

ARBOR NETWORKS APS

常時稼働のインライン型DDoS防御

Webベースのアプリケーションやサービスに対する依存度が高まるにつれ、分散型サービス拒否 (DDoS) 攻撃のリスクも増大しています。アーバーネットワークスの最新のワールドワイド・インフラストラクチャー・セキュリティ・レポート)の中で、多くの回答者が DDoSと組み合わせたボットネットやマルウェアなど、より複雑な攻撃にさらされていることを報告しています。また、従来のボリューム型攻撃においても、攻撃の規模は拡大する一方です。アーバーネットワークスのソリューション・ポートフォリオは、ネットワークの挙動に対する包括的な視認性を提供して、迅速な措置とエキスパート・レベルのブロックを可能にし、複雑な脅威と真っ向から対決します。

アーバーネットワークス® APSは、ますます増大するDDoS攻撃やその他の高度な脅威からビジネスの継続性と可用性を保護するのに役立ちます。世界の最先端を行く洗練された攻撃検知およびミティゲーション技術を、簡単に導入できるプラットフォームで提供し、クリティカルなアプリケーションおよびサービスに影響が出る前に IPv4およびIPv6攻撃を自動的に無力化します。

ATLAS® インテリジェンス・フィードにより、DDoS攻撃および高度な脅威に関する実施可能なインテリジェンスを含むリアルタイムのアップデートを入手できるため、攻撃がネットワークに侵入するのを未然に防止できます。主な機能は以下のとおりです。

- アクティブなボットネットからのDDoS防御
- IPレピュテーションを使用した、アクティブなDDoSキャンペーンからのDDoS防御
- 高度なWebクローラー・サービス
- IPジオロケーションの追跡
- ドメインとIPのレピュテーションによる、脅威のブロック

APS は、Cloud Signaling™ を使用してローカルな防御をクラウドベースのDDoSサービスと統合することにより、全体的な防御レベルを高めます。大規模な攻撃によって可用性が脅かされた場合、APSはクラウドシグナリングを活用して、ISPやArbor CloudSMといった上流のサービス・プロバイダーに自動的にアラートを送信します。これによって、攻撃のミティゲーションをより短時間で行うことができます。

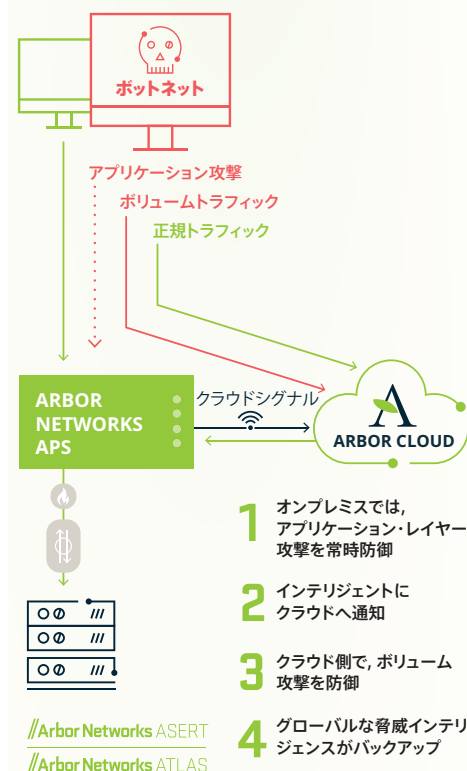
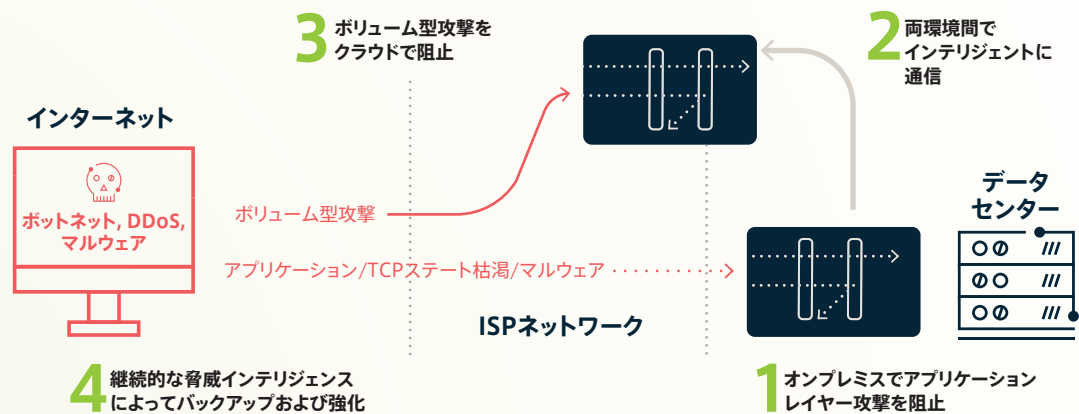


図1

以下を一貫して統合した、業界で最も包括的なDDoS保護ソリューションを実現。

- 1) 常時稼働のオンプレミスAPSによるアプリケーションレイヤー攻撃に対するインライン防御
- 2) インテリジェント・クラウドシグナリング
- 3) Arbor Cloudによる大規模攻撃の防御
- 4) ALTLAS/ASERTによる継続的なグローバル脅威インテリジェンス。



