Barracuda SecureEdge

Protection des utilisateurs, des sites et des objets et connexion à n'importe quelle application, où qu'elle soit hébergée

SecureEdge fournit un accès sécurisé aux applications, une sécurité basée sur le cloud pour les points de terminaison et une connectivité SD-WAN automatisée pour les sites et les installations industrielles de tout type ou de toutes dimensions. Les utilisateurs distants accèdent directement aux applications depuis tout type d'appareil. L'application Zero Trust, le filtrage des URL et l'optimisation du trafic sur le dernier kilomètre garantissent que l'accès aux applications est toujours sécurisé et optimisé pour tirer le meilleur parti des lignes Internet partagées.

Protection des utilisateurs, des sites et des objets

Barracuda SecureEdge a été conçu dès le départ comme une plateforme de sécurité gérée, présente dans le cloud, et disponible sous forme de services autogérés pour tout type d'appareil, de point de terminaison, de déploiement ou de plateforme.

Issues du vaste réseau Barracuda Threat Intelligence, les informations de sécurité alimentées par l'IA vont au-delà du simple déploiement d'un site ou d'un service cloud en étendant la sécurité avancée à tout utilisateur, sur n'importe quel appareil ou objet connecté.

Connexion de tout appareil, toute application ou tout environnement cloud ou hybride

Les nouvelles solutions Zero Trust ont été uniquement conçues pour sécuriser l'accès aux ressources basées sur le cloud et sont souvent difficiles à configurer, à gérer et à utiliser concrètement.

Aujourd'hui, les utilisateurs exigent un accès sécurisé et fiable à n'importe quelle application, hébergée dans le cloud ou sur site, et quel que soit leur appareil. La solution doit également être ergonomique et améliorer l'accès aux applications pour une expérience utilisateur optimale.

Barracuda SecureEdge Access répond à toutes ces exigences. Disponible pour tous les types d'appareils, toutes les plateformes et sur tous les clouds ou sur site, elle utilise les fonctionnalités SD-WAN locales des appareils et optimise le flux d'applications pour une expérience des utilisateurs à distance inégalée.

Facile à acquérir, à déployer et à exploiter

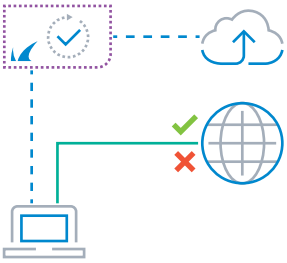
La plateforme Barracuda SecureEdge est une solution SASE à fournisseur unique qui intègre et automatise intelligemment ses composants. Les services de base sont disponibles en tant que SaaS dans Azure Virtual WAN ou bien en tant qu'instances privées. Tous sont gérés via la même interface Web facile à utiliser.

La connectivité du site est assurée par le déploiement sans intervention d'un dispositif sur site avec optimisation SD-WAN automatique vers le service.

Les utilisateurs distants, quel que soit leur système d'exploitation, s'inscrivent eux-mêmes auprès de SecureEdge Access Agent, disponible sur tous les app stores et pouvant être installé simultanément sur un maximum de 10 appareilspar utilisateur pour l'accès réseau Zero Trust (ZTNA) et l'accès Internet sécurisé (SIA).

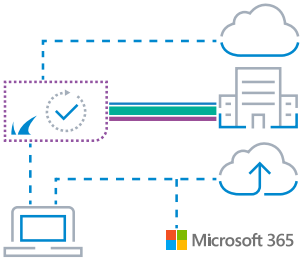
Tous les appareils du site se déploient rapidement sans contact et se connectent automatiquement aux services cloud. Ils optimisent le trafic de liaison montante vers le cloud via la réduction des pertes de paquets et d'autres fonctions avancées d'optimisation du SD-WAN qui évitent aux entreprises les frais élevés des lignes Internet.

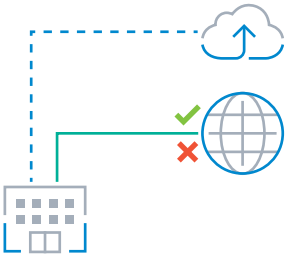
Exemples de cas d'utilisation de la plateforme SASE



Accès sécurisé à Internet (SIA) pour les utilisateurs mobiles
Aujourd'hui, de nombreux employés travaillent de manière fluide entre les sièges sociaux, les succursales, les bureaux à domicile et en déplacement. Et pourtant, le niveau des politiques de sécurité de l'entreprise, par exemple, pour un accès Web acceptable, doit être identique. Optimisées par le vaste réseau Barracuda Threat Intelligence, les informations de sécurité dérivées de l'IA, l'agent SecureEdge Access étend la sécurité et la conformité aux politiques à tout appareil sur n'importe quelle plateforme.

