GTI - V - NOTURNO
ARTHUR OLIVEIRA, ISADORA SERRANO, JOÃO MOITA MATHEUS FERREIRA

PROJETO DE REDES DE COMPUTADORES
FREE RADIUS

Trabalho realizado como tema do projeto Integrador
do componente curricular de Projeto de Redes de Computadores,
Ministrado pela professora: **Kelly Alves**

Goiânia
2018

O freeRadius é dos servidores de radius mais populares do mundo, implementa o protocolo de rede RADIUS, que é a abreviação para *"Remote Authentication Dial in User Service*", opera com o protocolo 802.1x, que é um protocolo de definição de redes wireless. É muito utilizado no meio acadêmico e em pesquisas, foi desenvolvido em 1999 por *Alan DeKok* e *Miquel Van Smoorendburg*. Atualmente o servidor é uma referência em hospedagem de informações de autenticação, autorização e contabilidade. Devido possuir código livre o servidor passa por várias atualizações rapidamente, evoluindo e se tornando mais seguro, é um dos poucos que suportam um grande número de tipos de autenticação e, é o único servidor que suporta o protocolo EAP - Protocolo de Autenticação Estendível.

O RADIUS é basicamente um protocolo de rede que implementa um sistema de regras e convenções para a comunicação entre dispositivos de rede.

O FreeRADIUS é o único que suporta virtualização, mantendo os custos de implantação e manutenção baixos. Segundo algumas organizações, um servidor RADIUS pode manipular de uma até milhares de requisições por segundo. Esse servidor trabalha com políticas AAA (*Authorisation, Authentication e Accounting*), que implementa o esquema de consultas SQL, é o que torna esse servidor mais robusto e eficaz.

Funções do FreeRADIUS

O FreeRadius pode definir regras e convenções para a comunicação entre dispositivos de rede, além de permitir que o usuário seja autorizado e autenticado. as principais funcionalidades do protocolo RADIUS são:

- Autenticar usuários ou dispositivos antes de permitir que acessem a rede;
- Autorizar usuários ou dispositivos do uso de determinados serviços da rede;

- Contabilizar e rastrear o uso desses serviços pelos usuários ou dispositivos.

COMO FUNCIONA - PROTOCOLO AAA

Como descrito anteriormente AAA é a sigla para autorização, autenticação e contabilidade, que são as funcionalidades do protocolo RADIUS, esse protocolo é o que garante uma arquitetura autêntica e os privilégios de autenticação para os usuários, além de manter um log de suas operações na rede, o que garante uma rastreabilidade das atividades realizadas na rede.

O padrão AAA, possibilitou a criação de vários protocolos para autenticação e segurança nos últimos tempos, o que vem tornando os procedimentos com operação de sistemas mais seguros e robustos.

O primeiro A, está relacionado a **autenticação**, que é o processo onde a identidade do usuário é validada, suas credenciais informadas são comparadas com o que está registrado no banco de dados do servidor AAA, as credenciais combinando, o usuário é autenticado e obtém acesso a rede ou ao sistema, se não coincidirem, o acesso é negado. Muitos sistemas hoje em dia permitem que o usuário faça várias tentativas de autenticação, e quando as tentativas muitos sistemas travam ou bloqueiam o usuário. Há ainda a opção de renovar a senha, informando um endereço de e-mail que foi cadastrado.

A autenticação pode acontecer de várias formas, login e senha, leitura de retina ou digital, combinação de um padrão, reconhecimento de voz ou facial, entre outros, porém o mais utilizado é a autenticação por login e senha. A autenticação pode ser configurada para ser um processo seletivo baseado em características de uso, de origem e principalmente em políticas de segurança.

O segundo A, está relacionado a **autorização**, que é o processo que determina quais permissões são garantidas para um usuário. Essas autorizações podem ser por política de proibitiva, onde tudo é negado e somente os processos autorizados ao usuário específico são liberado, ou por política permissiva, onde tudo é permitido e somente os processos e recursos não autorizados são negados. Essas políticas são definidas pelo NAS.

O NAS é basicamente o dispositivo do cliente, onde as regras serão implementadas, sua sigla significa, *Network Access Server*, ele é o responsável por fazer requisições dos serviços AAA do RADIUS.

O NAS envia também é responsável por enviar requisições ao RADIUS, que analisa se as informações de login (IP da máquina, usuário e senha), constam em sua base de dados, e quais permissões este possui, essa análise é feita via consultas SQL simples.

