een mismatch is tussen de FMC, het apparaat of de clouddatabase, kunnen beleidsresultaten inconsistent lijken, zelfs wanneer het toegangscontrolebeleid correct is geconfigureerd.

Een belangrijk onderdeel van de verificatie is de bevestiging dat de toewijzing van de URL-categorie consistent is voor de FMC en het apparaat. Het opzoeken van de URL-categorie wordt beïnvloed door de integratieinstellingen van Cloud Services en de apparaatcache. Als de instelling voor het vernieuwen van de cache is uitgeschakeld of de levensduur van de invoer te lang is, kunnen oude categoriegegevens in gebruik blijven nadat Talos de classificatie heeft bijgewerkt.

architectuur

Wanneer URL-filtering is ingeschakeld, controleert het apparaat eerst de lokale URL-cache. Als de categorie nog niet in de cache aanwezig is, kan het apparaat de lokale database of de Cisco Cloud bevragen. Het apparaat gebruikt zijn lokale URL-database en opzoekcache tijdens inspectie en communiceert met Talos om URL-filtergegevens te downloaden en bij te werken. Op apparaten die door de FMC worden beheerd, draait de bekerschijf op de FMC en bevindt deze zich in een wachttoestand op de CSF. Als de CSF lokaal wordt beheerd, wordt het proces op het apparaat zelf uitgevoerd.

Talos verstuurt volledige databasepakketten in meerdere formaten, die worden opgeslagen onder `/var/sf/cloud_download/cisco`.

Hier zijn enkele voorbeelden van hoe de databasebestanden van Talos eruit kunnen zien:

- `cisco_uridb_large_1541554243` (500 MB)
- `cisco_uridb_medium_1541553645` (125 MB)
- `cisco_uridb_small_1541553061` (33 MB)



Opmerking: de databasebestanden beginnen met `cisco_uridb` en vervolgens wordt de grootte vermeld (klein, middelgroot of groot). De grootte kan variëren afhankelijk van de gebruikte hardware.

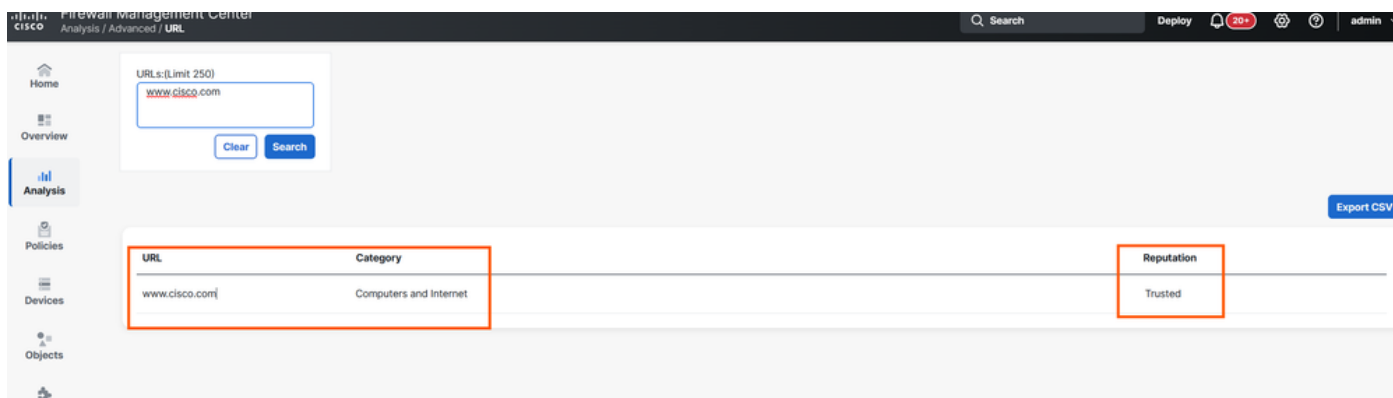
Stap 1: Zoek de URL-categorie op in FMC

De FMC onderhoudt een lokale URL-database die URL-bestemmingen toewijst aan hun toegewezen categorieën. Dit is de aanbevolen eerste stap bij het valideren van hoe een URL wordt geclassificeerd.

