Dispositifs de sécurité intégrés de la gamme Cisco Small Business ISA500

Solution d'accès et de sécurité Internet tout-en-un pour protéger votre PME

Le dispositif de sécurité intégré de la gamme Cisco® Small Business ISA500 propose une solution d'accès et de sécurité Internet tout-en-un qui associe un accès Internet, sans fil, site-à-site et distant hautement sécurisé à de nombreuses fonctionnalités de gestion unifiée des menaces (UTM). Ces fonctionnalités incluent un pare-feu, la sécurité Internet et la protection des e-mails, ainsi que le contrôle des applications pour vous assurer que votre PME est protégée. Spécialement conçue pour les petites et moyennes entreprises, la solution ISA500 est peu coûteuse et facile à utiliser. En quelques minutes seulement, vous pouvez la configurer pour protéger votre entreprise. Elle exploite pleinement la base Cisco Security Intelligence Operations (SIO), qui fournit une surveillance globale des menaces afin d'apporter une protection supérieure. La puissance combinée de l'ensemble exhaustif de fonctionnalités UTM incluses dans la solution ISA500, alliée à une conception facile à utiliser et à une surveillance accrue des menaces, préserve la sécurité de votre entreprise et augmente à la fois le temps d'activité et la productivité de vos employés, tout en réduisant les coûts opérationnels et le risque de perturbation de l'activité.

La gamme Cisco ISA500 utilise une approche de la sécurité Internet et de la protection des e-mails basée sur le Cloud Computing (informatique en nuage), qui réduit au minimum les tâches de gestion et permet une protection flexible et réactive contre les nouvelles menaces. Un tel niveau d'analyse en profondeur permet d'augmenter la productivité de vos employés en contrôlant les accès Internet, ainsi qu'en réduisant les e-mails indésirables et les attaques par phishing, les intrusions et autres menaces émergentes. De plus, les 75 To par jour de suivi des menaces par télémétrie fournis par les 1,6 million de périphériques de la base Cisco SIO offrent une meilleure surveillance globale des menaces et une protection supérieure contre les attaques sophistiquées. Cette approche exhaustive de la protection contre les menaces permet de libérer les ressources informatiques des tâches chronophages d'éradication des virus et de nettoyage du système.

Outre les nombreuses fonctionnalités déjà présentées, la solution Cisco ISA500 fournit de nombreuses options permettant d'optimiser le temps d'activité de votre entreprise. Elle fournit une redondance WAN qui prend en charge le basculement, l'équilibrage de charge et le routage PBR (Policy-Based Routing) afin de permettre la continuité de l'activité en cas de panne liée à la connexion Internet ou directement au niveau du FAI. En outre, en tant que composante du portefeuille de produits Cisco Small Business, la gamme Cisco ISA500 a été testée pour garantir sa compatibilité avec les autres produits du portefeuille Cisco Small Business. L'intégralité de la solution est ainsi plus fonctionnelle.

La gamme ISA500 est également conçue pour répondre aux besoins des entreprises dynamiques modernes. Elle permet aux employés mobiles et aux partenaires commerciaux de se connecter de façon plus sécurisée aux réseaux via Internet, à l'aide des services VPN IPsec (IP Security) ou SSL (Secure Socket Layer). Avec une solution Cisco de la gamme ISA500 pour protéger votre réseau, vous pouvez vous consacrer à répondre aux besoins de vos clients et à assurer la croissance de votre activité, plutôt que de vous préoccuper des questions de sécurité.

Le challenge

Les petites entreprises ont besoin d'une solution simple, peu coûteuse et facile à déployer qui permet d'accéder à Internet avec le niveau de protection adéquat pour garantir qu'Internet est utilisé de façon sûre et ne perturbe pas la productivité de l'entreprise. Elles ont besoin d'un moyen simple et direct d'accéder à Internet qui correspond à leur activité, mais ne souhaitent pas une solution trop simpliste qui laisserait la place à des failles. À mesure qu'elles ouvrent leurs réseaux et applications pour devenir plus collaboratives, mobiles et engagées, elles doivent s'assurer que cela ne fait pas de leur réseau une cible facile par rapport aux menaces de sécurité telles que les accès non autorisés, les virus, les menaces Internet et les logiciels espions. Voici une explication plus détaillée de ces challenges et de l'impact qu'ils peuvent avoir :

