

FortiADC

FortiADC 100F、200F、300D、400D、1000F、2000F、4000F、VM

FortiADC アプリケーションデリバリーコントローラ (ADC) は、エンタープライズアプリケーションデリバリーの可用性、ユーザーエクスペリエンス、パフォーマンス、拡張性を最適化します。

FortiADC ファミリーは、エンタープライズ環境のもっとも要件の厳しいアプリケーションの高速かつ安全でインテリジェントなアクセラレーションと分散を可能にする物理アプライアンスです。



アクセラレーションとパフォーマンス

マルチコアプロセッサテクノロジーとハードウェアベースのSSLオフロードの組み合わせによって、アプリケーションパフォーマンスのアクセラレーションを実現します。



アプリケーションの高可用性

自動フェイルオーバー、グローバルサーバーロードバランシングおよびリンクロードバランシング機能を使用してWAN接続を最適化することで、24時間365日のアプリケーションの可用性を実現します。



保護機能の強化

Webアプリケーションファイアウォール機能を提供し、脆弱性に対する攻撃からアプリケーションを保護します。



ハイライト

- 99.999%のアプリケーションアップタイムを実現する包括的なサーバーロードバランシング
- アプリケーションアクセラレーション、スケールアウトやTCO削減を実現するサーバーオフロード
- 最適化されたアプリケーションデリバリーコントロール (ADC) と高可用性を実現する高度なトラフィック管理
- ハードウェアベースのSSLオフロード、プロキシフォワーディングおよび可視化
- 認証処理のオフロード
- グローバルサーバーロードバランシング機能を内蔵
- リンクロードバランシング機能を内蔵
- 自動更新対応のWebアプリケーションファイアウォール
- スクリプトによる独自のロードバランシングやコンテンツの書き換え

ハイライト

ハードウェアベースの SSL オフロード、 SSL インспекションおよび可視化

FortiADC は、4096 ビットキーのサポートによってサーバーに集中する SSL 処理をオフロードするため、TCP 接続管理、データ圧縮および HTTP リクエスト処理がサーバーからオフロードされます。これにより、応答時間が短縮し、バックエンドサーバーの負荷が軽減されて、多くのユーザーにサービスを提供できるようになります。

SSL プロキシフォワーディングでは、FortiADC の高性能の復号 / 暗号化機能によって FortiGate ファイアウォールなどの他のデバイスがトラフィックに潜む脅威を簡単に検査できます。ファイアウォールのフロントエンドとバックエンドに FortiADC のペアを組み込むことで、すべての暗号化処理がオフロードされるため、SSL 処理によって増加する負荷からファイアウォールを解放できます。FortiADC では、ユーザーのサービスを中断することなく、証明書によるシームレスな再暗号化が保証されます。

FortiADC トランスペアレントな HTTP/S および TCP/S ミラーリング機能により、セキュアなトラフィックを復号して検査やレポートを実行できます。FortiADC は、アプリケーションデリバリーコントローラ機能を継続的に実行しながら、無害であると判定されたトラフィックの複製を FortiGate や他のサードパーティ製ソリューションに送信して分析し、暗号化されたトラフィックに隠されている可能性のある脅威を詳細に確認することが可能です。

また、ジェムアルト社の SafeNet エンタープライズ向けハードウェアセキュリティモジュール (HSM) との統合により、HSM によって管理された先進のセキュリティ証明書を活用するセキュアなアプリケーショントラフィックの暗号化と復号が可能になります。これにより、ジェムアルト社の SafeNet HSM を利用する企業組織は、一元管理された強固な証明書および暗号キーを活用するハイパフォーマンスの ADC ソリューションを導入配備できます。

グローバルサーバーロードバランシングによる ディザスタリカバリ

FortiADC のグローバルサーバーロードバランシング (GSLB) 機能により、複数のデータセンターにアプリケーションをスケールアウトすることでネットワークの信頼性と可用性が向上し、アプリケーションの応答時間の改善やディザスタリカバリへの対応が可能になります。管理者は、Web サイトの可用性、データセンターのパフォーマンス、およびネットワークのレイテンシに基づいて、トラフィックを振り分けるルールを設定できます。

