

O ProApps Security

O ProApps Security é um componente da suíte de Professional Appliance focada na segurança de sua empresa ou rede. A solução pode atuar como gateway e como solução IDS/IPS no ambiente.

Os principais recursos da solução são:

- **Dashboard:** Através da tela inicial do sistema é possível adicionar widgets de controle e gerenciamento de todo o comportamento do servidor, como estatísticas de uso de memória, CPU, uso de rede, entre outros;
- **Sistema:** Toda a configuração do sistema é feita através de interface web, podendo ser definido opções de roteamento, configuração de interfaces, Vlans, grupo de interfaces, Link Agregation, acesso de usuários de forma personalizada, entre outros;
- **HA – Alta Disponibilidade IP:** De modo simples e gerenciável é possível configurar uma ou mais máquinas para trabalharem em alta disponibilidade;
- **Menu de Status:** Menu com a possibilidade de obter informações detalhadas de todos os serviços em execução no servidor. Entre eles: Gráficos RRD de consumo, tráfego de banda, status Ipv6, etc.
- **Firewall:** Opção de configuração de firewall de forma simples e efetiva, através de filtros, nateamento, controle de banda (QoS), agendamento de horários e sincronia de estado em caso de servidores trabalhando em alta disponibilidade;
- **VPN:** Suporte aos seguintes protocolos VPN: IPSec, L2TP, OpenVPN e PPTP.
- **Filtro de Conteúdo WEB:** permite fazer filtro de conteúdo de acesso a sites por horário, grupos, palavras chaves e integração do AD ou LDAP;
- **Captive Portal:** Possibilidade de implementar de forma simples e gerenciável um captive portal para fazer autenticação de usuários ou visitantes de forma controlada com integração ao filtro de conteúdo WEB. É possível ainda gerar vouchers para cada um dos usuários com tempo controlado de acesso;
- **Servidor DHCP:** Disponível configuração DHCP server para melhor gerenciamento e distribuição de endereços IPs na rede;
- **Servidor Radius:** Possibilidade de gerar uma base de usuários local para fazer autenticação baseada em radius;
- **Balanceamento de carga:** Possibilidade de fazer balanceamento de carga entre servidores;
- **Servidor NTP:** Criação e configuração de servidor NTP na rede para sincronização de horários;

- **PPPoE Server:** criação de servidor PPPoE para integração local ou com outros servidores de autenticação na rede;
- **SNMP:** Monitoramento do servidor pode ainda ser feito através de SNMP a partir de qualquer outro ativo na rede;
- **Diagnósticos:** Menu onde é possível traçar a acompanhar todo o diagnóstico dos serviços implementados, assim como efetuar alguma operações básicas administrativas, como reboot, desligar máquina, verificar rotas, entre outras.

ProApps Security – Características Técnicas

Para fins de detalhamento técnico seguem as características do produto:

Firewall (firewall por filtragem de pacotes)

- Filtragem por IP de origem e de destino; por protocolo, por portas de origem e de destino para tráfego UDP, TCP e SCTP;
- Controle de conexões simultâneas por origem, destino, porta, regra-a-regra;
- Reconhecimento passivo de sistemas operacionais para serem filtrados;
- Log seletivo por regra;
- Policy Based Routing (PBR) com flexibilidade de seleção de gateway por regra, com corpo de regra prevendo flexibilidade mínima de protocolo, porta, origem e destino; PBR suportando balanceamento de carga, failover, multiplas WAN;
- Agrupamento de hosts por IP, por nome, redes e portas para gerar regras;
- Filtro de camada OSI 2 transparente, em modo de operação *bridge*, para sistemas de firewall sem IP e sem roteamento (transparente, *bright* firewall);
- Normalização de pacotes filtrando ambiguidades, inconformidades e fragmentação errônea de pacotes além de remontagem de pacotes;
- Desligamento completo de firewall para o caso de operação em modo apenas roteamento;
- Firewall Stateful;
- Firewall Stateful com *Deep Inspection*;
- Opção de gerar regras Stateless por regra;

- Habilidade de controle fino de estados de firewall filtrados;
- Número máximo de states configurável; máximo de 4KB de memória por estado sendo filtrado em modo *Deep Inspection Stateful*; suportando portanto no mínimo 500.000 sessões;
- Limite configurável de conexões simultâneas por regra;
- Limite configurável de estados por host por regra;
- Limite configurável de novas conexões por segundo;
- Limite configurável de timeout de estados;
- Limite configurável de tipo de estado;
- Tipos de estado suportado mínimos por regra: stateful, deep inspection, synproxy;
- Pelo menos 2 tipos de otimização de tabela de estado priorizando controle ou priorizando economia de recursos;

