

ARBOR NETWORKS APS

Proteção em linha e sempre ativa contra DDoS.

À medida que sua dependência de acesso à Internet e aplicativos on-line aumenta, aumenta também o risco de ataques de negação de serviço distribuídos (DDoS). No Relatório de Segurança de Infraestrutura Mundial (WISR) anual mais recente da Arbor Networks, os entrevistados informaram um aumento no tamanho, na frequência e na complexidade dos ataques DDoS em comparação com o ano anterior.

O portfólio da Arbor Networks de soluções de proteção contra ataques DDoS enfrenta essas ameaças avançadas de frente, fornecendo uma visão completa das atividades da rede para correção rápida e bloqueio de nível especializado. O Arbor Networks® APS ajuda a proteger a disponibilidade e a continuidade do negócio da constelação crescente de ataques DDoS e outras ameaças avançadas. Ele fornece a tecnologia de detecção e mitigação de ataques mais sofisticada e avançada do mundo em uma plataforma fácil de implantar desenvolvida para neutralizar automaticamente os ataques IPv4 e IPv6 antes que eles prejudiquem aplicativos e serviços críticos.

Com o ATLAS® Intelligence Feed, atualizações em tempo real que contêm inteligência acionável sobre DDoS e ameaças avançadas podem evitar a entrada de ataques na sua rede. Esses recursos são:

- Proteção contra DDoS de botnets ativos
- Proteção contra DDoS de campanhas de DDoS ativas com base em reputação de IP
- Serviço de crawler da web avançado
- Rastreamento geolP
- Reputação de IP e domínio para bloquear ameaças

O Arbor APS aumenta sua proteção geral por meio do uso do Cloud Signaling™ para conectar a proteção local com DDoS services baseados na nuvem. Com o Cloud Signaling, o APS alerta automaticamente os provedores de serviços upstream, como seu ISP ou o Arbor CloudSM, quando ataques maiores ameaçam a disponibilidade. Isso permite a mitigação mais rápida dos ataques.



Figura 1

A combinação totalmente integrada de 1) APS local para proteção em linha, sempre ativa, contra ataques na camada de aplicativo; 2) Cloud Signaling inteligente para 3) Arbor Cloud para interromper os maiores ataques, 4) todos continuamente equipados com a inteligência contra ameaças globais do ATLAS/ASERT, oferece a mais abrangente solução de proteção contra DDoS do setor.

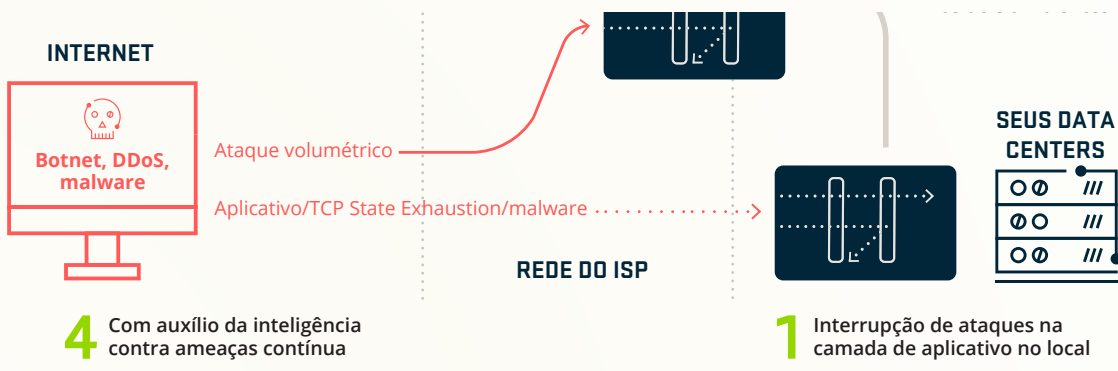


Figura 2 Proteção em camadas contra ataque DDoS

Principais recursos e benefícios



Proteção em linha e sempre ativa contra DDoS

Proteção no local pronta para uso contra ataques de DDoS na camada de aplicativo, de TCP State-Exhaustion e volumétricos.



