Probleemoplossing met URL-filtering op een FireSIGHT-systeem

Inhoud

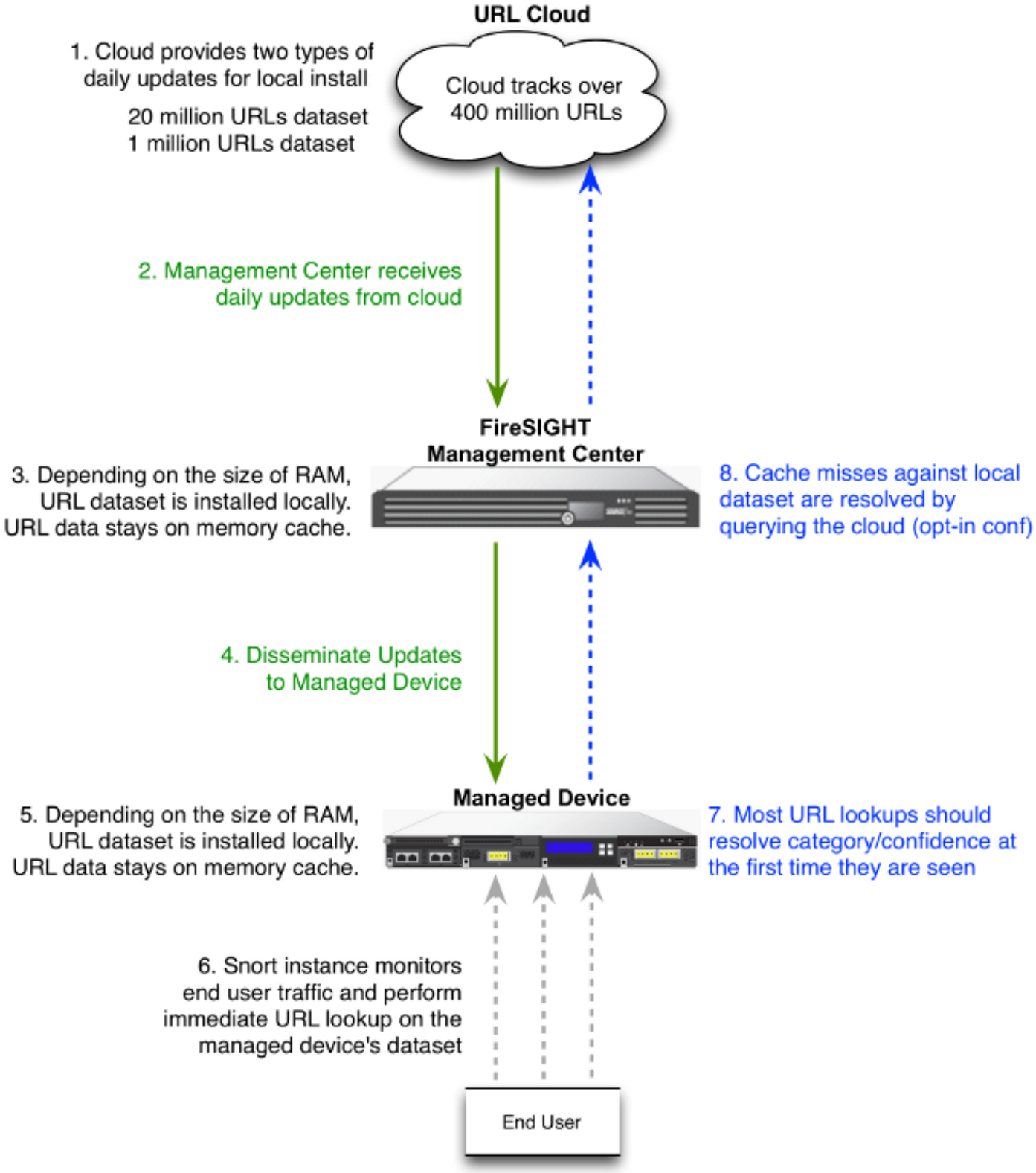
Inleiding

Dit document beschrijft veel voorkomende problemen met URL-filtering. De URL-filterfunctie in FireSIGHT Management Center categoriseert het verkeer van gemonitorde hosts en stelt u in staat een voorwaarde te schrijven in een toegangscontroleregel die op reputatie is gebaseerd.

URL-filterproces

Om het URL-lookup-proces te versnellen, biedt het URL-filtering een dataset die lokaal op een Firepower System is geïnstalleerd. Afhankelijk van de hoeveelheid geheugen (RAM) die op een apparaat beschikbaar is, zijn er twee gegevenssets:

Type dataset	Geheugenvereiste	
	Over versie 5.3	Over versie 5.4 of hoger
20 miljoen URL Dataset	>2 GB	>3,4 GB
1 miljoen URL Dataset	<= 2 GB	<= 3,4 GB



Cloudconnectiviteitsproblemen

Stap 1: Controleer de licenties

Is de licentie geïnstalleerd?