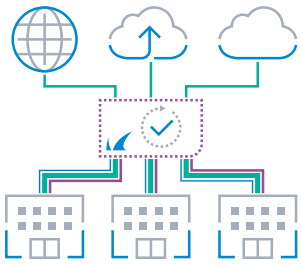
Accès sécurisé aux applications privées et SaaS (ZTNA)
Fournissez un accès direct et sécurisé à toutes les applications approuvées avec une sécurité continue et une évaluation de l'admissibilité, quel que soit l'endroit où les applications sont hébergées, pour tout utilisateur et sur n'importe quel appareil. Optimisez le trafic réseau last-mile pour tirer le meilleur parti des liaisons montantes partagées sur Internet.

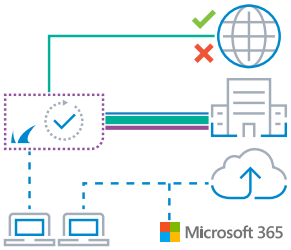




Passerelle Web sécurisée (SWG) pour les bureaux et les succursales
Les appareils du site SecureEdge protègent la périphérie du bureau et tout appareil du bureau des malwares, des spywares et d'autres contenus indésirables transmis sur Internet. Outre la détection de code malveillant, cela inclut le filtrage d'URL et le contrôle des applications pour des milliers d'applications populaires (même celles qui ne sont pas basées sur le Web). L'application peut être effectuée sur l'appareil ou dans la couche de service SecureEdge.

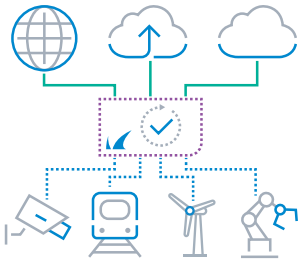
Connectivité et sécurité des bureaux dans le cloud
Connectez en toute sécurité n'importe quelle succursale au cloud et assurez-vous qu'elle est protégée des menaces sur Internet telles que les malwares, les ransomwares et les spywares. Le SD-WAN sécurisé fournit un accès au cloud pour des performances optimales des applications.





Firewall-as-a-service (FWaaS)
Les fonctionnalités de firewall nouvelle génération sont fournies à n'importe quel site ou n'importe quel client par un service cloud. Cela comprend les contrôles d'accès au réseau, le contrôle des applications, le filtrage Web, la prévention avancée des menaces, le système de prévention des intrusions (IPS) et l'inspection SSL/TLS en profondeur.

Sécurité, connectivité et accès à distance ZTNA pour les objets (IoT/ICS)
Sécurisez et connectez les appareils industriels au cloud de votre choix ou à vos locaux. Fournissez un accès sécurisé basé sur ZTNA aux appareils industriels, quel que soit leur emplacement.



Points forts de la solution Barracuda SecureEdge

Déploiement facile : Les agents SecureEdge Access, disponibles pour un maximum de 10 appareils par utilisateur simultanément, peuvent facilement être déployés à l'aide d'un enregistrement individuel ou groupé avec la gestion des appareils mobiles. Les Access Agents sont disponibles pour Windows, macOS, iOS, Android et Linux.

Optimisation last-mile : L'optimisation intégrée du trafic Internet, du service à l'agent SASE, permet aux points de terminaison d'utiliser davantage la bande passante disponible sur les lignes Internet partagées pour améliorer la performance des applications. La technologie sous-jacente pour remédier à la perte de paquets est basée sur des codes de réseau linéaire aléatoire (RLNC), un système d'encodage puissant. Ces algorithmes réagissent bien plus rapidement aux pertes et sont capables d'y remédier plus vite en temps réel, ce qui réduit le nombre de retransmissions de paquets nécessaire et les frais généraux des appareils.

Mise en réseau basée sur l'intention et gestion des politiques : Auparavant, les solutions de sécurité étaient compliquées à utiliser ou dépourvues de leurs fonctions de sécurité sous-jacentes. Les firewalls et autres solutions de sécurité reposaient sur l'attribution de réseaux, de plages d'adresses IP et de fonctions de sécurité des produits ponctuels à ces réseaux. Les opérations basées sur l'intention sont conçues en tant qu'élément du concept de SecureEdge Manager pour notre plateforme SASE unifiée. La plateforme SASE Barracuda SecureEdge est réservée aux utilisateurs, aux groupes et aux applications. Les utilisateurs distants peuvent ainsi accéder aux applications de cloud privé et public, et à Internet beaucoup plus rapidement.