Navigeer naar de locatie-analyse > Geavanceerd > URL in de FMC.

Voer de URL in die u wilt onderzoeken en bekijk de toegewezen categorie.

In het onderstaande voorbeeld wordt www.cisco.com vermeld onder de categorie Computers en internet.



Stap 2: Instellingen voor integratie van URL-filtering bekijken

De integratie-instellingen voor URL-filtering bepalen waar de FMC en het CSF-apparaat hun URL-rubriekdatabase vandaan halen. Elk apparaat onderhoudt zijn eigen lokale database voor het opzoeken van URL's en kan de Cisco Cloud bevragen voor aanvullende of bijgewerkte URL-informatie.

Navigeer naar Integratie > Overige Integraties > Cloudservices in het FMC om deze instellingen te bekijken.

URL Filtering

Last URL Filtering Update: 2026-08-26 10:28:52 [Update Now](#)

☒ Enable Automatic Updates

URL Query Source

☐ Local Database Only

☒ Local Database and Cisco Cloud

☐ Cisco Cloud Only

Cached URLs Expire

After 2 hours

[Dispute URL categories and reputations](#)

Save

Controleer of de integratie gezond is en of de cache voor het opzoeken van de URL is geconfigureerd om te worden vernieuwd op basis van de timing van uw verwachte beleid.



Waarschuwing: De URL-opzoekcache kan eerder opgehaalde categorie- en reputatieresultaten behouden. Als het verlopen van de cache is uitgeschakeld of geconfigureerd met een lange levensduur, kan het apparaat de informatie in de cache blijven gebruiken nadat Talos de classificatie heeft bijgewerkt, waardoor het apparaatresultaat tijdelijk kan verschillen van het huidige FMC- of Talos-opzoeken.

Stap 3: Bevestig de URL-categorie op het apparaat met behulp van System Support Trace

Als u wilt controleren of het CSF-apparaat de URL op dezelfde manier categoriseert als de FMC, voert u een systeemondersteuningstrace uit vanaf de CLI van het apparaat. Dit laat zien hoe de

Snort-inspectiemachine het verkeer evalueert en welke URL-categorie wordt geretourneerd wanneer de verbinding wordt geïnspecteerd.

Voer in de FTD CLI de opdracht System Support Trace in en reageer op de interactieve prompts:

```
> system support trace

Enable firewall-engine-debug too? [n]: y
Please specify an IP protocol: tcp
Please specify a client IP address: 192.168.0.11
Please specify a client port:
Please specify a server IP address: 173.37.145.84
Please specify a server port: 443
```



Opmerking: In dit voorbeeld is 173.37.145.84 het IP-adres voor www.cisco.com. Gebruik het IP-adres van de bestemming dat overeenkomt met de URL die u onderzoekt.

Voorbeeld uitvoer:

```
192.168.0.11 41328 -> 173.37.145.84 443 6 AS=0 ID=0 GR=1-1: returned from url lookup, url_info is 90 2003
192.168.0.11 41328 -> 173.37.145.84 443 6 AS=0 ID=0 GR=1-1 URL lookup for www.cisco.com/ found rep 90, 2003
```

In deze uitvoer geeft de URL een categorie-ID van 2003 terug. In de volgende stap wordt uitgelegd hoe u die numerieke waarde kunt oplossen in de corresponderende rubrieknaam.

Stap 4: Los het rubrieknummer op in een rubrieknaam

URL categorie opzoeken op het apparaat geeft een numerieke categorie ID terug. Als u dat nummer wilt toewijzen aan een voor mensen leesbare rubrieknaam, opent u het bestand `aup_categories.json` op het apparaat.

Navigeer naar de `/var/sf/cloud_download/directory` op de CSF in de expert modus. Zorg ervoor dat u zich in de root user mode bevindt.

Open het categoriedefinitiebestand:

```
root@firepower:/var/sf/cloud_download# less aup_categories.json
```

Zoek naar de categorie-ID die wordt geretourneerd in de uitvoer voor het overtrekken. Voorbeeld voor categorie 2003:

```
{
  "id": 2003,
  "uuid": "abba9b63-bb10-4729-b901-2e2aa0f02003",
  "mnemonic": "comp",
  "name": "Computers and Internet",
  "type": "aup_cats",
  "state": "active"
}
```



Opmerking: de categorie-ID-nummers zijn consistent voor alle CSF-apparaten. Op elk CSF-apparaat wordt met dezelfde numerieke ID dezelfde rubrieksnaam toegewezen.

Verifiëren

Gebruik de uitvoer van de stappen 1 tot en met 4 om te bevestigen dat de toewijzing van de URL-categorie consistent is tussen de FMC-database en de Snort-engine op het apparaat.

In dit voorbeeld:

- De FMC-database vermeldt www.cisco.com als computers en internet.
- Het apparaat CLI geeft categorie ID 2003, die toewijst aan computers en internet.

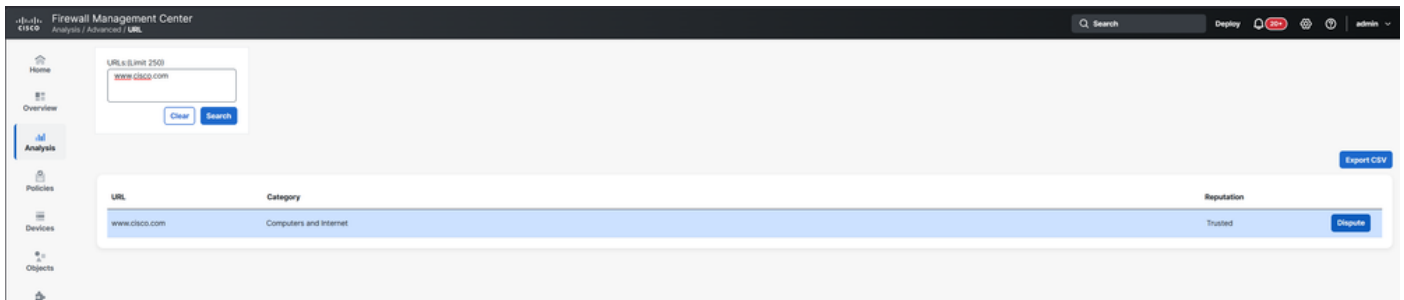
Beide bronnen zijn het hiermee eens, wat bevestigt dat het toegepaste URL-filterbeleid consistent is voor deze URL.

Knop Geschil

Als u van mening bent dat een URL is geclassificeerd in een onjuiste categorie, kunt u een geschil indienen bij Talos.

Navigeer naar Analyse > Geavanceerd > URL in de FMC:

Typ de URL in, klik op Zoeken, beweeg vervolgens over het URL-item en selecteer Geschil.



Dit opent de Talos-geschillenpagina, zodat de classificatie kan worden beoordeeld en gecorrigeerd door de juiste bron.

Problemen oplossen

Als de classificatie niet aan de verwachtingen voldoet, bekijk dan deze gebieden:

- Bevestig dat de URL Filtering-licentie is ingeschakeld en aan het apparaat is toegewezen.
- Controleer de gezondheid van Cloud Services en de verbinding met Talos.
- Controleer de instellingen voor de cache en de cache om te controleren of oude items niet opnieuw worden gebruikt.
- Controleer of het bekerproces wordt uitgevoerd op de FMC voor apparaten die door de FMC worden beheerd.

Voer voor apparaten die door de FMC worden beheerd deze opdracht uit in de FMC-expertmodus om te bevestigen dat het proces actief is:

```
pmtool status | grep beakerd
```



Opmerking: als u deze opdracht uitvoert in een beveiligde firewall die wordt beheerd door FMC, kan het proces in een wachtstand worden weergegeven. Als de Secure Firewall lokaal wordt beheerd, wordt het proces in een actieve staat weergegeven.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.