

FORTIGATE™ 400/500

中大規模企業に適した リアルタイム・ネットワーク・プロテクション

FortiGate™アンチウイルスファイアウォールは、ハードウェアベースの専用ユニットで、ネットワークエッジでの完全なリアルタイム・ネットワーク・プロテクション・サービスを提供します。Fortinet社の革新的なチップ、FortiASIC™ Content ProcessorをベースとするFortiGateのプラットフォームは、ネットワークパフォーマンスを低下させることなくウイルスやワームなどのコンテンツベースの脅威を検知・駆除する唯一のシステムです。ウェブブラウジングのようなリアルタイムのアプリケーションでさえもパフォーマンスの影響を受けません。FortiGateのシステムには、統合ファイアウォール、コンテンツフィルタリング、VPN、不正侵入の検知・防御、帯域制御などの諸機能も含まれ、市場に出ているネットワーク保護ソリューションの中で最も費用効果が高く、操作が容易で、かつパワフルな製品です。

FortiGate-400 および FortiGate-500 は、セキュリティ、パフォーマンス、柔軟性、信頼性の点で中大規模企業クラスの要求に応えるアンチウイルスファイアウォールです。柔軟な導入オプションにより、FortiGateのユーザは、ポートをカスタマイズし、Route / NAT モードオプションを個別のインターフェースに割り当てることができます。両モデルとも、マルチゾーン機能を介して高精度のセキュリティを提供します。管理者は、マルチゾーン機能を利用してネットワークをゾーンに分割し、ゾーンごとのポリシーを設定できます。FortiGate-400 / 500 は、オートセンシング 10 / 100 Base-T イーサネットポートをそれぞれ 4 基と 12 基搭載し、ネットワークベースのアンチウイルス、ファイアウォール、コンテンツフィルタリング、VPN、ネットワークベースの侵入検知・阻止、帯域制御といった、受賞実績のある優れた機能を提供します。さらに、この両モデルは、冗長化された待機ユニットへのステートフルな迂回機能を備えた高可用性オペレーションをサポートします。FortiGate-400、FortiGate-500 とともに、Fortinet社のFortiResponse Networkによって自動的に最新情報に更新されます。FortiResponse Networkは、最新のウイルス／ワーム／トロイの木馬、不正侵入などの脅威を確実に阻止するため、世界各国で24時間体制のもと、絶え間なくアップデートを提供しています。



製品ハイライト

- ・ネットワークベースのアンチウイルス、ウェブコンテンツ・フィルタリング、ファイアウォール、VPN、ネットワークベースの不正侵入検知・防御、帯域制御を組み合わせ、完全なネットワークプロテクションを提供します。
- ・ネットワークパフォーマンスを低下させることなく、Eメール、転送ファイル、リアルタイム(ウェブ)トラフィックからのウイルスやワームを駆除します。
- ・フロントパネルのLCDディスプレイとコントロールボタンにより、外部コンソールなしで基本的なシステムパラメータを設定できるため、導入が容易です。
- ・DoS(サービス妨害)攻撃やDDoS(分散型サービス妨害)攻撃など含む、30種類以上の不正侵入を検知・阻止することにより、脅威への露出を抑えます。
- ・使いやすく実装が容易——迅速かつ容易なコンフィギュレーションウィザードにより、管理者はグラフィカルユーザインターフェースを使った手順に従って初期設定を実行できます。
- ・高可用性オプションがミッションクリティカルなアプリケーションのためのトランスペアレントな障害迂回をサポートします。
- ・マルチゾーンのサポートにより、高精度のネットワークセグメンテーションが可能になり、個々のゾーンに独自のアクセス/セキュリティポリシーを設定できます。
- ・ハードウェアアクセラレートされたASICベースのアーキテクチャにより、優れたパフォーマンスと信頼性を提供します。
- ・最新のウイルスと攻撃に関するデータベースを自動的にダウンロードします。FortiResponse Networkからの瞬時の「プッシュ」アップデートを受けることができます。
- ・ウイルス検疫機能により、攻撃のサンプルをFortinet Threat Response Teamに容易に提出できます。
- ・ベースとなるFortiOS™オペレーティングシステムは、アンチウイルス、ファイアウォール、IPSec VPN、不正侵入検知の各項目でICSA研究所の認定を取得しています。

