

Risoluzione dei problemi e verifica della categoria dell'URL in CSF

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Prodotti correlati](#)

[Premesse](#)

[Architettura](#)

[Passaggio 1: Ricerca della categoria URL in FMC](#)

[Passaggio 2: Verifica impostazioni di integrazione filtro URL](#)

[Passaggio 3: Confermare la categoria dell'URL sul dispositivo utilizzando la traccia di supporto del sistema](#)

[Passaggio 4: Risolvi il numero di categoria in un nome di categoria](#)

[Verifica](#)

[Pulsante Controversia](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come verificare le assegnazioni delle categorie URL su Secure Firewall e FMC per verificare che il dispositivo utilizzi la stessa classificazione URL.

Prerequisiti

È necessario che la licenza del filtro URL sia abilitata per il dispositivo, che l'integrazione dei servizi cloud sia in uno stato integro e che i criteri di controllo dell'accesso includano il filtro URL e che siano stati distribuiti dopo la configurazione della condizione URL.

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Filtraggio URL e ricerche di categorie in Firepower Management Center (FMC)
- Ispezione del traffico e valutazione delle policy Cisco Secure Firewall (CSF)
- Classificazione degli URL e comportamento della reputazione, basati su Talos a partire dalla versione 6.5 di CSF

Componenti usati

In questo documento vengono descritte le funzionalità disponibili in Cisco Secure Firewall e FMC versione 6.5 e successive. Gli esempi di questa guida utilizzano la versione 7.6.5.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Prodotti correlati

Questo documento può essere utilizzato anche con questi prodotti e versioni:

- Centro gestione firewall protetto (FMC)
- Cisco Secure Firewall (CSF)
- Filtro URL e integrazioni di servizi cloud

Premesse

Il filtro URL si basa su un database delle categorie valutato durante l'ispezione del traffico. Il FMC memorizza le informazioni sulla categoria dell'URL di una destinazione e il dispositivo esegue una ricerca in fase di esecuzione quando il traffico viene ispezionato. In caso di mancata corrispondenza tra il FMC, il dispositivo o il database cloud, i risultati dei criteri possono apparire incoerenti anche quando i criteri di controllo dell'accesso sono configurati correttamente.

Una parte importante della verifica è costituita dalla verifica della coerenza dell'assegnazione della categoria dell'URL al FMC e al dispositivo. La ricerca della categoria URL è influenzata dalle impostazioni di integrazione dei servizi cloud e dalla cache dei dispositivi. Se l'impostazione di aggiornamento della cache è disattivata o la durata della voce è troppo lunga, i dati di categoria non aggiornati possono rimanere in uso dopo l'aggiornamento della classificazione da parte di Talos.

Architettura

Quando il filtro URL è abilitato, il dispositivo controlla prima la cache degli URL locali. Se la categoria non è già presente nella cache, il dispositivo può eseguire una query sul database locale o su Cisco Cloud. Il dispositivo usa il database locale degli URL e la cache di ricerca durante l'ispezione e beakerd comunica con Talos per scaricare e aggiornare i dati del filtro URL. Sui dispositivi gestiti da FMC, beakerd viene eseguito sul FMC e si trova in stato di attesa sul CSF. Se il file CSF è gestito localmente, il processo viene eseguito sul dispositivo stesso.

Talos invia pacchetti di database completi in più dimensioni, memorizzati in `/var/sf/cloud_download/cisco`.

Di seguito sono riportati alcuni esempi di un possibile aspetto dei file di database Talos:

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



Nota: I file del database iniziano con `cisco_uridb`, quindi vengono elencate le dimensioni (piccola, media o grande). Le dimensioni possono variare a seconda dell'hardware in uso.

