OGA IPS

IPS/IDS

OGASEC

AKER N-STALKER

Sistema de Prevenção de Intrusão

PROTEÇÃO AVANÇADA CONTRA AMEAÇAS VIRTUAIS

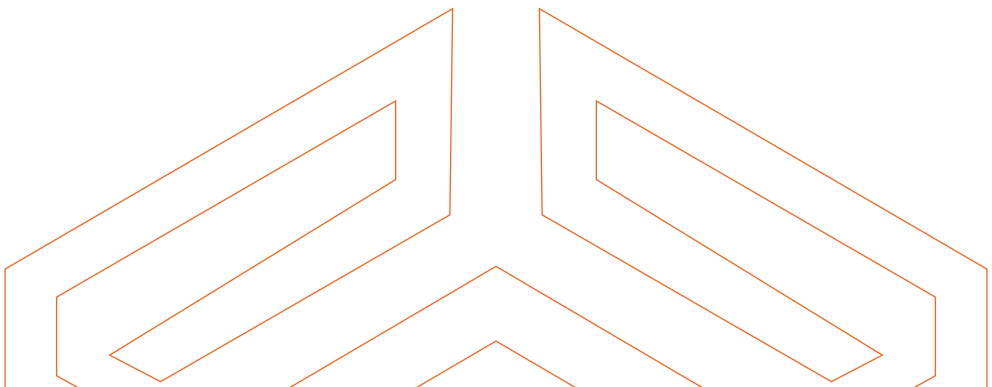
Um sistema de segurança avançado que oferece proteção contra ameaças virtuais. Conta com uma série de funcionalidades de detecção e proteção, além de processamento dedicado para a segurança de redes, dispositivos e aplicações, com uma arquitetura moderna e eficiente mantendo o desempenho até mesmo nos maiores data centers. Funcionalidades avançadas e processos operacionais possibilitam aos profissionais de segurança, mais tempo para se concentrarem em outras necessidades da área de segurança.

A indústria de malware evoluiu muito nos últimos anos e a segurança da informação tem sido cada vez mais discutida por corporações. Neste período grandes ameaças deixaram a sua marca, como o Worm Morris no final dos anos 80, Michelangelo nos anos 90, Loveletter também conhecido como Iloveyou em 2000, até o presente momento com ameaças que também fizeram história, como o WannaCryptor.

No decorrer desses anos houve uma crescente ação de malwares na procura de obter informações e sequestro de dados, softwares maliciosos a cada dia se aperfeiçoam para burlar os sistemas de segurança, com isso as organizações precisam estar preocupadas com a segurança contra esses ataques sofisticados, nessa linha de raciocínio a OGASEC desenvolveu um sistema de Detecção e/ou Proteção contra esses comportamentos.

PORQUE OGA IPS

- Detecta e bloqueia rapidamente as ameaças para proteger aplicativos e dados da sua organização;
- Solução expansível e de alto desempenho para ambientes dinâmicos;
- Gerenciamento centralizado para visibilidade e controle;
- Detecção avançada, incluindo análise de anomalias de ativos e aplicações;
- Decriptografia de conteúdo SSL de entrada e saída para inspecionar o tráfego de rede[1].



PROTEÇÃO AVANÇADA

Os sistemas de IPS possuem assinaturas baseadas em vulnerabilidades conhecidas de uma dada aplicação muitas delas são baseadas em comportamento da aplicação e/ou protocolo de rede, já outras assinaturas inspecionam por padrões comumente presentes em um comportamento afim de detectar e proteger contra anomalias, sendo assim permitindo detectar ataques zero day, tendo maior assertividade quando esse novo ataque é uma variação de um ataque já observado, possibilitando que assinaturas de ataques conhecidos tenham sucesso na detecção de ataques novos. A Solução de OGA IPS funciona de forma eficiente evitando a degradação do desempenho da rede, sua ação rápida na detecção e/ou proteção das ameaças que acontecem em tempo real toma ações de proteção evitando a perda de dados. Também detecta e responde com precisão, de modo a eliminar os falsos positivos (pacotes legítimos interpretados como ameaças).

SEGURANÇA INTEGRADA

Além dos relatórios e a possibilidade de customização dos mesmo o manager OGA IPS integra-se com um sistema de de centralizador de logs e eventos atendendo as normas de segurança da informação. OGA Report Center, armazena as informações por longos períodos e combina análise detalhada e geração de relatórios.

