

## A SEGURANÇA CIBERNÉTICA DO DIAGNÓSTICO À DEFESA



Pronto para realizar a prevenção e proteção completa de perímetro de rede, o OGA AKER UTM 438 Series são appliances que entregam funcionalidades *next generation* para pequenas empresas e escritórios distribuídos, com simples gestão e alta capacidade de processamento.

### PREVENÇÃO | PROTEÇÃO

#### FIREWALL

- Modos de operação: Router e Bridge;
- Suporte a gateway de sessão: FTP, PPTP, H323, SIP, DCE-RPC, RTSP, Real Audio;
- Filtro de pacote Stateful;
- NAT (por Origem, Destino, Porta e Estático).

#### IPS/IDS

- Assinaturas por ataques/vulnerabilidades conhecidas;
- Assinaturas por padrão de comportamento;
- Atualização automática de assinaturas
- Proteção contra DOS;
- Proteção contra pacotes malformados;
- Proteção contra anomalia de protocolos.

#### ANTIVÍRUS

- Proteção HTTP/FTP/SMTP/POP3/IMAP;
- Atualização automática;
- Suporte a análise heurística;
- Assinaturas de Malware Kaspersky ou ClamAV.



#### CONTROLE SMTP

- Filtro RBL;
- Filtro bayesiano;
- Filtro de anexo por nome, extensão e tipo MIME;
- Filtro customizável por conteúdo do corpo e cabeçalho;
- Checagem de DNS Reverso;
- Suporte à análise de antivírus;
- Suporte ao envio de cópia de mensagem.

#### VPN

- IPSec (IKEv1/IKEv2);
- OpenVPN;
- L2TP;
- PPTP;
- Secure Roaming;
- VPN-SSL.

#### SERVIÇOS DE REDE

- Roteamento dinâmico (OSPF, BGP4, RIPv2);
- Roteamento estático;
- Balanceamento de link;
- Serviços integrados DHCP, DNS Server (consulta recursiva);
- VLAN (802.1q);
- Multicast: DVMRP e PIM.

#### CONTROLE IMAP/POP3

- Filtro de anexo por nome, extensão e tipo MIME;
- Suporte à análise de antivírus;
- Suporte ao envio de cópia de mensagem.

Throughput (Mbps)

1.300

Throughput VPN (3DES | DES |  
AES | Blowfish) (Mbps)

135/234/446/351

Throughput OpenVPN  
(Blowfish) (Mbps)

170

Throughput IPS (Mbps)

240

## GESTÃO | DASHBOARDS

- Informações atualizadas automaticamente;
- Dashboard personalizável e layout responsivo;
- Interface amigável e suporte em português.

**Informações de saúde:**

- Utilização de recursos de hardware;
- Status dos agentes externos (itens de subscription e base de autenticação externa);
- Status das interfaces de rede;
- Gráfico de utilização do filtro Web.

**Visibilidade de rede:**

- Gráfico das conexões ativas;
- Gráfico de consumo de banda por interface;
- Gráfico de throughput global;
- Top conexões aceitas e rejeitadas;
- Clientes DHCP;
- Conexões VPN IPSec.

**Visibilidade de ameaças:**

- IPs bloqueados por atividade suspeita;
- Top ataques bloqueados;
- Top ataques detectados.

**Monitoramento dos usuários:**

- Sessões web ativas por usuário;
- Top URLs e categorias aceitas e rejeitadas;
- Top aplicações detectadas e rejeitadas;
- Visibilidade e gerenciamento dos usuários autenticados;
- Visibilidade e gerenciamento de cotas de uso de banda.

## RELATÓRIOS GERENCIAIS CUSTOMIZADOS

Os relatórios gerenciais apresentam um resumo executivo das principais atividades de rede do ambiente controlado, tais como:

- Filtragem de pacotes;
- Atividade web dos usuários;
- Utilização de aplicativos indevidos;
- Controle de e-mails indesejados;
- Detecção de arquivos infectados;
- Detecção de acessos maliciosos.

## MAIOR SEGURANÇA PARA A SUA REDE

**FILTRO DE CONTEÚDO WEB**

- Filtro de conteúdo por categoria de URL, palavras chaves e expressão regular;
- Filtro de anexo por extensão e tipo MIME;
- Suporte à análise de antivírus Kaspersky ou ClamAV;
- Suporte a redirecionamento para página de bloqueio;
- Filtro HTTPS Ativo e transparente (com ou sem inspeção SSL);
- Atualização automática de base de URLs;
- Bloqueio Java, JavaScript, ActiveX e Banner;
- Suporte à controle de banda, cota de tempo e volume granular por categoria e expressão de URL.

## FILTRO DE APLICAÇÕES

Controle o acesso a aplicações como Skype, Torrent, TOR, Streaming de vídeo, entre outras. A tecnologia DPI (Deep Packet Inspection/inspeção profunda de pacotes), proporciona recursos avançados de segurança e filtragem de dados, o que torna possível bloquear aplicativos peer-to-peer, como Torrents e evitar que a rede da sua empresa seja utilizada para fins pessoais.