フォーティネット セキュリティ ファブリックとの 密接な統合

脅威の状況が進化し、新たに多くの脅威が出現したことを受け、Web ベースのアプリケーションを保護する上で多目的なアプローチが求められています。APT (持続的標的型攻撃) は、攻撃経路が 1 つしかない従来型の攻撃タイプとは異なり、さまざまな攻撃形態をとります。また、単一のデバイスによる保護機能を回避することができます。FortiADC のアンチウイルスと FortiSandbox との統合によって、基本的なセキュリティ対策が強化され、添付ファイルに含まれる既知および未知の脅威を検知します。

リンクロードバランシング

リンクロードバランシング機能 (LLB) では、FortiADC を 2 つ以上の WAN リンクに接続することで、ネットワークアクセスが停止するリスクの軽減や、帯域幅の追加によるトラフィックの輻輳状態の緩和が可能です。FortiADC は、インバウンドおよびアウトバウンドのリンクロードバランシングをサポートし、デバイスが送受信するトラフィックを管理します。ポリシールーティングを使用することで NAT やルーティングの複雑な要件をサポートし、ほぼすべてのネットワーク LLB アーキテクチャに対応できます。トンネルルーティング機能によって、コストの高い WAN リンクをリースすることなく高速かつ信頼性の高いサイト間の接続を可能にします。時間が重視されるアプリケーションや単一セッションで大量の帯域幅を必要とするビデオ会議などにおいては、複数リンクのアグリゲーションによってリモートデータセンターへの仮想トンネルを作成することで、可用性を確保します。

PageSpeed、キャッシュ、および圧縮による パフォーマンスの最適化

FortiADC には、アプリケーションデリバリーの高速化に役立つ複数のサービスが提供されています。Web サイトのパフォーマンス向上ツールである PageSpeed スイートによって、ユーザーへの HTTP、CSS、JavaScript、および画像アプリケーションのデリバリーを自動的に最適化できます。FortiADC のキャッシングは、アクセス頻度の高いアプリケーションコンテンツ (画像、ビデオ、HTML ファイル、およびその他のファイルタイプ) を動的にキャッシュすることでサーバーリソースの有効活用を促進し、アプリケーションの全体的なパフォーマンスを向上させます。HTTP コンテンツ圧縮では、GZIP と DEFLATE を使用して、最新 Web ベースアプリケーションで使用される多くのコンテンツタイプをインテリジェントに圧縮することで帯域幅要件を抑制し、アプリケーションユーザーエクスペリエンスを向上させます。

Web アプリケーションファイアウォール、 Web フィルタリング、IP レピュテーションによる セキュリティの強化

Web アプリケーションがハッカーの標的になりやすいことは周知のとおりです。FortiADC は、複数レベルの保護によってこのような攻撃からアプリケーションを保護します。すべての FortiADC に組み込まれたステートフルファイアウォール機能と Web アプリケーションファイアウォールによって、レイヤー 7 攻撃シグネチャの FortiGuard WAF セキュリティサービス (サブスクリプション契約が必要です) を使用して既知の脅威を検出し、HTTP RFC コンプライアンスの制約を使用してリクエストが改ざんされていないことを確認します。FortiGuard Web フィルタリングと FortiADC の SSL プロキシフォワーディング機能の連携によって、セキュアトラフィック検査の例外管理のプロセスが簡素化されます。Web フィルタリングを利用すると、管理者がカテゴリタイプ別に Web サイトを選択し、サイト単位ではなくグループ単位で SSL トラフィックを有効化または無効化するように選択できるため、URL を手動で 1 つずつ構成する必要がなくなります。また、FortiADC は FortiGuard IP レピュテーションサービス (サブスクリプション契約が必要です) をサポートしているため、DoS / DDoS 攻撃、フィッシング詐欺、スパム、悪意あるソフトウェアやボットネットと関連性がある送信元からの保護にも対応します。

