データシート

A10 Defend DDoS Mitigator ハードウェアアプライアンス

DDoS Mitigator	Thunder 1060S *6	Thunder 3350-E
モジュラーライセンス	5/10/20 Gbps	—
パフォーマンス		
スループット（ソフトウェアスクラビング）*1	5/10/20 Gbps	10 Gbps
ハードウェアブロッキング	—	—
パケット数／秒（pps）*1	250万/500万/800万	600万
ソフトウェアベース - SYN認証（pps）	250万/500万/800万	600万
ハードウェアベース - アノマリーフラッドブロッキング（pps）	—	—
監視対象セッション最大数（非対称型導入）	800万/1,000万/1,600万	800万
平均遅延	15 µs	20 µs
最低レートリミットインターバル	100 ms	100 ms
権威DNSキャッシュパフォーマンス		
DNS クエリ数/秒（qps）	—	—
ネットワークインターフェイス		
1 GEカッパー	7	6
1 GEファイバー（SFP）	0	2
10/1 GEファイバー（SFP+/SFP）	4	8 + 4*3
25/10 GEファイバー（SFP28/SFP+）	2	0
40 GEファイバー（QSFP+）	0	0
100/40 GEファイバー（QSFP28/QSFP+）	0	0
400 GEファイバー（QSFP-DD）	0	0
管理ポート	イーサネット管理ポート x 1、RJ-45コンソールポート x 1	
ハードウェア仕様		
プロセッサー	Intel communications processor 20-core*6	Intel Xeon 8-core
メモリー（ECC RAM）	32 GB	16 GB
ストレージ	SSD	SSD
ハードウェアアクセラレーション	ソフトウェア	ソフトウェア
外形寸法	44.45 mm（高さ）x 444.5 mm（幅）x 438.15 mm（奥行）	44.45 mm（高さ）x 444.5 mm（幅）x 457.23 mm（奥行）
ラックユニット（マウント可能）	1U	1U
重量	5.44 kg	8.16 kg
電源（DCオプションあり）	デュアル 300W RPS	デュアル 750W RPS
	AC100～240V、50～60Hz、80 PLUS「Platinum」認定の電力変換効率	
消費電力（通常/最大）*2	112W / 127W	151W / 205W
発熱量（BTU/h）（通常/最大）*2	383 / 434	516 / 700
冷却ファン（前面吸気、背面排気）	リムーバブルファン	ホットスワップスマートファン
動作環境	動作時温度：0°～40°C、保管時温度：-20～75°C、動作時/保管時湿度：5%～95%（結露無きこと）	
規格準拠	FCC Class A, UL, ICES, CE, UKCA, CB^, VCCI, BSMI^, RCM | RoHS	FCC Class A, UL, CE, UKCA, CB, VCCI, BSMI, RCM, MTCTE^ | RoHS

