

**E10000  
Series**

La serie SuperMassive™ E10000 è la piattaforma di firewall di nuova generazione di SonicWALL® concepita per fornire a grandi ambienti di rete connessioni affidabili, scalabilità e protezione approfondita a velocità multi-gigabit. Sviluppata su misura per le esigenze di aziende, enti statali, università e service provider, la serie SuperMassive E10000 è ideale per la protezione di reti aziendali, data center e server farm. Grazie alla combinazione di una potente architettura multi-core con la brevettata\* tecnologia Reassembly-Free Deep Packet Inspection™ (RFDPI) di SonicWALL, la serie SuperMassive E10000 fornisce eccellenti funzioni di controllo delle applicazioni, prevenzione delle intrusioni, protezione anti-malware e ispezione SSL a velocità multi-gigabit. La serie E10000 di SonicWALL, progettata con particolare attenzione ai requisiti di consumo, ingombro e raffreddamento, offre la migliore efficienza energetica (Gbps/Watt) del settore per il controllo delle applicazioni e la prevenzione delle intrusioni.

Il motore SonicWALL RFDPI (Reassembly-Free Deep Packet Inspection) scansiona ogni byte di ogni singolo pacchetto, ispezionando il contenuto dell'intero flusso di dati ad alta velocità e bassa latenza. Questa tecnologia è superiore agli ormai datati sistemi proxy, che riassemblano il contenuto tramite socket associati a programmi anti-malware con notevoli inefficienze e un eccessivo thrashing per la memoria dei socket, che provoca elevati ritardi, calo di prestazioni e limitazioni alle dimensioni dei file. Il motore RFDPI utilizza l'ispezione completa dei contenuti per eliminare le minacce prima che possano entrare nella rete, proteggendo la rete da milioni di varianti di malware senza alcuna limitazione a livello di dimensioni dei file, prestazioni o latenza. Il motore RFDPI esegue anche l'ispezione completa del traffico crittografato con SSL e di applicazioni che non passano per il proxy, fornendo una solida protezione a prescindere dal tipo di trasporto e dal protocollo.

L'analisi del traffico delle applicazioni consente di identificare in tempo reale il traffico di applicazioni produttive e non produttive, con possibilità di controllarlo tramite potenti policy a livello di applicazione. Il controllo delle applicazioni è impostabile sia per singoli utenti che per gruppi e consente di definire orari pianificati e liste di eccezioni. Tutte le signature relative ad applicazioni, prevenzione delle intrusioni e malware vengono costantemente aggiornate dal team di ricerca di SonicWALL. Inoltre SonicOS, l'avanzato sistema operativo di SonicWALL, fornisce strumenti integrati per personalizzare i metodi d'identificazione delle applicazioni.

L'architettura della serie offre incrementi di prestazioni quasi lineari ed è ampliabile fino a 96 nuclei di elaborazione, fornendo throughput del firewall superiori a 40 Gbps, ispezione delle applicazioni e prevenzione delle intrusioni ad oltre 30 Gbps e protezione anti-malware a una velocità superiore a 10 Gbps. La serie SuperMassive E10000, composta dai modelli E10100, E10200, E10400 e E10800, è ampliabile direttamente in loco e consente di proteggere l'investimento nell'infrastruttura di sicurezza adattandosi alle crescenti esigenze di larghezza di banda e sicurezza della rete.