O último A refere se a **contabilidade,** que é o processo de gravação de registros sobre como o usuário utilizou os recursos autorizados, nessa parte é realizada a cobrança ou as limitações de uso e controle, com base nos seguintes parâmetros: tempo de uso, quantidade de dados enviada e recebida, entre outros. O resultado desses cálculos podem ser utilizados para auditoria e segurança, controle de acesso e horário. Informações como sites visitados, protocolos utilizados também são armazenados pelo NAS.

Um outro A que o RADIUS implementa, apesar de não constar na sigla, é o de **auditoria**, que é o processo de análise proativa dos registros da contabilidade e de outros metadados, tem como objetivo buscar relacionar o usuário com suas atividades na rede. esse processo busca analisar as atividades após a autenticação e adequar o uso a política visando evitar comportamentos inadequados. A auditoria também pode ser utilizada para checar a segurança de outros processos e protocolos, com o objetivo de prevenir violações na política de segurança.

Os principais componentes do sistema RADIUS são:

- Usuário e Dispositivo;
- NAS - Servidor de Acesso à Rede (Access Point);
- Servidor de autenticação (FreeRadius);
- Banco de Dados.

PROCESSO DE UMA SESSÃO RADIUS

1) Um usuário portando um dispositivo, se conecta a um cliente RADIUS (NAS), utilizando o protocolo 802.1x;
    - O NAS inicia a comunicação para autenticação com RADIUS.

- As informações enviadas são a critério do cliente.
- O Servidor RADIUS não controla o que NAS envia.

2) O NAS se comunica com o servidor RADIUS utilizando um protocolo secreto compartilhado, através de pacotes TCP ou UDP, utilizando portas previamente escolhidas para autenticação e contabilidade;
3) O NAS envia para o servidor RADIUS uma mensagem (Access-Request). Essa mensagem contém a informação sobre o usuário, suas credenciais de autenticação e serviços requisitados, também pode conter algumas informações sobre o NAS, tais como: hostname, endereço MAC ou SSID wireless;

3.1 A mensagem é enviada usando um protocolo de autenticação de senhas ou um protocolo de autenticação estendida EAP.

3.2 O servidor define se a autenticação será definida somente nas informações recebidas do NAS. Caso seja enviado um pacote não suportado pelo servidor RADIUS, o mesmo é descartado.

4) O servidor RADIUS processa a requisição e faz uma análise, verificando se a solicitação de login realizada consta na base de dados local. esse serviço pode conter servidores LDAP para verificação de domínio.
5) O servidor RADIUS envia a validação de volta ao NAS nos seguintes formatos: Access Reject, Access Challenge ou Access Accept.
    - ***Access Reject*** - Acesso negado: A autenticação não é aprovada pelo servidor, o usuário permanece do lado de fora da rede, sem acesso aos recursos solicitados;
    - ***Access Challenge*** - Desafio de acesso: Ocorre quando o servidor solicita informações adicionais do usuário, podendo ocorrer várias trocas por limitações de pacotes do servidor RADIUS;
    - ***Access Accept*** - Acesso permitido: A autenticação do usuário é aprovada pelo servidor, e o acesso aos serviços e recursos são fornecidos, de acordo com a política definida pelo NAS. Uma aceitação de conexão pode enviar várias aprovações para diversos recursos solicitados, não havendo herança de um para outro.
6) Uma vez estabelecida a sessão entre o cliente RADIUS, o processo de contabilidade pode ser inicializado.

- Uma requisição *Accounting-Request* (start) é enviada pelo NAS ao servidor, indicando o início da sessão de contabilidade.
- Uma requisição *Accounting-Request* (stop) indica o fim da sessão de contabilidade que deve ser gravada e fechada.
- A base de dados utilizada para contabilidade é usada para fins de informações e relatórios de uso.
- Podem ser registrados o tempo de sessão, o número de pacotes ou o total de dados transmitidos em ambas direções.

REFERÊNCIAS BIBLIOGRÁFICAS

FreeRadius noções básicas parte I. **Viva o Linux.** Último acesso em: 13/06/18. Disponivel em: < https://www.vivaolinux.com.br/artigo/FreeRADIUS-Nocoes-basicas-Parte-I>

Configurando um servidor freeRadius. **Viva o Linux.** Publicado por: **Victor Frazão.** Último acesso em: 14/06/18. Disponível em: <https://www.vivaolinux.com.br/artigo/Configurando-um-servidor-Freeradius-+-openLDAP>

PPLware. Aprenda a instalar e configurar o freeRadius. Publicado por: **Pedro Pinto.** Último acesso em: 13/06/18. Disponível em: <https://pplware.sapo.pt/microsoft/windows/aprenda-a-instalar-e-configurar-o-freeradius-parte-ii/>