Configurar a Autenticação de Logon Único Kerberos no SWA

Contents

Introdução

Este documento descreve as etapas para configurar usuários proxy para ter autenticação SSO (Single-Sign-On, Logon único) via Kerberos no Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Administração SWA.
- Administração básica do Ative Diretory.

A Cisco recomenda que você tenha estas ferramentas instaladas:

- SWA físico ou virtual.

- Acesso administrativo à interface gráfica do usuário (GUI) do SWA.
- Acesso Administrativo ao Ative Diretory.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Antes de Começar

Se o cliente proxy tentar acessar um site e for solicitado a inserir as credenciais manualmente, use estas etapas para solucionar problemas.

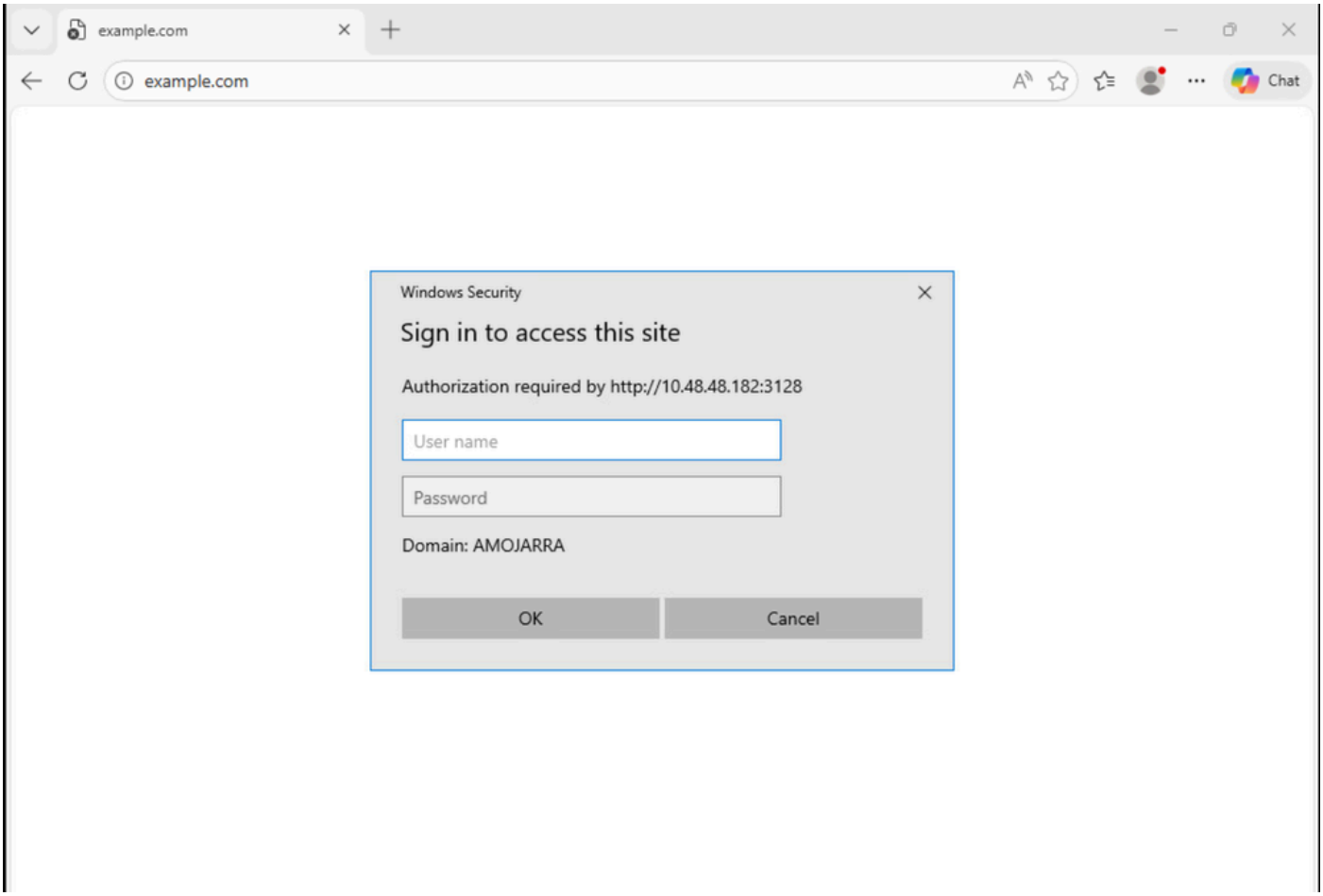


Imagem - Prompt de autenticação do usuário

Etapa 1. Verifique os registros de acesso relacionados ao cliente.

Etapa 1.1. Faça login na CLI.

Etapa 1.2. Execute grep.

Etapa 1.3. Selecione o número associado ao. logs de acesso.

Etapa 1.4. No campo Enter the regular expression to grep digite o endereço IP do cliente.

Etapa 1.5. Pressione Enter até ver Deseja colocar os logs no final, Digite "Y" e pressione Enter até ver os logs de acesso.