主な特長と利点



常時稼働のインライン型DDoS攻撃

設置後すぐに、ボリューム型攻撃なステートを枯渇させる攻撃、アプリケーション・レイヤーDDoS攻撃に対するオンプレミス防御を提供します。



マネージドAPS(mAS)サービス

業界の最先端をいくArbor Networksの専門技術を屈指してDDoS攻撃を管理および最適化できます。



インバウンドとアウトバウンドの防御

インバウンドのDDoS攻撃および危険な社内ホストからの有害なアウトバウンド・アクティビティを阻止します。



仮想環境をサポート

APSアプライアンスの仮想バージョンである、vAPSを提供。仮想環境のメリットを活用してDDoS防御をすばやく実装可能です。



インテリジェントなクラウドシグナリング

必要に応じて上流のArbor Cloud(またはISP)にシグナルを送信し、社内のオンプレミス防御を圧倒するような大規模攻撃を阻止します。



ATLASインテリジェント・フィード

Arbor's Security & Engineering Response Teams (ASERT) が提供する最新のグローバル脅威インテリジェンス常時活用して防御します。



SSL複合化

暗号化されたトラフィックに潜むDDoS攻撃を阻止します。



IPv6をサポート

IPv4およびIPv6両方の攻撃を検知し阻止します。

Features	2600	2800
物理的寸法	筐体: 2Uラックサイズ; 高さ: 3.45 インチ (8.67 cm); 幅: 17.4 インチ (43.53 cm); 奥行き: 20 インチ (50.8 cm); 重量: 36.95 lbs. (17.76 kg)	
電源オプション	DC: ホットスワップ可能DC冗長化電源 x 2; DC電源規格: -40 to -72 Vdc, 最大28/14 A (DC入力毎) AC: ホットスワップ可能AC冗長化電源 x 2; AC電源規格: 100 to 240 VAC, 50 to 60 Hz, 最大12/6 A Watts: 通常315, 最大375	
ハードドライブ	2 x 120 GB SSD RAID 1構成	2 x 240 GB SSD RAID 1構成
環境	動作時: 温度: 41°F to 104°F (5° to 40°C) 湿度: 5-85%; 非動作時: 温度 -40° to 158°F (-40° to 70°C); 湿度 95%	
メモリー	32 GB	64 GB
プロセッサ	2 x Intel Xeon E5-2608L v3 (6コア) 2 GHz	Dual Intel Xeon (12コア) E5-2648L v3 -1.80GHz
オペレーティング・システム	独自 組み込みArbOS®オペレーティングシステム	
管理インタフェース	2 x 10/100/1000 BaseT銅線; RJ-45シリアルコンソールポート	2 x 10/100/1000 BaseT銅線; RJ-45シリアルコンソールポート
防御インタフェース	<ul style="list-style-type: none"> 4, 8 および 12 1G バイパスポート (銅線, SXファイバー, ILXファイバー) 4 x 10 G バイパスポート および 0, 4 or 8, 1 G バイパスポート 	<ul style="list-style-type: none"> 4 x 10 GigE (SR または LR 混合) 8 x 10 GigE (SR または LR または 混合) 8 x 10 GigE (SR または LR または 混合) + 4 x 1 GigE (SX or LX ファイバー, または 銅線)
トラフィック・バイパス・オプション	統合されたハードウェアバイパス; 内部のソフトウェアバイパス(トラフィックを検査無しで通過)	
遅延	80 マイクロ秒以下	
可用性	インライン・バイパス、デュアル電源、ソリッドステート・ハードドライブの RAID クラスタ	
MTBF	44,000時間	
準拠規格	UL60950-1/CSA 60950-1 (米国/カナダ)、EN60950-1 (欧州)、IEC60950-1 (国際)、各国の偏差すべてを含む CB認証およびレポート、GS認証 (ドイツ)、EAC-R認証 (ロシア)、CE (低電圧指令) 73/23/EEE (欧州)、BSMI CNS 13436 (台湾)、KCC(韓国)、RoHS 指令 2002/95/EC(欧州)	
スループット	100 Mbs, 500 Mbs, 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps, 15 Gbps, 20 Gbpsのライセンス	10 Gbps, 20 Gbps, 30 Gbps, 40 Gbpsのライセンス、ソフトウェアによるアップグレードが可能
DDoSフラッド最大防御レート	最大15 Mpps	最大28.80 Mpps
同時接続数	対象外: APSはコネクションを追跡しない	
HTTP(s)接続 / 秒	368K (推奨防御レベル) 613K (フィルタリストのみの防御時)	1,351K 推奨防御レベル) 1,497K (フィルタリストのみの防御時)
SSL複合化オプション	スループット: 750 Mbps および 5 Gbpsのオプション HTTPS コネクション: 最大7,500 (750M HSM) または 45,000 (5G HSM) 同時セッション: 最大150,000	スループット: 最大5 Gbps HTTPS コネクション: 最大45,000 同時セッション: 最大150,000
鍵/証明書の最大ペアー数	1998	
被防御エンドポイント数	制限無し	
認証	ローカル, RADIUS, TACACS	
マネージメント	SNMP gets v1, v2c; SNMP traps v1, v2c, v3; CLI: カスタマイズ可能SSH, Web UI、ロールベースの管理に対応 最大50APS(アプライアンスおよびKVMハイパーバイザー上仮想APS)をAPSコンソールで管理可能; 被管理APSはv5.11以上が必要; vAPSコンソールはVM/HAIパーバイザー上で動作可能	
防御グループ数	50	
レポートおよび検証機能	リアルタイムおよび履歴のトラフィック・レポート (IPv4 および IPv6)、総トラフィック、通過/ブロック、URL /サービス/ドメイン別の宛先トップリスト、攻撃タイプ、ブロックされたソース、IP ロケーションによる発信元トップリストを含む、被防御グループ別およびブロックされたホスト別の幅広いドリルダウン。リアルタイムでのパケットの視認性。	
DDoS防御	TCP/UDP/HTTP(S) フラッド攻撃、ポットネット防御、ハクティビスト防御、ホストの挙動パターンによる防御、スプーフィング防止、設定可能なエクスプレッションを使ったフローのフィルタリング、エクスプレッションを使ったペイロードのフィルタリング、常時およびダイナミックなブラックリスト/ホワイトリスト、トラフィック帯域制御、多重防御 (HTTP、DNS、SIP)、TCP接続制限、フラグメンテーション攻撃、接続攻撃。	
動作モード	インライン・アクティブ; インライン・非アクティブ (レポート用, ブロックなし); SPANポートでのモニター	
通知	SNMPトラップ, syslog, 電子メール	
クラウドシグナリング	あり (サービスプロバイダーおよび Arbor Cloudとの連携によるDDoS攻撃ミティゲーション)	
WebベースGUI	日本語を含む複数言語に対応	
サポートブラウザ	Internet Explorer v10-11, Firefox ESR v31, Firefox v40, Chrome v44, Safari v6	

