FICHE PRODUIT

FortiGate®/FortiWiFi™-60C

Appliances de sécurité pour les sites et bureaux distants d'entreprise

La protection des bureaux et points de vente distants, et des équipements sur site client

Les appliances consolidées de la gamme FortiGate/FortiWiFi-60C offrent une sécurité exhaustive et de qualité professionnelle pour les petits sites, les bureaux et agences distantes, les équipements sur site client et les points de vente. Un seul équipement apporte toutes les technologies de sécurité essentielles pour protéger les applications et les données. Une tarification simple par équipement, une console d'administration intégrée et une gestion à distance sont autant de leviers pour maîtriser vos investissements et charges d'exploitation.

Protection intégrale, avec la convivialité du sans-fil en option

Les appliances de sécurité FortiGate intègrent un pare-feu, des VPN sur IPSec ou SSL, un antivirus, un antispam, une prévention des intrusions et un filtrage Web au sein d'un seul équipement et à un tarif unique. Ces appliances assurent également la prévention des fuites de données, le contrôle applicatif, l'inspection du trafic SSL, le contrôle d'accès des postes utilisateurs et la gestion des vulnérabilités. De plus, les FortiGuard Labs de Fortinet, actifs en permanence à l'échelle mondiale, surveillent toute nouvelle menace et assurent en temps réel des mises à jour qui protégeront votre réseau contre ces menaces émergentes.

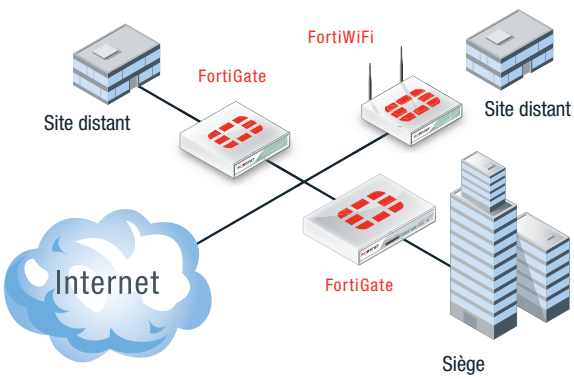
Les appliances FortiWiFi-60C/CM associent la protection et les performances requises avec la convivialité du sans-fil. La solution est compatible aux réseaux 802.11 a/b/g/n et prend ainsi en charge votre infrastructure existante. Plusieurs identifiants SSID vous permettent de déployer différents réseaux sans fil, pour, par exemple, offrir un accès invité à Internet uniquement, sans passerelle vers le réseau corporate.

Des performances et une fiabilité à la hauteur de vos ambitions

Les solutions matérielles et logicielles de Fortinet évitent que votre sécurité réseau ne devienne complexe. Les processeurs FortiASIC optimisent les performances tout en neutralisant les accès prohibés et en jugulant le trafic indésirable sur votre réseau. FortiOS, système d'exploitation dédié, accélère le traitement de vos données et assure l'application des règles de sécurité.

FortiGate/FortiWifi-60C en 8 avantages

- Protection intégrale contre les menaces qui ciblent le réseau, les contenus et les applications
- Segmentation et sécurité du trafic au sein du périmètre corporate
- Un pare-feu Gigabit grâce aux processeurs FS1 SoC de Fortinet
- Des ports internes en GbE et des interfaces WAN dédiées
- Stockage en local des logs et des tableaux de bord graphiques
- Optimisation WAN et mise en cache Web pour doper les performances réseau
- Slot ExpressCard et Wi-Fi haut-débit par USB pour déployer rapidement des réseaux sécurisés
- FortiExplorer, un assistant pour simplifier les opérations d'installation et de configuration



