Examine como o RADIUS funciona

Contents

Introduction

Este documento descreve o que é um servidor RADIUS e como ele funciona.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Conventions

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Informações de Apoio

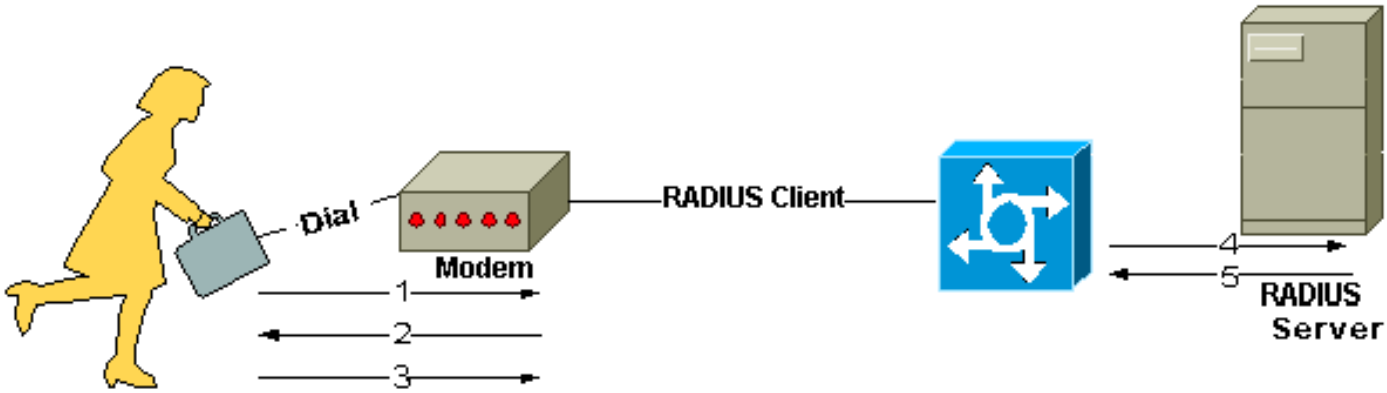
O protocolo RADIUS (Serviço de usuário de autenticação discada remota) foi desenvolvido pela Livingston Enterprises, Inc., como um protocolo de autenticação e contabilização de servidores de acesso. A especificação RADIUS RFC 2865 torna obsoleta a RFC 2138. O padrão de auditoria RADIUS RFC 2866 torna obsoleto a RFC 2139.

A comunicação entre um servidor NAS e um servidor RADIUS se baseia no protocolo UDP. Geralmente, o protocolo RADIUS é considerado um serviço sem conexão. Problemas relacionados a disponibilidade, retransmissão e timeouts do servidor são tratados por dispositivos preparados para RADIUS, em vez do protocolo de transmissão.

RADIUS é um protocolo cliente/servidor

O cliente RADIUS é geralmente um NAS e o servidor RADIUS é geralmente um processo daemon que é executado em uma máquina UNIX ou Windows NT. O cliente passa as informações do usuário para os servidores RADIUS designados e age na resposta retornada. Os servidores RADIUS recebem solicitações de conexão do usuário, autenticam o usuário e retornam as informações de configuração necessárias para o cliente entregar o serviço ao usuário. Um servidor RADIUS pode agir como um cliente proxy para outros servidores RADIUS ou outros tipos de servidor de autenticação.

Esta figura mostra a interação entre um usuário de discagem de entrada e o cliente e servidor RADIUS.



Interação entre o usuário de discagem e o cliente e servidor RADIUS

1. O usuário inicia a autenticação do PPP no NAS.
2. O NAS solicita o nome de usuário e a senha [se estiver usando o PAP (Protocolo de autenticação de handshake)] ou o desafio [se estiver usando o CHAP (Protocolo de desafio de autenticação de handshake)].
3. O usuário responde.
4. O cliente RADIUS envia o nome de usuário e senha criptografada para o servidor RADIUS.
5. O servidor RADIUS responde com Accept, Reject ou Challenge.
6. O cliente RADIUS age de acordo com os serviços e parâmetros de serviços embutidos em Accept ou Reject.

