FIREWALL AVANÇADO
/ ficha técnica

oni
a gigas group company

FIREWALL AVANÇADO FORTIGATE

A ONI incorpora no seu Cloud Datacenter Tecnologia Fortinet, fabricante líder em soluções avançadas de segurança de perímetro com experiência comprovada na proteção da informação, controlo, inspeção e gestão multi camada do tráfego em rigoroso cumprimento com as exigências das maiores corporações.

Firewall Avançado fornece aos utilizadores do Cloud DataCenter uma solução de segurança abrangente, sobre o Fortigate VM, que resolve as necessidades operacionais de proteção, controlo de informação e acesso aos recursos da Cloud. Além de garantir uma integração segura do ambiente cloud com as plataformas originais dos utilizadores e as suas necessidades de mobilidade, a Firewall Avançado simplifica a gestão das suas políticas de segurança específicas, a partir de uma gestão multiplataforma centralizada e abrangente.

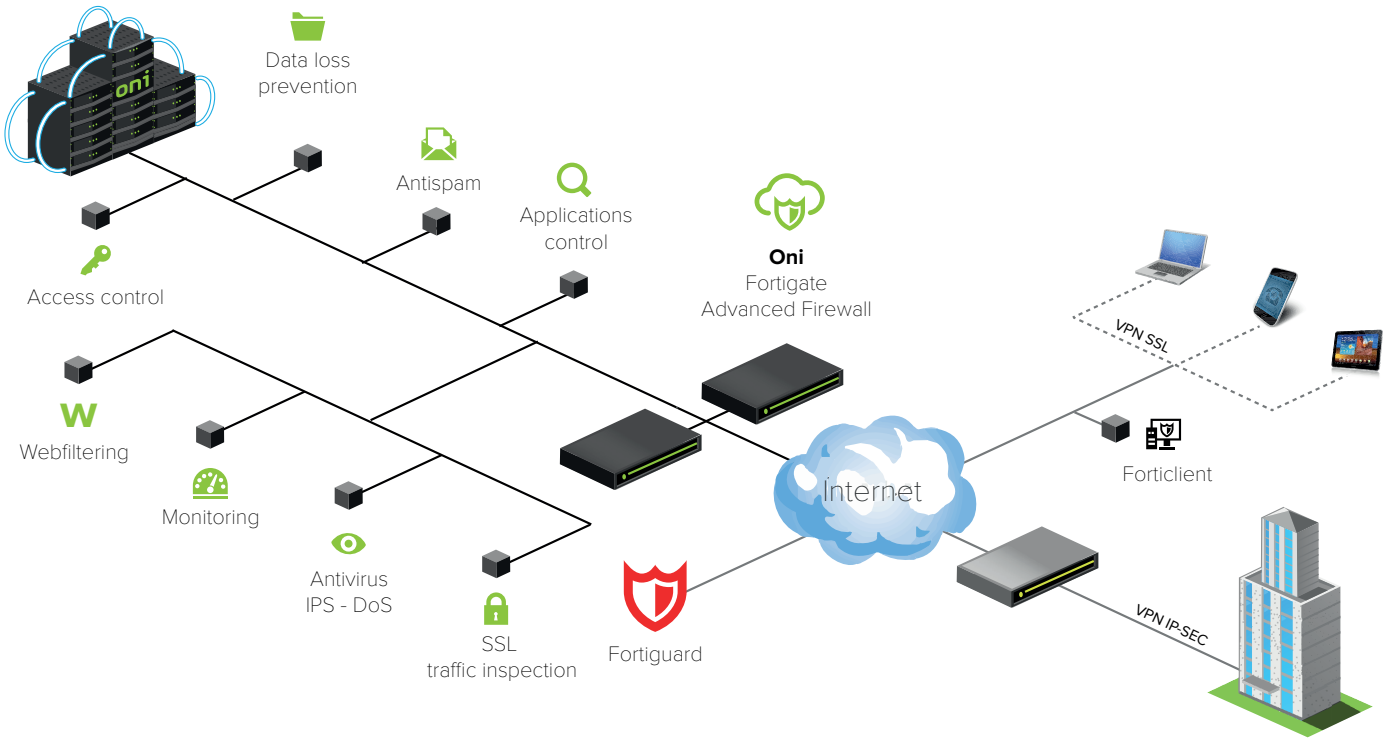
A ONI tem a sua própria equipa de engenharia, disponível para os nossos clientes 24 horas por dia, 365 dias por ano, que, além de garantir o bom funcionamento da plataforma, livre de ameaças e intrusões que possam interferir com a qualidade dos nossos serviços, podem assumir a gestão delegada do Firewall Avançado que os nossos clientes necessitam.