- Les solutions utilisant plusieurs périphériques pour fournir un accès Internet et une sécurité complète peuvent être encombrantes et engendrer une augmentation des dépenses.
- Un accès non autorisé peut entraîner pour la société des pertes de données, des interruptions d'activité non programmées, une instabilité au niveau du réseau et des problèmes de responsabilité.
- Des virus peuvent infecter les réseaux de l'entreprise, entraînant des pannes et une perte de revenu.
- Les menaces Internet peuvent vous empêcher de répondre aux normes réglementaires et exigences de conformité.
- Les menaces liées aux e-mails, telles que les courriers indésirables et le phishing, peuvent rendre disponibles des informations critiques et contribuer à une baisse de la productivité des employés.
- Les logiciels espions offrent une vue directe sur votre réseau et vos données, ce qui peut entraîner des vols d'identité et des pertes d'informations professionnelles.
- La technologie et les applications reposant sur le cloud nécessitent une sécurité robuste et un cryptage des données afin que les informations sensibles ne soient pas exposées à ces risques.
- Les entreprises ouvrent de plus en plus leurs réseaux à leurs clients, partenaires et utilisateurs publics via un accès sans fil et visiteur, qui engendre de nouveaux risques potentiels en matière de sécurité.
- La navigation sur des sites Web et réseaux sociaux sans rapport avec votre activité professionnelle et potentiellement dangereux peut entraîner des pertes de productivité, vous exposer aux attaques de virus et de logiciels malveillants, voire à des difficultés juridiques.

La solution

Le dispositif de sécurité de la gamme Cisco ISA500 fournit aux PME une solution tout-en-un permettant un accès Internet sécurisé avec une fonctionnalité UTM (gestion unifiée des menaces) complète, renforcée par la base de suivi SIO de Cisco, que vous pouvez déployer très facilement et qui offre un support VPN pour les employés mobiles ou géographiquement dispersés. Avec ses fonctionnalités complémentaires de pare-feu Zone-Based, de sécurité du contenu et d'accès hautement sécurisé, la solution Cisco ISA500 fait barrage aux menaces avant même qu'elles ne pénètrent votre réseau et ne perturbent l'activité de votre entreprise. La gamme Cisco ISA500 :