Gestion basée sur les intentions « unique » : En plus des milliers d'applications prédéfinies proposées, la plateforme SASE SecureEdge vous permet de créer des applications privées qui peuvent être hébergées n'importe où. C'est rapide et facile et ne doit être fait qu'une seule fois, puis partagé avec les définitions des politiques de sécurité, SD-WAN et ZTNA. Toutes les optimisations de réseau et de routage nécessaires sont effectuées de manière totalement transparente en arrière-plan et appliquées automatiquement à chaque site, utilisateur ou instance de service.

Connectivité Zero-Touch pour tous les sites : L'intégration des sites et des objets de la plateforme SASE Barracuda SecureEdge ne pourrait être plus simple. En quelques clics seulement, votre configuration dans le gestionnaire basé sur le cloud est terminée et les appareils du site sont envoyés à l'emplacement distant. Le déploiement sans intervention connecte automatiquement les sites et les appareils IoT au point d'entrée SecureEdge le plus proche.

SD-WAN automatique : Une fois connecté et activé, chaque appareil du site utilise automatiquement toutes les liaisons montantes disponibles pour se connecter au service SASE. Avec les paramètres de politique SD-WAN prédéfinis pour des milliers d'applications métiers courantes, les appareils garantissent que le meilleur chemin de liaison montante est toujours utilisé pour l'application.

Sécurité Web avancée : Protéger votre réseau et vos utilisateurs distants des menaces en ligne n'a jamais été aussi simple. Que les employés soient au bureau derrière un appareil, qu'ils travaillent à domicile ou n'importe où ailleurs, SecureEdge examine le trafic Web et bloque l'accès aux sites Web dangereux. Les règles de l'entreprise en matière de navigation sur Internet sont appliquées à des niveaux ultra-précis. La visibilité sur le trafic Web chiffré SSL/TLS et des filtres de mots clés suspects offrent une visibilité sans précédent sur ce qui se passe dans votre organisation.

Connectivité optimisée, partout et à tout moment : Chaque appareil sur site SecureEdge et SecureEdge Access Agent optimise le trafic réseau pour fournir la meilleure latence et la meilleure bande passante possibles aux applications hébergées dans le cloud. La bande passante physique disponible pour les liaisons montantes est souvent fournie sur un support partagé. Les méthodes intégrées de correction des erreurs directes basées sur les codecs RLNC assurent une utilisation optimale de la bande passante disponible par rapport aux autres composants sur le support partagé. SecureEdge permet d'étendre de façon efficace les avantages du SD-WAN aux sites comportant des utilisateurs distants à liaison montante unique.

Option de déploiement du Service Edge : Le service SASE Barracuda SecureEdge est disponible en tant que service SaaS directement géré par Barracuda Networks ou en tant que SecureEdge pour Virtual WAN dans Microsoft Azure et géré par Microsoft, ou encore en tant qu'appliances virtuelles et matérielles à gérer et à héberger par le client ou le partenaire de confiance. Quel que soit le type de déploiement, toute la gestion de la configuration basée sur l'intention s'effectue à partir du portail cloud SecureEdge Manager. Le service se charge ensuite de propager et d'appliquer les modifications à chaque périphérie de service, site, utilisateur ou objet.

Fournisseur unique : La plateforme Barracuda SecureEdge est la seule solution à offrir la sécurité et la connectivité des utilisateurs, des sites et des objets dans un format ergonomique basé sur le cloud qui intègre des technologies autrement disparates, comme SD-WAN pour accéder aux sites et la sécurité et la connectivité pour les objets et la sécurité industrielle, dans une plateforme unique.