A10 Defend DDoS Mitigator ハードウェアアプライアンス

DDoS Mitigator	Thunder 7465			Thunder 8665S
モジュラーライセンス	40 Gbps	100 Gbps	270 Gbps	—
パフォーマンス				
スループット(ソフトウェアスクラビング)[*1]	40 Gbps	100 Gbps	270 Gbps	550 Gbps
ハードウェアブロッキング	800 Gbps	800 Gbps	1 Tbps	4.8 Tbps
パケット数／秒(pps)[*1]	1,300万	2,800万	6,000万	1億2,000万
ソフトウェアベース - SYN認証(pps)	1,300万	2,800万	6,000万	1億2,000万
ハードウェアベース - アノマリーフラッドブロッキング(pps)	5億5,000万	5億5000万	5億5,000万	8億2,000万
監視対象セッション最大数(非対称型導入)	3,200万	6,400万	1億2800万	3億5,000万
平均遅延	40 µs	40 µs	40 µs	40 µs
最低レートリミットインターバル	100 ms	100 ms	100 ms	100 ms
権威DNSキャッシュパフォーマンス				
DNS クエリ数/秒(qps)	—	—	—	—
ネットワークインターフェイス				
1 GEカッパー	0	0	0	0
1 GEファイバー(SFP)	0	0	0	0
10/1 GEファイバー (SFP+/SFP)	0	0	0	0
25/10 GEファイバー (SFP28/SFP+)	24	24	24	0
40 GEファイバー(QSFP+)	0	0	0	0
100/40 GEファイバー(QSFP28/QSFP+)	8	8	8	0
400 GEファイバー (QSFP-DD)	0	0	0	12
管理ポート	イーサネット管理ポート x 1、RJ-45コンソールポート x 1			イーサネット管理ポート x 2、RJ-45コンソールポート x 1
ハードウェア仕様				
プロセッサー	Intel Xeon 36-core[*6]			Intel Xeon 36-core
メモリー(ECC RAM)	256 GB			512 GB
ストレージ	SSD			SSD
ハードウェアアクセラレーション	FTA-6 x 1 、SPE			FTA-6 x 3、SPE
外形寸法	44.45 mm(高さ) x 444.5 mm(幅) x 762 mm(奥行)			66.67 mm(高さ) x 444.5 mm(幅) x 762 mm(奥行)
ラックユニット(マウント可能)	1U			1.5U
重量	17.47 kg			20.36 kg
電源(DCオプションあり)	デュアル 1500W RPS			デュアル 2500W RPS
	AC100～240V、50～60Hz、80 PLUS「Platinum」認定の電力変換効率			
消費電力(通常/最大)[*2]	680W / 770W			1,491W / 1,720W
発熱量(BTU/h) (通常/最大)[*2]	2,321 / 2,628			5,088 / 5,869
冷却ファン(前面吸気、背面排気)	ホットスワップスマートファン			
動作環境	動作時温度:0°～40°C、保管時温度:-20～75°C、動作時/保管時湿度:5%～95%(結露無きこと)			
規格準拠	FCC Class A, UL, CE, UKCA, CB, VCCI, KCC, BSMI^, RCM, MTCTE^, ANATEL^ | RoHS			FCC Class A, UL, CE, UKCA, CB, VCCI, RCM | RoHS

仕様およびパフォーマンスの数値は予告なしに変更されることがあり、構成および環境条件によって異なります。ネットワークインターフェイスに関しては、ネットワークの信頼性と安定性の確保のため、A10が認定した光トランシーバー以外の利用はサポートしておりません。

*1 スループットのパフォーマンスはトラフィック転送キャパシティであり、DDoS対策を有効にした正規のトラフィックで測定されます | *2 標準構成時。値はSSLやハードウェアバイパスオプションによって異なる場合があります。| *3 10Gのみサポート | *4 RPSオプションあり | *5 デュアルレートの固定SFP+光ポート(10GBASE-SR及び1000BASE-SX) | *6 有効なCPUコア数はモジュラーライセンスによって異なります。| ^ 認可申請中

A10 Defend DDoS Mitigator 仮想アプライアンス

A10 Defend DDoS Mitigator 仮想アプライアンス	
ハイパーバイザー	VMware ESXi 7.0 or higher (SR-IOV, DirectPath I/O), KVM QEMU (SR-IOV, PCI Passthrough)
ハードウェア要件	インストールガイド参照

仮想アプライアンスのサイジングの推奨事項

スループット	Lab/1/2/5 Gbps	50 Gbps *1	100 Gbps *1
vCPU	6	16	32
vRAM	16 GB	32 GB	64 GB
vDisk	128 GB	256 GB	384 GB
ライセンス	帯域ライセンス（インスタンス毎）	FlexPool	FlexPool
ハイパーバイザー	ESXi, KVM	ESXi, KVM	ESXi, KVM

*1 ESXi の場合は ACOS 6.0 以上、KVM の場合は ACOS 7.0.2 以上でサポート。NVIDIA Mellanox ConnectX-6 NIC でテスト済