NAT (Network Address Translation)

- Redirecionamento de portas, suportando intervalos e uso de múltiplos IP na WAN;
- NAT 1:1 individual e (opcionalmente) subredes;
- NAT de saída seletivo;
- NAT inverso, permitindo serviços sendo acessados pelo IP público da interface de rede LAN ao invés de WAN;

Redundância IP

- Protocolo de redundância de endereço IP baseado em grupos multicast, similar ou compatível com VRRP da Cisco;
- Sincronia plena de estados de firewall garantindo que sistemas de firewall redundante possam assumir o firewall principal em caso de falha sem prejuízo das sessões ativas (0 downtime);

Balanceamento de Carga

- Balanceamento de Saída: balanceia o consumo de banda em múltiplas WAN, permitindo balanceamento de carga de saída por sessão e também prevendo redundância tipo failover; suporte a gateway seletivo ou *pool* de balanceamento por regra individual de firewall;
- Balanceamento de Entrada: permitindo a distribuição de carga entre diversos servidores na DMZ, com os

mesmos recursos de redundância e disponibilidade do balanceamento de saída;

Concentrador VPN (Virtual Private Network)

- Suporte a VPN tipo IPSec compatível com Cisco e Juniper;
- Suporte a VPN tipo OpenVPN;
- Suporte a VPN tipo PPTP com suporte a servidor Radius;

Servidor PPPoE

- Com suporte a autenticação local e autenticação em servidor RADIUS remoto;
- Com suporte a *accounting* em servidor RADIUS remoto;

Relatório Gráfico no mínimo diário, semanal, e intraday, prevendo:

- Consumo de CPU;
- Vazão total de bits por segundo;
- Estados totais de firewall;
- Vazão individual de bps por interfaces;
- Vazão individual de pps por interfaces;
- Tempo de resposta icmp dos gateway WAN;
- Filas de Controle de Banda;

Controle de Banda:

- Controle de banda por regra, usando no mínimo as disciplinas CBQ e PRIORITY ou opcionalmente WFQ em alternativa a PRIORITY.

Monitoração de Atividades

- Informações em tempo real prevendo no mínimo:
 - CPU
 - Memória
 - Swap
 - Consumo de disco

- Tráfego de controle de banda
- Estados de firewall;

Captive Portal suportando no mínimo os seguintes recursos:

- Número máximo de conexões simultâneas;
- Tempo de inatividade para timeout;
- Janela pop-up de logon;
- Redirecionamento de URL;
- Autenticação local, RADIUS ou sem autenticação;
- Suporte HTTP e HTTPS;
- Suporte a Whitelist por IP que nunca cairão no Captive Portal;

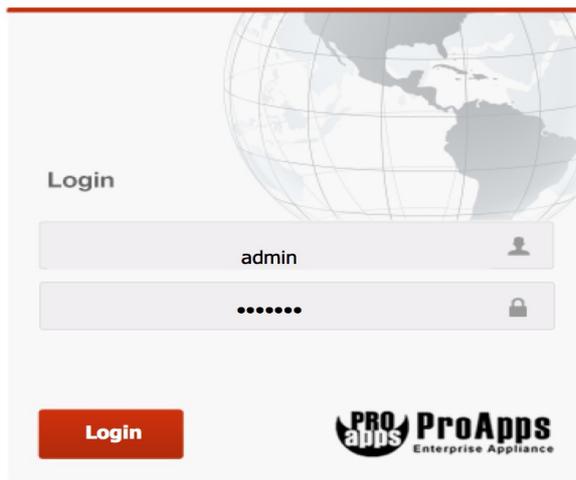
Outros recursos

- WoL (Wake on Lan) suportado pelo sistema;
- Acesso a console/terminal de comando por ssh para operações avançadas e diagnóstico quando a interface visual não estiver disponível;
- Filtro de Conteúdo por horário, grupo, palavra-chave e integração do AD ou LDAP;
- IDS/IPS com relatórios de alertas e regras de bloqueio configuráveis.
- Servidor DHCP e Relay DHCP plenamente configuráveis para IPv4 no mínimo;
- Recursos de diagnóstico mínimos: ping, traceroute, captura de pacote (sniffing);

