Arbor Networks® TMS

Proteção contra ameaças e aumento da disponibilidade de serviços comprovados e abrangentes

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 Cisco ASR9K roteador embutido (10-40 Gbps).

Command and control unificado com oito Tbps de mitigação

Leve as defesas contra DDoS a níveis 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 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

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. Arbor Networks® TMS é reconhecidamente o líder na proteção contra DDoS. Provedores de serviços, provedores de nuvem e grandes empresas utilizam TMS para mitigação de DDoS mais do que qualquer outra solução.

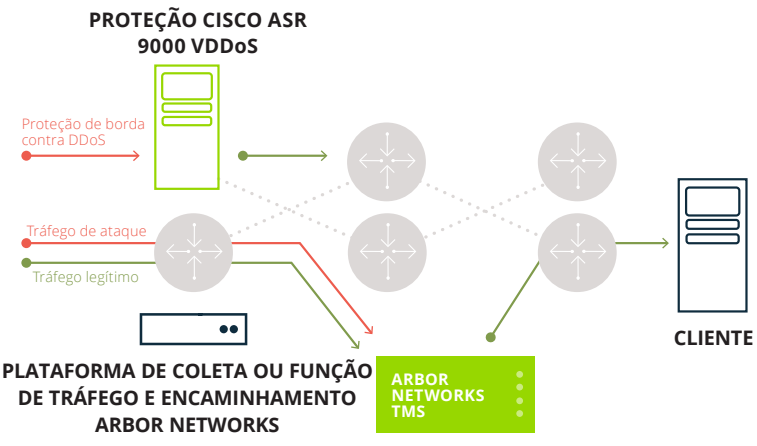
Solução Arbor Networks para proteção contra DDoS

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

O equipamento de rede TMS fornece o componente vital de limpeza de trafego da solução Arbor Networks. O 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 TMS através de atualizações de encaminhamento geradas pela solução Arbor Networks. O TMS remove somente o tráfego malicioso daquele fluxo e direciona o tráfego legítimo para o destino desejado.

Isto traz grandes vantagens para os provedores de serviço, grandes empresas e grandes provedores de hospedagem/nuvem. Isso permite um 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 TMS só precisa verificar o tráfego que lhe é redirecionado em resposta a um ataque a um destino específico.

O 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 Cisco ASR9K roteador embutido (10-40 Gbps de mitigação).



MÚLTIPLOS MÉTODOS DE DETECÇÃO E MITIGAÇÃO DE AMEAÇAS

Bloqueio de hosts reconhecidamente maliciosos
através do uso de white list/black list. A white list contém hosts autorizados enquanto a black contém zumbis ou hosts comprometidos que têm seu tráfego bloqueado.

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

Defesa contra ameaças baseadas na web
através 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.

Proteja 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.

Previna grandes ataques por reflexão/amplificação, tais como NTP, DNS, SNMP, SSDP, SQL RS ou Chargen ao ter até 80 Gbps de mitigação de ataque em um único chassi TMS.

Exponha e previna ataques escondidos em pacotes SSL através de um 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 TMS com novas proteções conforme os pesquisadores da Arbor localizam e neutralizam ameaças emergentes.

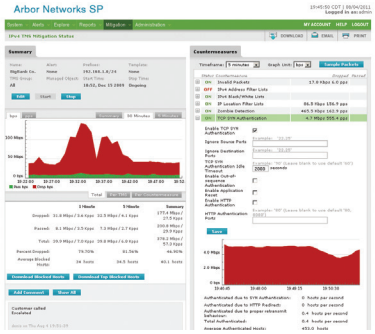
ARBOR® NETWORKS
The Security Division of NETSCOUT

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 combinados. Tais recursos incluem detecção de anomalias estatísticas, detecção de anomalias em protocolos, conferência de fingerprint e detecção de anomalias analisadas. A solução Arbor Networks 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 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 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.



Alertas em tempo real e painel de mitigação.

Painel de mitigação em tempo real

O painel de mitigação 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 contramedidas sobre o ataque. Ele permite modificar contramedidas 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 a operadores e gerentes visibilidade e relatórios completos sobre os ataques a suas operações de negócios.

