

FORTIGATE™ 5020

高パフォーマンス・コンテンツ セキュリティの 高密度ソリューション

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・防御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、URL 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-5020 は、FortiGate-5000 シリーズのエントリーレベルにあたるシステムです。FortiGate-5020 システムは、FortiGate-5020 シャシーにブレードサーバを 1 基または 2 基搭載する構成で、さまざまなスループット、冗長性、インターフェースの要求に応じることができます。FortiGate-5020 シャシーは、次世代のキャリアクラス機器のための仕様である AdvancedTCA(ATCA) に準拠しています。電源装置とファンはホットスワップ可能で、電源と冷却の高い可用性を約束します。FortiGate-5020 のシャシーが搭載する FortiGate-5001 ブレードは、高速ネットワークおよびコンテンツセキュリティサービス向けの FortiASIC™ Content Processor を採用しています。各 FortiGate-5001 ブレードには、ギガビット対応 Small Form-factor Pluggable(SFP) ポートが 4 基、10 / 100 / 1000 イーサネットポートが 4 基装備されています。FortiGate-5020 のバックプレーン接続は、アクティブ-アクティブ、アクティブ-パッシブのフェイルオーバー構成における有線ベースでの HA 接続が可能です。FortiGate-5020 は、Fortinet 社の FortiProtect™ Network によって自動的に最新情報に更新されます。FortiProtect 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

- ・大規模企業および管理セキュリティ・サービスプロバイダ (MSSP) に最適なソリューションです。
- ・ネットワークパフォーマンスを低下させることなく、HTTP、SMTP、POP3、IMAP、FTP のトラフィックをスキャン・防御します。
- ・ネットワークベースのアンチウイルス、URL 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侵入検知・防御、帯域制御、アンチスパム保護など、完全なネットワーク保護機能を提供します。
- ・「トランスペアレントモード」での運用は、既存のファイアウォールや VPN、侵入検知・防御、その他の既存システムと組み合わせたアンチウイルス、コンテンツフィルタリングの実装をサポートします。
- ・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、1300 種類以上の不正侵入を検知・防御することにより、脅威への露出を抑えます。
- ・仮想 LAN とセキュリティ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。
- ・CPU とメモリの使用、ネットワークとセッションの状態、ウイルス/不正侵入の検知をわかりやすくグラフィック表示します。このリアルタイムのシステムステータス・モニタリングにより、総所有コスト (TCO) の削減が可能です。
- ・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と冗長化されたホットスワップ可能な電源装置により、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。FortiProtect 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。
- ・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。

