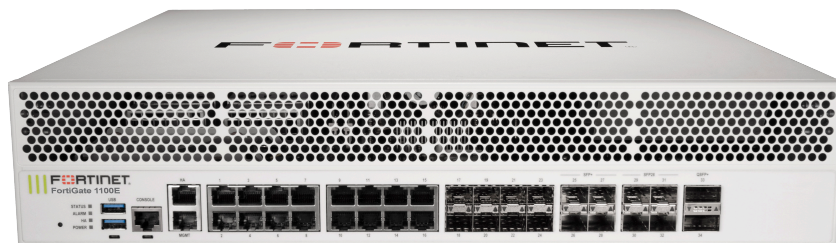


FortiGate® série 1100E

FG-1100E/-DC ET 1101E

Firewall nouvelle-génération
Segmentation
Passerelle web sécurisée
IPS
Sécurité mobile



Les FortiGate 1100E 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. Ces modèles FortiGate conviennent parfaitement aux déploiements en périphérie, aux déploiements au sein des 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 des 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 fournisseur 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
- Provisionnement sans contact, 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

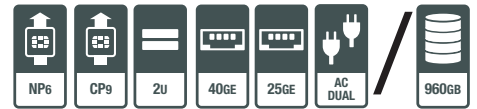
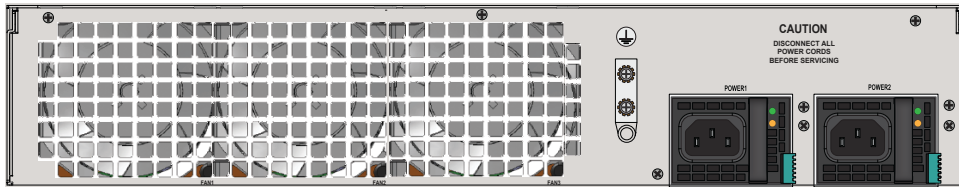
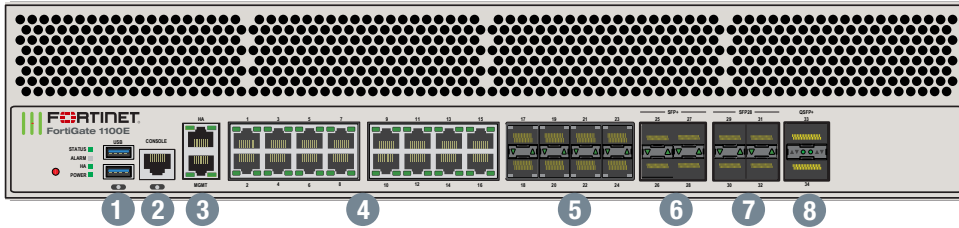
Approche Security Fabric

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

| Firewall | IPS | NGFW | Threat Protection | Interfaces |
|----------|-----------|----------|-------------------|---|
| 80 Gb/s | 12,5 Gb/s | 9,8 Gb/s | 7,1 Gb/s | Ports GE RJ45, GE SFP, 10 GE SFP+, 25 GE SFP28 et 40 GE QSFP+ |

Hardware

FortiGate 1100E/-DC et 1101E



Interfaces

- | | |
|--|---|
| <ol style="list-style-type: none"> 1. 2 ports USB 2. Port console 3. 2 ports GE RJ45 MGMT/HA 4. 16 ports GE RJ45 | <ol style="list-style-type: none"> 5. 8 emplacements GE SFP 6. 4 emplacements 10 GE SFP+ 7. 4 emplacements 25 GE SFP28 / 10 GE SFP+ 8. 2 emplacements 40 GE QSFP+ |
|--|---|

La puissance SPU



- Les processeurs SPU sur mesure délivrent la puissance dont vous avez besoin 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

Content Processor

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
- Prise en charge 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 1100E proposent des interfaces 40GE et 25GE, pour une conception réseau simplifiée, sans avoir à recourir à des composants de connectivité additionnels.

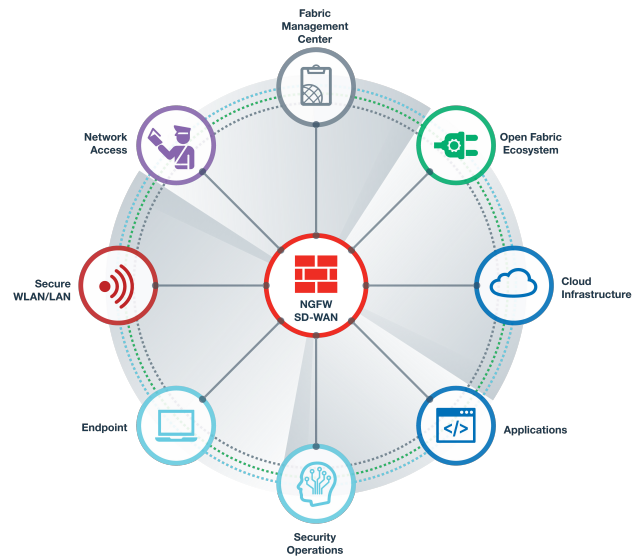
Fortinet Security Fabric

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 les aspects suivants :