A ONI oferece testes gratuitos da sua Firewall. Se estiver interessado, envie um email para business@oni.pt

BENEFICIOS

- **Proteção total da rede e Informação**
- **Instalação imediata**
- **Utilização eficiente dos recursos**
- **Mais Inteligência:"Smart policies"**
- **Tecnologia lider**
- **Testes gratuitos**

FORTINET



MÓDULOS

Módulo Firewall
A tecnologia Fortinet Firewall fornece inspeções de tráfego multicamadas de uma gestão abrangente de soluções com elevadas capacidades de segurança. Combina motores para controlo de aplicações, antivírus, IPS, filtragem web, anti spam e VPN, juntamente com funcionalidades avançadas, como uma base de dados de ameaças com atualizações automáticas, gestão de vulnerabilidades e uma inspeção baseada em fluxos, para identificar e mitigar as mais recentes e complexas ameaças.
O sistema operativo FortiOS é criado para inspeção e identificação de malware.

Características:
- NAT, PAT e Transparente (Bridge)
- NAT basado em políticas
- SIP/H.323/SCCP NAT Transversal
- VLAN Tagging (802.1Q)
- Gestão de vulnerabilidades
- Suporta IPv6

Módulo de Controlo de acessos Endpoint NAC
Este módulo pode forçar o uso de políticas de segurança em utilizadores ligados à sua rede corporativa. O módulo verifica a instalação, operações de firewall e atualizações de assinaturas de antivírus, antes de permitir o acesso à rede de novos clientes. Permite-lhe colocar em quarentena servidores com aplicações que não cumprem as normas de segurança.

Características:
- Monitorização e controlo de servidores funcionando com FortiClient
- Scanning de vulnerabilidades de Nós de Rede
- Portal de Quarentena
- Controlo e Deteção de aplicações
- Base de dados de aplicações predefinidas

Módulo Antivirus / Antispyware
A tecnologia de inspeção de conteúdo antivírus protege contra vírus, spyware, worms e outros tipos de malware que podem infetar a infraestrutura de rede e dispositivos dos utilizadores. Ao intercetar e inspecionar o tráfego e o conteúdo na Camada 7, a proteção antivírus garante que ameaças maliciosas e ocultas ao nível da aplicação sejam identificadas e removidas do fluxo de dados, antes que possam causar danos. O serviço de subscrição FortiGuard garante que os dispositivos estão atualizados com as mais recentes assinaturas de malware para altos níveis de deteção e atenuação.

Características:
- Atualizações automáticas das Bases de Dados
- Antivirus baseado em Proxy
- Antivirus baseado em Fluxos
- Repositório de Quarentena
- Suporta IPv6

Módulo de Prevenção de Intrusão IPS
A tecnologia IPS protege contra ameaças atuais e emergentes. Além da deteção fiável de ameaças, o IPS realiza a deteção de anomalias que alertam os utilizadores para qualquer tráfego que corresponda aos perfis de comportamento de ataque. A equipa de pesquisa de ameaças de Fortinet analisa comportamentos suspeitos, classifica ameaças emergentes e gera novas assinaturas para incluir nas atualizações do FortiGuard.

Características:
- Atualizações automáticas das bases de dados
- Suporta Anomalias protocolares
- Sensor de Prevenção IPS e DoS
- Suporta a Personalização de empresas
- Suporta IPv6

Módulo de Otimização WAN
A otimização do WAN destina-se a acelerar as aplicações através de redes geograficamente dispersas, garantindo simultaneamente uma inspeção multi-ameaça de todo o tráfego de core da rede. A otimização wan elimina tráfego desnecessário e malicioso, otimiza o tráfego legítimo e reduz a quantidade de largura de banda necessária para transmitir dados entre aplicações e servidores. Melhor desempenho, redução da largura de banda e otimização dos requisitos de utilização e infraestrutura dos recursos, para um maior controlo e poupança de gastos associados.

