Risoluzione dei problemi relativi al filtro URL su un sistema FireSIGHT

Sommario

[Introduzione](#)
[Processo di ricerca del filtro URL](#)
[Problemi di connettività del cloud](#)
[Passaggio 1: Controllo delle licenze](#)
[La licenza è installata?](#)
[La licenza è scaduta?](#)
[Passaggio 2: Verifica avvisi di stato](#)
[Passaggio 3: Verifica impostazioni DNS](#)
[Passaggio 4: Verifica della connettività alle porte richieste](#)
[Problemi di controllo dell'accesso e di classificazione erronea](#)
[Problema 1: L'URL con livello di reputazione non selezionato è consentito/bloccato](#)
[Azione regola consentita](#)
[L'azione regola è Blocca](#)
[Matrice di selezione URL](#)
[Problema 2: Il carattere jolly non funziona nella regola di controllo d'accesso](#)
[Problema 3: Categoria e reputazione dell'URL non popolate](#)
[Informazioni correlate](#)

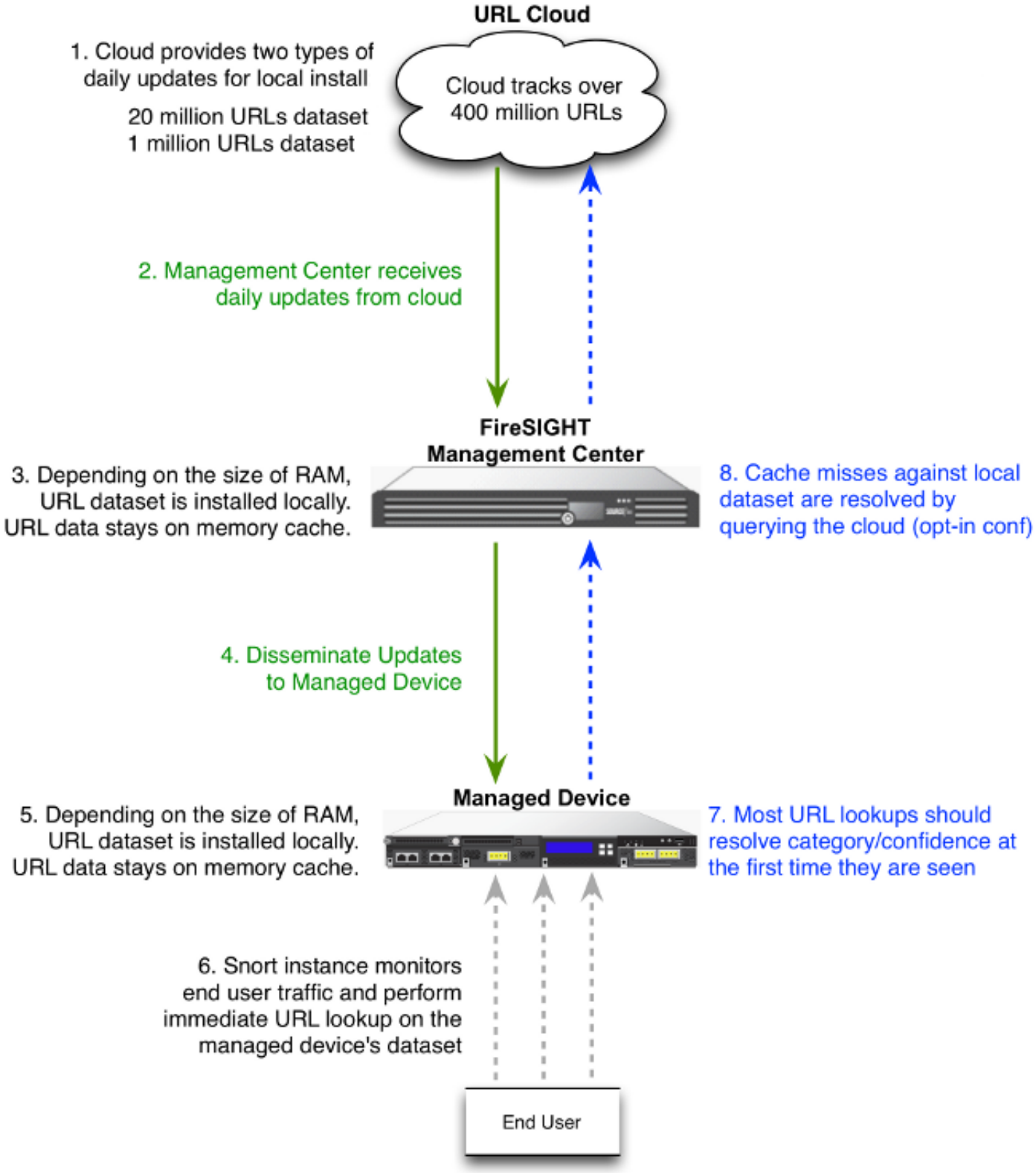
Introduzione

In questo documento vengono descritti i problemi più comuni relativi al filtro URL. La funzione di filtro URL di FireSIGHT Management Center classifica il traffico degli host monitorati e consente di scrivere una condizione in una regola di controllo dell'accesso basata sulla reputazione.

Processo di ricerca del filtro URL

Per accelerare il processo di ricerca degli URL, il filtro URL fornisce un dataset che viene installato localmente in un sistema Firepower. A seconda della quantità di memoria (RAM) disponibile su un accessorio, esistono due tipi di dataset:

Tipo di set di dati	Requisiti di memoria	
	Sulla versione 5.3	On versione 5.4 o successiva