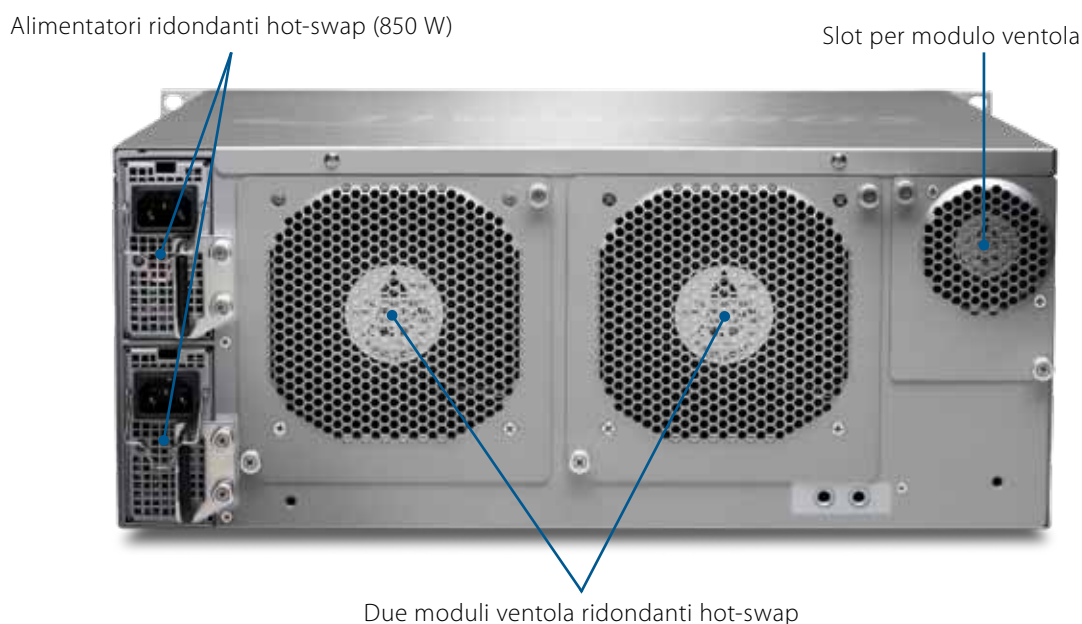
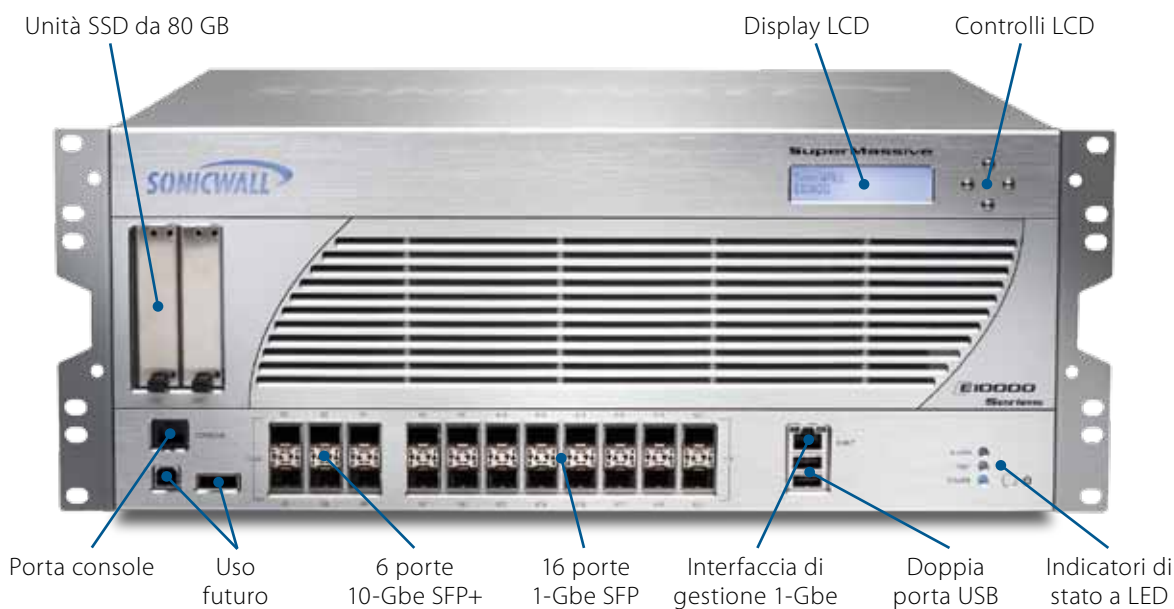
\* Brevetti USA 7,310,815; 7,600,257; 7,738,380; 7,835,361

- **Architettura multicore ad altissima scalabilità progettata per infrastrutture a 10/40 Gbps**
- **Analisi intelligente, controllo granulare e visualizzazione avanzata delle applicazioni**
- **Protezione completa dalle minacce con prevenzione delle intrusioni ad alte prestazioni e protezione anti-malware a bassa latenza**
- **Ispezione completa del traffico crittografato con SSL senza sovraccarichi, ritardi e fenomeni di thrashing associati a proxy SSL basati su socket**

**DESCRIZIONE DELLA SERIE**

Lo chassis di SonicWALL SuperMassive include 6 porte 10-GbE SFP+ e 16 porte 1-GbE SFP, due alimentatori ridondanti da 850 W AC, doppio modulo ventola ridondante hot-swap e massima scalabilità (fino a 96 core di elaborazione).

