Serie SonicWall SuperMassive

Protezione firewall di nuova generazione ad alte prestazioni e senza compromessi per le reti aziendali.

La serie SonicWall SuperMassive è la piattaforma firewall di nuova generazione (NGFW) di SonicWall progettata per reti di grandi dimensioni, in grado di fornire scalabilità, affidabilità e sicurezza in profondità a velocità multi-gigabit con latenza quasi nulla.

Creata per soddisfare le esigenze di imprese, enti pubblici, istituti d'istruzione, aziende sanitarie e fornitori di servizi, la serie SuperMassive è la soluzione ideale per proteggere reti aziendali distribuite, data center e service provider.

Grazie alla combinazione del sistema operativo SonicOS di SonicWall con la brevettata* tecnologia Reassembly-Free Deep Packet Inspection® (RFDPI) e la potente architettura hardware multi-core altamente scalabile, la serie SuperMassive 9000 offre eccellenti funzioni di controllo delle applicazioni, prevenzione delle intrusioni, protezione da malware e decrittazione e ispezione TLS/SSL a velocità multi-gigabit. La serie SuperMassive, progettata con particolare attenzione ai requisiti di consumo, ingombro e raffreddamento, offre i firewall di nuova generazione con la migliore efficienza energetica (Gbps/Watt) del settore per l'elaborazione di pacchetti e dati ad alte prestazioni, il controllo delle applicazioni e la prevenzione delle minacce.

Il motore SonicWall RFDPI analizza ogni byte di ogni singolo pacchetto su tutte le porte garantendo l'ispezione completa del contenuto dell'intero flusso di dati, il tutto a prestazioni elevate e bassa latenza. Questa tecnologia è superiore a quella dei sistemi proxy che riassemblano il contenuto utilizzando socket associati a programmi antimalware, con problemi di inefficienza e sovraccarico della memoria dei socket che provocano latenza elevata, prestazioni inadeguate e limitazioni riguardo alle dimensioni dei file. Il motore RFDPI offre l'ispezione completa dei contenuti per eliminare varie forme di malware prima che entrino nella rete, fornendo protezione contro le minacce in continua evoluzione – senza limitazioni a livello di dimensioni dei file, prestazioni o latenza.

Inoltre, il motore RFDPI esegue la decrittazione e ispezione completa del traffico TLS/SSL crittografato e di applicazioni che non passano per il proxy, fornendo una protezione totale indipendentemente dal tipo di trasporto e dal protocollo. Ogni singolo pacchetto (intestazione e parte dati) viene esaminato accuratamente alla ricerca di non conformità dei protocolli, minacce, zero-day, intrusioni e persino in base a criteri definiti per rilevare e prevenire attacchi nascosti nel traffico crittografato, arrestare la diffusione di infezioni e impedire comunicazioni di comando e controllo (C&C) e la sottrazione di dati. Le regole di inclusione ed esclusione consentono un controllo totale per la personalizzazione del traffico da sottoporre a decrittazione ed ispezione in base alla specifica compliance dell'organizzazione e/o a requisiti legali specifici.

L'analisi del traffico delle applicazioni permette di identificare in tempo reale il traffico di applicazioni produttive e non produttive e di monitorarlo mediante potenti policy a livello di applicazione. Il controllo delle applicazioni può essere eseguito a livello di utente o di gruppo utilizzando pianificazioni ed elenchi di eccezioni. Tutte le firme relative ad applicazioni, prevenzione delle intrusioni e malware sono costantemente aggiornate dal team di ricerca delle minacce del Capture Labs. Inoltre SonicOS, l'avanzato sistema operativo dedicato, fornisce strumenti integrati per personalizzare le funzioni di identificazione e controllo delle applicazioni.

Serie SuperMassive 9000

Vantaggi:

- Prevenzione completa delle violazioni con prevenzione delle intrusioni ad alte prestazioni, protezione antimalware a bassa latenza e sandboxing basato su cloud
- Identificazione, controllo e visualizzazione completi e granulari delle applicazioni
- Rilevamento e blocco di minacce nascoste con decrittazione e ispezione del traffico TLS/SSL e SSH crittografato, senza problemi di prestazioni
- Prestazioni di sicurezza scalabili per data center a 10/40 Gb/s
- Adattamento a incrementi del livello di servizio e garanzia che i servizi e le risorse di rete siano sempre disponibili e protetti

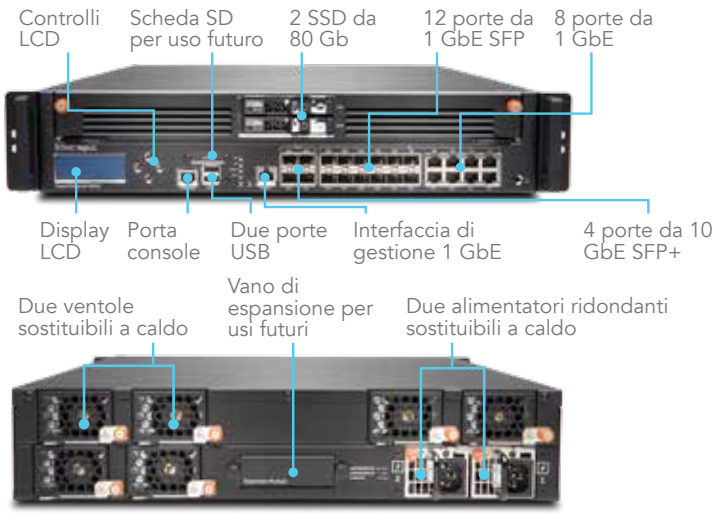
Partner Enabled Services
Serve aiuto per pianificare, ottimizzare o implementare una soluzione SonicWall? Gli Advanced Services Partner di SonicWall sono qualificati per fornire servizi professionali di altissimo livello. Per maggiori informazioni: www.sonicwall.com/PES.

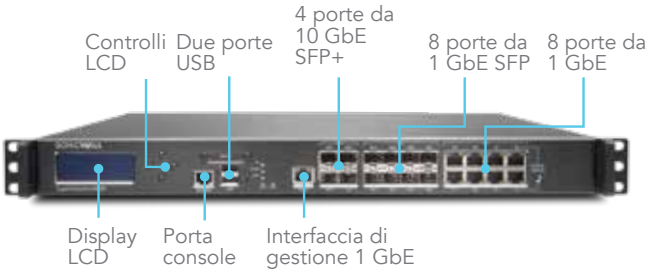
**Brevetti statunitensi 7,310,815; 7,600,257; 7,738,380; 7,835,361*

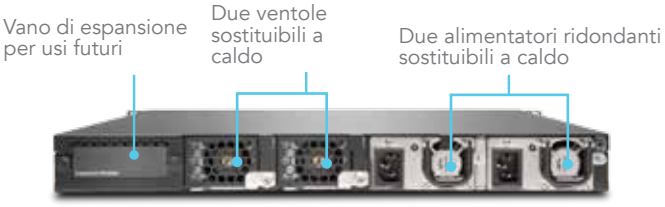
Descrizione della serie

La serie SonicWall SuperMassive 9000 dispone di 4 porte SFP+ a 10 GbE, fino a 12 porte SFP a 1 GbE, 8 porte a 1 GbE in rame e interfacce di gestione a 1 GbE, oltre ad una porta di espansione per 2 interfacce SFP+ a 10 GbE aggiuntive (per versioni future). I dispositivi della serie 9000 dispongono di moduli ventola e alimentatori sostituibili a caldo.