U kunt op klasse en reputatie gebaseerde URL voorwaarden aan toegangscontroleregels toevoegen zonder een URL Filtering licentie, maar u kunt het toegangscontrolbeleid niet toepassen totdat u eerst een URL Filtering licentie aan het FireSIGHT Management Center

toevoegt en het vervolgens inschakelen op de apparaten die door het beleid worden bedoeld.

Is de licentie verlopen?

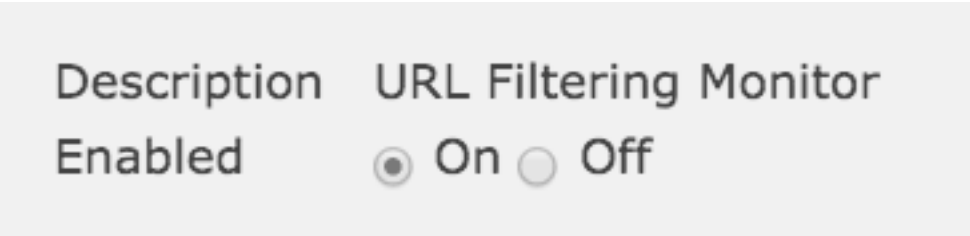
Als een URL-filtering verlopen is, maken toegangscontroleregels met categorie- en reputatiegebaseerde URL-voorwaarden een einde aan het filteren van URL's en neemt het FireSIGHT Management Center niet langer contact op met de cloudservice.

> **Tip**: Lees URL-filtering op een FireSIGHT System Configuration om te leren hoe u URL Filtering-functie op een FireSIGHT System kunt inschakelen en gebruik URL-filtering op een beheerd apparaat.

Stap 2: Waarschuwingen controleren

De URL Filtering van de monitor module van de monitor volgt communicatie tussen het FireSIGHT Management Center en de Cisco cloud, waar het systeem zijn URL-filtering (categorie en reputatie) gegevens voor algemeen bezochte URL's verkrijgt. De URL Filtering van de monitor module van de monitor volgt ook communicatie tussen een FireSIGHT Management Center en om het even welke beheerde apparaten waar u URL filtering hebt ingeschakeld.

Kies de **URL-filtermonitor** om de module voor URL-filtering van monitor in te schakelen op de pagina **Health Policy Configuration**. Klik op de radioknop **Aan** voor de **Ingeschakelde** optie om gebruik van de module voor het testen van de gezondheidsstatus mogelijk te maken. U moet het gezondheidsbeleid op het FireSIGHT Management Center toepassen als u wilt dat uw instellingen effect sorteren.



- **Kritische waarschuwing**: Als het FireSIGHT Management Center er niet in slaagt met de cloud te communiceren of een update uit de cloud te herstellen verandert de status classificatie voor die module in *Criticaal*.
- **Waarschuwing**: Als het FireSIGHT Management Center met succes met de cloud communiceert, verandert de modulestatus in *Waarschuwing* als het Management Center geen nieuwe URL-filtergegevens naar de beheerde apparaten kan duwen.

Stap 3: DNS-instellingen controleren

Een FireSIGHT Management Center communiceert met deze servers tijdens de cloud:

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

Nadat u ervoor hebt gezorgd dat beide servers zijn toegestaan in de firewall, voert u deze opdrachten uit op het FireSIGHT Management Center en controleert u of het Management Center de namen kan oplossen:

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

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

Stap 4: Controleer de Connectiviteit met de vereiste poorten

FireSIGHT Systems gebruikt poorten 443/HTTPS en 80/HTTP om met de cloudservice te communiceren.

Zodra u hebt bevestigd dat het Management Center in staat is om een succesvolle nslookup uit te voeren, controleert u de connectiviteit met poort 80 en poort 443 met telnet. De URL-database wordt gedownload met database.heldercloud.com in poort 443, terwijl de onbekende URL-vragen worden gedaan op service.heldercloud.com in poort 80.

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

Deze output is een voorbeeld van een succesvolle telnet verbinding met database.heldercloud.com.