Etapa 1.6. Reproduza o problema tentando acessar qualquer site a partir do PC cliente.

Etapa 1.7. confirme o Perfil de identificação que o tráfego está atingindo.

Neste exemplo, o perfil de identificação é Auth_ID:

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

Etapa 2. Verifique o Perfil de identificação.

Etapa 2.1. Faça login na GUI do SWA.

Etapa 2.2. No Web Security Manager, selecione Identification Profiles.

Etapa 2.3. Clique no nome do Perfil de identificação que o tráfego estava acessando.

Etapa 2.4. Confirme se o Esquema de Autenticação não está definido como Básico.

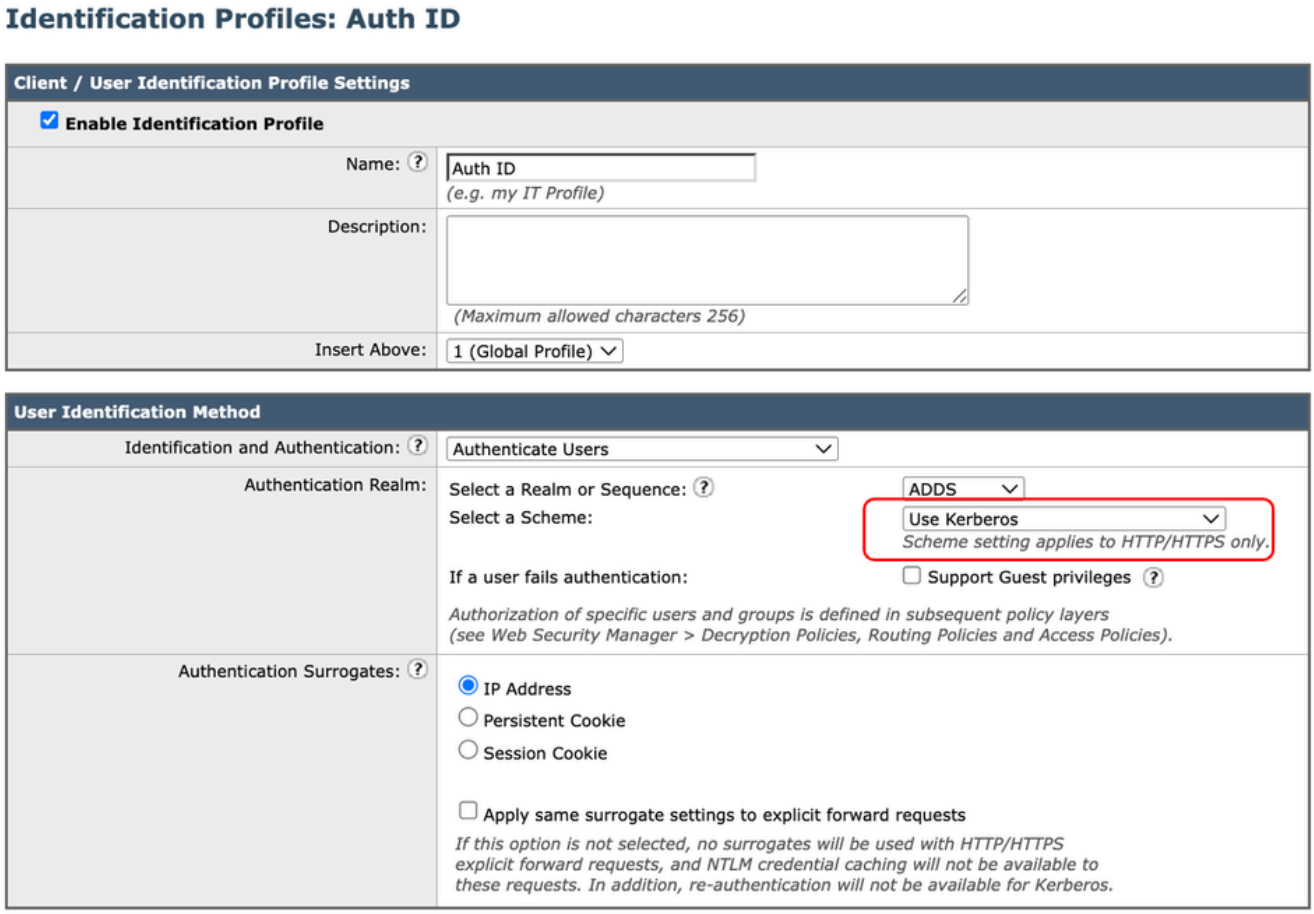


Imagem - Esquema de autenticação

Etapa 3. Teste o SWA e a conectividade do Ative Diretory.

Etapa 3.1. Na GUI do SWA, navegue até Network e selecione Authentication.

