Data Sheet

ARBOR NETWORKS TMS

Proteção contra ameaças e serviços de capacitação comprovados e extensivos.

Provedores de serviço de Internet (ISPs), provedores de nuvem e empresas enfrentam um problema em comum. Ataques distribuídos de negação de serviço (DDoS) são um grande risco à disponibilidade do serviço. A potência, a sofisticação e a frequência dos ataques DDoS estão aumentando. Operadores de data centers e provedores de rede precisam de uma defesa que seja eficiente, tenha bom custo-benefício e de fácil gerenciamento. O Arbor Networks® TMS é reconhecidamente o líder na proteção contra DDoS. Provedores de serviços, provedores de nuvem e grandes empresas utilizam o Arbor TMS para mitigação de DDoS mais do que qualquer outra solução.

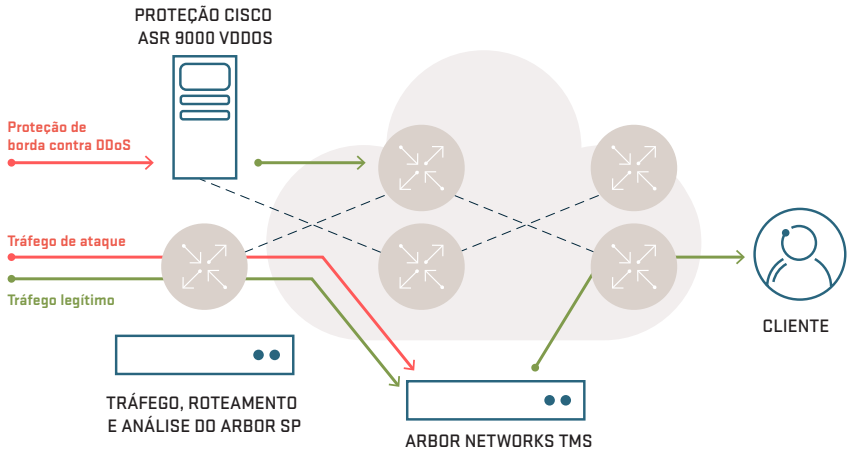
Solução Arbor Networks para proteção contra DDoS

A solução Arbor Networks integra inteligência em toda a rede e detecção de anomalias com gerenciamento de ameaças de classe de portadora para ajudar a identificar e deter ataques de exaustão de estado do TCP, ataques volumétricos e ataques de DDoS na camada de aplicativo.

Os equipamentos de rede do Arbor TMS fornecem o componente vital de limpeza de tráfego da solução Arbor Networks. O Arbor TMS pode ser implantado em linha para oferecer uma proteção "sempre ativa". Diferente de outros produtos, há suporte a uma arquitetura de mitigação chamada "desvio/retorno". Desta forma, somente o fluxo de tráfego com ataque DDoS é redirecionado para o Arbor TMS através de atualizações de encaminhamento geradas pela solução Arbor Networks. O Arbor TMS remove somente o tráfego malicioso daquele fluxo e direciona o tráfego legítimo para o destino desejado.

Isso traz grandes vantagens para os provedores de serviço, grandes empresas e grandes provedores de hospedagem/nuvem. Isso permite um Arbor TMS único e centralizado para proteger múltiplas conexões e data centers. O resultado é um uso muito mais eficiente da mitigação e uma segurança completamente não intrusiva. Os dispositivos em linha devem inspecionar todo o tráfego durante todo o tempo nas conexões monitoradas. O Arbor TMS só precisa verificar o tráfego que lhe é redirecionado em resposta a um ataque a um destino específico.

O Arbor TMS oferece uma variedade de plataformas de mitigação e recursos, que incluem: Equipamentos 2U (500 Mbps–160 Gbps de mitigação), chassis 6U (10–100 Gbps de mitigação) e roteador ASR 9000 integrado (10–60 Gbps de mitigação).



Principais recursos e benefícios

Mitigação cirúrgica
Remova de forma automática apenas o tráfego de ataque sem a interrupção do fluxo de tráfego legítimo de negócios.