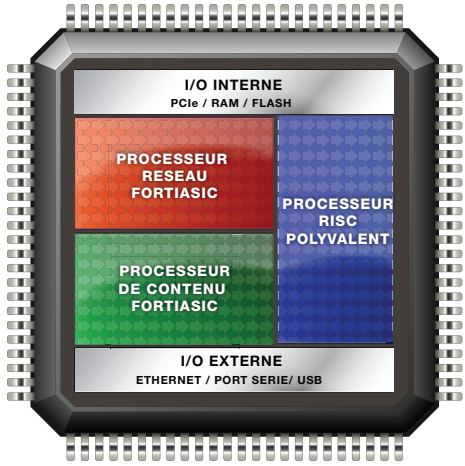
FORTIGATE ET FORTIWIFI AU SEIN DES ENTREPRISES MULTISITES

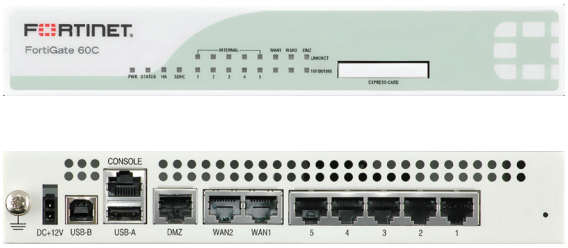
Labels de certification

Fortinet FS1 System-on-a-Chip

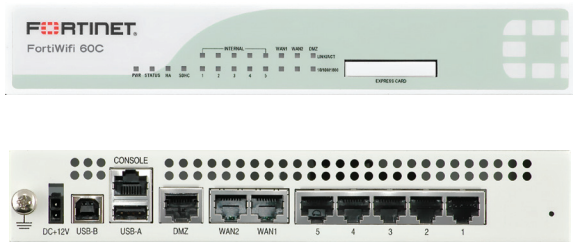
Les appliances FortiGate/FortiWiFi-60C constituent la nouvelle génération d'appliance de sécurité réseau de Fortinet. Elles sont équipées du tout premier Fortinet System-on-a-chip (SoC), le FS1. Le FS1 SoC associe une accélération FortiASIC, un processeur principal RISC et d'autres composants systèmes pour simplifier la conception de l'appliance et optimiser les performances des réseaux de petite envergure.

Le FS1 et les appliances FortiGate/FortiWiFi-60C permettent aux entreprises multisites d'activer une sécurité intégrée et multicouche sur l'ensemble de leur réseau, sans peser sur les performances.





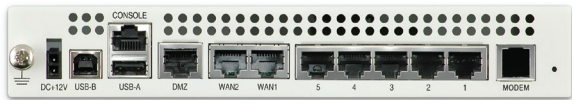
FortiGate-60C



FortiWiFi-60C

(Antennes Wi-Fi non représentées)

FortiWiFi-60C



FortiWiFi-60CM

(Antennes Wi-Fi non représentées)

FortiGuard® Security Subscription Services met à jour les produits Fortinet en temps réel. Les mises à jour créées par les chercheurs en sécurité de Fortinet assurent une protection à jour contre les menaces. Ces mises à jour portent sur les antivirus, la prévention d'intrusion, le filtrage Web, l'antispam, la gestion des vulnérabilités et de la conformité, le contrôle applicatif et la sécurité des bases de données.

FortiCare™ Support Services offre un support mondial sur tous les services et des produits Fortinet. FortiCare assure ainsi que vos produits restent optimisés. Ce support est disponible en mode 8h/5j avec un remplacement après reception du matériel défectueux, ou en 24h/7j, avec remplacement en avance. Sont disponibles en option : le Support Premium, le Premium RMA et les Services professionnels. La garantie matérielle est de 1 an et la garantie logicielle est de 90 jours.

FortiGuard Subscription Services						
Produit	**Antivirus**	**Prévention des Intrusions**	**Filtrage Web**	**Antispam**	**Contrôle applicatif**	**Gestion des vulnérabilités**
FortiGate-60C	Disponible	Disponible	Disponible	Disponible	Disponible	Disponible
FortiWiFi-60C	Disponible	Disponible	Disponible	Disponible	Disponible	Disponible
FortiWiFi-60CM	Disponible	Disponible	Disponible	Disponible	Disponible	Disponible

FortiOS 4.0, le nouvelle référence

FortiOS 4.0 : revisiter la sécurité réseau

FortiOS 4.0 est le socle logiciel des plates-formes de sécurité FortiGate. Dédié à la sécurité, aux performances et à la fiabilité, le système d'exploitation FortiOS 4.0 capitalise sur la puissance des composants matériels FortiASIC.

