

Fehlerbehebung und Überprüfung der URL-Kategorie im CSF

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Verwandte Produkte](#)

[Hintergrundinformationen](#)

[Architektur](#)

[Schritt 1: URL-Kategorie in FMC nachschlagen](#)

[Phase 2: Überprüfen der URL-Filterungsintegrationseinstellungen](#)

[Schritt 3: Bestätigen Sie die URL-Kategorie auf dem Gerät mithilfe der Ablaufverfolgung des Systemsupports.](#)

[Schritt 4: Kategorienummer in Kategorienamen auflösen](#)

[Überprüfung](#)

[Schaltfläche "Dispute"](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die URL-Kategoriezuweisungen in Secure Firewall und FMC überprüfen, um sicherzustellen, dass das Gerät dieselbe URL-Klassifizierung verwendet.

Voraussetzungen

Sie müssen die URL-Filterungslizenz für das Gerät aktivieren, die Cloud-Services-Integration muss fehlerfrei erfolgen können, und Sie müssen über eine Zugriffskontrollrichtlinie mit URL-Filterung verfügen, die nach der Konfiguration der URL-Bedingung bereitgestellt wurde.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- URL-Filterung und Kategoriesuche im FirePOWER Management Center (FMC)
- Cisco Secure Firewall (CSF)-Datenverkehrsprüfung und Richtlinienauswertung
- URL-Kategorisierung und Reputationsverhalten, basierend auf Talos ab CSF Version 6.5

Verwendete Komponenten

In diesem Dokument werden die Funktionen der Cisco Secure Firewall und der FMC-Versionen 6.5 und höher beschrieben. Bei den Beispielen in diesem Leitfaden wird Version 7.6.5 verwendet.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Verwandte Produkte

Dieses Dokument kann auch mit folgenden Produkten und Versionen verwendet werden:

- Secure Firewall Management Center (FMC)
- Cisco Secure Firewall (CSF)
- URL-Filterung und Integration von Cloud-Services

Hintergrundinformationen

Die URL-Filterung basiert auf einer Kategoriedatenbank, die während der Datenverkehrsanalyse ausgewertet wird. Das FMC speichert die URL-Kategorieinformationen für ein Ziel, und das Gerät führt bei der Prüfung des Datenverkehrs eine Laufzeitsuche durch. Bei einer Diskrepanz zwischen dem FMC, dem Gerät oder der Cloud-Datenbank können die Richtlinienenergebnisse selbst dann inkonsistent erscheinen, wenn die Zugriffskontrollrichtlinie richtig konfiguriert ist.

Ein wichtiger Teil der Verifizierung ist die Bestätigung, dass die URL-Kategoriezuweisung für das FMC und das Gerät konsistent ist. Die URL-Kategoriensuche wird durch die Cloud Services-Integrationseinstellungen und den Geräte-Cache beeinflusst. Wenn die Cacheaktualisierungseinstellung deaktiviert ist oder die Lebensdauer des Eintrags zu lang ist, können veraltete Kategoriedaten verwendet werden, nachdem Talos die Klassifizierung aktualisiert hat.

Architektur

Wenn die URL-Filterung aktiviert ist, überprüft das Gerät zuerst den lokalen URL-Cache. Wenn die Kategorie nicht bereits im Cache vorhanden ist, kann das Gerät die lokale Datenbank oder die Cisco Cloud abfragen. Das Gerät verwendet während der Überprüfung seine lokale URL-Datenbank und seinen Suchcache, und beakerd kommuniziert mit Talos, um URL-Filterungsdaten herunterzuladen und zu aktualisieren. Auf FMC-verwalteten Geräten wird Beakerd auf dem FMC ausgeführt und befindet sich im Wartezustand auf dem CSF. Wenn der CSF lokal verwaltet wird, wird der Prozess auf dem Gerät selbst ausgeführt.

Talos sendet vollständige Datenbankpakete in verschiedenen Größen, die unter `/var/sf/cloud_download/cisco` gespeichert sind.

Hier einige Beispiele, wie die Datenbankdateien von Talos aussehen können:

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



Anmerkung: Die Datenbankdateien beginnen mit `cisco_uridb`, dann wird die Größe aufgelistet (klein, mittel oder groß). Die Größe kann je nach verwendeter Hardware variieren.

