NETSCOUT AED（Arbor Edge Defense）

最前線で自動処理するネットワーク防御

サイバー脅威は日々巧妙化が進んでおり、もはや安心している時間はありません。BYODやIoTなどの脆弱性を抱えるデバイスの増加に伴い、企業は新たなDDoS攻撃やランサムウェア、フィッシングなどあらゆるタイプの高度なサイバー攻撃の脅威に絶えずさらされています。進化し続けるこのような脅威に継続的に対処するため、今日のセキュリティスタックは大規模化と複雑化が進んでいます。しかしながら、情報漏洩やサービスのダウンタイムが連日報道されていることから明らかなように、残念ながら現在のセキュリティ対策は万全ではありません。

企業組織のセキュリティ部門に必要としているのは、インバウンドの脅威だけでなく、感染してしまった社内デバイスからの悪質なアウトバウンド通信を含むあらゆるタイプのサイバー脅威を検知し、防止できる、強力なサイバーセキュリティソリューションなのです。同時に、既存セキュリティスタックへの統合や機能の強化に対応し、コスト削減や複雑さの排除、リスクの低減も実現することも極めて重要です。

NETSCOUT AED（Arbor Edge Defense）は、今日の企業組織が直面するこのような課題の解決に理想的なソリューションです。AEDは、ルーターとファイアウォールとの間というネットワークエッジ上の独特の配置場所、ステートレスなパケット処理エンジン、そしてNETSCOUTのATLAS脅威インテリジェンスフィードから継続的に受信するレピュテーションベースの脅威インテリジェンスによって、DDoS攻撃やマルウェアなどのインバウンドの脅威だけでなく、感染した社内ホストからのアウトバウンド通信も自動的に検知し、防止します。Arbor Edge Defenseは、高度なサイバー脅威に対する防御の最前線と最後の砦として、強力なセキュリティを提供します。

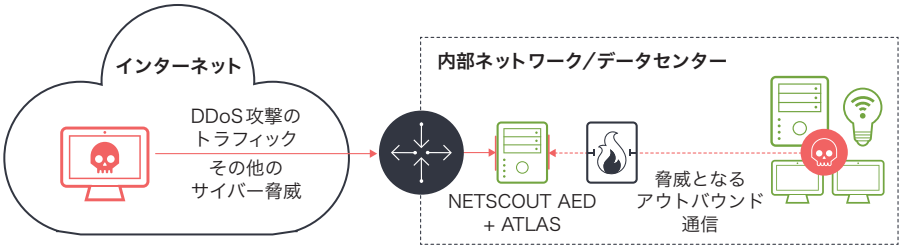

図1：AEDは、ネットワークエッジ上の独特の配置場所、ステートレスなパケット処理エンジン、ATLASグローバル脅威インテリジェンスが連携することで、高度なサイバー脅威に対する防御の最前線と最後の砦として、強力なセキュリティを提供します。

Arbor Edge Defenseのメリット

- **防御の最前線：**ネットワーク境界に配備され、ステートレステクノロジーを活用するとともに数百万ものIoC（侵害の痕跡）による防御機能を備えたAEDは、インバウンドの一般的なサイバー脅威を検知してブロックします。これにより、次世代ファイアウォールをはじめとするステートフルデバイスの負荷を軽減します。
- **防御の最後の出口：**既存のセキュリティスタックが検知できなかった脅威であっても、AEDは既知の悪意のあるIPアドレス、ドメイン、URL、あるいは地域へのアウトバウンドの通信を検知してブロックします。これにより、企業内におけるマルウェアのさらなる拡散やデータ漏洩の阻止を支援します。
- **コンテキストに基づく脅威インテリジェンス：**IoCがブロックされると、AEDはNETSCOUT ATLASのグローバルな脅威インテリジェンスを活用してIoCに関連したさらなるコンテキストを提供します。これにより、企業のセキュリティ部門はリスクの判断が容易になるとともに、より詳細な情報を入手して他のセキュリティツールを活用した脅威の検知が可能になります。
- **最高のDDoS攻撃対策：**AEDは、40Gbpsレベルの脅威保護スループットでインバウンドのアプリケーションレイヤー攻撃、TCP状態枯渇攻撃、そしてDDoS攻撃を自動的に検知し、阻止します。より大規模なDDoS攻撃を受けた場合は、クラウド・シグナリングによってArbor CloudまたはMSSPが提供するクラウドベースのDDoS防御センターにトラフィックが自動的に迂回されます。
- **統合：**AEDは、堅牢なREST API、そしてSTIX/TAXIIフィードのサポートにより、既存のセキュリティスタックやプロセスへの容易な統合が可能です。