Points forts des fonctionnalités Barracuda SecureEdge

Gestion générale et centralisée

- Toutes les fonctionnalités sont gérées de manière centralisée via SecureEdge Manager basé sur le cloud
- Langues de gestion disponibles : Anglais, Allemand, Français, Japonais
- Compatible Azure AD pour les opérations basées sur l'utilisateur
- Déploiement sans intervention pour les appareils sur site
- Autoprovisionnement (installation) pour l'agent SecureEdge Access
- Déploiements haute disponibilité faciles à configurer
- Environnements IoT industriels faciles à intégrer via les appliances Barracuda Secure Connector
- Capacités multi-tenant
- Plusieurs espaces de travail par locataire
- Abonnement au service Edge public SecureEdge disponible via Barracuda Networks dans 26 régions sur tous les continents
- Services Edge privés SecureEdge disponibles fournis avec l'appareil du site SecureEdge ou CloudGen Firewall, gérés via SecureEdge Manager
- Service Edge SecureEdge disponible avec Azure Virtual WAN, géré via SecureEdge Manager

Rapports et visibilité

- Tableaux de bord personnalisables avec widgets détaillés pour (extrait) :
  - Advanced Threat Protection
  - État de configuration de l'appareil
  - Risques liés aux applications
  - Etat du service Edge
  - Données géographiques des sources et destinations
  - Incidents IPS et événements récents
  - État des appareils
  - Carte SD-WAN et état des tunnels
  - ZTNA autorisé/bloqué (utilisateur, application, URL, domaine)
  - Carte des appareils ZTNA
- Connexions en direct : visibilité du trafic pour chaque site et service Edge SecureEdge avec filtrage avancé
- Connexions récentes : visibilité historique du trafic de session pour chaque site et le service Edge SecureEdge avec filtrage avancé pour un dépannage rapide
- Firewall Report Creator (inclus) pour des rapports personnalisés illimités sur plusieurs sites et services
- Intégration à Barracuda XDR
- Intégration à Azure Log analytics pour tous les appareils sur site et les services Edge

Sécurité Web et accès Internet sécurisé

Filtrage de contenu

- Inspection SSL/TLS
- Filtrage des URL par catégorie, catégorie personnalisée, domaine
- Catégories personnalisées
- Application du mode SafeSearch
- Blocage des publicités
- Contrôle et blocage des applications pour des milliers d'applications Web courantes

Création de politique avancée

- Stratégie par défaut personnalisable pour tous les utilisateurs et tous les sites
- Exceptions aux règles de gestion des utilisateurs, des groupes, du réseau et du site
- Catégories personnalisées et blocage de pages
- Règles de blocage, d'autorisation, d'alerte et de notification

Advanced Threat Protection

- Intégration au service Barracuda ATP
- Protection contre :
  - Ransomware
  - Menaces persistantes avancées
  - Virus polymorphes
  - Malware zero-hour

Surveillance du web

- Surveillance des réseaux sociaux
- Surveillance des mots clés personnalisés
- Alertes sur
  - Mots-clés suspects
  - Mots-clés de cyberharcèlement
  - Mots clés liés au terrorisme

Accès Internet sécurisé, filtrage à distance

- SecureEdge Access Agent pour Windows, macOS, iOS, Android et Linux
- Filtrage DNS local
- Application de la posture de sécurité des clients
- Inspection de sécurité sélective définie par l'utilisateur pour tout type de service Edge SecureEdge (SaaS, Azure, privé ou déploiements CloudGen Firewall existants)

CASB

- Support CASB basé sur proxy pour des centaines d'applications professionnelles (ex., Microsoft Office 365, Netsuite, SAP, etc.)

Connectivité et SD-WAN

- Déploiement sans intervention pour les appareils sur site
- Auto-inscription sans intervention à SecureEdge Access Agent
- Règles SD-WAN automatiques pour des centaines d'applications
- Sélection optimisée de liaisons Internet directes
- Optimisation de la liaison Internet montante (correction d'erreurs directe) pour les appareils et les clients du site
- Utilisation simultanée de plusieurs liaisons montantes (jusqu'à 16 transports) par connexion SD-WAN
- Détection dynamique de la bande passante
- Sélection du transport selon les performances
- Routage du trafic en fonction des applications
- Équilibrage de session adaptatif entre plusieurs liaisons montantes
- Sélection des applications en fonction du fournisseur
- Épinglage du fournisseur
- Vérification d'état de la liaison montante
- Types de liaisons montantes pris en charge : dynamique, statique, ExpressRoute, Bridge, WAN (modem LTE), PPPoE
- Protocoles de chiffrement : IPsec v2, TINA
- Connectivité utilisateur de point à site (VPN)