L'atout FortiASIC

Les FortiASIC sont des processeurs hautes-performances qui tirent avantage de moteurs d'analyse propriétaires et intelligents pour accélérer les services de sécurité.

Services de sécurité FortiOS

PARE-FEU
- Certification ICSA Labs (pare-feu d'entreprise)
- Translation NAT, PAT, Transparent (pont)
- Protocole de routage (RIP, OSPF, BGP, Multicast)
- Translation d'adresses NAT à base de règles
- Domaines virtuels (NAT/Mode Transparent)
- Tagging VLAN (802.1Q)
- Authentification et ordonnancement par groupe
- SIP/H.323 /SCCP NAT Traversal
- Prise en charge de WINS
- Proxy explicite (Citrix/TS etc.)
- Sécurité de la VoIP (pare-feu SIP/Pinholing RTP)
- Règles granulaires de sécurité
- Règles fondées sur le profil ou l'application
- Gestion des vulnérabilités
- IPv6 (NAT/NAT-T)

RÉSEAU PRIVÉ VIRTUEL (VPN)
- Certification ICSA Labs (IPSec)
- Tunnels PPTP, IPSec et SSL
- Concentrateur SSL-VPN (compatible à iPhone)
- Chiffrement DES, 3DES et AES
- Authentification SHA-1/MD5
- PPTP, L2TP, VPN Pass Through
- VPN Hub and Spoke
- Authentification par certificat IKE (v1 & v2)
- IPSec NAT-T
- Configuration IPSec automatique
- Détection des Dead Peers
- Authentification par RSA SecurID
- Favoris Single Sign-On sur SSL
- Authentification SSL à deux facteurs
- Authentification par groupe LDAP (SSL)

RÉSEAU/ROUTAGE
- Multiples liens WAN
- DHCP Client/Serveur
- Routage à base de règles
- Routage dynamique pour IPv4 et IPv6 (RIP, OSPF, BGP & Multicast pour IPv4)
- Zones multiples
- Routage entre zones
- Routage entre VLAN (domaines virtuels)
- Agrégation de liens multiples (802.3 ad)
- IPv6 (Pare-feu, DNS, mode Transparent, SIP, routage dynamique, accès admin, administration)
- Contrôle des VRRP et liens défaillants
- Client sFlow

AUTHENTIFICATION UTILISATEUR
- Base de données en local
- Intégration avec Active Directory (AD)
- Authentification RADIUS/LDAP externe
- Xauth sur RADIUS pour VPN IPSec
- Authentification par RSA SecurID
- Authentification par groupe LDAP

OPTIMISATION DU DATA CENTER
- Mise en cache des serveurs Web
- Multiplexage TCP
- Offloading HTTPS
- Prise en charge du protocole WCCP

ANTIVIRUS / ANTISPYWARE
- Certification ICSA Labs (passerelle antivirus)
- Antispyware et prévention des vers sur :

HTTP/HTTPS	SMTP/SMTPS
POP3/POP3S	IMAP/IMAPS
FTP	Messagerie Instantanée

- Analyse des flux par l'antivirus
- Push automatique des mises à jour
- Mise en quarantaine de fichiers
- Bases de données : Standard, Extended, Extreme, Flow
- IPv6

FILTRAGE WEB
- 76 catégories uniques
- Le service de filtrage Web FortiGuard catégorise plus de 2 milliards de pages Web
- Filtrage HTTP/HTTPS
- Neutralisation sur base d'URL ou de mot-clé
- Liste d'exclusion d'URL
- Profils de contenus
- Neutralise les applets Java, Cookies, Active X
- Filtrage des en-têtes MIME
- Prise en charge d'IPv6

CONTROL APPLICATIF
- Identification et contrôle de plus de 1 400 applications
- Contrôle des outils de messagerie et P2P, quel que soit le port ou le protocole utilisé :

