

Licenciatura em

Engenharia de Redes e Segurança Informática

Principais soluções do mercado de Cibersegurança



Docente: Manfred Ferreira

Ricardo Paulo Nº2023368 António Martins Nº2023367

# Índice

Capa 1

[Índice 2](#_TOC_250003)

[Introdução 3](#_TOC_250002)

[Soluções Next Generation Firewalls 4](#_TOC_250001)

Soluções Host Firewalls 5

Soluções Web Application Firewall 6

Soluções Secure Gateway 8

Soluções Firewall de Segurança de Email 9

[Soluções de Gestão de Identidades e Acessos (IAM) 10](#_TOC_250000)

Comparação entre NGFW e SWG 11

## Introdução

A segurança cibernética é uma preocupação crescente no mundo digital de hoje, onde a proteção de sistemas e dados é crucial. Este trabalho proposto pelo Professor Manfred examina as soluções mais recentes de Cibersegurança disponíveis no mercado. Exploraremos as vantagens, as tendências emergentes e a eficácia das soluções disponíveis, visando contribuir para uma compreensão mais profunda e a implementação de estratégias eficazes de segurança cibernética.

## Soluções Next Generation Firewalls

**Next-Generation Firewalls** (NGFW) são uma evolução dos tradicionais firewalls, projetados para enfrentar ameaças digitais cada vez mais sofisticadas. Vamos explorar o que torna esses firewalls de próxima geração tão avançados e como escolher a melhor opção para suas necessidades.

### Fortinet FortiGate:

* O FortiGate é um dos NGFWs mais amplamente implantados no mundo.
* Ele oferece proteção avançada contra ameaças, inteligência de ameaças baseada em IA/ML e convergência de segurança e rede.
* O sistema operativo FortiOS fornece visibilidade profunda e segurança em várias formas.
* [Além disso, o FortiGate possui recursos como SD-WAN, comutação, wireless e 5G](https://www.fortinet.com/products/next-generation-firewall) [integrados](https://www.fortinet.com/products/next-generation-firewall).

### Cisco Firepower:

* A Cisco é uma marca líder em soluções de rede e segurança.
* Os seus NGFWs, como a série Firepower, oferecem inspeção avançada de pacotes, prevenção de intrusões e proteção contra ameaças modernas.
* Eles também integram recursos de rede e segurança para uma abordagem holística.