Serie SuperMassive 9000





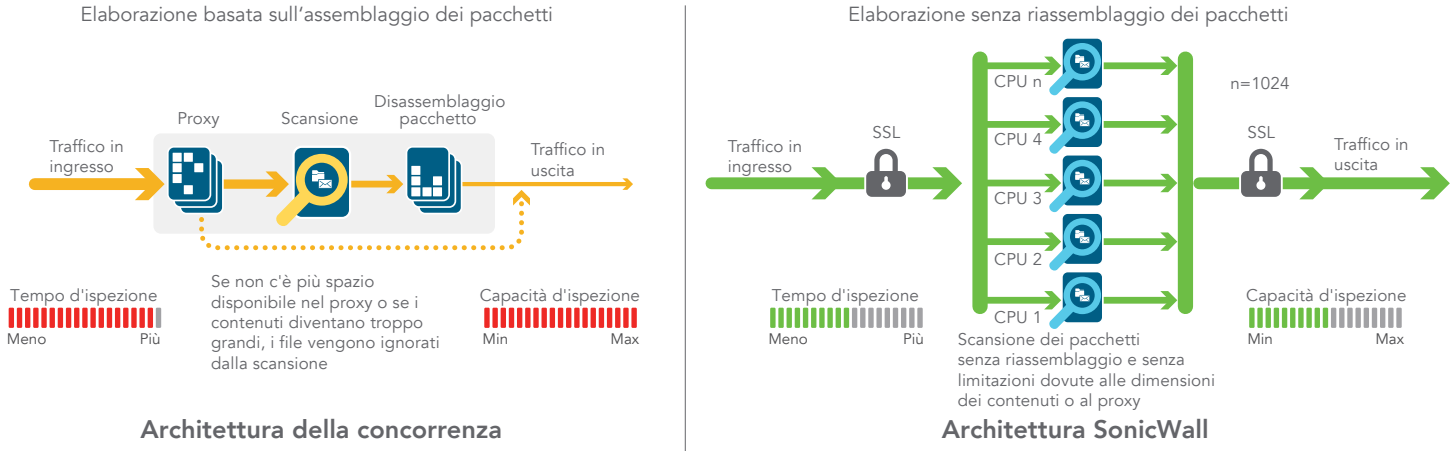


Funzionalità	9200	9400	9600	9800
Core di elaborazione	24	32	32	64
Throughput firewall	15 Gb/s	20 Gb/s	20 Gb/s	31,8 Gb/s
Throughput ispezione applicazioni	5 Gb/s	10 Gb/s	11,5 Gb/s	23 Gb/s
Throughput sistema di prevenzione delle intrusioni (IPS)	5 Gb/s	10 Gb/s	11,5 Gb/s	21,3 Gb/s
Throughput ispezione anti-malware	3,5 Gb/s	4,5 Gb/s	5 Gb/s	11 Gb/s
Numero massimo di connessioni DPI	1,5 milioni	1,5 milioni	2,0 milioni	8,0 milioni
Modalità di installazione	**9200**	**9400**	**9600**	**9800**
Modalità Bridge L2	Sì	Sì	Sì	Sì
Modalità Wire	Sì	Sì	Sì	Sì
Gateway/modalità NAT	Sì	Sì	Sì	Sì
Modalità Tap	Sì	Sì	Sì	Sì
Modalità trasparente	Sì	Sì	Sì	Sì

Motore Reassembly-Free Deep Packet Inspection

RFDPI è un sistema di ispezione a singolo passaggio e bassa latenza che esegue analisi ad alta velocità del traffico bidirezionale in base al flusso, senza proxy o buffering, per scoprire efficacemente tentativi di intrusione e malware e identificare il traffico applicativo indipendentemente dalla porta e dal protocollo. Questo motore proprietario ispeziona i payload del traffico in transito per rilevare eventuali minacce ai livelli da 3 a 7. Il motore RFDPI esamina i flussi di rete con ampie e ripetute procedure di normalizzazione e decrittazione, al fine di neutralizzare le tecniche avanzate di offuscamento ed evasione che tentano di confondere i motori di rilevamento e di introdurre codice dannoso nella rete.

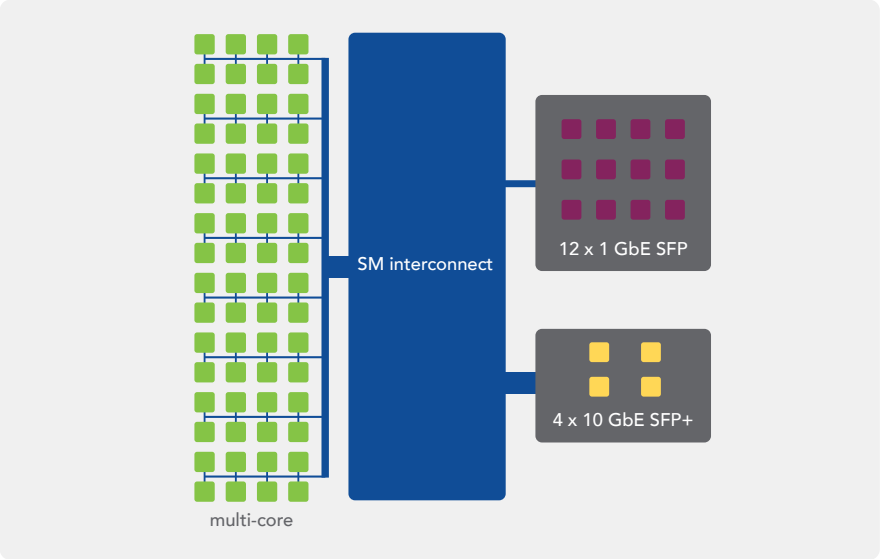
Una volta superata la necessaria elaborazione preliminare, che include anche la decrittazione TLS/SSL, ogni pacchetto viene analizzato in base a un'unica rappresentazione di memoria proprietaria di vari database di firme: attacchi intrusivi, malware, botnet e applicazioni. Lo stato di connessione viene quindi fatto progredire in modo che rappresenti la posizione del flusso riferita a questi database, finché non rileva uno stato di attacco o un altro evento "corrispondente". A questo punto viene intrapresa un'azione predefinita. Nella maggior parte dei casi, la connessione viene terminata e vengono generati eventi di log e di notifica. Il motore può comunque essere configurato solo per l'analisi oppure, se si tratta del rilevamento di applicazioni, per fornire servizi che gestiscano la larghezza di banda di livello 7 nel flusso restante non appena viene individuata l'applicazione.



Architettura ampliabile per massime prestazioni e scalabilità

Il motore RFDPI è stato appositamente progettato per fornire una scansione di sicurezza ad alte prestazioni compatibile con l'espansione continua e il parallelismo intrinseco del traffico di rete. In combinazione con sistemi di processori multi-core, questa architettura software incentrata sui parallelismi è perfettamente scalabile per gestire i requisiti di ispezione approfondita dei pacchetti (DPI) in presenza di carichi di traffico elevati. La piattaforma SuperMassive è basata su processori che, a differenza dei sistemi x86, sono ottimizzati per l'elaborazione di rete, crittografia e pacchetti, assicurando al tempo stesso flessibilità e possibilità di programmazione sul campo, un aspetto critico per i sistemi ASIC.