A10 Defend DDoS Mitigator for Cloud	Microsoft Azure
インスタンスごとのスループット	5 Gbpsまで
イメージフォーマット	Microsoft VHD
ライセンス	30日間のトライアルライセンス｜BYOL FlexPoolライセンス

機能一覧

機能はアプライアンスによって異なる場合があります。

検知 / 分析

- インライン構成によるパケットベースの DDoS 検知
- 25.6 万以上の検知ポリシー（サーバ / サービス）
- しきい値の手動 / 自動設定
- プロトコルアノマリー検知
- IPinIP 内の検査（ネットワーク化、カプセル化など）
- 許可リスト／拒否リスト
- トラフィックインジケーター /トップトーカー
- ミティゲーションコンソール
- パケットデバッガツール
- Top- k インサイト（送信元、宛先）
- アウトバウンドデテクション
- 攻撃対象 IP の識別

DDoS 脅威インテリジェンス リスト

- 最初の防御層として有害な IP アドレスをプロアクティブにブロックする、大容量クラスリスト
- 最大 9,600 万のアクティブ エントリ - 最大 8 つのリストにそれぞれ最大 1,600 万のエントリ
- リストごとにアクションまたは緩和ポリシーを定義可能
- ThreatSTOP や A10 Defend Threat Control の IP ブロックリストなど、さまざまな DDoS 脅威インテリジェンスフィードをサポート

ゼロデイ自動防御

- ZAPR: 機械学習型攻撃パターン認識・フィルタリング
- TCP プログレッショントラッキング
- ゼロデイ攻撃からの防御
- 事前設定や手動設定が不要
- 迅速な自動応答

リソース攻撃防御

- フラグメント攻撃
- Slowloris
- スロー GET/POST
- ロングフォーム送信
- SSL 再ネゴシエーション

アプリケーション攻撃防御

- アプリケーション認識型フィルタ
- 正規表現によるフィルタリング（TCP/UDP/HTTP/SIP）
- HTTP リクエストレートリミット（URL 単位）
- DNS リクエストレートリミット (Type、FQDN、Label count)
- SIP リクエストリミット (type 単位)
- アプリケーションリクエスト不正チェック (DNS/HTTP/SIP)
- DNS ドメインリスト
- HTTP/S プロトコル準拠
- アプリケーション（DNS/HTTP/SIP ）フラッド防御
- シグネチャ・ベース IPS
- QUIC のバージョン制御 / 不正ヘッダチェック
- ゲームトラフィック用パケットウォーターマーキング（UDP）
- 暗号化されたフラッド攻撃からの防御

プロトコル攻撃防御

- 無効パケット
- TCP フラグの異常な組み合わせ（フラグなし、SYN/FIN、SYN フラグ、LAND 攻撃）
- SYN-ACK 増幅攻撃防御
- IP オプション
- パケットサイズの検証（Ping of Death）
- POODLE 攻撃
- TCP/UDP/SSL/ICMP フラッド防御
- コネクション毎のトラフィック制御

チャレンジベース認証

- TCP SYN クッキー、SYN 認証
- ACK 認証
- スプーフ検知
- DNS 認証
- HTTP チャレンジ

保護対象サーバ / ネットワーク

- 自動的に検知・緩和可能な保護ゾーン
- 送信元 / 宛先 IP アドレス / サブネット
- 送信元 / 宛先 IP ペア
- 宛先ポート
- 送信元ポート
- プロトコル（HTTP、DNS、SIP、TCP、UDP、ICMP、その他）
- クラスリスト / ジオロケーション
- パッシブモード
- アウトバウンドミティゲーション（シンメトリックデプロイメント）

Non-Stop DNS Solution

- 権威 DNS キャッシュとして動作
- A10 Defend Mitigator と連携した階層型防御
- DNS 水攻め攻撃（ランダムサブドメイン攻撃）からの防御
- 選択 / カスタマイズ可能なレスポンス / フォワード / ドロップ