Portfólio completo de plataformas de mitigação e recursos
Escolha dentre uma variedade de plataformas de mitigação e recursos, que incluem: Equipamentos 2U (500 Mbps–160 Gbps), chassis 6U (10–100 Gbps) e roteador Cisco ASR 9000 integrado (10–60 Gbps).

Command and control unificado com oito Tbps de mitigação
Leve as defesas contra DDoS a um nível sem precedentes. Implante até oito terabytes de capacidade de mitigação agregada com gerenciamento central por implantação.

Facilitador de serviços gerenciados
Responda rapidamente à demanda por serviços de proteção contra DDoS. Use o Arbor TMS para oferecer lucrativos serviços de proteção contra DDoS na nuvem.

Lista abrangente de contramedidas a ataques
Proteja sua infraestrutura e/ou seus clientes dos maiores e mais complexos ataques de DDoS volumétricos, de exaustão de estado do TCP e na camada de aplicativo.

Implantação flexível
Implante inteligência de camada de aplicativo, detecção de ameaças e mitigação cirúrgica em diferentes partes da sua rede para proteção da infraestrutura e serviços gerenciados de proteção contra DDoS mais lucrativos.

ARBOR® NETWORKS
The Security Division of NETSCOUT

Múltiplos métodos de detecção e mitigação de ameaças

Bloqueio de hosts conhecidamente maliciosos por meio do uso de white lists e black lists. A white list contém hosts autorizados, enquanto a black list contém zumbis ou hosts comprometidos que têm seu tráfego bloqueado.

Bloqueio da exploração de camada de aplicativo por meio do uso de filtros complexos. O Arbor TMS oferece visibilidade da carga útil e filtragem para garantir que ataques dissimulados não consigam derrubar serviços críticos.

Defesa contra ameaças baseadas na web por meio da detecção e mitigação de ataques de HTTP específicos. Tais mecanismos também auxiliam no gerenciamento de cenários flash crowd.

Proteção de serviços DNS essenciais contra ataques de envenenamento de cache, exaustão de recursos e amplificação. Dê grande visibilidade aos serviços DNS.

Proteção de serviços VoIP contra scripts automatizados ou botnets que exploram a sobrecarga de pacotes por segundo e pedidos malformados com o uso da detecção de ataques específicos de VoIP/SIP e capacidades de mitigação.

Prevenção de grandes ataques por reflexão/amplificação, tais como NTP, DNS, SNMP, SSDP, SQL RS ou Chargen ao ter até 160 Gbps de mitigação de ataque em um único chassi Arbor TMS.

Exposição e prevenção de ataques escondidos em pacotes SSL por meio de um Arbor TMS Hardware Security Module (HSM) opcional, que é capaz de decifrar pacotes SSL, inspecionar e derrubar ataques de tráfego, além de reencriptar e retornar o tráfego legítimo.

ATLAS® Intelligence Feed

Com uma rede global de monitoramento e sensores de tráfego, os pesquisadores da Arbor desenvolveram ATLAS Intelligence Feed, uma biblioteca de defesas direcionadas que oferecem proteção automatizada contra a grande maioria dos ataques baseados em botnet. ATLAS Intelligence Feed atualiza de forma automática o Arbor TMS com novas proteções conforme os pesquisadores da Arbor localizam e neutralizam ameaças emergentes.