### Sophos XGS:

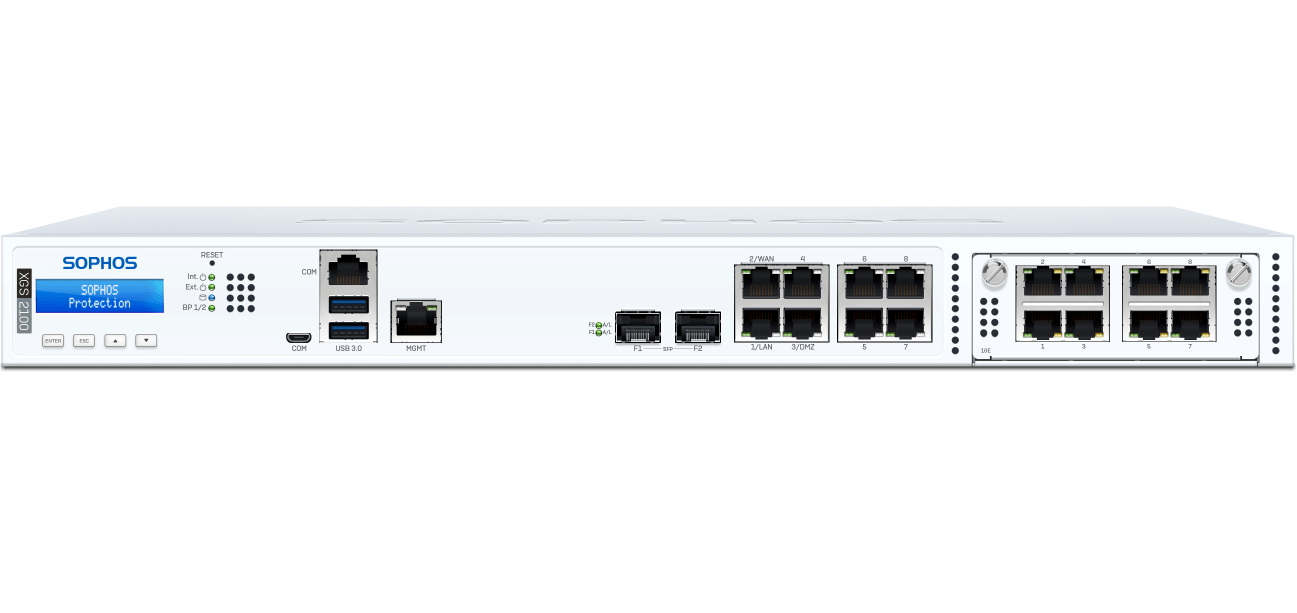
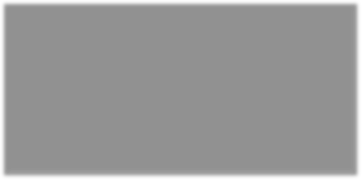
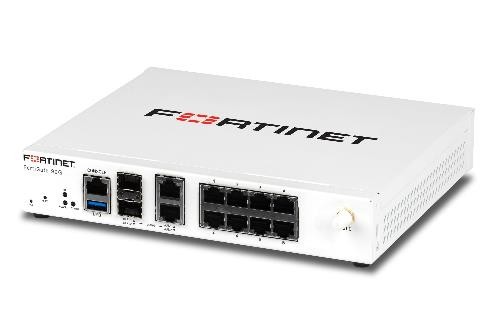
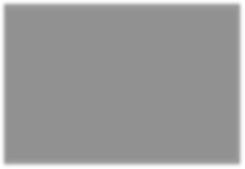
* A Sophos oferece o XGS, que combina firewall de próxima geração com proteção contra malware e recursos de SD-WAN.
* Ele é conhecido por sua simplicidade de gestão e eficácia na detecção de ameaças.

### Juniper Networks SRX Series

* A Juniper Networks oferece a série SRX, que inclui NGFWs escaláveis e flexíveis.
* Eles são adequados para ambientes de campus, data centers e cloud.

### Forcepoint NGFW

* A Forcepoint oferece soluções NGFW com foco na proteção de dados e na prevenção de ameaças internas.
* Os seus recursos incluem inspeção SSL, filtragem de conteúdo e controlo de aplicações.



## Soluções de Host Firewalls

Os **Host Firewalls** são aplicados diretamente em sistemas individuais (como computadores ou servidores). Eles protegem o próprio sistema operativo e os serviços que estão a ser executados nele. Esses firewalls são baseados em software e podem ser configurados para filtrar o tráfego com base em regras específicas, são eficazes para proteger um único dispositivo, mas não oferecem uma visão abrangente da rede como um todo

### Windows Defender Firewall:

* O Windows Defender Firewall é integrado ao sistema operacional Windows e oferece funcionalidades de firewall de host para proteger computadores contra ameaças de rede.

### Firewall do macOS:

* O Firewall do macOS é integrado ao sistema operacional macOS e oferece recursos de firewall de host para proteger computadores Mac contra acessos não autorizados e tráfego malicioso da rede.

### ZoneAlarm Firewall:

* O Check Point ZoneAlarm Firewall é uma solução de firewall de host popular para computadores Windows. Ele oferece recursos avançados de firewall para proteger contra ameaças de rede e ataques cibernéticos.

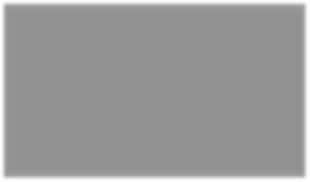
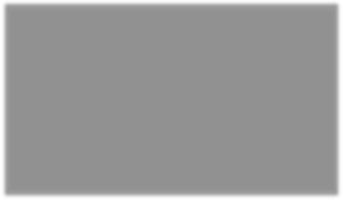
### Comodo Firewall:

* O Comodo Firewall é uma solução de segurança gratuita que oferece proteção contra ameaças de rede, ataques de hackers e tráfego malicioso.

