

## ↳ ÉDITO

DCI est depuis longtemps reconnu comme un des leaders dans la prescription de solutions de sécurisation du système d'information. Aujourd'hui, DCI est reconnu **meilleur revendeur européen 2004** par le leader des solutions appliances sécurité multifonctions, Fortinet.

Ce statut lui a été décerné tant pour son volume de vente que pour ses capacités d'intégration et de suivi des technologies du constructeur.

Ainsi, DCI dispose aujourd'hui de la plus grande base installée de solutions Fortinet. Ceci lui confère une expertise sans comparaison sur les spécificités de déploiement de ces solutions. En effet, DCI dispose d'un recul pertinent sur les problématiques d'intégration et les différents bugs référencés ou non qui peuvent en découler.

Formées directement par le centre de support et de formation du constructeur à Sophia Antipolis, les équipes de DCI sont certifiées au plus haut niveau (GOLD) auprès de Fortinet. Ce niveau de certifications permet à DCI de disposer d'un accès privilégié aux différentes bases d'informations et d'incidents du constructeur. En outre, DCI dispose d'un interlocuteur spécifiquement dédié par le constructeur pour assurer le support au plus haut niveau.

Loïc GUILLEMOT  
RESPONSABLE SÉCURITÉ & SYSTÈMES  
DCI

# SÉCURITÉ & INNOVATION AVEC DCI :

## répondez dès aujourd'hui aux problématiques de demain

↳ <b>À LA DÉCOUVERTE DE FORTINET</b>	
Qui est Fortinet ? Son marché, ses solutions.....	2
↳ <b>DES SOLUTIONS ADAPTATIVES</b>	
La gamme, les technologies, les performances.....	2
↳ <b>DES AVANTAGES SIGNIFICATIFS</b>	
Les nouveautés, le FortiLog™, le FortiManager™, le FortiProtect™.....	3
↳ <b>INNOVATION</b>	
DCI sécurise la VoIP multisite.....	4
↳ <b>NETWORK INSTRUMENTS OBSERVER</b>	
La réponse à tous vos problèmes de performance réseau.....	4

**FORTINET**  
REAL TIME NETWORK PROTECTION

**NETWORK  
INSTRUMENTS**

# FORTINET™

REAL TIME NETWORK PROTECTION



**FACE AU DÉVELOPPEMENT  
FIREWALL - VPN  
DES RISQUES,  
IDS/IPS  
IL EST IMPÉRATIF  
ANTIVIRUS  
D'ARRÊTER TOUTES  
FILTRAGE DE CONTENU  
LES MENACES  
QOS  
EN TEMPS RÉEL  
VIRTUALISATION  
DÈS L'ENTRÉE  
DE DOMAINES  
DU RÉSEAU.  
ANTISPAM**

## → QUI EST FORTINET ?

Fondée en 2000 par Ken Xie (fondateur de Netscreen), Fortinet est aujourd'hui reconnu comme le leader du marché des appliances de sécurité multifonctions (Unified threat Management). Basés sur la technologie ASIC et un OS propriétaire, les pare-feux antivirus FortiGate de Fortinet constituent la nouvelle génération de systèmes de protection réseau en temps réel. Les systèmes FortiGate sont les seuls produits de sécurité à avoir reçu la quadruple certification de l'ISCA (antivirus, pare-feu, IPSec, NIDS), et fournissent une gamme complète de services réseau et applications sur des plates-formes intégrées et simples à administrer.

## → LA GAMME

Pour répondre de façon pertinente aux besoins des petites agences comme aux exigences des grands comptes ou opérateurs, Fortinet articule son offre autour d'une large gamme d'appliances sécurité multifonctions.

L'ensemble des boîtiers Fortinet, du plus petit modèle - FortiGate 50A - au sommet de la gamme - FortiGate 5000 - dispose des fonctionnalités de Firewall, VPN, IDS-IPS, Antivirus, filtrage de contenu, gestion de la qualité de service ou encore de virtualisation de système.

Ils diffèrent par leur capacité de traitement ou encore par des fonctionnalités spécifiques telles que la haute disponibilité, le traitement gigabit Ethernet ou la redondance des alimentations.

## → LES BESOINS

### Des solutions multifonctions

Pour répondre à la diversification des menaces, il est nécessaire de disposer de solutions intégrant différentes fonctionnalités.