Questa flessibilità è un fattore essenziale quando si tratta di aggiornare comportamenti e nuovi codici per difendersi da attacchi inediti, che richiedono tecniche di rilevamento più sofisticate e innovative. L'architettura della piattaforma si distingue anche per la sua capacità unica di stabilire nuove connessioni su qualsiasi nucleo del sistema, garantendo la massima scalabilità e la capacità di gestire i picchi di traffico. Questo approccio consente di creare nuove sessioni (nuove connessioni al secondo) a una velocità estremamente elevata mentre è attiva l'ispezione deep packet – una metrica fondamentale che provoca spesso colli di bottiglia negli ambienti di data center.



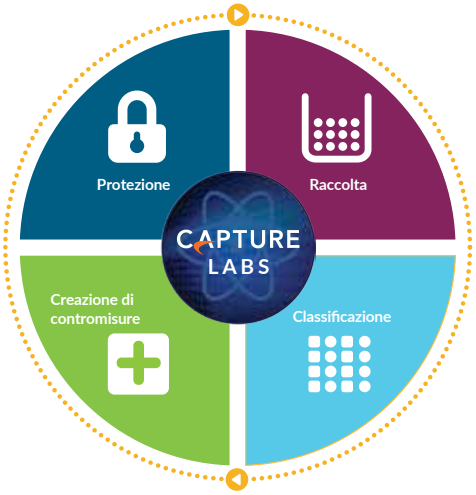
SONICWALL®

Capture Labs

Capture Labs, il team interno di SonicWall dedicato alla ricerca delle minacce, è costantemente impegnato a ricercare e sviluppare contromisure da implementare nei firewall dei clienti per garantire una protezione sempre aggiornata. Questo team raccoglie i dati sulle potenziali minacce da diverse fonti, tra cui il nostro premiato servizio sandbox di rete Capture Advanced Threat Protection, e da oltre 1 milione di sensori SonicWall situati in tutto il mondo per monitorare il traffico alla ricerca di minacce emergenti. Il traffico viene analizzato con tecniche di apprendimento automatico sfruttando gli algoritmi Deep Learning di SonicWall, in modo da estrarre il DNA dal codice e verificare che non sia associato a forme di codice dannoso.

I clienti che utilizzano un firewall SonicWall di nuova generazione con le funzionalità di sicurezza più recenti possono contare su una protezione dalle minacce costantemente aggiornata. I nuovi aggiornamenti hanno effetto immediato senza riavvii o interruzioni. Le firme nelle appliance contrastano classi di attacchi molto ampie, che coprono fino a decine di migliaia di minacce con una sola firma.

Oltre alle contromisure presenti sull'appliance, i firewall SuperMassive hanno anche accesso a SonicWall CloudAV[1], che amplia le funzionalità di intelligence integrate nei dispositivi con decine di milioni di firme, che aumentano di milioni ogni anno. I firewall accedono al database di CloudAV mediante un protocollo proprietario leggero, aumentando così la capacità d'ispezione dell'appliance. Grazie a Capture Advanced Threat Protection[1], una sandbox multi-engine basata sul cloud, le aziende possono esaminare i file e il codice sospetti in un ambiente isolato per bloccare le minacce avanzate come gli attacchi zero-day.



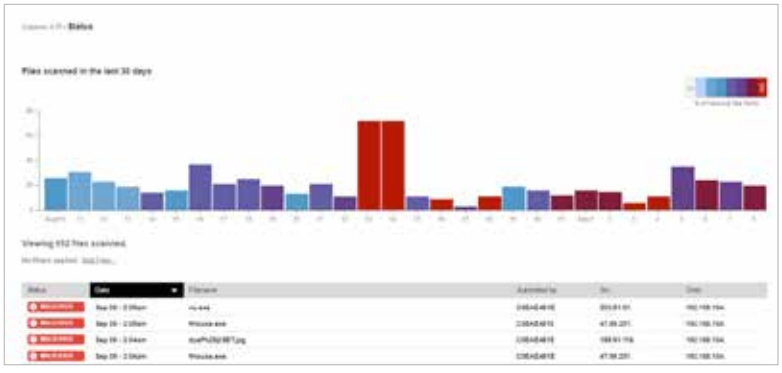
[1] Richiede un abbonamento aggiuntivo

Protezione contro le minacce avanzate

Il servizio SonicWall Capture Advanced Threat Protection[1] è una sandbox multi-engine basata sul cloud che amplia la protezione dei firewall contro le minacce per rilevare e prevenire gli attacchi zero-day. I file sospetti vengono inviati al cloud per l'analisi, con l'opzione di trattenerli al gateway finché non viene stabilito se siano sicuri o pericolosi. La piattaforma sandbox multi-engine, che include la piena emulazione di sistema e tecnologie di analisi a livelli hypervisor, esegue il codice sospetto nell'ambiente sandbox virtualizzato e ne analizza il comportamento. Appena un file viene identificato come dannoso, il sistema crea un hash in Capture e in seguito invia una firma ai firewall per prevenire attacchi successivi.

Il servizio analizza un'ampia gamma di sistemi operativi e tipologie di file, tra cui programmi eseguibili, DLL, PDF, documenti MS Office, archivi, JAR e APK.

Capture offre un dashboard intuitivo per l'analisi delle minacce e report con risultati dettagliati dell'analisi per i file che sono stati inviati al servizio, con informazioni come sorgente e destinazione, e un riepilogo accurato della reazione del malware dopo la detonazione.



SONICWALL

Controllo e intelligence delle applicazioni

L'intelligence delle applicazioni segnala agli amministratori il traffico delle applicazioni che attraversa la rete. Questo permette di pianificare opportuni controlli sulla base delle priorità aziendali, di circoscrivere le applicazioni poco produttive e bloccare quelle potenzialmente pericolose. La visualizzazione in tempo reale individua subito le anomalie nel traffico, consentendo di adottare contromisure immediate contro potenziali attacchi in entrata o uscita o colli di bottiglia per le prestazioni.

SonicWall Application Traffic Analytics[1] fornisce informazioni granulari sul traffico delle applicazioni, l'utilizzo della larghezza di banda e le minacce alla sicurezza, oltre a potenti funzionalità di risoluzione dei problemi e analisi forense. Inoltre le funzionalità di Single Sign-On (SSO) sicuro migliorano l'esperienza degli utenti, aumentano la produttività e riducono le chiamate al supporto tecnico. Un'interfaccia Web intuitiva semplifica la gestione e il controllo dell'intelligence delle applicazioni.

