



Description de l'offre – Produit

Gamme Cisco Secure Firewall

La présente Description de l'offre fait partie des [Conditions générales](#) ou de toute autre condition similaire existant entre Vous et Cisco (p. ex., Contrat de licence d'utilisateur final) (le « **Contrat** »). Les termes commençant par une majuscule, sauf s'ils sont définis dans le présent document, ont la signification qui leur est donnée dans le Contrat. Les références au Contrat de licence de l'utilisateur final supplémentaire ou au CLUFS font référence à la Description de l'offre.

1. Résumé

La gamme Cisco Secure Firewall (le « **Produit** ») offre des pare-feu sur site et dans le nuage qui exercent des fonctions de sécurité essentielles et mettent en œuvre les protocoles de sécurité du réseau. Les capacités spécifiques varient selon la solution et peuvent comprendre le filtrage d'URL, la connectivité de site à site et de VPN distant, la supervision du trafic réseau et le blocage des menaces, entre autres. Les fonctionnalités supplémentaires du Produit comprennent AI Assistant de Cisco pour la gestion des politiques de pare-feu, le moteur de visibilité chiffrée (ISE) de Cisco, SnortML et Talos Threat Intelligence. La gamme de produits comprend les éléments suivants :

- **Solutions sur site** : Les appareils de la série Cisco Firepower 1000s, 1200s, 3100s, 4100s, 4200s, 9300s et Cisco Secure Firewall ISA3000 (collectivement les « pare-feu de nouvelle génération » ou « NGFW »), Cisco Secure Firewall Management Center (« FMC »), Cisco Secure Firewall Threat Defense (« FTD »), Cisco Adaptive Security Appliance (« appareils de sécurité adaptables Cisco »), Firewall Device Manager (« FDM »), le pare-feu d'applications Web sécurisées (« WAF ») et Cisco Secure Cloud DDoS Protection.
- **Solutions en nuage** : Cisco Secure Firewall Threat Defense Virtual pour le nuage public et pour le nuage privé (« FTDv »), Cisco Adaptive Security Appliance Virtual (« ASAv »), Secure Cloud Web Application Firewall (« CWAF ») et Cisco Secure Cloud DDoS Protection.

2. Services d'assistance et autres services

- 2.1 **Assistance vendue séparément.** Votre achat du Produit n'inclut pas l'assistance, mais Vous pouvez acheter l'assistance séparément.
- 2.2 **Intégrations.** Les produits, services et intégrations supplémentaires qui peuvent être disponibles afin que Vous les utilisiez avec le produit, mais qui ne sont pas considérés comme faisant partie du Produit, comprennent, sans s'y limiter : Cisco Security Cloud Control (anciennement Cisco Defense Orchestrator), notamment Firewall Management Center en nuage (cdFMC), Cisco Multicloud Defense (MCD), Cisco Secure Workload, Cisco Security Analytics and Logging, Cisco XDR, Cisco Identity Services Engine et d'autres solutions tierces.

3. Protection des données

Fiche technique sur la confidentialité. La [Fiche technique sur la confidentialité de la gamme Cisco Secure Firewall](#) et la [Fiche technique sur la confidentialité de Cisco AI Assistant](#) décrivent les renseignements personnels que Cisco recueille et traite dans le cadre de la fourniture du Produit.

4. Conditions particulières

- 4.1 **Tests concurrentiels.** Vous n'êtes pas autorisé à publier ou à divulguer à des tiers les renseignements

ou analyses (par ex., les résultats des tests de référence ou de tests concurrentiels) sans l'autorisation écrite préalable de Cisco.

- 4.2 **Conditions supplémentaires pour le pare-feu d'applications Web sécurisées.** Si Vous achetez Cisco Secure Web Cloud Application Firewall (WAF) et/ou Cisco Secure Cloud DDoS Protection, Vous êtes également soumis à l'accord principal de services en nuage situé à l'adresse : <https://www.radware.com/WorkArea/DownloadAsset.aspx?ID=f78d23de-791f-435e-8d02-a564992231d8>
- 4.3 **Avis de non-responsabilité.** Bien que Cisco déploie des efforts commercialement raisonnables pour créer des technologies de sécurité efficaces, Cisco ne déclare ni ne garantit que le Produit offrira une sécurité absolue ou qu'il protégera tous Vos fichiers, vos systèmes, votre réseau ou vos terminaux contre tous les programmes malveillants, toutes les attaques malveillantes ou toute autre menace.