SONICWALL

SonicWall SuperMassive Series

Protezione senza compromessi per le reti aziendali tramite firewall di prestazioni elevate di prossima generazione.

SonicWall SuperMassive Series è la piattaforma di firewall di prossima generazione (NGFW) progettata da SonicWall per le reti di grandi dimensioni in funzione della modularità, dell'affidabilità e della sicurezza approfondita con velocità multi-gigabit e latenza quasi zero.

Realizzati per soddisfare le esigenze di imprese, governi, scuole, grande distribuzione, assistenza sanitaria e fornitori di servizi, i prodotti SuperMassive Series sono l'ideale per la sicurezza delle reti delle imprese distribuite, dei data center e dei fornitori di servizi.

Frutto della combinazione del sistema operativo SonicOS di SonicWall, della tecnologia brevettata* Reassembly-Free Deep Packet Inspection® (RFDPI) e di un'architettura hardware, decisamente multi-core e altamente modulare, i firewall SuperMassive 9000 Series mettono a disposizione il meglio a livello industriale per quanto riguarda il controllo delle applicazioni, la prevenzione delle intrusioni, la protezione contro il malware e la decrittazione e l'ispezione TLS/SSL con velocità multi-gigabit. La SuperMassive Series è stata accuratamente progettata in funzione delle caratteristiche di potenza, spazio e raffreddamento (PSC), che contraddistinguono i firewall di prossima generazione Gbps/watt leader in campo industriale per l'elaborazione di prestazioni elevate dei pacchetti e dei dati, il controllo delle applicazioni e la prevenzione delle minacce.

L'engine SonicWall RFDPI effettua la scansione di ogni byte e di ogni pacchetto su tutte le porte, realizzando l'ispezione completa di tutti i contenuti dell'intero flusso di dati, garantendo prestazioni elevate e bassa latenza. Si tratta di una tecnologia superiore a quelle che utilizzano i proxy che riassemblano i contenuti tramite socket associati a programmi anti-malware, che accusano inefficienze e overhead del trashing della memoria dei socket, il che comporta una latenza elevata, prestazioni insoddisfacenti e limitazioni delle dimensioni dei file. L'engine RFDPI effettua l'ispezione completa dei contenuti per eliminare diverse forme di malware prima che entrino in rete e fornisce protezione contro l'evoluzione delle minacce, senza limitazioni di file, prestazioni o latenza.

L'engine RFDPI esegue anche la decrittazione e l'ispezione completa del traffico crittografato TLS/SSL e SSH, e anche delle applicazioni non-proxyable, consentendo la protezione completa indipendentemente dal trasporto o dal protocollo. Guarda in profondità all'interno dei singoli pacchetti (l'header e la parte dati), cercando le non-conformità dei protocolli, minacce zero-day, intrusioni e anche criteri predefiniti per rilevare e impedire attacchi nascosti all'interno del traffico crittografato, interrompere la diffusione delle infezioni e bloccare le comunicazioni di comandi e controlli (C&C) e l'esfiltrazione dei dati. Le regole di inclusione ed esclusione consentono il controllo totale per personalizzare il traffico soggetto a decrittazione e ispezione, sulla base di specifici requisiti di conformità organizzativa e/o legale.

L'analisi del traffico delle applicazioni consente l'identificazione del traffico delle applicazioni produttivo e improduttivo in tempo reale e il traffico può quindi essere controllato tramite potenti politiche a livello di applicazione. Il controllo delle applicazioni può essere esercitato per singolo utente e per gruppi, anche tramite orari programmati ed elenchi di eccezioni. Tutte le segnature delle applicazioni, della prevenzione delle intrusioni e del malware vengono costantemente aggiornate dai ricercatori delle minacce di SonicWall Capture Labs. Inoltre, SonicOS, un sistema operativo avanzato appositamente realizzato, mette a disposizione strumenti integrati che consentono l'identificazione e il controllo personalizzati delle applicazioni.

Serie SuperMassive 9000

Vantaggi:

- Prevenzione completa delle violazioni, compresi la prevenzione delle intrusioni di prestazioni elevate, la protezione contro il malware a bassa latenza e il sandboxing basato sul cloud
- Identificazione, controllo e visualizzazione delle applicazioni completamente granulare
- Individuazione e blocco delle minacce nascoste, con decrittazione e ispezione del traffico crittografato TLS/SSL e SSH, senza problemi a livello di prestazioni
- Modularità delle prestazioni di sicurezza per data center 10/40 Gbp
- Adeguamento agli incrementi dei livelli di servizio e garanzia della disponibilità e della protezione dei servizi e delle risorse di rete

Servizi attivati dai partner

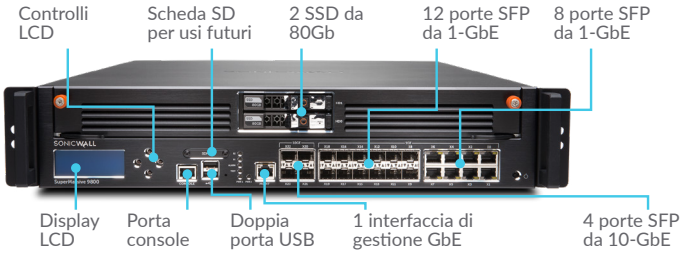
Serve aiuto per pianificare, installare od ottimizzare la soluzione SonicWall? I SonicWall Advanced Services Partner hanno seguito corsi di formazione per fornire servizi professionali di livello mondiale. Ulteriori informazioni su www.sonicwall.com/PES.