Características:
- Otimização ponto a ponto
- Otimização bidireccional cliente-servidor
- Web Cache
- Túnel seguro
- Modo transparente

Módulo de Gestão de Conexões VPN
A tecnologia Fortinet VPN fornece comunicações seguras entre várias redes e servidores, utilizando tecnologias SSL e IPsec VPN. Os serviços da FortiGate VPN são o complemento perfeito para completar a inspeção de conteúdos e a prevenção de proteção e intrusão em áreas privadas da rede. O módulo de gestão de ligação VPN permite definir políticas QoS com as quais prioriza perfis críticos de tráfego em comunicações que circulam através de túneis VPN.

Características:
- IPSec e VPN SSL
- DES, 3DES, AES e Autenticação SHA-1/MD5
- PPTP, L2TP, VPN PassThrough
- SSL Single Sign-on
- 2FA, Autenticação de Duplo Factor

Módulo de Inspeção de Tráfego Encriptado-SSL
A inspeção de tráfego encriptado-SSL protege de ameaças ocultas aos clientes finais, bem como servidores web e de aplicações. A inspeção SSL intercepta o tráfego encriptado e inspeciona as ameaças antes de encaminhá-las para o seu destino final. Pode ser aplicado ao tráfego SSL orientado para o cliente, bem como, por exemplo, aos utilizadores que gostariam de se conectar a um site de CRM baseado no Cloud, ou a todo o tráfego de entrada de servidores e aplicações web.
A funcionalidade de inspeção SSL permite-lhe impor o uso de políticas apropriadas em conteúdos web encriptados e proteger os servidores de ameaças que possam estar escondidas dentro do fluxo de tráfego encriptado.

Características:
- Suporta protocolos: HTTPS, SMTPS, POP3S, IMAPS
- Suporta Inspeção: Antivirus, Filtros Web, Antispam, Prevenção de perda de Dados, Terminadores SSL

Módulo de Prevenção da Perda de Dados (DLP)
A DLP utiliza um sofisticado motor de padrões para identificar e impedir a transferência de informação sensível fora do perímetro da sua rede, mesmo quando as aplicações encriptam as suas comunicações. Além de proteger dados críticos de organizações, o DLP fornece rastreio de registos para ajudar a garantir cumprimento da politica. O utilizador pode selecionar uma vasta gama de ações configuráveis para registar, bloquear e arquivar dados, e pôr em quarentena ou proibir os utilizadores.

Características:
- Controlo e Identificação sobre dados em movimento
- Base de dados de padrões pré-definidos
- Motor de Busca baseado em expressões regulares
- Inspeção dos formatos de ficheiros mais utilizados
- Suporta varios idiomas
- DLP baseado en Fluxos

Módulo de Filtros Web
A filtragem web protege servidores, redes e informações sensíveis contra ameaças baseadas na Web, impedindo os utilizadores de acederem a sites com riscos de phishing e fontes de malware. Mais ainda, os administradores podem forçar políticas baseadas em categorias que simplesmente impedem os utilizadores de aceder a conteúdos inadequados, impedindo-os de saturar redes com tráfego indesejado.

Características:
- Filtros de HTTP/HTTPS
- Bloqueio de URL/Palavra chave/Frase
- Bloqueio de Java Applet, Cookies ou Active X
- Filtro de Cabeçalhos de tipo MIME
- Filtro web baseado em Fluxos

Módulo de Alta Disponibilidade
A solução Firewall Avançado da ONI com Fortigate pode ser apresentada em modo autónomo ou HA (alta disponibilidade). As configurações em HA (alta disponibilidade) aumentam o desempenho e a fiabilidade através da criação de clusters FortiGate Multi-Node. FortiGate HA suporta modos Activo-Activo e Activo-Passivo para máxima flexibilidade. A alta disponibilidade está incluída no sistema operativo FortiOS.

Características:
- Activo-Passivo
- Failover de Sessões (FW e VPN)
- Conexão entre o monitor de estado e o failover
- Deteção e Notificação de Falhas do dispositivo
- Balanceador de carga

Módulo de controlo de Registo, Reporte e Monitorização
Os dispositivos de segurança FortiGate oferecem extensas possibilidades de registo para funcionalidades de tráfego, sistemas e proteção de rede. Além disso, recolhe detalhes e relatórios gráficos de informações detalhadas de registo. Os retransmissores fornecem análises atuais e históricas da atividade da rede para ajudar a identificar aspetos do acompanhamento e prevenir o uso indevido ou abusos ocorridos na rede.