- **Fournit une solution tout-en-un pour l'accès et la sécurité Internet.**

- **Protège votre entreprise contre les menaces Internet** : le dispositif Cisco ISA500 fournit des services essentiels de sécurité de périmètre pour une protection complète.
  - **Flux de trafic professionnels validés, visiteurs indésirables écartés** : le dispositif Cisco ISA500 inclut un pare-feu Zone-Based qui vous permet d'appliquer un contrôle flexible et basé sur une stratégie afin de déterminer qui peut accéder à votre réseau. De plus, il prend en charge une zone réseau accessible au public, appelée zone démilitarisée (DMZ), pour héberger en toute sécurité les serveurs de fichiers, les serveurs Web et d'autres serveurs accessibles via Internet, sans exposer aux menaces le réseau LAN interne de l'entreprise.
  - **Blocage et filtrage Internet** : le filtrage des URL et des sites Web en fonction de leur réputation peut être utilisé pour contrôler l'utilisation d'Internet par les employés en bloquant l'accès aux sites dangereux ou inappropriés. Ce contrôle avancé permet de réduire au minimum les menaces de sécurité via Internet, tout en améliorant la productivité des employés et en limitant le risque de procédures légales impliquant les employés exposés à du contenu choquant.
  - **Antivirus** : la technologie avancée sur laquelle repose l'antivirus passerelle exploite des flux de données actualisés pour protéger les ressources de votre réseau interne contre les virus les plus répandus et les plus actifs, au niveau le plus critique de votre infrastructure, la passerelle Internet. Le filtrage du trafic Web et des e-mails à la périphérie permet d'éviter les tâches chronophages et coûteuses de nettoyage après contamination, et d'assurer la continuité des activités.
  - **Anti-logiciel espion** : le blocage des logiciels espions les plus répandus et les plus actifs au niveau de la passerelle empêche ces derniers de pénétrer dans votre réseau via le trafic Internet (HTTP et FTP) et les e-mails, et évite les procédures coûteuses de suppression des logiciels espions tout en améliorant la productivité des employés.
  - **Limitation des courriers indésirables** : la solide fonction de filtrage des courriers indésirables basé sur la réputation permet de rétablir l'efficacité des e-mails afin d'assurer une communication ininterrompue avec les clients, fournisseurs et partenaires.
  - **Protection contre le phishing** : la protection contre le vol d'identité permet d'éviter les attaques de phishing, empêchant ainsi les employés de dévoiler par inadvertance des informations professionnelles ou personnelles, ce qui pourrait entraîner des pertes financières.
  - **Prévention active des intrusions et blocage des communications poste-à-poste dangereuses** : les fonctionnalités du système de prévention des intrusions (IPS) de la solution Cisco ISA500 sont capables d'identifier les éventuelles intrusions au sein du réseau professionnel et d'agir pour y mettre fin, et éviter ainsi tout risque supplémentaire. En outre, la gamme Cisco ISA500 peut bloquer le trafic poste-à-poste et les messageries instantanées, et réaliser une inspection de protocole pour améliorer la sécurité réseau, optimiser la productivité du personnel et laisser le réseau disponible pour le trafic de l'entreprise.
  - **Inclusion de la base SIO de Cisco pour une protection inégalée contre les menaces** : le dispositif Cisco ISA500 utilise les 75 To par jour de télémétrie des menaces fournis par la base SIO pour permettre une surveillance globale des menaces, combinée à la protection contre les menaces locales. Vous êtes ainsi protégé contre les attaques sophistiquées et disposez d'une protection étendue contre les menaces.

- **Protection contre les menaces internes et gestion du contrôle des accès** : pour protéger votre entreprise contre les menaces internes, le dispositif de sécurité Cisco ISA500 fournit un pare-feu Zone-Based et des services de sécurité, notamment un système de protection contre les intrusions (IPS) et des antivirus. Il contribue à protéger les environnements sans fil via un support LAN sans fil (WLAN) avec une authentification sécurisée et une gestion solide de l'accès des visiteurs.
- **Redondance WAN** : la solution Cisco ISA500 fournit une redondance WAN qui prend en charge le basculement, l'équilibrage de charge et le routage PBR (Policy-Based Routing) afin de permettre la continuité de l'activité en cas de panne liée à la connexion Internet ou directement au niveau du FAI.
- **Accès VPN sécurisé** : la solution Cisco ISA500 permet aux employés mobiles et distants d'établir une connexion sécurisée au VPN à l'aide du cryptage IPsec ou SSL. Une connexion VPN IPsec site-à-site est parfaite pour sécuriser la communication entre les agences et pour fournir un accès complet au réseau. Les travailleurs mobiles peuvent utiliser Cisco AnyConnect™ ou le client VPN Cisco pour établir une connexion VPN reposant sur le cryptage SSL ou IPsec avec l'agence principale lorsqu'ils travaillent sur un site client, dans un café Internet ou depuis l'aéroport.
- **Connectivité sans fil hautement sécurisée** : pour permettre aux employés d'accéder librement à Internet lorsqu'ils se déplacent au sein des locaux de l'entreprise, certains modèles de la gamme Cisco ISA500 prennent en charge une mobilité hautement sécurisée avec la connexion sans fil 802.11b, g et n dotée du cryptage WPA et de l'authentification 802.11x. La détection des points d'accès indésirables vous permet de limiter le risque d'intrusion par des utilisateurs sans fil non autorisés et de garder le contrôle sur votre infrastructure réseau.
- **Gestion simplifiée basée sur le cloud ou sur un matériel physique avec Cisco OnPlus et l'utilitaire de gestion intégré ISA500** : la solution Cisco ISA500 peut être gérée à l'aide de l'utilitaire intégré de configuration des dispositifs de sécurité. Il s'agit d'une interface de surveillance et de gestion basée sur un navigateur, à la fois puissante et facile à utiliser. Outre les fonctions de gestion et de surveillance, l'utilitaire de configuration fournit des rapports sur l'utilisation du réseau et la sécurité qui permettent aux administrateurs d'analyser facilement et rapidement l'activité et l'état du réseau. Votre partenaire peut également gérer la solution Cisco ISA500 pour vous, si vous optez pour le service Cisco OnPlus™. Cette plate-forme reposant sur le cloud permet d'explorer et de surveiller l'intégralité du réseau d'une petite entreprise. Elle vous permet, en outre, de déléguer les tâches de gestion du réseau à votre partenaire de confiance. Vous êtes ainsi plus disponible pour vous concentrer sur votre cœur de métier. Cisco OnPlus inclut également des services de rapport via ses services de sécurité avancés. Avec les services de sécurité avancés, vos partenaires peuvent générer des rapports sur la sécurité, l'utilisation du réseau et l'état du système, et visualiser des événements tels que les intrusions ou l'utilisation de la bande passante WAN à des intervalles ou à des heures programmés. Ces rapports peuvent être enregistrés dans un fichier PDF, puis partagés par e-mail. La solution Cisco ISA500 fournit donc un ensemble de fonctionnalités et d'options de gestion qui contribuent à un service et à une assistance réseau efficaces, pour une disponibilité accrue de votre réseau et plus de tranquillité.

