

ASA 8.3: Autenticação TACACS usando ACS 5.X

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurar o ASA para a autenticação do servidor ACS usando o CLI](#)

[Configurar o ASA para a autenticação do servidor ACS usando o ASDM](#)

[Configurar o ACS como um servidor de TACACS](#)

[Verificar](#)

[Troubleshooting](#)

[Erro: AAA que marca o server x.x.x.x TACACS+ em tacacs do Grupo de servidores AAA como FALHADOS](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento fornece a informação em como configurar a ferramenta de segurança para autenticar usuários para o acesso de rede.

[Pré-requisitos](#)

[Requisitos](#)

Este documento supõe que a ferramenta de segurança adaptável (ASA) é plenamente operacional e configurada para permitir que o Cisco Adaptive Security Device Manager (ASDM) ou o CLI façam alterações de configuração.

Nota: Refira [permitir o acesso HTTPS para o ASDM](#) para obter mais informações sobre de como permitir que o dispositivo seja configurado remotamente pelo ASDM.

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão de software adaptável 8.3 da ferramenta de segurança de Cisco e mais atrasado

- Versão 6.3 e mais recente do Cisco Adaptive Security Device Manager
- Serviço de controle de acesso Cisco Secure 5.x

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a [Command Lookup Tool](#) ([somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:

Nota: Os esquemas de endereçamento IP usados nesta configuração não são legalmente roteáveis na Internet. São os endereços do RFC 1918 que foram usados em um ambiente de laboratório.

Configurar o ASA para a autenticação do servidor ACS usando o CLI

Execute estas configurações para o ASA para autenticar do servidor ACS:

```
!--- configuring the ASA for TACACS server ASA(config)# aaa-server cisco protocol tacacs+
ASA(config-aaa-server-group)# exit !--- Define the host and the interface the ACS server is on.
ASA(config)# aaa-server cisco (DMZ) host 192.168.165.29 ASA(config-aaa-server-host)# key cisco
!--- Configuring the ASA for HTTP and SSH access using ACS and fallback method as LOCAL
authentication. ASA(config)#aaa authentication ssh console cisco LOCAL ASA(config)#aaa
authentication http console cisco LOCAL
```

Nota: Crie um usuário local no ASA usando o comando do [privilegio 15 de Cisco da senha Cisco username](#) alcançar o ASDM com autenticação local quando o ACS não está disponível.

Configurar o ASA para a autenticação do servidor ACS usando o ASDM

Procedimento ASDM

Termine estas etapas a fim configurar o ASA para a autenticação do servidor ACS:

1. Escolha o > **Add da configuração** > do **Gerenciamento de dispositivos** > **Users/AAA** > dos **Grupos de servidores AAA** a fim criar um **Grupo de servidores AAA**.

2. Forneça os detalhes do **Grupo de servidores AAA** no indicador de **Grupo de servidores AAA adicionar** como mostrado. O protocolo usado é **TACACS+** e o grupo de servidor criado é **Cisco**. Clique em **OK**.
3. Escolha a **configuração > o Gerenciamento de dispositivos > o Users/AAA > os Grupos de servidores AAA** e o clique **adiciona** sob **server** no grupo selecionado a fim adicionar o servidor AAA.
4. Forneça os detalhes do **servidor AAA** no indicador do **servidor AAA adicionar** como mostrado. O grupo de servidor usado é **Cisco**. **A APROVAÇÃO** do clique, clica então **aplica-se**. Você verá o **Grupo de servidores AAA** e o **servidor AAA** configurados no ASA.
5. Clique em **Apply**.
6. Escolha a **configuração > o Gerenciamento de dispositivos > o Users/AAA > o acesso > a autenticação AAA** e clique as caixas de seleção ao lado de **HTTP/ASDM** e de **SSH**. Então, escolha **Cisco** como o grupo de servidor e o clique **aplica-se**.

[Configurar o ACS como um servidor de TACACS](#)

Termine este procedimento a fim configurar o ACS como um servidor de TACACS:

1. Escolha **recursos de rede > dispositivos de rede e os clientes de AAA** e o clique **criam** a fim adicionar o ASA ao servidor ACS.
2. Forneça a informação requerida sobre o **cliente** (ASA é o cliente aqui) e o clique **submete-se**. Este enable the ASA a obter adicionou ao servidor ACS. Os detalhes incluem o **endereço IP de Um ou Mais Servidores Cisco ICM NT do ASA** e dos detalhes do **servidor de TACACS**. Você verá o cliente **Cisco** que está sendo adicionado ao servidor ACS.
3. Escolha **usuários e a identidade armazena > identidade interna armazena > usuários** e o clique **cria** a fim criar um novo usuário.
4. Forneça o **nome, senha, e permita a informação de senha**. **Permita a senha é opcional**. Quando você termina, o clique **submete-se**. Você verá o usuário **Cisco** que está sendo adicionado ao servidor ACS.

[Verificar](#)

Use esta seção para confirmar se a sua configuração funciona corretamente.

Use o **comando cisco** o mais thetest da **senha Cisco username de 192.168.165.29 do host de Cisco da autenticação de AAA-server** verificar se a configuração trabalha corretamente. Esta imagem mostra que a autenticação é bem sucedida e o usuário que conecta ao ASA esteve autenticado pelo servidor ACS.

A [Output Interpreter Tool \(apenas para clientes registrados\)](#) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

[Troubleshooting](#)

[Erro: AAA que marca o server x.x.x.x TACACS+ em tacacs do Grupo de servidores AAA como FALHADOS](#)

Esta mensagem significa que Cisco ASA perdeu a Conectividade com o server x.x.x.x. Certifique-se de você ter uma Conectividade válida no TCP 49 ao server x.x.x.x do ASA. Você pode igualmente aumentar o intervalo no ASA para o server TACACS+ de 5 ao número desejado de segundos caso que há uma latência da rede. O ASA não enviaria um pedido de autenticação ao servidor falho x.x.x.x. Contudo, usará o server seguinte nos tacacs do Grupo de servidores AAA.

[Informações Relacionadas](#)

- [Página de Suporte dos Cisco ASA 5500 Series Adaptive Security Appliances](#)
- [Referências de comandos do Dispositivos de segurança adaptáveis Cisco ASA série 5500](#)
- [Cisco Adaptive Security Device Manager](#)
- [Página de Suporte de Negociação IPSec/Protocolos IKE](#)
- [Cisco Secure Access Control Server for Windows](#)
- [Solicitações de Comentários \(RFCs\)](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)