FICHE PRODUIT

# Série FortiGate 40F

**SD-WAN sécurisé**
**Firewall nouvelle-génération**


La série FortiGate 40F offre une solution SD-WAN rapide et sécurisée dans un boîtier format bureau, sans ventilateur, pour les succursales et les moyennes entreprises. Ces FortiGate assurent une protection efficace contre les cybermenaces grâce à l'accélération system-on-a-chip et à un SD-WAN sécurisé à la pointe du secteur. Cette solution est simple, abordable et facile à déployer. L'approche réseau Fortinet axée sur la sécurité s'intègre parfaitement à la nouvelle génération de solutions de cybersécurité.

### Sécurité

- Identification de milliers d'applications au sein du trafic réseau, pour une inspection approfondie et une application modulaire des politiques de sécurité
- Protection contre les logiciels malveillants, les exploits et les sites web malveillants, à la fois sur le trafic chiffré et non-chiffré
- Prévention et détection des attaques connues grâce aux renseignements sur les menaces publiées par les services de sécurité de FortiGuard Labs reposant sur l'IA
- Blocage pro-actif des attaques sophistiquées inconnues en temps réel grâce à FortiSandbox, le système de sandboxing de Fortinet Security Fabric reposant sur l'IA

### Performances

- Recours à des processeurs de sécurité (SPU) spécialement conçus par Fortinet pour offrir les meilleures performances du secteur en matière de protection contre les menaces, avec une latence ultra-faible
- Performances et protection de pointe pour le trafic chiffré SSL. Premier firewall à fournir une inspection approfondie TLS 1.3

### Certification

- Efficacité et performances optimales, validées par des experts indépendants
- Certifications inégalées attribuées par NSS Labs, ICSA, Virus Bulletin et AV Comparatives

### Mise en réseau

- Routage adapté aux applications avec SD-WAN intégré pour des performances d'application optimales et une meilleure expérience utilisateur
- Fonctionnalités avancées de routage intégrées pour des performances de pointe, avec des tunnels IPSEC chiffrés à grande échelle

### Gestion

- Interface de gestion intuitive, offrant automatisation et visibilité complète sur le réseau
- Déploiement zero touch, via un unique panneau de contrôle, via le Fabric Management Center
- Checklists prédéfinies permettant de veiller à respecter les réglementations, avec analyse des déploiements et affichage des bonnes pratiques, pour une sécurité renforcée

### Approche Security Fabric

- Permet aux produits Fortinet et des partenaires Fabric-ready d'offrir une plus grande visibilité, une détection intégrée de bout en bout, une mise en commun des renseignements sur les menaces et des mesures correctives automatisées
- Création automatique de visualisations de la topologie réseau, pour identifier les appareils connectés et fournir une visibilité complète sur les produits Fortinet et des partenaires Fabric-ready

| Firewall | IPS | NGFW | Threat Protection | Interfaces |
|---|---|---|---|---|
| **5 Gb/s** | **1 Gb/s** | **800 Mb/s** | **600 Mb/s** | Multiples ports GE RJ45 |