- **Un réseau axé sur la sécurité** pour protéger, accélérer et unifier le réseau et l'expérience utilisateur
- **Accès réseau « tolérance zéro »**, pour identifier et protéger les utilisateurs et les appareils en temps réel, au sein du réseau et en-dehors
- **Sécurité cloud dynamique** pour protéger et contrôler les infrastructures et les applications cloud
- **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 de sécurité et réseau 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 ICASA.
- 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. Composée 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

| | FG-1100E/-DC | FG-1101E |
|---|--------------|---------------------------------------|
| Interfaces et modules | | |
| Ports 40 GE QSFP+ avec accélération hardware | | 2 |
| Ports 25 GE SFP28 / 10 GE SFP+ avec accélération hardware | | 4 |
| Ports 10 GE SFP+ avec accélération matérielle | | 4 |
| Ports GE SFP avec accélération hardware | | 8 |
| Ports GE RJ45 avec accélération hardware | | 16 |
| Gestion GE RJ45 / Ports HA | | 2 |
| Ports USB (Client / Serveur) | | 1 / 2 |
| Port Console | | 1 |
| Stockage embarqué | 0 | 2x 480 Go SSD. |
| Émetteurs-récepteurs inclus | | 2x SFP (SX 1 GE) |
| Performances système - Répartition du trafic | | |
| Débit IPS ² | | 12,5 Gb/s |
| Débit NGFW ^{2, 4} | | 9,8 Gb/s |
| Débit Threat Protection ^{2, 5} | | 7,1 Gb/s |
| Performances et capacités système | | |
| Débit firewall IPv4 (1518 / 512 / 64 byte, UDP) | | 80 / 80 / 45 Gb/s |
| Débit firewall IPv6 (1518 / 512 / 86 byte, UDP) | | 80 / 80 / 45 Gb/s |
| Latence Firewall (64 byte, UDP) | | 3 µs |
| Débit Firewall (Paquets par seconde) | | 67,5 Mp/s |
| Sessions concomitantes (TCP) | | 8 Million |
| Nouvelles sessions/seconde (TCP) | | 500 000 |
| Politiques de firewall | | 100 000 |
| Débit VPN IPsec (512 byte) ¹ | | 48 Gb/s |
| Tunnels VPN IPsec passerelle-passerelle | | 20 000 |
| Tunnels VPN IPsec client-passerelle | | 100 000 |
| Débit SSL-VPN | | 8,4 Gb/s |
| Utilisateurs simultanés SSL-VPN (Maximum recommandé, mode tunnel) | | 10 000 |
| Débit d'inspection SSL (IPS, moy. HTTPS) ³ | | 10,0 Gb/s |
| Inspection SSL CPS (IPS, moy. HTTPS) ³ | | 6500 |
| Sessions simultanées d'inspection SSL (IPS, moy. HTTPS) | | 780 000 |
| Débit de contrôle des applications (HTTP 64K) ² | | 26 Gb/s |
| Débit du CAPWAP (HTTP 64K) | | 43 Gb/s |
| Domaines virtuels (par défaut / maximum) | | 10 / 250 |
| Nombre maximum de FortiSwitch pris en charge | | 128 |
| Nombre maximum de FortiAP (Total / Tunnel) | | 4096 / 2048 |
| Nombre maximum de FortiTokens | | 20000 |
| Configurations haute disponibilité | | Actif-Actif, Actif-Passif, Clustering |