AOL-IM	Yahoo	MSN	KaZaa
ICQ	Gnutella	BitTorrent	MySpace
WinNY	Skype	eDonkey	Facebook

HAUTE DISPONIBILITÉ
- Actif-Actif, Actif-Passif
- Fonction de failover (pare-feu et VPN)
- Détection et notification des défaillances matérielles
- Surveillance du statut du lien
- Fonction de failover du lien
- Répartition des charges serveur

OPTIMISATION WAN
- Bidirectionnel / Passerelle à client à passerelle
- Cache intégré et optimisation du caching
- Accélération des flux CIFS/FTP/MAPI/HTTP/HTTPS/ TCP générique

DOMAINES VIRTUELS (VDOM)
- Domaines pare-feu/routage distincts
- Domaines d'administration distincts
- Interfaces VLAN distinctes
- Licence pour 10 VDOM en standard, avec expansion possible

CONTRÔLEUR WI-FI
- Gestion unifiée du Wi-Fi et des points d'accès
- Activation automatique des points d'accès
- Détection et neutralisation des points d'accès indésirables
- Points d'accès virtuels avec SSID différents
- Multiple méthodes d'authentification

TRAFFIC SHAPING
- Traffic shaping (lissage) à base de règles
- Traffic shaping selon l'application ou l'IP
- Prise en charge de DiffServ
- Bande passante : garantie, seuil max., prioritisation
- Shaping selon des classes et des quotas de trafic

PRÉVENTION D'INTRUSION
- Certification ICSA Labs (NIPS)
- Protection contre plus de 3 000 menaces
- Gestion des anomalies de protocole
- Signatures personnalisables
- Mise à jour automatique des bases d'attaques
- IPv6

PRÉVENTION DES FUITES DE DONNÉES
- Identification et monitoring des données confidentielles en transit
- Base de données de modèles
- Moteur d'expressions régulières pour personnaliser les filtres
- Actions configurables (neutralisation/mise en log)
- Surveillance de la messagerie instantanée, des flux HTTP/HTTPS, et autres
- Prise en charge des types de fichiers courants
- Prise en charge des caractères internationaux

ANTISPAM
- Compatible SMTP/SMTPS, POP3/POP3S, IMAP/ IMAPS
- Liste noire temps-réel/serveur Open Relay Database
- Vérification des en-têtes MIME
- Filtrage selon des mots clés et phrases
- Liste noire d'adresses IP et liste d'exceptions
- Mises à jour automatiques et temps-réel assurées par FortiGuard

CONFORMITÉ ET CONTRÔLE DES ENDPOINTS
- Monitoring & contrôle des hôtes qui exécutent la sécurité endpoint FortiClient

ADMINISTRATION
- Console (RS-232)
- Interface Web (HTTP/HTTPS)
- Telnet / Secure Command Shell (SSH)
- Interface de lignes de commande
- Administration selon le profil
- Multilingue : anglais, japonais, coréen, espagnol, chinois, français
- Différents niveaux administrateur et utilisateur
- Mises à jour via TFTP et l'interface Web
- Fonction rollback du logiciel système
- Règles configurables de mot de passe
- Administration centralisée avec FortiManager (en option)

LOGS/MONITORING/VULNÉRABILITÉS
- Log d'événements en local
- Log vers un serveur Syslog/WELF distant
- Tableau de bord en temps réel ou historique
- Compatible SNMP
- Notification par email des virus et attaques
- Monitoring des tunnels VPN
- Logs et reporting par FortiAnalyzer (en option)
- Services d'analyses et d'administration FortiGuard (en option)

Note : cette liste est exhaustive et susceptible de présenter des fonctionnalités de FortiOS non disponibles sur l'ensemble des FortiGate/FortiWiFi. Consultez les documents FortiGate/FortiWiFi pour connaître les fonctionnalités de votre appliance.

