



Barracuda Web Application Firewall

Segurança poderosa para camada de aplicativos para sites e servidores da Web

O Barracuda Web Application Firewall protege os sites e os aplicativos da Web contra invasores, utilizando vulnerabilidades de protocolo ou aplicativos para instigar o roubo de dados, recusa de serviço ou desfiguração do site da Web de uma empresa. Diferentemente dos tradicionais firewalls de rede ou dos sistemas de detecção de invasões que simplesmente transferem o tráfego de HTTP, HTTPS ou FTP para aplicativos da Web, o Barracuda Web Application Firewall procura este tráfego e inspeciona-o para verificação de ataques de modo a isolar servidores da Web do acesso direto de hackers.

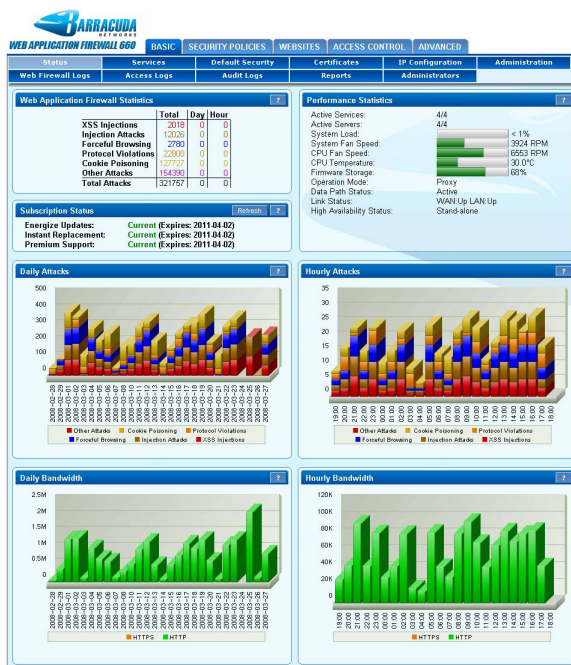
Proteção abrangente de sites da Web

O Barracuda Web Application Firewall oferece proteção premiada contra todos os ataques comuns aos aplicativos da Web, inclusive injeções de SQL, ataques de scripting entre locais, violação de sessões e estouros de buffer. Sendo um proxy completo, o Barracuda Web Application Firewall bloqueia ou oculta ataques, enquanto impede a perda de dados confidenciais de saída como os números do cartão de crédito ou do CPF.

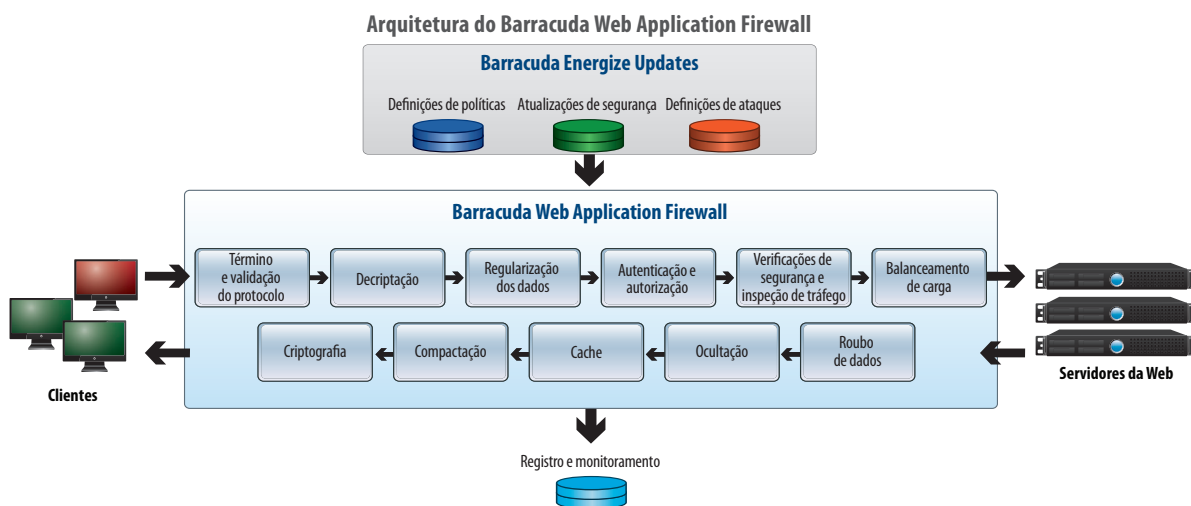
Além disso, o Barracuda Web Application Firewall reduz o controle inválido de acesso aos aplicativos, impedindo a violação e corrupção de cookies de um sistema de controle de acesso dos aplicativos. Diferentemente dos sistemas de detecção de intrusos, que somente analisam padrões de bytes, o Barracuda Web Application Firewall termina o tráfego HTTP em nome do servidor da Web para decodificar conjuntos de caracteres, remover espaçamento adicional e regularizar em relação às técnicas comuns de obscurecimento. Para segurança adicional, o Barracuda Web Application Firewall fornece integração completa de PKI para uso com os certificados do cliente a fim de verificar identidades de clientes que acessam os aplicativos da Web.

