DATA SHEET

FortiDDoS

提供形態：

アプライアンス　仮想マシン

FortiDDoS 200F、1500E、1500E-DC、1500F、2000E、2000E-DC、2000F、VM04 / 08 / 16

DDoS（Distributed Denial of Service）攻撃は、依然としてネットワークセキュリティに対する最大の脅威となっており、重要なオンラインサービスを停止させることを目的としてあらゆる面で巧妙化が進んでいます。

不正侵入やマルウェア攻撃とは異なり、DDoS の攻撃者は、エンドポイントサーバーを標的にしなくても被害を与えられることをわかっており、使用されていない IP アドレス、ISP リンクサブネット、ファイアウォール / プロキシ / WiFi ゲートウェイのパブリック IP アドレスなど、ネットワークにつながるあらゆる IP アドレスを攻撃対象にします。

CDN や DNS ベースのクラウドによる減災では、それらの攻撃を阻止できません。ファイアウォールが DDoS 攻撃を受けてユーザーがクラウドサービスにアクセスできなくなるとしたら、ビジネスにどのような影響が出るでしょうか。

高度なマルチベクトル / マルチレイヤー DDoS 攻撃では、直接的なパケット送信だけでなくリフレクション攻撃などが用いられ、ソース IP アドレスは偽装されランダムに変更されるので、ACL では対応できません。これらの攻撃は、Mirai のようなコードから多数の亜種が派生するにつれて、またストレッサー事業者によって攻撃の代行サービスが行われるようになるにつれて、ますます頻繁に発生するようになってきています。誰でもわずかな金額で大規模で匿名の攻撃を仕掛けることができます。

セキュリティチームが日常的に DDoS を経験するわけではなく、ネットワークを標的にする何千もの攻撃の亜種を理解することはできないでしょう。

このような攻撃に対抗するには、広範囲の攻撃対象領域を動的かつ自動的に保護するソリューションが必要です。

独自の優れたアプローチにより DDoS 攻撃を減災

FortiDDoS の超並列機械学習アーキテクチャは、最も高速で正確な DDoS 攻撃の減災を可能にします。

FortiDDoS では、一部の攻撃パターンを特定するための事前定義やサブリスクションベースのシグネチャは必要なく、自律型の機械学習を使用して平常時のアクティビティのベースライン（基準）を数十万ものパラメータから作成し、それらのベースラインに照らしてトラフィックパターンを監視します。攻撃が開始すると、FortiDDoS が逸脱を検知し、多くの場合に最初のパケットから攻撃を減災するアクションを実行します。

FortiDDoS は、お客様のチームやベンダーの ERT / NOC が介入することなく、攻撃を監視し、実行したレスポンスと減災のレポートを提示します。

ハイライト

- 100% のパケットインスペクションでレイヤー 3、4、7 の DDoS 攻撃を特定して減災し、超並列コンピューティングアーキテクチャによって大量のパラメータを同時に監視
- 機械学習による 100% の DDoS 攻撃検知
- IP アドレスも MAC アドレスもデータパスにないため、攻撃者からは完全に不可視（FortiDDoS はレイヤー 3 のルーティングデバイスでも終端デバイスでもありません）
- 継続的な脅威評価機能により、「誤検知」を最小限に抑制
- 高度な DNS / NTP DDoS の減災と高度な DTLS の減災（F シリーズ）
- 攻撃シグナリングにより、オンプレミス / クラウドの両方に対応するハイブリッド減災機能を利用可能

ハイライト

強力な並列アーキテクチャ：柔軟な自律型の防御力

FortiDDoS は、減災のためにローカルでシグネチャを作成したり、サブスクリプションサービスを利用したりしなくても、既知の攻撃や「ゼロデイ」攻撃を防ぐことができます。他のベンダーは、リアルタイムの CPU の使用率を抑えるため、明示的なシグネチャが作成されない限り、比較的少ない数のパラメータを低サンプリングレートでインスペクションすることでリソースを節約しようとします。FortiDDoS の超並列アーキテクチャは、最小サイズのパケットであっても、それぞれの保護プロファイルで 23 万以上のパラメータを使用して 100% のサンプリングを実行します。これにより、FortiDDoS は完全に自律的に機能して、特定の攻撃を最初のパケットで検知し、すべての攻撃をわずか 2 秒以内で検知できるようにしています。このように広範かつ迅速な減災策を提供できるベンダーや方式は他にはありません。攻撃を受けている最中に、設定を調整したり、pcap を読み込んだり、正規表現のシグネチャや ACL を追加したりする必要はありません。攻撃が軽減されても、FortiDDoS は、新たな脅威ベクトルや変更された脅威ベクトルに速やかに対応できるように、他のすべてのパラメータの監視を継続します。

ボットネットの再興

侵害されやすい IoT デバイスはボットネット攻撃が再び増加する原因となり、IoT の急増によってボットネットは間違いなく蔓延すると考えられます。デバイス毎のトラフィックはそれほど多くなくても、デバイス数が多ければ大量のトラフィックが発生します。攻撃者は、偽装したソース IP アドレスを使用して、直接型およびリフレクション型の UDP、SYN、TCP アウトオブステート（FIN、ACK、RST）、DNS、プロトコルフラッドを大量に発生させ、ボット感染したデバイスの実際のソース IP アドレスを隠そうとします。攻撃者がかつてないほど多種多様な攻撃ベクトルを同時に利用する可能性もあります。小さなパケットのフラッドによって、ルーター、ファイアウォール、多数の DDoS アプライアンスの負荷が急増するために、パケットインスペクションの完全な実行が妨げられ、予想外の事態を招くことがありますが、FortiDDoS であれば、小さいパケットでもクラス最高レベルのインスペクション率を実現します。