ハイライト

スクリプトによる内蔵機能の拡張

FortiADCのLuaベースのスクリプト言語を利用すると、イベント主導の独自のルールを定義済みのコマンド、変数、演算子を使用して柔軟に作成できます。簡単に作成できるスクリプトを利用し

て独自のビジネスルールを追加することで、FortiADCの機能がほぼ無限に拡大し、組織のビジネスニーズに合わせたサーバーロードバランシングやコンテンツ書き換えが可能になります。

主な機能と特長



先進のレイヤー7 ロードバランシング	直感的なポリシーベースのL7ルーティングでコンテンツを動的に書き換え、複雑なアプリケーションやサーバー構成をサポート
SSLオフロード、 プロキシフォワーディング および可視化	ハードウェアおよびソフトウェアベースのSSLオフロードによって、サーバーインフラストラクチャに対するパフォーマンスの影響を軽減。FortiGate向けにSSL復号 / 再暗号化機能を提供することで、トラフィックに潜む脅威を容易に検査可能
アプリケーション最適化	圧縮、キャッシュ、HTTP 2.0、HTTP Page Speed-UPによってWebアプリケーションデリバリーを高速化することで、ネットワークとWebサーバーの有効利用を推進
グローバルサーバーロード バランシング	グローバルサーバーロードバランシング (GSLB) 機能によって地理的に離れた複数の場所にトラフィックを分散し、ディザスタリカバリやユーザーへの応答時間の短縮を実現
リンクロードバランシング	リンクロードバランシング (LLB) によってトラフィックが複数のISPに分散されるため、耐障害性が向上し、コストのかかる帯域幅の追加を回避可能
Webアプリケーション ファイアウォールと IPレピュテーションサービス	Webアプリケーション攻撃シグネチャ、HTTP RFCコンプライアンス、およびボットネット / 悪意あるソースの識別によってアプリケーションを保護する、高度セキュリティ機能

主な機能

アプリケーションの高可用性

使いやすく構成も容易なレイヤー 4 / 7 ポリシーと

グループ管理機能

- セッション維持、ロードバランシングおよびプールメンバーによる仮想サービスの定義
- 静的、デフォルトおよびバックアップのポリシーとグループ
- レイヤー 4 / 7 アプリケーションのルーティングポリシー
- レイヤー 4 / 7 サーバーのセッション維持
- ラウンドロビン、重み付けラウンドロビン、最小コネクション数、最小レスポンスに基づくアプリケーションロードバランシング
- きめ細かいサーバー管理（レートリミットのウォームアップやセッションのランプダウンを伴うメンテナンスモードなど）
- カスタムスクリプトによる SLB とコンテンツの書き換え
- SharePoint、Exchange、Windows Remote Desktop をはじめとする Microsoft アプリケーション用のテンプレート

レイヤー 4 アプリケーションのロードバランシング

- TCP / UDP プロトコルをサポート
- ラウンドロビン、重み付けラウンドロビン、最小コネクション数、最小レスポンス
- サーバーのパラメータ（CPU、メモリおよびディスク）に基づく動的な L4 ロードバランシング
- IP セッション維持、ハッシュ IP / ポート、ハッシュヘッダー、クッキーセッション維持、ハッシュクッキー、送信先 IP ハッシュ、URI ハッシュ、ホストハッシュ、ホストドメインハッシュ

レイヤー 7 アプリケーションのロードバランシング

- HTTP、HTTPS、HTTPS GW、FTP、SIP、RDP、RADIUS、MySQL、RTMP、RTSP をサポート
- L7 コンテンツの振り分け
 - HTTP ホスト、HTTP リクエスト URL、HTTP リファラー
 - 送信元 IP アドレス
- URL リダイレクト、HTTP リクエスト / レスポンスの書き換え（HTTP ボディを含む）
- レイヤー 7 DNS ロードバランシング、セキュリティおよびキャッシング
- 403 Forbidden の書き換え
- コンテンツの書き換え

主な機能

リンクロードバランシング

- インバウンドとアウトバウンドのリンクロードバランシング (LLB)
- ポリシールートと SNAT のサポート
- 複数のヘルスチェック方式をサポート
- インターバル、再試行間隔およびタイムアウトを定義可能
- トンネルのルーティング