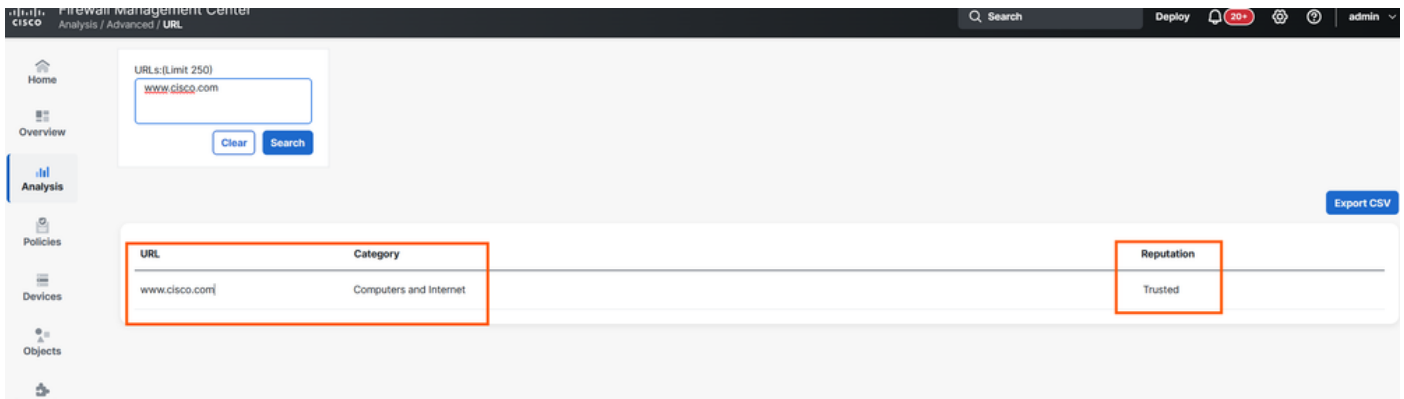
Schritt 1: URL-Kategorie in FMC nachschlagen

Das FMC unterhält eine lokale URL-Datenbank, die URL-Ziele den ihnen zugewiesenen Kategorien zuordnet. Dies ist der empfohlene erste Schritt, wenn überprüft werden soll, wie eine URL klassifiziert wird.

Navigieren Sie zum Speicherort Analyse > Erweitert > URL im FMC.

Geben Sie die URL ein, die Sie untersuchen möchten, und überprüfen Sie die zugewiesene Kategorie.

Im unten gezeigten Beispiel ist www.cisco.com unter der Kategorie Computer und Internet aufgeführt.



Phase 2: Überprüfen der URL-Filterungsintegrationseinstellungen

Die Integrationseinstellungen für die URL-Filterung legen fest, woher das FMC und das CSF-Gerät die URL-Kategoriedatenbank beziehen. Jedes Gerät unterhält eine eigene lokale Datenbank für die URL-Suche und kann in der Cisco Cloud weitere oder aktualisierte URL-Informationen abfragen.

Navigieren Sie zu **Integration > Other Integrations > Cloud Services** im FMC, um diese Einstellungen zu überprüfen.

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

Überprüfen Sie, ob die Integration fehlerfrei ist und ob der URL-Suchcache so konfiguriert ist, dass er entsprechend dem erwarteten Zeitrahmen aktualisiert wird.



Vorsicht: Im URL-Suchcache können zuvor abgerufene Kategorie- und Reputationsergebnisse gespeichert werden. Wenn der Cache-Ablauf deaktiviert oder mit einer langen Lebensdauer konfiguriert ist, kann das Gerät die zwischengespeicherten Informationen weiter verwenden, nachdem Talos die Klassifizierung aktualisiert hat. Dies kann dazu führen, dass sich das Geräteergebnis vorübergehend von der aktuellen FMC- oder Talos-Suche unterscheidet.

Schritt 3: Bestätigen Sie die URL-Kategorie auf dem Gerät mithilfe der Ablaufverfolgung des Systemsupports.

Um zu überprüfen, ob das CSF-Gerät die URL auf die gleiche Weise kategorisiert wie das FMC,

führen Sie eine Systemsupport-Ablaufverfolgung über die CLI des Geräts aus. Dies zeigt, wie die Snort-Prüfungs-Engine den Datenverkehr auswertet und welche URL-Kategorie bei der Prüfung der Verbindung zurückgegeben wird.

Geben Sie in der FTD-CLI den Befehl `system support trace` ein, und antworten Sie auf die interaktiven Aufforderungen:

```
> 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
```



Anmerkung: In diesem Beispiel ist 173.37.145.84 die IP-Adresse für www.cisco.com.
Verwenden Sie die Ziel-IP-Adresse, die der URL entspricht, die Sie untersuchen.

Beispiel:

```
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 20
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,
```

In dieser Ausgabe gibt die URL die Kategorie-ID 2003 zurück. Im nächsten Schritt wird erläutert, wie Sie diesen numerischen Wert in den entsprechenden Kategorienamen auflösen.

