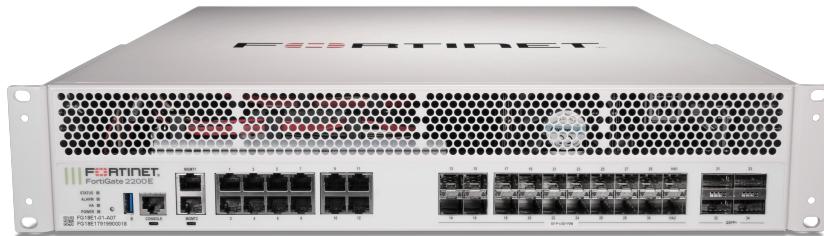


FICHE PRODUIT

Série FortiGate® 2200E

FG-2200E et 2201E

**Firewall nouvelle-génération
Segmentation
Passerelle web sécurisée
IPS
Sécurité mobile**



Les FortiGate 2200E offrent des fonctionnalités de firewall nouvelle génération (Next Generation Firewall - NGFW).

Ces modèles, destinés aux grandes entreprises et aux opérateurs télécoms, affichent de hautes performances : interfaces multiples ultra-rapides, densité de ports élevée et haut débit. Ils conviennent parfaitement aux déploiements en périphérie, aux déploiements en datacenters hybrides et sur les segments internes. Grâce à l'IPS de pointe, à l'inspection SSL et à la protection avancée contre les menaces, vous optimisez les performances de votre réseau. L'approche réseau de Fortinet s'intègre en toute sécurité aux solutions de cybersécurité nouvelle-génération.

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
158 Gb/s	16,5 Gb/s	13,5 Gb/s	11 Gb/s	Ports GE RJ45, 10 GE SFP+, 25 GE SFP28 et 40 GE QSFP+

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



Segmentation

- Une segmentation qui s'adapte à toute topologie réseau, pour une sécurité de bout en bout, depuis les succursales jusqu'au cloud en passant par les datacenters
- Réduction des risques grâce à la visibilité réseau offerte par Fortinet Security Fabric : autorisations d'accès adaptées aux scores de confiance et contrôles d'accès renforcés
- Défense renforcée grâce à l'inspection L7 et aux mesures de remédiation SPU Fortinet. Coût total de possession par Mb/s protégé validé par des experts indépendants
- Protection des applications critiques de l'entreprise et aide au respect des réglementations, sans avoir à reconcevoir le réseau



Passerelle de sécurisation web (SWG)

- Accès au web protégé contre les risques internes et externes, même pour le trafic chiffré à hautes performances
- Amélioration de l'expérience utilisateur grâce à la mise en cache dynamique du web et de la vidéo
- Blocage et contrôle de l'accès au web des utilisateurs ou de groupes d'utilisateurs en fonction des URL et domaines
- Prévention des pertes de données et identification des activités utilisateurs concernant les applications cloud connues et inconnues
- Blocage des requêtes DNS contre les domaines malveillants
- Protection avancée multicouche contre les menaces 0-day diffusées sur le web



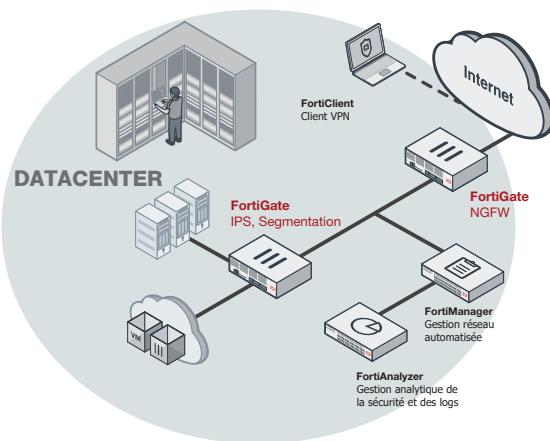
IPS

- Processeurs de sécurité spécialement conçus pour offrir des performances IPS validées par secteur, avec un débit élevé et une faible latence
- Déploiement de correctifs virtuels au niveau réseau pour assurer une protection contre l'exploitation des vulnérabilités réseau et optimiser le temps dédié à la protection du réseau
- L'inspection approfondie instantanée des paquets offre une visibilité inégalée sur les menaces pesant sur trafic réseau, y compris sur le trafic chiffré grâce à la nouvelle norme TLS 1.3
- Blocage proactif et en temps réel des attaques sophistiquées récemment identifiées, grâce à la protection avancée reposant sur les renseignements sur les menaces de Fortinet Security Fabric