Serviço APS gerenciado (mAPS)

Conte com a experiência líder do setor da Arbor Networks para gerenciar os produtos Arbor APS no local e otimizar sua proteção contra DDoS.



Proteção de entrada e de saída

Interrompa ataques DDoS de entrada e atividades maliciosas de saída de hosts internos comprometidos.



Suporte para ambientes virtuais

Aproveite os benefícios de um ambiente virtual para ativar rapidamente a proteção contra DDoS. vAPS é uma versão virtual do dispositivo APS.



Cloud Signaling inteligente

Quando necessário, informa o Arbor Cloud (ou seu ISP) para interromper ataques grandes que podem sobrecarregar sua proteção no local.



ATLAS Intelligence Feed

Proteção que é atualizada continuamente com a inteligência contra ameaças global mais recente da Arbor Security Engineering & Response Team (ASERT).



Descritografia SSL

Interrompa ataques DDoS ocultos no tráfego criptografado.



Suporte para IPV6

Detecte e interrompa ataques IPv4 e IPv6.

Plataformas do Arbor Networks APS

Recursos	2600	2800
Dimensões físicas	Chassis: altura do rack 2U; Altura: 8,67 cm (3,45 pol.); Largura: 43,53 cm (17,4 pol.); Profundidade: 50,8 cm (20 pol.); Peso: 17,76 kg (36,95 lb)	
Opções de energia	DC: 2 fontes de alimentação DC redundantes com suporte para troca a quente; Classificações de energia DC: -40 a -72 VDC, 28/14 A máx. (por entrada DC); AC: 2 fontes de alimentação AC redundantes com suporte para troca a quente; Classificações de energia AC: 100 a 240 VAC, 50 a 60 Hz, 12/6 A máx.; Watts: 315 típico, 375 máx.	
Discos rígidos	2 x 120 GB SSD com configuração RAID 1	2 x 240 GB SSD com configuração RAID 1
Ambiental	Em operação: temperatura de 5 a 40 °C (41 a 104 °F); umidade de 5 a 85%; Fora de operação: temperatura de -40 a 70 °C (-40 a 158 °F); umidade de 95%	
Memória	32 GB	64 GB
Processador	2 x Intel Xeon E5-2608L v3 (6 núcleos) de 2 GHz; Watts: 315 típico, 375 máx.	Dual Intel Xeon (12 núcleos) E5-2648L v3 de 1,80 GHz
Sistema operacional	Sistema operacional proprietário ArbOS® integrado	
Interfaces de gerenciamento	2 x 10/100/1.000 BaseT de cobre; porta do console serial RJ-45	2 x 10/100/1.000 BaseT de cobre; porta do console serial RJ-45
Interface de proteção	<ul style="list-style-type: none"> • 4, 8 ou 12 portas de desvio de 1 G (cobre, fibra SX, fibra LX) • 4 portas de desvio de 10 G e 0, 4 ou 8 portas de desvio de 1 G 	<ul style="list-style-type: none"> • 4 x 10 GigE (SR, LR ou fibra mista) • 8 x 10 GigE (SR, LR ou fibra mista) • 8 x 10 GigE (SR, LR ou fibra mista) + 4 x 1 GigE (fibra SX, fibra LX ou cobre)
Opções de desvio de tráfego	Desvio de hardware integrado; desvio de "software" interno para passagem de tráfego sem inspeção	
Latência	Menos de 80 microssegundos	
Disponibilidade	Desvio em linha, duas fontes de alimentação, cluster RAID do disco rígido de estado sólido	
MTBF	44.000 horas	
Cumprimentos regulatórios	UL60950-1/CSA 60950-1 (EUA/Canadá); EN60950-1 (Europa); IEC60950-1 (Internacional), certificado e relatório CB, incluindo todos os desvios internacionais; certificado GS (Alemanha); aprovação EAC-R (Rússia); CE — Diretiva Low Voltage 73/23/EEE (Europa); BSMI CNS 13436 (Taiwan); KCC (Coreia do Sul); RoHS Diretiva 2002/95/EC (Europa)	
