

Série FortiGate® 400E

FortiGate 400E et 401E

Firewall nouvelle-génération
SD-WAN sécurisé
Passerelle web sécurisée



La série FortiGate 400E 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 centre d'intelligence permanente sur les menaces par les services de sécurité de FortiGuard Labs
- Blocage pro-actif des attaques sophistiquées inconnues en temps réel grâce à FortiSandbox, le système de sandboxing de la 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 fabricant 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 des capacités intégrées de SD-WAN pour des performances applicatives optimales et une meilleure expérience utilisateur
- Fonctionnalités avancées de routage intégrées pour offrir des performances de pointe, notamment avec des tunnels IPSEC chiffrés à grande échelle

Administration

- Interface de gestion intuitive, offrant automatisation et visibilité complète sur le réseau
- Zero Touch Provisioning (Déploiement Sans Contact) grâce à une console centrale de gestion fourni par le Fabric Management Center
- Audits de configurations pré-définis permettant d'analyser et veiller à respecter les bonnes pratiques de déploiement, pour une sécurité renforcée

Approche Security Fabric

- Permet aux produits Fortinet et aux 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 de Fortinet et des partenaires Fabric-ready

Firewall	IPS	NGFW	Threat Protection	Interfaces
32 Gb/s	7,8 Gb/s	6 Gb/s	5 Gb/s	Multiples ports GE RJ45 et GE SFP

Pour plus de détails, consultez le tableau des spécifications

Deploiement



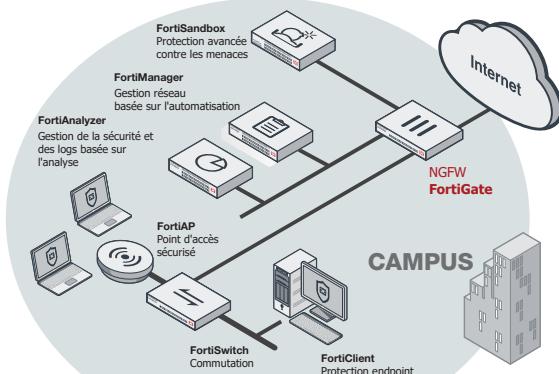
Firewall nouvelle-génération (NGFW)

- 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 au moteur de 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 optimales des applications métier grâce à une détection précise, un pilotage et une optimisation dynamiques des réseaux WAN
- Un accès multi-cloud pour une adoption plus rapide du SaaS avec une optimisation de bout en bout
- Simplification grâce au déploiement "zero touch" et à la 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

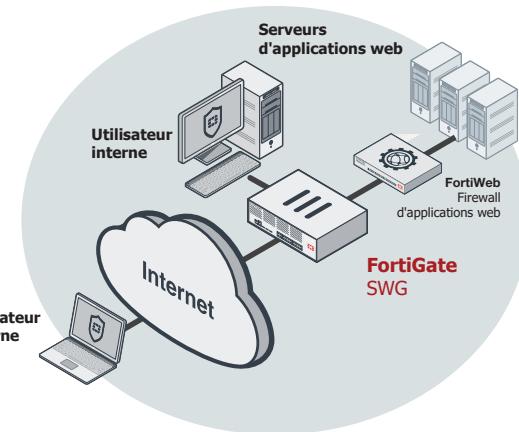


Déploiement FortiGate 400E en campus (NGFW)

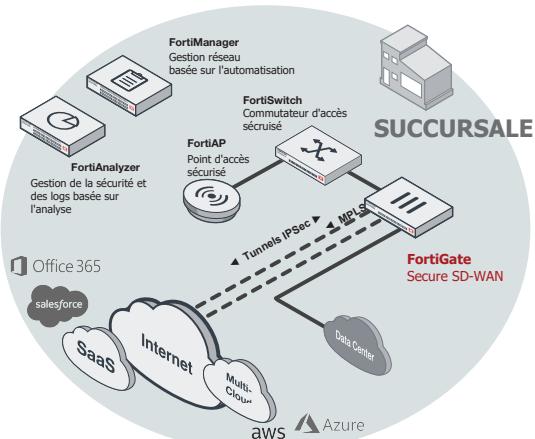


Passerelle de sécurisation web (SWG)

- Accès au web protégé contre les risques internes et externes, même pour le trafic chiffré 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



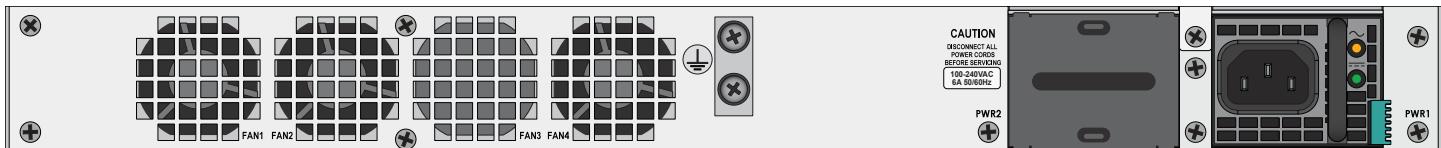
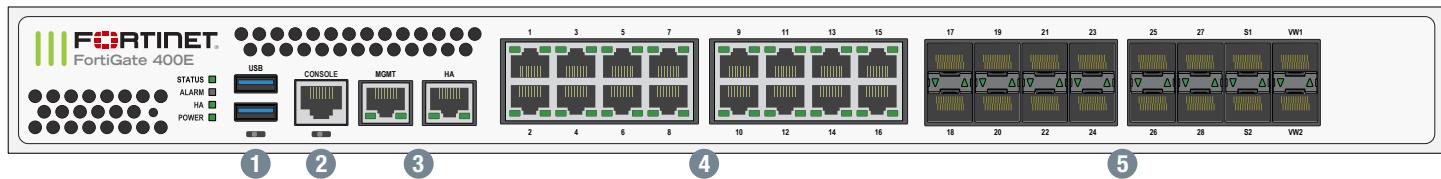
Déploiement SWG FortiGate 400E