アクション

- パケットキャプチャ
- スクリプト実行
- ドロップ
- TCP リセット
- 動的認証
- 拒否リストへの追加
- 許可リストへの追加
- ログ出力
- 同時接続の制限
- コネクションレートリミット
- トラフィックレートリミット（pps/bps）
- 他のデバイスへの転送
- Remote Triggered Black Hole（RTBH）
- BGP Flowspec

管理機能

- オンボックス専用管理インターフェイス（GUI、CLI、SSH、Telnet）
- A10 Defend Orchestrator による管理
- SNMP、syslog、電子メールアラート
- REST API（aXAPI）/SDK
- LDAP、TACACS+、RADIUS
- コントロール CPU 設定機能

ネットワーキング / デプロイメント

- プロアクティブ、リアクティブ、アシンメトリック、シンメトリック、アウトオブバンド（TAP）
- 透過型（L2）、ルーティング（L3）
- ヴァーチャルワイヤ
- ルーティング：スタティックルート、BGP4+、OSPF、OSPFv3、IS-IS
- Bidirectional Forwarding Detection (BFD)
- VLAN（802. 1Q）
- トランキング（802. 1AX）、LACP
- アクセス制御リスト（ACL）
- ネットワークアドレス変換（NAT）
- MPLS トラフィック保護
- BGP ルートインジェクション
- BGP FlowSpec
- IPinIP（送信元と終端）
- GRE トンネル終端
- VXLAN

テレメトリ

- トラフィック /DDoS 統計値カウンタ
- sFlow v5
- NetFlow（v9、IPFIX など）
- フローベースエクスポート用カスタムカウンタブロック
- 高速ログ出力
- CEF ロギング

ハイパフォーマンス・スケーラブルプラットフォーム

- Advanced Core Operating System（ACOS）
- リニアアプリケーションスケーリング
- ACOS によるデータプレーン制御
- コントロールプレーンに Linux を実装
- IPv6 対応
- SPE (Security policy engine): ポリシー制御のハードウェアアクセラレーション *
- 高性能ハードウェア ブロッキング *

キャリアグレードのハードウェア *

- 先進のハードウェアアーキテクチャ
- ホットスワップ冗長電源 (AC および DC)
- スマートファン (ホットスワップ)
- ソリッドステートドライブ (SSD)
- 改ざん検出
- 25GE, 40GE, 100GE および 400GE ポート

セキュリティおよび機能保証認定 *

- 共通基準 EAL 2+
- FIPS 140-1 レベル 1 準拠 (全モデル)

* 機能はアプライアンスによって異なる場合があります。

A10 Networks / A10 ネットワークス株式会社について

A10 Networks は、オンプレミス、ハイブリッドクラウド、エッジクラウド環境における、セキュリティ、インフラストラクチャの課題を解決するソリューションを提供しています。大手グローバル企業や通信、クラウド、Web サービス事業者まで 7000 社以上のお客様に導入いただいており、ビジネスに不可欠なアプリケーションやネットワークの安全性、可用性、効率性を高めています。A10 ネットワークスは 2004 年に設立されました。米国カリフォルニア州サンノゼに本社を置き、世界中のお客様にサービスを提供しています。

A10 ネットワークス株式会社は A10 Networks の日本子会社であり、お客様の意見や要望を積極的に取り入れ、革新的なアプリケーションネットワーキングソリューションをご提供することを使命としています。 詳しくはホームページをご覧ください。

• URL：https://www.a10networks.co.jp/ • X（旧 Twitter）：https://twitter.com/a10networksjp • Facebook：https://www.facebook.com/A10networksjapan

Learn More

About A10 Networks

お問い合わせ

A10networks.co.jp/contact

A10ネットワークス株式会社

www.a10networks.co.jp

Part Number: A10-DS-15136-JA-02 JUL 2026