Les bénéfices pour l’entreprise

La solution Cisco ISA500 vous apporte la sécurité et la connectivité nécessaires pour :

- **Assurer la sécurité de votre entreprise et augmenter le temps d'activité** : appliquez une stratégie complète de sécurité afin de protéger vos processus métiers les plus importants, notamment les activités qui constituent la vitrine de votre société, les sites Web, les services et la communication avec vos clients. Cette sécurité étendue vous permet de préserver l'accessibilité de vos ressources réseau et de vous défendre contre les attaques, tout en augmentant le temps d'activité.
- **Augmenter la productivité des employés** : augmentez la productivité de vos employés en limitant les courriers indésirables et les logiciels espions, et en surveillant les comportements inappropriés de navigation sur Internet. Le contrôle avancé des applications vous permet de réduire au minimum l'utilisation d'applications non professionnelles qui déconcentrent vos employés.
- **Améliorer la résistance de l'entreprise** : mettez en place une solution complète et tout-en-un afin d'éviter que vos applications et services critiques soient perturbés par des failles de sécurité.
- **Réduire les risques en matière de responsabilité** : réduisez l'exposition de votre entreprise à la responsabilité concernant la violation de données ou de contrôles professionnels inappropriés en appliquant un contrôle complet des accès et en mettant en place une protection unique contre les menaces, le tout grâce à des services qui tirent pleinement parti de la base de suivi SIO de Cisco. La fonction avancée de surveillance et d'atténuation des risques vous permet de vous conformer plus efficacement aux normes du secteur et à la réglementation, de protéger les données de vos clients, de préserver vos ressources humaines et toute autre information sensible de l'entreprise.
- **Réduire vos coûts informatiques** : libérez vos ressources consacrées à l'assistance informatique et épargnez-vous le coûteux processus de nettoyage des contaminations par logiciels espions, virus, attaques sophistiquées et autres logiciels malveillants en bloquant toute possibilité d'intrusion.
- **Rester productif grâce à un accès distant sécurisé** : permettez à vos employés et partenaires d'accéder de façon plus sécurisée au réseau depuis leur domicile, lorsqu'ils sont en déplacement ou détachés dans d'autres locaux grâce au support VPN intégré, flexible et facile à utiliser. Avec un accès distant hautement sécurisé et une protection solide de votre contenu, vos employés peuvent accéder aux outils et aux personnes dont ils ont besoin à tout moment et où qu'ils soient pour travailler plus efficacement et répondre plus rapidement aux demandes de leurs clients et collègues. Les employés mobiles peuvent utiliser le client Cisco AnyConnect afin de bénéficier d'un accès VPN intelligent toujours actif, avec une sécurité constante et sensible au contexte, à partir de leur ordinateur portable ou de leur smartphone.
- **Optimiser l'efficacité opérationnelle** : simplifiez l'installation et réduisez les coûts de gestion et de surveillance continue grâce à une interface intuitive basée sur un navigateur et à des assistants de configuration sophistiqués.
- **Assurer votre tranquillité d'esprit** : exploitez au mieux la solution Cisco en souscrivant à notre offre de services pour un prix très abordable. Le service Cisco d'assistance aux PME fournit une assistance au niveau du dispositif étendue à trois ans, afin de protéger vos investissements avec des mises à niveau logicielles, l'accès au Centre d'assistance aux PME et à la Communauté de soutien aux petites entreprises, ainsi que le remplacement du matériel sous 24 heures.