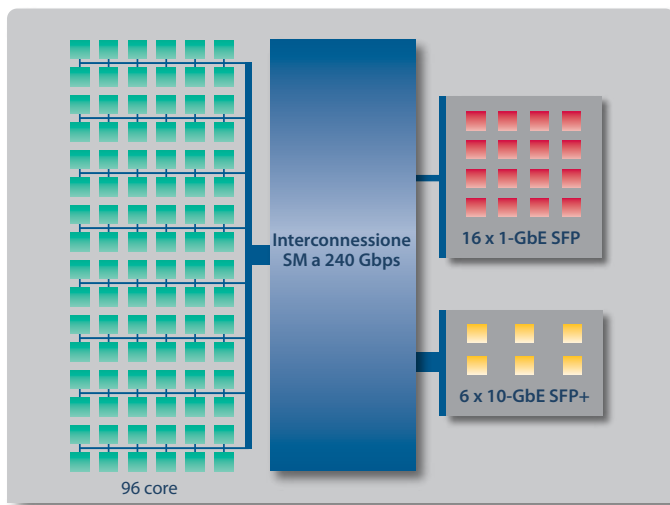
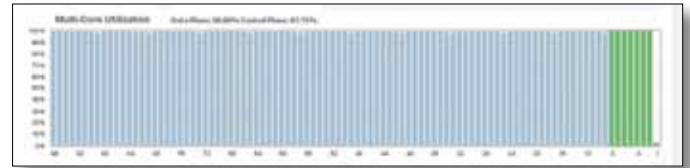
Funzionalità	E10100	E10200	E10400	E10800
Core di elaborazione	12 (+12 in modalità HA integrata)	24	48	96
Throughput firewall	5,0 Gbps	10 Gbps	20 Gbps	40 Gbps
Throughput Application Intelligence	4,0 Gbps	7,5 Gbps	15 Gbps	30 Gbps
Throughput IPS	4,0 Gbps	7,5 Gbps	15 Gbps	30 Gbps
Throughput anti-malware	2,0 Gbps	3,0 Gbps	6,0 Gbps	12 Gbps
Connessioni (max.)	1,5 milioni	3,0 milioni	6,0 milioni	12,0 milioni
Percorso di aggiornamento	Aggiornabile a E10200	Aggiornabile a E10400	Aggiornabile a E10800	—



## ARCHITETTURA AMPLIABILE PER MASSIME PRESTAZIONI E SCALABILITÀ

### Prestazioni scalabili con l'architettura multi-core

La serie SuperMassive E10000 di SonicWALL, progettata con particolare riguardo a prestazioni elevate, scalabilità e alta disponibilità, offre alle grandi aziende una piattaforma adeguata ai loro stringenti requisiti di sicurezza. Questa combinazione di scalabilità e prestazioni è il risultato di un'architettura multi-core potente e altamente scalabile combinata al motore RFDPI (Reassembly-Free Deep Packet Inspection) proprietario di SonicWALL, scalabile linearmente fino a un numero qualsiasi di nuclei di elaborazione. Le aziende con crescenti esigenze di protezione della rete possono aggiornare il proprio sistema nel corso del tempo per aumentare le prestazioni disponibili della piattaforma SuperMassive.



### Concepita per alte prestazioni

La serie SuperMassive E10000 è stata progettata per fornire l'ispezione Deep Packet a bassissima latenza, indispensabile per i grandi ambienti aziendali. Il sistema di interconnessione di SuperMassive fornisce una larghezza di banda non bloccante pari a 240 Gbps con una latenza inferiore a 1  $\mu$ s, garantendo una perfetta comunicazione tra i 96 core di elaborazione e le 6 porte 10-GbE SFP+ / 16 porte 1-GbE SFP.

### Architettura intelligente per un throughput DPI superiore

L'ispezione Stateful Packet è ancora necessaria, ma da sola non è sufficiente per proteggere dalle attuali minacce veicolate tramite applicazioni e contenuti. Le funzioni d'ispezione Deep Packet – controllo delle applicazioni, prevenzione delle intrusioni e anti-malware – offrono un livello di protezione e controllo della rete decisamente superiore, ma non devono provocare un rallentamento della rete.