DESEMPENHO E DISPONIBILIDADE

O OGA IPS Sensor possui engines de segurança em alto desempenho. Ele combina uma arquitetura de inspeção de passagem única com um hardware específico e extremamente confiável, evitando lentidão ou atrasos ocasionados por sobrecargas, proporcionando inspeção em situações reais em uma linha de produtos para pequenas, medias e grandes empresas. O OGA IPS Sensor conta com uma linha de hardware totalmente dimensionado para tratar com prioridade a operação da rede, um hardware totalmente moldado para atender aos níveis mínimos de disponibilidades, oferecendo failover de fluxos de proteção de rede.

VISIBILIDADE E CONTROLE

Com o OGA IPS Manager tenha as melhores informações em tempo real para tomar decisões sobre ameaças e informações de aplicações. A solução de OGA IPS conta com módulos de reconhecimento de aplicações, dando visibilidade na camada 7 com uma base de aplicações reconhecidas.

GERENCIAMENTO CENTRALIZADO E INTELIGENTE

A solução OGA IPS aproveita a tecnologia possibilitando o gerenciamento centralizado com mais segurança a partir do OGA IPS Manager, gerenciando, atualizando e centralizando todos os alertas dos seu parque de OGA IPS Sensor, oferecendo o gerenciamento totalmente intuitivo, amigável e reponsivo em sua plataforma baseado na web.

RECURSOS

OGASEC IPS SENSOR

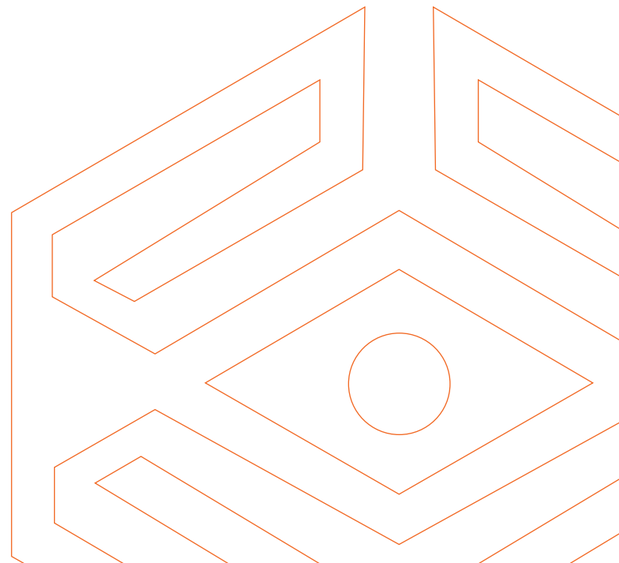
- Decriptografia de entrada SSL[1]
- Decriptografia de saída SSL[1]
- Proteção avançada contra evasão
- Detecção heurística de bots
- Banco de dados de comando e controle
- Detecção de aplicações (DPI).
- Prevenção avançada de intrusões
- Desfragmentação de IP e remontagem de fluxo TCP
- Suporte nativo para assinaturas do Snort
- Aperfeiçoamentos de listas negras e listas brancas
- Quarentena de host
- Prevenção de DoS e DDoS
- Detecção com base em heurística
- Detecção de ataques Zero-day
- Reputação de IPs
- Reputação de aplicativos e protocolos
- Geolocalização
- By-pass de interface física
- IPv6
- Túneis V4 em V4, V4 em V6, V6 em V4 e V6 em V6
- MPLS
- GRE
- VLAN

[1] Módulo adicional de hardware para a decriptação de SSL.

[2] O hardware dedicado para o gerenciamento centralizado estará condicionado a quantidade de sensores a serem gerenciados, podendo assim atender de pequenas a grandes infraestruturas baseando-se nos modelos de IPS Sensor.

OGA IPS MANAGER

- Gerenciamento centralizado via interface web com atualização, configurações e etc[2]
- Autenticação de usuário via LDAP
- Recuperação de desastres com dados de configurações essenciais
- O dashboard responsivo
- Atualizações centralizadas
- Relatórios customizados
- Comunicação totalmente segura com o OGA IPS Manager
- Exportação de relatórios em CVS, PDF, HTML
- Analise e exportação de pacotes capturados no formato PCAP



