Hoja de datos

ARBOR NETWORKS TMS

Protección contra amenazas y habilitación para servicios comprobados e integrales.

Los proveedores de servicio de Internet (ISP), los proveedores de nube y las empresas enfrentan un problema común. Los ataques de Denegación de servicio distribuidos (DDoS) son un riesgo importante para la disponibilidad del servicio. La potencia, la sofisticación y la frecuencia de los ataques DDoS cada vez son mayores. Los operadores de centros de datos y los proveedores de red necesitan una defensa eficaz, rentable y de fácil manejo. Arbor Networks® TMS es el líder reconocido en protección contra DDoS. La mayoría de los proveedores de servicios, proveedores de cloud y empresas grandes utilizan Arbor TMS para la mitigación de los DDoS antes que otras soluciones.

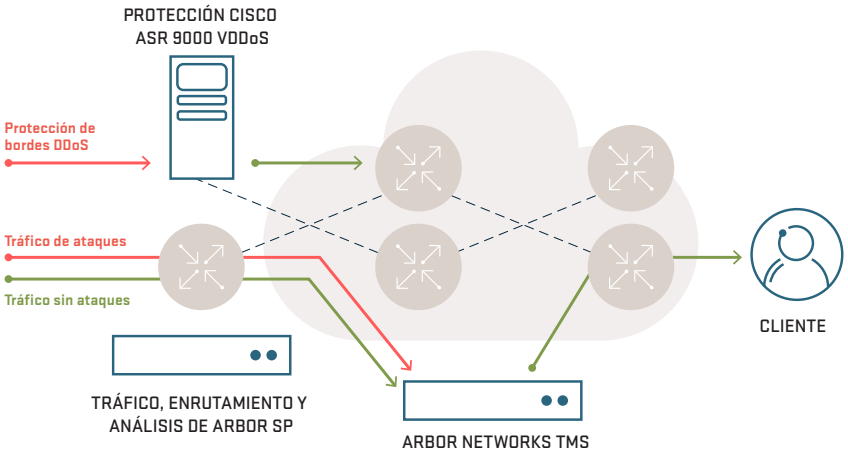
La solución Arbor Networks para la protección contra DDoS

La solución Arbor Networks integra inteligencia de toda la red y la detección de anomalías con la gestión de amenazas de primera categoría para ayudar a identificar y detener el agotamiento volumétrico y de estado de TCP y los ataque DDoS a nivel de aplicaciones.

Los dispositivos de red de Arbor TMS proporcionan el componente vital de depuración de tráfico de la solución Arbor Networks. Arbor TMS se puede implementar en línea para proporcionar una protección "siempre activa". A diferencia de otros productos, también admite una arquitectura de mitigación denominada "diversión/reinyección". En este modo, solo la secuencia de tráfico que lleva el ataque DDoS se redirige a Arbor TMS a través de actualizaciones de enrutamiento emitidas por la solución Arbor Networks. Arbor TMS remueve solamente el tráfico malintencionado de esa secuencia y reenvía el tráfico legítimo a su destino previsto.

Esto es de gran ventaja para los proveedores de servicios, las grandes empresas y los grandes proveedores de hosting/cloud. Permite un Arbor TMS único, ubicado de manera central para proteger múltiples enlaces y múltiples data centers. Resulta en un uso mucho más eficaz de la mitigación y en una seguridad completamente no intrusiva. Los dispositivos en línea deben inspeccionar todo el tráfico todo el tiempo en los enlaces que controlan. Arbor TMS solo debe inspeccionar el tráfico que se redirige a él en respuesta a un ataque en un objetivo específico.

Arbor TMS viene en una variedad de plataformas y capacidades de mitigación, entre otras: Dispositivos 2U (500 Mbps-160 Gbps de mitigación), chasis 6U (10–100 Gbps de mitigación) y enrutador Cisco ASR 9000 integrado (10–60 Gbps de mitigación).



Características principales y beneficios

Mitigación quirúrgica
Remueve de manera automática únicamente el tráfico del ataque sin interrumpir el flujo de tráfico comercial sin ataque.