Detecção abrangente de ameaças

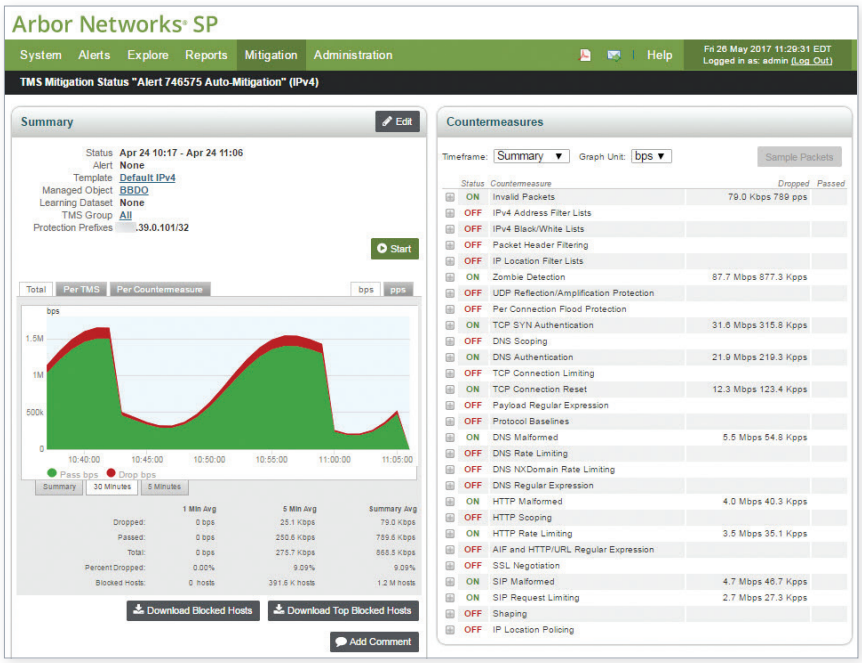
Data centers e redes públicas oferecem múltiplos destinos para ataques DDoS. Tais destinos incluem dispositivos de infraestrutura (ex.: roteadores, switches e Load Balancers), Domain Name System (DNS), capacidade da largura de banda e aplicativos cruciais como a Web, comércio eletrônico, voz e vídeo. Até mesmo dispositivos de segurança, como firewalls e sistemas de prevenção a invasões, são destinos dos ataques. A Solução Arbor Networks oferece o mais abrangente e adaptável pacote de recursos para detecção de ameaças do mercado, projetado para proteger diversos recursos contra ataques complexos e mistos. Tais recursos incluem detecção de anomalias estatísticas, detecção de anomalias em protocolos, conferência de fingerprint e detecção de anomalias analisadas. Nossa solução aprende e se adapta de forma contínua e em tempo real, alertando operadores sobre ataques e mudanças atípicas nos níveis de demanda e serviço.

Mitigação cirúrgica em segundos

A chave para uma mitigação efetiva é a habilidade de identificar e bloquear tráfego de ataque ao mesmo tempo em que o tráfego legítimo continua fluindo até seu destino desejado. Ataques DDoS em larga escala afetam não só a vítima desejada, mas também outros clientes que podem estar usando o mesmo serviço de rede compartilhada. A fim de reduzir esse dano colateral, provedores de serviços e de hospedagem frequentemente interrompem todo o tráfego destinado ao site da vítima, e desta forma completam o ataque DDoS. Seja um grande ataque volumétrico com o objetivo de exaurir a capacidade da largura de banda, ou um ataque com o objetivo de derrubar um site da web específico, em alguns casos, o Arbor TMS consegue isolar e remover o tráfego de ataque sem afetar outros usuários em apenas poucos segundos. Os métodos incluem a identificação de hosts maliciosos e sua inclusão na lista negra, mitigação baseada na localização do IP, filtragem de protocolo com base em anomalias, remoção de pacotes malformados e limite de dados (para gerenciar de forma delicada picos de demanda não maliciosos). As mitigações podem ser automatizadas ou iniciadas pelo operador e as contramedidas podem ser usadas em conjunto com ataques combinados.

Painel de mitigação em tempo real

O painel de mitigação do Arbor TMS em tempo real é uma tela única que mostra aos operadores exatamente o que está gerando o alerta DDoS e qual o efeito das medidas preventivas sobre o ataque. Ele permite modificar medidas preventivas e oferece um pacote completo de captura e decodificação para uma visão detalhada dos fluxos normais e de ataque do pacote. Essas informações são armazenadas para futuras referências e relatórios de gerenciamento, o que dá aos operadores e gerentes visibilidade e relatórios completos sobre os ataques a suas operações de negócios.



Alertas em tempo real e painel de mitigação

Detecção e mitigação de ataques DDoS em diversas escalas

O Arbor Networks SP é escalável em instâncias físicas e virtuais para oferecer detecção abrangente de DDoS em toda a rede do provedor de serviços, da borda do cliente à borda de rede ponto a ponto, da borda do data center (ou da nuvem) à borda de dispositivos móveis, incluindo a rede de backbone. Com essa visibilidade sem precedentes, o fluxo de trabalho do Arbor SP permite mitigação rápida e efetiva de qualquer ataque DDoS via Arbor TMS ou Cisco ASR 9000 vDDoS Protection. Mitigações baseadas em medidas preventivas são escaláveis a até 160 Gbps por TMS 1000 e até 8 Tbps em cada implantação. As listas negras oferecem uma camada adicional de proteção antes de qualquer outra medida preventiva de mitigação. A solução Cisco ASR 9000 vDDoS Protection usa OpenFlow para criar black lists em larga escala (até dezenas de Tbps de proteção) em qualquer borda da sua rede, protegendo seus vínculos centrais contra qualquer ataque.