Set di dati da 20 milioni di URL	>2 GB	>3,4 GB
Dataset da 1 milione di URL	<= 2 GB	<= 3,4 GB



Problemi di connettività del cloud

Passaggio 1: Controllo delle licenze

La licenza è installata?

Èpossibile aggiungere condizioni URL basate sulla categoria e sulla reputazione alle regole di controllo dell'accesso senza una licenza di filtro URL, tuttavia non è possibile applicare la policy di controllo dell'accesso finché non si aggiunge prima una licenza di filtro URL al centro di gestione

FireSIGHT, quindi la si abilita sui dispositivi interessati dalla policy.

La licenza è scaduta?

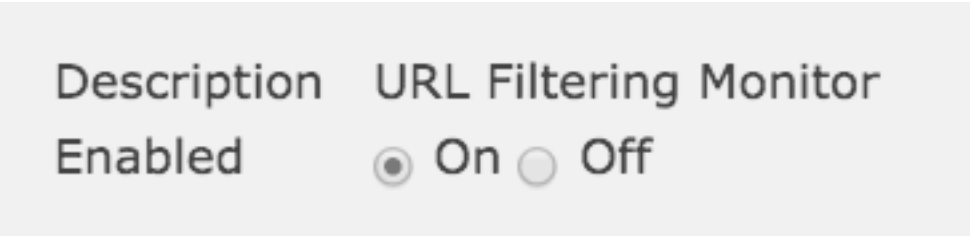
Se una licenza del filtro URL scade, le regole di controllo dell'accesso con condizioni di URL basate sulla categoria e sulla reputazione cessano di filtrare gli URL e il centro di gestione FireSIGHT non contatta più il servizio cloud.

> **Suggerimento**: Per informazioni su come abilitare la funzionalità di filtro URL su un sistema FireSIGHT e applicare la licenza del filtro URL su un dispositivo gestito, leggere l'esempio del filtro URL su un sistema FireSIGHT.

Passaggio 2: Verifica avvisi di stato

Il modulo URL Filtering Monitor tiene traccia delle comunicazioni tra il FireSIGHT Management Center e il cloud Cisco, in cui il sistema ottiene i dati del filtro URL (categoria e reputazione) per gli URL visitati più frequentemente. Il modulo URL Filtering Monitor tiene traccia anche delle comunicazioni tra un centro di gestione FireSIGHT e qualsiasi dispositivo gestito in cui è stato abilitato il filtro URL.