グローバルサーバーロードバランシング (GSLB)

- グローバルなデータセンターで Web アプリケーションの DNS ベースのフェイルオーバーが可能
- SSL-VPN を導入した複数サイト間で、ローカルおよびグローバルのロードバランシングを実現
- DNSSEC
- DNS アクセス制御リスト

導入モード

- ワンアームモード
(X-Forwarded-For 設定でのプロキシをサポート)
- ルーターモード
- トランスペアレントモード (スイッチ)
- 高可用性 (アクティブ/アクティブ、アクティブ/パッシブ構成のフェイルオーバー)

アプリケーションアクセラレーション

SSL オフロードとアクセラレーション

- HTTPS 処理のオフロードと機密データの保護を同時に実現
- 証明書管理の全機能
- SSL プロキシフォワーディングによるセキュアトラフィック検査
- トラフィックの分析とレポートを可能にする HTTP / S ミラーリング

HTTP および TCP の最適化

- TCP 処理のオフロードによる 100 倍のアクセラレーション
- HTTP / HTTPS の接続プールとマルチプレキシング
- HTTP Page Speed-UP による Web サーバーの最適化と高速化
- TCP バッファリング
- HTTP コンテンツの圧縮と復元
- HTTP キャッシング (静的および動的オブジェクト)
- QoS による帯域幅の割り当て
- HTTP およびレイヤー 4 のレートリミット

認証処理のオフロード

- ローカル
- LDAP
- RADIUS
- Kerberos
- SAML 2.0 (SP および IdP)

ネットワーク機能

- 柔軟性と拡張性を実現する NAT
- VLAN およびポートランキングをサポート
- Cisco ACI および OpenStack SDN のサポート
- NVGRE および VXLAN のサポート
- BGP および OSPF のサポート
- BGP と RHI (Route Health Injection) の使用
- IPv6 のサポート
- IPv6 ルーティング
- IPv6 ファイアウォールルール

セキュリティ

- FortiGuard アンチウイルスと FortiSandbox の統合
- 地域別 IP セキュリティとログ
(サブスクリプション契約が必要です)
- ステートフルファイアウォール
- Web フィルタリング (サブスクリプション契約が必要です)
- IP レピュテーションサービス
(サブスクリプション契約が必要です)
- IPv4 / IPv6 ファイアウォールルール
- きめ細かなポリシーベースの接続制限
- SYN クッキー保護
- 接続制限

Web アプリケーションファイアウォール

- Web 攻撃シグネチャ
- XML / JSON / SOAP の評価
- SQLi / XSS インジェクションの検知
- ボットの検知
- URL / ファイルの保護

管理機能

- クラスタの一元管理
- CLI インタフェースによる構成とモニタリング
- SSH によるセキュアなリモートネットワーク管理
- Web UI によるセキュアなアクセス
- RESTful API
- SNMP とプライベート MIB でのしきい値ベーストラップの使用
- リアルタイムのデータ分析
- Syslog のサポート
- ロールベースのユーザー管理
- 診断ユーティリティの実装
- リアルタイム モニタリング グラフ
- 内蔵のレポート機能
- 初回ログイン用ウィザード
- 仮想ドメイン (VDOM)