## SD-WAN

Possibilita criar várias conexões seguras entre a matriz e as filiais da sua rede corporativa, além de reduzir custos com links dedicados, estabelecendo VPNs entre o OGA AKER UTM e outros que suportem os padrões OpenVPN e IPsec. Com este recurso ainda é possível balancear o tráfego de duas VPNs e configurar rotas seguras automaticamente, caso o link de internet principal fique inativo.

## DISPONIBILIDADE | PERFORMANCE

### BALANCEAMENTO DE LINK INTELIGENTE

O OGA AKER UTM possui balanceamento de link por política através de 4 modos:

- Link Failover;
- Porcentagem;
- Conexões;
- Performance TCP.

### CLUSTER

O OGA AKER UTM permite clusterização com até 64 firewalls paralelos. Ao conectar dois firewalls à rede e replicar suas configurações, é possível manter sua rede segura 24 horas por dia e realizar a substituição imediata caso um deles pare de funcionar, sem afetar o desempenho da sua rede e sem perda de informações.

### LINK AGGREGATION

Com este protocolo é possível criar uma forma padronizada para agrupar múltiplos links entre ativos (equipamentos de camada 2) fazendo que estes se comportem como se fossem um único link, aumentando a capacidade de transferência de dados (throughput de rede) do link na comunicação. A técnica de Link Aggregation fornece ainda redundância caso um dos links venha a falhar.

### TECNOLOGIAS WIRELESS

O OGA AKER UTM vem com tecnologias de conectividade sem fio capazes de proteger e expandir a capacidade da rede wireless existente.

- WIDS (Wireless Intrusion Detection System);
- WDS (Wireless Distribution System).

## SPOTLIGHT



1. Botão Reset
2. Antenas Wireless (inclusas apenas no 438W)
3. Botão On / Off
4. Fonte de energia
5. Porta console RJ45
6. LEDs: On-Off / Bypass / armazenamento
7. 2 x Portas USB
8. 6 x Portas LAN RJ45 1 GBE



## CARACTERÍSTICAS

## MODELO 438 SERIES

Conexões simultâneas <sup>(1)</sup>	250.000
Conexões por segundo <sup>(1)</sup>	12.000
Velocidade UTM (HTTP/HTTP+AV/HTTPS) <sup>(1)(3)</sup>	400/250/100
Throughput (Mbps) <sup>(1)(2)</sup>	1.300
Throughput VPN (3DES/DES/AES/Blowfish) (Mbps) <sup>(1)(2)</sup>	135/234/446/351
Throughput OpenVPN (Blowfish) (Mbps) <sup>(1)(2)</sup>	170
Throughput IPS (Mbps) <sup>(1)(2)</sup>	240
Nº de túneis VPN <sup>(1)</sup>	400

## LICENCIAMENTO INCLUSO

IPs	Ilimitado
Cluster	HA (ativo-passivo)
Roaming / VPN SSL	5
Balanceamento de servidores	Sim
Balanceamento de links	Sim

## CARACTERÍSTICAS DE HARDWARE

USB (data / serial / 3G)	2 portas
Serial (DB9 / RJ45 / compatível)	Sim
LED de Atividade (rede, disco, ligado / desligado)	Sim
Placa de rede RJ45– LAN	6 (4x UTP 1GBE + 2x UTP 1GBE Bypass)
Placa de rede Wireless (a / b / g / n) <sup>(7)</sup>	Sim, modelo 438W
Memória RAM (GB) <sup>(3)</sup>	4
Armazenamento interno	HDD 320GB ou SSD 120 GB
Fonte de alimentação bivolt	Externa automática

## DIMENSÕES E DETALHAMENTO FÍSICO

Característica física	Desktop
Altura, largura, comprimento (cm)	4,4 x 14,55 x 17,7
Peso (Kg)	1,2
MTBF (Mean Time Between Failures)	80.000
Consumo máximo	60W
Temperatura de operação	0 - 40°C
Umidade de operação	5% - 90%

PLANO DE MANUTENÇÃO INCLUSO <sup>(4)</sup>

Base de antispam (ASM)	Anual
Base de IDS/IPS	Anual

Base de filtro de conteúdo Web	Anual
Base de antivírus	Anual

### GARANTIA E ATUALIZAÇÃO

Garantia estendida <sup>(5)</sup>	Anual
Plano de atualização de Firmware <sup>(6)</sup>	Anual

1- Valores máximos levantados em laboratório com otimização do produto. Outras variáveis como tipo de tráfego ou tipo de uso do sistema podem alterar este valor.

2- Tráfego de entrada e saída somados.

3- Valores médios de uso padrão do produto. Maior uso simultâneo de proxies pode exigir maiores valores de memória.

4- Licença de uso de software com obrigatoriedade de renovação anual.

5- Tempo máximo total de garantia é de 36 meses.

6- Refere-se apenas à parte de softwares do produto.

7 - Módulo Wireless AP - 2.4/5GHz 802.11a/b/g/n - até 350mW de potência

Personalização: Os modelos acima são padrões de fornecimento. Placas WAN, Aceleradores VPN, aceleradores em geral, VOIP ou outros dispositivos, podem ser integrados nos equipamentos de acordo com a necessidade e disponibilidade do projeto.