Pare-feu

Le pare-feu de Fortinet assure une protection intégrale du réseau et des contenus grâce à une inspection stateful des paquets associée à de nombreuses fonctionnalités de sécurité. Toutes les menaces, les plus récentes comme les plus complexes, sont neutralisées par les fonctionnalités de contrôle applicatif, d'antivirus, de prévention des intrusions, de filtrage Web et de VPN sécurisé. Le système d'exploitation FortiOS s'adosse à des processeurs FortiASIC dédiés pour accélérer les tâches d'inspection et identifier tout logiciel malveillant.

Fonctionnalités
NAT, PAT et Transparent (pont)
Translation d'adresses NAT à base de règles
SIP/H.323/SCCP NAT-T
Tagging VLAN (802.1Q)
Gestion des vulnérabilités
Prise en charge d'IPv6

Débit du pare-feu	
Paquets de 1518 octets	1 Gbps
Paquets de 512 octets	1 Gbps
Paquets de 64 octets	1 Gbps

Prévention des intrusions

Cette technologie neutralise les menaces émergentes. Elle détecte ces menaces compte tenu de leur signature, mais également selon certaines anomalies qui alertent les utilisateurs lorsqu'un flux de trafic correspond à un comportement d'attaque. Les équipes de recherche et de veille de Fortinet analysent tous les comportements suspects, pour identifier et classifier les menaces émergentes, et générer de nouvelles signatures qui seront intégrées dans les mises à jour du service FortiGuard.

Fonctionnalités
Mise à jour automatique des bases de données
Prise en charge des anomalies de protocole
Prévention des intrusions et des attaques de déni de service
Signature personnalisable
Prise en charge d'IPv6

Débit prévention d'intrusion	
IPS (UDP)	60 Mbps
IPS (HTTP)	50 Mbps

Antivirus / Antispyware

Cette technologie antivirale d'inspection des contenus est un rempart contre les virus, spyware, vers et autres malware susceptibles d'infecter les réseaux et postes clients. En interceptant et en analysant le trafic et les contenus applicatifs, l'antivirus identifie toute les menaces, notamment celles qui sont furtives car cachées au cœur d'applications, et les neutralise avant tout dommage. Parallèlement, l'offre FortiGuard subscription services apporte aux FortiGate les mises à jour des signatures virales qui garantissent leur efficacité sur le long terme.

Fonctionnalités
Mise à jour automatique des bases de données
Proxy antivirus
Inspection antivirale des flux
Mise en quarantaine des fichiers
Prise en charge d'IPv6

Performances	
Débit de l'antivirus	20 Mbps

Réseaux privés virtuels (VPN)

La technologie VPN de Fortinet sécurise les communications vers les réseaux et les hôtes, grâce des réseaux privés virtuels (VPN) sous SSL ou IPSec. Ces VPN tirent avantage de l'accélération matérielle qu'offrent nos processeurs FortiASIC pour assurer les phases de chiffrement et déchiffrement des données. Le VPN FortiGate effectue une inspection exhaustive des contenus et les fonctions intégrées d'antivirus, de prévention d'intrusion et de filtrage Web neutralisent les menaces de sécurité. L'optimisation du trafic est possible grâce à la prioritisation des flux acheminés via les tunnels VPN.

Fonctionnalités
VPN sous IPSec et SSL
Authentification DES, 3DES, AES et SHA-1/MD5
PPTP, L2TP, VPN Client Pass Through
Favoris Single Sign-On sur SSL
Authentification à deux facteurs SSL

Performances	
Débit VPN sur IPSec	70 Mbps
Débit VPN sur SSL	15 Mbps
Nombre max. d'utilisateurs simultané de VPN SSL	550
Nombre de tunnels VPN IPSec client à passerelle	800

Optimisation WAN

L'optimisation des réseaux WAN accélère les flux applicatifs sur des réseaux multisites, tout en sécurisant ce trafic. L'optimisation WAN élimine le trafic indésirable ou malveillant, accélère le trafic légitime et allège les besoins en bande passante requis pour acheminer les données entre les applications et les serveurs. L'amélioration des performances applicatives et la fourniture des services réseau permettent de maîtriser les besoins en infrastructure et en bande passante, et donc les coûts associés.

