

# Het gebruik van GREP om de toegangslogbestanden te filteren

## Inhoud

[Vraag:](#)

## Vraag:

**Milieu:** Cisco web security applicatie (WSA), alle versies van AsyncOS

Hoe kan ik de toegangsbestanden op het S-Series apparaat doorzoeken?

Vanuit de opdrachtregel interface van het Cisco web security applicatie, kunt u de **grep** opdracht gebruiken om de toegangsbestanden te filteren en bepalen wat wordt geblokkeerd. Dit is een voorbeeld van hoe alles geblokkeerd wordt:

```
—  
TestS650.wsa.com ()> grep
```

Op dit moment ingestelde logs:

1. Type "accessoires": "Toegangsloggen" ophalen: FTP-polis  
<...>
18. Type "welcomeack\_logs": "Welkom Pagina-bevestiging"  
Retrieval: FTP-polis

Voer het nummer in van het logbestand dat u wilt overschrijven.

```
[]> 1
```

Geef de reguliere expressie op om te openen.

```
[]> BLOCK_
```

Wil je dat deze zoekopdracht ongevoelig is? [Y]> n

Wil je de logs achtervolgen? [N]> n

Wilt u de uitvoer pagineren? [N]> n

(items worden weergegeven)

```
—
```

Voor de vraag naar reguliere expressies kunt u **BLOCK\_** (zonder de quotes) invoeren om elk verzoek te tonen dat WSA heeft geblokkeerd. (Waarschuwing: deze lijst kan zeer lang zijn . )

U kunt ook delen van site-URL invoeren als u lange items met betrekking tot een specifieke site

wilt weergeven. Bijvoorbeeld - het **venster** invoeren voor de reguliere expressie zal u alle items tonen die toegang hebben tot de URL van Windows Update van [windows.microsoft.com](http://windows.microsoft.com).

Om een beetje geavanceerder te worden, als u de logitems voor een site met Windows-supdate in de URL wilt weergeven, die ook geblokkeerd zijn, kunt u het **venster** reguliere expressies gebruiken **.\*BLOCK\_**.