Ces avantages font de la gamme Cisco ISA500 le choix idéal pour répondre à vos besoins de sécurité et permettre à votre réseau et à vos employés d'apporter le maximum de valeur ajoutée à votre entreprise.

Les spécifications des produits

Table 1. Modèles et spécifications des dispositifs de sécurité de la gamme Cisco Small Business ISA500

Fonctionnalités	ISA550	ISA550W	ISA570	ISA570W
Pare-feu				
Débit du filtrage dynamique de paquets [1]	200 Mbit/s	200 Mbit/s	500 Mbits/s	500 Mbits/s
Pare-feu Zone-Based	Oui	Oui	Oui	Oui
Nombre maximal de connexions	15 000	15 000	40 000	40 000
Nombre maximal de règles	100	100	100	100
Nombre de sessions par seconde (cps)	2 500	2 500	3 000	3 000
Planifications	Oui	Oui	Oui	Oui
Protection contre les attaques de type Déni de service (DoS)	Oui	Oui	Oui	Oui
Débit du système IPS [1]	60 Mbits/s	60 Mbits/s	90 Mbit/s	90 Mbit/s
Débit moyen [1]	50 Mbit/s	50 Mbit/s	80 Mbits/s	80 Mbits/s
Débit UTM [1]	45 Mbits/s	45 Mbits/s	75 Mbit/s	75 Mbit/s
VPN				
Débit VPN IPsec (norme de chiffrement de données [DES] / Triple DES [3DES] / norme de chiffrement avancée [AES]) [1]	75 Mbit/s	75 Mbit/s	130 Mbits/s	130 Mbits/s
Tunnels VPN IPSec (site à site)	25	25	100	100
Tunnels d'accès distant VPN IPsec	10	10	75	75
Tunnels VPN SSL	10	10	50	50
Cryptage	DES/3DES/AES (128, 192 et 256 bits)	DES/3DES/AES (128, 192 et 256 bits)	DES/3DES/AES (128, 192 et 256 bits)	DES/3DES/AES (128, 192 et 256 bits)
Authentification	MD5, SHA-1, SHA2 (256, 384 et 512 bits)	MD5, SHA-1, SHA2 (256, 384 et 512 bits)	MD5, SHA-1, SHA2 (256, 384 et 512 bits)	MD5, SHA-1, SHA2 (256, 384 et 512 bits)
DPD (Dead Peer Detection) IPsec	Oui	Oui	Oui	Oui
Traduction d'adresses réseau (NAT Traversal) IPsec	Oui	Oui	Oui	Oui
Diffusion NetBIOS IPsec sur VPN	Oui	Oui	Oui	Oui
Transfert VPN	IPsec/protocole PPTP (Point-to-Point Tunneling Protocol)/protocole L2TP (Layer 2 Tunneling Protocol)	IPsec/PPTP/L2TP	IPsec/PPTP/L2TP	IPsec/PPTP/L2TP
Assistance client VPN Cisco	Oui	Oui	Oui	Oui
Assistance VPN Cisco mode client	Oui	Oui	Oui	Oui
Assistance VPN Cisco mode extension réseau	Oui	Oui	Oui	Oui
Prise en charge de la tunnellisation fractionnée du VPN Cisco	Oui	Oui	Oui	Oui
Assistance client VPN SSL Cisco AnyConnect	Oui	Oui	Oui	Oui
Prise en charge de la tunnellisation fractionnée du VPN SSL	Oui	Oui	Oui	Oui
Certificats VPN SSL	Oui	Oui	Oui	Oui

