

E10000  
Series

La série SonicWALL® SuperMassive™ E10000 constitue la plate-forme de pare-feu nouvelle génération SonicWALL conçus pour fournir aux vastes réseaux une évolutivité, une fiabilité et une sécurité maximum à des débits multi-gigabits. Développée pour répondre aux besoins des grands comptes, des services publics, des universités et des fournisseurs de services, la série SuperMassive E10000 est idéale pour sécuriser les réseaux d'entreprises, les centres de données et les batteries de serveurs. L'architecture multiprocesseur extrêmement évolutive de SonicWALL associée à sa technologie RFDPI (Reassembly-Free Deep Packet Inspection™) brevetée\* permet à la série SuperMassive E10000 d'opérer les services leaders de contrôle applicatif, de prévention des intrusions, de protection anti-malware et de filtrage SSL à des débits multi-gigabits. Conçue dans un souci d'économie d'énergie, d'espace et de besoins en refroidissement, la série SonicWALL E10000 affiche la meilleure efficacité énergétique (Gbit/s/watt) de l'industrie dans les domaines du contrôle applicatif et de la prévention des menaces.

Le moteur RFDPI (Reassembly-Free Deep Packet Inspection) de SonicWALL analyse chaque octet de chaque paquet, assurant un filtrage exhaustif des contenus de la totalité du flux de données, le tout associé à de hautes performances et une faible latence. Une technologie supérieure aux systèmes dépassés de proxys qui réassemblent les contenus à l'aide de sockets associés à des programmes anti-malware. Ces derniers s'avèrent souvent inefficaces et surchargent la mémoire des sockets, entraînant une forte latence, des performances réduites et des restrictions dans la taille des fichiers. Le moteur RFDPI assure un filtrage complet des contenus en vue d'éliminer les menaces avant que celles-ci n'atteignent le réseau et protège contre des millions de variantes de programmes malveillants, sans aucune restriction que ce soit en termes de taille des fichiers, de performances ou de délais. Le moteur RFDPI effectue également un filtrage exhaustif du trafic chiffré en SSL, ainsi que des applications qui ne passent pas par le proxy, ce qui garantit une protection de bout en bout, quels que soient le mode de transmission ou le protocole utilisé.

L'analyse du trafic applicatif permet de distinguer en temps réel le trafic productif du trafic non productif et de le contrôler à l'aide de règles spécifiques. Le contrôle applicatif peut être opéré au niveau des utilisateurs ou de groupes, sur la base d'horaires et de listes d'exceptions. Toutes les signatures d'applications, d'intrusions et de programmes malveillants sont constamment mises à jour par l'équipe de recherche SonicWALL. De plus, le système d'exploitation évolué de SonicWALL, SonicOS, intègre des outils permettant une identification personnalisée des applications.

L'architecture de la série permet une augmentation quasi linéaire des performances et peut accueillir jusqu'à 96 cœurs de processeurs. Cela équivaut à un débit de plus de 40 Gbit/s pour le pare-feu, de plus de 30 Gbit/s pour le filtrage applicatif et la prévention des intrusions, et de plus de 10 Gbit/s pour la protection anti-malware. Composée des modèles E10100, E10200, E10400 et E10800, la série SuperMassive E10000 peut être mise à niveau sur place et constitue un investissement durable dans une infrastructure de sécurité capable d'évoluer au rythme des exigences en matière de bande passante et de sécurité.