Arbor APS コンソール

ハイパーバイザー	
サポートプラットフォーム	Arborアプライアンス, 仮想マシン
最大管理APS数	50
仮想APSコンソール要件	VMware vSphere 5.5+; 2 CPU; 100 GB ハードディスクスペース; 4 GB RAM; 1 マネージメントインターフェース (セカンドマネージメントインターフェースはオプション)
管理オプション	構成またはビュー (個別および/またはすべてのAPS): ハードウェアとソフトウェアの状態。システム警告とセキュリティ警告。ブロックされたホスト。ATLAS脅威の概要; サーバータイプ、保護グループ (IPv4 / 6)。ブラックリスト/ホワイトリスト; エグゼクティブ管理レポート
サポートブラウザ	Internet Explorer v10-11, Firefox ESR v31, Firefox v40, Chrome v44, Safari v6

Arbor APS コンソール 7000 アプライアンス

仕様	
メモリー	128G (8x16G DIMMs)
プロセッサ	Intel Xeon (12-Core) – ES-2648Lv3 – 1.8GHz – 20M Cache – 9.60 GT/sec – 75W
Power Requirements	冗長、ロードシェア、自動センシング 850W 二重化電源; AC: 100-240 VAC, 50/60 Hz, 12/6 A; DC: -40 to -72 V, 最大28/14 A
物理的寸法	Chassis: 2U rack 高さ; Height: 3.45 インチ (8.67 cm); 幅: 17.4 インチ (43.53 cm) 奥行き: 20 インチ (50.8 cm), 重量: 36.95 lbs. (17.76 kg), 標準 19 および 23 インチラックにマウント可能
ハード・ドライブ	480 GB SSD x6, RAID 5構成
Network Interfaces	2 x 1 GigE (SFP銅線, GigE SX, もしくは GigE LX)
環境	動作時: 温度 41° to 104°F (5° to 40°C); 湿度 95%; 非動作時: 温度 73° to 104°F (23° to 40°C)
オペレーティングシステム	Linuxベース独自組み込みArbOS® オペレーティングシステム
準拠規格	UL60950-1/CSA 60950-1; EN60950-1; IEC60950-1, 各国の偏差を含むCB認証及びレポート; SONCAP; EAC Mark; CE—Low Voltage Directive 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 EMC Directive, 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

仮想APS (vAPS)

ハイパーバイザー	
Virtual Network Function (VNF) オーケストレーション	Cloud-Init v0.7.6, Openstack Kilo および Mitaka
サポートハイパーバイザー	VMware vSphere 5.5+; KVM kernel 3.19 QEMU 2.0
仮想マシン最小要件	vCPUs: 1; NICs: 1 to 10; メモリー: 6 GB; ストレージ: 100 GB
スループット/インターフェース	1 Gbps
最大DDoSフラッドレート/インスタンス	910 Kpps 600 Kpps
スループット, 最大Flood/サーバー	4 Gbps, 2.40 Mpps