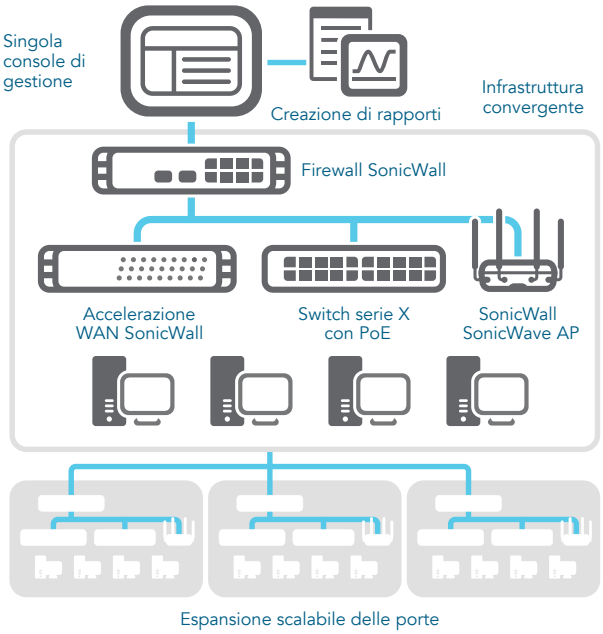
Creazione di rapporti e gestione globale

Per le organizzazioni ad elevata regolamentazione che desiderano creare una strategia coordinata di governance della sicurezza, compliance e gestione del rischio, il Global Management System[1] (GMS®) opzionale di SonicWall offre agli amministratori una piattaforma unificata, sicura e ampliabile per gestire firewall SonicWall, access point wireless e switch attraverso un processo di workstream correlato e verificabile. La soluzione GMS semplifica il consolidamento gestionale delle appliance di sicurezza, riduce le complessità relative all'amministrazione e alla risoluzione dei problemi e disciplina tutti gli aspetti operativi dell'infrastruttura di sicurezza, come l'applicazione e la gestione centralizzate delle policy, il monitoraggio degli eventi in tempo reale, le attività degli utenti, l'identificazione delle applicazioni, l'analisi forense e dei flussi, la creazione di rapporti di controllo e conformità e altro ancora. Inoltre, grazie a una funzionalità di automazione dei flussi di lavoro, il sistema GMS va incontro ai requisiti delle imprese per la gestione delle modifiche del firewall. L'automazione dei flussi di lavoro di GMS offre alle imprese la flessibilità e la sicurezza di applicare le policy del firewall in modo corretto, nel momento giusto e nel rispetto delle normative di conformità. La soluzione GMS offre un metodo coerente per gestire la sicurezza di rete, poiché non agisce dispositivo per dispositivo, ma in base a livelli di servizio e processi aziendali che semplificano drasticamente la gestione del ciclo di vita complessivo dell'ambiente di lavoro.

Applicazione sicura della conformità con SonicWall GMS

Vantaggi

- Gestione centralizzata
- Gestione delle policy senza errori
- Potente controllo degli accessi
- Procedure di controllo complete
- Modelli di report PCI, HIPAA, SOX
- Bassi costi di gestione



[1] *Richiede un abbonamento aggiuntivo*

Funzionalità

Motore RFDPI	
Funzionalità	Descrizione
Reassembly-Free Deep Packet Inspection (RFDPI)	Questo motore di ispezione proprietario brevettato ad alte prestazioni esegue analisi bidirezionali del traffico basate sui flussi, senza proxy o buffering, per rilevare tentativi di intrusione e malware e per identificare il traffico delle applicazioni indipendentemente dalla porta.
Ispezione bidirezionale	Con la scansione contemporanea del traffico in ingresso e in uscita per il rilevamento delle minacce, questa opzione impedisce l'utilizzo della rete come vettore di malware e come piattaforma per sferrare attacchi qualora venga introdotto un computer infetto.
Ispezione basata sui flussi	La tecnologia di ispezione priva di proxy e buffering genera una latenza estremamente bassa per le attività DPI su milioni di flussi di rete simultanei, senza limiti per la dimensione dei flussi e dei file. Inoltre può essere applicata tanto a protocolli comuni, quanto a flussi TCP primari.
Architettura altamente parallela e scalabile	L'esclusivo motore RFDPI basato su architettura multi-core offre l'ispezione DPI ad alta velocità e consente di creare nuove sessioni in tempi estremamente brevi, agevolando la gestione dei picchi di traffico in reti complesse.
Ispezione single-pass	Un'architettura DPI single-pass consente di rilevare contemporaneamente malware e intrusioni e identificare le applicazioni, in modo da ridurre notevolmente la latenza dell'ispezione DPI e mettere in correlazione tutte le informazioni sulle minacce in un'unica architettura.

Firewall e connettività di rete	
Funzionalità	Descrizione
API REST	Consentono ai firewall di ricevere e utilizzare tutti i feed di intelligence proprietari, dei produttori di dispositivi originali e di terze parti per combattere minacce avanzate come zero-day, utenti malintenzionati, credenziali compromesse, ransomware e minacce persistenti avanzate.
Stateful Packet Inspection	Tutto il traffico della rete viene ispezionato, esaminato e reso conforme alle policy di accesso del firewall.
Alta disponibilità/clustering	La serie SuperMassive supporta le modalità attiva/passiva (A/P) con sincronizzazione dello stato, DPI attiva/attiva (A/A) e clustering attivo/attivo ad alta disponibilità. La modalità DPI attiva/attiva trasferisce il carico di lavoro dell'ispezione deep packet ai nuclei dell'appliance passiva per ottimizzare il throughput.
Protezione da attacchi DDoS/DoS	La protezione da flooding SYN offre una difesa dagli attacchi DOS che si basa su tecnologie di blacklist SYN di livello 2 e proxy SYN di livello 3. Inoltre tutela dagli attacchi DOS/DDoS mediante la protezione da flooding UDP/ICMP e la limitazione della frequenza di connessione.
Supporto di IPv6	Il protocollo IPv6 (Internet Protocol versione 6) è in procinto di sostituire il protocollo IPv4. Con il più recente sistema SonicOS 6.2, l'hardware sarà in grado di supportare il filtraggio e le installazioni in modalità Wire.
Opzioni di installazione flessibili	La serie SuperMassive può essere installata nelle modalità NAT tradizionale, Layer 2 Bridge, Wire e Network Tap.
Bilanciamento del carico WAN	Bilancia il carico su più interfacce WAN con metodi basati sulle modalità round robin, percentuale o spill-over. Il routing in base alle policy crea degli instradamenti basati sui protocolli per dirigere il traffico verso una connessione WAN specifica, con possibilità di commutare su una WAN secondaria in caso di caduta dell'alimentazione.
Qualità del servizio (QoS) avanzata	Garantisce l'integrità delle comunicazioni strategiche tramite tagging 802.1p e DSCP e rimappatura del traffico VoIP sulla rete.
Supporto per gatekeeper H.323 e proxy SIP	Blocca le chiamate di spam richiedendo che tutte le chiamate in entrata siano autorizzate e autenticate dal gatekeeper H.323 o dal proxy SIP.
Gestione di switch di rete X-Series di Dell singoli e in cascata	Gestione delle impostazioni di sicurezza di porte aggiuntive, tra cui Portshield, HA, POE e POE+, da una singola interfaccia tramite il dashboard di gestione del firewall per gli switch di rete serie X di Dell.
Autenticazione biometrica	Supporta l'autenticazione dei dispositivi mobili come il riconoscimento delle impronte digitali, che non può essere facilmente duplicata o condivisa, in modo da autenticare in modo sicuro l'identità degli utenti per l'accesso alla rete.
Autenticazione aperta e login social	Consente agli utenti ospiti di utilizzare le proprie credenziali da servizi di social network come Facebook, Twitter o Google+ per accedere a Internet e ad altri servizi come ospiti attraverso la rete wireless, la LAN o le zone DMZ di un host tramite autenticazione pass-through.
Autenticazione multidominio	Offre un metodo semplice e veloce per amministrare le policy di sicurezza di tutti i domini di rete. Possibilità di gestire policy individuali per un singolo dominio o per un gruppo di domini.