### Des performances adaptées

Le traitement de l'information nécessite des solutions de plus en plus puissantes capables de gérer en temps réel la sécurité des flux et données.

### La simplicité d'administration

Gérer de façon simple et centrale l'ensemble de la politique de sécurité est stratégique.

### La réduction des coûts

Fortinet permet de réduire les coûts en fondant sa politique tarifaire non pas sur le nombre d'utilisateurs mais sur la capacité de traitement de ses boîtiers.

## → LES PERFORMANCES



FGT 100A



FGT 200A



FGT 300A



FGT 400A



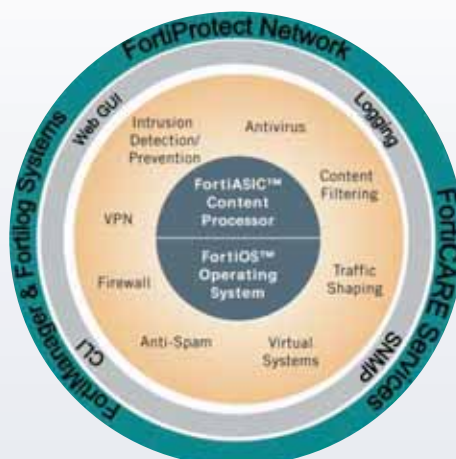
FGT 500A



PRODUITS	NBRE DE PORTS 10/100	NBRE DE PORTS GIGA	FW	TUNNELS VPN	RÈGLES	SESSIONS SIMULTANÉES
FGT-50A	2	-	50	20	200	25 000
FGT-60	7	-	70	40	500	50 000
FGT-60 Wifi	7	-	70	40	500	50 000
FGT-100	3	-	95	80	1 000	200 000
FGT-100A	8	-	100	80		
FGT-200	3	-	120	200	2 000	400 000
FGT-200A	8	-	150	200		
FGT-300	3	-	200	1 500	5 000	400 000
FGT-300A	4	2 C	400	1 500		
FGT-400	4	-	280	1 500	5 000	400 000
FGT-400A	4	2 C	450	1 500		
FGT-500	12	-	280	3 000	8 000	400 000
FGT-500A	8	2 C	500	3 000		
FGT-800	4	4 C	600	3 000	20 000	400 000
FGT-1000	4	2 C	1 000	5 000	30 000	600 000
FGT-3000	3	1 C / 2 F	2 250	5 000	50 000	975 000
FGT-3600	1	2 C / 4 F	4 000	5 000	50 000	1 000 000
FGT-4000	-	4 ou 20	20 000	5 000	500 000	1 000 000
FGT-5001	-	4 / 4 SFP	4 000	5 000	50 000	1 000 000
FGT-5020	-	8 / 8 SFP	8 000	5 000	100 000	2 000 000
FGT-5050	-	20 / 20 SFP	20 000	5 000	250 000	5 000 000
FGT-5140	-	56 / 56 SFP	56 000	5 000	700 000	14 000 000

C - cuivre / F - Fibre Mbps

**INNOVER  
POUR S'ADAPTER  
AUX BESOINS DE  
CHAQUE ENTREPRISE  
ET SIMPLIFIER  
LA GESTION  
DE SA SÉCURITÉ.**



➤ **LES NOUVEAUTÉS**

**Nouveaux boîtiers, nouveau système d'exploitation, nouvelles fonctionnalités, Fortinet élargit sa gamme afin d'améliorer encore ses réponses aux besoins du marché.**

**FORTINET SERIE A :**

La nouvelle gamme série A double les performances de la plupart des boîtiers pour permettre le support des besoins en bande passante Internet notamment dans le cadre de la mise en place de la VoIP, du téléchargement d'application Web qui nécessitent un traitement de la sécurité en temps réel. Elle augmente également le nombre d'interfaces pour rendre les options de configurations plus évolutives au niveau des DMZ et connexions WAN, y compris au niveau Gigabit Ethernet.

L'ensemble de la gamme séries A est disponible avec le FortiASIC™ pour le traitement Gigabit mais aussi le FortiOS™ 3.0. Ce dernier permet l'accès à de nouvelles fonctionnalités telles que le clustering A-A ou A-P, le support des vlan 802.1q, l'IPS, l'antispam, RIP V1 et V2, OSPF, policy routing, FortiGuard, blocage des grayware, VPN SSL.