### Firewalld

* O firewalld é um firewall de código aberto que visa prevenir o acesso não autorizado ao seu computador.O firewalld pode restringir o acesso a serviços, portas e redes.
* Ele inspeciona todo o tráfego que atravessa as várias interfaces do seu sistema e permite ou rejeita o tráfego com base em regras.
* O firewalld utiliza o conceito de zonas para segmentar o tráfego que interage com o seu sistema. Cada interface de rede é atribuída a uma ou mais zonas, e cada zona

contém uma lista de portas e serviços permitidos.



## Soluções de Web Application Firewalls

Um Web Application Firewall (WAF), ou firewall de aplicação web, é uma ferramenta de segurança que protege aplicações web contra ameaças comuns baseadas na web. Ele monitora, filtra e bloqueia pacotes de dados que trafegam para e a partir de aplicações web, protegendo-as contra ameaças.

### Imperva Web Application Firewall (WAF):

O Imperva WAF é uma solução híbrida que protege aplicações web contra-ataques comuns, garantindo operações comerciais ininterruptas.

* Precisão: Os Laboratórios de Pesquisa da Imperva garantem a precisão para os clientes bloquearem com segurança conforme o cenário de ameaças muda.
* Risco reduzido: A criação automática de políticas e a rápida propagação de regras permitem que suas equipes de segurança usem código de terceiros sem riscos, enquanto trabalham no ritmo do DevOps.
* [Ampla cobertura: Protege aplicações ativas, legadas, de terceiros, APIs, microsserviços e](https://www.imperva.com/br/web-application-firewall-waf/) [muito mais](https://www.imperva.com/br/web-application-firewall-waf/)
* ​

### Akamai App and API Protector:

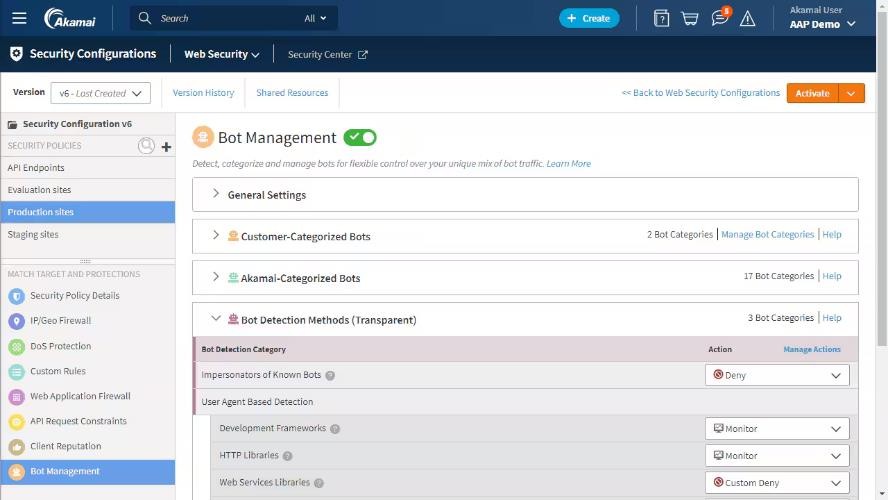
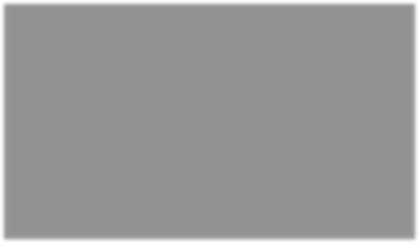
Ideal para aplicações empresariais de alto tráfego.

* Escalabilidade: Lida bem com grandes volumes de tráfego.
* Proteção contra DDoS: Oferece proteção contra ataques de negação de serviço distribuído (DDoS).

### AppTrana:

Uma opção acessível para pequenas e médias empresas (SMBs).

* Custo-benefício: Oferece proteção eficaz a um preço acessível.
* Fácil implantação: Adequado para organizações com recursos limitados.