DNS ベースの攻撃

ボットネットを利用した DNS 攻撃が頻繁に見られるようになっています。これは、それらの攻撃があらゆるタイプのインフラストラクチャを標的にしたり、DNS サーバーを不正利用して他のサーバーにリフレクション型 DDoS 攻撃を仕掛けたりできるためです。FortiDDoS は、双方向のすべての DNS トラフィックをインスペクションしてあらゆる直接型 / リフレクション型の DDoS 攻撃からユーザーを保護する唯一の DDoS 攻撃減災プラットフォームです。30 以上のパラメータを使用して、すべての DNS パケットを最大 1,200 万クエリ / 秒で検証します。また、内蔵キャッシュによってフラッド発生時にローカルサーバーの負荷を軽減することもできます。FortiDDoS は、革新的な DQRM 機能によって最初のパケットが受信された時点で DNS リフレクション攻撃を阻止します。また、独自の Legitimate Query（正当なクエリ）と DNS Allowlist（DNS 許可リスト）の機能により、権威 DNS サーバーがリフレクション型攻撃に悪用されるのを防止します。

セキュリティ ファブリック

フォーティネット セキュリティ ファブリックを構成する製品は、専用設計のハードウェアを専用のエンジニアリングサービスやサポートリソースと共に使用することで、各製品がフォーカスする領域でクラス最高レベルの保護を実現します。FortiDDoS は、それらの製品の機能を補完し強化します。FortiDDoS では、システムパフォーマンスと減災策がリアルタイムで FortiOS のセキュリティ ファブリックダッシュボードに表示され、DDoS 攻撃と減災状況を他のセキュリティ ファブリック製品やパートナー製品と併せて一元的に表示し、確認することができます。

オンプレミス / クラウドに対応するハイブリッドな DDoS 減災機能

FortiDDoS は受信トラフィック用の帯域幅を占有するあらゆる DDoS 攻撃を減災することができますが、攻撃が大規模な場合、受信リンクが飽和状態になり、ISP ルーターで正常なトラフィックがドロップされる可能性があります。攻撃がアップストリームリソース輻輳の脅威となる状況においても、FortiDDoS では一般公開と文書化がなされている攻撃シグナリング API を利用し、ファブリック レディ パートナー各社が提供するクラス最高レベルのハイブリッド CPE / クラウド DDoS 減災対策を選択することができます。FortiDDoS は、クラウド DDoS プロバイダーから受信した無害な GRE トラフィックのインスペクションによって、継続的なログ記録レポート、および完全な脅威の減災を保証します。また、オンプレミス用の FortiDDoS アプライアンスは、使用している ISP に Flowspec スクリプトを提供するため、攻撃トラフィックの迂回やマルチパラメータベースのブロックもサポートできます。

減災策の比較：常時稼働のインライン型とアウトオブパス型

アウトオブパス型の検知、迂回、検疫では重要なインフラストラクチャの保護には不十分であり、迅速な対応も不可能であるため、多くのホスティングサービスプロバイダーや MSSP、ISP が他の手法に移行しています。ネットフローベースの検知と減災では、数種類の攻撃しか監視できません。そのため、例えば監視対象外の UDP リフレクションポートが攻撃されると、減災が過度に拡大して、すべての UDP トラフィックをブロックすることになる可能性があります。Google のサービスや、Zoom や Teams などの会議サービスはいずれも UDP を使用しているため、このような状況はビジネス継続性にとって好ましいことではありません。

FortiDDoS は、150 以上の攻撃イベントを減災するだけでなく、それらの多くについて詳細な減災を実行します。例えば、すべての UDP ではなく、使用される可能性のある 10,000 以上の UDP リフレクションポートを監視して、攻撃ポートをブロックします。

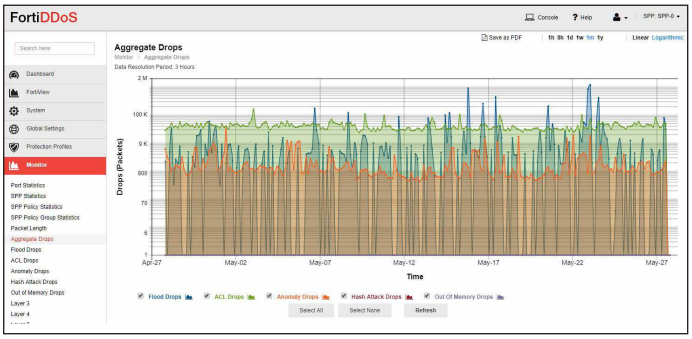
DDoS 攻撃の 75% は 15 分未満であることが研究によって明らかになっており、また、マルチベクトル型攻撃では攻撃ベクトルが逐次変更され、パルス型攻撃では断続的な攻撃が頻繁に行われます。FortiDDoS は、検知からわずか 2 秒以内に減災を開始し、大量の検知と減災を並行して行うことで、ユーザーの介入を必要とすることなく、マルチベクトル型、連続型、パルス型の攻撃を発見して阻止します。

システム障害の発生時においてもネットワークの継続性を確保するため、すべての FortiDDoS モデルは優れた可用性を備えており、光バイパス機能（最大 100 GbE）を提供するモデルもラインナップされています。