Autenticação e Autorização

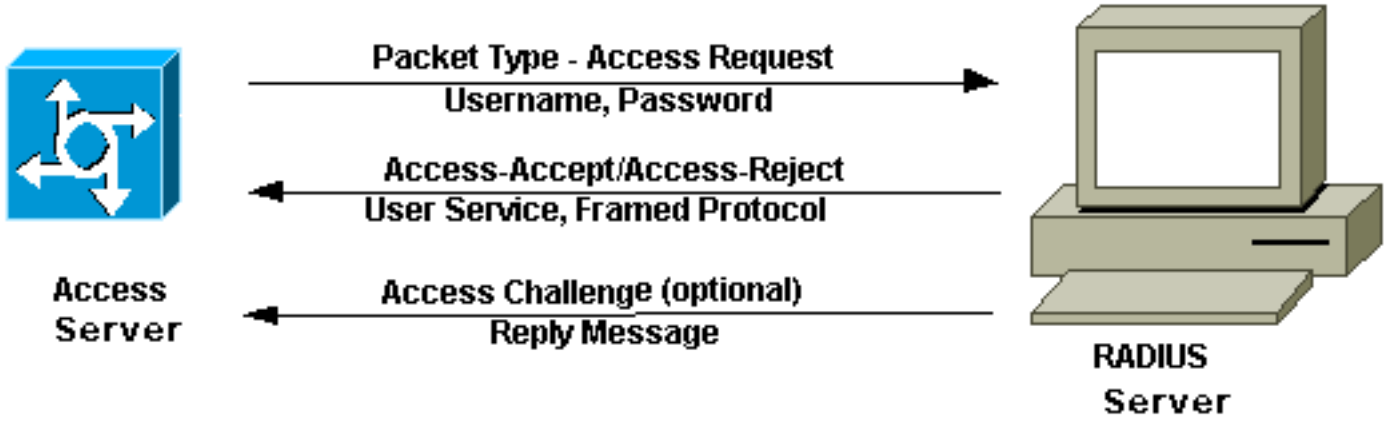
O servidor RADIUS pode suportar vários métodos de autenticação de usuário. Quando ele é fornecido com o nome de usuário e a senha original dados pelo usuário, é compatível com PPP, PAP ou CHAP, login do UNIX e outros mecanismos de autenticação.

Normalmente, um logon de usuário consiste em uma consulta (Access-Request) do NAS ao servidor RADIUS e uma resposta correspondente (Access-Accept ou Access-Reject) do servidor. O pacote Access-Request contém o nome de usuário, a senha criptografada, o endereço IP do NAS e a porta. A implantação inicial do RADIUS foi feita com a porta UDP número 1645, que conflita com o serviço de "métricas de dados". Devido a esse conflito, a RFC 2865 atribuiu

oficialmente o número de porta 1812 para RADIUS. A maioria dos dispositivos e aplicativos da Cisco oferece suporte para qualquer conjunto de números de porta. O formato da solicitação também oferece informações sobre o tipo de sessão que o usuário deseja iniciar. Por exemplo, se a consulta é apresentada no modo de caracteres, a conclusão é "Service-Type = Exec-User", mas se for apresentada no modo de pacotes de PPP, é "Service Type = Framed User" e "Framed Type = PPP".

Quando o servidor RADIUS recebe o Access-Request do NAS, ele pesquisa um banco de dados para o nome de usuário listado. Se o nome de usuário não existir no banco de dados, um perfil padrão será carregado ou o servidor RADIUS enviará imediatamente uma mensagem Access-Reject. Essa mensagem de Access-Reject pode ser acompanhada por uma mensagem de texto que indica o motivo da recusa.

No RADIUS, a autenticação e a autorização são feitas em conjunto. Se o nome de usuário for encontrado e a senha estiver correta, o servidor RADIUS retornará uma resposta Access-Accept, que inclui uma lista de pares de atributo/valor que descrevem os parâmetros a serem usados para essa sessão. Os parâmetros típicos incluem tipo de serviço (shell ou quadros configurados), tipo de protocolo, IP Address a ser atribuído ao usuário (estático ou dinâmico), lista de acessos a ser aplicada ou uma rota estática a ser instalada na tabela de roteamento NAS. As informações de configuração no servidor RADIUS definem o que pode ser instalado no NAS. A próxima figura ilustra a autenticação RADIUS e a sequência de autorização.



Autenticação RADIUS e sequência de autorização

Relatório

Os recursos de relatório do protocolo RADIUS podem ser usados independentemente de autenticação ou autorização RADIUS. As funções de contabilidade do RADIUS permitem que os dados sejam enviados no início e no fim das sessões, o que indica a quantidade de recursos (como tempo, pacotes, bytes e assim por diante) usados durante a sessão. Um provedor de serviços de Internet (ISP) pode usar o software de controle de acesso e tarifação RADIUS para atender a necessidades especiais de segurança e tarifação. A porta de contabilização para RADIUS da maioria dos dispositivos da Cisco é 1646, mas também pode ser 1813 (devido à alteração nas portas, conforme especificado em na RFC 2139).

As transações entre o cliente e o servidor RADIUS são autenticadas utilizando um segredo compartilhado, que nunca é enviado na rede. Além disso, as senhas de usuário são enviadas criptografadas entre o cliente e o servidor RADIUS para eliminar a possibilidade de que alguém espionando uma rede não segura possa determinar uma senha de usuário.

Informações Relacionadas

- Protocolos de Autenticação
- Solicitações de Comentários (RFCs)
- Suporte Técnico - Cisco Systems

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.