프록시를 통과할 때 "잘못된 요청(요청 헤더가 너무 깁니다)" 오류가 발생하는 이유는 무엇입니까?

질문:

Cisco WSA(Web Security Appliance)를 통과할 때 "Bad Request (Request Header Too Long)" 오류가 발생하는 이유는 무엇입니까?

환경:

Cisco WSA(Web Security Appliance) 모든 AsyncOS 버전

HTTP 요청 헤더가 대상 서버에 설정된 "헤더 크기 제한"을 초과하면 "Bad Request (Request Header Too Long)" 오류가 표시됩니다.

일반 HTTP 요청이 이 제한에 도달하지 않습니다.그러나 인증이 필요한 대상 서버와 같은 경우에 HTTP 요청 헤더가 증가하여 대상 서버에 설정된 제한에 도달할 수 있습니다.HTTP 요청 헤더가 대상 서버에 구성된 헤더 크기를 초과하면 서버는 "Bad Request (Request Header Too Long)" HTTP 응답을 보냅니다.

WSA를 통과할 때 WSA는 HTTP 요청에 "Via" 헤더와 같은 추가 헤더를 추가합니다.WSA에서 추가한 헤더는 일반적으로 HTTP RFC를 준수하는 선택적 HTTP 헤더입니다.드물게 프록시가 추가하는 추가 헤더로 인해 대상 서버 측에서 헤더 제한이 초과될 수 있습니다.

"Via" 헤더는 웹 GUI의 WSA(Web Security Appliance)에서 다음 아래에서 비활성화할 수 있습니다.

- "보안 서비스" > "웹 프록시" > "설정 편집"
- "Headers .."에서 Via 헤더에 대해 옵션을 "Do not Send"로 설정합니다.

AsyncOS 버전 7.5 이상에서는 특히 대상 서버로 전송되는 "Request Side VIA:" 헤더만 비활성화합니다.

일반적으로 웹 서버에서도 헤더 크기 제한을 구성할 수 있습니다.

IIS 서버의 제한 변경 구성 가이드:http://support.microsoft.com/kb/955585