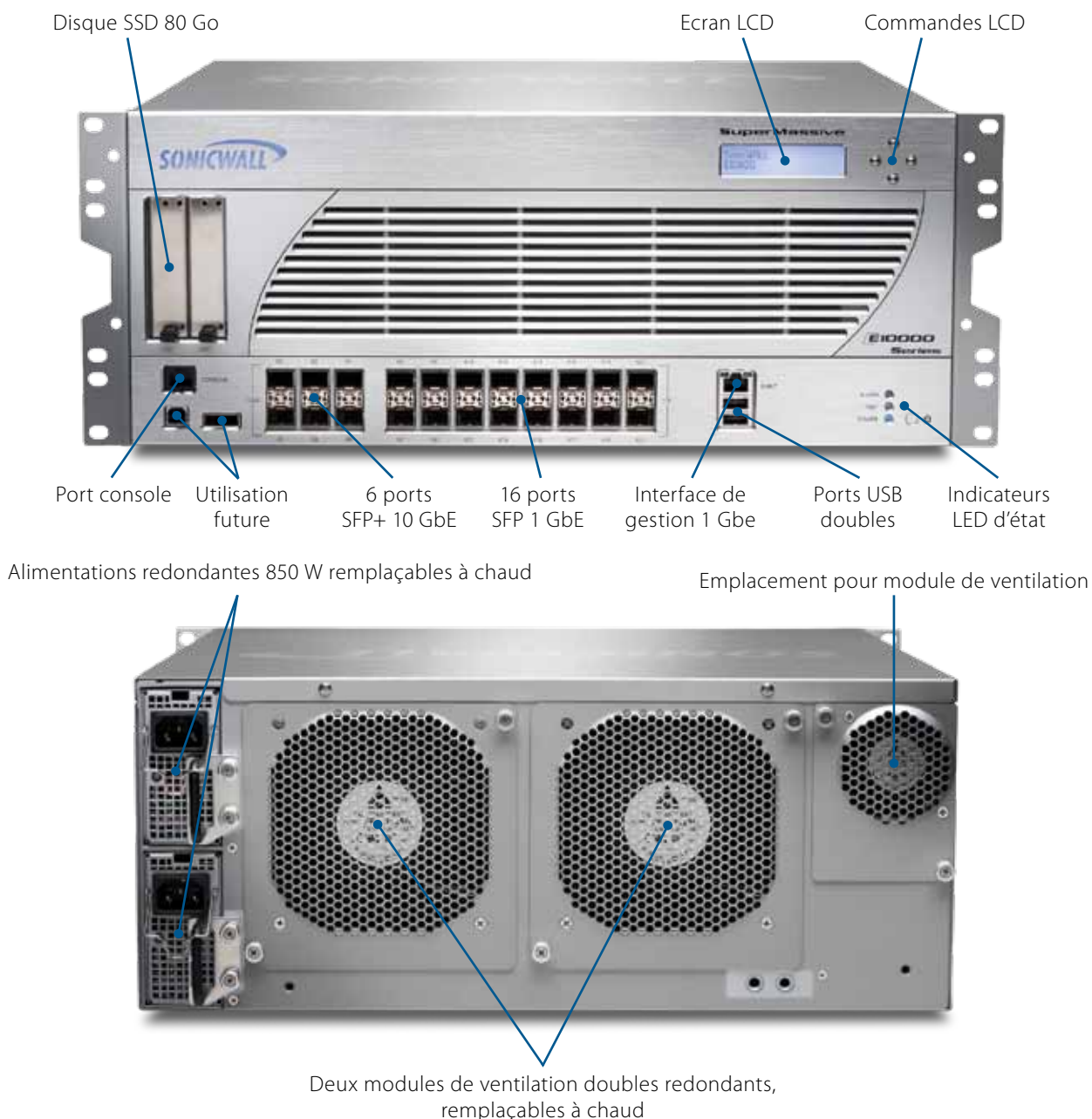
\* Brevets U.S. n° 7,310,815 ; 7,600,257 ; 7,738,380 ; 7,835,361

- Architecture multiprocesseur extrêmement évolutive, conçue pour des infrastructures de 10/40 Gbit/s
- Analyse intelligente, contrôle granulaire et visualisation avancée des applications
- Protection complète incluant une prévention hautes performances des intrusions et une protection anti-malware à faible latence
- Filtrage intégral du trafic chiffré en SSL sans la charge administrative, les délais ni la surcharge de mémoire associés aux proxys SSL basés sur des sockets

LA SÉRIE EN BREF

Le châssis SonicWALL SuperMassive comprend 6 ports SFP+ 10 GbE et 16 ports SFP 1 GbE, des alimentations CA redondantes de 850 W, ainsi que des modules de ventilation doubles, redondants et remplaçables à chaud. Il peut accueillir jusqu'à 96 cœurs de processeurs.