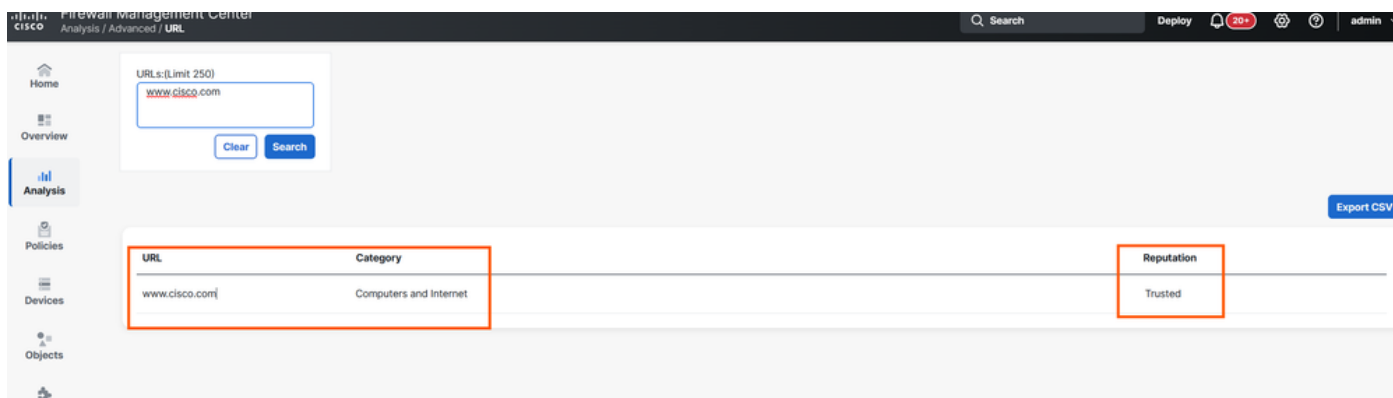
Passaggio 1: Ricerca della categoria URL in FMC

FMC gestisce un database locale degli URL che mappa le destinazioni degli URL alle categorie assegnate. Questo è il primo passaggio consigliato per la convalida della modalità di classificazione di un URL.

Passare alla posizione Analisi > Avanzate > URL in FMC.

Immettere l'URL che si desidera analizzare ed esaminare la categoria assegnata.

Nell'esempio riportato di seguito, www.cisco.com è elencato nella categoria Computer e Internet.



Passaggio 2: Verifica impostazioni di integrazione filtro URL

Le impostazioni di integrazione del filtro URL determinano l'origine del database delle categorie URL del FMC e del dispositivo CSF. Ogni dispositivo gestisce il proprio database locale per la ricerca degli URL e può eseguire query sul Cisco Cloud per ottenere informazioni aggiuntive o aggiornate sugli URL.

Passare a Integrazione > Altre integrazioni > Servizi cloud in FMC per esaminare queste impostazioni.

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

Verificare che l'integrazione sia integra e che la cache di ricerca URL sia configurata per l'aggiornamento in base ai tempi previsti per i criteri.



Attenzione: La cache di ricerca URL può conservare i risultati relativi alla categoria e alla reputazione recuperati in precedenza. Se la scadenza della cache è disabilitata o configurata con una durata prolungata, il dispositivo può continuare a utilizzare le informazioni memorizzate nella cache dopo l'aggiornamento della classificazione da parte di Talos, il che può causare differenze temporanee tra il risultato del dispositivo e la ricerca corrente di FMC o Talos.

Passaggio 3: Confermare la categoria dell'URL sul dispositivo utilizzando la traccia di supporto del sistema

Per verificare che il dispositivo CSF classifichi l'URL allo stesso modo del FMC, eseguire una

traccia di supporto del sistema dalla CLI del dispositivo. Questo comando mostra come il motore di ispezione Snort valuta il traffico e quale categoria URL viene restituita quando si controlla la connessione.

Dalla CLI di FTD, immettere il comando `system support trace` e rispondere ai prompt interattivi:

```
> 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
```



Nota: Nell'esempio, 173.37.145.84 è l'indirizzo IP di www.cisco.com. Utilizzare l'indirizzo IP di destinazione corrispondente all'URL su cui si sta eseguendo l'analisi.