Il brevettato\* motore RFDPI di SonicWALL con architettura single-pass ad alta efficienza consolida tutte le funzioni di sicurezza in un motore di scansione e controllo delle policy unificato che offre un'ispezione Deep Packet con prestazioni leader del settore.

\* Brevetti USA 7,310,815; 7,600,257; 7,738,380; 7,835,361



**CARATTERISTICHE**

**Application Intelligence and Control**

Funzionalità	Descrizione
Controllo applicazioni	Identificazione e controllo di applicazioni o singoli componenti di un'applicazione mediante la tecnologia RFDPI e non in base al controllo di porte e protocolli conosciuti.
Gestione della larghezza di banda delle applicazioni	Assegnazione della banda ad applicazioni strategiche, con limitazione del traffico di applicazioni non produttive, per una rete efficiente e produttiva.
Identificazione personalizzabile delle applicazioni	Creazione e configurazione di criteri personalizzati per identificare le applicazioni in base a parametri di traffico o a modelli di comunicazione univoci per ogni applicazione.
Analisi del traffico delle applicazioni	Offre alle aziende una visione granulare su traffico delle applicazioni, uso della larghezza di banda e minacce alla sicurezza, integrata da potenti funzioni di risoluzione dei problemi e analisi forense.
Database di signature delle applicazioni	Un database in continua espansione, con oltre 3.500 firme di applicazioni, consente agli amministratori di monitorare l'uso di tutte le più recenti applicazioni nella rete, sia per categoria che a livello singolo.
Reporting IPFIX/Netflow	Esportazione dei dati relativi all'uso delle applicazioni, con i protocolli IPFIX o NetFlow, per il successivo monitoraggio con SonicWALL Scrutinizer o con tool di reporting e monitoraggio di terze parti. Dati simili possono essere esportati in SonicWALL GMS e SonicWALL Analyzer tramite syslog.
Ispezione Deep Packet per SSL	Il traffico SSL viene decifrato e ispezionato alla ricerca di malware e intrusioni tramite il motore Reassembly-Free Deep Packet Inspection (RFDPI). Inoltre vengono applicate policy di controllo delle applicazioni, degli URL e dei contenuti per bloccare le minacce anche più difficili da identificare.
Monitoraggio delle attività degli utenti	Il servizio di identificazione degli utenti, integrabile in modo trasparente con Microsoft® Active Directory e altri sistemi di autenticazione, consente di monitorare le attività di singoli utenti e generare report.
GeoIP – Identificazione del traffico in base al paese	Rilevamento e controllo del traffico di rete proveniente o diretto in paesi specifici.

**Prevenzione delle minacce a livello del gateway**

Gateway Anti-Malware	Il motore RFDPI proprietario di SonicWALL scansiona tutte le porte e i protocolli alla ricerca di virus, senza alcuna limitazione a livello di dimensioni dei file o lunghezza dei flussi di dati. I ricercatori del SonicLabs forniscono costantemente una protezione aggiornata contro le minacce per garantire tempi di risposta e prevenzione più rapidi.
Reassembly-Free Deep Packet Inspection	L'ispezione approfondita dei pacchetti senza riassettaggio tiene traccia del malware indipendentemente dalla sequenza e dai tempi di arrivo dei pacchetti, garantendo una latenza estremamente bassa senza limitazioni sulle dimensioni dei file e dei flussi di dati. In questo modo fornisce migliori prestazioni e una maggiore sicurezza rispetto alla tradizionale architettura proxy, che riassetta il contenuto tramite socket associati a programmi anti-virus tradizionali con notevoli inefficienze e un eccessivo thrashing per la memoria dei socket, che provoca elevati ritardi, calo di prestazioni e limitazioni alle dimensioni dei file.
Cloud Anti-Virus (AV)	Oltre a utilizzare il database integrato, il motore RFDPI consulta anche il SonicWALL Cloud Service per ottenere informazioni aggiuntive su oltre 4 milioni di signature malware.
Ispezione bidirezionale	L'ispezione RFDPI può essere eseguita sulle connessioni in entrata e in uscita dalla rete, garantendo protezione per ogni direzione del traffico.
Aggiornamenti delle signature 24x7	Il team di ricerca del SonicLabs crea e aggiorna i database di signature, che vengono automaticamente inviati ai firewall in uso. Le signature hanno effetto immediato, senza bisogno di riavviare il sistema o interrompere i servizi.