Sécurité mobile pour 4G, 5G, et objets connectés

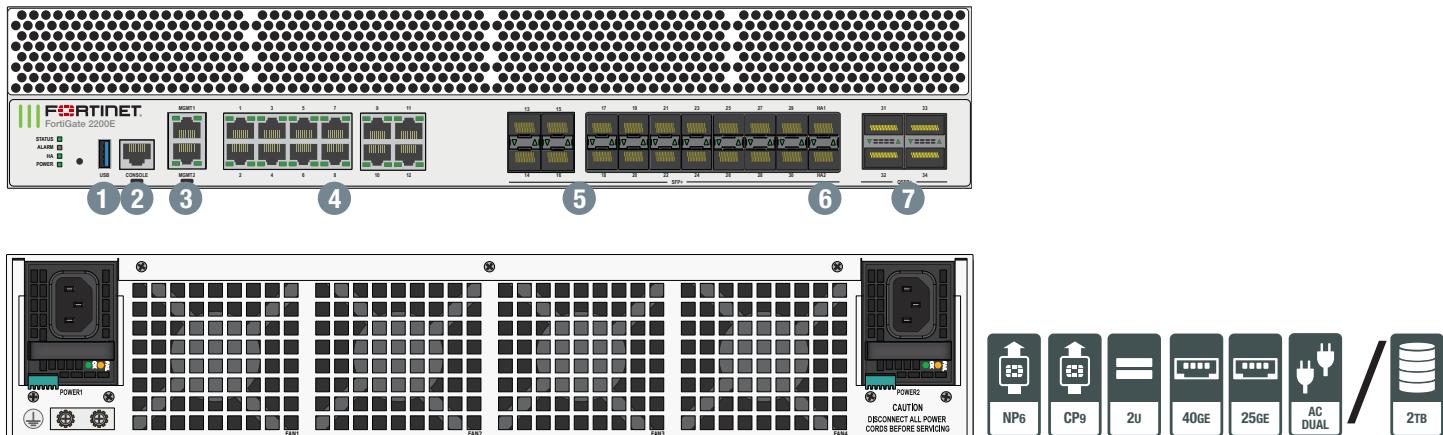
- Vitesses réseau hautes-performances avec FQ, CGNAT et un trafic IPv4 et IPv6 accéléré, alimenté par plusieurs SPU et une sécurité 4G SGi LAN et 5G N6.
- Sécurité d'accès au RAN via une passerelle de sécurité d'agrégation et de contrôle IPsec (SecGW) évolutive et performante
- Sécurisation du plan utilisateur assurée par une protection complète contre les menaces et par une visibilité accrue via l'inspection GTP-U
- Sécurisation des signaux 4G : inspection de divers protocoles tels que SCTP, Diameter, GTP-C, SIP et protection contre les attaques
- La 4G et la 5G, à la base de la prévention contre les orages de signaux (< signaling storms >)
- Interfaces ultra-rapides pour des déploiements flexibles



Déploiement de FortiGate 2200E en datacenter
(NGFW, IPS et segmentation)

Hardware

FortiGate 2200E/2201E



Interfaces

- 1. Port USB
- 2. Port de console
- 3. 2x Ports GE RJ45 MGMT
- 4. 12x Ports GE RJ45

- 5. 18x 25 GE SFP28 / 10 GE SFP+
- 6. 2x 25 GE SFP28 / 10 GE SFP+ HA
- 7. 4x 40 GE QSFP+

La puissance SPU



- Les processeurs SPU sur mesure délivrent la puissance qu'il vous faut pour détecter les contenus malveillants à des vitesses atteignant plusieurs gigabits.
- Les autres technologies de sécurité reposent sur des processeurs non-spécifiques, ce qui entraîne de dangereux écarts de performances.
- Les processeurs SPU offrent les performances dont vous avez besoin pour bloquer les cybermenaces émergentes, satisfaire aux critères des certifications indépendantes et éviter les ralentissements causés par d'autres solutions de sécurité réseau.

Processeur réseau

Le nouveau processeur réseau révolutionnaire SPU NP6 de Fortinet fonctionne en lien avec FortiOS :

- Performances supérieures du firewall pour le trafic IPv4/IPv6, SCTP et multicast, avec une latence ultra-faible de 2 microsecondes
- VPN, CAPWAP et accélération des tunnels IP
- Prévention des intrusions par anomalie, déchargement des sommes de contrôle (checksums) et défragmentation des paquets
- Façonnage du trafic et files d'attente prioritaires

Processeur de contenus

Le nouveau processeur de contenus SPU CP9 de Fortinet fonctionne en-dehors du flux direct du trafic et accélère l'inspection des fonctions de sécurité consommatrices de performances :

- Amélioration des performances IPS grâce à la correspondance complète des signatures au niveau du SPU
- Capacités d'inspection SSL établies selon les nouvelles suites de chiffrement préconisées par le secteur
- Déchargement du chiffrement et du déchiffrement

Connectivité ultra-rapide

La connectivité haut débit est essentielle à la segmentation de la sécurité au sein des réseaux de données. Les FortiGate 2200E offrent des interfaces 40 GE et 25 GE, pour une conception réseau simplifiée, sans avoir à recourir à des composants de connectivité additionnels.