Gerenciamento e relatórios abrangentes

O Arbor TMS simplifica e dinamiza operações ao permitir a visão e gerenciamento de até oito terabytes de capacidade de mitigação de um único ponto de controle. Isso permite frustrar múltiplos ataques de larga escala e produzir relatórios abrangentes que resumem o processo de mitigação para clientes e/ou gerentes.

Uma plataforma para serviços de DDoS gerenciados

A solução Arbor Networks permite que provedores de serviços e provedores de hospedagem/nuvem ofereçam a seus clientes serviços de proteção contra DDoS. Acesso personalizado ao painel, APIs e delegação de gerenciamento dão aos provedores de serviços gerenciados (MSPs) a flexibilidade e controle para oferecer serviços sob medida à necessidade de seus clientes. A Arbor Networks é a líder inquestionável na proteção gerenciada contra DDoS. É a solução da escolha da grande maioria dos serviços de DDoS gerenciados.

Especificações do Arbor TMS de defesa contra DDoS

Sessões simultâneas	Sem limite de sessões	
Modos de implantação	Ativação e monitoramento em linha, porta SPAN, desvio/retorno	
Bloqueio de ações	Bloqueio/suspensão de fonte, bloqueio de pacote, combinação de fonte, bloqueio com base em cabeçalho e taxa; bloqueio automatizado de fonte/destino de BGP Flowspec	
Proteções contra ataques	Ataques de sobrecarga de reflexão/amplificação (TCP, UDP, ICMP, DNS, mDNS, SSDP, NTP, NetBIOS, RIPv1, rpcbind, SNMP, SQL RS, Chargen, L2TP, Microsoft SQL Resolution Service); ataques de fragmentação (Teardrop, Targa3, Jolt2, Nestea), ataques à pilha TCP (SYN, FIN, RST, ACK, SYN-ACK, URG-PSH, outras combinações de TCP Flags, ataques slow TCP), ataques a aplicativos (sobrecarga HTTP GET/POST, ataques slow HTTP, sobrecarga SIP Invite, ataques DNS, ataques a protocolo HTTPS), ataques SSL/TLS (sobrecargas SSL malformado, renegociação SSL, sobrecargas de sessão SSL); envenenamento de cache DNS, ataques de vulnerabilidade, ataques de exaustão de recursos (Slowloris, Pyloris, LOIC etc.); proteção contra flash crowd; ataques em protocolos de jogos	
Medidas preventivas DDoS	**Medidas preventivas volumétricas (com suporte do Arbor TMS, 2800, 5000 e HD 1000)**	**Pacote completo de medidas preventivas (além das volumétricas)**
	Pacotes inválidos Listas com filtro por endereço IP Listas com filtros de permissão/bloqueio Filtro por cabeçalho do pacote Listas com filtro pela localização do IP Detecção de zumbis Proteção contra reflexão/amplificação UDP Proteção contra sobrecarga por conexão Autenticação TCP SYN Limite de Conexões TCP Reset de Conexões TCP Filtro de expressão regular de carga útil Modelagem Policiamento por localização do IP Filtro em linha Fingerprints da black list Linhas de base para protocolos	Autenticação de HTTP HTTP Malformado Escopo HTTP Limite de taxa HTTP Expressão regular HTTP/URL Autenticação DNS DNS Malformado Escopo DNS Limite de taxa DNS Expressão regular DNS SIP Malformado Limite de pedido SIP Negociação SSL ATLAS Intelligence Feed (AIF)

12º "Relatório de Segurança de Infraestrutura Mundial" anual da Arbor Networks

O 12º Relatório de Segurança de Infraestrutura Mundial anual da Arbor Networks abrange um período de 12 meses entre novembro de 2015 e outubro de 2016. Para o relatório, a Arbor recebeu 356 respostas de provedores de serviços Tier 1 e Tier 2/3, hosts, operadores móveis, empresas e outros tipos de operadores de rede em todo o mundo. A pesquisa foi projetada para registrar as experiências, observações e preocupações da comunidade de segurança operacional. Como nos anos anteriores, a pesquisa tratou de assuntos como ameaças à infraestrutura e clientes, técnicas utilizadas para proteger infraestrutura e mecanismos de gerenciamento, detecção e resposta a incidentes de segurança.

