

Firewall com pfSense

Instalação e configurações do pfSense como solução de firewall e proxy para o DNOCS.

Um pouco de Teoria

Firewall

Firewall pode ser definido como uma barreira de proteção, que controla o tráfego de dados entre um servidor e a Internet(ou entre uma rede e a Internet). Seu objetivo é permitir somente a transmissão e a recepção de dados autorizados. Existem firewalls baseados na combinação de hardware (appliance) e software e firewalls baseados somente em software. Este último é o tipo recomendado ao uso doméstico ou para pequenas empresas e também é o mais comum.

Uma vantagem do uso de firewalls em redes, é que basta um computador pode atuar como firewall, não sendo necessário instalá-lo em cada máquina conectada.

Firewall baseado em Hardware

Muito usado em empresas médias e grandes corporações, com uma grande quantidade de máquinas. Uma grande vantagem deste tipo de firewall é que tem um hardware dedicado, ao invés de compartilhar recursos com outros serviços.

Proxy

São aplicativos que efetuam a comunicação entre ambos os lados por meio da avaliação do número da sessão TCP dos pacotes.

Todas as aplicação são obrigadas a usar o proxy para funcionar, o que oferece um grande controle. O proxy permite um acompanhamento mais preciso do tráfego entre rede e internet, ou entre redes. É possível, inclusive, contar com recursos de log e ferramentas de auditoria. Tais características deixam claro que este tipo de firewall é voltado para redes de médio ou grande porte e que sua configuração exige mais experiência no assunto.

pfSense

O pfSense é um sistema operacional de código aberto baseado no Unix FreeBSD adaptado para ser um firewall e/ou roteador/gateway, portanto seu kernel é leve e contém somente o necessário para o funcionamento do firewall.

É uma das mais populares soluções de firewall e provavelmente a mais rica em recursos entre os sistemas para appliance, pré-configurado, pronto, amigável, amigável e fácil de usar, devido sua amigável interface Web e da versão simplificada do FreeBSD, focado em ambientes de roteamento e firewalling, bem como segurança de networking, proxy, com excelente solução para VPN, entre outros diversos recursos. É um projeto descendente do famoso m0n0wall. Ao lado do FreeNAS são os principais e grandes projetos derivados do m0n0wall.

Um dos únicos recursos que o Pfsense não integra – por opção dos criadores do Projeto – é um IPS (Intrusion Prevention System).

Atualmente o Pfsense pode ser considerado um serviço UTM, Unified Threat Management, ou Central Unificada de Gerenciamento de Ameaças, inclusive já é comercializado na forma de appliance (hardware + software) e seus serviços são abrangentes no quesito segurança de redes, sendo uma evolução do firewall tradicional, pois une a execução de vários serviços tais como vpn, balanceamento de carga, regras de NAT, regras de firewall, proxy/cache, geração de chaves RSA, monitoramento de tráfego, etc.

Site oficial

<http://pfsense.org>

Forum

<https://forum.pfsense.org/>

Forum em português

<https://forum.pfsense.org/index.php?board=12.0>

Suporta instalação full com ISO e em pendrive.

Squid

O Squid é um servidor proxy que suporta HTTP, HTTPS, FTP e outros protocolos.

Servidor proxy - No cache são armazenados os objetos da Internet (ex. dados de páginas web) disponíveis via protocolo HTTP, FTP e Gopher num sistema mais próximo ao do cliente.

Muito utilizado por provedores de hospedagem e em redes locais (LAN).

A aplicação cliente (exemplo: navegador) poderá usar um proxy transparente, para facilitar o trabalho da equipe de administração. Assim todos os pedidos HTTP para fora serão interceptados pelo Squid e todas as respostas serão armazenadas em cache. Desta forma não sendo necessário configurar o navegador.

Captive Portal

Captive portal é um programa de computador responsável por controlar e gerenciar o acesso a Internet em redes públicas, de forma "automatizada". Ao digitar o endereço de qualquer site no navegador o usuário é interceptado pelo sistema do Captive Portal e redirecionado para uma interface que solicita a autenticação. É importante lembrar que não existe uma fórmula ou receita pronta que indique passo-a-passo como o PfSense deve ser configurado, pois tudo depende da necessidade da aplicação do mesmo.

Requisitos Mínimos para instalar o pfSense 2.x

<https://www.pfsense.org/hardware/#requirements>

<https://www.freebsd.org/releases/10.3R/hardware.html>

Mínimo

CPU – 500 MHz
RAM – 256 MB

Recomendado

CPU – 1 GHz (recommded: modern 1.0 GHz Intel or AMD CPU)
RAM – 1 GB

Requisitos para plataformas específicas

Instalação completa:
CD-ROM ou pendrive para instalação inicial

Incorporado:
1 cartão de memória/pendrive com 1GB
Porta serial ou VGA para a console

Placas de rede

2 a 3 placas de rede, dependendo do servidor

pfSense® software has the flexibility to be installed on a wide range of hardware, but it is currently supported only on the x86 architecture. The types of devices supported range from embedded devices to rack mounted servers.

Since network environments differ dramatically, determining the exact hardware sizing for your pfSense deployment can be difficult, but the following will provide some base guidelines on choosing which hardware is sufficient for your installation.

Adaptação de:

Tutorial Pfsense

Instalação e Configurações Básicas

(De Aires Santos, Caíque Cabral, Jéssica Silva, Juliana Farias, Luiz Henrique Menezes e Oscar Junior

Março de 2013)

Encontrado em: https://eteredes.files.wordpress.com/2015/04/tutorial_pfsense.pdf