CARACTERÍSTICAS	MODELO 1000	MODELO 3000	MODELO 5000	MODELO 10000
Conexões simultâneas	4.500.000	9.500.000	12.000.000	15.000.000
Throughput IPS (Mbps)	1000	3000	5000	10000
Throughput SSL [1]	-	-	-	-
Interface bypass	Sim	Sim	Sim	Sim
LICENCIAMENTO INCLUSO				
Gerência centralizada	Sim	Sim	Sim	Sim
Atualização de base IPS/IDS	Sim	Sim	Sim	Sim
Atualização de base DPI (Deep Packt Inspection)	Sim	Sim	Sim	Sim
Módulo IPS	Sim	Sim	Sim	Sim
Módulo IDS	Sim	Sim	Sim	Sim
Aplicativo	+3mil	+3mil	+3mil	+3mil
CARACTERÍSTICAS DE HARDWARE				
Placa de rede RJ45 (100 / 1000)	8	4	8	8
Placa de rede SFP 10 Gbps	Não	Não	8	8
USB (data / serial / 3G)	2 portas			
Serial (DB9/RJ45/compatível)	Sim	Sim	Sim	Sim
LED de Atividades (Rede, Disco, Ligado / Desligado)	Incluso	Incluso	Incluso	Incluso
Memória RAM (GB)	8	16	32	32
Armazenamento Interno	SSD 240 GB	SSD 600 GB	SSD 512 GB	SSD 512 GB
Fonte de Alimentação	Interna automática	Interna automática Redundante Hot-swapping	Interna automática Redundante Hot-swapping	Interna automática Redundante Hot-swapping
DIMENSÕES E DETALHAMENTO FÍSICO				
Características Físicas	1U para rack 19"	1U para rack 19"	2U para rack 19	2U para rack 19
Altura, Largura, Comprimento (cm)	4,4/43/39,2	4,38/43,1/54,87	8,77/44,4/60	8,77/44,4/60
Peso (Kg)	8,5	17	23	23
MTBF (Mean Time Between Failures)	95.000	95.000	95.000	95.000
Consumo Máximo	270W	270W	600W	600W
Temperatura de Operação	0 - 40°C	0 - 40°C	0 - 40°C	0 - 40°C
Umidade	10% - 95%	5% - 95%	5% - 95%	5% - 95%
GARANTIA E ATUALIZAÇÃO				
Garantia Estendida	Anual	Anual	Anual	Anual
Plano de Atualização de Firmware	Anual	Anual	Anual	Anual

HARDWARES

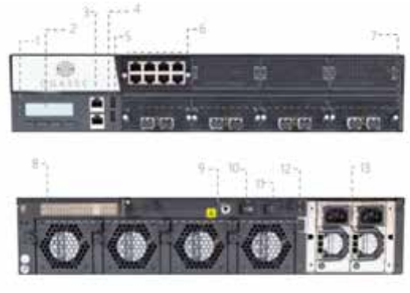
OGA IPS 1000

1. LEDs: On-Off / Bypass / armazenamento
2. Tela LCD
3. Botão reset
4. Porta console RJ45
5. 2 x Portas USB
6. 8 x Portas LAN RJ45 1 GBE
7. Slot de expansão PCI-e
8. Saída VGA
9. Botão On / Off
10. Módulo de ventilação
11. Fonte de energia

OGA IPS 3000

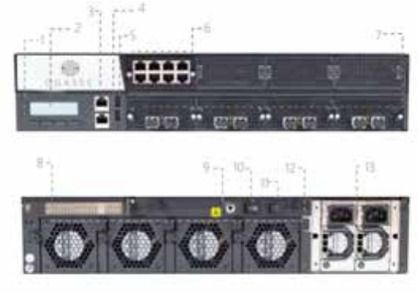
1. LEDs: On-Off / Bypass / armazenamento
2. Tela LCD
3. Porta de gerenciamento RJ45
4. Porta console RJ45
5. 2 x Portas USB
6. Botão reset
7. 12 Portas LAN RJ45 1 GGE
8. Módulo de ventilação
9. Aterramento eletrostático
10. Slot de expansão PCI-e
11. Saída VGA
12. Botão On / Off
13. Switch de alarme de fonte redundante
14. Fonte redundante de energia

OGA IPS 5000



1. LEDs: On-Off / Bypass / armazenamento
2. Tela LCD
3. Porta de gerenciamento RJ45
4. Porta console RJ45
5. 2 x Portas USB
6. 8 x Portas LAN RJ45 1 GBE
7. 8 x Portas SFP + 10 GBE
8. Slot de expansão PCI-e
9. Aterramento eletrostático
10. Botão On / Off
11. Switch de alarme de fonte redundante
12. Módulo de ventilação
13. Fonte redundante de energia

OGA IPS 10000



1. LEDs: On-Off / Bypass / armazenamento
2. Tela LCD
3. Porta de gerenciamento RJ45
4. Porta console RJ45
5. 2 x Portas USB
6. 8 x Portas LAN RJ45 1 GBE
7. 8 x Portas SFP + 10 GBE
8. Slot de expansão PCI-e
9. Aterramento eletrostático
10. Botão On / Off
11. Switch de alarme de fonte redundante
12. Módulo de ventilação
13. Fonte redundante de energia

OGASEC

AKER N-STALKER

www.ogasec.com