Cartera completa de plataformas y capacidades de mitigación
Elija de una variedad de plataformas y capacidades de mitigación incluyendo: Dispositivos 2U (500 Mbps-160 Gbps), chasis 6U (10–100 Gbps) y enrutador Cisco ASR 9000 integrado (10–60 Gbps).

Conexiones a "command and control" unificadas de ocho Tbps de mitigación
Escale las defensas contra DDoS a un nivel sin precedentes. Implemente hasta ocho terabits de capacidad de mitigación agregada y centralizada por implementación.

Facilitador de servicios gestionado
Cumpla con las demandas que crecen rápidamente para los servicios de protección contra DDoS. Use Arbor TMS para ofrecer servicios de protección de DDoS en cloud rentables.

Lista integral de tácticas defensivas contra ataques
Proteja su infraestructura y/o a sus clientes del agotamiento de estado TCP más grande y volumétrico más complejo y los ataques DDoS a nivel de aplicaciones.

Implementación flexible
Implemente inteligencia de capa de aplicaciones, detección de amenazas y mitigación quirúrgica en diferentes partes de su red para proteger la infraestructura y obtener servicios de protección de DDoS administrador más rentables.

ARBOR® NETWORKS
The Security Division of NETSCOUT

Múltiples métodos de detección y mitigación de amenazas

Bloquee los hosts malintencionados conocidos al utilizar listas blancas y negras. La lista blanca contiene hosts autorizados, mientras que la lista negra contiene hosts zombis o en peligro cuyo tráfico se bloqueará.

Bloquee las vulnerabilidades de capa de aplicaciones al utilizar filtros complejos. Arbor TMS proporciona visibilidad de carga y filtros para asegurar mejor que los ataques ocultos derroquen servicios importantes.

Defiéndase contra las amenazas basadas en la web al detectar y mitigar ataques de HTTP específicos. Estos mecanismos también ayudan a manejar escenarios de acceso masivo.

Proteja servicios DNS críticos del envenenamiento de caché, agotamiento de recursos y ataques de amplificación. Añada mayor visibilidad a los servicios DNS.

Proteja los servicios VoIP de secuencias de comandos automatizadas o botnets que aprovechan las inundaciones de paquete por segundo y solicitudes mal formadas al emplear capacidades de mitigación y detección de ataques específicos de VoIP/SIP.

Detenga los ataques de amplificación/reflexión grandes como NTP, DNS, SNMP, SSDP, SQL RS o Chargen al aprovechar hasta 160 Gbps de mitigación de ataques en un chasis de Arbor TMS único.

Exponga y detenga los ataques ocultos en paquetes SSL a través de un Módulo de seguridad de hardware (HSM) Arbor TMS opcional, que puede descifrar los paquetes SSL, inspeccionar y disminuir el tráfico de ataque y volver a cifrar y regresar el tráfico sin ataque al cable.

ATLAS® Intelligence Feed

Al aprovechar una red global de control de tráfico y sensores, los investigadores de Arbor han desarrollado ATLAS Intelligence Feed, una biblioteca de defensas dirigidas que proporcionan protección automatizada de una vasta mayoría de ataques basados en botnet. ATLAS Intelligence Feed actualiza automáticamente Arbor TMS con nuevas protecciones a medida que los investigadores de Arbor encuentran y neutralizan amenazas emergentes.