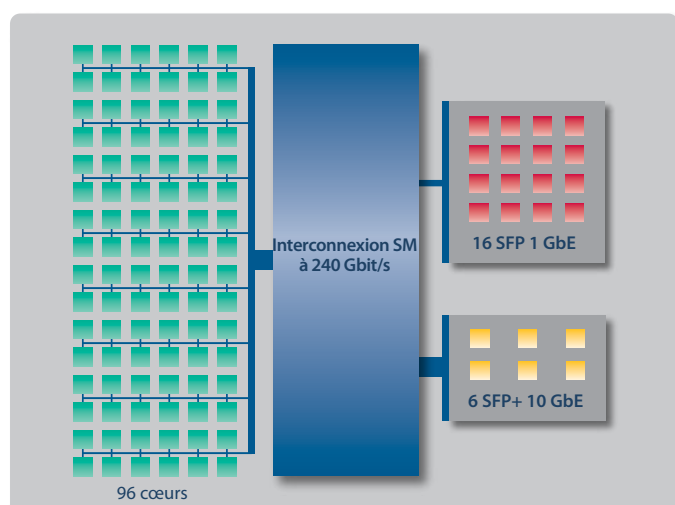
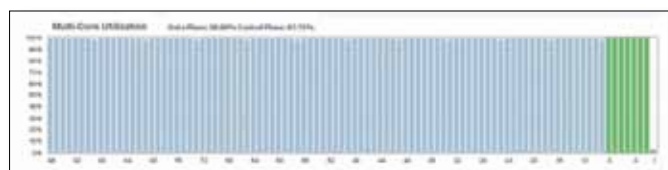
Fonctionnalité	E10100	E10200	E10400	E10800
Cœurs de processeurs	12 (+12, mode HA intégré)	24	48	96
Débit de pare-feu	5,0 Gbit/s	10 Gbit/s	20 Gbit/s	40 Gbit/s
Débit d'Application Intelligence	4,0 Gbit/s	7,5 Gbit/s	15 Gbit/s	30 Gbit/s
Débit IPS	4,0 Gbit/s	7,5 Gbit/s	15 Gbit/s	30 Gbit/s
Débit anti-malware	2,0 Gbit/s	3,0 Gbit/s	6,0 Gbit/s	12 Gbit/s
Nb max. de connexions	1,5 M	3,0 M	6,0 M	12,0 M
Possibilités de mise à niveau	Mise à niveau possible vers E10200	Mise à niveau possible vers E10400	Mise à niveau possible vers E10800	—



## ARCHITECTURE EXTENSIBLE POUR UNE ÉVOLUTIVITÉ ET DES PERFORMANCES MAXIMUM

### Des performances évolutives grâce à l'architecture multiprocesseur

Lors du développement de la série SonicWALL SuperMassive E10000, l'accent a été mis sur des performances élevées, l'évolutivité et la haute disponibilité, dans le but de fournir aux grandes entreprises une plate-forme capable de répondre aux besoins les plus exigeants en matière de sécurité. Cette alliance d'évolutivité et de performances est le fruit du moteur propriétaire RFDPI (Reassembly-Free Deep Packet Inspection) de SonicWALL associé à une architecture multiprocesseur puissante et extrêmement évolutive, capable d'accueillir de manière linéaire un nombre quelconque de cœurs de processeurs. Les entreprises aux besoins croissants en matière de sécurité réseau peuvent mettre à niveau leur système au fur et à mesure et augmenter ainsi les performances disponibles de la plate-forme SuperMassive.



### Conçue pour offrir de hautes performances

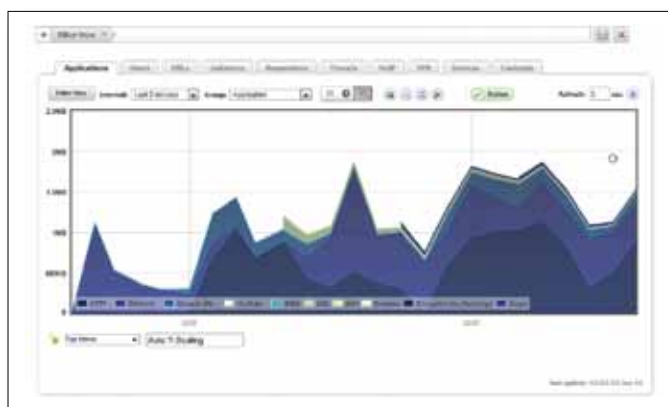
La série SuperMassive E10000 est conçue pour opérer le filtrage applicatif à très faible latence dont les grandes entreprises ont besoin. Le système d'interconnexion SuperMassive fournit une bande passante non bloquante de 240 Gbit/s avec moins d'1  $\mu$ s de latence, garantissant une communication parfaite entre les 96 cœurs de processeurs, les 6 ports SFP+ 10 GbE et les 16 ports SFP 1 GbE.