Gerenciamento avançado de tráfego e aceleração

Para minimizar a administração contínua associada à proteção de sites da Web contra vulnerabilidades de aplicativos, o Barracuda Web Application Firewall recebe automaticamente Energize Updates com as últimas definições de políticas, segurança e ataque. Além dos benefícios abrangentes de segurança, há também recursos de entrega de aplicativos como descarregamento de SSL, aceleração de SSL e balanceamento de carga. Esses recursos são desenvolvidos para aprimorar o desempenho, a capacidade de expansão e de gerenciamento das atuais infraestruturas mais exigentes de data center.



O Barracuda Web Application Firewall monitora e rastreia ataques comuns a aplicativos, estatísticas de desempenho e utilização de largura de banda.



BARRACUDA WEB APPLICATION FIREWALL

MODELO
360
460
660
860
960



BARRACUDA WEB APPLICATION FIREWALL

MODELO
360
460
660
860
960



Internet



Firewall da Internet



Barracuda Web Application Firewall



Servidor da Web

Implementação típica

ESPECIFICAÇÕES TÉCNICAS

Principais recursos

SEGURANÇA PARA APLICATIVOS DA WEB

- Protocolo HTTP/HTTPS/FTP validação
- Proteção contra ataques comuns
 - Injeção de SQL
 - Injeção de comando de SO
 - Scripting entre locais
 - Violação de cookies ou formulários
- Validação de metadados de campos de formulários
- Segurança dimensionável
- Ocultação de sites da Web
- Controle de respostas
 - Bloqueio de cliente
 - Redefinição de conexão
 - Redirecionamento
 - Resposta personalizada
- Proteção contra roubo de dados de saída
 - Números de cartão de crédito
 - Números de CPF
 - Correspondência de padrões personalizados (regex)
- Políticas granulares para elementos HTML

SEGURANÇA PARA APLICATIVOS DA WEB (continuação)

- AV para uploads de arquivos
- Verificações de limite de protocolo
- Controle de upload de arquivos
- Proteção de força bruta
- Rastreamento de sessões
- Controle de taxas

AUTENTICAÇÃO E AUTORIZAÇÃO

- Banco de dados de usuário LDAP/RADIUS/local
- Certificados do cliente
- Single Sign-On
- RSA SecurID
- CA SiteMinder

REGISTRO, MONITORAMENTO E EMISSÃO DE RELATÓRIOS

- Registro do sistema
- Registro de firewall da Web
- Registro de acesso
- Registro de auditorias
- Relatórios PCI
- Suporte a Syslog/FTP

ENTREGA E ACELERAÇÃO DE APLICATIVOS

- Alta disponibilidade
- Descarregamento de SSL
- Balanceamento de carga
- Aceleração de hardware SSL
- Cache
- Compactação
- Roteamento de conteúdo