| | FG-1100E/-DC | FG-1101E |
|--|--|---------------------|
| Dimensions et alimentation | | |
| Hauteur x Largeur x Longueur (pouces) | 3.5 x 17,44 x 17,62 | |
| Hauteur x Largeur x Longueur (mm) | 88,9 x 443 x 447,4 | |
| Poids | 11,3 kg (24,9 lbs) | 11,55 kg (25.4 lbs) |
| Format | Montage en rack 2 RU | |
| Alimentation électrique en courant alternatif | 100–240V AC, 50–60 Hz | |
| Alimentation électrique en courant continu (FG-1100E-DC) | 48-72VDC | – |
| Consommation d'énergie (moyenne / maximale) | 217 W / 336 W | 222 W / 346 W |
| Courant (Maximum) | 6A@120V, 3A@240V | |
| Dissipation de la chaleur | 1147 BTU/h | 1181 BTU/h |
| Alimentations électriques redondantes | Oui, échangeable à chaud | |
| Environnement opérationnel et certifications | | |
| Température de fonctionnement | 32–104°F (0–40°C) | |
| Température de stockage | -35–70°C (-31–158°F) | |
| Humidité | 10–90% sans condensation | |
| Niveau de bruit | 66,7 dBA | |
| Altitude de fonctionnement | Jusqu'à 2250 m (7400 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 1100E | FG-1100E | 2x 40 ports GE QSFP+, 4x 25 ports GE SFP28, 4x 10 ports GE SFP+, 8 ports GE SFP, 18 ports GE RJ45 (dont 16 ports, 2 ports de gestion/HA), SPU NP6 et CP9 avec accélération hardware et 2 alimentations CA. |
| FortiGate 1101E | FG-1101E | 2x 40 ports GE QSFP+, 4x 25 ports GE SFP28, 4x 10 ports GE SFP+, 8x ports GE SFP, 18x ports GE RJ45 (dont 16x ports, 2x ports de gestion/HA) SPU NP6 et CP9 avec accélération hardware, 960 Go de stockage embarqué SSD, et 2 alimentations AC. |
| FortiGate 1100E-DC | FG-1100E-DC | 2x 40 ports GE QSFP+, 4x 25 ports GE SFP28, 4x 10 ports GE SFP+, 8 ports GE SFP, 18 ports GE RJ45 (dont 16 ports, 2 ports de gestion/HA), SPU NP6 et CP9 avec accélération hardware et 2 alimentations DC. |
| Accessoires/pièces détachées en option | Référence (SKU) | Description |
| 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+. |
| 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+. |
| Module émetteur-récepteur longue portée 25 GE SFP28 | FG-TRAN-SFP28-LR | Module émetteur-récepteur longue portée 25 GE SFP28 pour tous les systèmes équipés de ports SFP28. |
| Module émetteur-récepteur courte portée dual rate 25 GE/10 GE SFP28 | 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+. |
| Émetteurs-récepteurs 40 GE QSFP+, courte portée | FG-TRAN-QSFP+SR | Émetteurs-récepteurs 40 GE QSFP+, courte portée, pour tous les systèmes équipés de ports QSFP+. |
| Émetteurs-récepteurs 40 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+. |
| Émetteurs-récepteurs 40 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-2500E, FG-3040B/-DC, FG-3140B/-DC, FG-3240C/-DC, FG-3000D/-DC, FG-3100D/-DC, FG-3200D/-DC, FG-3400/3401E, FG-3600/3601E, FG-3700D/-DC, FG-3700DX, FG-3810D/-DC et FG-3950B/-DC |
| Alimentation électrique en courant alternatif | SP-FG300E-PS | Alimentation en courant alternatif pour FG-300/301E, FG-400/401E, FG-500/501E, FG-600/601E, FG-1100/1101E, FAZ-200F/FAZ-300F/FMG-200F et FAZ-800F/FMG-300F. |
| Alimentation en courant continu | SP-FG300E-DC-PS | Alimentation en courant continu pour FG-1100E-DC |

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 | • | • | • | • |

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

FORTINET

www.fortinet.com

Copyright © 2019 Fortinet, Inc. Tous droits réservés. Fortinet®, FortiGate®, FortiCare® et FortiGuard®, et certaines autres marques sont des marques déposées de Fortinet, Inc. et d'autres noms de Fortinet dans le présent document peuvent également être des marques déposées et/ou de droit commun de Fortinet. Tous les autres noms de produits ou de sociétés peuvent être des marques de leurs propriétaires respectifs. Les performances et autres mesures contenues dans le présent document ont été obtenues lors de tests internes en laboratoire en conditions optimales, et les performances réelles et autres résultats peuvent varier. Les variables de réseau, les différents environnements réseau et d'autres conditions peuvent affecter les performances. Rien dans les présentes ne représente un engagement contraignant pour Fortinet, et Fortinet décline toute garantie, expresse ou implicite, sauf lorsqu'un contrat écrit contraignant a été signé conjointement par l'avocat général de Fortinet et par un acheteur et que ce contrat apporte des garanties expresse concernant les performances. Dans ce cas, seules les mesures de performance spécifiques expressément identifiées dans ce contrat écrit contraignant seront contraignantes pour Fortinet. Pour une clarté absolue, toute garantie de ce type sera limitée à la performance dans les mêmes conditions idéales que celles des tests de laboratoire internes de Fortinet. Fortinet décline entièrement tout engagement, représentation et garantie, explicites ou implicites, en vertu des présentes. Fortinet se réserve le droit de changer, modifier, transférer ou réviser cette publication sans préavis. La version la plus récente de cette publication prévaut. En cas de divergence, la version originale anglaise de ce document prévaut.