### Une conception intelligente pour un débit DPI supérieur

Si le filtrage dynamique de paquets reste nécessaire, il n'est plus à lui seul suffisant pour protéger contre les menaces modernes véhiculées par les applications et les contenus. Des fonctionnalités exhaustives de filtrage applicatif, comme le contrôle applicatif, la prévention des intrusions et la protection anti-malware offrent un niveau nettement supérieur de sécurité et de contrôle du réseau, mais elles ne doivent pas pour autant diminuer les performances de ce dernier.

Le moteur breveté\* RFDPI de SonicWALL présente une conception « single-pass » extrêmement efficace qui réunit toutes les fonctionnalités de sécurité au sein d'un moteur d'analyse et de règles unifié, permettant à la plate-forme d'offrir les meilleures performances de filtrage applicatif du marché.

\* Brevets U.S. n° 7,310,815 ; 7,600,257 ; 7,738,380 ; 7,835,361



## CARACTÉRISTIQUES

Application Intelligence and Control	
Caractéristique	Description
Contrôle applicatif	Identification et contrôle d'applications ou d'éléments d'une application sur la base de la technologie RFDPI et non des ports et protocoles connus.
Gestion de la bande passante applicative	Allocation de bande passante aux applications vitales et restriction du trafic d'applications non productives afin d'améliorer l'efficacité et la productivité du réseau.
Identification personnalisée des applications	Création et configuration d'une identification personnalisée des applications sur la base de paramètres du trafic ou de modes de communication propres à une application sur le réseau.
Analyse du trafic applicatif	Livre des informations précises sur la consommation de bande passante, le trafic applicatif et les atteintes à la sécurité, tout en fournissant des services performants de dépannage et d'analyse forensique.
Bibliothèque de signatures d'applications	Bibliothèque constamment enrichie de plus de 3 500 signatures d'applications garantissant que les administrateurs puissent contrôler l'utilisation des toutes dernières applications sur leur réseau au niveau d'une catégorie ou individuel.
Reporting IPFIX/Netflow	Permet d'exporter les données d'utilisation par les protocoles IPFIX ou Netflow à des fins de surveillance vers SonicWALL Scrutinizer ou des outils de surveillance et de reporting tiers. Des données similaires peuvent être exportées par le biais de syslog vers SonicWALL GMS ou SonicWALL Analyzer.
Filtrage applicatif pour SSL	Le trafic SSL est déchiffré et filtré à la recherche de programmes malveillants et d'intrusions par le moteur RFDPI (Reassembly-Free Deep Packet Inspection) en plus des règles de contrôle applications, d'URL et de contenu appliquées sur le trafic potentiellement nuisible.
Suivi des activités des utilisateurs	L'identification des utilisateurs est intégrée de manière transparente aux systèmes d'authentification Microsoft® Active Directory et autres, permettant un suivi et l'établissement de rapports sur l'identification d'utilisateurs individuels.
Identification du trafic par pays GeolP	Identification et contrôle du trafic réseau acheminé ou provenant de certains pays.
Prévention des menaces au niveau de la passerelle	
Anti-malware au niveau de la passerelle	Le moteur propriétaire RFDPI de SonicWALL analyse tous les ports et protocoles à la recherche de virus, sans limitation dans la taille des fichiers ou la longueur des flux. Les chercheurs du laboratoire SonicLabs actualisent en permanence la protection, garantissant des délais de réponse brefs et une prévention plus rapide des intrusions.
Filtrage RFDPI (Reassembly-Free Deep Packet Inspection)	Le filtrage RFDPI (Reassembly-Free Deep Packet Inspection) suit la trace des programmes malveillants indépendamment de l'ordre ou du moment d'arrivée des paquets, ce qui permet de garantir des délais extrêmement brefs, de supprimer les limites de taille des fichiers et des flux et de fournir des performances et une sécurité supérieures à celle des systèmes de proxys dépassés. Ceux-ci réassemblent le contenu à l'aide de sockets associés à programmes antivirus traditionnels qui s'avèrent souvent inefficaces et surchargent la mémoire des sockets, entraînant une forte latence, des performances réduites et des restrictions dans la taille des fichiers.
Cloud Anti-Virus (AV)	Outre sa bibliothèque intégrée, le moteur RFDPI peut également consulter les SonicWALL Cloud Services pour obtenir des compléments d'information sur plus de quatre millions de signatures de programmes malveillants, un chiffre en constante augmentation.
Filtrage bidirectionnel	Le filtrage RFDPI peut être opéré à la fois sur les connexions entrantes et sortantes, garantissant la protection du réseau dans toutes les directions du trafic.
Mises à jour des signatures 24h/24, 7j/7	L'équipe de recherche du laboratoire SonicLabs crée et met à jour des bibliothèques de signatures transmises automatiquement aux pare-feu en service. Ces signatures prennent effet immédiatement, sans redémarrage ni interruption de service.

