E mais…

Se você tem exigências razoáveis para um bom servidor de firewall como um escritório ou empresa de tamanho razoável com uma quantidade normal de tráfego e desempenho com segurança, o pfSense é o ideal para você que não quer gastar mas ao mesmo tempo precisa de um programa que lhe forneça confiabilidade em suas conexões com a rede. Ele possui outros recursos interessantes caso necessite ligar dois ou mais computadores numa rede individual para tirar vantagem de processamento paralelo desses computadores.

É possível fazer um balanceamento de carga caso você esteja executando vários servidores da web ao mesmo tempo, espalhando o seu tráfego de forma uniforme para cada servidor. Isso ajudará a evitar o sobrecarregamento deles. Ele possui redundâncias para conexões, quando configurar dois firewalls com pfSense se um falhar o outro vai assumir o posto do outro automaticamente. Se você tiver várias conexões de Internet e um falhar o pfSense fará um outro link que esteja funcionando assumir a conexão também de forma automática.

O pfense possui praticamente todas as ferramentas necessárias para o seu tipo de negócio, seja ela grande ou pequena. Porém nunca deixa de perder sua essência e eficácia para ser um excelente firewall.

Funcionalidades

pfSense® inclui a maioria dos valiosos recursos de firewalls comerciais, e , em muitos casos, vai além. A seguir, uma lista de recursos disponíveis Todas as seguintes funções podem ser gerenciadas através de uma interface web, sem ter que usar linha de comando.

Além dos recursos, esta página inclui também todas as limitações do sistema. A partir da nossa experiência e as experiências de milhares de usuários, sabemos bem as limitacoes do pfSense®. Sabemos que cada pacote de software tem suas devidas limitações e é onde nós diferencia da maioria porque nos comunicamos claramente este ponto. Todas as pessoas que querem ajudar a eliminar essas limitações são bem vindas. Muitas das limitações listadas são comuns a vários firewalls de código aberto e comerciais.

Firewall

Filtragem por origem e destino IP, protocolo IP, porta de origem e destino para o tráfego TCP e UDP

Habilitação dos limites para conexões simultâneas com regras básicas.

pfSense® utiliza p0f, uma utilidade de rede avançada para a impressão digital que permite a filtragem através do sistema operacional no início da conexão

Opção para registrar ou não registrar o tráfego correspondente de cada regra.

Políticas de roteamento altamente flexíveis para selecionar o gateway nas regras básicas para o equilíbrio da solicitação, failover, múltiplos WAN, backup sobre múltiplos ADSL, etc...

Os Alias permitem a criação de nomes e de grupos de IP, de redes e portas. Estas funcionalidades ajudam a manter a aparência limpa e fácil de entender, especialmente em contextos onde existem numerosos IP públicos e vários servidores.

Capaz de fazer firewall tipo camada 2 transparente – pode conectar as interfaces e filtrar o tráfego entre elas, mesmo admitindo um firewall sem IP (embora você provavelmente vai querer um IP para fins de gestão).

Packet normalização – Descrição na documentação pf scrub. Ativado em pfSense®por padrão. É possível desativar, se necessário.

Desativar filtro – você pode desativar o filtro de firewall inteiramente se você deseja transformar pfSense® em um roteador puro.

Tabela Estado

A tabela de estado do firewall mantém informações sobre as conexões de rede abertas. pfSense® é um firewall stateful, por padrão, todas as regras são stateful.

A maioria dos firewalls têm a capacidade de controlar finamente a sua tabela de estado. pfSense® tem muitas funcionalidades que permitem um controle granular da sua tabela de estado, graças às habilidades do OpenBSD pf.

Tamanho ajustável da tabela de estado – há múltiplas instalações de produção de pfSense®que usam centenas de milhares de estados. O tamanho padrão da tabela de estado varia de acordo com a memória RAM instalada no sistema, mas pode ser aumentada em tempo real para o tamanho desejado. Cada estado tem cerca de 1 KB de memória RAM, por isso é necessário manter em mente o uso da memória ao dimensionar da sua tabela de estado. Não defini-lo arbitrariamente alta.

Regras básicas:

Limitar conexões simultâneas de cliente

Limitar estados por host

Limitar novas conexões por segundo

Definir tempo limite estado

Definir tipo de estado

Tipos de Estado – pfSense® oferece múltiplas opções para a manipulação do estado.