XML FIREWALL

- Proteção XML DOS
- Imposição de Schema/WSDL
- Verificações de conformidade WS-I

Recursos do sistema

- Interface gráfica do usuário
- Administração baseada em funções
- Administração remota segura
- Bypass Ethernet ("falha na abertura")
- Políticas compartilhadas
- Isenção confiável de host

Recursos do hardware

CONECTORES

- Ethernet
 - Porta LAN
 - Porta WAN
 - Porta de gerenciamento
- Porta serial (DB-9) para console

REQUISITOS DE ENERGIA

- Tensão de entrada CA — 110 a 240 V CA
- Frequência — 50/60 Hz

Opções de suporte

INSCRIÇÃO PARA O ENERGIZE UPDATES

- Suporte técnico padrão
- Definições de políticas
- Atualizações de segurança
- Definições de ataques

SERVIÇO DE SUBSTITUIÇÃO INSTANTÂNEA

- A unidade de substituição é enviada no próximo dia útil
- Suporte técnico 24x7

COMPARAÇÃO DE MODELOS

	MODELO 360	MODELO 460	MODELO 660	MODELO 860	MODELO 960
CAPACIDADE*					
Servidores de back-end compatíveis	1 a 5	5 a 10	10 a 25	25 a 150	150 a 300
Tráfego de entrada na Web	25 Mbps	50 Mbps	100 Mbps	600 Mbps	1 Gbps
HARDWARE					
Chassi montável	Mini de 1 unidade	Mini de 1 unidade	Tamanho completo de 1 unidade	Tamanho completo de duas unidades	Tamanho completo de duas unidades
Dimensões (pol.)	16,8 x 1,7 x 14	16,8 x 1,7 x 14	16,8 x 1,7 x 22,6	17,4 x 3,5 x 25,5	17,4 x 3,5 x 25,5
Dimensões (cm)	42,7 x 4,3 x 35,6	42,7 x 4,3 x 35,6	42,7 x 4,3 x 57,4	44,2 x 8,9 x 64,8	44,2 x 8,9 x 64,8
Peso (lb /kg)	12/5,4	12/5,4	26/11,8	46/20,9	52/23,6
Portas dianteiras Ethernet	2 x 10/100	2 x Gigabit	2 x Gigabit	2 x Gigabit	2 x Gigabit
Portas traseiras Ethernet	1 x 10/100	1 x 10/100	1 x Gigabit	1 x Gigabit	1 x Gigabit
Corrente de entrada CA (A)	1,2	1,4	1,8	4,1	5,4
Memória ECC			✓	✓	✓
RECURSOS					
Validação de protocolo HTTP/HTTPS/FTP	✓	✓	✓	✓	✓
Proteção contra ataques comuns	✓	✓	✓	✓	✓
Validação de metadados de campos de formulários	✓	✓	✓	✓	✓
Ocultação de sites da Web	✓	✓	✓	✓	✓
Controle de respostas	✓	✓	✓	✓	✓
Proteção contra roubo de dados de saída	✓	✓	✓	✓	✓
Políticas granulares para elementos HTML	✓	✓	✓	✓	✓
Verificações de limite de protocolo	✓	✓	✓	✓	✓
Controle de upload de arquivos	✓	✓	✓	✓	✓
Registro, monitoramento e emissão de relatórios	✓	✓	✓	✓	✓
Alta disponibilidade	✓	✓	✓	✓	✓
Descarregamento de SSL	✓	✓	✓	✓	✓
Autenticação e autorização	✓	✓	✓	✓	✓
Integração de LDAP/RADIUS		✓	✓	✓	✓
Balanceamento de carga		✓	✓	✓	✓
Roteamento de conteúdo		✓	✓	✓	✓
XML Firewall			✓	✓	✓

PT-BR 13.0

Especificações sujeitas à alteração sem aviso prévio.

*A capacidade depende do ambiente e das opções selecionadas.