Pour plus de détails, consultez le tableau des spécifications

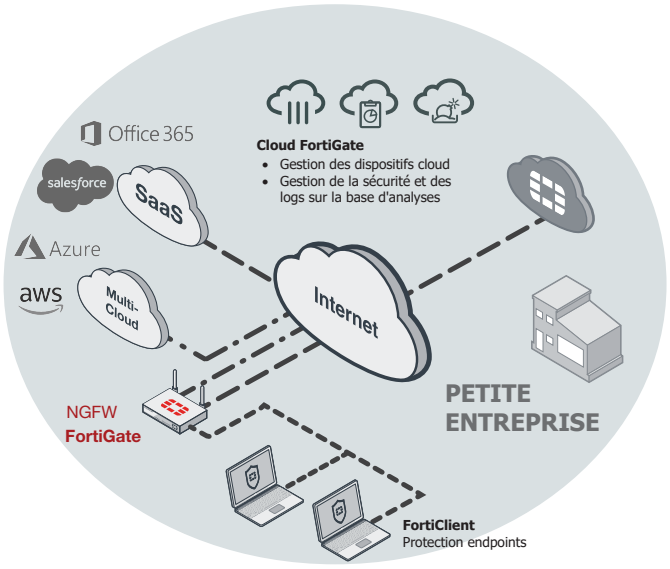
# Déploiement

## Firewall nouvelle-génération (NGFW)

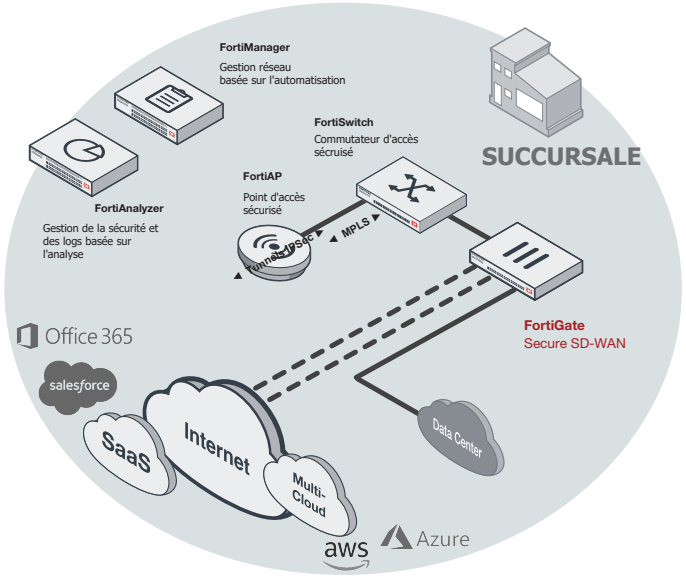
- Simplification des process et retour sur investissement maximisé, grâce à l'intégration des fonctionnalités de protection au sein d'une appliance unique hautes-performances, reposant sur le processeur de sécurité (SPU) Fortinet
- Visibilité totale sur les utilisateurs, les appareils et les applications, à travers toute la surface d'attaque. Application uniforme des politiques de sécurité, indépendamment de la localisation des actifs informatiques
- Protection contre les vulnérabilités réseau exploitables grâce à la sécurité IPS, pour une faible latence et des performances réseau optimisées
- Blocage automatique des menaces ciblant le trafic déchiffré, grâce à l'inspection SSL la plus avancée du secteur (nouvelle norme TLS 1.3 avec chiffrement obligatoire)
- Blocage proactif, en temps réel, des attaques sophistiquées récemment identifiées, grâce aux services FortiGuard Labs reposant sur l'IA et à la protection avancée contre les menaces assurée par Fortinet Security Fabric

## SD-WAN sécurisé

- Performances fiables pour les applications, avec détection précise, pilotage et optimisation dynamiques du cheminement WAN
- Accès multi-cloud pour une adoption plus rapide du SaaS, avec optimisation de bout en bout
- Déploiement zero touch et gestion centralisée avec auto-provisionnement, analyse et reporting
- Un dispositif de sécurité solide avec firewall nouvelle génération et protection contre les menaces en temps réel



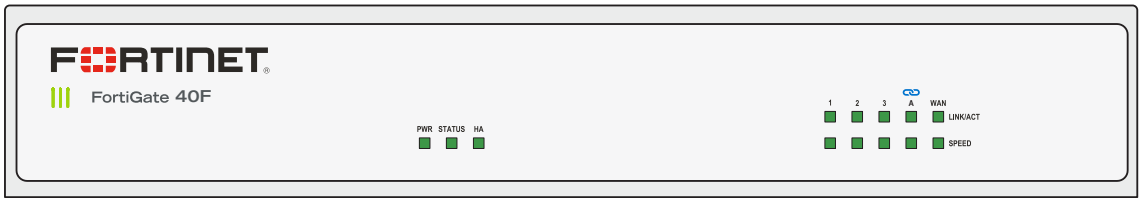

Déploiement FortiWiFi 40F dans les petits bureaux (NGFW)

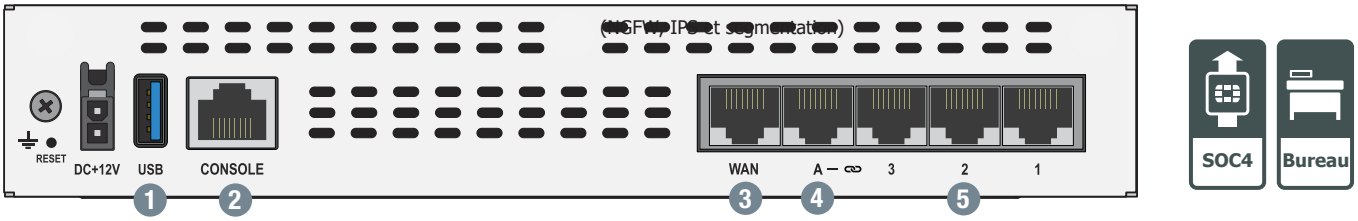



Déploiement FortiWiFi 40F en succursale (Secure SD-WAN)