ZTNA universel

- SecureEdge Access Agent inviolable pour les plateformes Windows, macOS, iOS, Android et Linux
- Convivialité, apparence et convivialité cohérentes sur toutes les plateformes
- Accès Internet sécurisé intégré sur toutes les plateformes
- Accès intégré basé sur les rôles en fonction des autorisations : utilisateurs/groupes
- Vérifications d'état des appareils intégrées basées sur les règles ZTNA
- Accès ZTNA à n'importe quelle application basée sur TCP/UDP, quel que soit le lieu d'hébergement
- Prise en charge des applications sur n'importe quel cloud public et sur site avec l'application SD-WAN Connector
- Prise en charge du trafic entrant pour les applications hébergées sur site derrière les appareils SecureEdge du site et/ou les déploiements CloudGen Firewall
- Règles d'état des appareils : blocage des appareils jailbreakés, verrouillage de l'écran, firewall, antivirus, mises à jour du système d'exploitation, mises à jour de SecureEdge Access Agent obligatoires, chiffrement du disque
- Limitation de l'accès aux applications en fonction du type de système d'exploitation
- Connectivité avant login Windows pour une gestion centralisée des appareils appartenant à l'entreprise
- Gestion des appareils et des utilisateurs inscrits
- Catalogue d'applications pour un accès rapide à des applications prédéfinies directement via les agents SecureEdge Access
- Extension de l'application des règles ZTNA aux campus, succursales et emplacements sur site

Sécurité du site et Firewall-as-a-service

- Inspection et transfert des paquets avec états
- Listes de contrôle d'accès spécifiques à un site ou à un service
- Détection de l'identité des utilisateurs
- Système de détection et de prévention des intrusions (IDS/IPS)
- NAT entrant
- Contrôle et mise en œuvre granulaire des applications
- Interception et inspection des applications chiffrées par SSL/TLS
- ATP, IPS, contrôle des applications et filtrage Web en un seul passage
- Serveur DHCP
- Routes dynamiques et statiques
- Pont réseau
- Prise en charge VLAN
- Domaines personnalisés "forwarded

Connectivité du réseau mondial

- Microsoft Global Network
- Teridion Connect
- Teridion China

Pour plus d'informations sur les fonctionnalités de Barracuda SecureEdge, rendez-vous sur rendez-vous sur barracuda.com.

Caractéristiques techniques

SecureEdge Access Agent

OS	Windows	macOS	Android	iOS / iPadOS	Linux
Versions du système d'exploitation prises en charge [1]	Windows 10 ou version ultérieure	macOS 12 (Monterey) ou version ultérieure	Android 10 ou version ultérieure	iOS/iPadOS 15 ou version ultérieure	Distributions Ubuntu et Fedora actuelles
Inscription en masse par groupe utilisateur, déploiement via MDM	✓	✓	✓	✓	✓
Auto-approvisionnement	✓	✓	✓	✓	✓
Renforcement de l'hygiène cyber des clients	✓	✓	✓	✓	✓
Prise en charge des applications	HTTP/HTTPS et TCP/UDP	HTTP/HTTPS et TCP/UDP	HTTP/HTTPS et TCP/UDP	HTTP/HTTPS et TCP/UDP	HTTP/HTTPS et TCP/UDP
Optimisation last-mile	✓	✓	✓	✓	✓
Filtrage d'URL	✓	✓	✓	✓	✓
Inspection de sécurité sélective	✓	✓	✓	✓	✓
Inviolable	✓	✓[2]	✓[2]	✓[2]	✓
Nombre maximal d'appareils simultanés par utilisateur	10 appareils par utilisateur (sur toutes les plateformes)				

SD-WAN Connector

OS	Windows	Linux
Versions du système d'exploitation prises en charge	Windows 10 (architecture Pro, Server, Intel) Windows 11 (architecture Pro, Server, Intel)	Distributions Ubuntu et Fedora actuelles (éditions Desktop, Server, Cloud) Linux x86_64 générique
Auto-provisionnement en un clic [3]	✓	✓
Chiffrement au service	Propriétaire (chiffrement TINA)	Propriétaire (chiffrement TINA)
Débit maximal [4]	100 Mbit/s à 1 Gbit/s (selon le matériel du serveur)	100 Mbit/s à 1 Gbit/s (selon le matériel du serveur)
Prise en charge plateforme cloud	Tout fournisseur de cloud offrant des services IaaS ou de conteneur pour Windows et Linux	

SecureEdge Edge Service fourni par Barracuda

	Amériques	EMEA	APAC
Disponible pour les régions suivantes	Brésil (Sud), Canada (Centre, Est), États-Unis (Centre, Est, Ouest)	Europe (Nord, Ouest), France, Allemagne, Norvège, Afrique du Sud, Émirats arabes unis, Royaume-Uni (Sud, Ouest)	Asie (Est, Sud-Est), Australie (Centre, Est, Sud-Est), Inde (Centre, Sud), Japon (Est, Ouest), Corée