Detección integral de amenazas

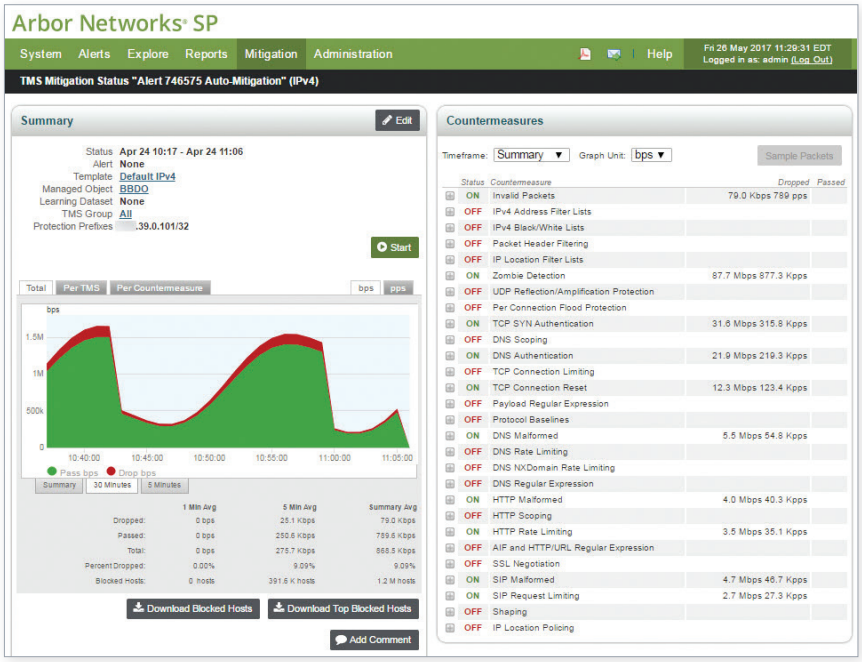
Los centros de datos y las redes públicas presentan múltiples objetivos para los ataques DDoS. Estos objetivos incluyen dispositivos de infraestructura (por ejemplo, enrutadores, interruptores y balanceadores de carga), sistemas de nombre de dominio (DNS), capacidad de ancho de banda y aplicaciones claves como web, comercio electrónico, voz y video. Incluso los dispositivos de seguridad como los sistemas de prevención de intrusión y firewalls son objetivos de ataque. La solución Arbor Networks proporciona el conjunto adaptable de capacidades de detección de amenazas de la industria, diseñado para proteger diversos recursos de ataques complejos y combinados. Estas capacidades incluyen la detección estadística de anomalías, la detección de anomalías de protocolo, la comprobación de huellas dactilares y la detección perfilada de anomalías. Nuestra solución aprende y se adapta continuamente en tiempo real, alertando a los operadores sobre ataques, así como sobre cambios inusuales en los niveles de demanda y servicio.

Mitigación quirúrgica en segundos

La clave de la mitigación eficaz es la capacidad de identificar y bloquear el tráfico de ataque a la vez que permite que un tráfico sin ataques fluya hasta su destino previsto. Los ataques DDoS a gran escala afectan no solo a la víctima intencional, sino también a otros clientes desafortunados que puedan estar utilizando el mismo servicio de red compartido. Para reducir este daño colateral, los Proveedores de servicios y los proveedores de hosting a menudo cierran todo el tráfico destinado al sitio de la víctima, completando así el ataque DDoS. Ya sea un ataque de inundación de alto volumen diseñado para agotar la capacidad de ancho de banda o un ataque dirigido que busca derrocar un sitio web, en algunos casos, Arbor TMS puede aislar y eliminar el tráfico de ataque, sin afectar a otros usuarios, en tan solo algunos segundos. Los métodos incluyen la identificación y la inclusión en lista negra de los hosts maliciosos, la mitigación basada en la ubicación IP, filtro basado en anomalías en el protocolo, eliminación de paquete mal formado y limitación de velocidad (para manejar con gracia los picos de demanda no malintencionados). Las mitigaciones pueden ser automáticas o iniciadas por un operador y las medidas defensivas se pueden combinar para abordar ataques mixtos.

Panel de mitigación en tiempo real

El panel de mitigación en tiempo real de Arbor TMS es una sola pantalla que muestra a los operadores exactamente lo que está generando una alerta de DDoS y qué efecto tienen las medidas defensivas sobre los ataques. Proporciona la capacidad de modificar medidas defensivas y ofrece captura de paquete completo y decodificación para obtener una visión detallada de las secuencias de paquetes de ataque y normales. Esta información se almacena para futura referencia y gestión de informes, lo que les brinda a los operadores y administradores visibilidad e informes completos sobre los ataques de sus operaciones comerciales.