# Hardware

## FortiGate 40F Series




## Interfaces

1. Port USB
2. Port console
3. 1x Port WAN GE RJ45
4. 1x Port FortiLink GE RJ45
5. 3x Ports Ethernet GE RJ45

## Processeur Secure SD-WAN ASIC SOC4

SPU

- Unité centrale RISC et processeurs réseau SPU (Security Processing Unit) de Fortinet pour des performances inégalées
- Identification et gestion des applications les plus rapides du secteur, pour optimiser les opérations commerciales
- Accélération des performances du VPN IPsec pour une meilleure expérience utilisateur sur internet
- Sécurité NGFW optimisée, inspection SSL approfondie et performances préservées
- Sécurisation de la couche d'accès, migration SD-WAN des succursales avec connectivité accélérée et intégrée des commutateurs et des points d'accès

## Connectivité WAN 3G/4G

La série FortiGate 40F est dotée d'un port USB permettant de brancher un modem USB 3G/4G tiers compatible afin d'établir une connectivité WAN supplémentaire ou une liaison redondante, pour une fiabilité maximale.

## Format compact et fiable

Conçu pour les environnements de petite envergure, ce FortiGate peut être placé sur un bureau ou fixé au mur. Ce modèle réduit, léger et très fiable, présente un MTBF (Mean Time Between Failure) supérieur, ce qui minimise les risques de perturbation réseau.

## Sécurisation de la couche d'accès grâce aux ports FortiLink

Le protocole FortiLink vous permet de concilier sécurité et accès réseau en intégrant FortiSwitch à FortiGate, sous la forme d'une extension logique du NGFW. Les ports activés FortiLink peuvent être reconfigurés en ports réguliers selon les besoins.

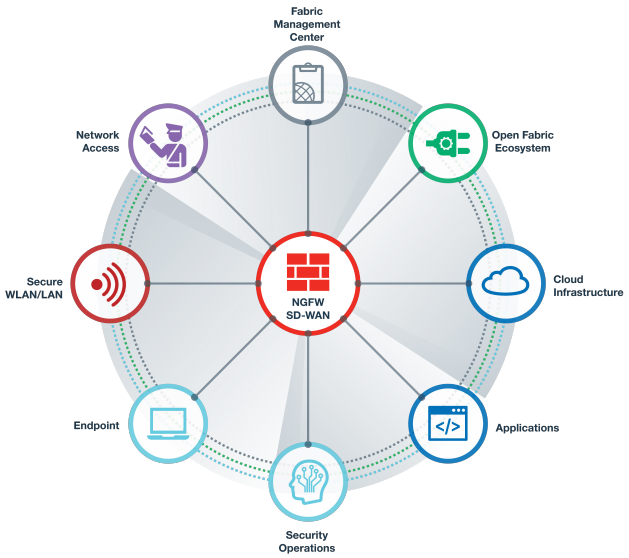
# Fortinet Security Fabric

## Security Fabric

Security Fabric est une plateforme de cybersécurité conçue pour l'innovation numérique. Elle offre une large visibilité sur l'ensemble de la surface d'attaque, pour une meilleure gestion des risques. Sa solution unifiée assure une intégration simplifiée des différents outils de sécurité. L'automatisation des flux augmente la vitesse opérationnelle et réduit les temps de réponse au sein de l'écosystème de déploiement Fortinet.