Fonctionnalités
Optimisation de passerelle à passerelle
Optimisation bi-directionnelle, passerelle à client
Cache Web
Tunnels sécurisés
Mode Transparent

Inspection du trafic SSL

L'inspection du trafic SSL protège les postes clients et les serveurs Web et applicatifs contre les menaces furtives. Cette inspection intercepte et analyse le trafic chiffré afin d'identifier les menaces avant routage vers la destination finale. L'inspection s'applique au trafic SSL des postes clients, lorsqu'un utilisateur se connecte à son outil CRM déployé en mode Cloud par exemple, ainsi qu'au trafic entrant (Web et serveur). L'inspection SSL permet d'appliquer des règles d'utilisation sur le contenu Web malveillant sous SSL et de protéger les serveurs contre les menaces dissimulées au sein de flux chiffrés.

Fonctionnalités
Protocoles pris en charge: HTTPS, SMTPS, POP3S, IMAPS
Inspection : antivirus, filtrage Web, antispam, prévention des pertes/fuites de données

Contrôle d'accès des postes clients

Ce contrôle d'accès s'applique aux utilisateurs qui se connectent à un réseau d'entreprise. Ce service vérifie que FortiClient Endpoint Security est correctement installé, que le pare-feu est activé et que les signatures antivirales sont à jour, avant d'octroyer l'accès au réseau. Les postes non conformes, hébergeant notamment des applications en violation des règles de sécurité, sont mis en quarantaine ou orientés vers des services de restauration.

Fonctionnalités
Monitoring et contrôle des hôtes qui utilisent FortiClient
Analyse des vulnérabilités sur les nœuds du réseau
Portail de mise en quarantaine
Détection et contrôle des applications
Base intégrée d'applications

Prévention des pertes de données

Cet outil de prévention utilise un moteur d'analyse de type pattern-matching pour identifier et prévenir tout transfert de données confidentielles hors du périmètre réseau, même si ces données sont chiffrées. Cette approche sécurise vos données confidentielles et propose un log d'audit qui vérifie votre conformité. Vous pouvez choisir d'enregistrer, de neutraliser ou d'archiver les données, mais aussi de mettre en quarantaine, voire de bannir certains utilisateurs.

Fonctionnalités
Identification et contrôle sur les données en transit
Base de comportements intégrée
Moteur de correspondance basé sur des expressions régulières
Inspection des fichiers dans des formats courants
Prise en charge des jeux de caractères internationaux
Prévention des pertes de données basées sur les flux

Filtrage Web

Le filtrage Web protège les postes clients, les réseaux et les données confidentielles contre les attaques Web, en empêchant l'accès utilisateur à des sites de phishing et autres sources de malware. De plus, les administrateurs peuvent appliquer des règles sur certaines catégories de sites Web pour prévenir tout accès à un contenu inapproprié, un contenu qui alourdirait la charge de trafic sur le réseau.

Fonctionnalités
Filtrage des flux HTTP/HTTPS
Filtrage selon des URL, mots-clés et phrases
Applets Java, Cookies et Active X neutralisés
Filtrage des en-têtes de contenu MIME
Filtrage Web sur les flux
Prise en charge d'IPv6

Logs, reporting et monitoring

Les appliances de sécurité FortiGate assurent la mise en logs des fonctions de protection du trafic, des systèmes et du réseau, avec la possibilité d'affiner les informations de logs ou d'en obtenir des représentations graphiques. Le reporting, historique ou ou temps-réel, sur l'activité réseau permet d'identifier les problématiques de sécurité et de proscrire tout abus ou mauvaise utilisation du réseau.

Fonctionnalités
Logs internes et génération de rapports
Monitoring graphique en temps réel ou historique
Production de rapports graphiques
Tableaux graphiques ciblés
En option, logs par FortiAnalyzer (notamment par domaine virtuel)
En option, service FortiGuard d'analyse et de gestion

Haute Disponibilité

Les configurations haute disponibilité (HA - High Availability) améliorent la fiabilité et les performances en regroupant plusieurs appliances FortiGate au sein d'un cluster. La haute disponibilité de FortiGate s'effectue en modes actif-actif et actif-passif pour offrir une souplesse d'utilisation de chaque entité d'un cluster HA. Cette haute disponibilité est assurée par le système d'exploitation FortiOS et est offerte par la majorité des appliances FortiGate.