FORTIGATE™ 400/500

主要機能と特長

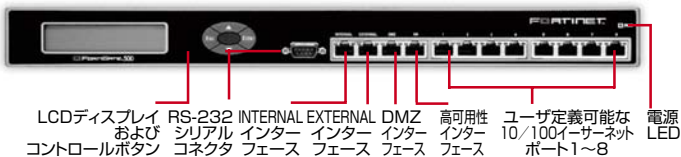
機能	概要	特徴
ネットワークベースのアンチウイルス (ICSA 認定)	リアルタイムでウイルスやワームを検知・駆除し、ウェブパフォーマンスを低下させることなく、送受信した Eメールの添付ファイル (SMTP、POP3、IMAP)、FTP、ウェブベース Eメールを含むウェブ (HTTP) トラフィックをスキャン	ウイルスやワームをネットワーク侵入前に阻止することにより脆弱性を解消
不正侵入検知 (ICSA 認定)	カスタマイズ可能なデータベースに 1300 種類以上の攻撃を登録し、それに基づいて警告	リアルタイムの警告と捜査データを提供し、攻撃を識別・分析
不正侵入阻止	ユーザ設定可能なスレッショルド (閾値) をベースに、DoS (サービス妨害) 攻撃や DDoS (分散型サービス妨害) 攻撃など含む 30 種類以上の不正侵入や攻撃を積極的に阻止	重大な損害を与えかねない攻撃をネットワークエッジで阻止
ファイアウォール (ICSA 認定)	ステートフル・インスペクション技術を採用した強力なファイアウォール	認定された保護性能、最大限のパフォーマンスとスケラビリティ
ウェブコンテンツ・フィルタリング	URL ブロッキングおよびキーワード/フレーズブロッキングを介して、不適切なコンテンツや悪意あるスクリプトを阻止するよう、すべてのウェブコンテンツを処理	企業に対して生産性向上を、CIPA (児童インターネット保護法) に準拠しようとする教育機関に対して規定遵守を保証
VPN (ICSA 認定)	業界標準規格の IPSec、PPTP、L2TP VPN をサポート	ネットワークとクライアント間で安全な通信トンネルを提供
トランスパレントモード	FortiGate ユニッツは、既存のファイアウォールなどの機器との併存で導入し、アンチウイルス、コンテンツフィルタリングなどのコンテンツ集約型アプリケーションを提供可能	レガシーシステムの統合/投資保護が容易
リモートアクセス	Fortinet Remote VPN Client を搭載するすべての PC からの安全なリモートアクセスをサポート	モバイル/リモート/在宅勤務者向けの低コストで場所を選ばない常時接続