Via un unique panneau de gestion, Fortinet Security Fabric permet de gérer :

- **Un réseau axé sur la sécurité** pour protéger, accélérer et unifier le réseau et l'expérience utilisateur
- **Un accès réseau « tolérance zéro »**, pour identifier et protéger les utilisateurs et les appareils en temps réel, au sein du réseau et en-dehors
- **une sécurité cloud dynamique** pour protéger et contrôler les infrastructures et les applications cloud
- **Des opérations de sécurité reposant sur l'IA** pour prévenir, détecter, isoler et répondre automatiquement aux cybermenaces




## FortiOS

Les FortiGate servent de piliers à l'infrastructure Fortinet Security Fabric, dont le socle est FortiOS. Toutes les fonctionnalités réseau et de FortiGate sont contrôlées par un seul système d'exploitation intuitif. FortiOS simplifie les process. Il réduit les coûts et les délais de réponse tout en intégrant des produits et services de sécurité nouvelle génération au sein d'une seule et même plateforme.

- Une plateforme véritablement intégrée : un seul système d'exploitation et un unique panneau de contrôle, pour gérer l'ensemble de la surface d'attaque numérique.
- Une protection de haut-niveau recommandée par NSS Labs. Performances et sécurité validées par VB100, AV Comparatives et ICSA.
- Recours à des technologies de pointe comme la « deception technology ».
- Contrôlez des milliers d'applications, bloquez les derniers exploits et filtrez le trafic web sur la base de millions d'évaluations URL en temps réel, avec prise en charge TLS 1.3.
- Prévenez, détectez et neutralisez automatiquement les cyberattaques avancées en quelques minutes, grâce à une sécurité intégrée basée sur l'intelligence artificielle et à une protection avancée contre les menaces.
- Améliorez et unifiez l'expérience utilisateur grâce à des fonctionnalités SD-WAN innovantes permettant de détecter, contenir et isoler les menaces via une segmentation automatisée.
- Utilisez l'accélération matérielle SPU pour améliorer les performances de sécurité réseau.

# Services

## Services de sécurité FortiGuard™

FortiGuard Labs offre des renseignements en temps réel sur les cyber menaces et fournit des mises à jour de sécurité complètes pour l'ensemble des solutions Fortinet. Composé de chercheurs, d'ingénieurs et de spécialistes forensiques, FortiLabs collabore avec les autorités, avec les plus grandes entités de surveillance des cybermenaces et avec d'autres fournisseurs réseaux et sécurité.

## Services d'assistance FortiCare™

Nos équipes de support client FortiCare fournissent une assistance technique globale pour tous les produits Fortinet. Elles sont présentes en Amérique, en Europe, au Moyen-Orient et en Asie. Les services FortiCare répondent aux besoins des entreprises de toutes tailles.

Pour plus d'informations, consultez les sites forti.net/fortiguard et forti.net/forticare

# Spécifications

| | FORTIGATE 40F |
|---|---|
| **Spécifications hardware** | |
| Ports GE RJ45 WAN / DMZ | 1 |
| Ports internes GE RJ45 | 3 |
| Ports FortiLink GE RJ45 | 1 |
| Ports PoE/+ GE RJ45 | – |
| Interface sans fil | – |
| Ports USB | 1 |
| Console (RJ45) | 1 |
| Stockage interne | – |
| **Performances système - Répartition du trafic** | |
| Débit IPS[2] | 1 Gb/s |
| Débit NGFW[2,4] | 800 Mb/s |
| Débit Threat Protection[2,5] | 600 Mb/s |
| **Performances et capacités système** | |
| Débit firewall (1518 / 512 / 64 byte UDP) | 5/5/5 Gb/s |
| Latence Firewall (64 byte UDP) | 4 µs |
| Débit Firewall (Paquets par seconde) | 7,5 Mp/s |
| Sessions concomitantes (TCP) | 700 000 |
| Nouvelles sessions/seconde (TCP) | 35 000 |
| Politiques de firewall | 5 000 |
| Débit VPN IPsec (512 byte)[1] | 4,4 Gb/s |
| Tunnels VPN IPsec passerelle-passerelle | 200 |
| Tunnels VPN IPsec client-passerelle | 250 |
| Débit SSL-VPN | 490 Mb/s |
| Utilisateurs simultanés SSL-VPN (Maximum recommandé, mode tunnel) | 200 |
| Débit d'inspection SSL (IPS, moy. HTTPS)[3] | 310 Mb/s |
| Inspection SSL CPS (IPS, moy. HTTPS)[3] | 320 |
| Sessions simultanées d'inspection SSL (IPS, moy. HTTPS) | 55 000 |
| Débit de contrôle des applications (HTTP 64K)[2] | 990 Mb/s |
| Débit du CAPWAP (HTTP 64K) | 3,5 Gb/s |
| Domaines virtuels (par défaut / maximum) | 10 / 10 |
| Nombre maximum de FortiSwitch pris en charge | 8 |
| Nombre maximum de FortiAP (Total / Tunnel) | 10 / 5 |
| Nombre maximum de FortiTokens | 500 |
| Nombre maximum de FortiClients enregistrés | 200 |
| Configurations haute disponibilité | Active / Active, Active / Passive, Clustering |

