FICHE PRODUIT

Série FortiGate® 600E

FortiGate 600E et 601E

Firewall nouvelle-génération
SD-WAN sécurisé
Passerelle web sécurisée
IPS

La série FortiGate 600E offre aux moyennes et grandes entreprises des fonctionnalités firewall nouvelle-génération (NGFW). Ces modèles ont été conçus pour être déployés au niveau des campus ou des succursales d'entreprises. Ils assurent une protection contre les cybermenaces grâce à de puissants processeurs de sécurité capables d'optimiser les performances du réseau tout en offrant une protection optimale et une visibilité accrue. 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
36 Gb/s	**10 Gb/s**	**9.5 Gb/s**	**7 Gb/s**	Multiples ports GE RJ45, GE SFP et 10 GE SFP+

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

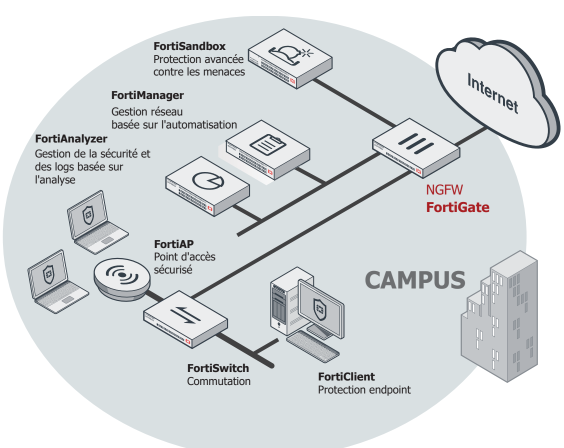
- Performances fiables pour les applications, avec détection précise, pilotage et optimisation dynamiques du cheminement WAN
- Accès multi-cloud pour une adoption plus rapide du SaaS, avec optimisation de bout en bout
- Déploiement zero touch et gestion centralisée avec auto-provisionnement, analyse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

Passerelle de sécurisation web (SWG)

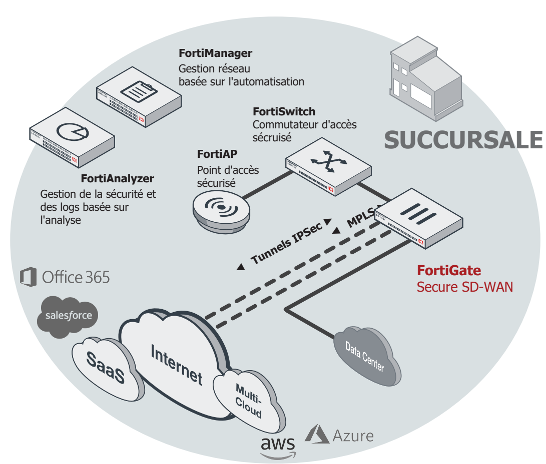
- Performances fiables pour les applications, avec détection précise, pilotage et optimisation dynamiques du cheminement WAN
- Accès multi-cloud pour une adoption plus rapide du SaaS, avec optimisation de bout en bout
- Déploiement zero touch et gestion centralisée avec auto-provisionnement, analyse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

IPS

- Processeurs de sécurité spécialement conçus pour offrir des performances IPS validées avec un débit élevé et une faible latence
- Déploiement de correctifs virtuels au niveau réseau afin d'assurer une protection contre l'exploitation des vulnérabilités réseau et d'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 TLS 1.3
- Blocage pro-actif 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



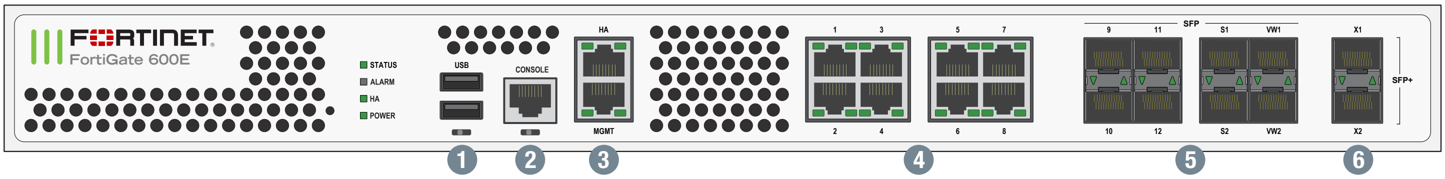
Déploiement FortiGate 600E en campus (NGFW)

