Filtern von Zugriffsprotokollen mithilfe von GREP

Inhalt

Frage:

Umgebung: Cisco Web Security Appliance (WSA), alle Versionen von AsyncOS

Wie kann ich die Zugriffsprotokolle auf der Appliance der S-Serie durchsuchen?

Über die Befehlszeilenschnittstelle der Cisco Web Security Appliance können Sie den Befehl **grep** verwenden, um die Zugriffsprotokolle zu filtern und festzustellen, was blockiert wird. Hier ein Beispiel, das alle blockierten Elemente zeigt:

—
TestS650.wsa.com ()> **grep**

Derzeit konfigurierte Protokolle:
1. "Accesslogs" Typ: "Zugriffsprotokolle" abrufen: FTP-Umfrage
<..>
18. "welcomeack_logs" Typ: "Protokolle für die Bestätigung der Willkommensseite"
Abrufen: FTP-Umfrage

Geben Sie die Nummer des Protokolls ein, das Sie grep erstellen möchten.
[]> **1**

Geben Sie den regulären Ausdruck in grep ein.
[]> **BLOCK_**

Soll diese Suche ohne Berücksichtigung der Groß- und Kleinschreibung durchgeführt werden?
[Y]> **n**

Möchten Sie die Protokolle abschalten? [N]> **n**

Möchten Sie die Ausgabe paginieren? [N]> **n**

(Einträge werden angezeigt)
—

Bei der Frage des regulären Ausdrucks können Sie **BLOCK_** (ohne die Anführungszeichen) eingeben, um jede von der WSA blockierte Anforderung anzuzeigen. (Warnung: Diese Liste kann sehr lang sein).

Sie können auch Teile der Site-URL eingeben, wenn Sie Zugriffslangeinträge für eine bestimmte

Site anzeigen möchten. Beispielsweise zeigt das Eingeben von **windowsupdate** für den regulären Ausdruck alle Zugriffsprotokolleinträge an, die die Windows Update-URL windowsupdate.microsoft.com enthalten.

Wenn Sie die Zugriffsprotokolleinträge für eine Site mit WindowSupdate in der URL anzeigen möchten, die ebenfalls blockiert wurden, können Sie das **Fenster** für reguläre Ausdrücke verwenden **.*BLOCK_**.