技術仕様

	FortiADC 100F	FortiADC 200F	FortiADC 300D
ハードウェア仕様			
L4 / L7 スループット	1.5 Gbps / 1.3 Gbps	3 Gbps / 2.2 Gbps	6 Gbps / 4 Gbps
L4 CPS	50,000	100,000	180,000
L4 HTTP RPS	150,000	300,000	725,000
最大 L4 同時接続数	3 M	5 M	9 M
L7 CPS (1:1) *	15,000	25,000	55,000
SSL CPS / TPS (1:1) 2 K キー **	400	1,000	1,500
SSL バルク暗号化スループット	400 Mbps	1 Gbps	1.4 Gbps
圧縮スループット	1 Gbps	1.5 Gbps	2 Gbps
SSL アクセラレーションテクノロジー	ソフトウェア	ソフトウェア	ソフトウェア
メモリ	4 GB	4 GB	8 GB
仮想ドメイン (VDOM)	0	3	10
ネットワークインタフェース	6 x GbE RJ45	4 x GbE RJ45、4 x GbE SFP	4 x GbE RJ45、4 x GbE SFP
10 / 100 / 1000 管理インタフェース	—	2	—
内蔵ストレージ	64 GB SSD	64 GB SSD	128 GB SSD
管理機能	HTTPS、SSH CLI、 Direct Console DB9 CLI、SNMP	HTTPS、SSH CLI、 Direct Console DB9 CLI、SNMP	HTTPS、SSH CLI、 Direct Console DB9 CLI、SNMP
電源	単一	単一	単一
動作環境			
形状	1 U アプライアンス	1 U アプライアンス	1 U アプライアンス
AC 電源	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)	40 W / 60 W	70.98 W / 109.9 W	96 W / 115 W
最大電流	100 V / 1.5 A、240 V / 0.6 A	100 V / 2 A、240 V / 0.84 A	100 V / 4 A、240 V / 2 A
放熱	132 ~ 163 BTU/h	374.9 BTU/h	392.4 BTU/h
動作温度	0 ~ 40 °C	0 ~ 40 °C	0 ~ 40 °C
保管温度	-20 ~ 75 °C	-35 ~ 70 °C	-25 ~ 70 °C
湿度	相対湿度 10 ~ 85% (非動作時、結露しないこと)	20 ~ 90% (結露しないこと)	5 ~ 95% (結露しないこと)
準拠規格・認定			
準拠規格	FCC Part 15 Class A、C-Tick、VCCI Class A、CE、UL/c		
安全性に関する注意事項	CSA、C/US、CE、UL		
サイズ			
高さ x 幅 x 奥行	44 x 440 x 268 mm	44 x 432 x 301.4 mm	44 x 438 x 416 mm
重量	4.5 kg	4.98 kg	9.07 kg

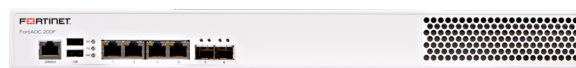
数値はすべて「最大」の性能値であり、システム構成に応じて異なります。

* レイヤー 7 CPS：新規の HTTP 接続数を計測 (TCP 接続あたり 1 HTTP リクエスト)

