BLUE COAT®

A segurança fortalece os negócios

GUIA DO COMPRADOR DE GATEWAYS DE WEB SEGURA

DOCUMENTO TÉCNICO

A Web é a fonte número 1 de distribuição de malware. Com mais de 2 milhões[1] de novas páginas adicionadas a cada dia e 10.000 novos sites maliciosos encontrados diariamente[2], como você se adapta ao volume e à crescente sofisticação de todas essas ameaças baseadas na Web? Se você é como a maioria das organizações, pretende consolidar ou fazer a transição das soluções existentes, como a filtragem de URL, para soluções de segurança na Web mais modernas, como os gateways de Web segura, para tentar se adaptar às realidades desse novo cenário de ameaças.

Os gateways de Web segura dão a você mais controle sobre o tráfego na Web, além de protegerem contra várias ameaças baseadas na Web (malware, phishing, botnets etc.). Ainda assim, nem todos os gateways de Web segura são iguais. O número de funcionalidades que você precisa considerar ao escolher um gateway de Web segura pode ser desanimador. O Guia do comprador foi pensado para ajudar você a determinar as principais áreas em que deve se concentrar durante a pesquisa, de modo que consiga selecionar a melhor solução em gateway de Web segura para sua organização.

Principais funcionalidades

A maioria dos gateways de Web segura oferece vários recursos diferentes, mas há alguns muito importantes aos quais você deverá dar mais atenção quando for avaliar um gateway de Web segura. A implementação dessas funcionalidades pode criar grandes diferenças em sua capacidade de se proteger de modo efetivo contra o alcance e a sofisticação das ameaças da Web que você está enfrentando. Essas funcionalidades também podem afetar suas operações em andamento. Você deseja encontrar soluções que possibilitem acrescentar segurança robusta sem causar interrupções, de modo que possa atender às necessidades de negócios de seus usuários.

Em alto grau, as funcionalidades em que você deseja se concentrar abrangem:

1. Proteção avançada contra ameaças da Web
2. Controle de aplicações
3. Opções flexíveis de implementação
4. Alto desempenho

Proteção avançada contra ameaças da Web

Para combater as ameaças baseadas na Web e em constante mudança que está enfrentando, você deseja encontrar uma solução que possa identificar os diversos vetores de ataques em potencial de um ataque sofisticado. Você está em busca de um gateway de Web segura que seja capaz de acompanhar as mudanças dinâmicas e dimensionáveis nas ameaças da Web. Em geral, isso requer a capacidade de realizar:

- **Filtragem avançada de URL/Web**
- **Detecção de malware**

Filtragem avançada de URL/Web

A filtragem é uma ferramenta essencial para combater o malware. Ela restringe o acesso a conteúdo inapropriado ou suscetível para sua organização bem como o acesso a sites conhecidos por promover ataques. Contudo, a filtragem baseada em categorizações estáticas fundamentadas na reputação de um URL específico não consegue acompanhar a capacidade de expansão e a natureza dinâmica da Web de hoje. A filtragem de URL/Web das soluções de gateway de Web segura deve ser avançada para fornecer suporte à aplicação de políticas e a caracterizações de modo:

- **Com precisão**
- **Em tempo real**
- **Multidimensional**

[1] Google
[2] http://www.securityweek.com/google-produces-informal-web-threat-report-shares-insights