### AWS WAF:

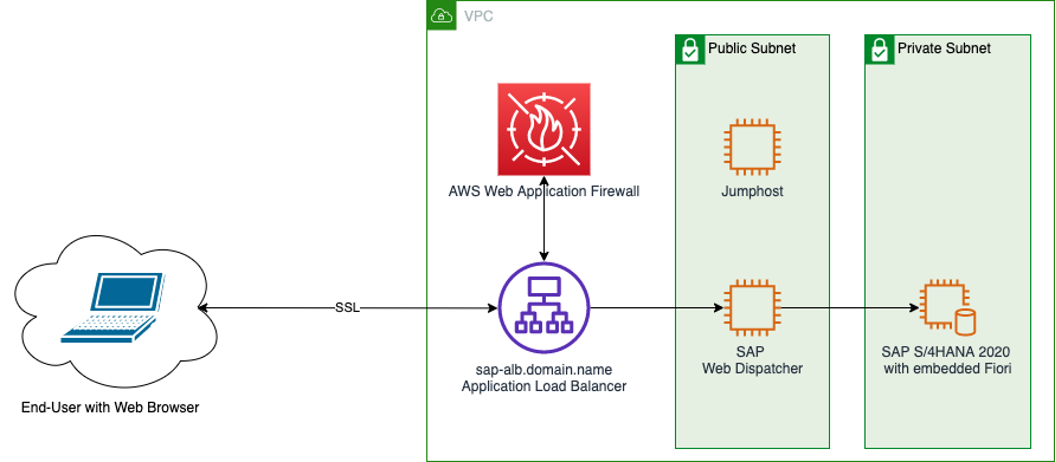
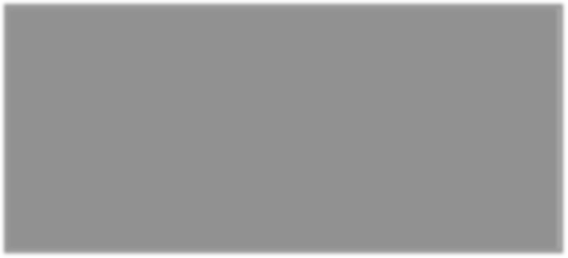
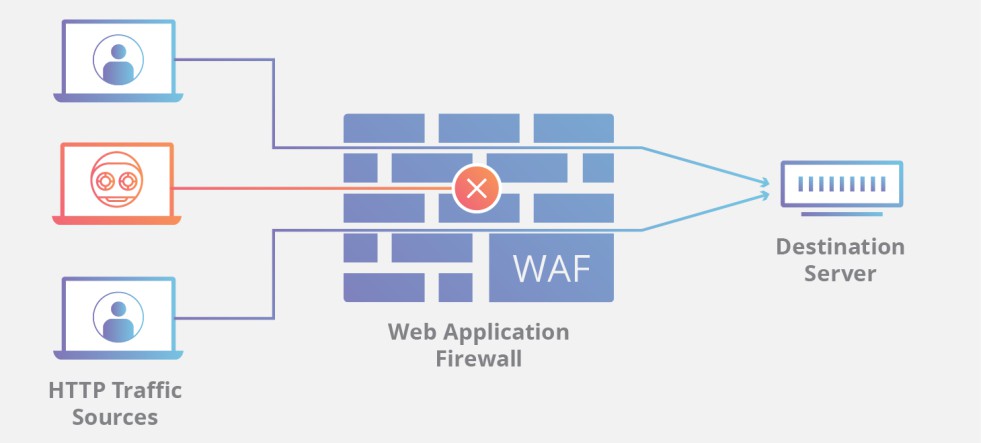
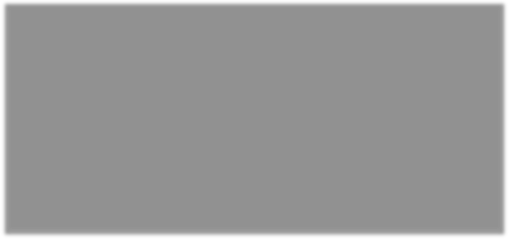
A melhor opção para ambientes AWS (Amazon Web Services).