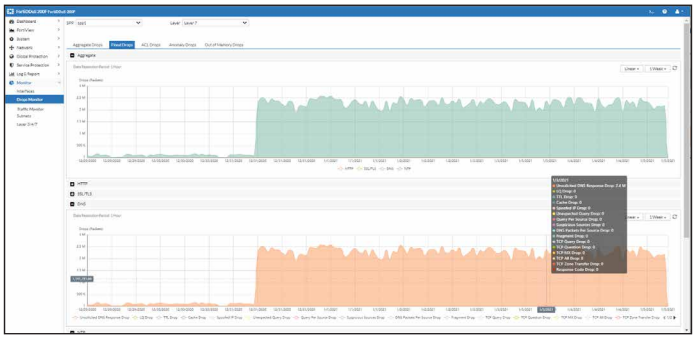
主な機能

機械学習による 100% の攻撃検知	FortiDDoS は、最新の脅威情報の更新が必要なシグネチャファイルに依存しないため、ユーザーは既知の攻撃だけでなく未知の「ゼロデイ」攻撃からも保護されます。「脅威保護」のためのサブスクリプションは不要で、運用コスト（OpEx）を節約することができます。
超並列アーキテクチャ	並列アーキテクチャの活用により、最小サイズのパケットであっても 100% のパケットインスペクションを実行し、レイヤー 3、4、7 の DDoS 攻撃の双方向の検知と減災を実現します。コストに対して期待するとおりのパフォーマンスが得られます。
攻撃の継続的な評価機能	「正常」なトラフィックを遮断してしまうことがないように攻撃の再評価を行い、「誤検知」のリスクを最小限に抑えます。管理に必要な時間の短縮に役立ちます。
高度な DNS 保護機能	FortiDDoS は、すべての DNS トラフィックを最大 1,200 万 QPS で 100% インスペクションすることにより、幅広い DNS に対する帯域幅占有型攻撃、アプリケーション攻撃、アノマリ攻撃からの保護を実現します。DNS リフレクション攻撃によるフラッドを、最初のパケットから阻止します。
高度な NTP 保護機能（一部のモデル）	FortiDDoS は、NTP のクエリと応答のすべてのトラフィックを最大 600 万 QPS で 100% インスペクションします。NTP リフレクション攻撃によるフラッドを、最初のパケットから阻止します。
継続的な学習	FortiDDoS では、最小限の設定を行うだけで平常時のトラフィックとリソースの振る舞いのプロファイルが自動的に作成されるため、時間や労力を節約して IT 管理リソースを有効活用できるようになります。
自律的な減災	どのような種類や規模の攻撃でも、オペレーターが介入する必要はありません。
オンプレミス / クラウドのハイブリッドなサポート	一般公開され、文書化されている API によってサードパーティのクラウド DDoS 減災サービスとの統合が可能となり、柔軟な導入配備オプションおよび大規模な DDoS 攻撃からの保護が提供されます。
フォーティネット セキュリティ ファブリックとの統合	攻撃の減災状況とネットワークパフォーマンスの一元的な可視化を実現し、管理に要する時間を短縮すると同時に、レスポンス時間を改善できます（一部のモデル）。
RESTful API	FortiDDoS は、独自の RESTful API を使用してほとんどすべての環境に統合することができます。
Central Manager による一元管理	複数の FortiDDoS ユニットを地理的に離れた場所で使用する場合は、FortiDDoS-CM（B / E シリーズ）を利用し、シングルサインオンですべてのデバイスを一元管理することが可能です。

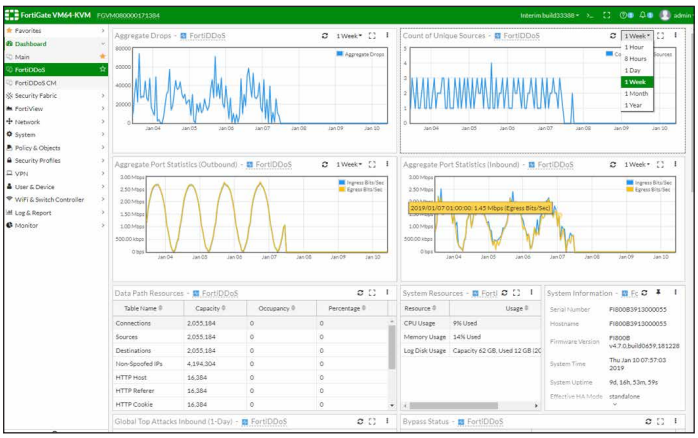
レポート



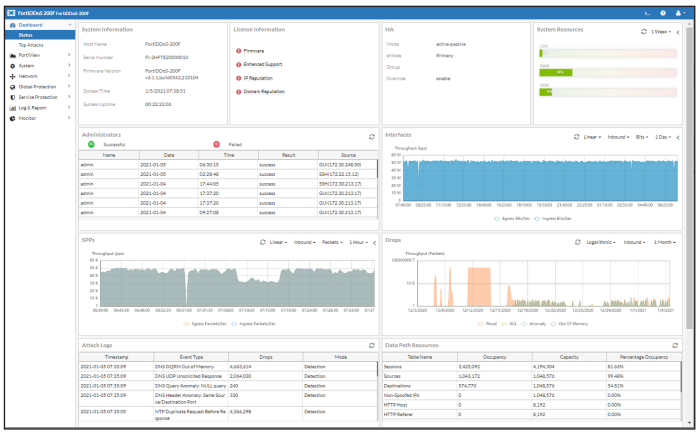
ドロップ数の総計（L3 ～ L7）（B / E シリーズ）



DNS 攻撃（F シリーズ）



FortiOS のセキュリティ ファブリックダッシュボード（B / E シリーズ）



ダッシュボード（F シリーズ）

FortiDDoS の主な機能 *

パケットインスペクションテクノロジー

- 100% のパケットインスペクション
- 単一の IP アドレスに対する IPv4 / IPv6 の完全サポート
- 予測分析、ヒューリスティック分析、適応分析のための機械学習
- 詳細なパケットインスペクション
- TCP ステートナレッジによるアウトオブステート型の攻撃の速やかな減災
- DNS 監視による DNS リフレクション攻撃の速やかな減災
- NTP 監視によるリフレクション攻撃の瞬時の減災（E シリーズ / F シリーズ）
- MAC や IP アドレスがデータパスに含まれず、攻撃者には完全に不可視
- 同時に発生する複数の攻撃ベクトルに対応可能な超並列処理

