



Características

O Fireflex inclui a maioria das características incluídas na grande maioria dos firewalls. Abaixo segue lista de recursos disponíveis na versão 1.2, é importante falar que todas as configurações podem ser realizadas através da interface web, dispensando linhas de comando.

Funcionalidades

Firewall

- Filtragem de pacotes por IP de origem e de destino, protocolo de origem e destino, tráfego TCP, UCP, etc
- Capacidade de filtrar conexões simultâneas
- Com base no sistema BSD, trabalha com p0f, um avançado sistema de fingerprint que detecta e permite a criação de regras utilizando como parâmetro sistemas operacionais.
- Capacidade de registrar ou não logs por regras
- Simplicidade na criação e manutenção de rotas por *hosts (gateways)*, entidades de balanceamento de carga, *fail-overs* e múltiplos *links*.
- Criação de apelidos para agrupar IPs, redes e portas. Isso ajuda a manter o Firewall mais limpo e facilita no gerenciamento das regras.
- Trabalha na camada 2 do modelo OSI permitindo a criação de pontes (bridge) filtrando assim o tráfego de forma transparente para um ambiente já homologado.
- Normalização de pacotes
- Possibilidade de desabilitar filtro (caso se deseje usar apenas como roteador).

Tabela de estado

A grande maioria dos Firewalls atuais mantém uma tabela de estado (*state*) para suas conexões abertas. O Fireflex trabalha com todas suas regras em *stateful*.

Como o Fireflex trabalha com base em sistemas BSD, ele como principal característica inúmeras formas de controlar sua tabela de estados (graças ao pf - packet filter portado do OpenBSD).

- Ajuste de tamanho da tabela de estado (*state table*) de forma geral- A tabela de estado padrão é de 10.000, mais pode tranquilamente ser aumentada ajustando a sua necessidade. Para realizar o cálculo é importante mencionar que cada estado equivale a aproximadamente 1Kb de memória RAM, por isso o Fireflex vem com 512Mb de memória por padrão.
- Por regra:
 - Limite de conexão simultânea
 - Limite de estado por host

- Limite de nova conexão por segundo
- Define timeout do estado
- Define tipo do estado
- Tipos de estado – O Fireflex oferece múltiplas opções de estado.
 - Keep state – Trabalha com todos os protocolos. É padrão pra todas as regras.
 - Modulate state – Trabalha somente com TCP.
 - Synproxy state – Proxy de entrada de conexões TCP, protege servidores contra pacotes *spoofed*. Esta opção combina os tipos *keep state* e *modulate*.
 - None – Desabilita a regra na tabela de estado. Isto não é recomendável, mas está disponível para algumas circunstâncias limitadas.
- Opções de otimização para a tabela de estado – O sistema packet filter oferece quatro opções para otimização da tabela.
 - Normal – Algoritmo padrão.
 - High latency – Útil para conexões com alta latência, como conexões com satélite.
 - Aggressive – Expira conexões agressivamente da tabela de estados. Isso pode diminuir drasticamente os requisitos de memória num firewall muito carregado, o preço é o risco de se descartar conexões muito cedo
 - Conservative – Configurações extremamente conservadoras. Evita o descarte de pacotes em conexões ociosas ao custo de maior utilização de memória e pequeno aumento no processamento.

Network Address Translation (NAT)

- *Port forwards* para ranges e múltiplos IPs públicos.
- 1:1 NAT para endereços individuais ou para redes inteiras.
- Outbound NAT
 - Pela configuração padrão, é feito NAT através do IP da interface WAN.
 - Usando o Advanced Outbound NAT ele permite o desligamento desta configuração padrão, permitindo assim a criação de regras para NAT Outbound mais flexíveis.
- NAT Reflection – Em algumas configurações o NAT reflection ou binat permite o NAT estático fazendo com que as máquinas internas possam ser acessadas por IPs externos.