## Prévention des intrusions

Caractéristique	Description
Analyse à base de signatures	Le service étroitement intégré de prévention des intrusions sur la base de signatures analyse la charge utile des paquets à la recherche de vulnérabilités et d'exploits visant les systèmes internes vitaux.
Mises à jour automatiques des signatures	L'équipe de recherche SonicWALL met à disposition une liste exhaustive et constamment mise à jour de plus de 5 400 signatures IPS couvrant 52 catégories d'attaques. Ces signatures prennent effet immédiatement, sans redémarrage ni interruption de service.
Prévention des menaces en sortie	La possibilité d'inspecter le trafic entrant et sortant garantit que le réseau ne sera pas impliqué involontairement dans des attaques par déni de service distribué (DDoS) et empêche toute communication C&C (commande et contrôle) de botnets.
Protection IPS inter-zone	La prévention des intrusions peut être déployée entre les zones de sécurité interne afin de protéger les serveurs sensibles et prévenir les attaques internes.

## VPN

VPN IPSec pour la connectivité site à site	Le VPN IPSec hautes performances permet à la série SuperMassive E10000 de faire office de concentrateur VPN pour des milliers d'autres sites importants, agences ou postes de télétravail.
Accès distant par VPN SSL ou client IPSec	Vous pouvez utiliser la technologie VPN SSL sans client ou un client IPSec facile à gérer pour accéder simplement à la messagerie électronique, aux fichiers, ordinateurs, pages intranet et applications depuis un vaste éventail de plates-formes.
Passerelle VPN redondante	En présence de plusieurs WAN, il est possible de configurer un VPN primaire et un VPN secondaire afin de permettre un basculement et une reprise automatiques de toutes les sessions VPN, en toute transparence.
VPN à base de routes	La capacité à réaliser un routage dynamique via les liaisons VPN garantit une disponibilité permanente en cas de panne temporaire d'un tunnel VPN : le trafic est réacheminé de manière transparente entre les terminaux par d'autres routes.

## VoIP

Qualité de service (QoS) avancée	Protection des communications vitales grâce au marquage 802.1p et DSCP, ainsi qu'au remappage du trafic VoIP sur le réseau.
Filtrage applicatif du trafic VoIP	Des signatures prédéfinies détectent et bloquent les menaces VoIP spécifiques.
Prise en charge des portiers H.323 et des proxys SIP	Bloque les appels non autorisés ou indésirables en exigeant que tous les appels entrants soient autorisés et authentifiés par le portier H.323 ou le proxy SIP.

## Pare-feu et réseau

Filtrage dynamique de paquets	Tout le trafic réseau est inspecté, analysé et mis en conformité avec les règles d'accès du pare-feu.
Protection contre les attaques DOS	La protection contre les attaques de type SYN Flood prévient les dénis de service à l'aide des technologies SYN proxy (couche 3) et SYN blacklisting (couche 2).
Déploiement flexible	Le déploiement peut se faire en mode NAT traditionnel, en mode pont couche 2, en « Wire Mode » ou en mode TAP réseau.
Routage à base de règles	Crée des routes sur la base de protocoles pour diriger le trafic vers une connexion WAN privilégiée avec capacité à basculer vers un WAN secondaire en cas de panne.

## CARACTÉRISTIQUES

### Pare-feu et réseau (suite)

Caractéristique	Description
Haute disponibilité	Prend en charge le filtrage dynamique actif/passif, le filtrage applicatif actif/actif et le clustering avec basculement actif/actif en vue de garantir non seulement une fiabilité accrue en protégeant contre les pannes matérielles et logicielles, mais aussi des performances accrues par le transfert de la charge de travail RFDPI vers les processeurs disponibles sur les machines de secours.
Équilibrage de charge WAN	Jusqu'à quatre interfaces WAN sont utilisées pour équilibrer la charge selon les méthodes cyclique (Round Robin), par débordement (Spillover) ou suivant le pourcentage (Percentage based).