Output di esempio:

```
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 questo output, l'URL restituisce un ID categoria di 2003. Nel passaggio successivo viene illustrato come risolvere il valore numerico nel nome della categoria corrispondente.

Passaggio 4: Risolvi il numero di categoria in un nome di categoria

La ricerca di categorie URL nel dispositivo restituisce un ID categoria numerico. Per mappare tale numero a un nome di categoria leggibile, aprire il file `aup_categories.json` sul dispositivo.

Passare alla directory `/var/sf/cloud_download/` sul CSF in modalità Expert. Assicurarsi di essere in modalità utente root.

Aprire il file delle definizioni delle categorie:

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

Cerca l'ID categoria restituito nell'output di traccia. Voce di esempio per la categoria 2003:

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



Nota: I numeri ID delle categorie sono coerenti su tutti i dispositivi CSF. Lo stesso ID numerico viene mappato allo stesso nome di categoria su ogni dispositivo CSF.

Verifica

Utilizzare l'output dei passaggi da 1 a 4 per verificare che l'assegnazione della categoria dell'URL sia coerente tra il database FMC e il motore Snort del dispositivo.

In questo esempio:

- Nel database di FMC www.cisco.com è indicato come Computer e Internet.
- La CLI del dispositivo restituisce l'ID categoria 2003, che viene mappato a Computer e Internet.

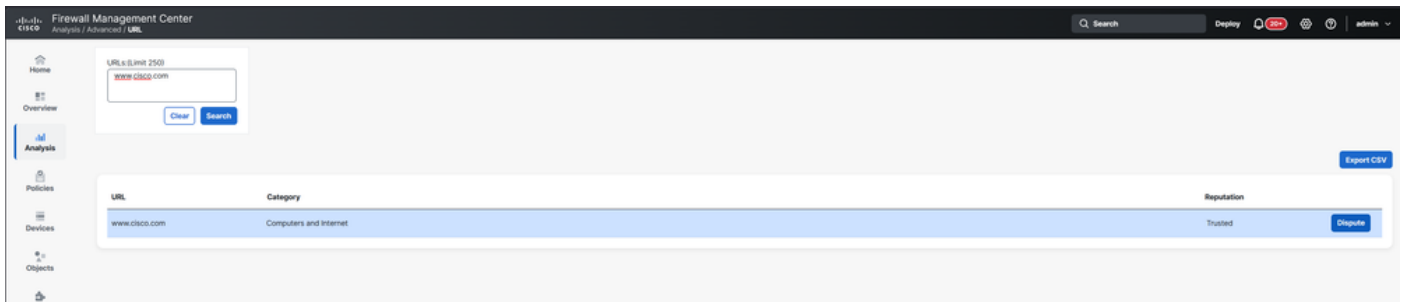
Le due origini sono concordi. Ciò conferma che i criteri di filtro URL applicati sono coerenti per questo URL.

Pulsante Controversia

Se ritieni che un URL sia stato classificato in una categoria errata, puoi inviare una controversia a Talos.

Passare ad Analisi > Avanzate > URL in FMC:

Digitare l'URL, fare clic su Cerca, passare il mouse sulla voce URL e selezionare Controversia.



In questo modo viene aperta la pagina Controversia Talos in modo che la classificazione possa essere rivista e corretta dalla fonte appropriata.

Risoluzione dei problemi

Se la classificazione non corrisponde alle aspettative, esaminare le aree seguenti:

- Confermare che la licenza del filtro URL sia abilitata e assegnata al dispositivo.
- Verificare lo stato dei servizi cloud e la connessione a Talos.
- Esaminare le impostazioni di aggiornamento della cache e della cache del dispositivo per verificare che le voci non aggiornate non vengano riutilizzate.
- Verificare se il processo di interruzione è in esecuzione nel FMC per i dispositivi gestiti da FMC.

Per i dispositivi gestiti da FMC, eseguire questo comando in modalità esperto di FMC per verificare che il processo sia attivo:

```
pmtool status | grep beakerd
```



Nota: Se si esegue questo comando in un firewall protetto gestito da FMC, il processo può essere visualizzato in stato di attesa. Se il firewall protetto è gestito localmente, il processo è in esecuzione.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).