Fonctionnalités

- Actif-Actif et Actif-Passif
- Failover stateful (pare-feu et VPN)
- Monitoring du statut des liens et failover
- Détection et notification des dysfonctionnements
- Répartition des charges serveur

Contrôle applicatif

Le contrôle applicatif consiste à définir et à appliquer des règles pour les milliers d'applications actives sur votre réseau, quel que soit le port ou le protocole de communication utilisé. La prolifération des applications Internet et Web 2.0 sur les réseaux corporate rend le contrôle applicatif impératif, puisque le trafic applicatif est, pour l'essentiel, considéré comme normal par les pare-feu classiques. Fortinet offre un contrôle précis des applications, ainsi qu'un lissage du trafic et une inspection des flux.

Fonctionnalités

- Identification et contrôle sur plus de 1 400 applications
- Lissage du trafic, par application
- Contrôle des outils de messagerie et P2P, quel que soit le port ou le protocole utilisé :

AOL-IM	Yahoo	MSN	KaZaa
ICQ	Gnutella	BitTorrent	MySpace
WinNY	Skype	eDonkey	Facebook

et autres ...

Domaines virtuels

Avec les domaines virtuels (VDOM), une plate-forme physique FortiGate se démultiplie en plusieurs systèmes virtuels. Chaque domaine dispose de ses propres interfaces virtuelles, table de routage, fonctions d'administration et autres fonctionnalités. Les VDOM sécurisent plusieurs réseaux, grâce à la virtualisation des ressources sur la plateforme FortiGate, avec réduction de la consommation énergétique et gain d'espace à la clé. Une solution idéale pour les grandes entreprises et les fournisseurs de services.

Fonctionnalités

- Domaines distincts pour le pare-feu et le routage
- Domaines d'administration distincts
- Interfaces VLAN distinctes
- VDOM max.: 10
- VDOM par défaut: 10

Options d'installation et de configuration

Fortinet offre aux administrateurs différents assistants et processus pour installer et configurer les appliances FortiGate. De l'interface Web conviviale à l'interface experte en ligne de commande, les systèmes FortiGate offrent la souplesse et la simplicité dont vous avez besoin.

Fonctionnalités

- Assistant d'installation par USB pour FortiExplorer
- Interface utilisateur Web
- Interface en ligne de commande via la connexion série
- Paramètres pré-configurés par USB

Contrôleur sans fil

Toutes les plates-formes de sécurité FortiGate et FortiWiFi™ disposent d'un contrôleur sans fil, assurant une gestion centralisée et sécurisée des points d'accès FortiAP™ et des réseaux sans fil. Le trafic sans fil prohibé est ainsi neutralisé, tandis que les flux légitimes sont sujets à des règles de pare-feu fondées sur l'identité et à une inspection qui identifie toute forme de menace. À partir d'une simple console, vous contrôlez l'accès au réseau, mettez à jour les règles de sécurité et identifiez automatiquement les points d'accès "rogues" (indésirables ou pirates).

Fonctionnalités

- Gestion unifiée du Wi-Fi et des points d'accès
- Activation automatique des points d'accès
- Détection et neutralisation en temps-réel des points d'accès indésirables
- Points d'accès virtualisé avec activation de SSID distincts
- Plusieurs méthodes d'authentification