Gestione e reporting	
Funzionalità	Descrizione
Global Management System[1] (GMS)	SonicWall GMS monitora, configura e crea report su più appliance SonicWall tramite un'unica console di gestione con un'interfaccia intuitiva, riducendo costi e complessità di gestione.
Gestione avanzata con un unico dispositivo	Configurazione comoda e veloce tramite l'interfaccia Web intuitiva, oltre a un'interfaccia CLI completa e al supporto per SNMPv2/3.
Creazione di rapporti sul flusso delle applicazioni IPFIX/NetFlow	Grazie ai protocolli IPFIX o NetFlow, le analisi sul traffico delle applicazioni e i dati di utilizzo possono essere impiegati per scopi di monitoraggio e per creare rapporti cronologici o in tempo reale con SonicWall Scrutinizer o altri strumenti che supportano IPFIX e NetFlow.

Funzionalità

Virtual Private Networking (VPN)	
Funzionalità	Descrizione
Provisioning automatico delle VPN	Semplifica l'installazione dei firewall in ambienti distribuiti complessi automatizzando il provisioning iniziale del gateway VPN da sito a sito tra i firewall SonicWall, garantendo l'applicazione istantanea e automatica della sicurezza e della connettività.
VPN IPSec per la connettività site-to-site	La rete VPN IPSec ad alte prestazioni consente di utilizzare la serie SuperMassive come concentratore di VPN per migliaia di utenti privati, filiali o altri siti di grandi dimensioni.
VPN SSL o accesso remoto da client IPSec	Sfruttando la tecnologia VPN SSL senza client o un client IPSec semplice da gestire, è possibile accedere in tutta semplicità a messaggi e-mail, file, computer, siti Intranet e applicazioni da un'ampia serie di piattaforme.
Gateway per la rete 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 basato su routing	La possibilità di eseguire il routing dinamico tramite collegamenti VPN garantisce un'operatività continua anche in caso di guasto temporaneo al tunnel VPN, perché il traffico viene instradato senza interruzioni tra gli endpoint attraverso route alternative.

Sensibilità al contesto/al contenuto	
Funzionalità	Descrizione
Tracciamento delle attività degli utenti	Le tecnologie AD/LDAP/Citrix[1]/Terminal Services[1] SSO integrate si combinano con le informazioni esaustive ricavate dall'ispezione DPI per consentire il tracciamento delle attività e l'identificazione degli utenti.
GeoIP per l'identificazione del traffico da Paesi specifici	Con questa opzione è possibile identificare e controllare il traffico di rete in ingresso o in uscita da Paesi specifici. Lo scopo è proteggere dagli attacchi provenienti da origini note o sospette di attività pericolose o analizzare il traffico sospetto che ha origine nella rete. Possibilità di creare elenchi personalizzati di paesi e botnet per ignorare il tag non corretto di un paese o una botnet associato a un indirizzo IP.
Filtro DPI con espressioni regolari	Questa opzione identifica e controlla i contenuti che attraversano la rete mediante la corrispondenza delle espressioni regolari per impedire perdite di dati.

Capture Advanced Threat Protection[1]	
Funzionalità	Descrizione
Sandbox multi-engine	La piattaforma sandbox multi-engine, che include la piena emulazione di sistema e tecnologie di analisi a livelli hypervisor, esegue il codice sospetto nell'ambiente sandbox virtualizzato, ne analizza il comportamento e fornisce visibilità sulle attività malevole.
Blocco fino al verdetto	Consente di creare elenchi personalizzati di paesi e botnet per ignorare il tag non corretto di un paese o una botnet associato a un indirizzo IP.
Analisi di un'ampia varietà di file	Supporta l'analisi di un'ampia gamma di tipi di file, tra cui programmi eseguibili (PE), DLL, PDF, documenti MS Office, archivi, JAR e APK, su diversi sistemi operativi come Windows, Android, Mac OS e ambienti multi-browser.
Rapida installazione delle firme	Quando un file viene identificato come dannoso, una firma viene inviata immediatamente ai firewall con abbonamento al servizio SonicWall Capture e ai database con le firme per l'antivirus GRID a livello gateway e l'ispezione IPS e ai database di reputazione degli URL, degli IP e dei domini entro 48 ore.
Capture Client	Capture Client è una piattaforma client unificata che offre molteplici funzionalità di protezione degli end point, tra cui la protezione avanzata da malware e supporto per la visibilità del traffico crittografato. La piattaforma sfrutta tecnologie di protezione su più livelli, reporting completo e applicazione della protezione degli end point.

Prevenzione delle minacce crittografate[1]	
Funzionalità	Descrizione
Decrittazione e ispezione TLS/SSL	Il traffico SSL/TLS viene decrittografato e analizzato in tempo reale senza proxy per individuare malware, intrusioni e perdite di dati, e vengono applicate policy per il controllo di contenuti, URL e applicazioni che difendono dalle minacce nascoste nel traffico TLS/SSL crittografato. Inclusa negli abbonamenti di sicurezza per tutti i modelli.
Ispezione SSH	La Deep Packet Inspection dell'SSH (DPI-SSH) esegue la decrittazione e l'ispezione dei dati che attraversano il tunnel SSH per prevenire gli attacchi che sfruttano l'SSH.

Prevenzione delle intrusioni[1]	
Funzionalità	Descrizione
Protezione basata su contromisure	Il sistema di prevenzione delle intrusioni (IPS) integrato utilizza le firme e altre contromisure per eseguire la scansione dei payload dei pacchetti in cerca di exploit e vulnerabilità, coprendo un'ampia serie di vulnerabilità e attacchi.
Aggiornamenti automatici delle firme	Il team del SonicWall Threat Research ricerca continuamente nuovi aggiornamenti e li installa in numerose contromisure IPS, che interessano oltre 50 categorie di attacchi. Gli aggiornamenti sono subito attivi senza la necessità di riavvii o interruzioni del servizio.
Protezione IPS interna alle zone	La segmentazione della rete in varie zone di sicurezza, protette dalle intrusioni, consente di potenziare la sicurezza interna poiché impedisce alle minacce di propagarsi oltre i confini di una zona.
Rilevamento e blocco di comando e controllo Botnet (CnC)	Questa opzione consente di individuare e bloccare il traffico di comando e controllo proveniente dai bot nella rete locale e diretto ai domini e agli indirizzi IP che sono stati identificati come fonte di propagazione di malware o punti CnC noti.
Rilevamento e prevenzione di abusi/anomalie dei protocolli	Questa opzione individua e blocca gli attacchi che abusano dei protocolli per tentare di aggirare l'IPS.
Protezione zero-day	Per proteggere la rete dagli attacchi zero-day, questa opzione assicura un aggiornamento costante a fronte delle tecniche e dei metodi di exploit più recenti, coprendo migliaia di singoli exploit.
Tecnologia antievasione	La normalizzazione estesa dei flussi, la decodifica e altre tecniche impediscono l'ingresso non rilevato delle minacce nella rete, grazie all'uso di tecniche di evasione nei livelli da 2 a 7.

Funzionalità

Prevenzione delle minacce[1]	
Funzionalità	Descrizione
Antimalware a livello gateway	Il motore RFDPI sottopone a scansione tutto il traffico in ingresso, in uscita e interno alle zone in cerca di virus, trojan, keylogger e altri malware, interessando file di dimensioni e lunghezza illimitati in tutte le porte e in tutti i flussi TCP.
Protezione antimalware CloudAV	Un database residente sui server cloud SonicWall, costantemente aggiornato con decine di milioni di firme delle minacce, viene consultato per ottimizzare le capacità del database di firme integrato nel dispositivo, garantendo così un'ampia copertura delle minacce da parte del motore RFDPI.
Aggiornamenti di sicurezza costanti	I nuovi aggiornamenti sulle minacce vengono inviati automaticamente ai firewall sul campo con servizi di sicurezza attivi e sono subito attivi senza riavvii o interruzioni.
Ispezione bidirezionale dei TCP primari	Il motore RFDPI è in grado di scansionare flussi TCP primari in entrambe le direzioni su qualsiasi porta, bloccando gli attacchi che tentano di passare attraverso sistemi di sicurezza obsoleti, concepiti per proteggere solo poche porte note.
Supporto esteso dei protocolli	Oltre a identificare i protocolli più comuni come HTTP/S, FTP, SMTP, SMBv1/v2 e altri, che non inviano dati nel TCP primario, questa opzione consente di decodificare i payload in cerca di malware, anche se non sono eseguiti in porte standard note.