システム仕様

FortiGate-400



FortiGate-500



FORTIGATE™ 400/500

仕様

	FortiGate-400	FortiGate-500	FortiGate-400	FortiGate-500
インターフェース				
10/100イーサネットポート	4	12		
システムパフォーマンス				
同時セッション数	40万	40万		
新規セッション数/秒	1万	1万		
ファイアウォールスループット (Mbps)	280	280		
168ビット3DESスループット (Mbps)	80	90		
無制限の同時ユーザ	・	・		
ポリシー 5000 8000	5000	8000		
スケジュール 256 256	256	256		
アンチウイルス、ワーム検知&駆除				
FortiResponse Networkからの自動ウイルスデータベース更新	・	・		
HTTP、FTP、SMTP、POP3、IMAP、VPNトンネル内のスキャン	・	・		
感染したメッセージの検疫	・	・		
ファイアウォールのモードと機能				
NAT、PAT、トランスベアレント (ブリッジ)	・	・		
ルーティングモード (RIPv1、v2)	・	・		
VLANタギング (802.1q)	・	・		
アクセス制限リスト (ソースIP、デスティネーションIP、TCPポート、UDPポート)	・	・		
ユーザグループベースの認証	・	・		
H.323 NATトラバース	・	・		
WINSサポート	・	・		
VPN				
PPTP、L2TP、IPSec	・	・		
トンネル数	2000	2000		
暗号化方式 (DES、3DES、AES)	・	・		
SHA-1/MD5認証	・	・		
Fortinet Remote VPN Clientのサポート	・	・		
PPTP、L2TP、VPNクライアントパスル	・	・		
ハブ&スポーク	・	・		
IKE認証 (X.509)	・	・		
IPSec NATトラバース	・	・		
デッドピア検知	・	・		
大手VPNベンダーとの相互運用性	・	・		
コンテンツフィルタリング				
URLブロック	・	・		
キーワード/フレーズブロック	・	・		
URL除外リスト	・	・		
コンテンツポリシープロファイル	32	32		
Javaアプレット、クッキー、Active Xのブロック	・	・		
Eメールフィルタリング (キーワード、ブラックリスト、除外リスト)	・	・		
不正侵入検知				
1300種類以上の攻撃の検知	・	・		
30種類以上の攻撃の阻止	・	・		
複数のインターフェースでの検知および阻止	・	・		
カスタマイズ可能な検知シグニチャリスト	・	・		
ロギング/モニタリング				
内部保存可能なログ容量/リムーバブルHD	40GB	40GB		
リモートSyslog/WELFサーバーへのログ	・	・		
グラフィカルなリアルタイム/ヒストリカルモニタリング	・	・		
SNMP	・	・		
ウイルスや攻撃をEメールで通知	・	・		
VPNトンネルのモニター	・	・		
高可用性 (HA)				
アクティブパッシブ	・	・		
ステートフルフェールオーバー (FW&VPN)	・	・		
機器障害の検知・通知	・	・		
リンクステータスのモニター	・	・		
ネットワーク				
マルチWANリンクサポート	・	・		
マルチゾーンサポート	・	・		
ゾーン間のルート	・	・		
ポリシーベース・ルーティング	・	・		
PPPoEクライアント(HA構成を除く)	・	・		
システム管理				
コンソールインターフェース	・	・		
WebUI (HTTP/HTTPS)、複数言語サポート	・	・		
コマンドライン・インターフェース (Telnet/ssh)	・	・		
セキュアコマンドシェル (SSH)	・	・		
FortiManagerシステム	・	・		
管理				
複数管理者およびユーザレベル定義	・	・		
TFTPとWebUIを介した更新および変更	・	・		
システムソフトウェア・ロールバック	・	・		
ユーザ認証				
内部データベース	・	・		
RADIUS/LDAP DBのサポート	・	・		
RADIUSによるXauthサポート(IPSec)	・	・		
IP/MACアドレスバインディング	・	・		
トラフィック管理				
ポリシーベースの帯域制御	・	・		
帯域保証	・	・		
最大帯域幅	・	・		
優先割当	・	・		
寸法				
高さ		4.5cm	4.5cm	
幅		42.5cm	42.5cm	
長さ		30.5cm	30.5cm	
重量		5kg	5kg	
ラックマウント		・	・	
電源				
AC入力電圧		100~240V	100~240V	
AC入力電流		4A	4A	
周波数		47~63Hz	47~63Hz	
消費電力		最大180W	最大180W	
環境				
動作温度		0~40°C	0~40°C	
保管温度		-25~70°C	-25~70°C	
湿度		5~95%	5~95%	
		(結露しないこと)	(結露しないこと)	
規格準拠				
FCCクラスAパート15	・	・		
CSA/CUS	・	・		
CE	・	・		
UL	・	・		
ICSAアンチウイルス	・	・		
ICSAファイアウォール	・	・		
ICSA IPSec	・	・		
ICSA不正侵入検知	・	・		