* Integração nativa: Totalmente integrado com outros serviços da AWS.
* Flexibilidade: Pode ser personalizado para atender às necessidades específicas da aplicação.

### Cloudflare WAF:

Oferece proteção robusta contra ameaças comuns a aplicações web, alem disso a cloudflare foi escolha dos clientes para WAF 2022 pelo Gartner Peer Insights e também é lider no relatório Forrester Wave: Web Application Firewalls

* Defesas em Camadas: Regras geridas, personalizadas e Machine Learning para detectar ataque, inclusive Zero Day.
* Limitação de Taxa Avançada: Impede abusos e ataques DDoS.
* Recursos Empresariais: Suporte 24/7, garantia de disponibilidade e preços previsíveis.



## Soluções de Secure Web Gateway

Um Secure Web Gateway (SWG) é um produto de cibersegurança que protege os dados da empresa e aplica políticas de segurança. Ele atua entre os funcionários da empresa e a Internet, filtrando conteúdo inseguro do tráfego web para impedir ameaças cibernéticas e exfiltração de dados.

### Zscaler Secure Internet Access:

* Uma solução líder em segurança na nuvem.
* Oferece proteção robusta contra ameaças e filtragem de conteúdo.

### Skyhigh Security Secure Web Gateway:

* Focado em segurança de aplicativos em nuvem.
* Integração com serviços de segurança da nuvem.

### Palo Alto Networks Prisma Cloud SWG:

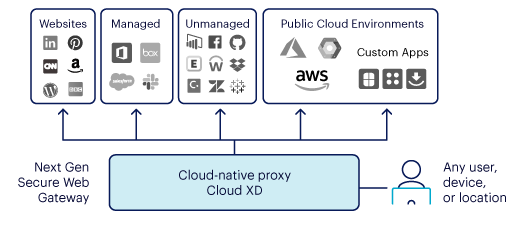
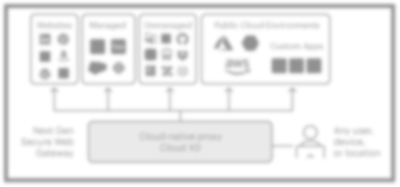
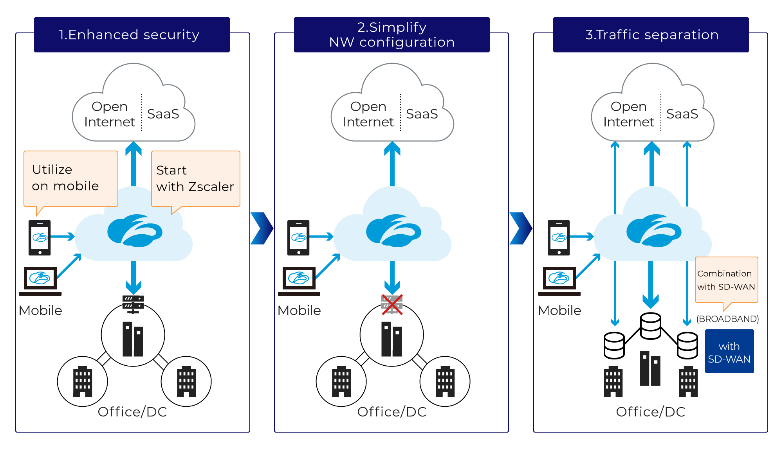
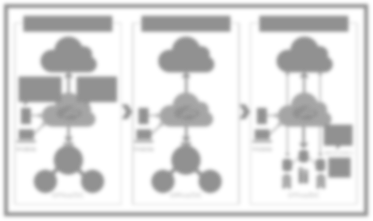
* Parte do ecossistema Prisma Cloud.
* Protege contra ameaças em ambientes híbridos e multicloud.

### Netskope Next Gen Secure Web Gateway:

* Oferece proteção empresarial contra ameaças e roubo de dados na nuvem.
* [Nomeado líder no Quadrante Mágico do Gartner® de 2024 para Security Service Edge](https://www.netskope.com/pt/security-defined/next-gen-secure-web-gateway)

### Menlo Security Secure Web Gateway:

* Foca em proteger contra ameaças avançadas.
* Implementação baseada em nuvem.