Fonctionnalités	ISA550	ISA550W	ISA570	ISA570W
Client VPN télétravailleur (Client VPN matériel Cisco)	Oui	Oui	Oui	Oui
Serveur L2TP	Oui	Oui	Oui	Oui
Services de sécurité				
Système de prévention des intrusions (IPS)	Oui	Oui	Oui	Oui
Contrôle des applications	Oui	Oui	Oui	Oui
Filtrage des URL	Oui	Oui	Oui	Oui
Protection contre les menaces du Web	Oui	Oui	Oui	Oui
Anti-hameçonnage	Oui	Oui	Oui	Oui
Antivirus	Oui	Oui	Oui	Oui
Protection contre les logiciels espions	Oui	Oui	Oui	Oui
Filtre de courrier indésirable	Oui	Oui	Oui	Oui
Filtre selon réputation du réseau	Oui	Oui	Oui	Oui
Réseautage				
Affectation d'adresses IP	Statique, protocoles DHCP (Dynamic Host Configuration Protocol), PPPoE (Point-to-Point Protocol over Ethernet), L2TP et PPTP	Statique, protocoles DHCP, PPPoE, L2TP, PPTP	Statique, protocoles DHCP, PPPoE, L2TP, PPTP	Statique, protocoles DHCP, PPPoE, L2TP, PPTP
DHCP	Serveur et relais	Serveur et relais	Serveur et relais	Serveur et relais
VLAN	16	16	16	16
Jonction (802.1Q)	Oui	Oui	Oui	Oui
Traduction d'adresses réseau (NAT)	Oui	Oui	Oui	Oui
Transfert de port	Oui	Oui	Oui	Oui
Déclenchement de port	Oui	Oui	Oui	Oui
Routage	Routage statique et RIP (Routing Information Protocol) v1, v2	Statique, RIP v1, v2	Statique, RIP v1, v2	Statique, RIP v1, v2
DMZ	Oui	Oui	Oui	Oui
WAN double	Oui	Oui	Oui	Oui
Équilibrage de charge	Symétrique	Symétrique	Symétrique	Symétrique
Routage PBR (liaison par protocole)	Oui	Oui	Oui	Oui
Basculement et re-basculement automatique et intégré	Oui	Oui	Oui	Oui
Équilibrage de charge pondéré	Oui	Oui	Oui	Oui
DNS dynamique (DDNS)	Oui	Oui	Oui	Oui
Assistance VoIP (Voice over IP)	SIP, H.323, compatible avec la plupart des passerelles et appareils de communication VoIP	SIP, H.323, compatible avec la plupart des passerelles et appareils de communication VoIP	SIP, H.323, compatible avec la plupart des passerelles et appareils de communication VoIP	SIP, H.323, compatible avec la plupart des passerelles et appareils de communication VoIP
Prise en charge SIP ALG	Oui	Oui	Oui	Oui
Prise en charge ALGP H.323	Oui	Oui	Oui	Oui
QoS	Oui	Oui	Oui	Oui
Mise en file d'attente hiérarchisée stricte	Oui	Oui	Oui	Oui

