Configurazione dell'autenticazione Kerberos Single Sign-On in SWA

Sommario

Introduzione

In questo documento viene descritto come configurare gli utenti proxy per l'autenticazione Single Sign-On (SSO) tramite Kerberos in Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione della SWA.
- Amministrazione di base di Active Directory.

Cisco consiglia di installare i seguenti strumenti:

- SWA fisico o virtuale.

- Accesso amministrativo all'interfaccia grafica (GUI) SWA.
- Accesso amministrativo ad Active Directory.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Operazioni preliminari

Se il client proxy tenta di accedere a un sito Web e gli viene richiesto di immettere manualmente le credenziali, eseguire la procedura seguente per risolvere il problema.

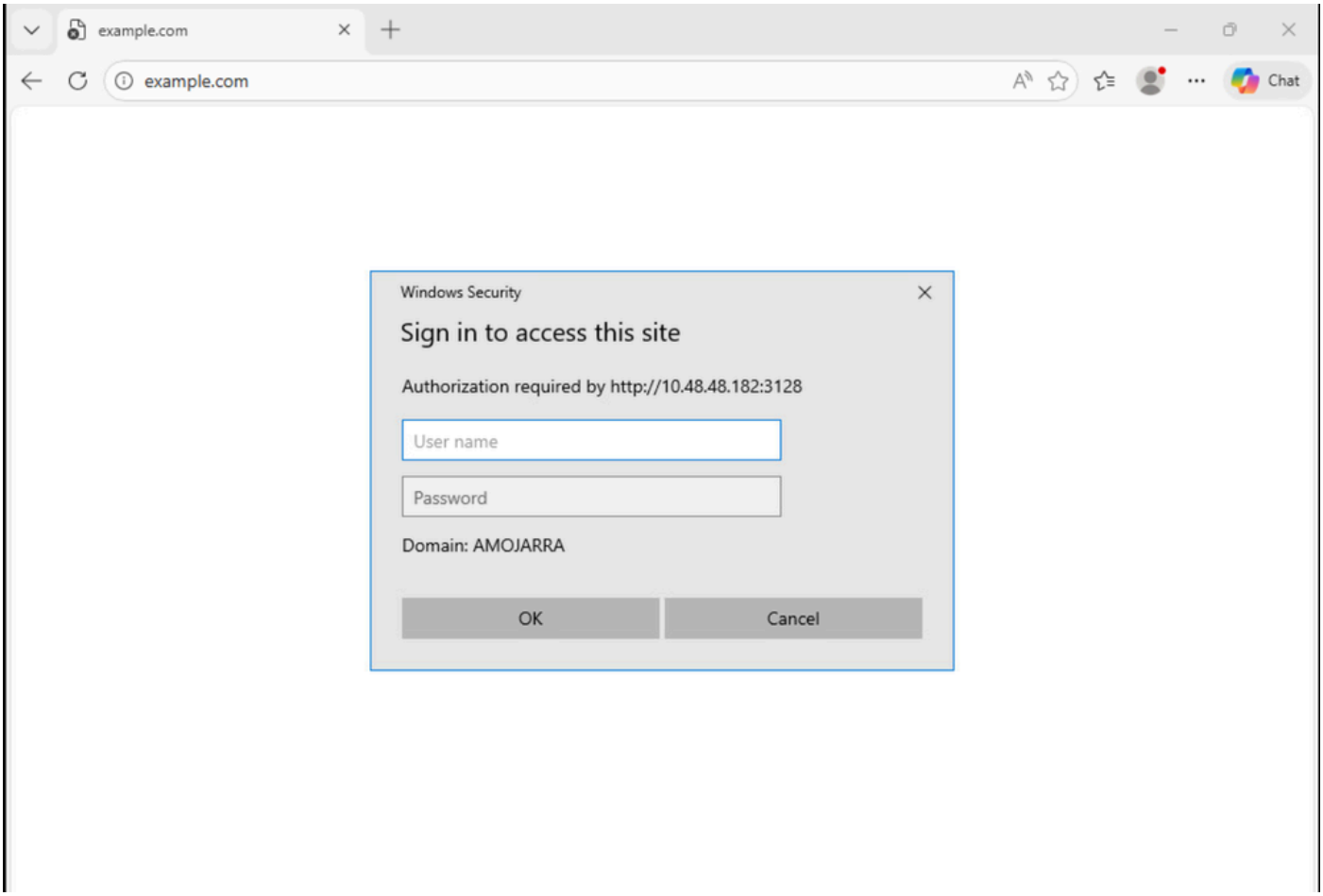


Immagine - Richiesta di autenticazione utente

Passaggio 1. Controllare i log degli accessi relativi al client.

Passaggio 1.1. Accedere alla CLI.

Passaggio 1.2. Eseguire grep.

Passaggio 1.3. Selezionare il numero associato a. accessi.

Passaggio 1.4. Nella casella Immettere l'espressione regolare per digitare l'indirizzo IP del client.

Passaggio 1.5. Premere Invio fino a quando non viene visualizzato Do you want to tail the logs (Si desidera ridurre la lunghezza dei log), Digitare "Y" (Sì) e premere Invio fino a quando non vengono visualizzati i log degli accessi.

Passaggio 1.6. Riprodurre il problema tentando di accedere a qualsiasi sito Web dal PC client.

Passaggio 1.7. Confermare il profilo di identificazione raggiunto dal traffico.

In questo esempio, il profilo di identificazione è Auth_ID:

```
1776248928.353 0 10.48.48.195 TCP_DENIED/407 0 GET http://cisco.com/ - NONE/- - OTHER-NONE-Auth_ID-NONE
```

Passaggio 2. Controllare il profilo di identificazione.

Passaggio 2.1. Accedere alla GUI dell'SWA.

Passaggio 2.2. Da Web Security Manager, selezionare Profili di identificazione.

Passaggio 2.3. Fare clic sul nome del profilo di identificazione raggiunto dal traffico.

Passaggio 2.4. Confermare che lo schema di autenticazione non sia impostato su Basic.

