

POINTS FORTS DES FORTIGATE 300A

- Offre complète de services de protection réseau incluant l'antivirus, le filtrage des contenus Web, le firewall, VPN, la détection d'intrusions, la gestion de la bande passante et l'anti-spam.
- Élimine les virus et les vers dans le trafic Web (http) et FTP sans dégrader les performances réseau.
- Diminue l'exposition aux menaces provenant de l'Internet en détectant et en prévenant 1300 types d'intrusions incluant les attaques DOS et DDOS.
- Écran LCD et clavier sur le FortiGate-300A pour réaliser la configuration de base sans utiliser une console externe.
- Disque interne de grande capacité pour le stockage de fichiers de trace.
- La mise en quarantaine des virus facilite l'envoi des exemples de virus au réseau FortiResponse.
- Niveau de performance et fiabilité garantis par une architecture basée sur un circuit ASIC.
- Port DMZ/HA configurable.
- Mise à jour automatique des dernières bases de données de signatures des virus et des attaques par téléchargement ou en mode "push".
- Système d'exploitation FortiOS™ certifié ICSA pour l'antivirus, le firewall, le VPN IPSec et la détection d'intrusions.
- Utilisation et déploiement aisé par l'intermédiaire d'une interface graphique.
- Compatible avec la plate-forme d'administration centralisée FortiManager.
- Interface utilisateur Web (GUI) et filtrage des contenus supportant plusieurs langues.

FORTIGATE™ 300A

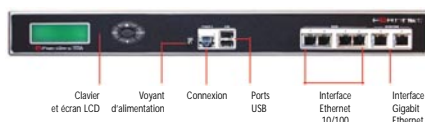
Protection des réseaux en temps réel pour les PME/PMI

Les solutions Antivirus Firewalls FortiGate sont des appliances offrant une gamme complète de services dédiés à la protection en temps réel des réseaux.

Basées sur un circuit spécialisé dans le traitement des contenus (FortiASIC™) et sur un système d'exploitation sécurisé, les Antivirus Firewalls FortiGate sont les seules solutions du marché capables de détecter et d'éliminer les virus, les vers et bien d'autres types de contenus dangereux sans réduire les performances réseaux, même pour les applications en temps réel telles que la navigation Web. Les solutions FortiGate intègrent de base les fonctions de pare-feu, de filtrage des contenus, de VPN, de détection d'intrusions et de gestion de bande passante ou encore d'anti-spam. Ces fonctionnalités combinées à un haut niveau de performances font des Antivirus Firewall FortiGate les solutions proposant le meilleur rapport prix/performance du marché.



Les Antivirus Firewalls FortiGate-300A ont été conçus pour répondre aux besoins des petites et moyennes entreprises aussi bien qu'à ceux des agences distantes. Disposant de 4 interfaces Ethernet 10/100 BaseT auto-configurables et 2 interfaces 10/100/1000, le FortiGate-300A fournit les fonctions de firewall "Stateful Inspection", d'antivirus réseau, de VPN, de filtrage de contenus, de détection d'intrusions et de gestion de bande passante et anti-spam. Les FortiGate-300A disposent d'un disque interne de 20 Go pour le stockage des fichiers de trace. Le FortiGate-300A offre la possibilité d'utiliser le port DMZ en tant que port haute disponibilité pour les entreprises qui souhaitent mettre en œuvre une configuration redondante. Le réseau mondial FortiResponse de Fortinet assure la mise à jour automatique des FortiGate-300A pour garantir la protection contre les derniers virus, vers, chevaux de troie et autres menaces potentielles.



Fonctionnalités	Description	Bénéfices
Antivirus réseau (Certifié ICSA)	Détecte, met en quarantaine et élimine les virus et les vers en temps réel. Inspecte les attachements emails entrants et sortants (SMTP, POP3, IMAP), le Web (HTTP) et le trafic FTP sans dégrader les performances.	Élimine les vulnérabilités potentielles en stoppant les virus, les vers et les spywares avant qu'ils ne pénètrent dans le réseau.
Détection d'intrusions (Certifié ICSA)	Fournit des alarmes paramétrables à partir d'une base de données de plus de 1300 signatures.	Avertissement en temps réel et mise à disposition de données pour l'identification et l'analyse des attaques.
Prévention d'intrusions	Une prévention active contre plus de 1300 attaques incluant les attaques DOS et DDOS. Les seuils d'alerte sont paramétrables par l'administrateur.	Stoppe les attaques les plus dangereuses à la frontière du réseau de l'entreprise.
Filtrage des contenus Web	Analyse tous les contenus Web afin de bloquer les contenus inappropriés et les scripts malveillants.	Améliore la productivité des employés en interdisant l'accès aux contenus non appropriés.
Anti-Spam	Détecte, tag ou élimine les courriels non-solicités.	Soulage les serveurs de messagerie ainsi que les boîtes aux lettres des utilisateurs, du trafic de courriel indésirable.
Firewall (Certifié ICSA)	Puissant firewall basé sur le standard "Stateful Inspection".	Protection certifiée performante et évolutive.
VPN (Certifié ICSA)	Conforme aux standards PPTP, L2TP, et support des VPN IPSec et SSL certifiés ICSA. Support du déploiement de WLANs avec authentification des utilisateurs, des tunnels chiffrés, et le support de LDAP.	Diminue les coûts en utilisant le réseau Internet pour les communications privées de site à site et pour les accès distants.
Mode transparent	Les solutions FortiGate peuvent être déployées dans une architecture sécurisée comprenant déjà des firewalls pour assurer la protection antivirus et le filtrage des contenus	Intégration aisée dans une architecture existante et protection de l'investissement initial.
Accès distants	Support des accès distants sécurisés à partir de n'importe quel PC équipé d'un client Remote VPN de Fortinet.	Accès distants sécurisés, fiables et économiques pour les utilisateurs distants et mobiles.

