클라이언트가 NEGOEXTS를 사용하는 경우 WSA를 통해 인증이 실패합니다.

목차

소개

이 문서에서는 클라이언트가 NEGOEXTS를 사용할 때 Cisco WSA(Web Security Appliance)를 통해 인증이 실패할 경우 문제를 오버코딩하는 방법에 대해 설명합니다.

배경 정보

Cisco WSA(Web Security Appliance)는 사용자를 인증하여 사용자 또는 그룹을 기반으로 정책을 적용할 수 있습니다.사용 가능한 방법 중 하나는 Kerberos입니다.ID에서 Kerberos를 인증 방법으로 사용할 경우 WSA는 헤더가 포함된 401(투명) 또는 407(명시적) HTTP 응답으로 클라이언트의 HTTP 요청에 **응답합니다. WWW-Authenticate:협상**. 이 시점에서 클라이언트는 권한 부여와 함께 새 HTTP 요청을 **전송합니다.GSS**-API(Generic Security Service Application Program Interface) 및 SPNEGO(Simple Protected Negotiation) 프로토콜을 포함하는 협상 헤더SPNEGO에서 사용자는 지원하는 mechTypes를 표시합니다.다음은 WSA에서 지원하는 매치 유형입니다.

- KRB5- Kerberos가 클라이언트에서 올바르게 지원 및 구성되어 있고 액세스 중인 서비스에 대해 유효한 Kerberos 티켓이 있는 경우 사용되는 Kerberos 인증 방법입니다.
- NTLMSSP- 유효한 Kerberos 티켓을 사용할 수 없지만 협상 인증 방법이 지원되는 경우 사용되는 Microsoft NTLM 보안 지원 공급자 방법

문제/장애:클라이언트가 NEGOEXTS를 사용하는 경우 WSA를 통해 인증 실패

최신 버전의 Microsoft Windows에서는 NegoExts라는 새 인증 방법이 지원되는데, 이는 협상 인증 프로토콜의 확장입니다.이 mechType은 NTLMSSP보다 더 안전한 것으로 간주되며, 지원되는 유일한 방법이 NEGOEXTS 및 NTLMSSP인 경우 클라이언트가 선호합니다.자세한 내용은 다음 링크를 참조하십시오.

[협상 인증 패키지에 확장 도입](#)

이 시나리오는 일반적으로 협상 인증 방법이 선택되고 KRB5 mechType이 없을 때 발생합니다(WSA 서비스에 대한 유효한 Kerberos 티켓이 없기 때문일 수 있음). 클라이언트가 NEGOEXTS(Wireshark의 NEGOEX로 볼 수 있음)를 선택한 경우 WSA는 인증 트랜잭션을 처리할 수 없으며 클라이언트에 대한 인증이 실패합니다.이 경우 인증 로그에 다음 로그가 표시됩니다.

```
14 Nov 2016 16:06:20 (GMT -0500) Warning: PROX_AUTH : 123858 : [DOMAIN]Failed to parse NTLMSSP
packet, could not extract NTLMSSP command14 Nov 2016 16:06:20 (GMT -0500) Info: PROX_AUTH :
123858 : [DOMAIN][000] 4E 45 47 4F 45 58 54 53 00 00 00 00 00 00 00 00 NEGOEXTS ........
```

인증이 실패할 경우 다음과 같이 발생합니다.

게스트 권한이 활성화된 경우 - 클라이언트가 **인증되지** 않은 상태로 분류되고 웹 사이트로 리디렉션됩니다.

게스트 권한이 비활성화된 경우 - 클라이언트는 다른 401 또는 407(프록시 방법에 따라 다름)과 함께 응답 헤더에 표시되는 나머지 인증 방법(협상이 다시 표시되지 않음)을 제공합니다. NTLMSSP 및/또는 기본 인증이 구성된 경우 인증 프롬프트가 발생할 수 있습니다.다른 인증 방법이 없는 경우(ID는 Kerberos에 대해서만 구성됨) 인증 이 실패합니다.

솔루션

이 문제의 해결 방법은 ID에서 Kerberos 인증을 제거하거나 WSA 서비스에 대한 유효한 Kerberos 티켓을 가져오도록 클라이언트를 수정하는 것입니다.