BLUE COAT®

A segurança fortalece os negócios

Lista de verificação da filtragem avançada de URL/Web

PRINCIPAL FUNCIONALIDADE	DESCRIÇÃO	O QUE VERIFICAR
PRECISÃO DO BANCO DE DADOS	Embora muitos acreditem que os bancos de dados de URLs tenham se tornado mercadorias, a capacidade de categorizar URLs de modo preciso varia muito de um fornecedor para outro, assim como ocorre com a velocidade com a qual desempenham a análise.	• De onde o gateway obtém as informações que são armazenadas no banco de dados? • Como as informações são verificadas/validadas? • Foram feitos testes de terceiros para verificar a precisão da solução?
ANÁLISE EM TEMPO REAL	Como um URL confiável pode ser atacado e começar imediatamente a distribuir malware a seus visitantes, é importante que a solução possa identificar riscos em tempo real, de modo que você consiga identificar: • Se um URL confiável em particular foi comprometido recentemente (até algumas horas atrás). • Qual conteúdo reside em um URL específico, mesmo se for um URL totalmente novo, sem histórico ou reputação anterior.	• Com que frequência o banco de dados é atualizado? › É estático, com atualizações regulares? (ineficiente) › É atualizado dinamicamente? • Qual é o ponto de vantagem da solução? › É o monitoramento do tráfego? › É parte da infraestrutura da Web, de modo que ela seja posicionada para ver exatamente o que está acontecendo?
CATEGORIAS MULTIDIMENSIONAIS	Categorias únicas, como Esportes, Entretenimento, Jogos de azar etc., não são caracterizações precisas de um URL específico no cenário da Web de hoje. O uso de múltiplas categorias é um requisito para qualquer gateway. É necessário que se consiga definir políticas usando quaisquer ou todas as categorias identificadas.	• Como você classifica páginas como o Facebook, que apresentam conteúdo de entretenimento, notícias, jogos etc.? • Qual nível de granularidade você pode obter na categorização? › Por exemplo, é possível aplicar uma política que permita o acesso a sites categorizados como redes sociais e entretenimento, contanto que isso não inclua também conteúdo de jogos de azar?

Detecção de malware

Com novos URLs emergindo a cada dia e os URLs existentes se tornando alvos e sendo comprometidos por hackers, a filtragem de URL/Web não pode proteger os usuários e as redes corporativas em tempo real sozinha. Todos os gateways de Web segura devem incluir alguma forma de detecção de malware que possa identificar e proteger contra vírus e ataques polimórficos. Deve haver suporte a:

- **Antivírus e proteção contra ataques baseada em assinatura**
- **Análise proativa**

Lista de verificação de detecção de malware

PRINCIPAL FUNCIONALIDADE	DESCRIÇÃO	O QUE VERIFICAR
ANTIVÍRUS E PROTEÇÃO CONTRA ATAQUES BASEADA EM ASSINATURA	As soluções de antivírus de rede continuam sendo parte essencial de qualquer estratégia de segurança. A maioria usa assinaturas (padrões) de ataques conhecidos para procurar e bloquear a entrada do ataque na rede. O desafio está em escolher o fornecedor de antivírus, já que diferentes fornecedores de antivírus se destacam na identificação de tipos diferentes de ataques.	• O fornecedor de antivírus é respeitado no setor? • Qual o nível de flexibilidade do mecanismo antivírus? › Com quanta rapidez/facilidade as atualizações podem ser ativadas? › Todas as atualizações são verificadas para garantir a operação contínua? • Complementa a solução de antivírus que você implementou no desktop/laptop? › Se já existe a implementação por um fornecedor no desktop, convém considerar a implementação por outro fornecedor na rede para aumentar a cobertura e a eficácia geral.
ANÁLISE PROATIVA	Muitos gateways de segurança da Web são desenvolvidos em arquiteturas inerentemente reativas: aguardam o início de um ataque e então tentam identificar o malware específico. Em vez de esperar para reagir a um ataque que já ocorreu, o gateway de segurança na Web deveria verificar de forma proativa os possíveis ataques. Deveria, por exemplo, monitorar as redes de malware (malnets), que são a fonte de mais de 2/3 de malware no mundo.	• A solução é capaz de bloquear a transmissão de ataques de uma fonte específica antes que um ataque ocorra? • Como a solução antecipa possíveis ataques? › Há exemplos de ataques detectados semanas ou mesmo meses antes de terem sido iniciados?

BLUE COAT®

A segurança fortalece os negócios

Controle de aplicações

O controle de aplicações da Web é uma tecnologia emergente que está rapidamente se tornando um requisito para todos os gateways de Web segura. O controle de aplicações oferece o que há de mais atual em controles granulares, além de ativar ou desativar o uso de aplicações. Ele oferece controle sobre as operações individuais disponíveis em uma aplicação específica.