Per abilitare il modulo di monitoraggio del filtro URL, andare alla pagina **Configurazione dei criteri di integrità** e scegliere **Monitoraggio filtro URL**. Per abilitare l'uso del modulo per il test dello stato di integrità, fare clic sul pulsante di opzione **On** (Attivato) per l'opzione **Enabled** (Attivato). Per rendere effettive le impostazioni, è necessario applicare il criterio di integrità al centro di gestione FireSIGHT.



- **Avviso critico**: Se il centro di gestione FireSIGHT non riesce a comunicare con il cloud o a recuperare un aggiornamento dal cloud, la classificazione dello stato del modulo passa a *Critico*.
- **Avviso**: Se la comunicazione tra il centro di gestione FireSIGHT e il cloud ha esito positivo, lo stato del modulo cambia in *Avviso* se il centro di gestione non è in grado di inviare nuovi dati di filtro URL ai dispositivi gestiti.

Passaggio 3: Verifica impostazioni DNS

Un centro di gestione FireSIGHT comunica con questi server durante la ricerca nel cloud:

```
database.brightcloud.com
service.brightcloud.com
```

Dopo aver verificato che entrambi i server siano autorizzati sul firewall, eseguire questi comandi sul centro di gestione FireSIGHT e verificare se il centro di gestione è in grado di risolvere i nomi:

```
admin@FireSIGHT:~$ sudo nslookup database.brightcloud.com

admin@FireSIGHT:~$ sudo nslookup service.brightcloud.com
```

Passaggio 4: Verifica della connettività alle porte richieste

I sistemi FireSIGHT utilizzano le porte 443/HTTPS e 80/HTTP per comunicare con il servizio cloud.

Dopo aver verificato che il Management Center è in grado di eseguire correttamente un'operazione di nslookup, verificare la connettività alla porta 80 e alla porta 443 con telnet. Il database URL viene scaricato con database.brightcloud.com sulla porta 443, mentre le query URL sconosciute vengono eseguite su service.brightcloud.com sulla porta 80.

```
telnet database.brightcloud.com 443
telnet service.brightcloud.com 80
```

Questo output è un esempio di una connessione telnet riuscita a database.brightcloud.com.

```
Connected to database.brightcloud.com.
Escape character is '^]'.
```

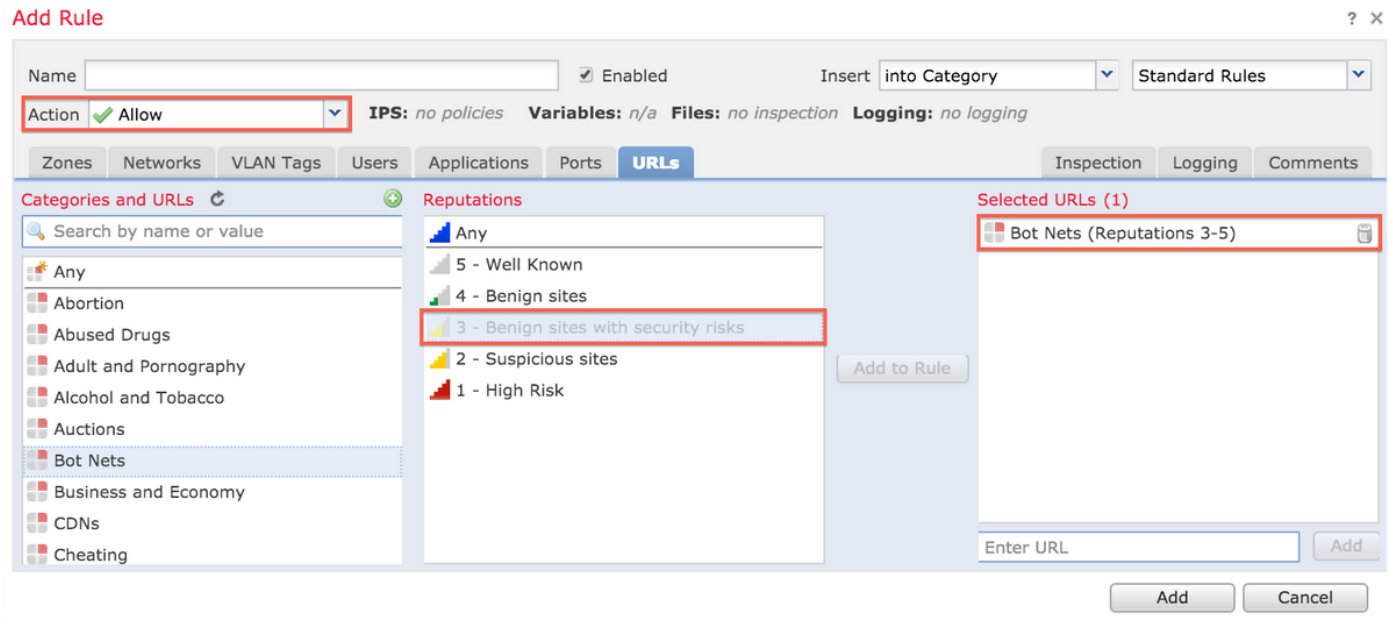
Problemi di controllo dell'accesso e di classificazione erronea