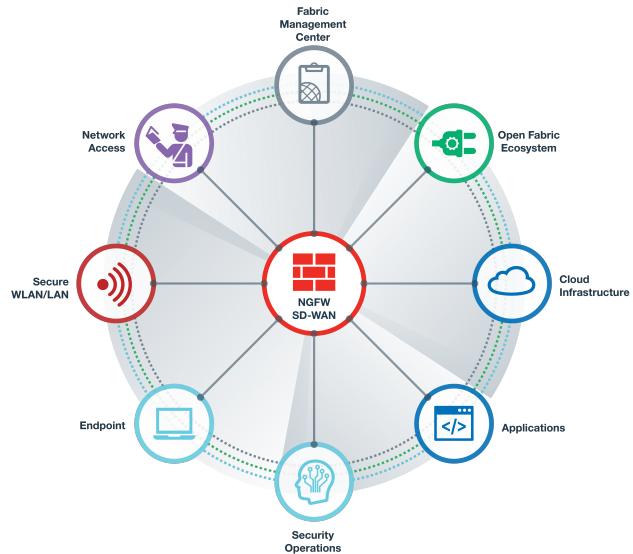
Fortinet Security Fabric

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 2200E	FORTIGATE 2201E	FORTIGATE 2200E	FORTIGATE 2201E
Interfaces et modules				
Ports 40 GE QSFP+ avec accélération hardware	4			
Emplacements SFP+ HA 25 GE SFP28 / 10 GE avec accélération matérielle	2			
Emplacements SFP+ 25 GE SFP28 / 10 GE avec accélération matérielle	18			
Ports GE RJ45 avec accélération matérielle	12			
Ports de gestion GE RJ45	2			
Ports USB (Client / Serveur)	1			
Port Console	1			
Stockage embarqué	0	2x 1 To SSD		
Emetteurs-récepteurs inclus		2x SFP+ (SR 10 GE)		
Performances système - Répartition du trafic				
Débit IPS ²	16,5 Gb/s			
Débit NGFW ²⁴	13,5 Gb/s			
Débit Threat Protection ²⁵	11 Gb/s			
Performances et capacités système				
Débit firewall IPv4 (1518 / 512 / 64 byte, UDP)	158 / 155 / 100 Gb/s			
Débit firewall IPv6 (1518 / 512 / 86 byte, UDP)	158 / 155 / 100 Gb/s			
Latence Firewall (64 byte, UDP)	4 µs			
Débit Firewall (Paquets par seconde)	150 Mp/s			
Sessions concomitantes (TCP)	24 millions			
Nouvelles sessions/seconde (TCP)	500 000			
Politiques de firewall	100 000			
Débit VPN IPsec (512 byte) ¹	98 Gb/s			
Tunnels VPN IPsec passerelle-passerelle	20 000			
Tunnels VPN IPsec client-passerelle	100 000			
Débit SSL-VPN	10 Gb/s			
Utilisateurs simultanés SSL-VPN (Maximum recommandé, mode tunnel)	30 000			
Débit d'inspection SSL (IPS, moy. HTTPS) ³	17 Gb/s			
Inspection SSL CPS (IPS, moy. HTTPS) ³	9 500			
Sessions simultanées d'inspection SSL (IPS, moy. HTTPS)	2,5 millions			
Débit de contrôle des applications (HTTP 64K) ²	52 Gb/s			
Débit du CAPWAP (HTTP 64K)	60 Gb/s			
Domaines virtuels (par défaut / maximum)	10 / 500			
Nombre maximum de FortiSwitch pris en charge	128			
Nombre maximum de FortiAP (Total / Tunnel)	4 096 / 2 048			
Nombre maximum de FortiTokens	20 000			
Configurations haute disponibilité	Active-Active, Active-Passive, Clustering			
Dimensions et alimentation				
Hauteur x Largeur x Longueur (pouces)	3,5 x 17,44 x 21,89			
Hauteur x Largeur x Longueur (mm)	88,9 x 443 x 556			
Poids	18,2 kg (40,0 lbs)	18,8 kg (41,4 lbs)		
Format	Montage en rack, 2 RU			
Alimentation électrique en courant alternatif	100–240V AC, 60–50 Hz			
Consommation d'énergie (moyenne / maximale)	408 W / 571 W	412 W / 577 W		
Courant (Maximum)	12A@100V, 9A@240V			
Dissipation de la chaleur	1948 BTU/h	1968 BTU/h		
Alimentations électriques redondantes	Oui, échangeable à chaud			
Environnement opérationnel et certifications				
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	70 dBA			
Altitude de fonctionnement	Jusqu'à 2 250 m (7 400 ft)			
Conformité	FCC Partie 15 Classe A, C-Tick, VCCI, CE, UL/cUL, CB			
Certifications	ICSA Labs : Firewall, IPsec, IPS, Antivirus, SSL-VPN; USGv6/IPv6			