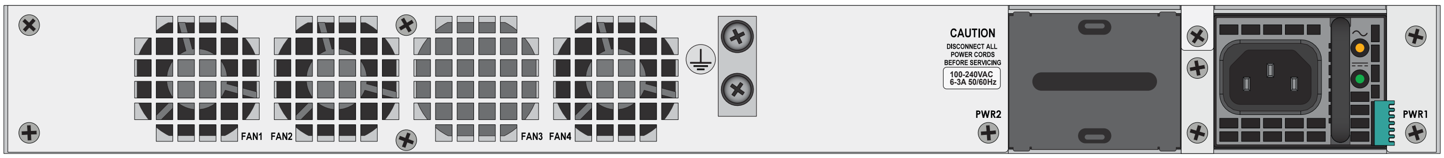


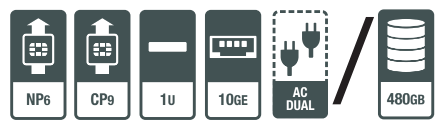
Déploiement FortiGate 600E en succursale (Secure SD-WAN)

Hardware

FortiGate 600E/601E







Interfaces

1. Port USB
2. Port de console
3. 2x Ports GE RJ45 MGMT/HA
4. 8x Ports GE RJ45
5. 8x Emplacements GE SFP
6. 2x Emplacements 10 GE SFP+

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 :

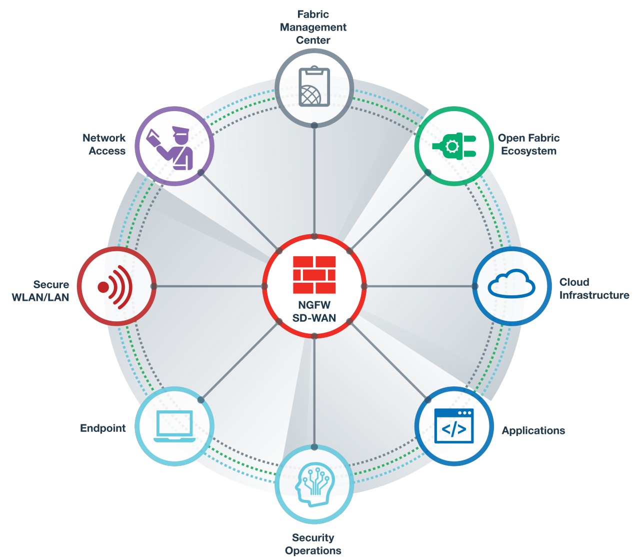
- Amélioration des performances IPS grâce à la correspondance complète des signatures au niveau du SPU
- Capacités d'inspection SSL établies selon les nouvelles suites de chiffrement préconisées par le secteur
- Déchargement du chiffrement et du déchiffrement