Manter estado – Funciona com todos os protocolos. Padrão para todas as regras

Modular estado – Funciona apenas com TCP. pfSense® irá gerar Números de Sequência Inicial (ISNs) em nome do host

Estado synproxy – proxies das conexões TCP em entrada, para ajudar a proteger os servidores de inundações de TCP SYN falsificados . Esta opção inclui a funcionalidade de manter estado e modular estado, combinadas.

Nenhum – Não mantém nenhuma entrada de estado para este tráfego. Isto é muito raramente desejável , mas está disponível porque pode ser útil em algumas circunstâncias limitadas.

Opções de otimização da tabela do estado – PF oferece quatro opções para otimização tabela de estado

Normal – O algoritmo padrão

Alta latência – Útil para links de alta latência, como conexões via satélite. Expira conexões ociosas mais tarde do que o normal

Agressivo – Expira conexões ociosas mais rapidamente. Uma utilização mais eficiente dos recursos de hardware, mas pode deixar cair conexões legítimas

Conservador – Tenta evitar o descarte de conexões legítimas à custa do aumento da utilização da memória e utilização de CPU

Network Address Translation (NAT) Conversão de endereços de rede

Nas configurações padrão todo o tráfego NAT vai para o IP WAN. Em cenários de múltiplos WAN, nas configurações padrão o tráfego NAT vai para a interface IP WAN utilizada

Avançado Outbound NAT permite que esse comportamento padrão seja desativado, e permite a criação de regras NAT (ou não NAT) muito flexível

Outband NAT

1:1 NAT para IP individuais ou sub-redes inteiras

Encaminhamento das portas, incluindo faixas e utilização de múltiplos IP públicos

NAT Reflection – NAT reflexão é possível assim que serviços podem ser acessado a partir de IP público nas redes internas

High Availability

CARP do OpenBSD permite controlar para failover de hardware. Dois ou mais firewalls podem ser configurados como um grupo de falha. Se uma interface falhar no ensino primário, ou primário ficar offline por completo, o secundário se torna ativo. O software pfSense®também inclui capacidades de sincronização de configuração, para que você faça as alterações de configuração no primário e ele automaticamente sincroniza com o firewall secundário.

pfSync garante que tabela de estado do firewall é replicada para todos failover dos

firewalls configurados. Isso significa que suas conexões existentes serão mantidas em caso de falha, o que é importante para evitar interrupções de rede.

Server Load Balancing

O servidor de balanceamento de carga é usado para distribuir a carga entre vários servidores. Isto é comumente usado com servidores web, servidores de e-mail e outros. Os servidores que não respondem a pedidos de ping ou conexões de porta TCP são removidos do grupo.

Virtual Private Network (VPN)

O software pfSense® oferece três opções para conectividade VPN : IPsec, OpenVPN, ePPTP.

IPsec

IPsec permite a conectividade com qualquer dispositivo que suporte padrão IPsec. Este é mais comumente usado para a conectividade entre site, para outras instalações pfSense, outros firewalls de código aberto (m0n0wall, etc), e na maioria das soluções de firewall comercial (Cisco, Juniper, etc.) Ele também pode ser usado para a ligação de cliente móvel.

OpenVPN

OpenVPN é uma solução flexível e poderosa de SSL VPN, que suporta uma ampla gama de clientes, em vários sistemas operativos. Veja o site do OpenVPN para obter detalhes sobre as suas habilidades.

PPTP Servidor

PPTP VPN era uma opção popular, porque quase todos os sistemas operativos tem um cliente PPTP, incluindo todas as versões do Windows desde o Windows 95 OSR2. No entanto, é agora considerado inseguro e não deve ser utilizado. Veja este artigo da Wikipédia para mais informações sobre o protocolo PPTP.

Limitações

Devido a limitações no pf NAT, quando o servidor PPTP está habilitado, os clientes PPTP não podem usar o mesmo IP público para conexões PPTP de saída. Isto significa que se você tiver apenas um IP público, e utilizar o PPTP Server, clientes PPTP dentro de sua rede não vão funcionar. A solução é usar um segundo IP público com o Advanced Outbound NAT para seus clientes internos. Veja também a limitação PPTP sob NAT nesta página.

Servidor PPPoE

O software pfSense® oferece um servidor PPPoE. Para mais informações sobre o protocolo PPPoE, consulte esta página da Wikipedia. Um banco de dados local de usuário pode ser usado para autenticação, e autenticação RADIUS com a accounting opcional também é suportado.