## Prevenzione delle intrusioni

Funzionalità	Descrizione
Scansione basata sulle signature	La prevenzione delle intrusioni integrata e basata sulle signature scansiona i payload dei pacchetti alla ricerca di vulnerabilità ed exploit diretti ai sistemi interni critici.
Aggiornamenti automatici delle signature	Il team di ricerca di SonicWALL aggiorna e distribuisce costantemente un elenco dettagliato di oltre 5.400 signature IPS relative a 52 categorie di attacchi. Queste signature sono immediatamente attive e non richiedono il reboot del sistema o altre interruzioni dei servizi.
Prevenzione delle minacce in uscita	La capacità di ispezionare il traffico sia in entrata che in uscita garantisce che la rete non venga utilizzata a insaputa degli amministratori per attacchi DDoS (Distributed Denial of Service) e impedisce qualsiasi comunicazione tramite canali "Command & Control" di botnet.
Protezione IPS interzona	La prevenzione delle intrusioni può essere implementata tra diverse zone di sicurezza interne per proteggere server con dati sensibili e impedire attacchi interni.

## VPN

VPN IPSec per connettività site-to-site	La VPN IPSec ad alte prestazioni consente alla serie SuperMassive E10000 di operare come un concentratore VPN per migliaia di altri grandi ambienti di rete, home office o sedi distaccate.
Accesso remoto tramite VPN SSL o client IPSec	Possibilità di usare la tecnologia clientless VPN SSL oppure un client IPSec di facile gestione per offrire un accesso semplificato a posta elettronica, file, computer, siti intranet e applicazioni da svariate piattaforme.
Gateway VPN ridondante	Se si utilizzano più WAN è possibile configurare una VPN principale e una secondaria per assicurare failover e failback automatizzati e trasparenti per tutte le sessioni VPN.
VPN route-based	La capacità di eseguire il routing dinamico tramite collegamenti VPN garantisce la continuità delle connessioni in caso di interruzione temporanea del tunnel VPN, con un reinstradamento trasparente del traffico tra gli endpoint attraverso percorsi alternativi.

## VoIP

QoS avanzata	Protezione delle comunicazioni mission-critical tramite tagging 802.1p e DSCP e rimappatura del traffico VoIP sulla rete.
Ispezione deep packet del traffico VoIP	Rilevazione e blocco di minacce specifiche del traffico VoIP mediante signature predefinite.
Supporto per gatekeeper H.323 e proxy SIP	Blocco delle chiamate di spam: tutte le chiamate in entrata devono essere autorizzate e autenticate dal gatekeeper H.323 o dal proxy SIP.

## Firewall e networking

Ispezione Stateful Packet	Tutto il traffico in transito nella rete viene ispezionato, analizzato e conformato alle policy di accesso del firewall.
Protezione da attacchi DoS	La protezione SYN Flood offre una difesa contro gli attacchi DoS mediante tecnologie di blacklisting sia al layer 3 (SYN proxy) che al layer 2 (SYN).
Implementazione flessibile	Possibilità di implementazione nelle tradizionali modalità NAT, Bridge (Layer 2), Wire e Network Tap.
Routing basato sulle policy	Creazione di instradamenti basati sui protocolli per dirigere il traffico verso una determinata connessione WAN, con possibilità di commutare su una WAN secondaria in caso di caduta dell'alimentazione.

## CARATTERISTICHE

### Firewall e networking (continuazione)

Funzionalità	Descrizione
Alta disponibilità	Supporto failover per stateful attivo/passivo, DPI attivo/attivo e clustering attivo/attivo per garantire non solo una maggiore affidabilità con la protezione da errori hardware o software ma anche un aumento di prestazioni, in quanto il carico di lavoro dell'ispezione Reassembly-Free Deep Packet viene assegnato ai core disponibili sulle unità in stand-by.
Bilanciamento del carico WAN	Bilanciamento del carico per un massimo di quattro interfacce WAN con metodi basati sulle modalità round robin, percentuale e spill-over.