Problema 1: L'URL con livello di reputazione non selezionato è consentito/bloccato

Se si nota che un URL è consentito o bloccato, ma non è stato selezionato il livello di reputazione di tale URL nella regola di controllo dell'accesso, leggere questa sezione per informazioni sul funzionamento di una regola di filtro URL.

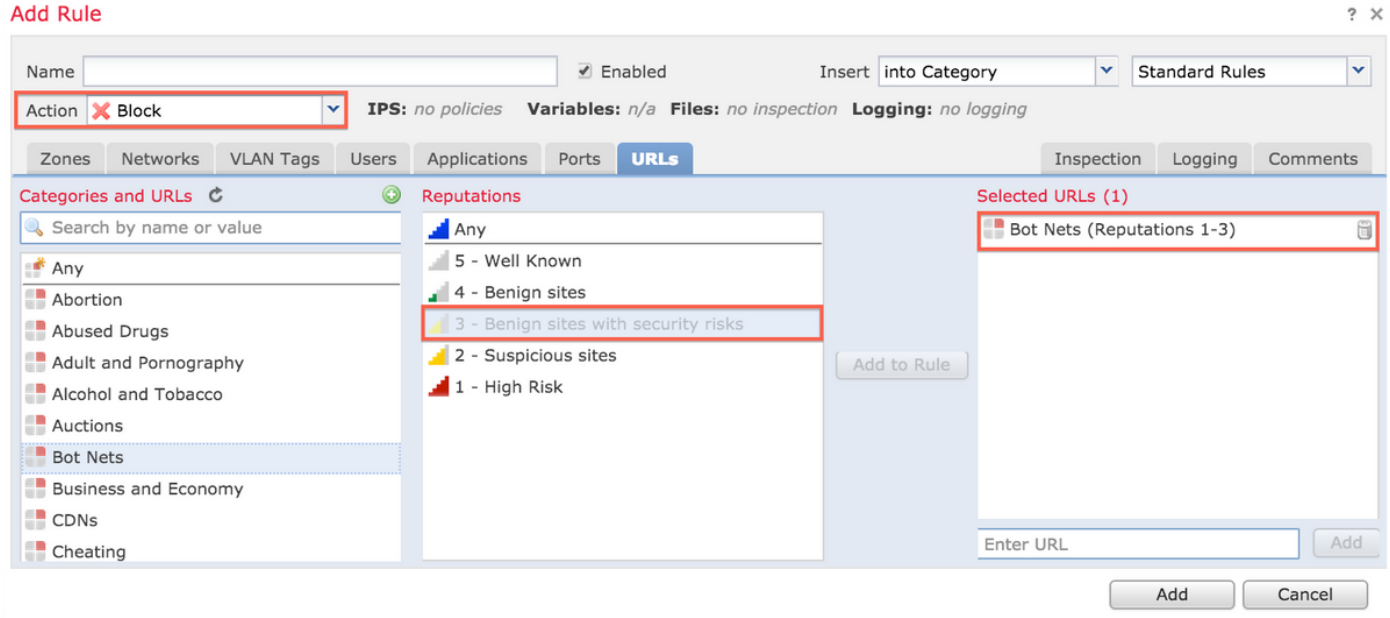
Azione regola consentita

Quando si crea una regola per **Consenti** traffico in base a un livello di reputazione, la selezione di un livello di reputazione seleziona anche tutti i livelli di reputazione meno sicuri del livello selezionato in origine. Ad esempio, se si configura una regola per consentire *siti benigni con rischi di protezione* (livello 3), verranno automaticamente consentiti anche *siti benigni* (livello 4) e siti *conosciuti* (livello 5).



L'azione regola è Blocca

Quando si crea una regola per **bloccare il** traffico in base a un livello di reputazione, la selezione di un livello di reputazione seleziona anche tutti i livelli di reputazione più gravi del livello selezionato in origine. Ad esempio, se si configura una regola per bloccare *i siti benigni con rischi di protezione* (livello 3), verranno automaticamente bloccati anche i *siti sospetti* (livello 2) e i siti *ad alto rischio* (livello 1).



Matrice di selezione URL

Livello di reputazione selezionato	Azione regola selezionata				
	Rischio elevato	**Sito sospetto**	**Sito benigno con rischi per la sicurezza**	**Sito benigno**	**Conos**
1 - Rischio elevato	Blocco, Consenti	Allow (Autorizza)	Allow (Autorizza)	Allow (Autorizza)	Allow (Autor
2 - Siti sospetti	Block (Blocca)	Blocco, Consenti	Allow (Autorizza)	Allow (Autorizza)	Allow (Autor
3 - Siti benigni con rischi per	Block	Block	Blocco, Consenti	Allow	Allow

la sicurezza	(Blocca)	(Blocca)		(Autorizza)	(Autor
4 - Siti benigni	Block (Blocca)	Block (Blocca)	Block (Blocca)	Blocco, Consenti	Allow (Autor