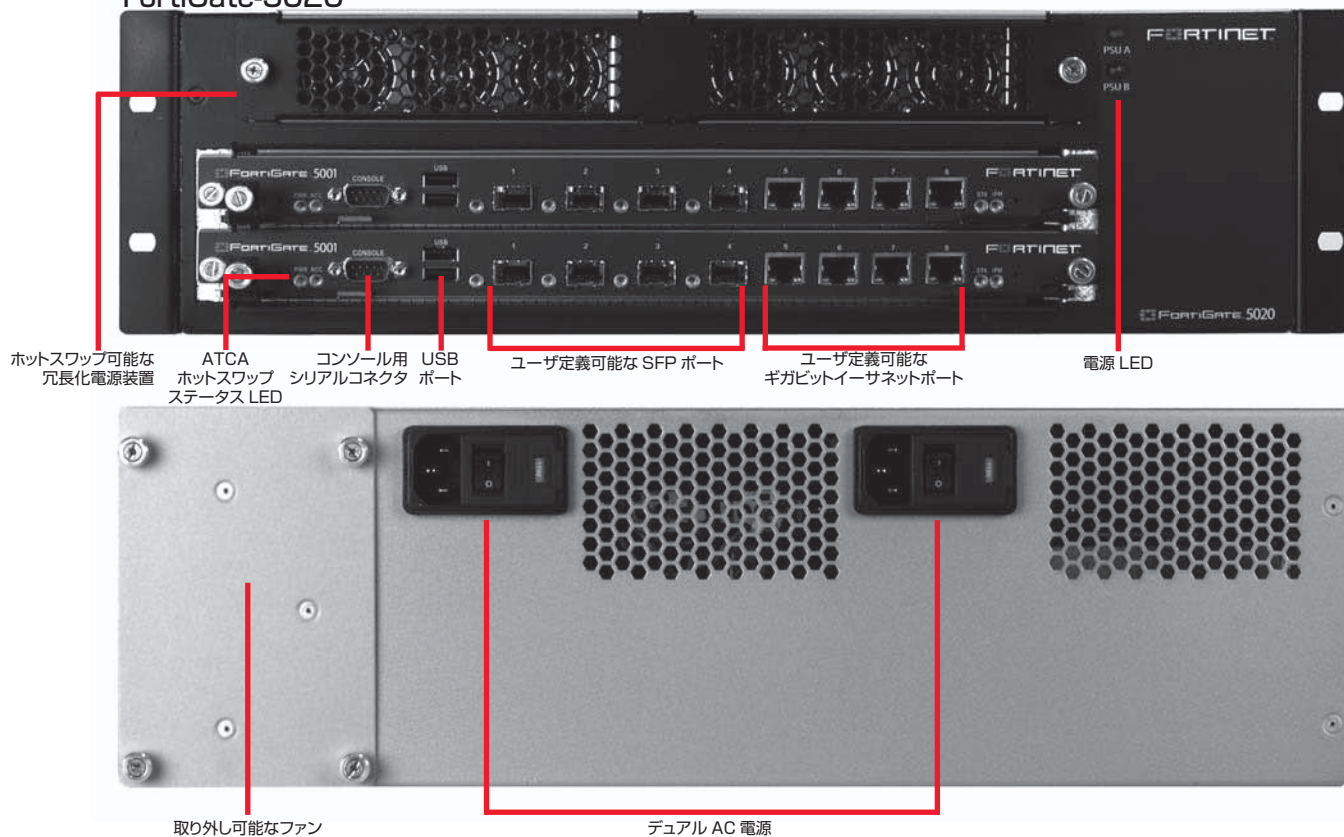
FORTIGATE™ 5020

主要機能と特長

機能	概要	特長
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・防御し、送受信した Eメールの添付ファイル (SMTP、POP3、IMAP)、ウェブベース Eメールを含む HTTP や FTP、暗号化された VPNトンネルをスキャン	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・防御 (ICSA 認定)	ユーザ設定可能なスレッショルド (閾値) をベースに、1300 種類以上の不正侵入や攻撃を検知して防御。検知シグニチャは FortiProtect Network によって自動的に最新状態に更新	従来のアンチウイルス製品を回避する攻撃も、急速な攻撃拡大にリアルタイムで対応して阻止
URL 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。FortiGuard のポリシーベースの URL フィルタリングもサポート	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
ファイアウォール (ICSA 認定)	業界標準のステートフル・インスペクション技術を採用したファイアウォール	認定された保護性能、最大限のパフォーマンスとスケーラビリティ
VPN (ICSA 認定)	業界標準規格の PPTP、L2TP、IPSec VPN をサポート	サイトツーサイトの専用通信用やリモートアクセス通信用に公共のインターネット網を利用することによりコストを低減
トランスパレントモード	FortiGate ユニットは、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	FortiClient ホストセキュリティ・ソフトウェア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-5020



