Warum erhalte ich beim Durchlaufen des Proxys den Fehler "Bad Request (Request Header Too Long)" (Ungültige Anforderung (Header zu lange anfordern))?

Frage:

Warum erhalte ich beim Durchlaufen der Cisco Web Security Appliance (WSA) den Fehler "Bad Request (Request Header Too Long)" (Ungültige Anfrage (Header zu lang))?

Umgebung:

Cisco Web Security Appliance (WSA) jeder AsyncOS-Version

Der Fehler "Bad Request (Request Header Too Long)" wird angezeigt, wenn der HTTP-Anforderungsheader die auf dem Zielserver festgelegte Headergrößenbeschränkung überschreitet.

Normale HTTP-Anfragen erreichen dieses Limit nicht. In bestimmten Fällen, z. B. beim Zielserver, der eine Authentifizierung erfordert, kann der HTTP-Anforderungs-Header jedoch wachsen und sich dem auf dem Zielserver festgelegten Grenzwert nähern. Wenn der HTTP-Anforderungs-Header die auf dem Zielserver konfigurierte Headergröße überschreitet, sendet der Server die HTTP-Antwort "Bad Request (Request Header To Long)" (Ungültige Anforderung (Header zu lang anfordern)).

Beim Durchlaufen der WSA fügt die WSA der HTTP-Anforderung zusätzliche Header, z. B. den Header "Via", hinzu. Die von WSA hinzugefügten Header sind in der Regel optionale HTTP-Header, die HTTP-RFC entsprechen. In seltenen Fällen kann der zusätzliche Header, den der Proxy hinzufügt, dazu führen, dass die Headergrenze auf der Seite des Zielservers überschritten wird.

Der "Via"-Header kann in unserer Web Security Appliance (WSA) über die Web-GUI unter:

- "Sicherheitsdienste" > "Webproxy" > "Einstellungen bearbeiten"
- Legen Sie unter "Headers" die Option "Do not Send" (Nicht senden) für Via-Header fest.

In AsyncOS-Versionen 7.5 und höher deaktivieren wir speziell den "Request Side VIA:"-Header, der an die Zielserver gesendet wird.

In der Regel sollte die Header-Größenbeschränkung auch auf dem Webserver konfiguriert werden können.

Konfigurationsanleitung zum Ändern des Limit auf IIS-Servern:
http://support.microsoft.com/kb/955585