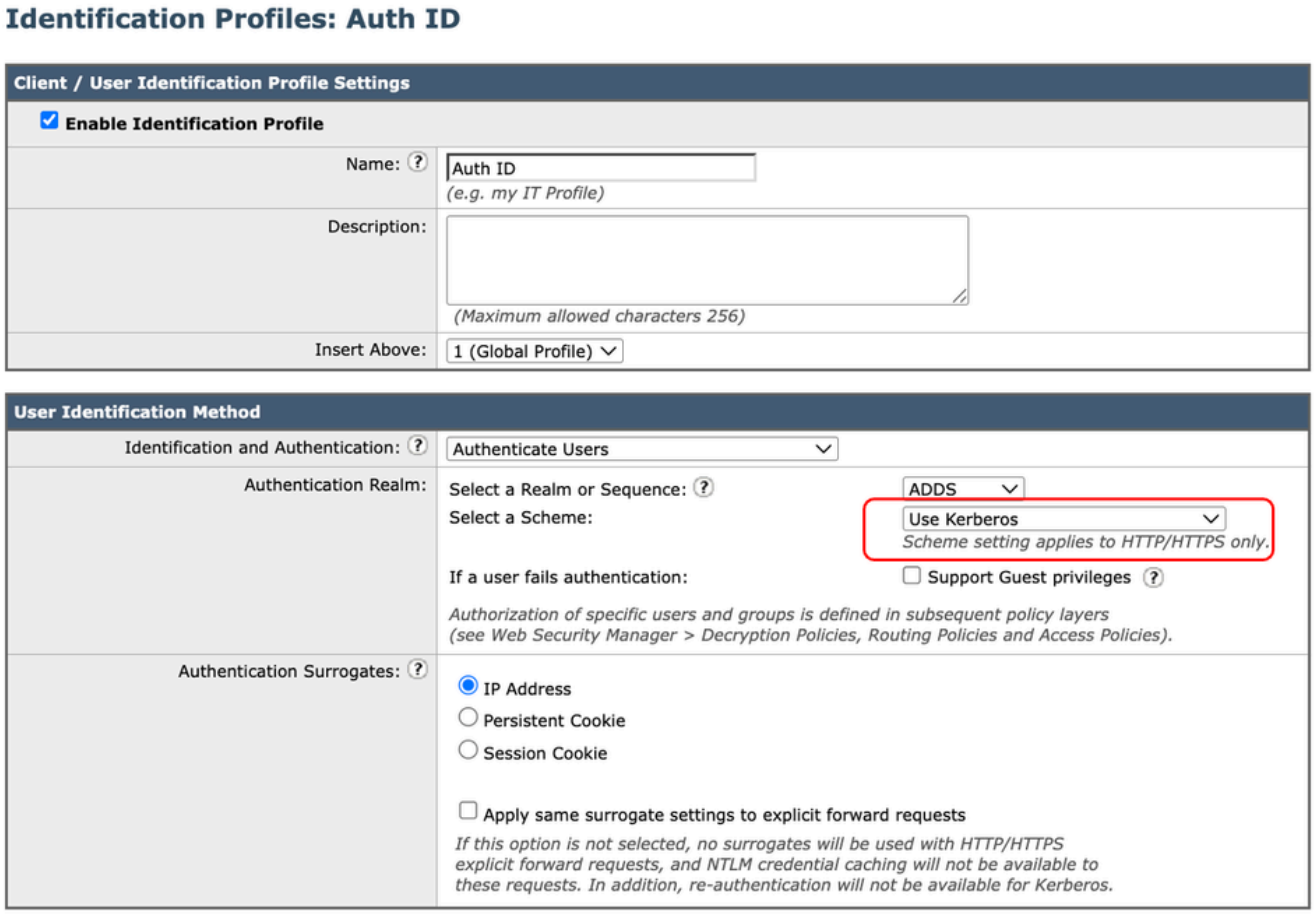


Immagine - Schema di autenticazione

Passaggio 3. Verificare la connettività SWA e Active Directory.

Passaggio 3.1. Dalla GUI SWA, passare a Network (Rete) e selezionare Authentication (Autenticazione).

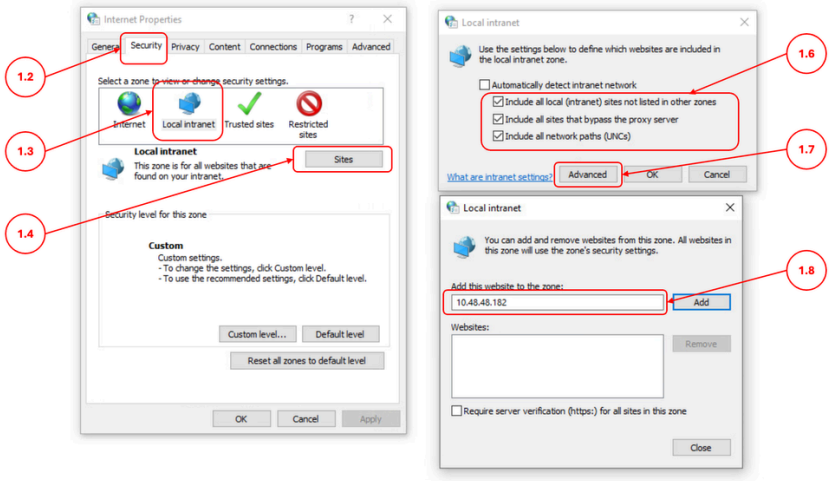
Passaggio 3.2. Fare clic sul nome del realm di autenticazione.