Panel de mitigación y alerta en tiempo real

Detección y mitigación de ataques DDoS escalable

Arbor Networks SP escala en instancias físicas y virtuales para proporcionar la detección integral de DDoS por una red completa de proveedores de servicios, desde el cliente hasta el perímetro de intercambio de tráfico y el data center (o cloud) hasta el extremo móvil, incluida la red troncal intermedia. Con esta visibilidad sin igual, los flujos de trabajo de Arbor SP permiten una mitigación eficaz rápida del ataque DDoS a través de cualquier protección Arbor TMS o Cisco ASR 9000 vDDoS. Las mitigaciones basadas en las medidas de defensa escalan hasta 160 Gbps por TMS 1000 y hasta 8 Tbps en una implementación. La generación de listas negras desbloquea una capa adicional de protección frente a cualquier mitigación de las medidas de defensa. La solución de protección Cisco ASR 9000 vDDoS utiliza OpenFlow para generar listas negras a una escala masiva de hasta decenas de Tbps de protección en cualquier perímetro de su red y, por lo tanto, salvaguardar sus enlaces centrales del ataque.

Administración e informes integrales

Arbor TMS simplifica las operaciones proporcionando la capacidad de visualizar y lidiar hasta ocho terabits de capacidad de mitigación de un solo punto de control. Esto proporciona la capacidad de frustrar múltiples ataques a gran escala y producir informes integrales que resumen el proceso de mitigación para clientes o administradores.

Una plataforma de DDoS services administrados

La solución Arbor Networks permite que los proveedores de servicios y los proveedores de hosting/cloud ofrezcan servicios de protección DDoS a sus clientes. El acceso personalizado al portal, las API y la administración delegada les otorgan a los proveedores de servicios administrados (MSP) la flexibilidad y el control para adaptar servicios de modo que satisfagan las necesidades de sus clientes. Arbor Networks es el líder indiscutido para la protección contra DDoS. Es la solución preferida para la vasta mayoría de servicios administrados DDoS líderes.

Especificaciones de defensa DDoS Arbor TMS

Sesiones simultáneas	Sin sesiones limitadas	
Modos de implementación	Activo en línea, control en línea, puerto SPAN, diversión/reinyección	
Acciones de bloqueo	Bloqueo de source/suspensión de source, bloqueo por paquete, combinación de source, encabezado y bloqueo basado en la velocidad; source Flowspec BGP automatizada/ bloqueo de destino	
Protecciones contra ataques	Ataques de inundación de reflejo/amplificación (TCP, UDP, ICMP, DNS, mDNS, SSDP, NTP, NetBIOS, RIPv1, rpcbind, SNMP, SQL RS, Chargen, L2TP, servicio de resolución Microsoft SQL); ataques de fragmentación (Teardrop, Targa3, Jolt2, Nestea), ataques en pila TCP (SYN, FIN, RST, SYN-ACK, URG-PSH, otras combinaciones de TCP Flags, ataques TCP lentos); ataques de aplicación (inundaciones HTTP GET/POST, ataques HTTP lentos, inundaciones SIP Invite, ataques DNS, ataques de protocolo HTTPS); ataques SSL/TLS (inundaciones SSL mal formadas, renegociación de SSL, inundaciones de sesión SSL); envenenamiento de caché DNS, ataques de vulnerabilidad, ataques de agotamiento de recursos (Slowloris, Pyloris, LOIC, etc.); protección contra acceso masivo; ataques sobre protocolos de juego	
Medidas de defensa de DDoS	**Medidas de defensa solo volumétricas (soportadas por Arbor TMS, 2800, 5000 y HD 1000)**	**Conjunto completo de medidas de defensa (además de las solo volumétricas)**
	Paquetes no válidos Listas de filtros de direcciones IP Listas de filtro negras/blancas Filtro de encabezado del paquete Listas de filtros de ubicación de IP Detección de zombis Protección de reflejo/amplificación UDP Protección de inundación por conexión Autenticación de sincronización de TCP Limitación de la conexión de TCP Reinicio de la conexión de TCP Filtro de expresión regular de carga Formación Política de ubicación de IP Filtro en línea Huellas digitales de la lista negra Lineamientos del protocolo	Autenticación HTTP HTTP mal formado Alcance de HTTP Límite de velocidad de HTTP Expresión regular de HTTP/URL Autenticación de DNS DNS mal formado Alcance de DNS Límite de velocidad de DNS Expresión regular de DNS SIP mal formado Límite de solicitud de SIP Negociación de SSL ATLAS Intelligence Feed (AIF)