## Soluções de Firewall de Segurança de Email

Um Firewall de Segurança de Email protege a superfície de ataque de uma organização contra ameaças que exploram contas de email.

Filtra e gere todo o tráfego de email, tanto de entrada quanto de saída, para evitar ameaças como malware, ransomware e vazamento de dados.

O email é uma ferramenta crítica para a comunicação organizacional, mas também é um dos principais alvos de ataques cibernéticos.

### Barracuda Email Security Gateway:

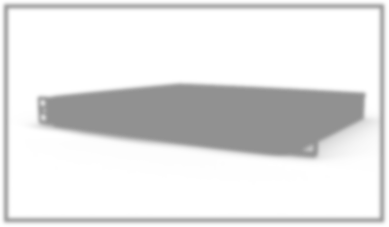
* Gere e filtra todo o tráfego de email de entrada e saída.
* Protege contra ameaças cibernéticas e vazamento de dados.
* Modelos variados, incluindo 1530, 1550, 1570, 1590, 1600, 1800 e outros.
* Oferece controle de aplicativos, prevenção contra perda de dados e muito mais.

### ProtonMail:

* Focado em privacidade e segurança.
* Usa criptografia de ponta a ponta para proteger os emails.

### Tutanota:

* Outra opção de email seguro com criptografia de ponta a ponta.
* Oferece planos gratuitos e pagos.



## Soluções de Gestão de Identidades e Acessos (IAM)

A Gestão de Identidades e Acessos (IAM) é crucial para proteger os recursos da sua organização e garantir que apenas os usuários autorizados tenham acesso a eles. Ela permite controlar quem pode aceder quais recursos e como eles podem ser acedidos.

### Microsoft:

* Azure Active Directory (AAD): Uma solução IAM completa baseada na nuvem, oferecendo autenticação, autorização, provisionamento de usuários, gestão de acesso privilegiado e muito mais. Ideal para empresas que já utilizam outros serviços do Microsoft 365.

### Google Cloud Identity and Access Management (IAM):

* Uma solução IAM nativa da nuvem do Google, fornecendo controle granular de acesso a recursos do Google Cloud Platform (GCP), aplicativos do Google Workspace e dados de terceiros. Integra-se facilmente com outros serviços do Google Cloud.

### Amazon Web Services (AWS) Identity and Access Management (IAM):

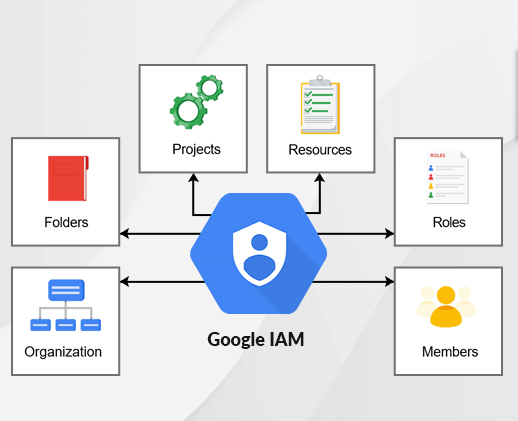
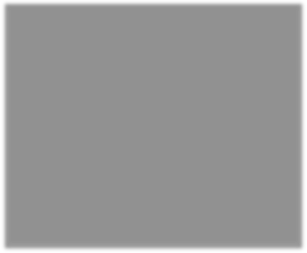
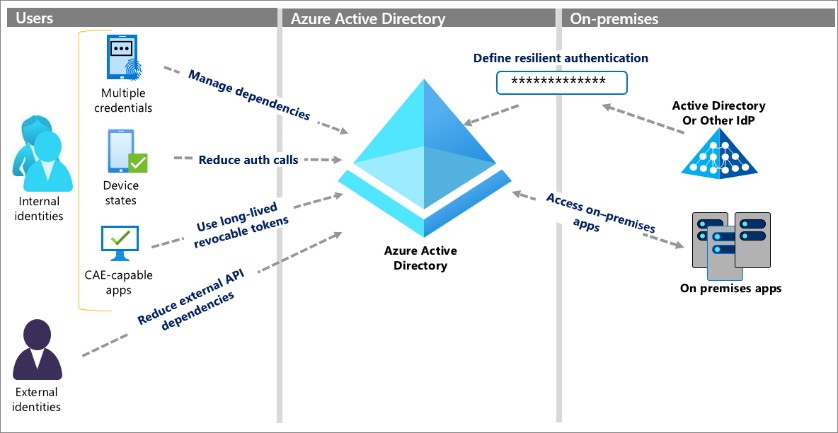
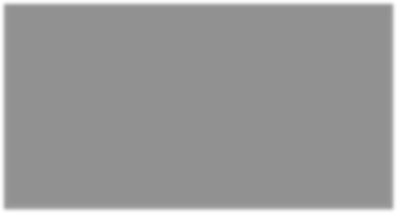
* Uma solução IAM abrangente para gerer o acesso a recursos da AWS, incluindo Amazon EC2, Amazon S3 e Amazon RDS. Permite criar usuários, grupos e políticas para controlar quem pode aceder quais recursos e como eles podem acessá-los.