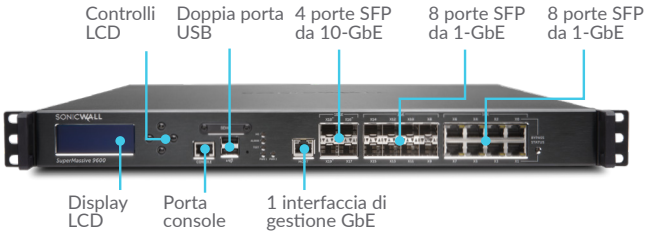
*Brevetti USA 7.310.815; 7.600.257; 7.738.380; 7.835.361

Descrizione della serie

La serie SonicWall SuperMassive 9000 è dotata delle seguenti interfacce di gestione: 4 SFP+ da 10-GbE, fino a 12 SFP da 1-GbE, 8 1-GbE rame e 1 GbE, e una porta di espansione per altre 2 interfacce SFP+ da 10-GbE (disponibilità futura). La serie 9000 è dotata di moduli ventola e alimentatori sostituibili a caldo.

Serie SuperMassive 9000





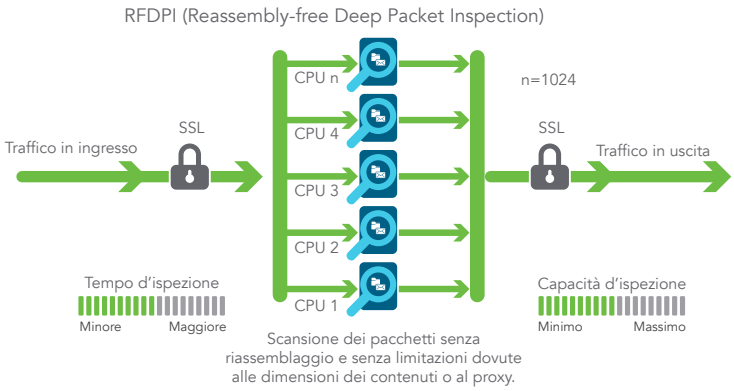
FUNZIONI	9200	9400	9600	9800
Core di elaborazione	24	32	32	64
Throughput del firewall	15 Gbps	20 Gbps	20 Gbps	31,8 Gbps
Throughput di ispezione delle applicazioni	5 Gbps	10 Gbps	11,5 Gbps	23 Gbps
Throughput del sistema di prevenzione delle intrusioni (IPS)	5 Gbps	10 Gbps	11,5 Gbps	21,3 Gbps
Throughput di ispezione anti-malware	3,5 Gbps	4,5 Gbps	5 Gbps	11 Gbps
Numero massimo di connessioni DPI	1,5 M	1,5 M	2,0 M	8,0 M
MODALITÀ DI INSTALLAZIONE	**9200**	**9400**	**9600**	**9800**
Modalità L2 bridge	Sì	Sì	Sì	Sì
Modalità wire	Sì	Sì	Sì	Sì
Modalità gateway/NAT	Sì	Sì	Sì	Sì
Modalità Tap	Sì	Sì	Sì	Sì
Modalità trasparente	Sì	Sì	Sì	Sì

Engine Reassembly-Free Deep Packet Inspection

La tecnologia 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 i tentativi di intrusione, malware ed esaminare il traffico applicativo indipendentemente dalla porta e dal protocollo. Questo engine proprietario ispeziona i payload del traffico in transito per rilevare eventuali minacce ai livelli 3-7. L'engine RFDPI esamina i flussi di rete, con procedure complesse e ripetute di normalizzazione e decrittazione, per sventare le tecniche di offuscamento ed evasione avanzate che tentano di confondere i motori di rilevamento e introdurre codice dannoso nella rete.

Una volta superata la necessaria elaborazione preliminare, che comprende anche la decrittazione TLS/SSL, ogni pacchetto viene analizzato in base a un'unica rappresentazione di memoria proprietaria di diversi database di segnature: 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". Nella maggior parte dei casi, la connessione viene terminata e vengono generati eventi di log e di notifica. L'engine può anche essere configurato per eseguire solo l'ispezione oppure, in caso di rilevamento delle applicazioni, per fornire servizi di gestione della larghezza di banda al livello 7 per il rimanente flusso dell'applicazione non appena viene identificata l'applicazione.

Architettura competitiva basata su proxy

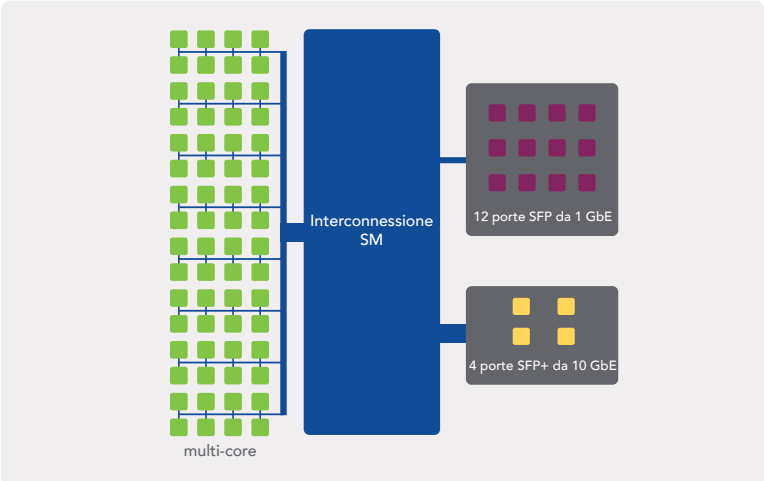


Architettura SonicWall basata sullo stream

Architettura estensibile per modularità e prestazioni estreme

L'engine RFDPI è progettato espressamente con una particolare attenzione alla scansione di sicurezza a livelli di prestazione elevati, per far fronte alla natura intrinsecamente parallela e in costante espansione del traffico di rete. Abbinata a sistemi di processore multi-core, questa architettura software incentrata sul parallelismo è perfettamente modulabile per far fronte alla domanda di ispezione approfondita dei pacchetti (DPI) in presenza di carichi di traffico elevati. La piattaforma SuperMassive si basa su processori che, diversamente dall'x86, sono ottimizzati per l'elaborazione dei pacchetti, del traffico crittografato e del traffico di rete, mantenendo al tempo stesso la flessibilità e la programmabilità sul campo, che sono un punto debole dei sistemi ASIC.