FORTIGATE™ 5020

仕様	FortiGate-5001 ブレード	FortiGate-5020 システム (ブレード2基搭載時)	FortiGate-5001 ブレード	FortiGate-5020 システム (ブレード2基搭載時)
インターフェース				
SFPポート	4	8	•	•
10/100/1000Base-Tポート	4	8	•	•
システムパフォーマンス				
同時セッション数	100万	200万	•	•
新規セッション数/秒	2万5000	5万	•	•
ファイアウォールスループット(Gbps)	50	95	•	•
168ビット3DESスループット(Mbps)	600	1.2Gbps	•	•
無制限の同時ユーザ	•	•	•	•
ポリシー	5万	10万	•	•
スケジュール	256	512	•	•
アンチウイルス、ワーム検知&防御				
HTTP、FTP、SMTP、POP3、IMAP、 VPNトンネル内のスキャン	•	•	•	•
ファイルサイズによるブロック	•	•	•	•
ファイアウォールのモードと機能				
NAT、PAT、トランスパレント(ブリッジ)	•	•	•	•
ルーティングモード(RIPv1、v2)	•	•	•	•
ポリシーベースNAT	•	•	•	•
VLANタギング(802.1q)	•	•	•	•
バーチャルドメイン数	最大250	最大250	•	•
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	5000	1万	•	•
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・パススルー	•	•	•	•
ハブ・スポーク型	•	•	•	•
IKE認証(X.509)	•	•	•	•
IPSec NATトラバース	•	•	•	•
アグレッシブモード	•	•	•	•
リプレイプロテクション	•	•	•	•
デッドピア検知	•	•	•	•
大手VPNベンダーとの相互運用性				
URLフィルタリング	•	•	•	•
URL/キーワード/フレーズブロック	•	•	•	•
URL除外リスト	•	•	•	•
コンテンツプロファイル	32	64	•	•
Javaアプレット、クッキー、Active Xの ブロック	•	•	•	•
FortiGuard™URLフィルタリングのサポート	•	•	•	•
動的な不正侵入検知&防御				
1300種類以上の攻撃の防御	•	•	•	•
FortiProtect Networkによるリアル タイムの自動更新	•	•	•	•
カスタマイズ可能な検知シグニチャリスト	•	•	•	•
アンチスパム				
オープン・リレー・データベース・サーバー によるブラックリストのリアルタイム更新	•	•	•	•
MIMEヘッダのチェック	•	•	•	•
キーワード/フレーズ・フィルタリング	•	•	•	•
IPアドレスによるブラックリスト/除外リスト	•	•	•	•
ロギング/モニタリング				
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	•	•	•	•
メールによるウイルスや攻撃の通知	•	•	•	•
VPNトンネルのモニター	•	•	•	•
ハイアベイラビリティ(HA)				
アクティブ-アクティブ、アクティブ-パッシブ	•	•	•	•
ステートフルフェールオーバー	•	•	•	•
機器障害の検知・通知	•	•	•	•
リンクステータスのモニター	•	•	•	•
リンクフェイルオーバー	•	•	•	•
ネットワーク				
マルチWANリンクサポート	•	•	•	•
マルチゾーンのサポート	•	•	•	•
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)	•	•	•	•
FortiManagerシステム	•	•	•	•
管理				
役割ベースの管理	•	•	•	•
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	•	•	•	•
RSA SecureID	•	•	•	•
RADIUSによるXauthのサポート (IPSec)	•	•	•	•
IP/MACアドレスバインディング	•	•	•	•
トラフィック管理				
DiffServ技術による制御	•	•	•	•
ポリシーベースの帯域制御	•	•	•	•
帯域幅保証/最大帯域幅/優先割当	•	•	•	•
寸法				
高さ/幅/長さ			13.3cm / 43.2cm / 39.4cm	
重量			16.1kg	
ラックマウント			•	
電源				
AC入力電圧			100~240V	
AC入力電流			10A	
周波数			47~63Hz	
消費電力			最大800W	
環境				
動作温度			0~40°C	
保管温度			-25~70°C	
湿度			5~95%	
(結露しないこと)				
規格準拠				
FCCクラスAパート15			•	
CE			•	
UL			•	
ICSAアンチウイルス/ファイアウォール /IPSec/NIDS			•	

Specifications subject to change without notice. Copyright 2004 Fortinet, Inc. All rights reserved. Fortinet, FortiGate, FortiAsic, FortiOS and FortiProtect are trademarks of Fortinet, Inc.

2005/05