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 600E	FORTIGATE 601E
Interfaces et modules		
Emplacements 10 GE SFP+	2	
Interfaces GE RJ45	8	
Emplacements GE SFP	8	
Ports de gestion GE RJ45	2	
Ports USB	2	
Port de console RJ45	1	
Stockage local	NIL	2x 240 Go SSD
Émetteurs-récepteurs inclus	2x SFP (SX 1 GE)	
Performances système - Répartition du trafic		
Débit IPS[2]	10 Gb/s	
Débit NGFW[2,4]	9,5 Gb/s	
Débit Threat Protection[2,5]	7 Gb/s	
Performances et capacités système		
Débit firewall IPv4 (1518 / 512 / 64 byte, UDP)	36 / 36 / 27 Gb/s	
Débit firewall IPv6 (1518 / 512 / 86 byte, UDP)	36 / 36 / 27 Gb/s	
Latence Firewall (64 byte, UDP)	2 μs	
Débit Firewall (Paquets par seconde)	40,5 Mp/s	
Sessions concomitantes (TCP)	8 millions	
Nouvelles sessions/seconde (TCP)	450 000	
Politiques de firewall	10 000	
Débit VPN IPsec (512 byte)[1]	20 Gb/s	
Tunnels VPN IPsec passerelle-passerelle	2 000	
Tunnels VPN IPsec client-passerelle	50 000	
Débit SSL-VPN	7 Gb/s	
Utilisateurs simultanés SSL-VPN (Maximum recommandé, mode tunnel)	10 000	
Débit d'inspection SSL (IPS, moy. HTTPS)[3]	8 Gb/s	
Inspection SSL CPS (IPS, moy. HTTPS)[3]	5 500	
Sessions simultanées d'inspection SSL (IPS, moy. HTTPS)	800 000	
Débit de contrôle des applications (HTTP 64K)[2]	15 Gb/s	
Débit du CAPWAP (HTTP 64K)	18 Gb/s	
Domaines virtuels (par défaut / maximum)	10 / 10	
Nombre maximum de FortiSwitch pris en charge	64	
Nombre maximum de FortiAP (Total / Tunnel)	1 024 / 512	
Nombre maximum de FortiTokens	5 000	
Configurations haute disponibilité	Active-Active, Active-Passive, Clustering	

	FORTIGATE 600E	FORTIGATE 601E
Dimensions et alimentation		
Hauteur x Largeur x Longueur (pouces)	1,75 x 17,0 x 15,0	
Hauteur x Largeur x Longueur (mm)	44,45 x 432 x 380	
Poids	7,3 kg (16,1 lbs)	7,5 kg (16,6 lbs)
Format	1 RU	
Consommation d'énergie (moyenne / maximale)	129 W / 244 W	
Alimentation	100–240V 60–50Hz	
Courant (Maximum)	6A @ 100V	
Dissipation de la chaleur	832 BTU/h	
Alimentations électriques redondantes (hot swap)	en option	
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	59 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 600E	FG-600E	2x 10 emplacements GE SFP+, 10x ports GE RJ45 (dont 1x port MGMT, 1x port HA, 8x ports de commutation), 8x emplacements GE SFP, SPU NP6 et CP9 avec accélération matérielle.
FortiGate 601E	FG-601E	2x 10 emplacements GE SFP+, 10x ports GE RJ45 (dont 1x port MGMT, 1x port HA, 8x ports de commutation), 8x emplacements GE SFP, SPU NP6 et CP9 avec accélération matérielle, 2x 240 Go de stockage SSD embarqué.
Accessoires en option		
1 module émetteur-récepteur GE SFP LX	FG-TRAN-LX	1 module émetteur-récepteur GE SFP LX pour tous les systèmes équipés de ports SFP et de SFP/SFP+.
1 module émetteur-récepteur GE SFP RJ45	FG-TRAN-GC	1 module émetteur-récepteur GE SFP RJ45 pour tous les systèmes équipés de ports SFP et de SFP/SFP+.
1 module émetteur-récepteur GE SFP SX	FG-TRAN-SX	1 module émetteur-récepteur GE SFP LX pour tous les systèmes équipés de ports SFP et de SFP/SFP+.
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+.
Module émetteur-récepteur 10 GE cuivre SFP+, jusqu'à 30m	FS-TRAN-SFP+GC	Module émetteur-récepteur 10 GE cuivre SFP+ RJ45. Pour FortiSwitch uniquement, jusqu'à 30m.
Câble à fixation directe active 10 GE SFP+ 10 m/32,8 ft	SP-CABLE-ADASFP+	Câble à fixation directe 10 GE SFP+ 10m / 32,8 ft pour tous les systèmes équipés de ports SFP+ et SFP/SFP+.
Alimentation optionelle	SP-FG300E-PS	Alimentation CA pour FG-300/301E, FG-400/401E, FG-500/501E, FG-600/601E, FAZ-200F/300F/800F et FMG-200F/300F.

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 FortiAnalyzer2	•			
Cloud FortiManager2	•			

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

FERTINET

www.fortinet.com