O número de aplicações, bem como o número de operações que podem ser controladas, varia muito de um gateway de Web segura para outro. Alguns fornecedores oferecem controles de aplicações como uma extensão de suas categorias, o que limita basicamente a rapidez do suporte a novas aplicações; outros se concentram especificamente em aplicações de redes sociais. Embora sejam um tópico importante, as redes sociais não representam as únicas aplicações que precisam ser controladas.

O gateway de Web segura deve ser capaz de fornecer em nível abrangente:

- **Controle de aplicações da Web**
- **Controle de aplicações móveis**

Lista de verificação do controle de aplicações

PRINCIPAL FUNCIONALIDADE	DESCRIÇÃO	O QUE VERIFICAR
CONTROLE DE APLICAÇÕES DA WEB	As funcionalidades ideais dos controles de aplicações da Web devem fornecer suporte aos vários tipos de aplicações, incluindo e-mail, mensagens instantâneas, áudio, vídeo, serviços financeiros, notícias etc.	• Há um registro de rastreamento comprovado de suporte a uma ampla variedade de aplicações? • Há suporte para quantas aplicações? › Deve haver suporte para, pelo menos, mais de 100 aplicações diferentes, compreendendo todos os diferentes tipos de aplicações. › Deve haver mais de 250 controles para as operações de aplicações. • Com quanta facilidade é possível acrescentar suporte a uma aplicação?
CONTROLE DE APLICAÇÕES MÓVEIS	As aplicações devem ter diferentes recursos e funcionalidades quando acessadas por navegador da Web, aplicações nativas em um smartphone ou navegador móvel. Cada uma fornece diferentes recursos e experiências do usuário. Sendo assim, um gateway de Web segura deve ser capaz de controlar aplicações móveis, sejam elas aplicações nativas ou acessadas via navegador móvel.	• Há suporte para qual tipo (número) de aplicações móveis? • Ele é capaz de distinguir aplicações nativas em um smartphone de aplicações acessadas via navegador móvel?

BLUE COAT®

A segurança fortalece os negócios

Opções flexíveis de implementação

Como sua rede contém cada vez mais uma variedade de hardware, appliances virtuais e soluções baseadas na nuvem, você precisa de um fornecedor que possa oferecer suporte à variedade de opções de implementação que você solicitar. Vários fornecedores para diferentes cenários de implementação podem acrescentar muitos custos e complexidade a seu ambiente. Idealmente, você procura um único fornecedor capaz de oferecer suporte a todos os seus diferentes requisitos de implementação com uma solução coordenada, apoiada por uma arquitetura comum. Você está em busca de um fornecedor que ofereça:

- **Várias opções de implementação,** com um appliance tradicional, appliance virtual e opções de soluções baseadas na nuvem
- **Aplicação de segurança consistente**, independentemente do modo de implementação

Lista de verificação da opção de implementação

PRINCIPAL FUNCIONALIDADE	DESCRIÇÃO	O QUE VERIFICAR
VÁRIAS OPÇÕES DE IMPLEMENTAÇÃO	As organizações precisam de diferentes opções de implementação para atender a diferentes requisitos de negócios, por exemplo, podem querer implementar um appliance tradicional na sede e um appliance virtual nos escritórios remotos bem como uma solução baseada na nuvem para seus funcionários remotos/em campo. Ao selecionar o melhor gateway de Web segura, a organização dever levar em consideração que as necessidades futuras podem indicar que é preciso suporte para uma ampla variedade de opções de implementação.	• Se o fornecedor oferece: › Appliance tradicional, no local › Appliance virtual › Solução baseada em nuvem • Há um registro de rastreamento comprovado de suporte a essas diferentes opções de implementação? › A solução virtual foi elaborada para fins específicos ou é simplesmente o software da solução de appliance?
APLICAÇÃO CONSISTENTE	O gerenciamento comum e a aplicação de políticas em todas as implementações simplificam as operações em andamento associadas às soluções. No entanto, muitas soluções que fornecem uma GUI comum não fornecem recursos e aplicação de políticas consistentes nas implementações – não é surpresa se você considerar que muitos fornecedores acrescentaram soluções na nuvem a seu portfólio por meio de aquisições.	• Você consegue aplicar as políticas de forma consistente em todas as implementações? › Appliance tradicional no local › Appliance virtual › Solução baseada na nuvem • As soluções compartilham uma GUI comum? • As soluções compartilham uma arquitetura comum? • Qual é o histórico das soluções? (São domésticas ou aquisições)