振る舞いのしきい値管理

- 機械学習による数百万の L3 ～ L7 パラメータのしきい値設定
- 重要な L3、L4、および L7 パラメータのしきい値を自動推定し、適応

100% のアノマリインスペクション

- L3 / L4 / L7 HTTP ヘッダー
- DNS ヘッダーとペイロード
- TCP ステートと状態遷移のアノマリ
- NTP ヘッダーとペイロード（E シリーズ / F シリーズ）

レイヤー 3 攻撃の減災

- プロトコルフラッド攻撃（256 種類すべてを監視）
- フラグメントフラッド攻撃（TCP / UDP / その他のプロトコル）
- ソースフラッド攻撃（最大 2,400 万種類まで監視）
- FortiGuard IP レピュテーションサブスクリプション
- 完全な L3 ～ L7 の GRE インスペクション

レイヤー 4 攻撃の減災

- TCP ポート（65,000 ポートすべて）
- UDP ポート（65,000 ポートすべて）
- TCP / UDP サービスポート（10,000 以上）
- ICMP タイプ / コード（65,000 ポートすべて）
- SYN、SYN / ラインスピードの送信先検証、SYN / ソース
- **最初のパケット**での TCP ステートフラット攻撃の減災
- 低速接続攻撃
- L4 接続のアグレッシブエージング

HTTP 攻撃の減災

- HTTP URL、リファラー、クッキー、ホスト、ユーザーエージェント
- HTTP METHOD フラッド攻撃（8 つの METHOD すべて、および METHOD 合計数 / ソース）
- SSL 再ネゴシエーション攻撃
- L7 アグレッシブエージング攻撃
- プロトコルのアノマリ（F シリーズ）
- 暗号のアノマリ（F シリーズ）
- GET / POST クライアント評価（F シリーズ）

攻撃の減災

- **最初のパケット**での DNS（B / E / F シリーズ）、NTP（E / F シリーズ）応答フラッド攻撃の減災（DQRM / NRM）
- DNS / NTP ヘッダー / ペイロード / ステートのアノマリ
- ソースごとの DNS クエリ / MX / ALL / ZT / フラグメントフラッド攻撃
- DNS 応答コードフラッド攻撃の減災
- NTP リクエスト / レスポンス / デスティネーションフラッドごとの応答
- DNS クエリ送信元の評価、予期しないクエリ、正当なクエリ
- DNS クエリ TTL 評価
- フラッド攻撃状態の DNS 応答キャッシュ
- DNS リソースレコードの ACL
- DNS ドメインレピュテーションサブスクリプション
- NTP 増幅リフレクションモード 7（monlist）、モード 6（varlist）レスポンスフラッドを**最初のパケット**から減災

* 注：すべての機能をすべてのプラットフォームがサポートしているわけではありません。一部のプラットフォームでのみサポートしている機能については、シリーズ名（B / E / F）を明記します。

FortiDDoS の主な機能 *

アクセス制御リスト

FortiDDoS は、パフォーマンスを損なわずに大量の ACL をハードウェアでサポートする業界唯一の製品です。ほとんどの DDoS 攻撃では偽装したソース IP アドレスが使用されますが、他のインフラストラクチャの負荷を軽減するため、既存の Indicators of Compromise IP address and Domain（感染 IP アドレスとドメインの侵害指標）リストをアップロードすることができます。

- IP レピュテーション：FortiGuard のサブスクリプションサービス
- IP / サブネットのブロックリスト / 許可リスト
- ユーザーによる IPv4 ブロックリストの一括アップロード（100 万アドレス以上に対応）
- ジオロケーション
- BCP38 送信元アドレスの評価 / ローカルアドレスアンチスプーフィング機能拡張（2,000 サブネット以上に対応）
- プロトコル、UDP、TCP、およびその他のプロトコルのフラグメント、DNS フラグメント、L4 ポート、ICMP タイプ / コード
- HTTP METHOD、URL、ホスト、リファラー、ユーザーエージェント
- DNS ドメインレピュテーション：FortiGuard サブスクリプションサービス（25 万以上の悪意あるドメインに対応）
- ユーザーによる DNS ドメインブロックリストの一括アップロード（50 万以上のドメインに対応）
- DNS リソースレコードの ACL（256 件のリソースレコード）
- IPv4 / v6、プロトコル、TCP / UDP ポート、ICMP タイプとコード、TCP / UDP / その他のフラグメントの ACL
- Flowspec ACL スクリプトの生成

包括的なレポート

- フィルタリング / エクスポート可能な攻撃ログ
- 以下を要約表示するグラフおよびログ機能：
  - 攻撃上位リスト / 攻撃者上位リスト
  - ACL がブロックしたトラフィック上位リスト
  - 攻撃されたサブネット / IP アドレス上位リスト
  - 攻撃されたプロトコル上位リスト
  - 攻撃された TCP / UDP ポート上位リスト
  - 攻撃された ICMP タイプ / コード上位リスト
  - 攻撃された URL、HTTP ホスト、リファラー、クッキー、ユーザーエージェント上位リスト
  - 攻撃された DNS サーバー上位リスト
  - 攻撃された DNS アノマリ上位リスト
  - 物理ポート、SPP、SPP ポリシー（サブネット）、SPP ポリシーグループの統計情報：Mbps / pps とドロップ数のグラフ
  - さまざまな形式のカスタム、オンデマンド、スケジュール指定、攻撃しきい値指定のレポート
  - 数百万の内蔵レポート用グラフをリアルタイム / フォレンジック分析に利用可能