Questa flessibilità è essenziale quando è necessario proteggere nuovo codice e aggiornamenti dei comportamenti contro i nuovi attacchi che richiedono tecniche di rilevamento aggiornate e più sofisticate. Un altro aspetto della progettazione della piattaforma è l'esclusiva capacità di stabilire nuove connessioni su qualsiasi core del sistema, il che consente una modularità estrema e la capacità di far fronte ai picchi di traffico. Questo approccio consente percentuali di avvio di nuove sessioni estremamente elevate (nuove conn/sec) quando è abilitata l'ispezione approfondita dei pacchetti, una metrica fondamentale che spesso costituisce un collo di bottiglia nell'installazione dei data center.

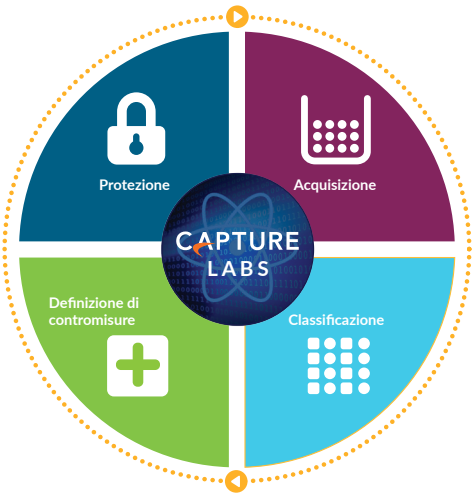


Capture Labs

Gli esperti del gruppo interno SonicWall Capture Labs si occupano di ricerca delle minacce e mettono a punto le contromisure da attuare sui firewall dei clienti per una protezione aggiornata. I tecnici acquisiscono i dati sulle minacce potenziali raccolte da molteplici fonti, tra cui il nostro premiato servizio sandbox di rete multi-engine Capture Advanced Threat Protection, e oltre 1 milione di sensori SonicWall situati in tutto il mondo che monitorano il traffico per individuare le minacce emergenti. L'analisi viene effettuata tramite apprendimento automatico con gli algoritmi Deep Learning di SonicWall per estrarre il DNA dal codice onde verificare se sia o meno collegato a qualche forma sconosciuta di codice dannoso.

A chi utilizza i firewall di prossima generazione SonicWall con le più recenti funzioni di sicurezza viene fornita una protezione delle minacce costantemente aggiornata 24 ore su 24. I nuovi aggiornamenti vengono attivati immediatamente senza riavvii o interruzioni. Le segnature nelle apparecchiature forniscono protezione da numerose classi di attacchi, coprendo fino a decine di migliaia di singole minacce con un'unica segnatura.

Oltre alle contromisure installate nell'apparecchiatura, i firewall SuperMassive hanno anche accesso al database SonicWall CloudAV[1], che amplia l'intelligenza delle segnature integrata con decine di milioni di segnature, che aumentano ogni anno di svariati milioni. Il firewall accede a questo database CloudAV attraverso un semplice protocollo brevettato per ampliare i controlli a livello dell'applicazione. Con Capture Advanced Threat Protection[1], un sandbox multi-engine basato sul cloud, le organizzazioni possono esaminare i file e i codici 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

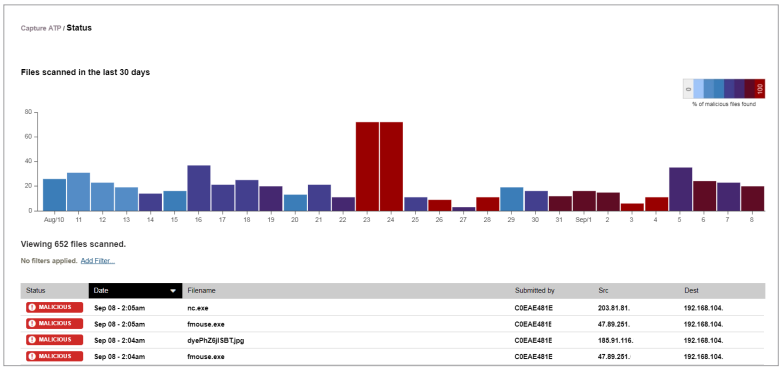
Al centro della prevenzione automatica delle violazioni in tempo reale vi sono due tecnologie di rilevamento del malware avanzate: Capture Advanced Threat Protection™ (Capture ATP) e Capture Security appliance™ (CSa).