BLUE COAT®

A segurança fortalece os negócios

Alto desempenho

O desempenho de uma solução de segurança in-line, como o gateway de Web segura, é essencial para as operações em andamento de sua empresa. Como você depende mais e mais de aplicações da Web para se conectar, colaborar e conduzir os negócios, o desempenho de todos os recursos da rede é cada vez mais importante. Você não pode se sujeitar a degradações de rede ou interrupções no serviço. É preciso prestar especial atenção às arquiteturas que os fornecedores usam para suas soluções, pois isso pode ter um impacto significativo no desempenho geral. Você está em busca de fornecedores que ofereçam:

- **Alto desempenho com qualificação**
- **Análise no sistema**

Lista de verificação de desempenho

PRINCIPAL FUNCIONALIDADE	DESCRIÇÃO	O QUE VERIFICAR
ALTO DESEMPENHO COM QUALIFICAÇÃO	A arquitetura do gateway de Web segura pode ter impacto significativo sobre o desempenho. Por exemplo, é difícil para as soluções baseadas em software que usam hardware de terceiros distribuir alto desempenho, pois o hardware não é otimizado para funcionar com o software. Conforme as necessidades aumentam e mudam, pode ser difícil para esses fornecedores recomendar o hardware apropriado para atingir o dimensionamento requerido. Você está em busca de um fornecedor que tenha a experiência para oferecer a solução com o mais alto desempenho possível.	• O fornecedor tem um histórico de oferta de um appliance real, com a experiência de desenvolver os componentes de hardware e software necessários da solução? • Como é desenvolvida a arquitetura da solução? • O fornecedor pode dimensionar a solução para atender às suas necessidades conforme elas crescem e mudam?
ANÁLISE NO SISTEMA	As soluções tradicionais frequentemente são elaboradas para analisar o tráfego usando os recursos do appliance. Quando o tráfego da rede excede a capacidade do appliance, o fluxo excessivo de tráfego costuma ser descartado. Para evitar essa situação, algumas soluções são desenvolvidas para verificar o tráfego de modo seletivo, apostando que o tráfego não inspecionado seja confiável, deixando-o vulnerável. A abordagem preferida para lidar com gargalos no desempenho é descarregar funcionalidades específicas, como a análise em tempo real, na nuvem. Essa arquitetura oferece a vantagem da capacidade computacional quase ilimitada da nuvem. Os gateways de Web segura baseados nessa arquitetura garantem que todo o tráfego de rede seja inspecionado.	• O que acontece quando o tráfego de rede excede a capacidade do gateway? • Em períodos de pico, todo o tráfego continua sendo inspecionado?

Sobre a Blue Coat

A Blue Coat Systems é um provedor líder de soluções de segurança na Web e de otimização de WAN que dinamizam e protegem o fluxo de informações pela rede. Essas tecnologias aceleram a tomada de decisões, maximizam a produtividade do funcionário e reduzem os custos com largura de banda enquanto oferecem proteção contra ameaças baseadas na Web.

Para obter informações adicionais, visite www.bluecoat.com.

BLUE COAT®

A segurança fortalece os negócios

Blue Coat Systems Inc.
latam.sales@bluecoat.com

Sede Corporativa
Sunnyvale, CA USA
+1.408.220.2200

Blue Coat Brasil
São Paulo
+55 11 3443 6879

Blue Coat México
México D.F.
+52 55 3300 5825

Blue Coat Argentina
Buenos Aires
+54 (11) 4850 1215

v.WP-SWG-BUYERS-GUIDE-A4-EN-v2b-1013