イベントの一元レポート機能

- SNMP v2 / v3 MIB およびトラップ
- メールアラート、レポート
- オープン RESTful API
- FortiAnalyzer、FortiSIEM、サードパーティサーバーの Syslog サポート
- FortiDDoS の Central Manager による攻撃ログとサマリの一元管理（B / E シリーズ）

監査証跡

- ログインの監査証跡
- 構成の監査証跡

管理

- 完全な TLS 1.3 管理 GUI
- 完全な CLI
- オープン RESTful API（B / E シリーズ）
- 2FA やプロキシを含む RADIUS、LDAP、TACACS+ 認証
- マルチテナント対応 MSSP 用ポータル（B / E シリーズ）
- 複数の FortiDDoS を管理する Central Manager
- オープンクラウド減災シグナリング

* 注：すべての機能をすべてのプラットフォームがサポートしているわけではありません。一部のプラットフォームでのみサポートしている機能については、シリーズ名（B / E / F）を明記します。

技術仕様



	FortiDDoS 200F	FortiDDoS 1500F	FortiDDoS 2000F
ハードウェア仕様			
LAN インタフェース：Copper GbE、バイパス機能内蔵	4	—	—
WAN インタフェース：Copper GbE、バイパス機能内蔵	4	—	—
LAN インタフェース：SFP GbE	2	—	—
WAN インタフェース：SFP GbE	2	—	—
LAN インタフェース：LC コネクタ（850 nm、GbE）、バイパス機能内蔵	2	—	—
WAN インタフェース：LC コネクタ（850 nm、GbE）、バイパス機能内蔵	2	—	—
LAN インタフェース：SFP+ 10 GbE / SFP GbE	—	2	2（10 GbE のみ）
WAN インタフェース：SFP+ 10 GbE / SFP GbE	—	2	2（10 GbE のみ）
LAN インタフェース：LC コネクタ（850 nm、10 GbE）、バイパス機能内蔵	—	2	—
WAN インタフェース：LC コネクタ（850 nm、10 GbE）、バイパス機能内蔵	—	2	—
LAN インタフェース：QSFP+ 40 GbE	—	—	2
WAN インタフェース：QSFP+ 40 GbE	—	—	2
パッシブオプティカルバイパス	—	—	8 ポート（2 接続） 10 / 40 GbE LR / ER / ZR
トラステッドプラットフォームモジュール（TPM）	○	○	○
ストレージ	1 × 480 GB SSD	1 × 480 GB SSD	1 × 960 GB SSD
形状	1 U アプライアンス	2 U アプライアンス	2 U アプライアンス
電源	AC ホットスワップ対応冗長電源	AC ホットスワップ対応冗長電源	AC ホットスワップ対応冗長電源
システム性能			
最大インスペクションスループット（Gbps）	8	30	76
インスペクションスループット（エンタープライズトラフィック混合、Gbps）	8	30	76
インスペクションパケットスループット（M pps）	8.8	28	60
最大減災（Gbps / Mpps）	8 / 8.8	30 / 28	76 / 60
SYN フラッド攻撃減災（SYN In + Cookie Out）M pps	5.7	16	21
同時 TCP 接続数（単位：百万）	4.2	16.7	33
同時処理ソース数（単位：百万）	1	4	8
セッションセットアップ / ティアダウン（kcps）	375	700	920
レイテンシ（µs）最大 / 標準	50 µs 未満	50 µs 未満	50 µs 未満
DDoS 攻撃に対する応答時間（秒）	最初のパケット：2 秒未満	最初のパケット：2 秒未満	最初のパケット：2 秒未満
高度な DNS / NTP 減災	DNS / NTP / DTLS	DNS / NTP / DTLS	DNS / NTP / DTLS
1 秒あたりの DNS / NTP クエリ（M）	2 / 1	8 / 4	8 / 4
フラッド攻撃状態の DNS / NTP 応答検証（M / 秒）	2 / 1	8 / 4	8 / 4
オープンハイブリッドクラウド減災サポート	○	○	○
Central Manager による一元管理	—	—	—
FortiOS のセキュリティ ファブリックダッシュボード統合	○	○	○
動作環境			
AC 電源（入力電圧）	100 ～ 240 V AC、50 ～ 60 Hz	100 ～ 240 V AC、50 ～ 60 Hz	100 ～ 240 V AC、50 ～ 60 Hz
消費電力（平均 / 最大）	117 W / 152 W	333 W / 433 W	333 W / 433 W
最大電流（AC）	100 V / 1.5 A、240 V / 0.7 A	100 V / 4.4 A、240 V / 1.9 A	100 V / 4.4 A、240 V / 1.9 A
放熱（BTU/h）/（kjoules/h）	519 / 574	1,477 / 1,558	1,477 / 1,558
動作温度	0 ～ 40 ºC	0 ～ 40 ºC	0 ～ 40 ºC
保管温度	-20 ～ 70 ºC	-20 ～ 70 ºC	-20 ～ 70 ºC
エアフロー	前面 ～ 背面	前面 ～ 背面	前面 ～ 背面
湿度	5 ～ 90%（結露しないこと）	5 ～ 90%（結露しないこと）	5 ～ 90%（結露しないこと）
準拠規格・認定			
準拠規格	FCC Class A Part 15、UL / CB / cUL、RCM、VCCI、CE		
サイズ			
高さ x 幅 x 奥行	44 × 438 × 550 mm	88.2 × 438 × 580 mm	88.2 × 438 × 580 mm
重量	9.6 kg	9.0 kg	9.0 kg

