Come configurare correttamente NTLM con SSO (credenziali inviate in modo trasparente)?

Sommario

Domanda:

Sintomi: il browser richiede le credenziali quando viene utilizzata l'autenticazione NTLM.

Ambiente: Cisco Web Security Appliance (WSA), tutte le versioni di AsyncOS

Diversi fattori possono influire sull'invio automatico delle credenziali da parte del client (SSO - Single Sign On) o sulla richiesta all'utente finale di immettere manualmente le credenziali. Verificare gli elementi seguenti durante il tentativo di implementare NTLM con SSO:

Configurazione autenticazione WSA:

Verificare che WSA sia configurato per utilizzare NTLMSSP e non solo NTLM Basic

Questa impostazione è disponibile nella GUI in Web Security Manager > pagina Identità. Modificare l'identità appropriata, quindi selezionare l'impostazione Definisci membri per autenticazione > Schemi di autenticazione.

Selezionate una delle seguenti opzioni:

- Usa NTLMSSP
- Usa Basic o NTLMSSP
- Usa standard

NTLMSSP consente al client di inviare le credenziali in modo sicuro e trasparente al proxy Web.

NTLM Basic consente al client di inviare il nome utente e la password in testo normale quando vengono richieste le credenziali.

Il client sceglie il miglior metodo disponibile quando l'opzione Usa standard o NTLMSSP è selezionata (scelta consigliata). Se il client supporta NTLMSSP, utilizzerà questo metodo e tutti gli altri browser utilizzeranno Basic. Ciò consente la massima compatibilità.

Attendibilità client:

Se il client non considera attendibile l'account WSA, non invierà le credenziali in modo trasparente. Di seguito sono riportate le linee guida per la risoluzione dei problemi relativi agli ambienti in cui il client non considera attendibile WSA.

Il client non considera attendibile l'URL di reindirizzamento dell'autenticazione (solo distribuzioni trasparenti)

In una distribuzione trasparente, il server di distribuzione Windows deve reindirizzare il client a se stesso per eseguire l'autenticazione. Il client può considerare attendibile il percorso reindirizzato.

Per impostazione predefinita, il WSA reindirizza all'FQDN dell'interfaccia P1 (o all'interfaccia M1 se utilizzata per i dati proxy). Poiché si tratta di un nome di dominio completo, Internet Explorer non lo considererà attendibile, in quanto ritiene che si tratti di una risorsa esterna alla rete.

Per impostare Internet Explorer come attendibile per WSA, è possibile procedere in due modi:

1. Aggiungere l'FQDN dell'interfaccia WSA ai siti attendibili. Scegliere Strumenti > Opzioni Internet > Protezione > Siti attendibili e fare clic sul pulsante Siti.
   Nota: questa configurazione deve essere modificata su ogni client.

2. Modificare l'URL di reindirizzamento utilizzato da WSA come nome host risolvibile DNS con una sola parola.

   A tale scopo, è possibile utilizzare l'interfaccia Web. Accedere al proprio account WSA come amministratore e selezionare Rete > Autenticazione. Quindi fare clic su "Modifica impostazioni globali ..." e modificare "Nome host reindirizzamento autenticazione trasparente"

   Se WSA non è in grado di risolvere il nome host utilizzando DNS, verranno visualizzati messaggi di avviso per gli errori di configurazione. Si consiglia di utilizzare il comando DNSCONFIG > localhosts (Nota: 'localhosts' è un comando nascosto) e aggiungere questo nome host per risolvere l'interfaccia WSA utilizzata per i dati proxy.

   Se i client non sono in grado di risolvere il nome host tramite DNS, non saranno in grado di eseguire il proxy.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).