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

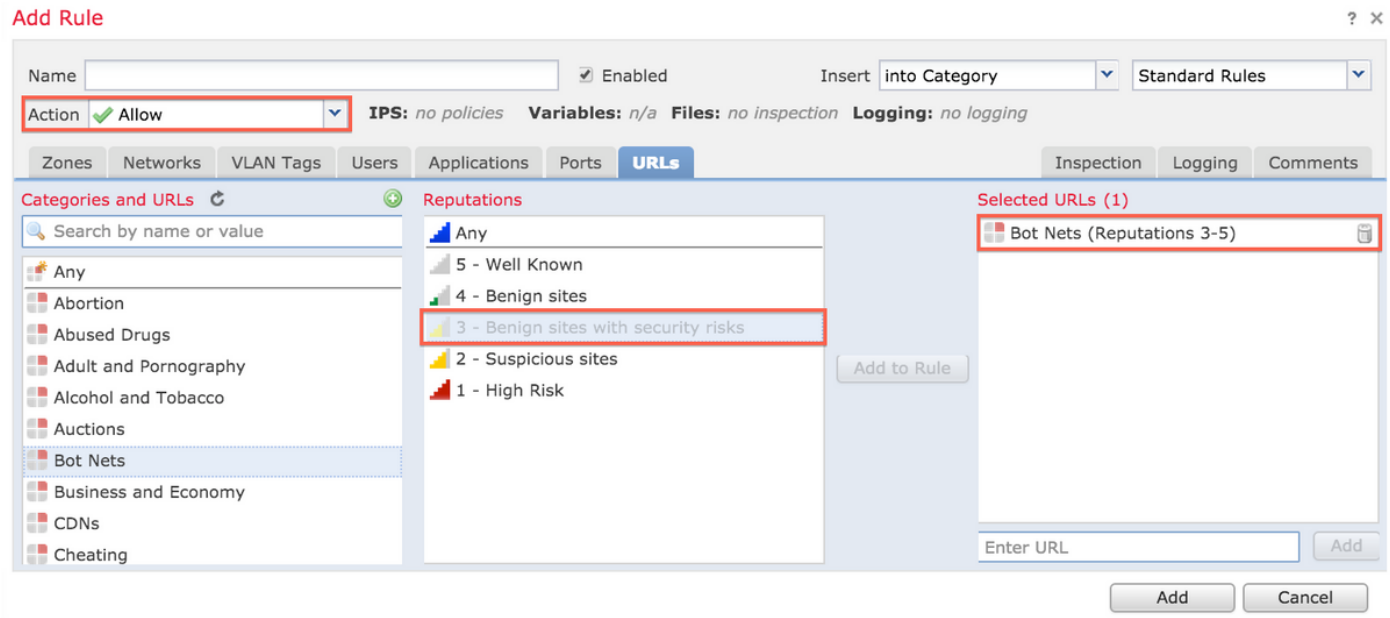
Problemen met toegangscontrole en verkeerde categorisering

Probleem 1: URL met niet-geselecteerd herstellingsniveau is toegestaan / geblokkeerd

Als u opmerkt dat een URL is toegestaan of geblokkeerd, maar u hebt het reputatieniveau van die URL in uw Regel van de Toegangscontrole niet geselecteerd, lees deze sectie om te begrijpen hoe een URL filterregel werkt.