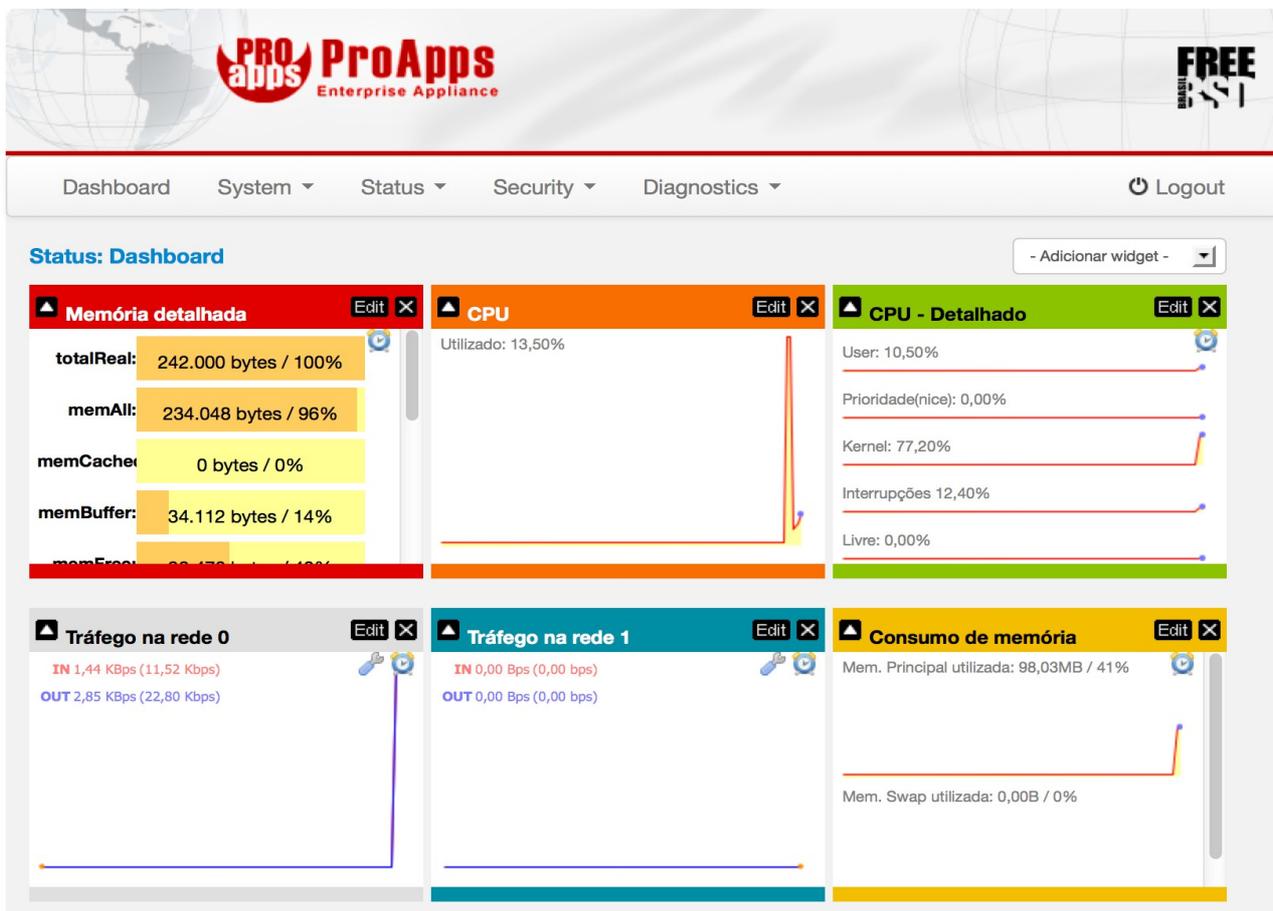
ProApps Security – Screenshots

A gestão de serviços via ProApps Security é muito mais simples, acompanhe abaixo algumas telas do produto:

- **Login**



- **Dashboard**



• Acesso aos recursos do Appliance

The screenshot displays the ProApps Enterprise Appliance web interface. At the top, there is a navigation bar with tabs for Dashboard, System, Status, Security, and Diagnostics. The Security menu is expanded, showing options like Firewall, VPN, IPS/IDS, Web Filter, Services, Aliases, NAT, Rules, Schedules, Traffic Shaper, and Virtual IPs. Below the navigation, there are several widgets: 'Memória detalhada' showing memory usage for totalReal, memAll, memCache, memBuffer, and memFree; 'Tráfego na rede 0' and 'Tráfego na rede 1' showing network traffic; and 'Consumo de memória' showing memory usage for Mem. Principal and Mem. Swap. The interface also includes a 'Logout' button and a '+ Adicionar widget -' dropdown.