技術仕様


	FortiDDoS 1500E / 1500E-DC	FortiDDoS 2000E / 2000E-DC
ハードウェア仕様		
LAN インタフェース：Copper GbE、バイパス機能内蔵	—	—
WAN インタフェース：Copper GbE、バイパス機能内蔵	—	—
LAN インタフェース：SFP GbE	—	—
WAN インタフェース：SFP GbE	—	—
LAN インタフェース：SFP+ 10 GbE / SFP GbE	8	8
WAN インタフェース：SFP+ 10 GbE / SFP GbE	8	8
LAN インタフェース：LC コネクタ（850 nm、10 GbE）、バイパス機能内蔵	—	—
WAN インタフェース：LC コネクタ（850 nm、10 GbE）、バイパス機能内蔵	—	—
LAN インタフェース：QSFP+ 40 GbE / QSFP28 100 GbE	2	2
WAN インタフェース：QSFP+ 40 GbE / QSFP28 100 GbE	2	2
パッシブオプティカルバイパス	8 ポート（2 接続） 1 / 10 / 40 / 100 GbE 1,310nm	8 ポート（2 接続） 1 / 10 / 40 / 100 GbE 1,310nm
トラステッドプラットフォームモジュール（TPM）	—	—
ストレージ	1 × 960 GB SSD	1 × 960 GB SSD
形状	2 U アプライアンス	2 U アプライアンス
電源	AC / DC ホットスワップ対応冗長電源	AC / DC ホットスワップ対応冗長電源
システム性能		
最大インスペクションスループット（Gbps）	45	90
インスペクションスループット（エンタープライズトラフィック混合、Gbps）	35	70
インスペクションパケットスループット（M pps）	38	77
最大減災（Gbps / Mpps）	280 / 420	280 / 420
SYN フラッド攻撃減災（SYN In + Cookie Out）M pps	27	55
同時 TCP 接続数（単位：百万）	12	25
同時処理ソース数（単位：百万）	12	25
セッションセットアップ / ティアダウン（kcps）	1,500 以上	3,000 以上
レイテンシ（µs）最大 / 標準	50 µs 未満 / 10 µs 未満	50 µs 未満 / 10 µs 未満
DDoS 攻撃に対する応答時間	最初のパケット：2 秒未満	最初のパケット：2 秒未満
高度な DNS / NTP 減災	DNS / NTP	DNS / NTP
1 秒あたりの DNS / NTP クエリ（M）	4 / 3	7 / 6
フラッド攻撃状態の DNS / NTP 応答検証（M / 秒）	4 / 3	7 / 6
オープンハイブリッドクラウド減災サポート	○	○
Central Manager による一元管理	○	○
FortiOS のセキュリティ ファブリックダッシュボード統合	○	○
動作環境		
電源（入力電圧）	100 ～ 240 V AC、50 ～ 60 Hz、40 ～ 72 V DC	100 ～ 240 V AC、50 ～ 60 Hz、40 ～ 72 V DC
消費電力（平均 / 最大）	314 W / 580 W	314 W / 580 W
最大電流	110 V AC / 5.3 A、220 V AC / 2.6 A、48 V DC / 12 A	110 V AC / 5.3 A、220 V AC / 2.6 A、48 V DC / 12 A
放熱（BTU/h）/（kjoules/h）	2,151 / 2,269	2,151 / 2,269
動作温度	0 ～ 40 ºC	0 ～ 40 ºC
保管温度	-25 ～ 70 ºC	-25 ～ 70 ºC
エアフロー	前面 ～ 背面	前面 ～ 背面
湿度	20 ～ 90%（結露しないこと）	20 ～ 90%（結露しないこと）
準拠規格・認定		
準拠規格	FCC Class A Part 15、UL / CB / cUL、RCM、VCCI、CE	
サイズ		
高さ x 幅 x 奥行	88 × 438 × 560 mm	88 × 438 × 560 mm
重量	20.0 kg	20.0 kg

技術仕様

	FortiDDoS-VM04	FortiDDoS-VM08	FortiDDoS-VM16
ハードウェア仕様			
Hypervisor Support	ハードウェアを活用した仮想化（VT）が BIOS で有効な VMware ESX / ESXi 6.x / 7.x		
スループット [1, 3]	3 Gbps	5 Gbps	10 Gbps
減災 [2, 3]	3 Gbps / 4 Mpps	5 Gbps / 6 Mpps	10 Gbps / 10 Mpps
サービス保護プロファイル	4	8	16
vCPU サポート	4	8	16
ネットワークインタフェースのサポートについて	8（4 つのブリッジポートペア）、インタフェース速度はハードウェアに依存		
メモリ	16 GB	16 GB	32 GB
ストレージ	200 GB 以上		

[1] 1.7 KB の HTTP レスポンス
[2] 64 バイトのパケットを 100% インスペクションした場合
[3] 実際の性能は使用するハードウェアによって異なります。記載されている性能の結果は、Inte Xeon W-3245 CPU @ 3.20 GHz を搭載し、VMware ESXI 7.0.0 と SR-IOV が動作するベアメタルアプライアンスを使用した場合のものです。

注：FortiDDoS VM は、AWS、Azure、Google Cloud などのクラウドサービス環境への導入に適していません。FortiDDoS VM（およびアプライアンス）には設計によりデータポートに IP アドレスがないため、クラウド環境でアドレスを指定できません。トラフィックの宛先を指定する方法がありません。VM（およびアプライアンス）を物理リンクに接続する必要があります。