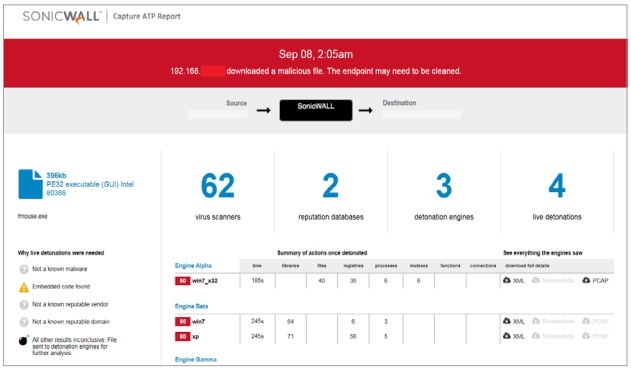
Capture ATP è una piattaforma di sandbox multi-engine basata sul cloud, che comprende Real-Time Deep Memory Inspection™ (RTDMI), sandboxing virtualizzato, emulazione completa del sistema e tecnologia di analisi a livello di hypervisor. CSa è un dispositivo per installazione interna dotato di tecnologia RTDMI, che utilizza tecniche dinamiche e statiche basate sulla memoria per emettere verdetti definitivi e precisi. Entrambe le soluzioni ampliano la protezione contro le minacce avanzate al rilevamento e alla prevenzione degli attacchi zero-day in tutta una gamma di soluzioni SonicWall come i firewall di prossima generazione.

I file sospetti vengono inviati a una delle due soluzioni dove vengono analizzati utilizzando algoritmi di deep learning con la possibilità di trattenerli nel gateway fino a quando non viene stabilito un verdetto. Nel caso di Capture ATP, quando i file vengono identificati come nocivi vengono bloccati e viene immediatamente creato un hash nel database Capture ATP per tutti i clienti per beneficiare del blocco degli attacchi successivi. In ultima analisi queste segnature vengono inviate ai firewall per realizzare difese statiche. Per motivi di privacy ed esigenze di conformità i risultati prodotti da CSa non vengono diffusi fuori dall'organizzazione.

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

Per una protezione completa degli endpoint, SonicWall Capture Client abbina la tecnologia antivirus di prossima generazione alla sandbox multi-engine basata sul cloud di SonicWall integrandola facoltativamente con firewall SonicWall.

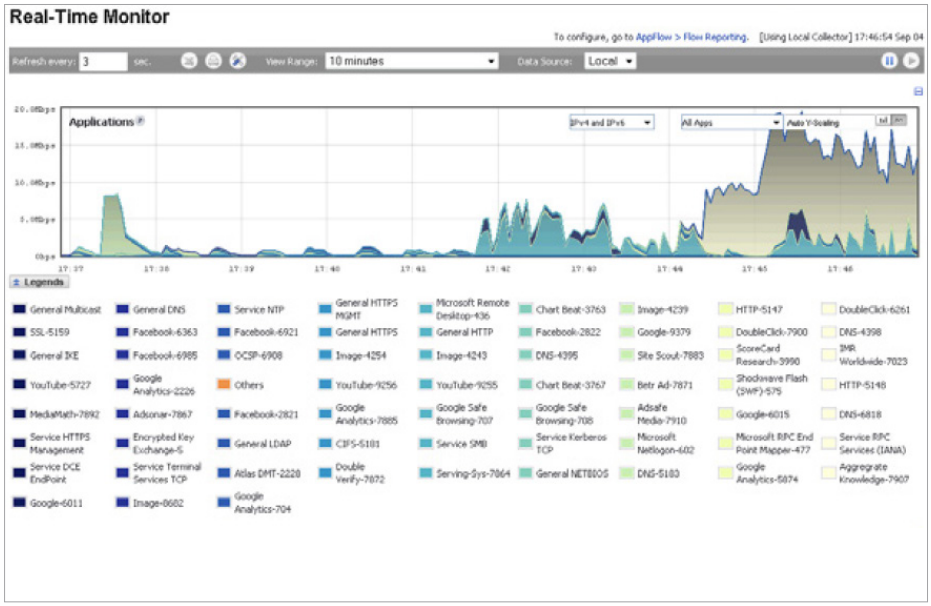




Intelligenza e controllo delle applicazioni

L'intelligenza delle applicazioni comunica agli amministratori il traffico delle applicazioni che attraversa la rete per consentire loro di programmare i controlli delle applicazioni sulla base delle priorità aziendali, limitando e bloccando quelle potenzialmente pericolose. La visualizzazione in tempo reale identifica le anomalie del traffico man mano che si manifestano, consentendo di adottare contromisure immediate nei confronti dei potenziali attacchi dall'interno e dall'esterno e dei colli di bottiglia prestazionali.

SonicWall Application Traffic Analytics[1] mette a disposizione delle organizzazioni informazioni granulari sul traffico delle applicazioni, l'uso della larghezza di banda e le minacce di sicurezza, oltre a funzioni di eliminazione delle anomalie e indagini investigative. Inoltre, le funzioni di Single Sign-On (SSO) sicuro facilitano l'esperienza dell'utente, aumentano la produttività e riducono le richieste di assistenza. La gestione dell'intelligenza e del controllo delle applicazioni risulta semplificata grazie all'interfaccia web di tipo intuitivo.