Taxa de transferência inspecionada	Licenças para 100 Mbs, 500 Mbs, 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps, 15 Gbps, 20 Gbps	Licenças para 10 Gbps, 20 Gbps, 30 Gbps, 40 Gbps; software passível de upgrade
Taxa máxima de prevenção contra sobrecarga de DDoS	Até 15 Mpps	Até 28,80 Mpps
Conexões simultâneas	Não aplicável: o APS não controla conexões	
Conexões HTTP(s) por segundo	368 K no nível de proteção recomendado; 613 K com proteção somente na lista de filtros	1.351 K no nível de proteção recomendado; 1.497 K com proteção somente na lista de filtros
Opções decriptografia SSL	Taxa de transferência inspecionada: opções de 750 Mbps e 5 Gbps Conexões HTTPS: até 7.500 (750M HSM) ou 45.000 (5G HSM) Sessões simultâneas: até 150.000	Taxa de transferência inspecionada: até 5 Gbps Conexões HTTPS: até 45.000 Sessões simultâneas: até 150.000
	Suporte para FIPS 140-2 nível 2 e 3; administração separada via "caminho confiável" para FIPS 140-2 nível 3; gabinete seguro à prova de violação; exclusão das chaves em caso de violação do gabinete; energia: < 25 Watts; temperatura de operação: 0 a 50 °C; conformidade regulamentar: CTUVus UL (EUA/Canadá), FCC/ICES classe A Suporte para FIPS 140-2 nível 2 e 3; administração separada via "caminho confiável" para FIPS 140-2 nível 3; gabinete seguro à prova de violação; exclusão das chaves em caso de violação do gabinete; energia: < 25 Watts; temperatura de operação: 0 a 50 °C; conformidade regulamentar: CTUVus UL (EUA/Canadá), FCC/ICES classe A	
Número máximo de pares de chaves/certificados	1.998	
Terminais protegidos	Número ilimitado	
Autenticação	Um dispositivo, RADIUS; TACACS	
Gerenciamento	Gets SNMP v1, v2c; traps SNMP v1, v2c, v3; CLI; Web UI; HTTPS; gerenciamento de SSH personalizável e baseado em função; até 50 APS (dispositivos e/ou APS virtual com hypervisor KVM) podem ser gerenciados pelo console do APS; o APS gerenciado deve ter a versão v5.11 ou superior; o console do vAPS pode ser executado em um hypervisor VM.	
Grupos de proteção	50	
Relatórios e análise forense	Relatórios históricos e em tempo real de tráfego IPv4 e IPv6; detalhamento abrangente por grupo de proteção e host bloqueado, incluindo tráfego total, transmitido/bloqueado, principais URLs/serviços/domínios de destino, tipos de ataque, fontes bloqueadas, principais fontes por localização de IP. Visibilidade do pacote em tempo real.	
Proteção contra DDoS	Ataques de sobrecarga TCP/UDP/HTTP(S), proteção contra botnet, proteção contra hackers, proteção comportamental do host, anti-spoofing, filtragem configurável de expressão do fluxo, filtragem baseada em expressão da carga útil, black lists/white lists dinâmicas e permanentes, modelagem de tráfego, várias proteções para HTTP, DNS e SIP, limitação da conexão TCP, ataques de fragmentação, ataques de conexão.	
Modos	Em linha ativo; em linha inativo (relatório, sem bloqueio); monitor de porta SPAN	
Notificações	Trap SNMP, syslog, e-mail	
Cloud Signaling	Sim (mitigação colaborativa de ataque DDoS com provedor de serviços ou Arbor Cloud)	
GUI baseada na web	Suporte a interfaces com o usuário em vários idiomas	
Navegadores compatíveis	Internet Explorer v10-11, Firefox ESR v31, Firefox v40, Chrome v44, Safari v6	