### Gestion et surveillance

Interface utilisateur Web	Une interface Web intuitive assure une configuration rapide et pratique, en plus de la gestion via SonicWALL GMS® (Global Management System) ou l'interface CLI.
SNMP	SNMP permet de surveiller et de répondre aux menaces et aux alertes.
Netflow/IPFIX	Permet d'exporter un vaste ensemble de données par les protocoles IPFIX ou Netflow pour bénéficier d'informations précises sur la consommation de bande passante, le trafic applicatif et les atteintes à la sécurité, tout en fournissant des services performants de dépannage et d'analyse forensique. Compatible avec SonicWALL Scrutinizer et les applications de surveillance et de reporting de tiers. Des données similaires peuvent être exportées par le biais de syslog vers SonicWALL GMS ou SonicWALL Analyzer.
Gestion centralisée des règles	Le système de gestion globale SonicWALL (GMS®) permet de surveiller, de configurer et d'établir des rapports sur diverses appliances SonicWALL, à partir d'une seule et même interface intuitive, et de personnaliser votre environnement de sécurité en fonction de vos propres règles.

### Récapitulatif des fonctionnalités de SonicOS

#### Pare-feu

- Filtrage RFDPI (Reassembly-Free Deep Packet Inspection)
- Filtrage applicatif pour SSL
- Filtrage dynamique de paquets
- Protection contre les attaques DOS
- Réassemblage TCP
- Mode furtif

#### Contrôle applicatif

- Contrôle applicatif
- Blocage d'éléments d'applications
- Gestion de la bande passante applicative
- Création de signatures d'applications personnalisées
- Visualisation du flux applicatif
- Prévention des fuites de données
- IPFIX avec rapports sur les extensions
- Suivi des activités des utilisateurs
- Identification du trafic par pays GeoIP
- Bibliothèque exhaustive de signatures d'applications

#### Prévention des intrusions

- Analyse à base de signatures
- Mises à jour automatiques des signatures
- Prévention des menaces en sortie
- Liste d'exclusions IPS
- Messages de journalisation avec hyperliens
- Filtrage de contenu unifié et contrôle applicatif avec restriction de bande passante

#### Anti-malware

- Analyse anti-malware au niveau du flux
- Antivirus au niveau de la passerelle
- Anti-spyware au niveau de la passerelle
- Déchiffrement SSL
- Anti-spam
- Filtrage bidirectionnel
- Pas de limites dans la taille des fichiers

#### VPN

- VPN IPSec pour la connectivité site à site
- Accès distant par VPN SSL ou client IPSec
- Passerelle VPN redondante
- VPN à base de routes
- Mobile Connect pour iOS

#### Filtrage de contenu Web

- Filtrage d'URL
- Technologie anti-proxy
- Blocage par mots-clés
- Catégories de classification CFS pour la gestion de bande passante
- Modèle Unified Policy avec contrôle applicatif

#### VoIP

- Qualité de service (QoS) avancée
- Gestion de la bande passante
- Filtrage applicatif du trafic VoIP
- Interopérabilité totale
- Prise en charge des portiers H.323 et des proxys SIP

#### Mise en réseau

- Routage dynamique
- Routage à base de règles

- NAT avancé
- Serveur DHCP
- Gestion de la bande passante
- IPv6
- Agrégation de liens
- Redondance de ports
- Haute disponibilité
- Équilibrage de charge

#### Gestion et surveillance

- Interface utilisateur Web
- Interface en ligne de commande (CLI)
- SNMP
- Reporting via Analyzer
- Reporting via Scrutinizer
- Gestion et reporting via GMS
- Journalisation
- Netflow/IPFIX
- Visualisation applicative
- Écran de gestion LCD
- Gestion centralisée des règles
- Signature unique (SSO)
- Prise en charge Terminal Services/Citrix
- Intégration de l'analyse forensique de Solera Networks

#### Services de sécurité

- Intrusion Prevention Service
- Service anti-malware au niveau de la passerelle
- Content Filtering Service
- Enforced Client Anti-Virus and Anti-Spyware Service
- Application Intelligence, Control and Visualization Service