主な機能と特長

防御の最前線と最後の出口

AEDは、ネットワークエッジ上の独特の配置場所、ステートレスなパケット処理エンジン、そしてATLAS®グローバル脅威インテリジェンスフィードが連携して機能することで、インバウンドの脅威だけでなく、感染したホストからのアウトバウンド通信も防止することが可能です。

セキュリティスタックとの統合

REST APIの活用、STIX/TAXIIのサポート、そしてATLASが提供するコンテキストに基づく脅威インテリジェンスによって、AEDを既存のセキュリティスタックとプロセスに統合することが可能です。

インテリジェントに自動化されたハイブリッドDDoS防御ソリューション

インテリジェントに自動化された、クラウドベースのArbor CloudおよびオンプレミスのAEDの組み合わせによる完全なマネージド型のサービスは、ATLASグローバル脅威インテリジェンスによって継続的に保護されており、今日の高度なDDoS攻撃に対して包括的な保護体制を構築することができます。

脅威となるアウトバウンド通信の検知とブロック

AEDのATLASから配信されるレピュテーションベースの脅威インテリジェンスによって、感染した社内ホストからのアウトバウンド通信を検知し、ブロックします。これにより、マルウェアのさらなる拡散、データ漏洩および侵害を阻止できるようになります。

仮想環境、ハイブリッドクラウド環境に対応

AEDアプライアンスの仮想バージョンであるvAED（仮想AED）は、Amazon Web Servicesをはじめとする仮想プライベート環境で動作するため、ハイブリッドクラウド環境において統一された保護対策を適用することが可能になります。

NETSCOUT AEDアプライアンス

技術仕様	2600	2800
サイズ	**シャーシ：**2Uラックサイズ、**高さ：**3.45インチ（8.67cm）、**幅：**17.14インチ（43.53cm）、**奥行：**20インチ（50.8cm）、**重量：**36.95lbs（17.76kg）	
電源オプション	**DC：**ホットスワップ対応DC電源 x 2（冗長構成）、**DC出力定格：**-40 ～ -72 VDC、最大28/14 A（各DC入力あたり）、**AC：**ホットスワップ対応AC電源 x 2（冗長構成）、**AC出力定格：**100 ～ 240 VAC、50 ～ 60Hz、最大12/6A、**消費電力（W）：**315W（標準）、375W（最大）	
内蔵ストレージ	2 x 120GB SSD（RAID 1構成）	2 x 240GB SSD（RAID 1構成）
環境	**動作時：**温度：41°F ～104°F（5° ～ 40°C）湿度：5 ～ 85% **非動作時：**温度：-40° ～158°F（-40° ～ 70°C）、湿度：95%	
メモリ	32GB	64GB
プロセッサ	2 x Intel Xeon E5-2608L v3（6コア）、2GHz 消費電力（W）：315W（標準）、375W（最大）	2 x Intel Xeon（12コア）E5-2648L v3、1.80GHz
オペレーティングシステム	独自の組込み型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
防御用インタフェース	• 4、8、12 x 1Gバイパスポート（銅線/SXファイバー/LXファイバー） • 4 x 10Gバイパスポートおよび0、4、8 x 1Gバイパスポート	• 4 x 10 GigE（SR/LR/混合ファイバー） • 8 x 10 GigE（SR/LR/混合ファイバー） • 8 x 10 GigE（SR/LR/混合ファイバー）+ 4 x 1 GigE（SXファイバー/LXファイバー/銅線）
トラフィックバイパスオプション	統合ハードウェアバイパス、内部ソフトウェアバイパス（トラフィックを検査せずに通過）	
レイテンシ	80 マイクロ秒未満	
可用性	インラインバイパス、冗長電源、SSDのRAIDクラスタ	
MTBF（平均故障間隔）	44,000時間	
準拠規格	KCC（韓国）、RoHS指令2002/95/EC（欧州）、UL60950-1/CSA 60950-1（USA/Canada）、IEC60950-1（International）	