オーダー情報

Product	Description
FortiDDoS 200F	DDoS Protection Appliance - 8 port-pairs DDoS Defence Ports, including 4 pairs x GE RJ45 with bypass protection, 2 pairs x GE LC SR MM with optical bypass protection, 2 pairs GE SFP (no bypass protection), 2x GE RJ45 Management Ports, dual redundant AC power supplies. Includes 480 GB SSD storage. >8 Gbps / 8.8 Mpps inspected Mitigation. Supports Advanced DNS and NTP DDoS attack mitigation.
FortiDDoS 1500F	DDoS Protection Appliance - 4 port-pairs DDoS Defence Ports, including 2 pairs x 10 GE SFP+ (or GE SFP) (no bypass protection) and 2 pairs x 10 GE LC SR MM ports with optical bypass protection, 2x GE RJ45 Management Ports, Dual redundant AC power supplies. Includes 480GB SSD storage. >30 Gbps / 28 Mpps inspected Mitigation. Supports Advanced DNS and NTP DDoS attack Mitigation.
FortiDDoS 1500E	DDoS Protection Appliance — 10 port-pairs DDoS Defence Ports, including 8 pairs x 10 GE SFP+ or GE SFP and 2 pairs x 40 GE QSFP+ or 100GE QSFP28 ports plus 2-link optical bypass module (1310nm), 2x GE RJ45 Management Ports, Dual AC Power Supply. Includes 960 GB SSD storage. >35 Gbps / 38 Mpps inspected Mitigation (280 Gbps Max Mitigation). Supports Advanced DNS and NTP DDoS attack mitigation.
FortiDDoS 1500E-DC	DDoS Protection Appliance — 10 port-pairs DDoS Defence Ports, including 8 pairs x 10 GE SFP+ or GE SFP and 2 pairs x 40 GE QSFP+ or 100GE QSFP28 ports plus 2-link optical bypass module (1310nm), 2x GE RJ45 Management Ports, Dual DC Power Supply. Includes 960 GB SSD storage. >35 Gbps / 38 Mpps inspected Mitigation (280 Gbps Max Mitigation). Supports Advanced DNS and NTP DDoS attack mitigation.
FortiDDoS 2000F	DDoS Protection Appliance - 2 pairs x 10GE SFP+, 2 pairs 40GE QSFP+ 4 pairs (2 links) LR (1310 nm) optical bypass , 2x GE RJ45 Management Ports, Dual AC Power Supply. Includes 960GB SSD storage. Supports advanced DNS, NTP, DTLS mitigation.
FortiDDoS 2000E	DDoS Protection Appliance — 10 port-pairs DDoS Defence Ports, including 8 pairs x 10 GE SFP+ or GE SFP and 2 pairs x 40 GE QSFP+ or 100 GE QSFP28 ports plus 2-link optical bypass module (1310nm), 2x GE RJ45 Management Ports, Dual AC Power Supply. Includes 960 GB SSD storage. >70 Gbps / 77 Mpps inspected Mitigation (280 Gbps Max Mitigation). Supports Advanced DNS and NTP DDoS attack mitigation.
FortiDDoS 2000E-DC	DDoS Protection Appliance — 10 port-pairs DDoS Defence Ports, including 8 pairs x 10 GE SFP+ or GE SFP and 2 pairs x 40 GE QSFP+ or 100GE QSFP28 ports plus 2-link optical bypass module (1310nm), 2x GE RJ45 Management Ports, Dual DC Power Supply. Includes 960 GB SSD storage. >70 Gbps / 77 Mpps inspected Mitigation (280 Gbps Max Mitigation). Supports Advanced DNS and NTP DDoS attack mitigation.
Virtual Machine	**Description**
FortiDDoS-VM04	DDoS Protection System - virtual appliance for all supported platforms. Supports up to 4 x vCPU cores, 8 x NIC Ports, 2 x MGMT Ports.
FortiDDoS-VM08	DDoS Protection System - virtual appliance for all supported platforms. Supports up to 8 x vCPU cores, 8 x NIC Ports, 2 x MGMT Ports.
FortiDDoS-VM16	DDoS Protection System - virtual appliance for all supported platforms. Supports up to 16 x vCPU cores, 8 x NIC Ports, 2 x MGMT Ports.

注：FortiDDoS VM は、AWS、Azure、Google Cloud などのクラウドサービス環境への導入に適していません。FortiDDoS VM（およびアプライアンス）には設計によりデータポートに IP アドレスがないため、クラウド環境でアドレスを指定できません。トラフィックの宛先を指定する方法がありません。VM（およびアプライアンス）を物理リンクに接続する必要があります。