Fonctionnalités	ISA550	ISA550W	ISA570	ISA570W
Mise en file d'attente WRR (Weighted Round Robin)	Oui	Oui	Oui	Oui
Low Latency Queuing (mise en file d'attente à faible latence)	Oui	Oui	Oui	Oui
Marquage DSCP	Oui	Oui	Oui	Oui
Limitation de débit	Oui	Oui	Oui	Oui
Virtual Router Redundancy Protocol (VRRP)	Oui	Oui	Oui	Oui
Proxy IGMP (Internet Group Management Protocol)	Oui	Oui	Oui	Oui
Surveillance IGMP	Oui	Oui	Oui	Oui
Sans fil				
802.11b/g/n, 2,4 GHz, 2 x 2 MIMO (Multiple Input Multiple Output)	Non	Oui	Non	Oui
SSID multiples	Non	4	Non	4
Qualité de service (QoS) WMM (Wi-Fi Multimedia)	Non	Oui	Non	Oui
Mode d'économie d'énergie automatique non programmé U-APSD (WMM Power Save [WMM-PS])	Non	Oui	Non	Oui
MAC Filtering (Filtrage MAC)	Non	Oui	Non	Oui
WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access), WPA2-PSK (Wi-Fi Protected Access Pre-Shared Key), WPA2-ENT	Non	Oui	Non	Oui
Identifiant BSSID (Basic Service Set Identifier) ou points d'accès virtuels	Non	Oui	Non	Oui
Puissance de transmission ajustable de façon dynamique et manuelle	Non	Oui	Non	Oui
WPS (Wi-Fi Protected Setup)	Non	Oui	Non	Oui
Accès visiteur	Non	Oui	Non	Oui
Portail captif	Non	Oui	Non	Oui
Détection des points d'accès indésirables	Non	Oui	Non	Oui
Administration				
Contrôle automatique des micro-programmes pour détecter une nouvelle version	Oui	Oui	Oui	Oui
Base de données utilisateur locale	100	100	100	100
Authentification	Locale, RADIUS, Active Directory, LDAP (Lightweight Directory Access Protocol)	Locale, RADIUS, Active Directory, LDAP	Locale, RADIUS, Active Directory, LDAP	Locale, RADIUS, Active Directory, LDAP
Diagnostic	Ping, résolution DNS, capture de paquets	Ping, résolution DNS, capture de paquets	Ping, résolution DNS, capture de paquets	Ping, résolution DNS, capture de paquets
Protocoles Discovery	CDP (Cisco Discovery Protocol), Bonjour, service uPnP (Universal Plug and Play)	CDP (Cisco Discovery Protocol), Bonjour, service uPnP	CDP (Cisco Discovery Protocol), Bonjour, service uPnP	CDP (Cisco Discovery Protocol), Bonjour, service uPnP
Journalisation et surveillance	journal local, syslog	journal local, syslog	journal local, syslog	journal local, syslog

Fonctionnalités	ISA550	ISA550W	ISA570	ISA570W
Création de rapports d'avancement	État d'utilisation du réseau, état des services de sécurité, état d'activité du réseau	État d'utilisation du réseau, état des services de sécurité, état d'activité du réseau	État d'utilisation du réseau, état des services de sécurité, état d'activité du réseau	État d'utilisation du réseau, état des services de sécurité, état d'activité du réseau
Caractéristiques matérielles				
Interface totale	7 GE	7 GE	10 GE	10 GE
Ports LAN (10/100/1000)	Jusqu'à 6	Jusqu'à 6	Jusqu'à 9	Jusqu'à 9
Ports WAN (10/100/1000)	Jusqu'à 2	Jusqu'à 2	Jusqu'à 2	Jusqu'à 2
Port DMZ (10/100/1000)	Jusqu'à 4	Jusqu'à 4	Jusqu'à 4	Jusqu'à 4
Ports USB 2.0	1	1	1	1
Format	Montage en rack 1 U Possibilité de montage en rack et mural	Montage en rack 1 U Possibilité de montage en rack et mural	Montage en rack 1 U Possibilité de montage en rack et mural	Montage en rack 1 U Possibilité de montage en rack et mural
Dimensions (l x p x h)	308 mm x 180 mm x 49 mm ou 12,1 po x 7,1 po x 1,9 po (avec patins en caoutchouc)	308 mm x 180 mm x 49 mm ou 12,1 po x 7,1 po x 1,9 po (avec patins en caoutchouc)	308 mm x 180 mm x 49 mm ou 12,1 po x 7,1 po x 1,9 po (avec patins en caoutchouc)	308 mm x 180 mm x 49 mm ou 12,1 po x 7,1 po x 1,9 po (avec patins en caoutchouc)
Poids	1,2 kg	1,3 kg	1,3 kg	1,4 kg
Interrupteur marche/arrêt	Oui	Oui	Oui	Oui
Antennes	Aucune	2	Aucune	2
Température de fonctionnement	De 0 à 40 ºC (de 32 à 104 ºF)	De 0 à 40 ºC (de 32 à 104 ºF)	De 0 à 40 ºC (de 32 à 104 ºF)	De 0 à 40 ºC (de 32 à 104 ºF)
Température de stockage	De –20 à 70 °C (de –4 à 158 °F)	De –20 à 70 °C (de –4 à 158 °F)	De –20 à 70 °C (de –4 à 158 °F)	De –20 à 70 °C (de –4 à 158 °F)
Plage de tensions	100 à 240 V CA	100 à 240 V CA	100 à 240 V CA	100 à 240 V CA
Fréquence d'entrée	50–60 Hz	50–60 Hz	50–60 Hz	50–60 Hz
Tension de sortie	11,4 V ~ 12,6 V	11,4 V ~ 12,6 V	11,4 V ~ 12,6 V	11,4 V ~ 12,6 V
Courant de sortie	1,667 A max.	1,667 A max.	2,5 A max.	2,5 A max.