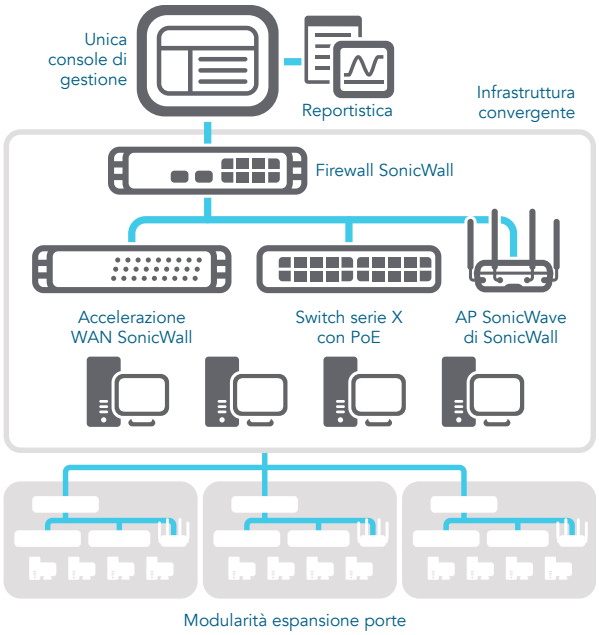
Gestione e reportistica globali

Per le organizzazioni ad elevata regolamentazione che desiderano creare una strategia coordinata di gestione della sicurezza, conformità e gestione del rischio, la soluzione opzionale Global Management System[1] (GMS®) di SonicWall mette a disposizione degli amministratori una piattaforma unificata, sicura ed espandibile per gestire i firewall, gli access point wireless e gli switch SonicWall attraverso un processo di workstream correlato e verificabile. GMS consente alle imprese di consolidare facilmente la gestione delle apparecchiature di sicurezza, ridurre la complessità amministrativa e di risoluzione dei problemi e gestire tutti gli aspetti operativi dell'infrastruttura di sicurezza, compresa la gestione e l'applicazione centralizzata delle politiche, il monitoraggio degli eventi in tempo reale, le attività degli utenti, l'identificazione delle applicazioni, l'analisi investigativa e dei flussi, la conformità e la reportistica di verifica e altro ancora. Inoltre, GMS soddisfa i requisiti di gestione delle modifiche dei firewall delle imprese tramite una funzione di automazione dei flussi di lavoro, grazie alla quale tutte le imprese potranno contare sull'affidabilità e la fiducia necessarie per l'attuazione delle corrette politiche dei firewall al momento giusto e nel rispetto delle normative. GMS è un metodo coerente per gestire la sicurezza delle reti in funzione dei processi gestionali e dei livelli di servizio, semplificando drasticamente la gestione del ciclo vitale di tutti gli ambienti di sicurezza nel loro complesso rispetto alla gestione basata sui singoli dispositivi.

Attuazione sicura della conformità con GSM di SonicWall

Vantaggi

- Gestione centralizzata
- Gestione delle politiche priva di errori
- Potente controllo accessi
- Controlli di verifica completi
- Modelli di report PCI, HIPAA, SOX
- Bassi costi operativi



[1] *Richiede un abbonamento aggiuntivo*

Funzioni

ENGINE RFDPI

Funzione	Descrizione
Reassembly-Free Deep Packet Inspection (RFDPI)	Si tratta di un engine di ispezione proprietario, brevettato e di prestazioni elevate, che esegue analisi bidirezionali del traffico basate sui flussi senza proxy o buffering allo scopo di individuare tentativi di intrusione, rilevare malware e identificare il traffico delle applicazioni in qualsiasi 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 di ispezione DPI su milioni di flussi di rete simultanei, senza limiti per la dimensione dei flussi e dei file. Inoltre può essere applicata sia a protocolli comuni, sia a flussi TCP primari.
Architettura altamente parallela e modulabile	L'esclusivo engine RFDPI basato su architettura multi-core consente un'elevata velocità di DPI e la creazione di 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, riducendo notevolmente la latenza dell'ispezione DPI e correlando tutte le informazioni sulle minacce in un'unica architettura.

FIREWALL E CONNETTIVITÀ DI RETE

Funzione	Descrizione
API REST	Consentono al firewall di ricevere e sfruttare tutti i feed di intelligenza proprietari dei produttori di dispositivi originali e di terzi per contrastare minacce avanzate come zero-day, utenti malintenzionati, credenziali compromesse, ransomware e minacce persistenti avanzate.
Ispezione Stateful Packet	Tutto il traffico della rete viene ispezionato, esaminato e reso conforme alle politiche di accesso del firewall.
Alta disponibilità/clustering	La serie SuperMassive supporta le modalità ad alta disponibilità Attivo/Passivo (A/P) con sincronizzazione statica, DPI Attivo/Attivo (A/A) e clustering Attivo/Attivo. La modalità DPI Attivo/Attivo trasferisce il carico di lavoro dell'ispezione deep packet ai core dell'appliance passiva per ottimizzare il throughput.
Protezione da attacchi DDoS/DoS	La protezione da flood SYN offre una difesa contro gli attacchi DOS mediante tecnologie di blacklisting al layer 3 (SYN proxy) e al layer 2 (SYN). Inoltre, protegge da DOS/DDoS attraverso la protezione da flood UDP/ICMP e la limitazione della velocità di connessione.
Supporto IPv6	Il protocollo IPv6 (Internet Protocol versione 6) è in procinto di sostituire il protocollo IPv4. Con l'ultimo SonicOS 6.2 , l'hardware supporterà il filtraggio e la modalità wire.
Opzioni di implementazione flessibili	SuperMassive Series può essere installata con le modalità tradizionali NAT, bridge Layer 2, 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 basato sulle politiche crea percorsi basati sul protocollo per indirizzare il traffico a una connessione WAN preferita, con la possibilità di ricadere su una WAN secondaria in caso di interruzione.
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 gatekeeper H.323 e proxySIP	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+, attraverso un unico pannello di controllo utilizzando il dashboard di gestione del firewall per gli switch di rete serie X di Dell.
Autenticazione biometrica	Supporto dell'autenticazione per dispositivi mobili come il riconoscimento delle impronte digitali, che non può essere facilmente condivisa o duplicata, per autenticare in modo sicuro l'identità degli utenti che accedono alla rete.
Autenticazione aperta e social login	Consente agli utenti ospiti di utilizzare le loro 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 multi-dominio	Mette a disposizione un modo semplice e rapido per amministrare le politiche di sicurezza in tutti i domini di rete e la gestione delle singole politiche per un dominio o un gruppo di domini.