Controllo e intelligence delle applicazioni[1]	
Funzionalità	Descrizione
Controllo delle applicazioni	Per potenziare la sicurezza e la produttività della rete vengono controllate le applicazioni, o singole funzionalità delle applicazioni, identificate dal motore RFDPI utilizzando un database in continua espansione, contenente migliaia di firme di applicazioni.
Identificazione di applicazioni personalizzate	Per verificare le applicazioni personalizzate e quindi acquisire maggiore controllo sulla rete vengono generate firme basate su schemi o parametri specifici, che sono univoci per ogni applicazione nelle relative comunicazioni di rete.
Gestione della larghezza di banda delle applicazioni	Il traffico delle applicazioni superflue viene bloccato, mentre la larghezza di banda disponibile viene regolamentata e allocata in modo granulare per le applicazioni o le categorie di applicazioni più importanti.
Controllo granulare	Consente di controllare le applicazioni o i componenti specifici di un'applicazione in base a pianificazioni, gruppi di utenti, elenchi di esclusione e una serie di attività con identificazione SSO degli utenti completa, mediante l'integrazione di LDAP/AD/Terminal Services/ Citrix.

Filtraggio dei contenuti[1]	
Funzionalità	Descrizione
Filtraggio dei contenuti interno/ esterno	Il Content Filtering Service applica le policy di utilizzo accettabili e blocca l'accesso a siti Web contenenti informazioni o immagini discutibili o non produttive.
Content Filtering Client	Estende l'applicazione delle policy per bloccare i contenuti Internet per dispositivi Windows, Mac OS, Android e Chrome situati all'esterno del perimetro del firewall.
Controlli granulari	L'uso di categorie predefinite o di una combinazione qualsiasi di categorie consente di bloccare determinati contenuti. Il filtraggio può essere pianificato in base all'ora del giorno, ad esempio durante l'orario scolastico o lavorativo, e applicato a gruppi o singoli utenti.
Cache Web	Le classificazioni degli URL sono memorizzate nella cache locale del firewall SonicWall, in modo che il tempo di risposta per l'accesso successivo ai siti Web visitati con maggior frequenza sia inferiore a un secondo.

Antivirus e antispyware applicati[1]	
Funzionalità	Descrizione
Protezione su più livelli	Utilizza le funzionalità del firewall come primo livello di difesa sul perimetro, insieme alla protezione degli endpoint, per bloccare i virus che entrano nella rete tramite laptop, chiavette USB e altri sistemi non protetti.
Opzione di implementazione automatizzata	Garantisce che in tutti i computer che accedono alla rete sia installata e attiva la versione più recente delle firme antivirus e antispyware, eliminando così i costi normalmente legati alla gestione degli antivirus e degli antispyware sui computer desktop.
Distribuzione e implementazione automatizzate	Per ridurre il carico amministrativo, l'installazione dei client per antivirus e antispyware avviene automaticamente, computer per computer, in tutta la rete.
Protezione automatica e sempre attiva contro i virus	Per migliorare la produttività degli utenti finali e ridurre le attività di gestione della sicurezza, gli aggiornamenti antivirus e antispyware più frequenti vengono distribuiti in modo trasparente a tutti i file server e i computer desktop.
Antivirus di nuova generazione	Capture Client utilizza un motore statico di intelligenza artificiale (AI) per determinare le minacce prima che possano essere eseguite e per ripristinare uno stato precedente non infetto.
Protezione antispyware	La potente protezione contro gli spyware garantisce il massimo livello di prestazioni e sicurezza analizzando e bloccando i programmi spyware più diffusi e pericolosi, prima che questi possano carpire dati sensibili da computer fissi o portatili.

[1] *Richiede un abbonamento aggiuntivo*

Riepilogo delle funzionalità

Firewall

- Stateful Packet Inspection
- Reassembly-Free Deep Packet Inspection
- Protezione da attacchi DDoS (UDP/ICMP/SYN flood)
- Supporto di IPv4/IPv6
- Autenticazione biometrica per l'accesso remoto
- Proxy DNS
- API REST

Ispezione e decrittografia SSL/SSH[2]

- Deep Packet Inspection per TLS/SSL/SSH
- Inclusione/esclusione di oggetti, gruppi o nomi di host
- Controllo SSL

Capture Advanced Threat Protection[2]

- Analisi multi-engine basata sul cloud
- Sandbox virtuale
- Analisi a livello hypervisor
- Emulazione di sistema completa
- Ispezione di un'ampia varietà di file
- Invio automatizzato e manuale
- Intelligence sulle minacce con aggiornamenti in tempo reale
- Blocco fino al verdetto
- Capture Client

Prevenzione delle intrusioni[2]

- Scansione basata sulle firme
- Aggiornamenti automatici delle firme
- Motore di ispezione bidirezionale
- Impostazione di regole IPS granulari
- Implementazione GeoIP
- Filtraggio Botnet con elenchi dinamici
- Corrispondenza con espressioni regolari

Anti-malware[2]

- Scansione antimalware basata sui flussi
- Antivirus per gateway
- Antispyware per gateway
- Ispezione bidirezionale
- Nessun limite alle dimensioni dei file
- Database dei malware cloud

Identificazione delle applicazioni[2]

- Controllo delle applicazioni
- Visualizzazione del traffico delle applicazioni
- Blocco dei componenti delle applicazioni
- Gestione della larghezza di banda delle applicazioni
- Creazione di firme per applicazioni personalizzate
- Prevenzione di eventuali perdite di dati
- Creazione di report sulle applicazioni tramite NetFlow/IPFIX
- Tracciamento delle attività degli utenti (SSO)
- Ampio database di firme delle applicazioni

Filtraggio dei contenuti Web[2]

- Filtraggio degli URL
- Proxy avoidance
- Blocco della parole chiave
- Inserimento intestazione HTTP
- Gestione della banda secondo categorie CFS
- Modello di policy unificato con controllo delle applicazioni
- Content Filtering Client

VPN

- Provisioning automatico delle VPN
- VPN IPSec per una connettività Site-to-Site
- VPN SSL e accesso remoto da client IPSec
- Gateway per la rete VPN ridondante
- Mobile Connect per iOS, Mac OS X, Windows, Chrome, Android e Kindle Fire
- VPN basata su routing (OSPF, RIP, BGP)