Spécifications système	E10100	E10200	E10400	E10800
Système d'exploitation	SonicOS			
Cœurs de processeurs	12 (+ 12 HA)	24	48	96
Interfaces 10 GbE	6 x SFP+ 10 GbE			
Interfaces 1 GbE	16 x SFP 1 GbE			
Interfaces de gestion	1 GbE, 1 console			
Mémoire vive	8 Go	16 Go	32 Go	64 Go
Stockage	SSD 80 Go, Flash			
Débit de filtrage pare-feu	5,0 Gbit/s	10 Gbit/s	20 Gbit/s	40 Gbps
Débit de filtrage applicatif	4,0 Gbit/s	7,5 Gbit/s	15 Gbit/s	30 Gbit/s
Débit IPS	4,0 Gbit/s	7,5 Gbit/s	15 Gbit/s	30 Gbit/s
Débit de filtrage anti-malware	2,0 Gbit/s	3,0 Gbit/s	6,0 Gbit/s	12 Gbit/s
Débit VPN	2,5 Gbit/s	5,0 Gbit/s	10 Gbit/s	20 Gbit/s
Connexions/s	80 000/s	160 000/s	320 000/s	640 000/s
Nb max. de connexions (SPI)	1,5 M	3,0 M	6,0 M	12,0 M
Nb max. de connexions (DPI)	1,2 M	2,5 M	5,0 M	10,0 M

### VPN

Tunnels site à site	10 000	10 000 (20 000)*	10 000 (40 000)*	10 000 (80 000)*
Clients VPN IPSec	2 000	2 000 (4 000)*	2 000 (8 000)*	2 000 (16 000)*
Licences VPN SSL	20 (1 000)*	50 (2 000)*	50 (4 000)*	50 (8 000)*
Chiffrement	DES, 3DES, AES (128, 192, 256 bits)			
Authentification	MD5, SHA-1			
Echange de clés	Diffie Hellman Groups 1, 2, 5, 14			
VPN à base de routes	RIP, OSPF			

### Mise en réseau

Attribution d'adresses IP	Statique (client DHCP, PPPoE, L2TP et PPTP), serveur DHCP interne, relais DHCP			
Modes NAT	1:1, plusieurs:1, 1:plusieurs, NAT flexible (chevauchement d'adresses IP), PAT, mode transparent			
Interfaces VLAN	512			
Protocoles de routage	BGP*, OSPF, RIPv1/v2, routes statiques, routage à base de règles, multidiffusion			
QoS	Priorité, bande passante max., garantie, marquage DSCP, 802.1p			
Authentification	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, base de données utilisateurs interne, Terminal Services, Citrix			
IPv6	IPv6 RFDPI, pare-feu, VPN, NAT ; Dual Stack IPv4/IPv6 ; traductions IPv6 de/vers IPv4 ; ICMPv6 ; DHCPv6 ; DNSv6			
VoIP	H323-v1-5 intégral, SIP			
Normes	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Certifications (en instance)	FIPS 140-2, Critères Communs EAL4+, NEBS, ICSA Firewall			

Prise en charge de la carte CAC (Common Access Card)

(en instance)

### Matériel

Alimentation	Double, redondante, remplaçable à chaud, 850 W			
Ventilateurs	Doubles, redondants, remplaçables à chaud			
Affichage	Ecran frontal LCD			
Alimentation d'entrée	100-240 VCA, 60-50 Hz			
Consommation max. (W)	350	400	550	750
Facteur de forme	4U montable en rack			
Dimensions	43x43,5x17,8 cm (17x18x7 in)			
Poids	26,3 kg (58 lb)	26,3 kg (58 lb)	27,7 kg (61 lb)	30,3 kg (67 lb)
Poids DEEE	26,8 kg (59 lb)	26,8 kg (59 lb)	28,1 kg (62 lb)	30,8 kg (68 lb)
Poids de transport	35,8 kg (79 lb)	35,8 kg (79 lb)	37,2 kg (82 lb)	39,9 kg (88 lb)
Conformité aux normes suivantes	FCC classe A, CE, C-Tick, VCCI, MIC, UL, cUL, TÜV/GS, CB, NOM, RoHS, DEEE			
Environnement	5-40 °C, 40-105 °F			
Humidité	10-90 % non condensée			

\*Disponible avec la licence étendue.

Sous réserve de modification des spécifications, des fonctionnalités et de la disponibilité.

