

WSA - Häufig gestellte Fragen: Wie kann ich die Protokolle auf der Cisco WSA anzeigen?

Inhalt

[Einführung](#)

[Wie kann ich die Protokolle auf der Cisco WSA anzeigen?](#)

[CLI](#)

[Benutzeroberfläche](#)

Einführung

In diesem Dokument wird beschrieben, wie die Protokolle der Cisco Web Security Appliance (WSA) mithilfe des Befehls **grep** über die CLI angezeigt werden.

Wie kann ich die Protokolle auf der Cisco WSA anzeigen?

CLI

1. Um die Protokolle von der CLI anzuzeigen, stellen Sie mithilfe von Secure Shell (SSH) eine Verbindung zur WSA her. Dazu können Sie einen SSH-Client wie puTom verwenden.
2. Geben Sie nach der Anmeldung bei der CLI die **fett** Befehl. Daraufhin wird eine Liste der Protokolle auf der WSA angezeigt.
3. Geben Sie die Nummer des Protokollabonnements ein, um das `grep on` auszuführen, und drücken Sie die Eingabetaste.
4. Geben Sie den regulären Ausdruck für `grep` ein, oder lassen Sie ihn leer, um nach allem zu suchen, und drücken Sie die Eingabetaste.
5. Geben Sie Y oder N für die verbleibenden Aufforderungen ein, um die Ausführung des `grep` zu ändern.

Im Folgenden finden Sie ein Beispiel dafür, wie Sie einen `grep` ausführen, um eine bestimmte Domäne in den Accesslogs zu finden:

```
wsa.hostname> grep
Currently configured logs:
1. "accesslogs" Type: "Access Logs" Retrieval: FTP Poll
2. "amp_logs" Type: "AMP Engine Logs" Retrieval: FTP Poll
3. "authlogs" Type: "Authentication Framework Logs" Retrieval: FTP Poll
4. "avc_logs" Type: "AVC Engine Logs" Retrieval: FTP Poll
5. "bypasslogs" Type: "Proxy Bypass Logs" Retrieval: FTP Poll
...
42. "webcat_logs" Type: "Web Categorization Logs" Retrieval: FTP Poll
43. "webrootlogs" Type: "Webroot Logs" Retrieval: FTP Poll
44. "welcomeack_logs" Type: "Welcome Page Acknowledgement Logs" Retrieval:
    FTP Poll
```

```
Enter the number of the log you wish to grep.  
[]> 1  
Enter the regular expression to grep.  
[]> domain.com  
Do you want this search to be case insensitive? [Y]>  
Do you want to search for non-matching lines? [N]>  
Do you want to tail the logs? [N]>  
Do you want to paginate the output? [N]>
```

Benutzeroberfläche

1. Um die Protokolle über die Benutzeroberfläche anzuzeigen, stellen Sie eine Verbindung zur WSA über einen Webbrowser an Port 8080 (Standard) für HTTP oder 8443 (Standard) für HTTPS her.
2. Klicken Sie nach der Anmeldung auf **Systemverwaltung > Protokollabonnements**.
3. Klicken Sie auf den FTP-Link, um das Protokoll-Abonnement anzuzeigen.
4. Wählen Sie die anzuzeigende Protokolldatei aus, und die Ausgabe wird im Browser angezeigt.

Hinweis: Standardmäßig verwendet die WSA bei der Verbindung mit der Verwaltungsschnittstelle Port 21 für FTP. Wenn dieser Port geändert wird, schlägt das Klicken auf den FTP-Link in der GUI fehl. Um dieses Problem zu beheben, fügen Sie den FTP-Port für die Verwaltungsschnittstelle nach dem WSA-Hostnamen in der URL im Browser hinzu.