Wie richte ich NTLM mit SSO korrekt ein (Anmeldeinformationen werden transparent gesendet)?

Inhalt

Frage:

Symptome: Der Browser fordert bei Verwendung der NTLM-Authentifizierung zur Eingabe von Anmeldeinformationen auf.

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

Mehrere Faktoren können beeinflussen, ob der Client seine Anmeldeinformationen automatisch sendet (SSO - Single Sign On) oder den Endbenutzer auffordert, seine Anmeldeinformationen manuell einzugeben.
Überprüfen Sie beim Implementieren von NTLM mit SSO die folgenden Elemente:

Konfiguration der WSA-Authentifizierung:

Stellen Sie sicher, dass die WSA so eingerichtet ist, dass sie NTLMSSP und nicht nur NTLM Basic verwendet.

Diese Einstellung finden Sie auf der GUI unter **Web Security Manager > Identities** Seite. Bearbeiten Sie die entsprechende Identität, und überprüfen Sie dann die Einstellung **Member definieren durch Authentication > Authentication Schemes.**

Wählen Sie eine der folgenden Optionen aus:

NTLMSSP ermöglicht es dem Client, die Anmeldeinformationen sicher und transparent an den Webproxy zu senden.

Mit NTLM Basic kann der Client bei Aufforderung zur Eingabe der Anmeldeinformationen Benutzername und Kennwort im Klartext senden.

Der Client wählt die beste verfügbare Methode aus, wenn die Option **Use Basic (Grundlegende oder NTLMSSP** verwenden) aktiviert ist (empfohlen). Wenn der Client NTLMSSP unterstützt, wird diese Methode verwendet, und alle anderen Browser verwenden Basic. Dies ermöglicht maximale Kompatibilität.

Client-Vertrauenswürdigkeit:

Wenn der Client der WSA nicht vertraut, sendet er die Anmeldeinformationen nicht transparent. Im Folgenden sind Richtlinien aufgeführt, um bei der Fehlerbehebung in Umgebungen zu helfen, in denen der Client der WSA nicht vertraut.

Der Client vertraut der URL für die Authentifizierungsumleitung nicht (nur transparente Bereitstellungen).

Bei einer transparenten Bereitstellung muss die WSA den Client an sich selbst umleiten, um die Authentifizierung durchzuführen. Der Kunde kann diesem umgeleiteten Standort vertrauen.

Standardmäßig leitet die WSA an den FQDN des P1 (oder, wenn sie für Proxydaten verwendet wird, an die M1-Schnittstelle) um. Da es sich um einen FQDN handelt, wird dieser von Internet Explorer nicht vertrauenswürdig, da er davon ausgeht, dass es sich um eine Ressource außerhalb seines Netzwerks handelt.

Es gibt zwei Möglichkeiten, Internet Explorer als vertrauenswürdig für die WSA zu machen: