



# GAMME DE PRODUITS

**FORTINET**<sup>TM</sup>  
REAL TIME NETWORK PROTECTION

**[www.fortinet.com/contact](http://www.fortinet.com/contact)**

Tél : +33 1 5858 2864 - Support Ventes : +33 4 8987 0510 - Assistance technique : +33 4 8987 0555

Caractéristiques susceptibles d'être modifiées sans préavis. Copyright 2005 Fortinet, Inc. Tous droits réservés. Fortinet, FortiGate, FortiWiFi, FortiReporter, FortiProtect, FortiASIC et FortiOS sont des marques de Fortinet, Inc. BRO1030506

# PRÉSENTATION DE LA GAMME FORTIGATE – SOHO / Succursales / SMB

Liste des fonctions	FGT-50A	SOHO / Succursales			PME	
		FGT-50A	FGT-60	WiFi-60	FGT-100A	FGT-200A
<b>Interfaces</b>	Ports Ethernet 10/100	2	7	7	8	8
<b>Performances du système</b>	Sessions simultanées	25K	50K	50K	200K	400K
	Nouvelles sessions/seconde	2K	2K	2K	4K	4K
	Débit du pare-feu (Mbps)	50	70	70	100	150
	Débit Triple-DES, 168 bits (Mbps)	10	20	20	40	70
	Nombre d'utilisateurs simultanés illimité	•	•	•	•	•
	Règles	200	500	500	1K	2K
	Plannings	256	256	256	256	256
<b>Antivirus/Détection et élimination de vers (Certifié ICSA)</b>	Détection HTTP, SMTP, POP3, IMAP, FTP et tunnels VPN encryptés	•	•	•	•	•
	MAJ automatique de la base de données virus	•	•	•	•	•
	Mise en quarantaine des messages infectés	•	•	•	•	Option
	Blocage par taille de fichier	•	•	•	•	•
<b>Pare-feu (Certifié ICSA)</b>	NAT, PAT, Transparent (pont), Mode Routage	•	•	•	•	•
	Support des VLAN 802.1q	•	•	•	•	•
	Domaines virtuels	•	•	•	•	•
	Authentification par groupe d'utilisateurs	•	•	•	•	•
	NAT Traversal H.323	•	•	•	•	•
	Profils de protection paramétrables	32	32	32	32	32
<b>VPN (Certifié ICSA)</b>	Nombre de tunnels dédiés	20	40	40	80	200
	Cryptage (DES, 3DES, AES)	•	•	•	•	•
	PPTP, L2TP, VPN Client Pass Through	•	•	•	•	•
	Support de l'Architecture Concentrateur VPN	•	•	•	•	•
	Authentification par certificat (X.509) pour IKE	•	•	•	•	•
	IPSec NAT Traversal	•	•	•	•	•
	Support de la solution d'authentification forte de RSA	•	•	•	•	•
<b>Filtrage de contenu</b>	Blocage d'URL, de mots clés, liste d'exemptions	•	•	•	•	•
	Filtrage des Applet Java, Cookies, Active X	•	•	•	•	•
	Support du Filtrage par catégorie via FortiGuard	•	•	•	•	•
<b>Système dynamique de de prévention des intrusions (IPS)</b>	Prévention de plus de 1 400 attaques	•	•	•	•	•
	Paramétrage de la liste dyn. de détection d'attaques	•	•	•	•	•
	MAJ automatique de la BDD des attaques	•	•	•	•	•
<b>Anti-spam</b>	Liste noire temps réel/serveur BDD type relais ouvert	•	•	•	•	•
	Contrôle sur les en-tête MIME	•	•	•	•	•
	Filtrage par mot-clé/phras	•	•	•	•	•
	Liste noire des adresses IP/liste des exemptions	•	•	•	•	•
<b>Journalisation / Supervision</b>	Capacité interne pour la journalisation	•	•	•	•	Option
	Notification par courriel des virus et des attaques	•	•	•	•	•
	Syslog, SNMP	•	•	•	•	•
<b>Haute disponibilité (HA)</b>	Actif-Actif, Actif-Passif	•	•	•	•	•
	Sauvegarde sessions FW et VPN en cas de bascule	•	•	•	•	•
	Détection et notification périphériques défectueux de l'état des liaisons réseaux	•	•	•	•	•
<b>Réseau</b>	Support de multiples liaisons WAN	•	•	•	•	•
	PPPoE	•	•	•	•	•
	Client/Serveur DHCP	•	•	•	•	•
	Routage en fonction source ou type de protocole	•	•	•	•	•
	Routage dynamique (RIP v1 & v2, OSPF)	•	•	•	•	•
<b>Gestion du système</b>	Interface console (RS-232)	•	•	•	•	•
	Interface utilisateur Web (HTTPS), multilingue	•	•	•	•	•
	Interface ligne de commande, Shell de commande sécurisé (SSH)	•	•	•	•	•
	Contrôlable depuis un FortiManager	•	•	•	•	•
<b>Administration</b>	Niveaux multi-administrateurs et multi-utilisateurs	•	•	•	•	•
	MAJ via TFTP et interface utilisateur Web	•	•	•	•	•
	Restauration logicielle du système	•	•	•	•	•
<b>Authentification des utilisateurs</b>	Base de données interne	•	•	•	•	•
	Base de données RADIUS/LDAP externe	•	•	•	•	•
	Couplage d'adresses IP/MAC	•	•	•	•	•
	Xauth via RADIUS pour VPN IPSec	•	•	•	•	•
	Authentification forte RSA SecurID	•	•	•	•	•
<b>Contrôle de bande passante</b>	Contrôle de bande passante selon les règles de FW	•	•	•	•	•
	Paramétrage DiffServ	•	•	•	•	•
	Bande passante : Garantie, Maximum, par Priorité	•	•	•	•	•

# PRÉSENTATION DE LA GAMME FORTIGATE – Entreprise

Liste des fonctions		FGT-300A	FGT-400A	FGT-500A	FGT-800
<b>Interfaces</b>	Ports Ethernet 10/100 Ports Ethernet Gigaoctet (cuivre/fibres)	4 2C	4 2C	8 2C	4 4C
<b>Performances du système</b>	Sessions simultanées Nouvelles sessions/seconde Débit du pare-feu (Mbps) Débit Triple-DES, 168 bits (Mbps) Nombre d'utilisateurs simultanés illimité Règles Plannings	400K 10K 400 120 • 5K 256	400K 10K 450 135 • 5K 256	400K 10K 500 150 • 8K 256	400K 10K 1Gbps 200 • 20K 256
<b>Antivirus / Détection et élimination de vers (Certifié ICESA)</b>	Détection HTTP, SMTP, POP3, IMAP, FTP et tunnels VPN encryptés MAJ automatique de la BDD des virus Mise en quarantaine des messages infectés Blocage par taille de fichier	• • Option •	• • Option •	• • Option •	• • • •
<b>Pare-feu (Certifié ICESA)</b>	NAT, PAT, Transparent (pont), Mode Routage Support des VLAN 802.1q Domaines virtuels Authentification par groupe d'utilisateurs NAT Traversal H.323 Profils de protection paramétrables	• • • • • • 32	• • • • • • 32	• • • • • • 32	• • • • • • 32
<b>VPN (Certifié ICESA)</b>	Nombre de tunnels dédiés Cryptage (DES, 3DES, AES) PPTP, LZTP, VPN Client Pass Through Support de l'Architecture Concentrateur VPN Authentification par certificat (X.509) pour IKE IPSec NAT Traversal Support de la solution d'authentification forte de RSA	1.5K • • • • • •	2K • • • • • •	3K • • • • • •	3K • • • • • •
<b>Filtrage de contenu</b>	Blocage d'URL, de mots clés, liste d'exemptions Filtrage des Applet Java, Cookies, Active X Support du Filtrage par categorie via FortiGuard	• • •	• • •	• • •	• • •
<b>Système dynamique de prévention des intrusions (IPS)</b>	Prévention de plus de 1 400 attaques Parametrage de la liste dyn. de détection d'attaques MAJ automatique de la BDD des attaques	• • •	• • •	• • •	• • •
<b>Anti-spam</b>	Liste noire temps réel/serveur BDD type relais ouvert Contrôle sur les en-tête MIME Filtrage par mot-clé/phrased Liste noire des adresses IP/liste des exemptions	• • • •	• • • •	• • • •	• • • •
<b>Journalisation / Supervision</b>	Capacité interne pour la journalisation Notification par courriel des virus et attaques Syslog, SNMP	Option • •	Option • •	Option • •	40G • •
<b>Haute disponibilité (HA)</b>	Actif-Actif, Actif-Passif sauvegarde sessions FW et VPN en cas de bascule Détection, notification périphériques défectueux Contrôle de l'état des liaisons réseaux	• • • •	• • • •	• • • •	• • • •
<b>Réseau</b>	Support de multiples liaisons WAN PPPoE Client/Serveur DHCP Routage en fonction source ou type de protocole Routage dynamique (RIP v1 & v2, OSPF)	• • • • •	• • • • •	• • • • •	• • • • •
<b>Gestion du système</b>	Interface console (RS-232) Interface utilisateur Web (HTTPS), multilingue Interface ligne commande, Shell commandé sécurisé (SSH) Controlable depuis un FortiManager	• • • •	• • • •	• • • •	• • • •
<b>Administration</b>	Niveaux multi-administrateurs et multi-utilisateurs MAJ via TFTP et interface utilisateur Web Restauration logicielle du système	• • •	• • •	• • •	• • •
<b>Authentification des utilisateurs</b>	Base de données interne Base de données RADIUS/LDAP externe Couplage d'adresses IP/MAC Xauth via RADIUS pour VPN IPSec Authentification forte RSA SecurID	• • • • •	• • • • •	• • • • •	• • • • •
<b>Contrôle de bande passante</b>	Contrôle de bande passante selon les règles de FW Paramétrage DiffServ Bande passante : Garantie, Maximum, par Priorité	• • •	• • •	• • •	• • •

# PRÉSENTATION DE LA GAMME FORTIGATE – Grandes entreprises / Prestataires de services

Liste des fonctions		Grandes entreprises / Prestataires de services					
		FGT-3000	FGT-3600	FGT-5001	FGT-5020	FGT-5050	FGT-5140
<b>Interfaces</b>	Ports Ethernet 10/100 Ports Ethernet Gigaocet (cuivre/fibres)	3 1C/2F	1 2C/4F	4/4SFP	8/8SFP	20/20SFP	56/56SFP
<b>Performances du système</b>	Sessions simultanées Nouvelles sessions/seconde Débit du pare-feu (Mbps) Débit Triple-DES, 168 bits (Mbps) Nombre d'utilisateurs simultanés illimité Règles Plannings	975K 20K 2.25Gbps 530 50K 256	1M 25K 4Gbps 600 50K 256	1M 25K 4Gbps 600 50K 256	2M 50K 8Gbps 1.2Gbps 100K 256	5M 125K 20Gbps 3Gbps 250K 1280	14M 350K 56Gbps 8.4Gbps 700K 3584
<b>Antivirus / Détection et élimination de vers (Certifié ICSA)</b>	Détection HTTP, SMTP, POP3, IMAP, FTP et tunnels VPN encryptés MAJ automatique de la BDD des virus Mise en quarantaine des messages infectés Blocage par taille de fichier	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •
<b>Pare-feu (Certifié ICSA)</b>	NAT, PAT, Transparent (pont), Mode Routage Support des VLAN 802.1q Domaines virtuels Authentification par groupe d'utilisateurs NAT Traversal H.323 Profil de protection paramétrables	• • • • • • 200	• • • • • • 200	• • • • • • 200	• • • • • • 200	• • • • • • 200	• • • • • • 200
<b>VPN (Certifié ICSA)</b>	Nombre de tunnels dédiés Cryptage (DES, 3DES, AES) PPTP, L2TP, VPN Client Pass Through Support de l'Architecture Concentrateur VPN Authentification par certificat (X.509) pour IKE IPSec NAT Traversal Support de la solution d'authentification forte de RSA	5K • • • • • •	5K • • • • • •	5K • • • • • •	10K • • • • • •	25K • • • • • •	70K • • • • • •
<b>Filtrage de contenu</b>	Blocage d'URL, de mots clés, liste d'exemptions Filtrage des Applet Java, Cookies, Active X Support du Filtrage par categorie via FortiGuard	• • •	• • •	• • •	• • •	• • •	• • •
<b>Système dynamique de prévention des intrusions (IPS)</b>	Prévention de plus de 1 400 attaques Paramétrage de la liste dyn. de détection d'attaques MAJ automatique de la BDD des attaques	• • •	• • •	• • •	• • •	• • •	• • •
<b>Anti-spam</b>	Liste noire temps réel/serveur BDD type relais ouvert Contrôle sur les en-tête MIME Filtrage par mot-clé/phras Liste noire des adresses IP/liste des exemptions	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •
<b>Journalisation / Supervision</b>	Capacité interne pour la journalisation Notification par courriel des virus et attaques Syslog, SNMP	40G • •	40G • •	• • •	• • •	• • •	• • •
<b>Haute disponibilité (HA)</b>	Actif-Actif, Actif-Passif Sauvegarde sessions FW et VPN en cas de bascule Détection, notification périphériques défectueux Onduleurs Contrôle de l'état des liaisons réseaux	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •
<b>Réseau</b>	Support de multiples liaisons WAN PPPoE Client/Serveur DHCP Routage en fonction source ou type de protocole Routage dynamique (RIP v1 & v2, OSPF)	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •
<b>Gestion du système</b>	Interface console (RS-232) Interface utilisateur Web (HTTPS), multilingue Interface ligne commande, Shell commandé sécurisé (SSH) Controlable depuis un FortiManager	• • • •	• • • •	• • • •	• • • •	• • • •	• • • •
<b>Administration</b>	Niveaux multi-administrateurs et multi-utilisateurs MAJ via TFTP et interface utilisateur Web Restauration logicielle du système	• • •	• • •	• • •	• • •	• • •	• • •
<b>Authentification des utilisateurs</b>	Base de données interne Base de données RADIUS/LDAP externe Couplage d'adresses IP/MAC Xauth via RADIUS pour VPN IPSec Authentification forte RSA SecurID	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •	• • • • •
<b>Contrôle de bande passante</b>	Contrôle de bande passante selon les règles de FW Paramétrage DiffServ Bande passante : Garantie, Maximum, par Priorité	• • •	• • •	• • •	• • •	• • •	• • •