**FORTIMAIL SECURE MESSAGING PLATFORM**

La plateforme FortiMail Secure Messaging est un système dédié. Elle est basée sur le FortiOS et intègre un moteur de détection de virus pour la protection antivirale contre les spyware, mais aussi le scan complet des emails.

La plateforme FortiMail Secure Messaging utilise des méthodes avancées de détection et de filtrage de spam tels que :

- FortiGuard AntiSpam Service
- Filtrage des règles d'accès,
- Filtrage de contenu,
- Filtrage global ou par utilisateur grâce à des listes noires et blanches,
- Vérification en temps réel de la présence du domaine émetteur dans une base de spameurs (Real Time Blackhole List - RBL)
- Filtrage heuristique

- Filtrage Bayésien qui repose sur un moteur statistique et permet à l'utilisateur de configurer ses propres profils de spameurs afin de procéder à un filtrage personnalisé.

La plateforme FortiMail Secure Messaging propose 3 types de modes de protection :

- Mode Transparent
- Mode Passerelle
- Mode Serveur

Le FortiMail 400 est architecturé pour répondre aux attentes des PME, des grands comptes et des sites distants en terme de sécurisation de la messagerie.

**FORTIGUARD ANTISPAM SERVICE**

FortiGuard Antispam est le nouveau service antispam entièrement managé aidant les entreprises de toutes tailles à réduire la quantité de spam en les éliminant du périmètre réseau.

Le service FortiGuard Antispam réduit de façon significative la quantité de messages non souhaités et possiblement malicieux transitant sur les serveurs emails des entreprises.

En utilisant une technologie en deux phases ce service de Fortinet vérifie en profondeur chaque message email pour rechercher les contenus reconnus comme spam tels que les liens URL. Le service FortiGuard Antispam est présent à la fois dans les solutions FortiMail et FortiGate.

Le service FortiGuard Antispam est entièrement géré par l'équipe Fortinet Global Response qui le met à jour en temps réel afin de toujours vous offrir le meilleur niveau de protection. Cette solution peut être déployée sur n'importe quel antivirus Firewall FortiGate ou plateforme FortiMail Secure Messaging.

➤ **Le FortiLog™**

L'appliance de gestion de logs FortiLog permet à l'administrateur du système d'information d'adresser rapidement les problématiques de vulnérabilité réseau en agrégeant et en analysant les informations émanant des boîtiers FortiGate. Minimisant les efforts requis pour la supervision et le maintien optimal du niveau de sécurité, le FortiGate prend notamment en charge la gestion des logs relatives au trafic, aux événements, virus, attaques ou encore contenu et données filtrés. Au delà des fonctions de collecte et corrélation des logs, FortiLog constitue une véritable interface graphique de gestion des logs et fournit un ensemble de rapports entièrement paramétrables. La solution fournit ainsi une vision pertinente des usages réseau et du niveau de sécurité de ce dernier.

➤ **Le FortiManager™**

Le FortiManager est un outil intégré de management et de supervision qui permet à son utilisateur de gérer simplement un grand nombre de boîtiers FortiGate locaux ou distants. Il minimise les efforts nécessaires au déploiement, à la configuration, à la supervision et au maintien à jour d'une large gamme de services de protection dispensés par les appliances de la marque. Toutes les fonctionnalités des FortiGate peuvent être visualisées, paramétrées et gérées en temps réel à partir d'une interface de commande en ligne (sécurisé SSH) ou d'une interface graphique de type web (sécurisée SSL). Le FortiManager autorise également la configuration des boîtiers en ou hors ligne, l'import, l'export ou encore la visualisation des configurations.

➤ **Le FortiProtect™**

Avec le FortiProtect Premier, Fortinet propose à l'utilisateur un service rapide et de haut niveau pour :

- La mise à jour de nouvelles signatures virales sous 3 heures 24h/7j sur demande client,
- La gestion d'alertes sur une possible manifestation virale,
- Le conseil expert pour réduire les manifestations de virus,
- La détection de virus prioritaire via le service de support rattaché,
- La mise en place de rapports d'activité virale mensuels. Ce service, accessible via un portail web, permet une mise à jour des signatures de virus et d'attaques des FortiGate en moins de 5 minutes et assure aux utilisateurs de FortiGate la plus récente protection antivirale et IDS disponible.