Déploiement FortiGate 400E en succursale (Secure SD-WAN)

Hardware

FortiGate 400E/401E



Interfaces

- 1. Ports USB
- 2. Port de console
- 3. 2x Ports GE RJ45 MGMT/HA
- 4. 16x Ports GE RJ45
- 5. 16x Emplacements 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
- Limitation et priorisation de trafic / bande passante

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 favoriser la transformation digitale. 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 une console centrale d'administration, 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 sécurité du 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.

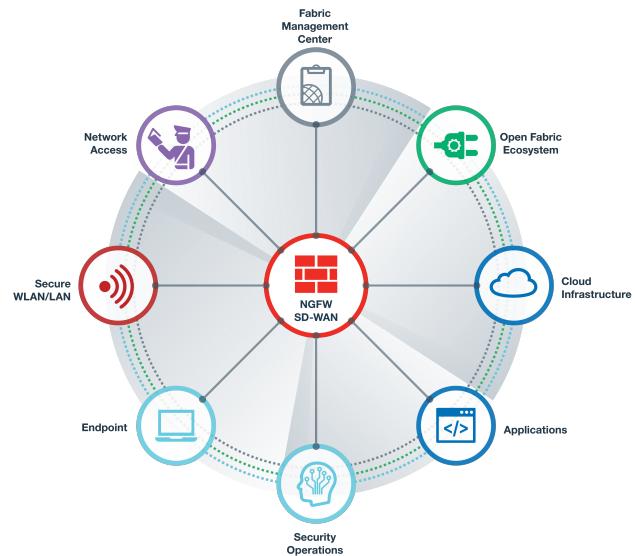
- Une plateforme véritablement intégrée : un seul système d'exploitation et un unique panneau de contrôle, pour gérer l'ensemble de la surface d'attaque numérique.
- Une protection de haut-niveau recommandée par NSS Labs. Performances et sécurité validées par VB100, AV Comparatives et ICSA.
- Recours à des technologies de pointe comme la « deception technology ».

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.



- 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 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 400E	FORTIGATE 401E	FORTIGATE 400E	FORTIGATE 401E
Interfaces et modules				
Interfaces GE RJ45	16			
Emplacements GE SFP	16			
Ports de gestion GE RJ45	2			
Ports USB	2			
Port de console RJ45	1			
Stockage local	NIL	2x 240 GB SSD		
Émetteurs-récepteurs inclus		2x SFP (SX 1 GE)		
Performances système - Répartition du trafic				
Débit IPS ²	7,8 Gb/s			
Débit NGFW ²	6 Gb/s			
Débit Threat Protection ⁵	5 Gb/s			
Performances et capacités système				
Débit firewall IPv4 (1518 / 512 / 64 byte, UDP)	32 / 32 / 24 Gb/s			
Débit firewall IPv6 (1518 / 512 / 86 byte, UDP)	32 / 32 / 24 Gb/s			
Latence Firewall (64 byte, UDP)	3 µs			
Débit Firewall (Paquets par seconde)	36 Mp/s			
Sessions concomitantes (TCP)	4 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	4,5 Gb/s			
Utilisateurs simultanés SSL-VPN (Maximum recommandé, mode tunnel)	5 000			
Débit d'inspection SSL (IPS, moy. HTTPS) ³	4,8 Gb/s			
Inspection SSL CPS (IPS, moy. HTTPS) ³	4 000			
Sessions simultanées d'inspection SSL (IPS, moy. HTTPS)	300 000			
Débit de contrôle des applications (HTTP 64K) ²	12 Gb/s			
Débit du CAPWAP (HTTP 64K)	14,8 Gb/s			
Domaines virtuels (par défaut / maximum)	10 / 10			
Nombre maximum de FortiSwitch pris en charge	48			
Nombre maximum de FortiAP (Total / Tunnel)	512 / 256			
Nombre maximum de FortiTokens	5 000			
Configurations haute disponibilité	Active-Active, Active-Passive, Clustering			
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	7,4 kg (16,4 lbs)	7,9 kg (16,9 lbs)		
Format	1 RU			
Consommation d'énergie (moyenne / maximale)	109 W / 214 W	115 W / 221 W		
Alimentation	100-240V 60-50Hz			
Courant (Maximum)	6A			
Dissipation de la chaleur	730 BTU/h	754 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	48 dBA			
Altitude de fonctionnement	Jusqu'à 2 250 m (7 400 ft)			
Conformité	FCC Partie 15 Clases 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 400E	FG-400E	18 ports GE RJ45 (dont 1 port MGMT, 1 port HA, 16 ports de commutation), 16 emplacements GE SFP, SPU NP6 et CP9 avec accélération matérielle.
FortiGate 401E	FG-401E	18 ports GE RJ45 (dont 1 port MGMT, 1 port HA, 16 ports de commutation), 16 emplacements GE SFP, SPU NP6 et CP9 avec accélération matérielle, 2 emplacements SSD de 240 Go.
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+.
Alimentation optionnelle	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 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