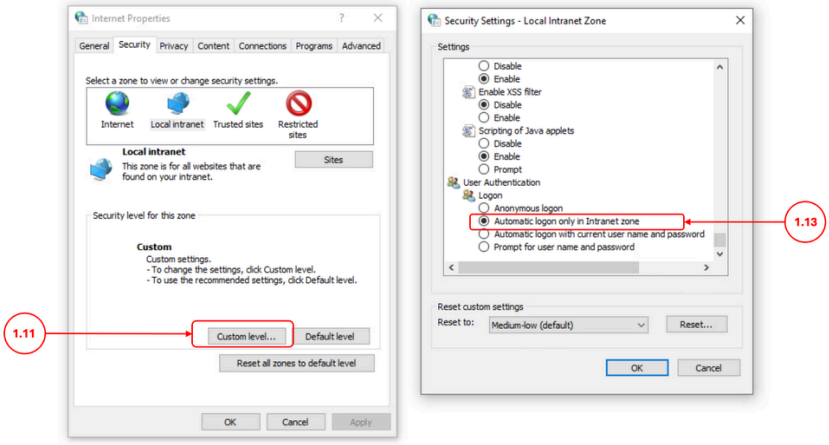
Passaggio 3.3. Fare clic su Avvia test per esaminare lo stato della connettività SWA e Active Directory.

Se non vengono rilevati errori, verificare la configurazione del PC client come descritto in questo articolo.

Configurazione del PC client

Per verificare la configurazione del PC client, attenersi alla procedura seguente:

Passi	Dettagli
Passaggio 1. Siti Intranet locali	Passaggio 1.1. Nel menu Start, digitare Internet Option, quindi premere Invio. Passaggio 1.2. Nella finestra Proprietà Internet, fare clic sulla scheda Protezione. Passaggio 1.3. Selezionare Intranet locale. Passaggio 1.4. Fare clic su Siti. Passaggio 1.5. Assicurarsi che la casella di controllo Rileva automaticamente rete Intranet non sia selezionata. Passaggio 1.6. Selezionare tutte e tre le opzioni: • Includi tutti i siti locali (Intranet) non elencati in altre aree • Includi tutti i siti che ignorano il server proxy • Includi tutti i percorsi di rete (UNC) Passaggio 1.7. Fare clic su Avanzate. Passaggio 1.8. Immettere il nome di dominio completo o l'indirizzo IP del file SWA e aggiungerlo all'elenco. Passaggio 1.9. (Facoltativo) A seconda dei criteri di sicurezza interni, è possibile disabilitare Richiedi verifica server.  Immagine - Configurazione dei siti Internet locali Passaggio 1.10. Fare clic su Chiudi e OK. Passaggio 1.11. Nella scheda Protezione fare clic su Livello

	personalizzato. Passaggio 1.12. Scorrere fino a Autenticazione utente. Passaggio 1.13. Verificare che l'opzione Accesso automatico solo nell'area Intranet sia selezionata.  Immagine - Accesso automatico per utenti Intranet
Passaggio 2. Raccolta dei log	Se nel passaggio 1 non è stata corretta l'autenticazione SSO tramite Kerberos: Passaggio 2.1. Modificare i registri di autenticazione SWA in Traccia ed esaminare i registri. Passaggio 2.2. Aggiungere [Auth-Method = %m] come campo personalizzato ai log degli accessi. per maggiori informazioni, visitare: Configurare il parametro Performance nei log degli accessi. Passaggio 2.3. Eseguire un filtro di acquisizione dei pacchetti per l'indirizzo IP del client e l'indirizzo IP di Active Directory e confermare che il PC client sta inviando il ticket di servizio Kerberos all'SWA.

Nota: Accertarsi di aver configurato l'FQDN dell'SWA nelle impostazioni proxy del browser.

Informazioni correlate

- Guida per l'utente di AsyncOS 15.0 per Cisco Secure Web Appliance
- Configurare il firewall per Secure Web Appliance
- Configurazione dell'acquisizione pacchetti su Content Security Appliance

- Configura parametro prestazioni nei log degli accessi
- Accesso ai registri protetti di Web Appliance
- Uso delle best practice di Secure Web Appliance - Cisco
- Bypass Authentication in Secure Web Appliance - Cisco

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).