### Okta:

* Uma plataforma IAM independente que se integra com diversos aplicativos e serviços na nuvem e on-premises. Oferece autenticação centralizada, provisionamento de usuários, gestão de ciclo de vida de identidade e muito mais. Ideal para empresas com ambientes híbridos ou multicloud.

### Ping Identity:

* Uma plataforma IAM abrangente que oferece autenticação, autorização, gestão de acesso privilegiado e detecção e resposta a fraudes. Ideal para grandes empresas com requisitos de segurança complexos.



## Comparação entre Next Generation Firewalls e Secure Web Gateways

|  |  |  |
| --- | --- | --- |
| **Análise SWOT** | **Pontos Fortes (Strengths)** | **Pontos Fracos (Weaknesses)** |
| **Next Generation Firewalls (NGFW)** | Inspeção de Pacotes Avançada: Examinam o tráfego de rede em nível de pacote, permitindo a detecção de ameaças sofisticadas e ataques de dia zero.  Políticas de Segurança Personalizadas: Permitem a criação de regras granulares para controlar o tráfego com base em aplicativos, usuários e outros parâmetros.  Proteção contra Ameaças Desconhecidas: Detectam ameaças que firewalls tradicionais não conseguem identificar. | Foco Limitado em Tráfego Web: Não são especializados em filtrar tráfego da web.  Complexidade de Configuração: Configurar políticas detalhadas pode ser desafiador. |
| **Secure Web Gateways( SWG)** | Filtragem de Tráfego Web: SWGs focam na inspeção e gestão do tráfego da web.  Proteção contra Malware e Phishing: Identificam e bloqueiam ameaças provenientes da internet.  Controle de Aplicativos: Gerem o acesso a aplicativos da web. | Escopo Limitado: Concentram- se principalmente no tráfego da web.  Menos Efetivos para Tráfego Não Web: Não inspecionam todo o tráfego de rede. |

|  |  |  |
| --- | --- | --- |
| **Análise SWOT** | **Oportunidades** | **Ameaças (Threats)** |
| **Next Generation Firewalls (NGFW)** | Integração com Outras Soluções: NGFWs podem se integrar com sistemas de autenticação, proteção de endpoints e SIEM (Security Information and Event Management).  Visibilidade Aprimorada: Monitoramento detalhado do tráfego de rede. | Evasão de Tráfego: Ataques que tentam contornar a inspeção do NGFW. Complexidade de Gestão: Manter políticas e atualizações pode ser trabalhoso. |
| **Secure Web Gateways( SWG)** | Integração com Firewalls e Outras Soluções: Combinar SWGs com NGFWs para uma defesa em camadas. | Evasão de Filtros: Ataques que tentam contornar as políticas do SWG.  Tráfego Criptografado: Dificuldade em inspecionar tráfego criptografado. |

Em resumo, os NGFWs oferecem proteção abrangente em nível de rede, enquanto os SWGs são especializados em filtrar tráfego da web. Combinar essas tecnologias pode fortalecer a segurança geral da organização.