DDoSおよび高度なサイバー脅威に対する保護

技術仕様	2600	2800
検査スループット	100Mbps、250Mbps、500Mbps、1Gbps、2Gbps、5Gbps、10Gbps、15Gbps、20Gbps（ライセンスに依存）	10Gbps、20Gbps、30Gbps、40Gbps（ライセンスに依存）、ソフトウェアによるアップグレードが可能
DDoSフラッド攻撃の防御レート（最大）	最大15M pps	最大28.80M pps
同時接続数	非該当：AEDは接続をトラッキングしません	
秒あたりのHTTP(S)接続数	368K（推奨保護レベルの場合） 613K（フィルタリングリストのみによる保護の場合）	1,351K（推奨保護レベルの場合） 1,497K（フィルタリングリストのみによる保護の場合）
SSL復号オプション	**検査スループット：**750Mbpsおよび5Gbps（オプション） **HTTPS接続数：**最大7,500（750M HSM）/45,000（5G HSM） **同時セッション数：**最大150,000セッション	**検査スループット：**最大5Gbps **HTTPS接続数：**最大45,000 **同時セッション数：**最大150,000セッション
	サポートする暗号化プロトコル：SSL 3.0、TLS 1.0/1.1.1.2、サポートする暗号化スィート：RSA、ECDH、ECDHE、FIPS 140-2 Level 2および3をサポート、FIPS 140-2 Level 3向けの個別のTrusted-Path（高信頼パス）管理、セキュアな不正開封防止エンクロージャ（エンクロージャが侵害されるとキーはクリアされます）	
キーと証明書のペア数（最大）	1998	
保護可能なエンドポイント数	無制限	
認証	デバイス上、RADIUS、TACACS	

技術仕様	2600	2800
管理	SNMP get v1/v2c、SNMP trap v1/v2c/v3、CLI、Web UI、HTTPS、SSH（カスタマイズ可能なロールベース管理）、AEDコンソールで最大50台のAED（ハードウェアアプライアンス/KVMハイパーバイザー上で実行する仮想AED）を管理可能、管理対象のAEDはv5.11以上の実行が必要、vAEDコンソールはハイパーバイザー上で実行可能	
保護グループ数	100	
レポートおよびフォレンジクス	IPV4/IPV6トラフィックのリアルタイムおよび履歴レポート、総トラフィック、通過/ブロックしたトラフィック、URL/サービス/ドメインの上位宛先リスト、攻撃のタイプ、ブロックされた発信元、IPロケーションによる上位発信元リストをはじめとする、保護グループおよびブロックされたホスト別の詳細なドリルダウン機能を提供。リアルタイムのパケット可視化が可能	
DDoS防御	TCP/UDP/HTTP(S)フラッド攻撃、ボットネットからの防御、ハクティビストからの防御、ホストの挙動パターンに基づく防御、アンチスプーフィング、設定可能なエクスプレッションを使用するフローのフィルタリング、エクスプレッションを使用するペイロードのフィルタリング、常時および動的ブラックリスト/ホワイトリスト、トラフィックシェーピング、HTTP/DNS/SIPに対する多重防御、TCP接続制限、フラグメンテーション攻撃、コネクションフラッド攻撃	
動作モード	インラインアクティブ、インラインインアクティブ（レポートのみ、ブロックは無効）、SPANポートによる監視	
クラウドシグナリング	対応（サービスプロバイダー/Arbor Cloudとの連携による協調的なDDoS攻撃ミティゲーション）	
通知	SNMP trap、syslog、メール	
Webベース GUI	日本語を含む複数言語のユーザーインタフェースを利用可能	
サポートするブラウザ	Internet Explorer v10/11、Firefox ESR v31、Firefox v40、Chrome v44、Safari v6	
最大IoC（侵害の痕跡）サポート数	300万種類以上	
IoCの種類	IPアドレス、完全修飾ドメイン名、URL	