| | FORTIGATE 40F |
|---|---|
| **Dimensions** | |
| Hauteur x Largeur x Longueur (pouces) | 1,5 x 8,5 x 6,3 |
| Hauteur x Largeur x Longueur (mm) | 38,5 x 216 x 160 |
| Poids | 1 kg (2,2 lbs) |
| Format | Bureau |
| **Environnement opérationnel et certifications** | |
| Entrée | 12Vdc, 3A |
| Alimentation requise | Alimenté par un adaptateur de courant continu externe, 100–240V AC, 50–60 Hz |
| Courant (Maximum) | 100V AC / 0,2A, 240V AC / 0,1A |
| Consommation d'énergie (moyenne / maximale) | 12,4 W / 15,4 W |
| Dissipation de la chaleur | 52.55 BTU/hr |
| Température de fonctionnement | 0–40°C (32–104°F) |
| Température de stockage | -35–70°C (-31–158°F) |
| Humidité | 10–90% sans condensation |
| Niveau de bruit | sans ventilateur : 0 dBA |
| Altitude de fonctionnement | Jusqu'à 2 250 m (7 400 ft) |
| Conformité | FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB |
| Certifications | ICSA Labs : Firewall, IPsec, IPS, Antivirus, SSL-VPN |

Remarque : Toutes les valeurs de performances indiquées représentent les valeurs optimales et varient en fonction de la configuration du système.

1. Le test de performances du VPN IPsec utilise AES256-SHA256.
2. Les performances de l'IPS (Enterprise Mix), du contrôle des applications (Application Control), du firewall nouvelle-génération (NGFW) et de Threat Protection sont mesurées avec la journalisation activée.
3. Les valeurs de performances de l'inspection SSL utilisent une moyenne de sessions HTTPS provenant de différentes suites de chiffrement.
4. Les performances du firewall NGFW sont mesurées avec le firewall, l'IPS et le contrôle des applications activés.
5. Les performances Threat Protection sont mesurées avec le firewall, l'IPS, le contrôle des applications et la protection anti-malware sont activés.

# Informations relatives aux commandes

| Produit | Référence (SKU) | Description |
|---|---|---|
| FortiGate 40F | FG-40F | 5 x ports GE RJ45 (dont 4 x ports internes, 1 x ports WAN), Maximum de FortiAP gérés (Total / Tunnel) 10 / 5 |

# Packs

**Pack FortiGuard**

FortiGuard Labs fournit plusieurs services de renseignements de sécurité destinés à renforcer la plateforme firewall FortiGate. Vous pouvez facilement optimiser votre protection FortiGate avec l'un de ces pack FortiGuard.

| Packs | Protection 360 | Protection Enterprise | UTM | Threat Protection |
|---|---|---|---|---|
| FortiCare | ASE[1] | 24x7 | 24x7 | 24x7 |
| Service de contrôle des applications FortiGuard | • | • | • | • |
| Service IPS FortiGuard | • | • | • | • |
| Protection avancée anti-malware (AMP) FortiGuard - Antivirus, Mobile Malware, Botnet, CDR, Virus Outbreak Protection et service cloud FortiSandbox | • | • | • | • |
| Service de filtrage web FortiGuard | • | • | • | |
| Service antispam FortiGuard | • | • | • | |
| Service d'évaluation de la sécurité FortiGuard | • | • | | |
| Service industriel FortiGuard | • | • | | |
| Service FortiCASB - SaaS uniquement | • | • | | |
| Service FortiConverter | • | | | |
| Surveillance assistée via cloud SD-WAN[2] | • | | | |
| Service VPN contrôleur de superposition SD-WAN[2] | • | | | |
| Cloud FortiAnalyzer[2] | • | | | |
| Cloud FortiManager[2] | • | | | |

1. 24 heures sur 24, 7 jours sur 7 + services avancés de traitement des tickets
2. Disponible avec FortiOS 6.2

www.fortinet.com