Como o RAIO trabalha?

Índice

Introdução

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.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

Convenções

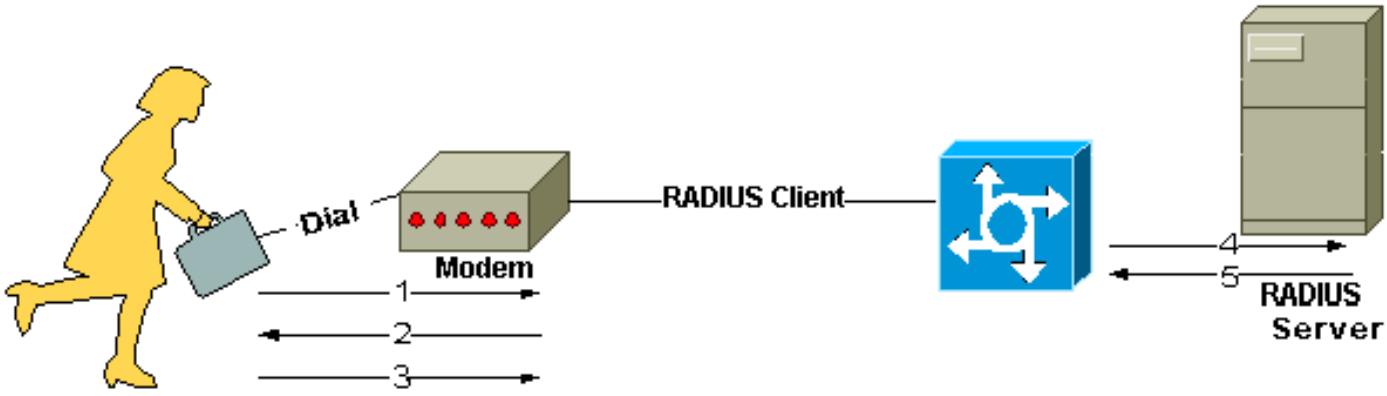
Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Informações de Apoio

A comunicação entre um servidor NAS e um servidor RADIUS se baseia no protocolo UDP. Geralmente, o protocolo de raio 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.

O RAIO é um protocolo cliente/servidor. O cliente RADIUS é tipicamente um NAS e o servidor Radius é geralmente um processo de demônio que é executado em UNIX ou em uma máquina do Windows NT. O cliente passa a informação sobre o usuário aos servidores radius designados e aos atos na resposta que é retornada. Os servidores Radius recebem pedidos de conexão do usuário, autenticam o usuário, e retornam então a informação de configuração necessária para que o cliente entregue 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.



1. O usuário inicia a autenticação de PPP ao 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. Respostas do usuário.
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

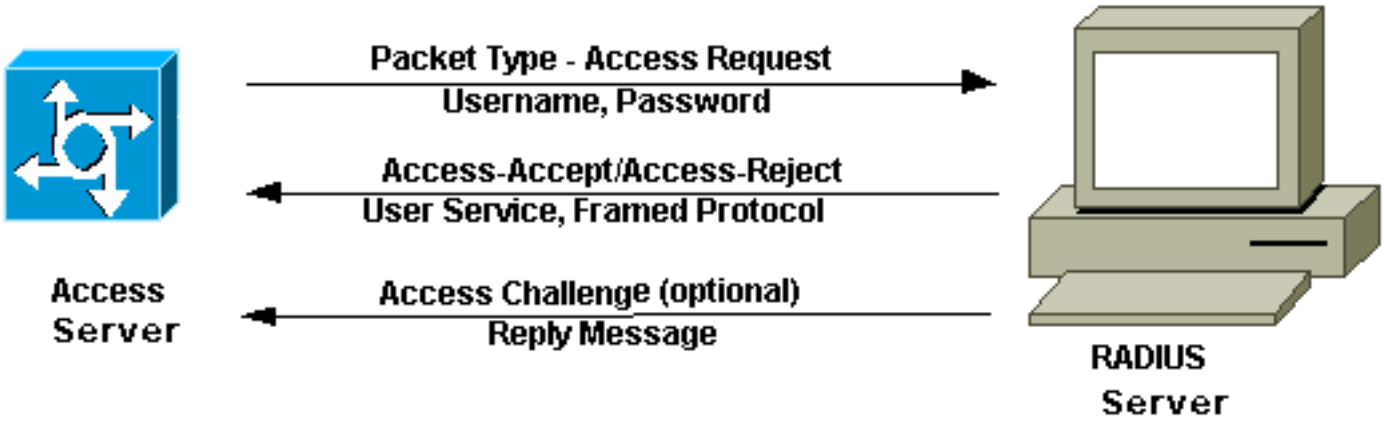
O servidor RADIUS pode suportar vários métodos de autenticação de usuário. Quando se fornece com o username e a senha original dados pelo usuário, pode apoiar o início de uma sessão PPP, PAP ou de RACHADURA, de UNIX, e os outros mecanismos da autenticação.

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 de solicitação de acesso contém o username, a senha criptografada, o endereço IP de Um ou Mais Servidores Cisco ICM NT NAS, e a porta. O Early Deployment do RAIO foi feito usando o número de porta 1645 UDP, que opõe ao serviço do “datametrics”. Devido a este conflito, o RFC 2865 atribuiu oficialmente o número de porta 1812 para o RAIO. A maioria dispositivos Cisco e de aplicativos oferecem o apoio para um ou outro números do conjunto 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 a solicitação de acesso do NAS, procura um base de dados

pelo username alistado. Se o nome de usuário não constar do banco de dados, um perfil padrão é carregado ou o servidor RADIUS envia imediatamente uma mensagem Access-Reject. Essa mensagem Access-Reject pode ser acompanhada por uma mensagem de texto indicando o motivo da recusa.

No RADIUS, a autenticação e a autorização são feitas em conjunto. Se o nome de usuário for localizado e a senha estiver correta, o servidor RADIUS retorna uma resposta de aceitação de acesso, incluindo uma lista dos pares de valor e atributo que descrevem os parâmetros a serem usados para esta 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 do servidor RADIUS definem o que será instalado no NAS. A figura abaixo ilustra a autenticação do RADIUS e a seqüência de autorização.



Relatório

Os recursos de relatório do protocolo RADIUS podem ser usados independentemente de autenticação ou autorização RADIUS. As funções de contabilização do RADIUS permitem que dados sejam enviados no inicio e no término de sessões, indicando a quantidade de recursos (como horário, pacotes, bytes, etc.) usados durante a sessão. Um provedor de serviços de Internet (ISP) pode usar o controle de acesso RADIUS e um software de contabilidade para atender necessidades especiais de segurança e faturamento. A porta de relatório para o RAIO para a maioria de dispositivos Cisco é 1646, mas pode igualmente ser 1813 (devido à mudança nas portas como especificado no RFC 2139).

As transações entre o cliente e o servidor RADIUS são autenticadas utilizando um segredo compartilhado, que nunca é enviado na rede. Além, as senhas do usuário são enviadas cifradas entre o cliente e o servidor Radius para eliminar a possibilidade que alguém espião em uma rede insegura poderia determinar uma senha de usuário.

Informações Relacionadas

- Página de suporte de tecnologia RADIUS
- Solicitações de Comentários (RFCs)
- Suporte Técnico - Cisco Systems