GESTIONE E REPORTISTICA

Funzione	Descrizione
Global Management System[1] (GMS)	GMS di SonicWall effettua il monitoraggio, la configurazione e la reportistica di diverse apparecchiature SonicWall attraverso un'unica console di gestione con un interfaccia intuitiva, riducendo i costi e la complessità della 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.
Report sul flusso delle applicazioni con IPFIX/ NetFlow	Le statistiche di traffico e i dati sull'uso delle applicazioni possono essere esportati tramite i protocolli IPFIX o NetFlow per il monitoraggio e la creazione di report in tempo reale e storici con strumenti come SonicWall Scrutinizer o altri che supportano IPFIX e NetFlow con estensioni.

Funzioni

RETE PRIVATA VIRTUALE (VPN)

Funzione	Descrizione
Provisioning automatico delle VPN	Semplifica l'installazione dei firewall in ambienti distribuiti complessi automatizzando il provisioning iniziale del gateway VPN da sede a sede tra i firewall SonicWall, garantendo l'applicazione istantanea e automatica della sicurezza e della connettività.
VPN per la connettività da sede a sede	La rete VPN IPSec di prestazioni elevate consente di utilizzare la serie SuperMassive come concentratore di VPN per migliaia di altre sedi di grandi dimensioni, filiali e per chi lavora da casa.
Accesso remoto tramite VPN SSL o client IPSec	Sfruttando la tecnologia VPN SSL senza client o un client IPSec semplice da gestire, è possibile accedere in tutta semplicità a messaggi di posta elettronica, file, computer, siti intranet e applicazioni da un'ampia serie di piattaforme.
Gateway per la rete VPNridondante	Se si utilizzano più WAN, è possibile configurare una VPN principale e una secondaria per consentire failover e failback automatizzati e trasparenti per tutte le sessioni VPN.
VPN basata 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 percorsi alternativi.

SENSIBILITÀ AL CONTESTO/AL CONTENUTO

Funzione	Descrizione
Tracciamento delle attività degli utenti	Le tecnologie AD/LDAP/Citrix1/Terminal Services1 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 determinati paesi	Con questa opzione è possibile identificare e controllare il traffico di rete in ingresso o in uscita da determinati paesi. 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 associati 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]

Funzione	Descrizione
Sandboxing multi-engine	La piattaforma sandbox multi-engine, che comprende l'emulazione completa del sistema e tecnologie di analisi a livelli hypervisor, esegue il codice sospetto nell'ambiente sandbox virtualizzato, ne analizza il comportamento e fornisce visibilità completa sulle attività dannose
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 associati aunindirizzo IP.
Analisi di un'ampia varietà di file	Supporta l'analisi di un'ampia gamma di tipi di file, compresi programmi eseguibili (PE), DLL, PDF, documenti MS Office, archivi, JAR e APK, oltre a svariati sistemi operativi, tra cui Windows, Android, Mac e ambienti multi-browser.
Rapida distribuzione delle segnature	Quando un file è identificato come dannoso, viene immediatamente distribuita una segnatura ai firewall con abbonamento a SonicWall Capture e ai database delle segnature per Gateway Anti-Virus GRID e IPS, nonché ai database di URL, IP e reputazione dei domini nel giro di 48 ore.
Capture Client	Capture Client è una piattaforma client unificata che presenta numerose funzioni di protezione dell'endpoint, tra cui quella avanzata contro i 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 endpoint.

CAPTURE SECURITY APPLIANCE (CSa)

Funzione	Descrizione
Rilevamento del malware basato sulla conformità	Analizza i file sospetti direttamente nel proprio ambiente senza inviare il file con i risultati a cloud esterni.
Integrazioni preinstallate	CSa supporta integrazioni preinstallate con altre soluzioni di sicurezza (sicurezza firewall e posta elettronica) di SonicWall.
Protezione quasi in tempo reale	La tecnologia brevettata RTDMI di SonicWall aiuta a rilevare rapidamente il malware, anche quello sconosciuto, che può essere bloccato da CSa fino al verdetto di validazione sui firewall SonicWall di prossima generazione.
Installazione	CSa può essere configurato su reti private collegate direttamente a un unico edge firewall o essere raggiungibile direttamente da Internet o utilizzando VPN sui firewall delle filiali.

PREVENZIONE DELLE MINACCE CRITTOGRAFATE[1]

Funzione	Descrizione
Decrittazione e ispezione TLS/SSL	Esegue la decrittazione e l'ispezione del traffico SSL/TLS in tempo reale, senza proxy, di malware, intrusioni e fughe di dati, e applica politiche di controllo di applicazioni, URL e contenuti per proteggere la rete dalle minacce nascoste nel traffico crittografato TLS/SSL. Opzione compresa negli abbonamenti di sicurezza per tutti i modelli.
Ispezione SSH	La Deep Packet Inspection di SSH (DPI-SSH) esegue la decrittazione e l'ispezione dei dati che attraversano il tunnel SSH per prevenire gli attacchi che sfruttano SSH.