Características:
- Armazenamento de logs interno e geração de reportes
- Monitorização gráfica em tempo real e histórico
- Suporte de reportes gráficos personalizados
- Gráficos em detalhe
- Opcional FortiAnalyser Logging (incluido para VDOM)
- Opcional FortiGuard Analysis e Serviço de Gestão

Módulo de Controlo de Aplicações
O módulo de controlo de aplicações permite reforçar e otimizar a gestão das políticas de segurança de milhares de aplicações em execução na rede, independentes do porto ou protocolo utilizado para a comunicação, bem como otimizar o uso da largura de banda em cada rede. O aumento das aplicações baseadas na Internet, que hoje bombardeiam redes, torna o controlo essencial, uma vez que a maioria de tráfego em aplicações parece um tráfego normal para as firewalls tradicionais. O módulo de controlo de aplicações da Fortinet fornece controlo de aplicações granulares, juntamente com a capacidade de definir políticas de configuração de tráfego e de inspeção baseadas no fluxo.

Características:
- Identifica e controla mais de 1.800 aplicações
- Configuração de Tráfego (por Aplicação)
- Controlo generalizado de Apps apesar do porto ou do protocolo
- Inclui Aplicações conhecidas como:
  - AOL-IM
  - ICQ
  - WinNY
  - Yahoo
  - Gnutella
  - Skype
  - MSN
  - BitTorrent
  - eDonkey
  - KaZaa
  - MySpace
  - Facebook
  - Outras

OPÇÕES DE CONFIGURAÇÃO

Fortinet oferece aos administradores uma variedade de métodos e assistentes ao configurar dispositivos na instalação. De uma simples interface web a uma interface de linha de comando com capacidades avançadas, o sistema oferece a flexibilidade e a simplicidade que o cliente necessita.

Características:
- Interface de utilizador basado en web
- Interface de Linha de Comandos (CLI)

ESPECIFICAÇÕES TÉCNICAS

ESPECIFICAÇÕES	GIGAS FG 200	GIGAS FG 400	GIGAS FG 600	GIGAS FG 700	GIGAS FG 800
Especificações Técnicas					
vCPU (Min / Max)	1 / 1	1 / 1	1 / 2	1 / 4	1 / 8
Memoria RAM (Min / Max)	1GB / 2GB	1GB / 2GB	1GB / 4GB	1GB / 6GB	1GB / 12GB
Dominios Virtuais (vDOM)	1	10 / 10	10 / 25	10 / 50	10 / 250
Políticas de Firewall (VDOM / System)	5.000	20.000 / 40.000	50.000 / 100.000	50.000 / 100.000	50.000 / 100.000
Licença de Utilizadores Ilimitados	Sim	Sim	Sim	Sim	Sim
Rendimento					
Firewall Throughtput (UDP packets)	12Gbps	12 Gbps	15 Gbps	28 Gbps	33 Gbps
IPSec VPN Throughput (AES256+SHA1)	1 Gbps	1 Gbps	1.5 Gbps	3 Gbps	5.5 Gbps
IPS Throughput	3.5 Gbps / 1 Gbps	3.5 Gbps / 1 Gbps	5.5 Gbps / 1.5 Gbps	8 Gbps / 3 Gbps	15.5 Gbps / 6 Gbps
Antivirus Throughput	100 Mbps	200 Mbps	300 Mbps	350 Mbps	400 Mbps
Gateway to Gateway IPSec VPN Tunnels (System / VDOM)	2.000	2.000	2.000	2.000	40.000
Client-to-Gateway IPSec VPN Tunnels	6.000	6.000	12.000	20.000	40.000
Sessões Concorrentes	1.0 Milhão	1.0 Milhão	2.6 Milhão	4.3 Milhão	8.5 Milhão
Novas Sessões/Sec	85.000	85.000	100.000	125.000	150.000
Utilizadores VPN SSL Concorrentes	1.000	1.000	2.000	4.500	10.000
VPN - SSL Throughput	800 Mbps	800 Mbps	830 Mbps	2 Gbps	4.5 Gbps