SecureEdge Edge Service pour Microsoft Azure Virtual WAN

	UNITÉ D'ÉCHELLE MICROSOFT AZURE VIRTUAL WAN							
	2	4	10	20	30	40	60	80
Bande passante disponible	1 Gbit/s	2 Gbit/s	5 Gbit/s s	10 Gbit/s	15 Gbit/s	20 Gbit/s	30 Gbit/s	40 Gbit/s

SecureEdge site devices

	DISPOSITIFS MATÉRIELS SUR SITE									DISPOSITIFS VIRTUELS SUR SITE				
	BUREAU		MONTAGE SUR RACK DE 1U			COMPATIBLE AVEC LES RAILS DIN								
	T100B	T200C	T400C	T600D	T900B	FSC2	FSC3	T93A	T193A	VT100	VT500	VT1500	VT3000	VT5000
Fonctions du Edge Service	✓	✓	✓	✓	✓	-	-	✓	✓	✓	✓	✓	✓	✓
NOMBRE D'UTILISATEURS RECOMMANDÉ (veuillez vous référer à la brochure Spécifications (Anglais) pour des informations détaillées sur les performances)														
Protection contre les menaces	50 á 100	150 á 300	300 á 1 000	1 000 á 4 000	6 000 á 9 000	1 á 10 [5]	1 á 10 [5]	50 á 100	150 á 300	50 á 100	150 á 300	300 á 1 000	1 000 á 4 000	6 000 á 9 000
Sécurité Web uniquement	300	1 000	5 000	10 000	20 000	1 á 10 [5]	1 á 10 [5]	100	150	300	1 000	5 000	10 000	20 000
MATÉRIEL (veuillez vous référer à la brochure Spécifications (Anglais) pour des informations détaillées sur le matériel)														
Version matérielle robuste	-	-	-	-	-	-	✓[6]	✓[6]	✓[6]	-	-	-	-	-
Processeurs virtuels sous licence (virtuel)	-	-	-	-	-	-	-	-	-	2	4	8	10	jusqu'à 32
Cartes réseau en cuivre	5x 1 GbE	12x 1 GbE	8x 1 GbE	10x 1 GbE	8x 1 GbE	4x 1 GbE	4x 1 GbE	2x 1 GbE	5x 1 GbE	-	-	-	-	-
Cartes réseau fibre (SFP)	-	4x 1 GbE	-	8x 1 GbE	8x 1 GbE	-	-	1x 1 GbE	2x 1 GbE	-	-	-	-	-
Cartes réseau fibre (SFP+)	-	-	2x 10 GbE	2x 10 GbE	4x 10 GbE	-		-	-	-	-	-	-	-
Cartes réseau fibre (QSFP+)	-	-	-	-	2x 40 GbE	-	-	-	-	-	-	-	-	-
Cartes réseau virtuelles	-	-	-	-	-	-	-	-	-	5 à 16x	5 à 16x	5 à 16x	5 à 16x	5 à 16x
WiFi (AP / Client)	-	-	-	-	-	✓[7]	✓[9]	-	-	-	-	-	-	-
GSM / UTMS	-	-	-	-	-	✓[8]	✓[10]	-	-	-	-	-	-	-
4G / LTE	-	-	-	-	-	✓[8]	✓[10]	-	-	-	-	-	-	-

Pour plus de détails sur les licences, veuillez consulter la brochure Licensing (Anglais).

1 Barracuda SecureEdge Access Agent fonctionne généralement bien sur les versions antérieures du système d'exploitation, mais il n'est pas officiellement testé ni pris en charge. L'utilisation de versions non prises en charge n'est pas recommandée pour les déploiements en production.

2 Nécessite MDM.

3 Nécessite uniquement une connectivité Internet et un jeton généré via SecureEdge Manager.

4 En fonction du matériel installé et de l'attribution de mémoire ; utilise un thread CPU unique.

5 La sécurité est appliquée au composant du service Edge SecureEdge auquel l'appliance SC est connectée.

6 Appareils sur site sans ventilateur avec une plage de températures de fonctionnement étendue (-20 á +70 °C) spécialement conçus pour les environnements difficiles.

7 Sous-modèles FSC21 et FSC25.

8 Sous-modèles FSC24 et FSC25.

9 Sous-modèles FSC31 et FSC35.

10 Sous-modèles FSC34 et FSC35.

Barracuda
Your journey, secured.