## Pare-feu nouvelle génération de la série SuperMassive E10000

## INFOS DE COMMANDE

Produit	Référence
SuperMassive E10100, 6 ports SFP+ 10 GbE, 16 ports SFP 1 GbE, ventilateurs doubles, alimentations CA doubles	01-SSC-8883
SuperMassive E10200, 6 ports SFP+ 10 GbE, 16 ports SFP 1 GbE, ventilateurs doubles, alimentations CA doubles	01-SSC-8882
SuperMassive E10400, 6 ports SFP+ 10 GbE, 16 ports SFP 1 GbE, ventilateurs doubles, alimentations CA doubles	01-SSC-8881
SuperMassive E10800, 6 ports SFP+ 10 GbE, 16 ports SFP 1 GbE, ventilateurs doubles, alimentations CA doubles	01-SSC-8856
Mises à niveau système	Référence
Mise à niveau SuperMassive E10100 vers E10200	01-SSC-9496
Mise à niveau SuperMassive E10200 vers E10400	01-SSC-9497
Mise à niveau SuperMassive E10400 vers E10800	01-SSC-9498
Services E10100	Référence
Prévention des menaces : prévention des intrusions, antivirus et anti-spyware au niveau de la passerelle, Cloud Anti-Virus pour E10100 (1 an)	01-SSC-9500
Application Intelligence and Control : intelligence et contrôle applicatifs et visualisation des flux applicatifs pour E10100 (1 an)	01-SSC-9506
Content Filtering Service Premium Business Edition pour E10100 (1 an)	01-SSC-9503
Support Platinum pour l'appliance SuperMassive E10100 (1 an)	01-SSC-9512
Comprehensive Gateway Security Suite : intelligence applicative, prévention des menaces, filtrage de contenu et support pour E10100 (1 an)	01-SSC-9515
Services E10200	Référence
Prévention des menaces : prévention des intrusions, antivirus et anti-spyware au niveau de la passerelle, Cloud Anti-Virus pour E10200 (1 an)	01-SSC-9518
Application Intelligence and Control : intelligence et contrôle applicatifs et visualisation des flux applicatifs pour E10200 (1 an)	01-SSC-9524
Content Filtering Service Premium Business Edition pour E10200 (1 an)	01-SSC-9521
Support Platinum pour l'appliance SuperMassive E10200 (1 an)	01-SSC-9530
Comprehensive Gateway Security Suite : intelligence applicative, prévention des menaces, filtrage de contenu et support pour E10200 (1 an)	01-SSC-9533
Services E10400	Référence
Prévention des menaces : prévention des intrusions, antivirus et anti-spyware au niveau de la passerelle, Cloud Anti-Virus pour E10400 (1 an)	01-SSC-9536
Application Intelligence and Control : intelligence et contrôle applicatifs et visualisation des flux applicatifs pour E10400 (1 an)	01-SSC-9542
Content Filtering Service Premium Business Edition pour E10400 (1 an)	01-SSC-9539
Support Platinum pour l'appliance SuperMassive E10400 (1 an)	01-SSC-9548
Comprehensive Gateway Security Suite : intelligence applicative, prévention des menaces, filtrage de contenu et support pour E10400 (1 an)	01-SSC-9551
Services E10800	Référence
Application Intelligence and Control : intelligence et contrôle applicatifs et visualisation des flux applicatifs pour E10800 (1 an)	01-SSC-9560
Prévention des menaces : prévention des intrusions, antivirus et anti-spyware au niveau de la passerelle, Cloud Anti-Virus pour E10800 (1 an)	01-SSC-9554
Content Filtering Service Premium Business Edition pour E10800 (1 an)	01-SSC-9557
Support Platinum pour l'appliance SuperMassive E10800 (1 an)	01-SSC-9566
Comprehensive Gateway Security Suite : intelligence applicative, prévention des menaces, filtrage de contenu et support pour E10800 (1 an)	01-SSC-9569
Accessoires	Référence
Ventilateur système (FRU) pour la série SuperMassive E10000	01-SSC-8885
Module ventilateur SSD pour la série SuperMassive E10000	01-SSC-8886
Alimentation (FRU) pour la série SuperMassive E10000	01-SSC-8887



## La gamme SonicWALL de solutions de sécurité dynamique

SÉCURITÉ  
RÉSEAUACCÈS DISTANT  
SÉCURISÉSÉCURISATION WEB  
ET DE MESSAGERIESAUVEGARDE ET  
RÉCUPÉRATIONGESTION  
ET RÈGLES

## SonicWALL France

T +33 1 49 33 73 19 France@sonicwall.com

## SonicWALL BeNeLux

T +32 (0) 15 280 985 Benelux@sonicwall.com

## Contacts du support SonicWALL

www.sonicwall.com/emea/4724.html



DYNAMIC SECURITY FOR THE GLOBAL NETWORK™