12 anos de relatório DDoS:

- O maior ataque DDoS relatado em 2016 foi de 800 Gbps. Um ataque 60 vezes maior do que no ano anterior. Outros entrevistados informaram ataques de 600 Gbps, 550 Gbps e 500 Gbps. Os dados do ATLAS também demonstraram que a frequência de ataques extremamente grandes aumentou de forma significativa neste ano, uma vez que um terço dos entrevistados informaram tamanhos de ataques de pico superiores a 100 Gbps. Mais de 61% das empresas e data centers que responderam à pesquisa viram ataques que saturaram completamente suas conectividades à Internet, um aumento em relação aos 33% de 2014.
- Os que responderam à pesquisa continuam vendo um aumento no número de ataques DDoS; 53% dos provedores de serviços que responderam viram mais de 21 ataques/mês, um crescimento de 44% do ano passado; 45% das empresas que responderam indicaram que haviam sofrido mais de 10 ataques/mês, um aumento em relação aos 17% do ano anterior; 21% dos operadores de data center viram 50 ou mais ataques/mês, um aumento em relação aos 8% do ano anterior.
- Ataques DDoS continuam cada vez mais complexos, uma vez que 67% dos provedores de serviços entrevistados e 40% dos entrevistados nas áreas corporativas, governamentais e educacionais (EGE) informaram terem vivenciado ataques multivetor (i.e. volumétrico, exaustão de estado do TCP e camada de aplicativo).

Para fazer download do relatório mais atualizado, acesse:
www.arbornetworks.com/report