PREVENZIONE DELLE INTRUSIONI[1]

Funzione	Descrizione
Protezione basata su contromisure	Il sistema di prevenzione delle intrusioni (IPS) integrato utilizza le segnature e altre contromisure per eseguire la scansione dei payload dei pacchetti in cerca di exploit e vulnerabilità, coprendo un'ampia serie di attacchi e vulnerabilità.
Aggiornamenti automatici dellesegnature	Il team SonicWall Threat Research ricerca continuamente nuovi aggiornamenti e li installa in numerose contromisure IPS, che interessano oltre 50 categorie di attacchi. Gli aggiornamenti hanno effetto immediato, 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.

Funzioni

PREVENZIONE DELLE INTRUSIONI[1] (CONT.)	
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 protezione dell'uso improprio e delle anomalie dei protocolli	Individua e blocca gli attacchi che sfruttano i protocolli noti per tentare di eludere il controllo IPS.
Protezione zero-day	Per proteggere la rete dagli attacchi zero-day, questa opzione assicura aggiornamenti costanti 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 assicurano che le minacce basate su tecniche di evasione ailivelli 2-7 non possano entrare in rete senza essere rilevate.

PREVENZIONE DELLE MINACCE[1]	
Funzione	Descrizione
Antimalware a livello gateway	L'engine 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 illimitate in tutte le porte e in tutti i flussi TCP.
Protezione del malware CloudAV	Un database residente sui server cloud SonicWall, costantemente aggiornato con decine di milioni di segnature delle minacce, viene consultato per ottimizzare le capacità del database di segnature integrato nel dispositivo, garantendo così un'ampia copertura delle minacce da parte dell'engine 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	L'engine 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.
Ampio supporto di 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.

INTELLIGENZA E CONTROLLO DELLE APPLICAZIONI[1]	
Funzione	Descrizione
Controllo delle applicazioni	Per potenziare la sicurezza e la produttività della rete vengono controllate le applicazioni, o le singole funzioni delle stesse, identificate dall'engine RFDPI utilizzando un database in continua espansione, contenente migliaia di segnature di applicazioni.
Identificazione di applicazioni personalizzate	Controlla le applicazioni personalizzate generando segnature basate su parametri specifici o su modelli di comunicazione in rete univoci per ogni applicazione, in modo da garantire un maggiore controllo sulla 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]	
Funzione	Descrizione
Filtraggio dei contenuti interno/esterno	Mette in atto le politiche di utilizzo accettabili e blocca l'accesso a siti web contenenti informazioni o immagini discutibili o non produttive con Content Filtering Service.
Filtraggio contenuti applicato al client	Estende l'applicazione delle politiche 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]	
Funzione	Descrizione
Protezione su più livelli	Utilizza le funzioni del firewall come primo livello di difesa perimetrale, insieme alla protezione degli endpoint, per bloccare i virus che entrano nella rete tramite laptop, chiavette USB e altri sistemi non protetti.
Opzione di applicazione automatizzata	Garantisce che tutti i computer che accedono alla rete siano dotati della versione più recente delle segnature antivirus e antispyware installate e attive, eliminando i costi normalmente associati alla gestione antivirus e antispyware sui singoli desktop.
Distribuzione e installazione automatizzate	La distribuzione e l'installazione macchina per macchina dei client antivirus e antispyware sono automatizzate sull'intera rete, il che riduce al minimo l'impegno amministrativo.
Protezione virus automatica, sempre attiva	I frequenti aggiornamenti antivirus e antispyware vengono installati in modo trasparente su tutti i desktop e i file server per migliorare la produttività dell'utente finale e ridurre la gestione della sicurezza.
Antivirus di prossima generazione	Capture Client utilizza un engine 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 iprogrammi spyware più diffusi e pericolosi, prima che questi possano carpire dati sensibili da computer fissi o portatili.

[1] *Richiede un abbonamento aggiuntivo*

SONICWALL®

Riepilogo delle funzioni

Firewall

- Ispezione Stateful Packet
- 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

Decrittazione e ispezione 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
- Intelligenza delle minacce con aggiornamenti in tempo reale
- Blocco fino al verdetto
- Capture Client

Prevenzione delle intrusioni[2]

- Scansione basata sulle segnature
- Aggiornamenti automatici delle segnature
- Engine di ispezione bidirezionale
- Gruppo di regole IPS granulari
- Implementazione GeoIP
- Filtraggio botnet con elenco dinamico
- 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 componenti applicazioni
- Gestione della larghezza di banda delle applicazioni
- Creazione di segnature per applicazioni personalizzate
- Prevenzione della perdita di dati
- Creazione di report sulle applicazioni tramite NetFlow/IPFIX
- Tracciamento delle attività degli utenti (SSO)
- Ampio database di segnature delle applicazioni

Filtraggio dei contenuti Web[2]

- Filtraggio degli URL
- Proxy avoidance
- Blocco in base a parole chiave
- Inserimento intestazione HTTP
- Categorie CFS per la gestione della larghezza di banda
- Modello di politica unificato con controllo delleapplicazioni
- Content Filtering Client

VPN

- Provisioning automatico delle VPN
- VPN IPSec per la connettività da sede a sede
- 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 sul routing (OSPF, RIP, BGP)

Connettività di rete

- LAG dinamico tramite LACP
- PortShield
- Frame Jumbo
- Individuazione percorsi MTU
- Registrazione avanzata
- VLAN trunking
- Port mirroring
- QoS layer 2
- Sicurezza delle porte
- Routing dinamico (RIP/OSPF/BGP)
- Controller wireless SonicWall
- Routing basato sulle politiche (ToS/metrico ed ECMP)
- NAT
- Server DHCP
- Gestione della larghezza di banda
- Aggregazione dei link (statica e dinamica)
- Porte ridondanti
- Alta disponibilità A/P con sincronizzazione statica
- Clustering A/A
- Bilanciamento del carico in ingresso/in uscita
- Bridge L2, modalità wire/virtual wire, modalità tap, modalità NAT
- Failover WAN 3G/4G (non su SuperMassive 9800)
- Routing asimmetrico
- Supporto CAC (Common Access Card)

