Hoe stel ik NTLM op de juiste manier in met SSO (aanmeldingsgegevens worden transparant verzonden)?

Inhoud

Vraag:

Symptomen: De browser vraagt naar referenties wanneer NTLM-verificatie wordt gebruikt.

Omgeving: Cisco Web Security Applicatie (WSA), alle versies van AsyncOS

Verschillende factoren kunnen van invloed zijn of de client automatisch zijn referenties verstuurt (SSO - Single Sign On), of vraagt de eindgebruiker om handmatig hun referenties in te voeren. Controleer de volgende items wanneer u probeert NTLM met SSO te implementeren:

Configuratie WSA-verificatie:

Controleer dat de WSA is ingesteld om NTLMSSP te gebruiken en niet alleen NTLM Basic

Deze instelling is te vinden op de GUI onder Web Security Manager > Identity page. Bewerk de juiste Identity en controleer vervolgens de optie Leden definiëren door verificatie > instelling verificatiesystemen.

Selecteer een van de volgende opties:

- NTLMSSP gebruiken
- Basic gebruiken voor NTLMSSP
- Basis gebruiken

NTLMSSP laat de functionaliteit voor de cliënt toe om de geloofsbrieven veilig en doorzichtig naar de Webvolmacht te verzenden.

NTLM Basic staat de client toe om de gebruikersnaam en het wachtwoord in onbewerkte tekst te verzenden wanneer om de referenties wordt gevraagd.

De client kiest de beste beschikbare methode wanneer de optie Basis gebruiken of NTLMSSP is geselecteerd (aanbevolen). Als de client NTLMSSP ondersteunt, wordt deze methode gebruikt en

alle andere browsers gebruiken Basic. Dit zorgt voor maximale compatibiliteit.

Clientvertrouwen:

Als de client niet vertrouwt op de WSA, zal het niet transparant verzenden. Hieronder volgen richtlijnen voor probleemoplossing in omgevingen waarin de client geen vertrouwen heeft in de WSA.

De client vertrouwt niet op de URL van de verificatieomleiding (alleen transparante implementaties)

In een transparante plaatsing, moet WSA de cliënt aan zich opnieuw richten om de authentificatie uit te voeren. De klant kan al dan niet vertrouwen op deze omgeleide locatie.

Standaard wordt de WSA omgeleid naar de FQDN van de P1 (of de M1-interface als deze wordt gebruikt voor proxygegevens). Aangezien dit een FQDN is, zal Internet Explorer het niet vertrouwen, aangezien het gelooft dit een middel buiten zijn netwerk is.

Er zijn twee manieren om Internet Explorer vertrouwen de WSA:

1. Voeg de WSA-interface FQDN toe aan de vertrouwde sites. Kies Gereedschappen > Internet-opties > Beveiliging > Vertrouwde locaties en klik op de knop Sites.
   Opmerking: deze configuratie moet op elke client worden gewijzigd.

2. Verander de omleiding URL die de WSA gebruikt om een DNS oplosbare, single-word hostname te zijn.

   Dit kan via de webinterface. Meld u als beheerder aan bij uw WSA en navigeer naar Network > Verification. Klik vervolgens op "Algemene instellingen bewerken ..." en wijzig "Transparent Verification Redirect Hostname"

   Als de WSA deze hostnaam niet kan oplossen met DNS, verschijnen er waarschuwingsberichten voor configuratiefouten. Aanbevolen wordt om DNSCONFIG > localhosts te gebruiken (Opmerking: 'localhosts' is een verborgen opdracht) en deze hostnaam toe te voegen om op te lossen aan de WSA-interface die gebruikt wordt voor proxy-gegevens.

   Als uw cliënten niet DNS deze hostname kunnen oplossen, zullen uw cliënten niet aan volmacht kunnen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.