Especificações do Arbor TMS 2800, 5000 e HD 1000

	ARBOR TMS 2800	ARBOR TMS 5000	ARBOR TMS HD 1000
Taxa de transferência e mitigação *2300 e 2800 series são licenças de software passíveis de upgrade*	Licenças para 10 Gbps, 20 Gbps, 30 Gbps, 40 Gbps, até 30 Mpps	**1 x APMe:** Até 25 Gbps, 10 Mpps **2 x APMe:** Até 50 Gbps, 20 Mpps **3 x APMe:** Até 75 Gbps, 30 Mpps **4 x APMe:** Até 100 Gbps, 40 Mpps	Até oito Packet Processing Modules (PPMs); para cada PPM adicionar 20 Gbps (14 Mpps) de taxa de mitigação, máximo 160 Gbps, 110 Mpps
Requisitos de alimentação	Fontes de alimentação redundantes **AC:** 100-127 VAC, 200-240 VAC, 12 A a 100 VAC, 6 A a 200 VAC, 50/60 Hz; **DC:** de -48 a -72 VDC, 30 A a -48 VDC	Fontes de alimentação quádruplas e redundantes **AC:** 100-120 VAC/ 200-240 VAC, de 50 a 60 Hz, 15 A; **DC:** -48/-60 Vdc, 90 A máx.	**AC:** Duas fontes de alimentação redundantes de 1.100 watts; 110-240 VAC, 50-60 Hz, 12-15 A; **DC:** Duas fontes de alimentação redundantes de 1.100 watts; de -40 a -72 VDC, 30 A
Requisitos de alimentação e aquecimento	325 Watts (máx.), a 280 Watts (nom.) 955 BTU/hora	**1xAPMe:** 1.090 Watts (máx.), a 610 Watts (nom.) 2.081 BTU/hora **2x APMe:** 1.125 Watts (máx.), a 800 Watts nom. 2.730 BTU/hora **3 x APMe:** 1.440 Watts máx. a 980 Watts nom. 3.344 BTU/hora **4 x APMe:** 1.595 Watts máx. a 1.160 Watts nom. 3.958 BTU/hora	(1) MM, (5) ventiladores, (8) SFP+, (2) QSFP, mais: (1) PPM = 472 Watts (nom) 1.610 BTU/hora; (4) PPM = 718 Watts (nom) 2.450 BTU/hora; (8) PPM = 1.046 Watts (nom) 3.569 BTU/hora
Dimensões	**Chassis:** altura do rack 2U **Peso:** 17,7 kg (39 lb) **Altura:** 8,76 cm (3,45 pol.) **Largura:** 43,53 cm (17,14 pol.) **Profundidade:** 50,8 cm (20 pol.)	**Chassis:** altura do rack 6U **Peso:** com AC: 34,99 kg (77,15 lb), com DC: 26,54 kg (58,52 lb); adicione 2,72 kg (6 lb) por APM-E blade **Altura:** 265,76 mm (10,463 pol.) **Largura:** 482,6 mm (19,00 pol.) **Profundidade:** 462,00 mm (18,19 pol.) com alças	**Chassis:** altura do rack 2U **Peso:** 20,5 kg (45,2 lb) com 1 PPM, adicionar 0,73 kg (1,6 lb) por PPM (máximo de oito) **Altura:** 88,1 mm (3,5 pol.) **Largura:** 449 mm (17,6 pol.) **Profundidade:** 50,8 mm (21 pol.)
Interfaces de rede	8 x 10 GigE (SFP+ para SR ou LR ou fibra mista)	32 x 10 GigE (QSFP+ com cabos breakout, SR4 ou 4LR); 8 x 40 GigE (QSFP+ SR4 ou LR4); 4 x 100 GigE (QSFP28 SR4 ou LR4)	Transceptores 8 x 10 GbE SFP+ (SR ou LR); até 2 transceptores 4 x 10 GbE QSFP+ (SR ou LR Lite); cada 4 x 10 GbE QSFP+ requer um cabo breakout de fibra óptica 4 x 10 GbE
Armazenamento	Dual RAID 1, 240 GB SSD Drives	Dual Hard Drive RAID 1	Dual Hard Drive RAID 1
Ambiental	**Temperatura em operação:** entre 5° e 55 °C (41° a 131 °F) **Umidade relativa (em operação):** de 5% a 85%, (fora de operação) 95% entre 23 e 40 °C (73 a 104 °F)	**Temperatura em operação:** entre -5° e 40 °C (23° a 104 °F) **Umidade relativa (em operação):** de 5% a 85% sem condensação	**Temperatura em operação:** entre -5 e 55 °C (23 a 131 °F) **Umidade relativa (em operação):** de 5% a 93% sem condensação
Regulatório	UL 60950-1 2nd edition/CSA C22.2 No. 60950-1-07 2nd Edition, Diretiva Low Voltage 2006/95/EC, Diretiva Safety 2001/95/EC, certificado e relatório CB da IEC60950-1, 2ª edição e todos os desvios internacionais, FCC 47CFR Parts 15, Verified Class A limit, ICES-003 Class A Limit, Diretiva EMC, 2004/108/EC, EN55022, EN55024, EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN61000-4-8, EN61000-4-11, EN61000-3-2, EN61000-3-3, VCCI Class A ITE (CISPR 22, Class A Limit), BSMI Approval, CNS 13438, Class A and CNS13436 Safety, KCC Approval, Gost Approval, CISPR 22 Class A Limit, CISPR 24 Immunity, RoHS (recast) Diretiva 2011/65/EU	RoHS 6/6, IEC/EN/UL 60950-1, FCC Part 15 Subpart B Class A, ETSI EN 300 386, UL Mark, CE Mark	RoHS 6/6, IEC/EN/UL/CSA 60950-1, FCC Part 15 Subpart B Class A, EN 55022, EN55024, ETSI EN 300 386, cCSAus Mark, CE Mark, KN22, KN24, RCM Mark, KCC Mark, EAC Mark, BIS, CCC Mark (pendente).
Bypass de hardware	Externo		

ARBOR NETWORKS
The Security Division of NETSCOUT

DS/TMS/PT/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: +57.1.508.7099
nola@arbor.net

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

www.arbornetworks.com