Schritt 4: Kategorienummer in Kategorienamen auflösen

Die URL-Kategoriensuche auf dem Gerät gibt eine numerische Kategorie-ID zurück. Um diese Nummer einem für Menschen lesbaren Kategorienamen zuzuordnen, öffnen Sie die Datei `aup_categories.json` auf dem Gerät.

Navigieren Sie zum Verzeichnis `/var/sf/cloud_download/` auf dem CSF im Expert-Modus. Stellen Sie sicher, dass Sie sich im Root-Benutzermodus befinden.

Öffnen Sie die Datei mit den Kategoriedefinitionen:

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

Suchen Sie nach der Kategorie-ID, die in der Ablaufverfolgungsausgabe zurückgegeben wird.
Beispieleintrag für Kategorie 2003:

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



Anmerkung: Kategorie-ID-Nummern sind für alle CSF-Geräte gleich. Dieselbe numerische ID wird auf jedem CSF-Gerät demselben Kategorienamen zugeordnet.

Überprüfung

Verwenden Sie die Ausgabe der Schritte 1 bis 4, um sicherzustellen, dass die URL-Kategoriezuweisung zwischen der FMC-Datenbank und der Snort-Engine auf dem Gerät konsistent ist.

In diesem Beispiel:

- Die FMC-Datenbank listet www.cisco.com als Computer und Internet auf.
- Die CLI des Geräts gibt die Kategorie ID 2003 zurück, die Computer und Internet zugeordnet ist.

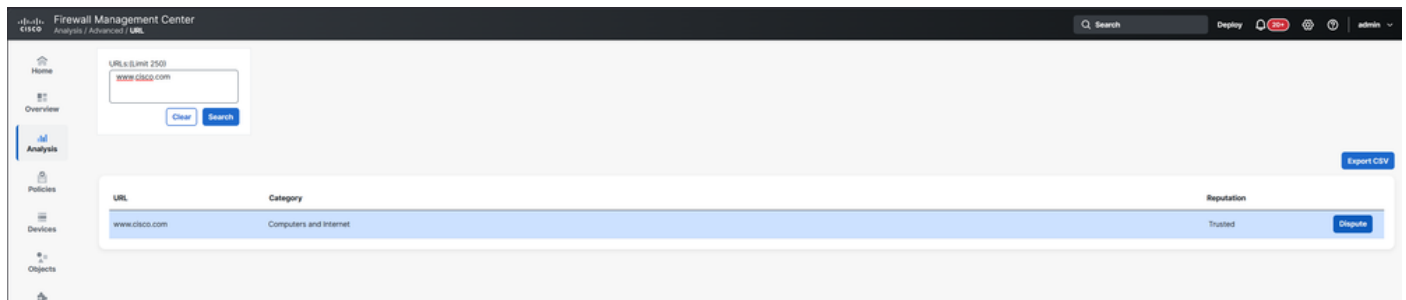
Beide Quellen stimmen überein, was bestätigt, dass die angewendete URL-Filterungsrichtlinie für diese URL konsistent ist.

Schaltfläche "Dispute"

Wenn Sie glauben, dass eine URL in eine falsche Kategorie eingeordnet wurde, können Sie eine Anfechtung bei Talos einreichen.

Navigieren Sie zu Analyse > Erweitert > URL im FMC:

Geben Sie die URL ein, klicken Sie auf Suchen, bewegen Sie den Mauszeiger über den URL-Eintrag, und wählen Sie Dispute (Anfechten).



Dadurch wird die Seite über die Anfechtung von Talos geöffnet, sodass die Klassifizierung von der entsprechenden Quelle überprüft und korrigiert werden kann.

Fehlerbehebung

Wenn die Klassifizierung nicht den Erwartungen entspricht, überprüfen Sie folgende Bereiche:

- Bestätigen Sie, dass die URL-Filterungslizenz aktiviert und dem Gerät zugewiesen ist.
- Überprüfen Sie die Integrität der Cloud-Services und die Verbindung zu Talos.
- Überprüfen Sie den Gerätecache und die Einstellungen für die Cacheaktualisierung, um sicherzustellen, dass veraltete Einträge nicht wiederverwendet werden.
- Überprüfen Sie, ob der Beakerd-Prozess auf dem FMC für FMC-verwaltete Geräte ausgeführt wird.

Bei FMC-verwalteten Geräten führen Sie diesen Befehl im FMC-Expertenmodus aus, um zu bestätigen, dass der Prozess aktiv ist:

```
pmtool status | grep beakerd
```



Anmerkung: Wenn Sie diesen Befehl in einer sicheren Firewall ausführen, die von FMC verwaltet wird, kann der Vorgang im Wartezustand angezeigt werden. Wenn die sichere

Firewall lokal verwaltet wird, befindet sich der Prozess im Ausführungszustand.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.