オーダー情報

FortiDDoS 対応トランシーバ						
型番	説明	ファイバーモード / 波長	FDD-200F	FDD-1500F	FDD-2000F Ports/Bypass	FDD-1500E / FDD-2000E Ports/Bypass
FS-TRAN-FX	100Mb multimode SFP transceivers, -40/85c operation, 2km range for systems with SFP Slots and capable of 10/100Mb mode selection.	MM 850nm	N	N	N / N	N / N
FN-TRAN-DSL	VDSL2/ADSL2 SFP transceiver module, for all systems with SFP and SFP+ slots.	Copper	N	N	N/N	N / N
FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.	SM 1310nm	Y	Y	N / N	Y / Y
FR-TRAN-ZX	1 G SFP transceivers, -40–85˚C operation, 90 km range for all systems with SFP slots.	SM 1550nm	Y	Y	N / N	Y/ Y
FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.	MM 850nm	Y	Y	N / N	Y / N
FR-TRAN-SX	1 GE SFP SX transceiver module, -40–85˚C, over MMF, for all systems with SFP and SFP/SFP+ slots.	MM 850nm	Y	Y	N / N	Y / N
FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+ slots.	Copper	Y	Y	N / N	Y / N
FS-TRAN-GC	1GE SFP RJ45 transceiver module for FortiSwitch D Series with SFP and SFP/SFP+ slots	Copper	Y	Y	N / N	Y / N
FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.	SM 1310nm	N	Y	Y / Y	Y / Y
SP-CABLE-FS-SFP+1	10 GE SFP+ passive direct attach cable, 1 m for systems with SFP+ and SFP/SFP+ slots.	End-to-End	N	Y	Y / N	Y / N
SP-CABLE-FS-SFP+3	10 GE SFP+ passive direct attach cable, 3 m for systems with SFP+ and SFP/SFP+ slots.	End-to-End	N	Y	Y / N	Y / N
SP-CABLE-FS-SFP+5	10 GE SFP+ passive direct attach cable, 5 m for systems with SFP+ and SFP/SFP+ slots.	End-to-End	N	Y	Y / N	Y / N
SP-CABLE-FS-SFP+7	10 GE SFP+ passive direct attach cable, 7 m for systems with SFP+ and SFP/SFP+ slots.	End-to-End	N	Y	Y / N	Y / N
FN-TRAN-SFP+GC	10GE copper SFP+ RJ45 Fortinet Transceiver (30m range) for systems with SFP+ slots.	Copper	N	Y	Y / N	Y / N
SP-CABLE-ADASFP+	10 GE SFP+ active direct attach cable, 10 m/32.8 ft for all systems with SFP+ and SFP/SFP+ slots.	End-to-End	N	Y	Y / N	Y / N
FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.	MM 850nm	N	Y	Y / N	Y / N
FN-TRAN-SFP+ER	10Gbase-ER SFP+ transceivers for FortiSwitch and FortiGate, 1550nm. Single Mode. 40 km range for systems with SFP+ slots.	SM 1550nm	N	Y	Y / Y	Y / Y
FG-TRAN-SFP28-LR	25GE SFP28 transceiver module, long range for all systems with SFP28 slots.	SM 1310nm	N	N	N / N	N / N
FN-TRAN-SFP28-LR	25GE SFP28 transceiver module, long range for all systems with SFP28 slots.	SM 1310nm	N	N	N / N	N / N
FN-TRAN-SFP28-SR	25GE/10GE Dual Rate SFP28 transceiver module, short range for all systems with SFP28/SFP+ slots.	MM 850nm	N	N	N / N	N / N

Note 1：E シリーズの pluggable 光インタフェースで使用できます。E シリーズの光バイパスモジュールとの互換性はありません。

オーダー情報

FortiDDoS 対応トランシーバ						
型番	説明	ファイバーモード / 波長	FDD-200F	FDD-1500F	FDD-2000F Ports/Bypass	FDD-1500E / FDD-2000E Ports/Bypass
FG-TRAN-QSFP-4XSFP	40G/100G QSFP+/QSFP28 to SFP+/SFP28 Parallel Breakout MPO to 4xLC connectors, 1m reach, transceivers not included.	MM 850nm	N	N	N / N	N / N
FG-TRAN-QSFP-4SFP-5	40G/100G QSFP+/QSFP28 to SFP+/SFP28 Parallel Breakout MPO to 4xLC connectors, 5m reach, transceivers not included.	MM 850nm	N	N	N / N	N / N
FN-TRAN-QSFP+LR	40 GE QSFP+ transceivers, long range for all systems with QSFP+ slots.	SM 1310nm	N	N	Y / Y	Y / Y
FN-TRAN-QSFP+SR	40 GE QSFP+ transceivers, short range for all systems with QSFP+ slots.	MM 850nm	N	N	Y / N	Y / N
FG-TRAN-QSFP+SR-BIDI	40 GE QSFP+ transceiver, short range BiDi for systems with QSFP+ slots.	MM 850nm	N	N	Y / N	Y / N
SP-CABLE-FS-QSFP+1	40 GE QSFP+ passive direct attach cable, 1 m for systems with QSFP+ slots.	End-to-End	N	N	Y / N	Y / N
SP-CABLE-FS-QSFP+3	40 GE QSFP+ passive direct attach cable, 3 m for systems with QSFP+ slots.	End-to-End	N	N	Y / N	Y / N
SP-CABLE-FS-QSFP+5	40 GE QSFP+ passive direct attach cable, 5 m for systems with QSFP+ slots.	End-to-End	N	N	Y / N	Y / N
FG-TRAN-CFP2-LR4	100GE CFP2 transceivers, long range, over single mode fiber, for all systems with CFP2 Slots.	CP2-to-10xLC	N	N	N / N	N / N
FG-TRAN-CFP2-SR10	100GE CFP2 transceivers, 10 channel parallel fiber, short range for all systems with CFP2 Slots.	CP2-to-10xLC	N	N	N / N	N / N
FG-CABLE-SR10-SFP+	100G CFP2 Parallel Breakout MPO to 10xLC conectors, 1m reach, transceivers not included.	CP2-to-10xLC	N	N	N / N	N / N
FG-CABLE-SR10-SFP+5	100G CFP2 Parallel Breakout MPO to 10xLC conectors, 5m reach, transceivers not included.	CP2-to-10xLC	N	N	N / N	N / N
FN-TRAN-QSFP28-LR	100 GE QSFP28 transceivers, long range for all systems with QSFP28 slots.	SM 1310nm	N	N	N / N	Y / Y
FN-TRAN-QSFP28-SR	100 GE QSFP28 transceivers, 4 channel parallel fiber, short range for all systems with QSFP28 slots.	MM 850nm	N	N	N / N	Y / N
FN-TRAN-QSFP28-ER	100 GE QSFP28 transceivers, extended long range 20KM for all systems with QSFP28 Slots.	SM 1310nm	N	N	N / N	Y / Y
FN-TRAN-QSFP28-CWDM4	100 GE QSFP28 transceivers, LC connectors, 2KM for all systems with QSFP28 Slots.	SM CWDM	N	N	N / N	Y / Y

フォーティネットジャパン合同会社

〒106-0032
東京都港区六本木 7-7-7　Tri-Seven Roppongi 9 階
www.fortinet.com/jp/contact

お問い合わせ