### Gestione e monitoraggio

GUI basata sul Web	Un'intuitiva interfaccia basata sul Web consente una configurazione rapida e conveniente, con possibilità di gestione tramite il Global Management System (GMS®) di SonicWALL o l'interfaccia a riga di comando (CLI).
SNMP	SNMP offre la possibilità di monitorare il sistema e reagire prontamente a minacce e allarmi.
Netflow/IPFIX	Mediante i protocolli IPFIX o Netflow è possibile esportare un ampio set di dati per ottenere una visione granulare su traffico delle applicazioni, banda utilizzata e minacce alla sicurezza, insieme a potenti funzioni di risoluzione dei problemi e analisi forense. Compatibile con SonicWALL Scrutinizer e applicazioni di reporting e monitoraggio di terzi. Dati simili possono essere esportati in SonicWALL GMS e SonicWALL Analyzer tramite syslog.
Gestione centralizzata delle policy	Il SonicWALL Global Management System (GMS®) consente di monitorare, configurare e creare report per svariate appliance SonicWALL da un'unica e intuitiva interfaccia, con possibilità di personalizzare il proprio ambiente di sicurezza in conformità alle policy definite.

### Riepilogo delle funzionalità di SonicOS

#### Firewall

- Reassembly-Free Deep Packet Inspection
- Deep Packet Inspection per SSL
- Stateful Packet Inspection
- Protezione da attacchi DoS
- Riassemblaggio TCP
- Modalità Stealth

#### Controllo applicazioni

- Controllo delle applicazioni
- Blocco di componenti delle applicazioni
- Gestione della larghezza di banda delle applicazioni
- Creazione di firme personalizzate per le applicazioni
- Visualizzazione del flusso delle applicazioni
- Prevenzione di fughe di dati
- IPFIX con reporting sulle estensioni
- Monitoraggio delle attività degli utenti
- Identificazione del traffico in base al paese (GeoIP)
- Ampio database di signature delle applicazioni

#### Prevenzione intrusioni

- Scansione basata sulle signature
- Aggiornamenti automatici delle signature
- Prevenzione delle minacce in uscita
- Lista di esclusione IPS
- Messaggi di log interattivi
- CFS unificato e controllo applicazioni con limitazione della larghezza di banda

#### Anti-Malware

- Scansione anti-malware basata sui flussi
- Gateway Anti-Virus
- Gateway Anti-Spyware
- Decrittazione SSL
- Anti-spam
- Ispezione bidirezionale
- Dimensioni illimitate dei file

#### VPN

- VPN IPSec per connettività site-to-site
- Accesso remoto tramite VPN SSL o client IPSec
- Gateway VPN ridondante
- VPN route-based
- Mobile Connect per iOS

#### Filtraggio dei contenuti Web

- Filtraggio URL
- Tecnologia anti-proxy
- Blocco in base a parole chiave
- Gestione della banda secondo categorie di valutazione CFS
- Modello di policy unificato con controllo delle applicazioni

#### VoIP

- QoS avanzata
- Gestione della larghezza di banda
- Ispezione deep packet del traffico VoIP
- Interoperabilità completa
- Supporto per gatekeeper H.323 e proxy SIP

#### Networking

- Routing dinamico

- Routing basato sulle policy
- NAT avanzato
- Server DHCP
- Gestione della larghezza di banda
- IPv6
- Aggregazione dei link
- Ridondanza delle porte
- Alta disponibilità
- Bilanciamento del carico

#### Gestione e monitoraggio

- GUI basata sul Web
- Interfaccia a riga di comando
- SNMP
- Reporting con Analyzer
- Reporting con Scrutinizer
- Gestione policy e reporting con GMS
- Logging
- Netflow/IPFIX
- Visualizzazione delle applicazioni
- Display di gestione LCD
- Gestione centralizzata delle policy
- Single Sign-On
- Supporto Terminal Service/Citrix
- Integrazione con le appliance di analisi di Solera Networks

#### Servizi di sicurezza

- Prevenzione delle intrusioni
- Anti-malware a livello del gateway
- Filtraggio dei contenuti
- Enforced client anti-virus e anti-spyware
- Controllo intelligente e visualizzazione delle applicazioni