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 2200E	FG-2200E	4x 40 emplacements GE QSFP+, 20x 25 emplacements GE SFP28 (dont 18x ports, 2x ports HA), 14x ports GE RJ45 (dont 12x ports, 2x ports de gestion), SPU NP6 et CP9 avec accélération matérielle et double AC
FortiGate 2201E	FG-2201E	4x 40 emplacements GE QSFP+, 20x 25 emplacements GE SFP28 (dont 18x ports, 2x ports HA), 14x ports GE RJ45 (dont 12x ports, 2x ports de gestion), SPU NP6 et CP9 avec accélération matérielle, double AC avec 2x 1 To SSD de stockage embarqué.
Accessoires optionnels / Pièces détachées		
Module émetteur-récepteur courte portée 10 GE SFP+	FG-TRAN-SFP+SR	Module émetteur-récepteur courte portée 10 GE SFP+ pour tous les systèmes équipés de ports SFP+ et SFP/SFP+.
Module émetteur-récepteur longue portée 10 GE SFP+	FG-TRAN-SFP+LR	Module émetteur-récepteur 10 GE SFP+ longue portée pour tous les systèmes équipés de ports SFP+ et SFP/SFP+.
Câble à fixation directe 10 GE SFP+ 10 m/32,8 ft	SP-CABLE-ADASFP+	Câble à fixation directe 10 GE SFP+ 10m / 32,8 ft pour tout système équipé de ports SFP+ et SFP/SFP+.
Module émetteur-récepteur 25 GE SFP28 longue portée	FG-TRAN-SFP28-LR	Module émetteur-récepteur longue portée 25 GE SFP28 pour tous les systèmes équipés de ports SFP28.
Module émetteur-récepteur SFP28 25 GE/10 GE courte portée dual Rate	FG-TRAN-SFP28-SR	Module émetteur-récepteur courte portée SFP28 dual rate 25 GE/10 GE, pour tous les systèmes équipés de ports SFP28/SFP+.
40 émetteurs-récepteurs GE QSFP+ courte portée	FG-TRAN-QSFP+SR	Émetteurs-récepteurs 40 GE QSFP+, courte portée, pour tous les systèmes équipés de ports QSFP+.
40 émetteurs-récepteurs GE QSFP+ courte portée, BiDi	FG-TRAN-QSFP+SR-BIDI	Émetteurs-récepteurs 40 GE QSFP+ BiDi à courte portée pour les systèmes équipés de ports QSFP+.
40 émetteurs-récepteurs GE QSFP+, longue portée	FG-TRAN-QSFP+LR	Émetteurs-récepteurs 40 GE QSFP+ longue portée pour tous les systèmes équipés de ports QSFP+.
Câble break out optique, 40 GE QSFP+ à 4x 10GE SFP+	FG-TRAN-QSFP+4XSFP	Câble optique actif 40GE QSFP+ à rupture parallèle d'une longueur de 1m, pour tous les systèmes équipés d'emplacements QSFP+.
Câble 5m breakout optique, de QSFP+ à 4xSFP+	FG-TRAN-QSFP+4SFP-5	Connecteurs parallèles 40G QSFP+, portée 5m, MPO - 4xLC, émetteurs-récepteurs non inclus.
Rails coulissants pour montage en rack	SP-FG3040B-RAIL	Rails coulissants pour montage en rack pour FG-1000C-/DC, FG-1100/1101E, FG-1200D, FG-1500D-/DC, FG-2000E, FG-2200E/2201E, FG-2500E, FG-3040B-/DC, FG-3140B-/DC, FG-3240C-/DC, FG-3000D-/DC, FG-3100D-/DC, FG-3200D-/DC, FG-3300E/3301E, FG-3400/3401E, FG-3600/3601E, FG-3700D-/DC, FG-3700DX, FG-3810D-/DC et FG-3950B-/DC.
Alimentation courant alternatif	SP-FG3800D-PS	Alimentation en courant alternatif pour FG-2200/2201E, FG-3300/3301E, FG-3400/3401E, FG-3600/3601E, FG-3700D, FG-3700D-NEBS, FG-3700DX, FG-3810D et FG-3815D.

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