Spécifications techniques	FortiGate-60C	FortiWiFi-60C	FortiWiFi-60CM
Interfaces			
Nombre d'interfaces réseau	8	8	8
Interfaces internes 10/100/1000 (cuivre, RJ-45)	5	5	5
Interfaces WAN 10/100 (cuivre, RJ-45)	2	2	-
Interfaces DMZ 10/100 (cuivre, RJ-45)	1	1	-
Interfaces WAN 10/100/1000 (cuivre, RJ-45)	-	-	2
Interfaces DMZ 10/100/1000 (cuivre, RJ-45)	-	-	1
Port modem analogique v.90	-	-	1
Interface pour console d'administration (cuivre, RJ-45)	1		
Interfaces USB	2 (1 Type-A, 1 Type-B)		
Slot ExpressCard	1		
Stockage interne	8 Go		
Normes Wi-Fi	-	802.11 a/b/g/n	802.11 a/b/g/n
Performances systèmes			
Performances du pare-feu (paquets UDP, 1518 octets)	1 Gbps		
Performances du pare-feu (paquets UDP, 512 octets)	1 Gbps		
Performances du pare-feu (paquets UDP, 64 octets)	1 Gbps		
Performances VPN sur IPSec	70 Mbps		
Performances VPN sur SSL	15 Mbps		
Performances IPS (paquets UDP, 512 octets)	60 Mbps		
Performances IPS (HTTP)	50 Mbps		
Performances Antivirus* (Proxy)	20 Mbps		
Tunnels VPN IPSec, passerelle à passerelle (système/VDOM)	50 / 50		
Tunnels VPN sur IPSec, client à passerelle	800		
Nombre max. de sessions de pare-feu en simultané	80 000		
Sessions de pare-feu par seconde	3 000		
Nombre max. d'utilisateurs de VPN sur SSL	550		
Règles de pare-feu (système / VDOM)	5 000 / 500		
Domaines virtuels (max. / par défaut)	10 / 10		
Points d'accès sans fil gérés	4		
Nombre d'utilisateurs par licence	Pas de limite		
Dimensions			
Hauteur x Largeur x Longueur	3,66 x 21,59 x 14,76 cm (1,44 x 8,50 x 5,81")		
Poids	0,86 kg (1,9 lb)	0,95 kg (2,1 lb)	0,85 kg (1,89 lb)
Montage sur mur	Non	Oui	Oui
Données environnementales			
Alimentation électrique	100-240 VAC, 50-60 Hz, 1,5 Amp Max		
Puissance énergétique (moyenne)	15,7 W	19 W	11,6 W
Refroidissement	53,6 BTU/h	64,8 BTU/h	47,5 BTU/h
Température d'exploitation	0 à 40° C (32 à 104° F)		
Température de stockage	- 25 à 70 ° C (-13 à 158° F)		
Humidité	20 à 90%, non-condensé		
Conformité			
Certifications industrielles	ICSA Labs: Pare-feu, Antivirus, VPN sur IPSec, VPN sur SSL, Prévention d'intrusion		
Certifications de sécurité	FCC Part 15, UL/CUL, C Tick, CE, VCCI		

*Les performances antivirus sont mesurées sur trafic HTTP avec un fichier de 32 Ko. les performances réelles sont susceptibles de varier en fonction du trafic et de l'environnement réseau.

Référence de commande

Référence produit	Description
FG-60C	2 ports WAN 10/100, 1 ports DMZ 10/100, 5 ports internes 10/100/1000, (2) ports USB, slot ExpressCard, 8Go de stockage interne.
FWF-60C	Wi-Fi (802.11a/b/g/n), 2 ports WAN 10/100, (1) port DMZ 10/100, 5 ports internes 10/100/1000, 2 ports USB, slot ExpressCard, 8Go de stockage interne.
FWF-60CM	Wi-Fi (802.11a/b/g/n), 2 ports WAN 10/100/1000, 1 port DMZ 10/100/1000, 5 ports internes 10/100/1000, 2 ports USB, slot ExpressCard, 8Go de stockage interne, port pour modem analogique.

SIÈGE SOCIAL MONDIAL
Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tél +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

SIÈGE SOCIAL EMEA – FRANCE
Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tél +33.(0)4.89.87.05.10
Fax +33.(0)4.89.87.05.01

SIÈGE SOCIAL APAC – SINGAPOUR
Fortinet Incorporated
300 Beach Road #20-01
The Concourse, Singapore 199555
Tél: +65-6513-3734
Fax: +65-6295-0015

FG-FWF-60C-DAT-R6-201103