Spécifications

	FortiGate-300A	FortiGate-300A
Interfaces		
10/100/1000 Gigabit Ethernet Ports	2	
10/100 Ethernet Ports	4	
USB ports	2	
Performances des équipements		
Concurrent sessions	400 000	
New sessions/second	10 000	
Firewall throughput (Mbps)	400	
168-bit Triple-DES throughput (Mbps)	120	
Antivirus throughput* (Mbps)	70	
Unlimited concurrent users	•	
Policies	5000	
Schedules	256	
Détection et élimination des virus et des vers		
Scans HTTP,FTP,SMTP,POP3,IMAP, and encrypted VPN Tunnels	•	
Quarantine infected messages	•	
Block by file size	•	
Modes et fonctionnalités du firewall		
NAT,PAT,transparent (bridge)	•	
Routing mode (RIP v1,v2)	•	
Virtual domains (NAT/transparent mode)	2/10	
VLAN tagging (802.1q)	•	
User Group-based authentication	•	
H.323 NAT Traversal	•	
WINS Support	•	
VPN		
PPTP,L2TP,and IPSec	•	
Dedicated tunnels	1500	
Encryption (DES,3DES,AES)	•	
SHA-1 /MD5 authentication	•	
PPTP,L2TP,VPN client pass through	•	
Hub and Spoke VPN support	•	
IKE certificate authentication	•	
IPSec NAT Traversal	•	
Dead peer detection	•	
Interoperability with major VPN vendors	•	
Filtrage de contenus		
URL block	•	
Keyword/Phrase block	•	
URL Exempt List	•	
Content policy profiles	32	
Blocks Java Applet,Cookies,Active X	•	
Email filtering (keyword,blacklist,exempt list)	•	
Détection d'intrusions		
Detection for over 1300 attacks	•	
Prevention for over 30 attacks	•	
Detection and prevention on multiple interfaces	•	
Customizable detection signature list	•	
Journaux de trace et supervision		
Internal logging/removable HD	20G (optional)	
Log to remote Syslog/WELF server	•	
Graphical real-time and historical monitoring	•	
SNMP	•	
Email notification of viruses and attacks	•	
VPN tunnel monitor	•	
Anti-Spam		
Real-time Blacklist/Open Relay Database Server	•	
MIME header check	•	
Keyword/phrase filtering	•	
IP address blacklist/exempt list	•	
Haute disponibilité		
Active-active HA	•	
Active-passive HA	•	
Stateful failover (FW and VPN)	•	
Device failure detection ¬ification	•	
Link status monitor	•	
Réseau		
Multiple WAN link support	•	
PPPoE client	•	
DHCP client/server	•	
Policy-based routing	•	
Interfaces d'administration		
Console interface	•	
WebUI (HTTPS)	•	
Command line interface	•	
Secure Command Shell (SSH)	•	
FortiManager System	•	
Administration		
Multiple administrators and user levels	•	
Upgrades &changes via TFTP &WebUI	•	
System software rollback	•	
Trusted host enforcement (IP/mac binding)	•	
Authentification des utilisateurs		
Internal database	•	
LDAP support	•	
RADIUS (external)database	•	
Xauth over RADIUS support for IPSec VPN	•	
IP/MAC address binding	•	
Gestion du trafic		
DiffServ setting	•	
Guarantee bandwidth	•	
Maximum bandwidth	•	
Priority assignment	•	
Dimensions		
Height x Width x Length (inches)		1,75x17x12,6
Weight		5,4 kg
Alimentation		
AC input voltage		100 to 240VAC
AC input current		1,6A
Frequency		50 to 60Hz
Power Dissipation		50W max
Environnement de fonctionnement		
Operating Temperature		0 to 40 °C
Storage Temperature		-25 to 70 °C
Humidity, non-condensing		5 to 95%
Conformité / certification		
FCC Class A Part 15, CE, UL, CUL, VCCI, C-Tick, CB		•
ICSA Antivirus, Firewall, IPSec,NIDS		•

*AV Performance for HTTP, FTP, POP3, IMAP, and SMTP traffic only