Networking

- LAG dinamico tramite LACP
- PortShield
- Frame Jumbo
- Indagine del percorso MTU
- Registrazione avanzata
- VLAN trunking
- Mirroring delle porte
- QoS Layer-2
- Sicurezza delle porte
- Routing dinamico (RIP/OSPF/BGP)
- Controller wireless SonicWall[1]
- Routing basato su policy (ToS/metrico ed ECMP)
- NAT
- Server DHCP
- Gestione della larghezza di banda
- Aggregazione dei link (statica e dinamica)
- Ridondanza delle porte
- Alta disponibilità A/P con sincronizzazione dello stato
- Clustering A/A
- Bilanciamento del carico in ingresso/in uscita
- Modalità Bridge (L2), Wire/Wire virtuale, Tap, NAT
- Failover WAN 3G/4G (non per SuperMassive 9800)
- Routing asimmetrico
- Supporto CAC (Common Access Card)

Wireless

- WIDS/WIPS
- Analisi dello spettro RF
- Prevenzione di access point non autorizzati
- Fast roaming (802.11k/r/v)
- Visualizzazione in pianta/della topologia
- Band steering
- Beamforming
- AirTime fairness
- MiFi Extender
- Quote cicliche guest
- Portale ospite LHM

VoIP

- Controllo QoS granulare
- Gestione della larghezza di banda
- DPI per il traffico VoIP
- Gatekeeper H.323 e supporto per proxy SIP

Gestione e monitoraggio

- GMS, Web, UI, CLI, API REST, SNMPv2/v3
- Logging
- Esportazione per Netflow/IPFix
- Backup della configurazione basato su cloud
- Piattaforma Security Analytics di BlueCoat
- Gestione dei punti di accesso SonicWall
- Gestione di switch N-Series e X-Series di Dell[1]

[1] *Non supportato su SuperMassive 9800*
[2] *Richiede un abbonamento aggiuntivo*

SONICWALL®

Specifiche di sistema della serie SuperMassive 9000

Firewall in generale	9200	9400	9600	9800
Sistema operativo	SonicOS			
Core di elaborazione di sicurezza	24	32		64
Interfacce	4 x 10 GbE SFP+, 8 x 1 GbE SFP, 8 x 1GbE, 1 GbE di gestione, 1 Console			4 x 10 GbE SFP+, 12 x 1 GbE SFP, 8 x 1GbE, 1 GbE di gestione, 1 Console
Memoria (RAM)	8 GB	16 GB	32 GB	64 GB
Capacità	Flash			2 SSD da 80GB, Flash
Espansione	1 slot di espansione (posteriore)*, scheda SD*			
Gestione	CLI, SSH, GUI, GMS			
Utenti SSO	80.000	90.000	100.000	110.000
Access point max. supportati	128			-
Logging	Analyzer, registro locale, Syslog			
Alta disponibilità	Attiva/passiva con State Sync, DPI attiva/attiva con State Sync			
Firewall/prestazioni VPN	**9200**	**9400**	**9600**	**9800**
Throughput ispezione firewall[1]	15 Gb/s	20 Gb/s	20 Gb/s	31,8 Gb/s
Throughput prevenzione minacce[2]	3 Gb/s	4,4 Gb/s	4,5 Gb/s	10,5 Gb/s
Throughput ispezione applicazioni[2]	5 Gb/s	10 Gb/s	11,5 Gb/s	23 Gb/s
Throughput IPS[2]	5 Gb/s	10 Gb/s	11,5 Gb/s	21,3 Gb/s
Throughput ispezione antimalware[1]	3,5 Gb/s	4,5 Gb/s	5,0 Gb/s	11 Gb/s
Throughput IMIX	4,4 Gb/s	5,5 Gb/s	5,5 Gb/s	7,3 Gb/s
Throughput decrittografia e ispezione SSL (SSL DPI)[2]	1,0 Gb/s	2,0 Gb/s	2,0 Gb/s	3,5 Gb/s
Throughput VPN[3]	5 Gb/s	10 Gb/s	11,5 Gb/s	14,3 Gb/s
Connessioni al secondo	100.000	130.000	130.000/sec	229.000/sec
Connessioni max. (SPI)	5 milioni	7,5 milioni	10 milioni	20,0 milioni
Connessioni max. (DPI)	1,5 milioni	1,5 milioni	2 milioni	8,0 milioni
Connessioni DPI SSL[6] (max.)	8.000 (15.500[6])	10.000 (17.500[6])	12.000 (22.500[6])	400.000
VPN	**9200**	**9400**	**9600**	**9800**
Tunnel VPN site-to-site	10.000			25.000
Client VPN IPSec (max)	2.000(4.000)	2.000(6.000)	2.000(10.000)	
Client VPN SSL NetExtender (max)	2 (3.000)	2 (3.000)	50 (3.000)	50 (3.000)
Autenticazione/crittografia	DES, 3DES, AES (128, 192, 256 bit)/MD5, SHA-1, Suite B, Common Access Card (CAC)			
Key exchange	Gruppi Diffie-Hellman 1, 2, 5, 14v			
VPN basato su routing	RIP, OSPF			
Connettività di rete	**9200**	**9400**	**9600**	**9800**
Assegnazione indirizzo IP	Statico, client DHCP, PPPoE, L2TP e PPTP, server DHCP interno, DHCP relay[4]			
Modalità NAT	1 a 1, molti a 1, 1 a molti, NAT flessibile (IP sovrapposti), PAT, modalità trasparente			
Interfacce VLAN	512			
Protocolli di routing	BGP, OSPF, RIPv1/v2, routing statico, routing basato su policy, multicast			
Qualità del servizio (QoS)	Priorità della larghezza di banda, larghezza di banda massima, larghezza di banda garantita, contrassegno DSCP, 802.1p			
Autenticazione	LDAP (multidominio), XAUTH/RADIUS, SSO, Novell, database utenti interno, Terminal Services[5], Citrix[5]			
VoIP	Full H323-v1-5, SIP			
Standard	TCP/IP, ICMP, HTTP, HTTPS, IPSec, ISAKMP/IKE, SNMP, DHCP, PPPoE, L2TP, PPTP, RADIUS, IEEE 802.3			
Certificazioni	UC APL[4], ICSA Enterprise Firewall, IPV6 Phase 2, VPNC, VPAT, FIPS 140-2[4], Common Criteria NDPP[4], ICSA Anti-Virus[4]			
Hardware	**9200**	**9400**	**9600**	**9800**
Alimentazione	Due alimentatori ridondanti sostituibili a caldo, 300 W			Due alimentatori ridondanti sostituibili a caldo, 500 W
Ventole	Due, ridondanti, sostituibili a caldo			
Display	Display LED anteriore			
Alimentazione in ingresso	100-240 V CA, 50-60 Hz			
Consumo energetico massimo (W)	200			350
MTBF a 25 °C in ore	188.719	187.702	186.451	126.144
MTBF a 25 °C in anni	21,53	21,43	21,28	14,40
Fattore di forma	Montabile su rack 1U			Montabile su rack 2U
Dimensioni	43,3x48,5x4,5 cm (17x19,1x1,75 in)			9x60x43 cm (17x24x3,5 in)
Peso	8,2 kg (18,1 lb)			18,38 kg (40,5 lb)
Peso WEEE	10,4 kg (23 lb)			22,4 kg (49,5 lb)
Peso con la confezione	13,3 kg (29,3 lb)			29,64 kg (65 lb)
Normative principali	FCC Classe A, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe A, MSIP/KCC Classe A, UL, cUL, TÜV/GS, CB, CoC UL (Messico), WEEE, REACH, ANATEL, BSMI, CU			
Condizioni ambientali	15-40 °C			
Umidità	10-90% senza condensa			