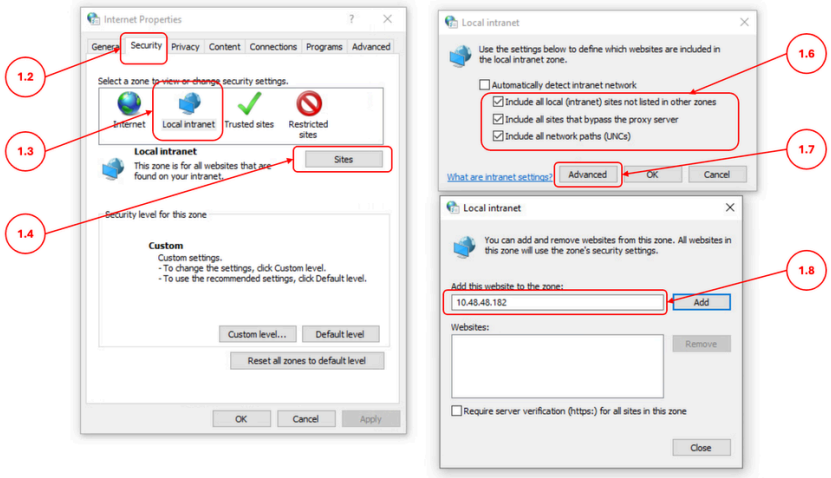
Etapa 3.2. Clique em Authentication Realm Name.

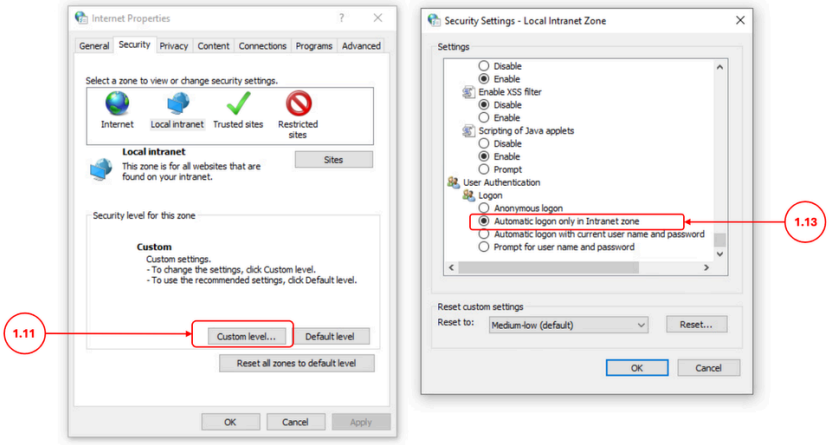
Etapa 3.3. Clique em Start Test para revisar o status de conectividade do SWA e do Ative Diretory.

Se nenhum erro for encontrado, verifique a configuração do PC cliente conforme descrito neste artigo.

Configurar o PC Cliente

Siga estas etapas para verificar a configuração do PC Cliente:

Etapas	Detalhes
Etapa 1. Sites da Intranet Local	Etapa 1.1. No menu Iniciar, digite Internet Option e pressione Enter. Etapa 1.2. Na janela Propriedades da Internet, clique na guia Segurança. Etapa 1.3. Selecione Intranet local. Etapa 1.4. Clique nos Sites. Etapa 1.5. Certifique-se de que a caixa de seleção Detectar automaticamente a rede intranet não esteja marcada. Etapa 1.6. Selecione todas estas três opções: • Incluir todos os sites locais (intranet) não listados em outras zonas • Incluir todos os sites que ignoram o servidor proxy • Incluir todos os caminhos de rede (UNCs) Etapa 1.7. Clique em Avançado. Etapa 1.8. Insira o FQDN ou o endereço IP do SWA e adicione à lista. Etapa 1.9. (Opcional) Dependendo das suas políticas de segurança internas, você pode desabilitar Exigir verificação do servidor.  Imagem - Configurando os sites locais da Internet Etapa 1.10. Clique em Fechar e em OK. Etapa 1.11. Na guia Segurança, clique em Nível

	personalizado. Etapa 1.12. Role até User Authentication. Etapa 1.13. Certifique-se de que Logon automático somente na zona da Intranet esteja selecionado.  Imagem - Login Automático para Usuários da Intranet
Etapa 2. Coletar os Logs	Se a Etapa 1, não corrigiu a autenticação SSO via Kerberos: Etapa 2.1. Altere os registros SWA Auth para Trace e revise os registros. Etapa 2.2. Adicione [Auth-Method = %m] como um campo personalizado aos logs de acesso. para obter mais informações, acesse: Configure o parâmetro de desempenho nos logs de acesso. Etapa 2.3. Execute um filtro de captura de pacotes para o IP do cliente e o endereço IP do Ative Diretory e confirme se o PC cliente está enviando o tíquete de serviço Kerberos ao SWA.

Note: Verifique se você configurou o FQDN do SWA nas configurações de proxy do navegador.

Informações Relacionadas

- Manual do usuário do AsyncOS 15.0 para Cisco Secure Web Appliance
- Configurar firewall para dispositivo seguro da Web
- Configurar a captura de pacotes no dispositivo de segurança de conteúdo

- Configurar Parâmetro de Desempenho em Logs de Acesso
- Acessar logs do dispositivo da Web seguro
- Use as práticas recomendadas de dispositivos da Web seguros - Cisco
- Autenticação de desvio no Secure Web Appliance - Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.