Specifiche di sistema	E10100	E10200	E10400	E10800
Sistema operativo	SonicOS			
Core	12 (+ 12 in modalità HA)	24	48	96
Interfacce 10-GbE	6 x 10-GbE SFP+			
Interfacce 1-GbE	16 x 1-GbE SFP			
Interfacce di gestione	1 GbE, 1 console			
Memoria (RAM)	8 GB	16 GB	32 GB	64 GB
Capacità	SSD 80 GB, Flash			
Throughput ispezione firewall	5,0 Gbps	10 Gbps	20 Gbps	40 Gbps
Throughput ispezione applicazioni	4,0 Gbps	7,5 Gbps	15 Gbps	30 Gbps
Throughput IPS	4,0 Gbps	7,5 Gbps	15 Gbps	30 Gbps
Throughput ispezione anti-malware	2,0 Gbps	3,0 Gbps	6,0 Gbps	12 Gbps
Throughput VPN	2,5 Gbps	5,0 Gbps	10 Gbps	20 Gbps
Connessioni al secondo	80.000/sec	160.000/sec	320.000/sec	640.000/sec
Connessioni max. (SPI)	1,5 milioni	3,0 milioni	6,0 milioni	12,0 milioni
Connessioni max. (DPI)	1,2 milioni	2,5 milioni	5,0 milioni	10,0 milioni
<b>VPN</b>				
Tunnel site-to-site	10.000	10.000 (20.000)*	10.000 (40.000)*	10.000 (80.000)*
Client VPN IPSec	2.000	2.000 (4.000)*	2.000 (8.000)*	2.000 (16.000)*
Licenze VPN SSL	20 (1.000)*	50 (2.000)*	50 (4.000)*	50 (8.000)*
Crittografia	DES, 3DES, AES (a 128, 192, 256 bit)			
Autenticazione	MD5, SHA-1			
Scambio delle chiavi	Gruppi Diffie-Hellman 1, 2, 5, 14			
VPN route-based	RIP, OSPF			
<b>Networking</b>				
Assegnazione indirizzo IP	Statica (DHCP, PPPoE, L2TP e client PPTP), server DHCP interno, DHCP relay			
Modalità NAT	1:1, many:1, 1:many, NAT flessibile (IP sovrapposti), PAT, modalità trasparente			
Interfacce VLAN	512			
Protocolli di routing	BGP*, OSPF, RIPv1/v2, route statici, routing basato su policy, multicast			
QoS (Quality of Service)	Priorità larghezza di banda, larghezza di banda massima / garantita, DSCP marking, 802.1p			
Autenticazione	XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, database utenti interno, servizi Terminal Server, Citrix			
IPv6	IPv6 RFDPI, firewall, VPN, NAT; Dual stack IPv4/IPv6; traduzioni IPv6 da/verso IPv4; ICMPv6; DHCPv6; DNSv6			
VoIP	H323-v1-5 completo, SIP			
Standard	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Certificazioni (in attesa)	FIPS 140-2, Common Criteria EAL4+, NEBS, ICSA Firewall			
Supporto CAC (Common Access Card)	In attesa			
<b>Hardware</b>				
Alimentazione	Due alimentatori ridondanti hot-swap, 850 W			
Ventole	Due ventole ridondanti hot swap			
Display	Display LCD anteriore			
Tensione d'esercizio	100-240 VAC, 60-50 Hz			
Potenza max. assorbita (W)	350	400	550	750
Fattore di forma	4U rack-mount			
Misure	43x43,5x17,8 cm			
Peso	26,3 kg	26,3 kg	27,7 kg	30,3 kg
Peso sec. WEEE	26,8 kg	26,8 kg	28,1 kg	30,8 kg
Peso confezione	35,8 kg	35,8 kg	37,2 kg	39,9 kg
Principali normative di conformità	FCC Class A, CE, C-Tick, VCCI, Compliance MIC, UL, cUL, TÜV/GS, CB, NOM, RoHS, WEEE			
Condizioni ambientali	da 5 a 40 °C			
Umidità	10-90%, non condensante			

\*Disponibile con licenza estesa.  
Specifiche, funzionalità e disponibilità soggette a modifiche.