NETSCOUT AEDコンソール

技術仕様	2600	2800
サポートするプラットフォーム	アーバー製アプライアンス、仮想マシン	
管理可能なAED数（最大）	50台	
仮想AEDコンソールの動作要件	VMware vSphere 5.5以降、2 CPU、100GBのストレージ領域、4GB RAM、1つの管理インタフェース（オプションで2番目の管理インタフェースを利用可能）	
管理オプション	個別/すべてのAEDで構成と確認が可能：ハードウェア/ソフトウェアの状態、システム/セキュリティに関するアラート、ブロックされたホスト、ATLASによる脅威サマリー、サーバーの種類、保護グループ（IPv 4/6）、ブラックリスト/ホワイトリスト、エグゼクティブ向け管理レポート	
サポートするブラウザ	Internet Explorer v10/11、Firefox ESR v31、Firefox v40、Chrome v44、Safari v6	

NETSCOUT AEDコンソール 7000アプライアンス

技術仕様	2600	2800
メモリ	128GB（8 x 16GB DIMM）	
プロセッサ	Intel Xeon（12コア）— ES-2648Lv3 —1.8GHz — 20Mキャッシュ — 9.60GT/秒 — 75W	
電源要件	冗長構成の負荷分散型、自動感知式850W二重化電源、AC：100 ～ 240VAC、50/60Hz、12/6A、DC：-40 ～ -72V、最大28/14A	
サイズ	**シャーシ：**2Uラックサイズ、**高さ：**3.45インチ（8.67cm）、**幅：**17.4インチ（43.53cm）、**奥行：**20インチ（50.8cm）、**重量：**36.95 lbs（17.76Kg）、標準的な19インチ/23インチラックに搭載可能	
内蔵ストレージ	6 x 480GB SSD（RAID 5構成）	
ネットワークインタフェース	2 x 1GigE（銅線SFP、GigE SX、GigE LX）	
環境	**動作時：**温度：41° ～ 104°F（5° ～ 40°C）、湿度：95%　**非動作時：**温度：73° ～ 104°F（23° ～ 40°C）	
オペレーティングシステム	独自の組込み型ArbOS®オペレーティングシステム（Linuxベース）	
準拠規格	EN61000-3-2、EN61000-3-3、CISPR22Class A、CISPR 24 Immunity、FCC 47CFR Parts 15Class A	

仮想 AED

技術仕様	2600	2800
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 シリーズ、OpenStack Heat、OpenStack Tacker、Ansible、Nokia Cloudband、Cisco NSO/ESC、Cisco NFVIS、Amdocs、Netcracker、およびその他の ONAP、ETSI NFV Management and Orchestration（MANO）などの各種テクノロジー	
Amazon AWS のサポート	Amazon EC2 をサポート	
仮想マシンの最小要件	vCPU*：2、NIC：1 ～ 10、メモリ：6GB、ストレージ容量：100GB	
サポートするハイパーバイザー	VMware vSphere 5.5 以降	KVM カーネル 3.19 QEMU 2.0
インスタンスあたりの検査スループット	1Gbps	1Gbps
インスタンスあたりの DDoS フラッド攻撃防御レート（最大）	910Mbps	600Kpps
保護グループ数	10（4 vCPU、12GB RAM の場合 50）	10（4 vCPU、12GB RAM の場合 50）

NETSCOUT

米国本社
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
TEL：+1 978-614-4000
www.netscout.com

アーバーネットワークス株式会社
101-0063　東京都千代田区神田淡路町 2-105
ワテラスアネックス 13 階
TEL：03-3525-8040
EMAIL：japan@arbor.net
WEB：jp.arbornetworks.com

NETSCOUT は、世界 32 カ国以上の国々で製品、サポート、サービスを提供しています。各国の事業拠点所在地、電話番号などのお問い合わせ先は、NETSCOUT の Web サイトでご参照ください。
www.netscout.com/company/contact-us

SECPDS_013_JP-1804 11/2018