[1] Méthodologie de test des performances : performances maximales basées sur la norme RFC 2544. Tous les résultats sont en agrégation bidirectionnelle. Les performances réelles peuvent varier en fonction de l'environnement et de la configuration du réseau.

Commande

Table 2. Références produit et licence des dispositifs de sécurité intégrés de la gamme Cisco Small Business ISA500

Produit	SKU
Cisco Integrated Security Appliance 550 avec abonnement sécurité complète pendant un an	ISA550-BUN1-K9
Cisco Integrated Security Appliance 550 avec abonnement sécurité complète pendant un an et sécurité sans fil	ISA550W-BUN1-K9
Cisco Integrated Security Appliance 570 avec abonnement sécurité complète pendant un an	ISA570-BUN1-K9
Cisco Integrated Security Appliance 570 avec abonnement sécurité complète pendant un an et sécurité sans fil	ISA570W-BUN1-K9
Cisco Integrated Security Appliance 550 avec abonnement sécurité complète pendant trois ans	ISA550-BUN3-K9
Cisco Integrated Security Appliance 550 avec abonnement sécurité complète pendant trois ans et sécurité sans fil	ISA550W-BUN3-K9
Cisco Integrated Security Appliance 570 avec abonnement sécurité complète pendant trois ans	ISA570-BUN3-K9
Cisco Integrated Security Appliance 570 avec abonnement sécurité complète pendant trois ans et sécurité sans fil	ISA570W-BUN3-K9

Licence	SKU
Abonnement Cisco sécurité complète pour la gamme ISA550 – 1 an	L-ISA550-CS-1YR=
Abonnement Cisco sécurité complète pour la gamme ISA570 – 1 an	L-ISA570-CS-1YR=
Abonnement Cisco sécurité complète pour la gamme ISA550 – 3 ans	L-ISA550-CS-3YR=
Abonnement Cisco sécurité complète pour la gamme ISA570 – 3 ans	L-ISA570-CS-3YR=

Service et assistance

Le dispositif de sécurité intégré de la gamme Cisco Small Business ISA500 est renforcé par le service Cisco d'assistance aux PME, qui fournit une couverture à prix abordable pour votre tranquillité d'esprit. Ce service peu coûteux, sur abonnement, inclut les mises à niveau et mises à jour logicielles, l'accès étendu au centre Cisco d'assistance aux PME et le remplacement, le cas échéant, du matériel sous 24 heures. Il fournit une assistance communautaire afin de vous permettre de partager vos connaissances et de collaborer avec vos homologues à l'aide de forums en ligne et de sites wiki. Le service Cisco d'assistance aux PME vous permet de réduire les risques, de fournir un meilleur service à vos collaborateurs et clients, tout en bénéficiant d'une tranquillité d'esprit.

Informations complémentaires

Pour en savoir plus sur les dispositifs de sécurité intégrés de la gamme Cisco Small Business ISA500, consultez le site www.cisco.com/go/isa500resources ou contactez votre fournisseur Cisco local. Pour en savoir plus sur Cisco OnPlus, consultez le site www.cisco.com/en/US/products/ps11792/index.html ou contactez votre fournisseur Cisco local.

Pour en savoir plus sur le service Cisco d'assistance aux PME, consultez le site www.cisco.com/cisco/web/solutions/small_business/services/index.html.

Siège social aux États-Unis
Cisco Systems, Inc.
San Jose, Californie

Siège social en Asie-Pacifique
Cisco Systems (USA) Pte. Ltd
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam.
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et numéros de fax sont répertoriés sur le site Web de Cisco, à l'adresse www.cisco.com/go/offices.

Imprimé aux États-Unis C78-717565-00 2/13