Relatórios e Monitoramento

RRD Graphs. Os gráficos RRD no software pfSense®mantêm informações históricas sobre o seguinte.

utilização da CPU

rendimento total

estados do Firewall

Rendimento individual para todas as interfaces

tarifas de Pacotes por segundo para todas as interfaces

Tempos de resposta de ping da Interface WAN Gateway (s)

Filas do modelador de tráfego em sistemas com modelagem de tráfego habilitados

Informações em tempo real

A informação histórica é importante, mas às vezes é mais importante ver informações em tempo real.

Os Gráficos SVG estão disponíveis e mostram taxa em tempo real para cada interface

Para os usuários do modelador de tráfego, o Estado -> tela das Filas permite a visualização de uso das filas usando medidores AJAX atualizados em tempo real.

A primeira página inclui medidores AJAX para exibição de CPU em tempo real, memória, swap e uso de disco e tamanho da tabela de estado

Dynamic DNS

Um cliente de DNS dinâmico está incluído para permitir que você registre o seu IP público com um número de prestadores de serviços de DNS dinâmico.

Personalizado – permite a definição do método de atualização para os prestadores não especificados nesta listagem aqui.

DNS-O-Matic

DynDNS

DHS

DNSexit

DyNS

EasyDNS

FreeDNS

HE.net

Loopia

Namecheap

No-IP

ODS.org

OpenDNS

Route 53

SelfHost

ZoneEdit

Um cliente também está disponível para RFC 2136 atualizador de DNS dinâmico, para uso com servidores de DNS como o BIND que suportam este meio de atualização.

Portal Captive

Captive portal permite forçar autenticação, ou o redirecionamento para um clique através da página para acesso à rede. Isto é comumente usado em redes de hot spots, mas também é amplamente usado em redes corporativas para uma camada adicional de segurança no acesso sem fio ou Internet. Para mais informações sobre a tecnologia do Captive Portal em geral, consulte o artigo da Wikipedia sobre o tema. A seguir está uma lista de características do Captive Portal pfSense®.

Máximo numero de conexões simultâneas – Limitar o número de conexões para o próprio portal por cliente IP. Este recurso evita que uma negação de serviço a partir de PCs de clientes que enviam tráfego de rede várias vezes, sem autenticação ou clicando através da página inicial.

Tempo limite de ociosidade – desconectar clientes que estão sem uso por mais do que o número definido de minutos

Forte timeout – Força a desconexão de todos os clientes após o número definido de minutos.

Logon janela pop-up – Opção para aparecer uma janela com um botão de log off.

Redirecionamento de URL – após a autenticação ou clicando através do Portal Captive, os usuários podem ser forçado ao redirecionameno da URL definida.

Filtragem MAC – por padrão, pfSense®filtra usando endereços MAC. Se você tem uma sub-rede atrás de um roteador em uma interface habilitada Portal Captive, cada máquina por trás do roteador será autorizada após um primeiro usuário é autorizado. Para esses cenários, filtragem MAC pode ser desativado.

Opções de autenticação – Há três opções de autenticação disponíveis.

Sem autenticação – Isso significa que o usuário clicará através de sua página do portal, sem introduzir as credenciais.

Gerente de usuário local – Um banco de dados de usuário local pode ser configurado e utilizado para autenticação.

Autenticação RADIUS – Este é o método de autenticação preferido para ambientes corporativos e provedores de acesso. Ele pode ser usado para autenticar a partir do Microsoft Active Directory e vários outros servidores RADIUS.

capacidades RADIUS

Forçada re-autenticação

Capaz de enviar atualizações Accounting

Autenticação RADIUS MAC permite ao Portal Captive se autenticar em um servidor RADIUS, usando o endereço MAC do cliente como nome de usuário e senha.

Permite a configuração de servidores RADIUS redundantes.

HTTP ou HTTPS – A página do portal pode ser configurada para usar HTTP ou HTTPS

Pass-through MAC e endereços IP – endereços MAC e IP pode ser autorizado para usar o portal. Todas as máquinas com NAT Port Forward precisará ser autorizado para que o tráfego de resposta não pare no portal. Você pode querer excluir algumas máquinas por outras razões.

Gerenciador de Arquivos – Isso lhe permite carregar imagens para uso em suas páginas do portal.

Limitações

Portal “reverso”, ou seja, capturar o tráfego proveniente da Internet e entrar em sua rede, isto não é possível. Somente endereços IP e MAC inteiros podem ser excluído do portal, isto não se aplica aos protocolos e nem portas individuais.

DHCP Server and Relay

O software pfSense®inclui tanto DHCP Server e funcionalidade Relay.