DÉCIMO PRIMEIRO RELATÓRIO DE SEGURANÇA DE INFRAESTRUTURA MUNDIAL ANUAL

O Décimo primeiro Relatório de Segurança de Infraestrutura Mundial anual da Arbor Networks abrange um período de 12 meses entre novembro de 2014 e outubro de 2015. A Arbor recebeu 354 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.

Onze anos de relatório DDoS:

- O maior ataque DDoS relatado em 2015 foi de 500 Gbps. Um ataque 62 vezes maior que há dez anos, quando o ataque máximo registrado foi de apenas 8 Gbps. Mais da metade das empresas e data centers que responderam à pesquisa viram ataques que saturaram completamente sua conectividade à Internet.
- Ataques DDoS continuam cada vez mais complexos, refletindo os 56% que responderam terem vivenciado ataques multivetor (i.e. volumétrico, exaustão de estado do TCP e camada de aplicativo). Um crescimento de 42% se comparado ao ano anterior.
- Os que responderam à pesquisa continuam vendo um aumento no número de ataques DDoS; 44% dos provedores de serviços que responderam viram mais de 21 ataques/mês, um crescimento de 38% do ano passado; 28% das empresas que responderam indicaram que haviam sofrido mais de 10 ataques/mês; 9% dos operadores de data center viram 50 ou mais ataques/mês, contudo nenhum neste nível no ano passado.

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

ARBOR NETWORKS
The Security Division of NETSCOUT

Detecção e mitigação de ataques DDoS em diversas escalas

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 SP permite mitigação rápida e efetiva de qualquer ataque DDoS através de qualquer TMS ou Cisco ASR 9000 vDDoS Protection. Mitigações baseadas em contramedidas são escaláveis a até 160 Gbps por TMS 1000 e até 8 Tbps em cada implantação. As blacklists oferecem uma camada adicional de proteção antes de qualquer outra contramedida de mitigação. Cisco ASR 9000 vDDoS Protection usa OpenFlow para criar blacklist 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 TMS simplifica e dinamiza operações ao permitir a visão e gerenciamento de até oito terabytes de capacidade de mitigação a partir 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 serviço a flexibilidade e controle para oferecer serviços sob medida à necessidade de seus clientes. A solução Arbor Networks é a líder inquestionável na proteção gerenciada contra DDoS. É a escolha da grande maioria dos serviços de DDoS gerenciados.

Especificações do TMS de defesa contra DDoS

Sessões simultâneas	Sem limite de sessões	
Modes de implantação	Ativação e monitoramento inline, SPAN, desvio/ retorno	
Bloqueio de ações	Bloqueio/suspensão de fonte, por bloqueio de pacote, combinação de fonte, bloqueio com base em cabeçalho e taxa	
Proteção contra ataques	Ataques de sobrecarga (TCP, UDP, ICMP, DNS, SSDP, NTP, SNMP, SQL RS, ataque de amplificação Chargen, amplificação DNS, Microsoft SQL Resolution Service Amplification, amplificação NTP, amplificação SNMP, amplificação SSDP), ataques de fragmentação (Teardrop, Targa3, Jolt2, Nestea), ataques à pilha TCP (SYN, FIN, RST, SYN ACK, URG-PSH, TCP Flags), ataques a aplicativos (sobrecarga HTTP GET, sobrecarga SIP Invite, ataques DNS, ataques a protocolo HTTPS), envenenamento do cache DNS, ataques de vulnerabilidade, ataques de exaustão de recursos (Slowloris, Pyloris, LOIC etc.). Proteção contra flash crowd. Ataques IPv4 e IPv6 escondidos em pacotes encriptados com SSL	
Contramedidas DDoS	**Contramedidas somente volumétricas: (Com suporte a TMS 2310, 2800, 5000 e HD 1000)**	**Pacote completo de contramedidas (além das volumétricas):**
	Pacotes Inválidos Listas com filtro por endereço IPv4/IPV6 Black/White list com filtro por IPv4/IPV6 Filtro por cabeçalho do pacote Listas com filtro pela localização do IP Detecção de Zumbis 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 blacklist Linha de base para protocolos	Autenticação de HTTP HTTP Malformado Escopo HTTP Limite de tráfego HTTP Expressão regular HTTP/URL Autenticação DNS DNS Malformado Escopo DNS Limite de tráfego DNS Expressão regular DNS SIP Malformado Limite de pedido SIP Negociação SSL ATLAS Intelligence Feed (AIF)