## Firewall di nuova generazione della serie SuperMassive E1000

## INFORMAZIONI PER L'ORDINAZIONE

Prodotto	Codice
SuperMassive E10100, 6 porte SFP+ 10-GbE, 16 porte SFP 1-GbE, due ventole, due alimentatori AC	01-SSC-8883
SuperMassive E10200, 6 porte SFP+ 10-GbE, 16 porte SFP 1-GbE, due ventole, due alimentatori AC	01-SSC-8882
SuperMassive E10400, 6 porte SFP+ 10-GbE, 16 porte SFP 1-GbE, due ventole, due alimentatori AC	01-SSC-8881
SuperMassive E10800, 6 porte SFP+ 10-GbE, 16 porte SFP 1-GbE, due ventole, due alimentatori AC	01-SSC-8856
Aggiornamenti di sistema	Codice
Upgrade da SuperMassive E10100 a E10200	01-SSC-9496
Upgrade da SuperMassive E10200 a E10400	01-SSC-9497
Upgrade da SuperMassive E10400 a E10800	01-SSC-9498
Servizi per E10100	Codice
Prevenzione delle minacce – Prevenzione delle intrusioni, gateway anti-virus, gateway anti-spyware, cloud anti-virus per E10100 (1 anno)	01-SSC-9500
Controllo intelligente delle applicazioni – Application Intelligence, controllo applicazioni, visualizzazione del flusso di applicazioni per E10100 (1 anno)	01-SSC-9506
Content Filtering, edizione Premium Business per E10100 (1 anno)	01-SSC-9503
Supporto Platinum per SuperMassive E10100 (1 anno)	01-SSC-9512
Comprehensive Gateway Security Suite – Application Intelligence, prevenzione delle minacce, filtraggio dei contenuti con supporto per E10100 (1 anno)	01-SSC-9515
Servizi per E10200	Codice
Prevenzione delle minacce – Prevenzione delle intrusioni, gateway anti-virus, gateway anti-spyware, cloud anti-virus per E10200 (1 anno)	01-SSC-9518
Controllo intelligente delle applicazioni – Application Intelligence, controllo applicazioni, visualizzazione del flusso di applicazioni per E10200 (1 anno)	01-SSC-9524
Content Filtering, edizione Premium Business per E10200 (1 anno)	01-SSC-9521
Supporto Platinum per SuperMassive E10200 (1 anno)	01-SSC-9530
Comprehensive Gateway Security Suite – Application Intelligence, prevenzione delle minacce, filtraggio dei contenuti con supporto per E10200 (1 anno)	01-SSC-9533
Servizi per E10400	Codice
Prevenzione delle minacce – Prevenzione delle intrusioni, gateway anti-virus, gateway anti-spyware, cloud anti-virus per E10400 (1 anno)	01-SSC-9536
Controllo intelligente delle applicazioni – Application Intelligence, controllo applicazioni, visualizzazione del flusso di applicazioni per E10400 (1 anno)	01-SSC-9542
Content Filtering, edizione Premium Business per E10400 (1 anno)	01-SSC-9539
Supporto Platinum per SuperMassive E10400 (1 anno)	01-SSC-9548
Comprehensive Gateway Security Suite – Application Intelligence, prevenzione delle minacce, filtraggio dei contenuti con supporto per E10400 (1 anno)	01-SSC-9551
Servizi per E10800	Codice
Controllo intelligente delle applicazioni – Application Intelligence, controllo applicazioni, visualizzazione del flusso di applicazioni per E10800 (1 anno)	01-SSC-9560
Prevenzione delle minacce – Prevenzione delle intrusioni, gateway anti-virus, gateway anti-spyware, cloud anti-virus per E10800 (1 anno)	01-SSC-9554
Content Filtering, edizione Premium Business per E10800 (1 anno)	01-SSC-9557
Supporto Platinum per SuperMassive E10800 (1 anno)	01-SSC-9566
Comprehensive Gateway Security Suite – Application Intelligence, prevenzione delle minacce, filtraggio dei contenuti con supporto per E10800 (1 anno)	01-SSC-9569
Accessori	Codice
Ventola di sistema (FRU) per la serie SuperMassive E10000	01-SSC-8885
Modulo ventola SSD per la serie SuperMassive E10000	01-SSC-8886
Alimentatore (FRU) per la serie SuperMassive E10000	01-SSC-8887



## Linea di soluzioni di sicurezza dinamica SonicWALL



SICUREZZA  
DI RETE



ACCESSO  
REMOTO SICURO



SICUREZZA  
WEB / E-MAIL



BACKUP E  
RECOVERY



GESTIONE  
BASATA SU POLICY

**SonicWALL Italy**  
T + 39.010.7407851  
Italy@sonicwall.com

**Contatti Supporto SonicWALL**  
[www.sonicwall.com/emea/4724.html](http://www.sonicwall.com/emea/4724.html)

**SONICWALL**®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™