5 - Noto	Block (Blocca)	Block (Blocca)	Block (Blocca)	Block (Blocca)	Blocco Conse

Problema 2: Il carattere jolly non funziona nella regola di controllo d'accesso

Il sistema FireSIGHT non supporta la specifica di un carattere jolly in una condizione URL. Questa condizione potrebbe non essere soddisfatta per l'avviso su cisco.com.

```
*cisco*.com
```

Inoltre, un URL incompleto può corrispondere ad altro traffico e questo produce un risultato indesiderato. Quando si specificano singoli URL nelle condizioni dell'URL, è necessario considerare con attenzione gli altri tipi di traffico che potrebbero essere interessati. Ad esempio, si consideri uno scenario in cui si desidera bloccare in modo esplicito cisco.com. Tuttavia, la corrispondenza delle sottostringhe significa che il blocco di cisco.com blocca anche sanfrancisco.com, il che potrebbe non essere l'intenzione dell'utente.

Quando si immette un URL, immettere il nome del dominio e omettere le informazioni sul sottodominio. Ad esempio, digitare cisco.com anziché www.cisco.com. Quando si utilizza cisco.com in una regola **Allow**, gli utenti possono selezionare uno qualsiasi degli URL seguenti:

```
http://cisco.com
http://cisco.com/newcisco
http://www.cisco.com
```

Problema 3: Categoria e reputazione dell'URL non popolate

Se un URL non si trova in un database locale ed è la prima volta che viene visualizzato nel traffico, è possibile che una categoria o la reputazione non vengano popolate. Ciò significa che la prima volta che viene visualizzato un URL sconosciuto, questo non corrisponde alla regola AC. A volte, la prima volta che un URL viene visualizzato, la ricerca di URL visitati frequentemente potrebbe non riuscire. Questo problema è risolto nelle versioni 5.3.0.3, 5.3.1.2 e 5.4.0.2, 5.4.1.1.

Informazioni correlate

- Configurazione del filtro URL su un sistema FireSIGHT
- Documentazione e supporto tecnico – Cisco Systems