** SSL 接続あたり 1 HTTP リクエストの状態テスト、SSL 暗号は AES256-SHA、2000 キー



FortiADC 100F



FortiADC 200F



FortiADC 300D

技術仕様

	FortiADC 400D	FortiADC 1000F	FortiADC 2000F	FortiADC 4000F
ハードウェア仕様				
L4 / L7 スループット	12 Gbps / 8 Gbps	20 Gbps / 15 Gbps	40 Gbps / 25 Gbps	60 Gbps / 35 Gbps
L4 CPS	240,000	425,000	750,000	800,000
L4 HTTP RPS	1 M	1.5 M	2.6 M	3.8 M
最大 L4 同時接続数	9 M	18 M	36 M	72 M
L7 CPS (1:1) *	80,000	150,000	250,000	300,000
SSL CPS / TPS (1:1) 2 K キー **	7,000	20,000	37,000	54,000
SSL バルク暗号化スループット	4 Gbps	9.5 Gbps	13.5 Gbps	17.5 Gbps
圧縮スループット	6 Gbps	12 Gbps	18 Gbps	25 Gbps
SSL アクセラレーションテクノロジー	ASIC	ASIC	ASIC	ASIC
メモリ	8 GB	16 GB	32 GB	64 GB
仮想ドメイン (VDM)	20	45	60	90
ネットワークインタフェース	2 x 10 GbE SFP+, 4 x GbE SFP, 4 x GbE	4 x 10 GbE SFP+, 8 x GbE SFP, 8 x GbE RJ45	8 x 10 GbE SFP+, 8 x GbE SFP, 8 x GbE RJ45	8 x GbE, 4 x 10 GbE, 2 x 40 GbE
10 / 100 / 1000 管理インタフェース	—	1	1	1
内蔵ストレージ	128 GB SSD	240 GB SSD	240 GB SSD	480 GB SSD
管理機能	HTTPS, SSH CLI, Direct Console DB9 CLI, SNMP	HTTPS, SSH CLI, Direct Console DB9 CLI, SNMP	HTTPS, SSH CLI, Direct Console DB9 CLI, SNMP	HTTPS, SSH CLI, Direct Console DB9 CLI, SNMP
電源	単一 (オプションで冗長化可能)	冗長	冗長	冗長
動作環境				
形状	1 U アプライアンス	1 U アプライアンス	1 U アプライアンス	2 U アプライアンス
AC 電源	100 ~ 240 V AC, 50 ~ 60 Hz	100 ~ 240 V AC, 63 ~ 47 Hz	100 ~ 240 V AC, 63 ~ 47 Hz	100 ~ 240 V AC, 63 ~ 47 Hz
消費電力 (平均 / 最大)	109 W / 130.8 W	267 W / 320 W	282 W / 340 W	300 W / 360 W
最大電流	100 V / 5 A, 240 V / 3 A	120 V / 7.1 A, 240 V / 3.4 A	120 V / 7.1 A, 240 V / 3.4 A	120 V / 8 A, 240 V / 4 A
放熱	446.3 BTU/h	1092 BTU/h	1160 BTU/h	1228 BTU/h
動作温度	0 ~ 40 °C	0 ~ 40 °C	0 ~ 40 °C	0 ~ 40 °C
保管温度	-25 ~ 70 °C	-20 ~ 70 °C	-20 ~ 70 °C	-20 ~ 70 °C
湿度	5 ~ 95% (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)	5 ~ 90% (結露しないこと)
準拠規格・認定				
準拠規格	FCC Part 15 Class A, C-Tick, VCCI Class A, CE, UL/c			
安全性に関する注意事項	CSA, C/US, CE, UL			
サイズ				
高さ x 幅 x 奥行	44 x 438 x 416 mm	44 x 438 x 530 mm	44 x 438 x 530 mm	88 x 438 x 530 mm
重量	9.97 kg	10.3 kg	10.3 kg	12.25 kg

数値はすべて「最大」の性能値であり、システム構成に応じて異なります。

* レイヤー 7 CPS : 新規の HTTP 接続数を計測 (TCP 接続あたり 1 HTTP リクエスト)

** SSL 接続あたり 1 HTTP リクエストの状態でのテスト、SSL 暗号は AES256-SHA、2000 キー



FortiADC 400D



FortiADC 1000F



FortiADC 2000F



FortiADC 4000F

技術仕様

	FortiADC VM01	FortiADC VM02	FortiADC VM04	FortiADC VM08
ハードウェア仕様				
サポートするハイパーバイザー	VMware ESX / ESXi, Citrix XenServer, Open Source Xen, Microsoft Hyper-V, KVM。 サポートされている最新ハイパーバイザーバージョンについては、『FortiADC VM Install Guide』を参照してください。			
L4 スループット*	1 Gbps	2 Gbps	4 Gbps	10 Gbps
仮想ドメイン (VDM)	0	0	5	10
仮想 CPU 数 (最大)	1	2	4	8
メモリ (最大)	4 GB	4 GB	8 GB	16 GB
仮想 NIC 枚数 (最大)	10	10	10	10
ストレージ容量 (最小 / 最大)	50 MB / 1 TB	50 MB / 1 TB	50 MB / 1 TB	50 MB / 1 TB
スループット	システム構成に依存	システム構成に依存	システム構成に依存	システム構成に依存
管理機能	HTTPS、SSH CLI、Direct Console DB9 CLI、SNMP			

* 数値は、ネットワークトラフィックとシステム構成によって異なります。記載されている性能の結果は、Intel CPU E5-1650 v2 @ 3.50 GHzでVMware ESXi 5.5が動作するアプライアンスを使用した場合のものであります。

FORTINET®

フォーティネットジャパン株式会社

〒106-0032

東京都港区六本木 7-7-7

Tri-Seven Roppongi 9 階

www.fortinet.co.jp/contact

お問い合わせ