Especificações TMS 2300, 2800, 5000 e HD 1000

	TMS 2300	TMS 2800	TMS 5000	TMS HD 1000
Taxa de transferência e mitigação *2300 e 2800 series são licenças de software passíveis de upgrade*	**2301:** 1,5 Gbps, 3,5 Mpps **2302:** 2,5 Gbps, 5 Mpps **2305:** 5 Gbps, 7 Mpps **2310:** 10 Gbps, 10 Mpps	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 duplas e redundantes **AC:** 100-127 V/200-240 V, de 50 a 60 Hz, 6/3 A; **DC:** de -48 a -60, 13 A max	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 max	**AC:** Duas fontes de alimentação redundantes de 1100 watts; 110-240 VAC, 50-60 Hz, 12-15 A; **DC:** Duas fontes de alimentação redundantes de 1100 watts; de -40 a -72 VDC, 30 A
Requisitos de energia e aquecimento	**3x1G:** 275 Watts (max.), a 200 Watts (nom.) 682 BTU/hora **3x10G:** 250 Watts (max.), a 180 Watts (nom.) 615 BTU/hora	325 Watts (max.), a 280 Watts (nom.) 955 BTU/hora	**1xAPMe:** 1090 Watts (max.), a 610 Watts (nom.) 2081 BTU/hora **2x APMe:** 1125 Watts (max.), a 800 Watts nom. 2730 BTU/hora **3 x APMe:** 1440 Watts max., a 980 Watts nom. 3344 BTU/hora **4 x APMe:** 1595 Watts max., a 1160 Watts nom. 3958 BTU/hora	(1)MM, (5) ventiladores, (8) SFP+ e (2) QSFP, mais: (1) PPM = 472 Watts (nom) 1610 BTU/ hora; (4) PPM = 718 Watts (nom) 2450 BTU/hora; (8) PPM = 1046 Watts (nom) 3569 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 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	12 x 1 GigE (SFP para cobre, GigE SX, ou GigE LX); ou 6 x 10 GigE (SFP+ para SR ou LR)	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 SSD Drives	Dual RAID 1, 240 GB SSD Drives	Dual Hard Drive RAID 1	Dual Hard Drive RAID 1
Ambiental	**Temperatura em operação:** entre 5° e 40 °C (41° a 104 °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 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	RoHS 2002/95/EC, IEC/EN/UL 60950-1 2nd ed., E2006/95/EC, 2001/95/EC, FCC Part 15 Subpart B Class A, EN 55022, EN 55024, EN 61000-3-2, EN 61000-3-3, EN 61000-4-2, EN 61000-4-3, EN 61000-4-4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11, IC ICES-003 Class A, ETSI EN 300 386, ETS 300-019-2-1, ETS 300-019-2-2, ETS 300-019-2-3, ETS 753, CISPR 22 Class A, CISPR 24, Gost, BSMI, VCCI Class A, KCC Class A, UL Mark, CE Mark, ETSI, NEBS-3 (DC), NEBS-1 (AC)	UL 60950-1 2nd edition/CSA C22.2 No. 60950-1-07 2nd Edition, Low Voltage Directive 2006/95/EC, Safety Directive 2001/95/EC, CB Certificate and Report to IEC60950-1, 2nd edition and all international deviations, FCC 47CFR Parts 15, Verified Class A limit, ICES-003 Class A Limit, EMC Directive, 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) Directive 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			Não compatível

ARBOR NETWORKS
The Security Division of NETSCOUT

Sede corporativa
76 Blanchard Road
Burlington, MA 01803 USA
Chamada gratuita
dos EUA: +1 866 212 7267
Tel.: +1 781 362 4300

www.arbornetworks.com

Vendas na América Latina
Chamada gratuita: +1 855 773 9200
Estados Unidos
T: +1 781 362 4300
contact@arbor.net

Brasil
T: +55.11.4380.8035
brasil@arbor.net

Mexico, Caribe & América Central
T: +52.55.4624.4842
mxcca@arbor.net

América Latina do Norte
T: +57.1.508.7099
nola@arbor.net

América Latina do Sul
T: +54.11.5218.4007
sola@arbor.net

DS/TMS/PT/1016-LETTER