*[1] Metodologie di test: prestazioni massime come da RFC 2544 (per il firewall). Le prestazioni effettive possono variare a seconda delle condizioni di rete e dei servizi attivati. [2] Rilevazione throughput per prevenzione minacce/Gateway AV/Anti-Spyware/IPS tramite il test di performance Spirent WebAvalanche HTTP standard nell'industria e gli strumenti di test Ixia. Test eseguiti con flussi multipli attraverso coppie di porte multiple. Rilevazione throughput prevenzione delle minacce con Gateway AV, Anti-Spyware, IPS e Application Control attivati. [3] Rilevazione throughput VPN mediante il traffico UDP con pacchetti di 1.280 byte. [4] Valido per SuperMassive 9200, 9400 e 9600. La certificazione per SuperMassive 9800 UC APL è in corso di approvazione. [5] Supportato su SonicOS 6.1 e 6.2. [6] Il numero di connessioni DPI SSL aumenta di 750 ogni 125.000 connessioni DPI ridotte. *Utilizzo futuro. Tutte le specifiche, le funzioni e le informazioni sulla disponibilità sono soggette a modifiche.*

SONICWALL®

Informazioni per l'ordinazione della serie SuperMassive 9000

Prodotto	SKU
SuperMassive 9800 Total Secure Advance Edition (1 anno)	01-SSC-0312
SuperMassive 9600 Total Secure Advance Edition (3 anni)	02-SSC-0410
SuperMassive 9400 Total Secure Advance Edition (3 anni)	02-SSC-0409
SuperMassive 9200 Total Secure Advance Edition (3 anni)	02-SSC-0408
SuperMassive 9200 – Abbonamenti a servizi di supporto e sicurezza	**SKU**
Advanced Gateway Security Suite – Capture ATP, prevenzione delle minacce, filtraggio dei contenuti e supporto 24x7 per SuperMassive 9200 (1 anno)	01-SSC-1570
Capture Advanced Threat Protection per SuperMassive 9200 (1 anno)	01-SSC-1575
Comprehensive Gateway Security Suite: application intelligence, prevenzione delle minacce, filtraggio dei contenuti con supporto per 9200 (1 anno)	01-SSC-4172
Prevenzione delle intrusioni, antimalware, CloudAV, Application Intelligence, Control and Visualization per SuperMassive 9200 (1 anno)	01-SSC-4202
Content Filtering, edizione Premium Business per 9200 (1 anno)	01-SSC-4184
Supporto Platinum per SuperMassive 9200 (1 anno)	01-SSC-4178
SuperMassive 9400 – Abbonamenti a servizi di supporto e sicurezza	**SKU**
Advanced Gateway Security Suite – Capture ATP, prevenzione delle minacce, filtraggio dei contenuti e supporto 24x7 per SuperMassive 9400 (1 anno)	01-SSC-1580
Capture Advanced Threat Protection per SuperMassive 9400 (1 anno)	01-SSC-1585
Comprehensive Gateway Security Suite: application intelligence, prevenzione delle minacce, filtraggio dei contenuti con supporto per 9400 (1 anno)	01-SSC-4136
Prevenzione delle intrusioni, antimalware, CloudAV, Application Intelligence, Control and Visualization per SuperMassive 9400 (1 anno)	01-SSC-4166
Content Filtering, edizione Premium Business per 9400 (1 anno)	01-SSC-4148
Supporto Platinum per SuperMassive 9400 (1 anno)	01-SSC-4142
SuperMassive 9600 – Abbonamenti a servizi di supporto e sicurezza	**SKU**
Advanced Gateway Security Suite – Capture ATP, prevenzione delle minacce, filtraggio dei contenuti e supporto 24x7 per SuperMassive 9600 (1 anno)	01-SSC-1590
Capture Advanced Threat Protection per SuperMassive 9600 (1 anno)	01-SSC-1595
Comprehensive Gateway Security Suite: application intelligence, prevenzione delle minacce, filtraggio dei contenuti con supporto per 9600 (1 anno)	01-SSC-4100
Prevenzione delle intrusioni, antimalware, CloudAV, Application Intelligence, Control and Visualization per SuperMassive 9600 (1 anno)	01-SSC-4130
Content Filtering, edizione Premium Business per 9600 (1 anno)	01-SSC-4112
Supporto Platinum per SuperMassive 9600 (1 anno)	01-SSC-4106
SuperMassive 9800 – Abbonamenti a servizi di supporto e sicurezza	**SKU**
Advanced Gateway Security Suite: Capture ATP, prevenzione delle minacce, filtraggio dei contenuti e supporto 24x7 per SuperMassive 9800 (1 anno)	01-SSC-1183
Capture Advanced Threat Protection per SuperMassive 9800 (1 anno)	01-SSC-1188
Comprehensive Gateway Security Suite: application intelligence, prevenzione delle minacce, filtraggio dei contenuti con supporto per 9800 (1 anno)	01-SSC-0809
Prevenzione delle intrusioni, antimalware, CloudAV, Application Intelligence, Control and Visualization per SuperMassive 9800 (1 anno)	01-SSC-0827
Content Filtering, edizione Premium Business per 9800 (1 anno)	01-SSC-0821
Supporto Gold 24x7 per SuperMassive 9800 (1 anno)	01-SSC-0815
Moduli e accessori*	**SKU**
Ventola di sistema (FRU) per la serie SonicWall SuperMassive 9800	01-SSC-0204
Alimentatore CA (FRU) per la serie SonicWall SuperMassive 9800	01-SSC-0203
Ventola di sistema (FRU) per la serie SonicWall SuperMassive 9000	01-SSC-3876
Alimentatore CA (FRU) per la serie SonicWall SuperMassive 9000	01-SSC-3874
Modulo a corto raggio (Short Reach) 10GBASE-SR SFP+	01-SSC-9785
Modulo a lungo raggio (Long Reach) 10GBASE-LR SFP+	01-SSC-9786
Modulo a corta distanza (Short Haul) 1000BASE-SX SFP	01-SSC-9789
Modulo a lunga distanza (Long Haul) 1000BASE-SX SFP	01-SSC-9790
Modulo in rame 1000BASE-T SFP	01-SSC-9791
Gestione e reporting	**SKU**
Licenza software (10 nodi) per SonicWall GMS	01-SSC-3363
Supporto software E-Class 24x7 per SonicWall GMS 10 nodi (1 anno)	01-SSC-6514
SonicWall Scrutinizer (appliance virtuale) con licenza software per il modulo Flow Analytics fino a 5 nodi (include 1 anno di supporto software 24x7)	01-SSC-3443
SonicWall Scrutinizer con licenza software per il modulo Flow Analytics fino a 5 nodi (include 1 anno di supporto software 24x7)	01-SSC-4002
SonicWall Scrutinizer con licenza software per il modulo Advanced Reporting fino a 5 nodi (include 1 anno di supporto software 24x7)	01-SSC-3773

**Per un elenco completo dei moduli SFP e SFP+ supportati, contattare un ingegnere di soluzioni SonicWall.*

Informazioni su SonicWall

Da oltre 27 anni SonicWall combatte il crimine informatico proteggendo piccole, medie e grandi imprese in ogni parte del mondo. La nostra combinazione di prodotti e partner ha permesso di realizzare una soluzione di rilevamento e prevenzione automatizzata delle violazioni in tempo reale ottimizzata per le esigenze specifiche di oltre 500.000 organizzazioni in più di 215 paesi e regioni, per consentire loro di fare più affari con maggior sicurezza.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

Datasheet-SuperMassive-US-VG-MKTG4043