—

12.° "Informe de seguridad de infraestructura mundial (WISR)" anual

El 12.° "Informe de seguridad de infraestructura mundial (WISR)" anual de Arbor Networks cubre un período de 12 meses desde noviembre de 2015 hasta octubre de 2016. Para el informe, Arbor recopiló 356 respuestas de una mezcla de proveedores de servicios de nivel 1 y nivel 2/3, operadores de hosting, móviles, de empresa y otros tipos de operadores de red de todo el mundo. Se diseñó para recopilar las experiencias, las observaciones y las preocupaciones de la comunidad de seguridad operativa. Tal como en los años anteriores, la encuesta abordó temas como amenazas contra la infraestructura y los clientes, técnicas empleadas para proteger la infraestructura y mecanismos utilizados para administrar, detectar y responder ante incidentes de seguridad.

Doce años de informes de DDoS:

- El ataque DDoS más grande informado en 2016 fue de 800 Gbps. Eso representa un aumento de 60 veces en el último año. Otros encuestados informaron ataques de 600 Gbps, 550 Gbps y 500 Gbps. Los datos de ATLAS también muestran que la frecuencia de los ataques extremadamente grandes ha aumentado dramáticamente este año, ya que un tercio de los encuestados de este año informaron tamaños de ataques pico de más de 100 Gbps. Más del 61 % de los que respondieron del data center y la empresa vieron ataques que saturaron por completo su conectividad en Internet, más que el 33 % de 2014.
- Los entrevistados siguieron viendo un aumento en la cantidad de ataques DDoS; el 53 % de entrevistados del proveedor de servicios han visto más de 21 ataques por mes, más que el 44 % del año anterior; 45 % de entrevistados de la empresa indicaron que padecieron más de 10 ataques por mes, más que el 17 % del año anterior; 21 % de los operadores de data centers observaron más de 50 ataques por mes, más que el 8 % del año anterior.
- Los ataques DDoS siguen aumentando en complejidad ya que el 67 % de los proveedores de servicios y el 40 % de Empresas, gobierno y educación (EGE) experimentaron ataques multivectoriales (es decir, volumétrico, agotamiento de estado TCP y capa de aplicaciones) en sus redes.

Para descargar el informe más reciente, diríjase a: **www.arbornetworks.com/report**