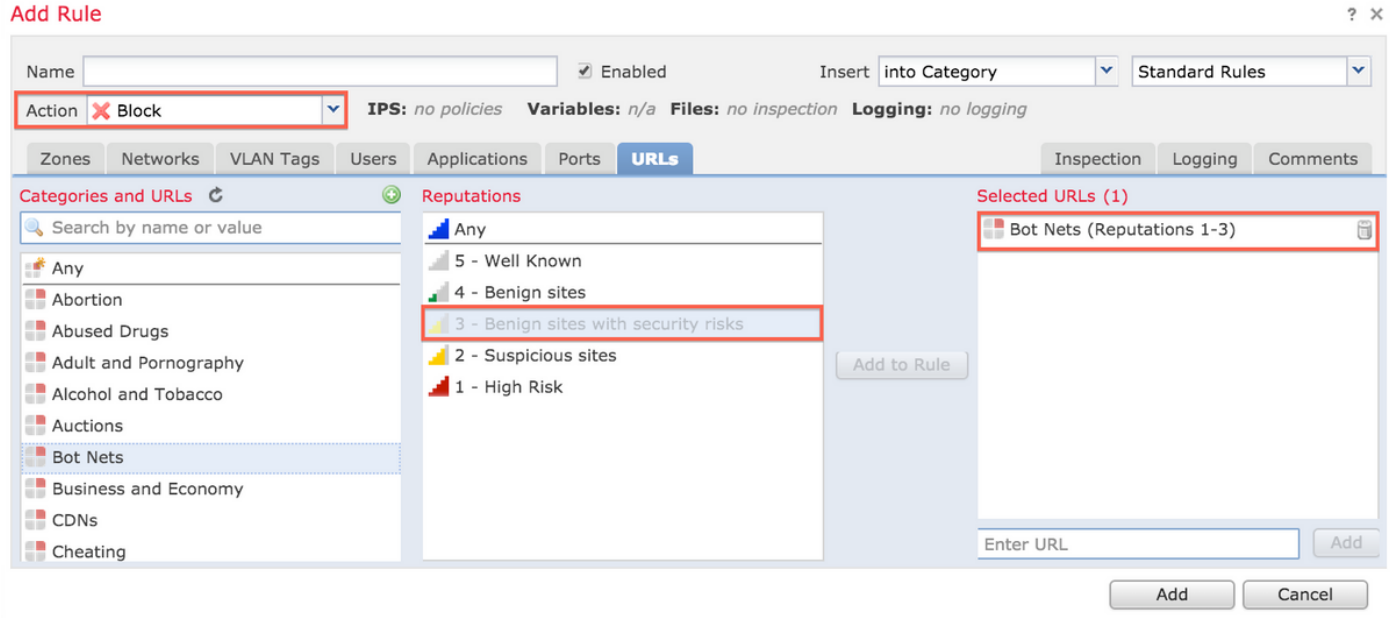
Handeling op regel staat toe

Wanneer u een regel maakt om verkeer **toe te staan** op basis van een reputatieniveau, selecteert de selectie van een reputatieniveau ook alle reputatieniveaus die minder veilig zijn dan het niveau dat u oorspronkelijk geselecteerd had. Bijvoorbeeld, als u een regel vormt om *Benigne plaatsen met veiligheidsrisico's* toe te staan (niveau 3), dan staat het ook automatisch *Benigne plaatsen* (niveau 4) en *Goed gekende* (niveau 5) toe.



Handeling op regels is blokkeren

Wanneer u een regel maakt om verkeer **te blokkeren** op basis van een reputatieniveau, selecteert de selectie van een reputatieniveau ook alle reputatieniveaus ernstiger dan het niveau dat u oorspronkelijk geselecteerd hebt. Bijvoorbeeld, als u een regel vormt om *BenigNE plekken met veiligheidsrisico's* te blokkeren (niveau 3), blokkeert deze ook automatisch *Verdachte sites* (niveau 2) en *Hoge risico* (niveau 1).



URL-selectietype

Geselecteerd reproductieniveau	Handeling geselecteerd regel				
	Hoog risico	**verdachte plaats**	**Benigne plaats met veiligheidsrisico**	**Benign Site**	**beken**
1 - Hoog risico	Blokken, toestaan	Allow (toestaan)	Allow (toestaan)	Allow (toestaan)	Allow (toesta
2 - Verdachte locaties	Block (blokkeren)	Blokken, toestaan	Allow (toestaan)	Allow (toestaan)	Allow (toesta
3 - Benigde locaties met een	Block	Block	Blokken, toestaan	Allow	Allow

beveiligingsrisico	(blokkeren)	(blokkeren)		(toestaan)	(toesta
4 - Benigde locaties	Block (blokkeren)	Block (blokkeren)	Block (blokkeren)	Blokken, toestaan	Allow (toesta
5 - Goed bekend	Block (blokkeren)	Block (blokkeren)	Block (blokkeren)	Block (blokkeren)	Blokke toesta

Probleem 2: Wildcard werkt niet onder de toegangscontroleregel

FireSIGHT System ondersteunt geen specificatie van een jokerteken in een URL-toestand. Deze conditie kan niet alert zijn op cisco.com.

```
*cisco*.com
```

Daarnaast kan een onvolledige URL overeenkomen met ander verkeer dat een onnodig resultaat veroorzaakt. Wanneer u individuele URLs in URL voorwaarden specificeert, moet u zorgvuldig ander verkeer overwegen dat zou kunnen worden beïnvloed. Neem bijvoorbeeld een scenario in overweging waar u cisco.com expliciet wilt blokkeren. Substring matching betekent echter dat het blokkeren van cisco.com ook sanfrancisco.com blokkeert, wat misschien niet uw bedoeling is.

Wanneer u een URL ingaat, voer de domeinnaam in en bewaar subdomein informatie. Bijvoorbeeld, type cisco.com in plaats van www.cisco.com. Wanneer u cisco.com in een **Allow** regel gebruikt, kunnen de gebruikers naar een van deze URL's bladeren:

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

Probleem 3: URL-categorie en -reputatie worden niet bevolkt

Als een URL niet in een lokale database is en het de eerste keer is dat de URL in verkeer wordt gezien, kan een categorie of reputatie niet worden ingevuld. Dit betekent dat de eerste keer dat er een onbekende URL wordt gezien, deze niet overeenkomt met de AC-regel. Soms kunnen de URL lookups voor veelbezochte URL's niet de eerste keer dat er een URL wordt gezien, worden opgelost. Dit punt is vastgesteld op versie 5.3.0.3, 5.3.1.2 en 5.4.0.2, 5.4.1.1.

Gerelateerde informatie

- Configuratie van URL-filtering op een FireSIGHT-systeem
- Technische ondersteuning en documentatie – Cisco Systems