Console do Arbor APS

Recursos	Hypervisor
Plataformas compatíveis	Equipamento Arbor, máquina virtual
Número máximo de APS gerenciados	50
Requisitos do console do APS virtual	VMware vSphere 5.5+; 2 CPUs; 100 GB de espaço em disco rígido; 4 GB de RAM; 1 interface de gerenciamento (segunda interface de gerenciamento opcional)
Opções de gerenciamento	Configuração ou visualizações de (APS individual e/ou todos os APS): funcionamento de hardware e software; alertas do sistema e de segurança; hosts bloqueados; resumo de ameaças do ATLAS; tipos de servidor, grupos de proteção (IPV4/6); black list/white list; relatórios de gerenciamento executivo
Navegadores compatíveis	Internet Explorer v10-11, Firefox ESR v31, Firefox v40, Chrome v44, Safari v6

Equipamento Arbor APS Console 7000

Recursos	Descrição
Memória	128 G (8 DIMMs de 16 G)
Processador	Intel Xeon (12 núcleos) ES-2648Lv3 de 1,8 GHz, 20 M de cache, 9,60 GT/s, 75 W
Requisitos de alimentação	Duas fontes de alimentação redundantes, com balanceamento de carga e detecção automática de 850 W; AC: 100-240 VAC, 50/60 Hz, 12/6 A; DC: de -40 a -72 V, 28/14 A máx.
Dimensões físicas	Chassis: altura do rack 2U; Altura: 8,67 cm (3,45 pol.); Largura: 43,53 cm (17,4 pol.) Profundidade: 50,8 cm (20 pol.); Peso: 17,76 kg (36,95 lb); padrão 19 e 23 polegadas montável em rack
Discos rígidos	Seis SSDs de 480 GB configurados para RAID 5
Interfaces de rede	2 x 1 GigE (SFP para cobre, GigE SX ou GigE LX)
Ambiental	Em operação: temperatura de 5 a 40 °C (41 a 104 °F); umidade de 95%; Fora de operação: temperatura de 23 a 40 °C (73 a 104 °F)
Sistema operacional	Sistema operacional proprietário ArbOS® integrado, baseado em Linux
Cumprimentos regulatórios	UL60950-1/CSA 60950-1; EN60950-1; IEC60950-1, certificado e relatório CB, incluindo todos os desvios internacionais; SONCAP; EAC Mark; CE—Diretiva Low Voltage 2014/35/EU; KCC Mark; RoHS 2011/65/EU; Telcordia GR-63; ETSI EN 300 019; NEBS; ETSI EN 300 753; cULus Mark; IC ICES-003 Class A; CE Mark to Diretiva EMC, 2014/30/EU; EN55022, Class A; EN55024; EN61000-3-2; EN61000-3-3, CISPR22, Class A, CISPR 24 Immunity; FCC 47 CFR Parts 15, Class A

APS virtual (vAPS)

Recursos	Hypervisor
Orquestração da função de rede virtual (VNF)	Cloud-Init v0.7.6, Openstack Kilo e Mitaka series
Hypervisor compatível	VMware vSphere 5.5+; KVM kernel 3.19 QEMU 2.0
Requisitos mínimos de máquina virtual	vCPUs: 1; NICs: de 1 a 10; memória: 6 GB; armazenamento: 100 GB
Taxa de transferência/instância de inspeção	1 Gbps
Instância/taxa máxima de sobrecarga de DDoS	910 Kpps 600 Kpps
Taxa de transferência, sobrecarga máxima/servidor	4 Gbps, 2,40 Mpps



©2017 Arbor Networks, Inc. Todos os direitos reservados. Arbor Networks, o logotipo da Arbor Networks, ArbOS e ATLAS são marcas registradas da Arbor Networks, Inc. Todas as outras marcas podem ser marcas registradas de seus respectivos proprietários.

DS/APS/PDRT/0717-LETTER

Estados Unidos
T: +1.781.362.4300
contact@arbor.net

Brasil
T: +55.11.4380.8035
brasil@arbor.net

México, Caribe & Central America
T: +52.55.4624.4842
mxcca@arbor.net

North of Latin America
T: +571.508.7099
nola@arbor.net

South of Latin America
T: +54.11.5218.4007
sola@arbor.net

www.arbournetworks.com