Especificaciones para Arbor TMS 2800, 5000 y HD 1000

	ARBOR TMS 2800	ARBOR TMS 5000	ARBOR TMS HD 1000
Capacidad de proceso y mitigación *Las series 2300 y 2800 pueden actualizar la licencia de software*	Licencias para 10 Gbps, 20 Gbps, 30 Gbps, 40 Gbps, hasta 30 Mpps	**1 x APMe:** Hasta 25 Gbps, 10 Mpps **2 x APMe:** Hasta 50 Gbps, 20 Mpps **3 x APMe:** Hasta 75 Gbps, 30 Mpps **4 x APMe:** Hasta 100 Gbps, 40 Mpps	Hasta ocho módulos de procesamiento de paquete (PPM); cada PPM añade 20 Gbps (14 Mpps) de capacidad de proceso de mitigación, máximo 160 Gbps, 110 Mpps
Requisitos de alimentación	Suministros de alimentación redundante **CA:** 100-127 VCA, 200-240 VCA, 12 A a 100 VCA, 6 A a 200 VCA, 50/60 Hz; **CC:** -48 a -72 VCC, 30 A a -48 VCC	Suministros de alimentación cuádruple redundante **CA:** 100-120 VCA / 200-240 VCA, 50 a 60 Hz, 15 A; **CC:** -48/-60 VCC, 90 A máx.	**CA:** Dos suministros de alimentación redundantes de 1100 vatios; 110-240 VCA, 50-60 Hz, 12-15 A; **CC:** Dos suministros redundantes de 1100 vatios; -40 a -72 VCC, 30 A
Requisitos de alimentación y calor	325 vatios (máx.), a 280 vatios (nom.) A 955 BTU/h	**1xAPMe:** 1090 vatios (máx.), a 610 vatios (nom.) A 2081 BTU/h **2x APMe:** 1125 vatios (máx.), a 800 vatios (nom.) A 2730 BTU/h **3 x APMe:** 1440 vatios (máx.), a 980 vatios (nom.) A 3344 BTU/h **4 x APMe:** 1595 vatios (máx.), a 1160 vatios (nom.) A 3958 BTU/h	(1) MM, (5) ventiladores, (8) SFP+ y (2) QSFP, además: (1) PPM = 472 vatios (nom.) 1610 BTU/h; (4) PPM = 718 vatios (nom.) 2450 BTU/h; (8) PPM = 1046 vatios (nom.) 3569 BTU/h
Dimensiones	**Chasis:** Altura de soporte de 2U **Peso:** 39 lb (17.7 kg) **Altura:** 3.45 pulg. (8.76 cm) **Ancho:** 17.14 pulg. (43.53 cm) **Profundidad:** 20 pulg. (50.8 cm)	**Chasis:** Altura de soporte de 6U **Peso:** Con CA: 77.15 lb (34.99 kg), con CC: 58.52 lb (26.54 kg); añade 6 lb (2.72 kg) por hoja APM-E **Altura:** 10.463 pulg. (265.76 mm) **Ancho:** 19.00 pulg. (482.6 mm) **Profundidad:** 18.19 pulg. (462.00 mm) con manijas	**Chasis:** Altura de soporte de 2U **Peso:** 45.2 lb (20.5 kg) con 1 PPM, añade 1.6 lb (0.73 kg) por PPM (hasta ocho) **Altura:** 3.5 pulg. (88.1 mm) **Ancho:** 17.6 pulg. (449 mm) **Profundidad:** 21 pulg. (50.8 mm)
Interfaces de red	8 x 10 GigE (SFP+ por SR o LR o fibra mixta)	32 x 10 GigE (QSFP+ con cables de conexión, SR4 o 4LR); 8 x 40 GigE (QSFP+ SR4 o LR4); 4 x 100 GigE (QSFP28+ SR4 o LR4)	8 x 10 GbE SFP+ transmisor (SR o LR); hasta 2, 4 x 10 GbE QSFP+ transmisores (SR o LR Lite); cada 4 x 10 GbE QSFP+ requiere un cable de conexión de fibra óptica de 4 x 10 GbE
Almacenamiento	Unidades dobles RAID 1, 240 GB SSD	Unidad rígida doble RAID 1	Unidad rígida doble RAID 1
Condiciones ambientales	**Temperatura de funcionamiento:** 41° a (131 °F 5° a 55 °C) **Humedad relativa (en funcionamiento):** 5 a 85 %, (sin funcionar) 95 % entre 73° y 104 °F (23° y 40 °C)	**Temperatura de funcionamiento:** 23 °F a 104 °F (-5 °C a 40 °C) **Humedad relativa (en funcionamiento):** De 5 % a 85 % sin condensación	**Temperatura de funcionamiento:** 23 °F a 131 °F (-5 °C a 55 °C) **Humedad relativa (en funcionamiento):** De 5 % a 93 % sin condensación
Disposiciones legales	UL 60950-1 2.ª edición/CSA C22.2 N.° 60950-1-07 2.ª edición, Norma de bajo voltaje 2006/95/EC, Norma de seguridad 2001/95/EC, Certificado CB e Informe a IEC60950-1, 2.ª edición y todas las derivaciones internacionales, FCC 47CFR Artículos 15, Límite Clase A verificada, Límite Clase A ICES-003, Norma 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 Clase A ITE (CISPR 22, Límite Clase A), Aprobación BSMI, CNS 13438, Clase A y Seguridad CNS13436, Aprobación KCC, Aprobación Gost, CISPR 22 Límite Clase A, Inmunidad CISPR 24, Norma RoHS (reformular) 2011/65/EU	RoHS 6/6, IEC/EN/UL 60950-1, FCC Artículo 15 Subapartado B Clase A, ETSI EN 300 386, Marca UL, Marca CE	RoHS 6/6, IEC/EN/UL/CSA 60950-1, FCC Artículo 15 Subapartado B Clase A, EN 55022, EN55024, ETSI EN 300 386, Marca cCSAus, Marca CE, KN22, KN24, Marca RCM, Marca KCC, Marca EAC, BIS, Marca CCC (pendiente).
Derivación de hardware	Externa		

ARBOR NETWORKS
The Security Division of NETSCOUT

arbornetworks.com

DS/TMS/SP/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.arbornetworks.com