Limitações do NAT no Fireflex

- PPTP e GRE – Apenas uma conexão pode ser feita por servidor, ou seja, é possível conectar a 1000 servidores diferentes, mas não é possível conectar mais de um cliente no mesmo servidor. Uma alternativa pra isso é fazer um NAT por conexão, sendo necessário mais de um IP público. Uma solução pra isso já esta em desenvolvimento.
- SIP Limitation – Por padrão, todo tráfego (endereço de origem) TCP e UDP deve ser reescrito, e isso acarreta problemas como do SIP e IPSec. Uma boa solução pra isso é criar o túnel IPSec a partir do próprio Fireflex evitando assim a criação vários túneis. Quanto ao SIP, na próxima versão estará sendo implementado o pacote sipproxy que implementa o Proxy para este protocolo.

Redundância

Como trabalhamos com base em sistemas BSD, é feita a implementação do protocolo CARP e com isso conseguimos failover caso haja falha no hardware, mantendo a alta disponibilidade.

Utilizando um componente chamado *pfsync*, conseguimos manter a tabela de estado caso haja um pool de Fireflex (montando um sistema de alta disponibilidade), com ele também conseguimos manter uma copia fiel das regras e configurações de todos os firewalls do pool.

Limitações

- Só funciona com IPs estáticos, ou seja, não é possível realizar redundância com conexões DHCP, PPTP.
- São necessários três endereços IPs no mínimo.
- Failover não é instantâneo, demora cerca de 5 segundos para habilitar o backup. Durante este tempo não haverá tráfego, mas as sessões/conexões (exceto SSH e algumas conexões seguras como banckline), serão mantidas.

Balanceamento de carga (para Internet)

O balanceamento de carga é utilizado com múltiplas conexões WAN, fornece a maximização de links, podendo ser criado capacidades de failover e direcionamento de tráfegos para gateway específicos (criando QoS).

Limitações

- A distribuição de carga é feita igualmente, não é possível distribuir a carga de forma desigual.
- A verificação dos links só feita através de pacotes ICMP (ping) ou portas TCP ligadas. Não é possível a verificação de retorno de testes na porta TCP (não conseguindo interpretar se é valido ou não).

VPN

O Fireflex oferece duas opções de VPN: IPsec e PPTP.

IPsec

Esta opção permite conexão com qualquer implementação IPsec (qualquer sistema operacional ou appliance). Esta é a opção mais usada para a implementação de VPN site-to-site.

Limitação do IPsec

- O NAT-T não é suportando, ou seja, clientes móveis posicionados atrás de NAT não são suportados neste tipo de VPN, ideal para fazer túneis. Neste caso PPTP é a melhor solução.
- A ponta principal do túnel deve ter IP estático e público, somente clientes móveis ou pontas secundárias podem ter endereços dinâmicos.

- Não são suportados DPD, NAT-T e Xauth

PPTP

PPTP é uma das opções mais populares, tendo em quase todos os sistemas operacionais um cliente para acesso.

O servidor PPTP do Fireflex possui base de dados local para usuários e consulta servidores RADIUS. É possível criar regras usando a interface PPTP como origem.

Limitações do PPTP

- Devido a limitações no NAT do pf (packet filter), quando o servidor PPTP ficar ativo, os clientes não poderão sair (NAT) pelo mesmo endereço IP que ele estiver listando.

Relatório e monitoramento

Gráficos RRD

Com gráficos RRD o Fireflex mantém um histórico de:

- Utilização de CPU
- Total de throughput
- Estado do Firewall
- Throughput individual ou para todas as interfaces
- Pacotes por segundo (de todas as interfaces)

Informações em tempo real

A informação histórica é importante, mas às vezes é mais importante termos as informações em tempo real. Por isso disponibilizamos gráficos SVG para monitoramento em tempo real de interfaces de rede conectadas a links.

Para permitir um melhor monitoramento, a interface é desenvolvida em AJAX permitindo visualizar informações de disco, CPU, memória em tempo real.

Servidor DHCP

O Fireflex inclui as funcionalidades de um servidor DHCP.