Wireless

- WIDS/WIPS
- Analisi dello spettro di RF
- Prevenzione di rogue AP
- Fast roaming (802.11k/r/v)
- Visualizzazione in pianta/della topologia
- Band steering
- Beamforming
- AirTime Fairness
- MiFi Extender
- Quota ciclica ospite
- Portale ospite LHM

VoIP

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

Gestione e monitoraggio

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

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

Specifiche di sistema della serie SuperMassive 9000

CARATTERISTICHE GENERALI DEI FIREWALL	9200	9400	9600	9800
Sistema operativo	SonicOS			
Core di elaborazione di sicurezza	24	32		64
Interfacce	4 SFP+ da 10GbE, 8 SFP da 1GbE, 8 da 1GbE, gestione 1GbE, 1 console			4 SFP+ da 10GbE, 12 SFP da 1GbE, 8 da 1GbE, gestione 1GbE, 1 console
Memoria (RAM)	8 GB	16 GB	32 GB	64 GB
Memorizzazione	Flash			2 SSD da 80GB SSD, Flash
Espansione	1 slot di espansione (sul retro)*, scheda SD*			
Gestione	CLI, SSH, GUI, GMS			
Utenti SSO	80.000	90.000	100.000	110.000
Numero massimo di access point supportati	128			-
Accesso	Analyzer, Local Log, Syslog			
Elevata disponibilità	Attivo/Passivo con sincronizzazione statica, DPI Attivo/Attivo con sincronizzazione statica			
PRESTAZIONI FIREWALL/VPN	**9200**	**9400**	**9600**	**9800**
Throughput di ispezione del firewall[1]	15 Gbps	20 Gbps	20 Gbps	31,8 Gbps
Throughput di prevenzione delle minacce[2]	3 Gbps	4,4 Gbps	4,5 Gbps	10,5 Gbps
Throughput di ispezione delle applicazioni[2]	5 Gbps	10 Gbps	11,5 Gbps	23 Gbps
Throughput IPS[2]	5 Gbps	10 Gbps	11,5 Gbps	21,3 Gbps
Throughput di ispezione anti-malware[1]	3,5 Gbps	4,5 Gbps	5,0 Gbps	11 Gbps
Throughput IMIX	4,4 Gbps	5,5 Gbps	5,5 Gbps	7,3 Gbps
Throughput di ispezione approfondita del traffico TLS crittografato (DPI SSL)[2]	1,0 Gbps	2,0 Gbps	2,0 Gbps	3,5 Gbps
Throughput VPN[3]	5 Gbps	10 Gbps	11,5 Gbps	14,3 Gbps
Connessioni al secondo	100.000/sec	130.000/sec	130.000/sec	229.000/sec
Numero massimo di connessioni (SPI)	5,0M	7,5M	10,0M	20,0M
Numero massimo di connessioni (DPI)	1,5M	1,5M	2,0M	8,0M
Connessioni SSL DPI[6] (numero massimo)	8.000 (15.500[6])	10.000 (17.500[6])	12.000 (22.500[6])	650.000
VPN	**9200**	**9400**	**9600**	**9800**
Tunnel VPN da sede a sede	10.000			25.000
Client VPN IPSec (max)	2.000 (4.000)	2.000 (6.000)	2.000 (10.000)	
Client VPN SSL NetExtender (numero massimo)	2 (3.000)	2 (3.000)	50 (3.000)	50 (3.000)
Crittografia/autenticazione	DES, 3DES, AES (128, 192, 256-bit)/MD5, SHA-1, Suite B, Common Access Card (CAC)			
Scambio chiavi	Gruppi Diffie-Hellman 1, 2, 5, 14v			
VPN basata su routing	RIP, OSPF			
CONNETTIVITÀ DI RETE	**9200**	**9400**	**9600**	**9800**
Assegnazione indirizzo IP	Statica (DHCP, PPPoE, L2TP e client PPTP), server DHCP interno, DHCP relay[4]			
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, static route, routing basato sulle politiche, multicast			
Qualità del servizio (QoS)	Priorità della larghezza di banda, larghezza di banda massima, larghezza di banda garantita, contrassegno DSCP, 802.1p			
Autenticazione	LDAP (multi-dominio), XAUTH/RADIUS, SSO, Novell, database utenti interno, Terminal Services[5], Citrix[5]			
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	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	Alimentatore doppio, ridondante, sostituibile a caldo, 300 W			Alimentatore doppio, ridondante, sostituibile a caldo, 500 W
Ventole	Doppie, ridondanti, sostituibili a caldo			
Visualizzazione	Display a LED frontale			
Alimentazione in ingresso	100-240 Vca, 50-60 Hz			
Potenza max assorbita (W)	200			350
MTBF @25°C in ore	188.719	187.702	186.451	126.144
MTBF @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			9x60x43 cm
Peso	8,2 kg			18,38 kg
Peso RAEE	10,4 kg			22,4 kg
Peso con la confezione	13,3 kg			29,64 kg
Principali normative di conformità	FCC Classe A, ICES Classe A, CE (EMC, LVD, RoHS), C-Tick, VCCI Classe A, UL/cUL, TUV/GS, CB, CoC UL (Messico), RAEE, REACH, BSMI, KCC/MSIP, ANATEL			
Temperatura di funzionamento	15-40°C			
Umidità	10-90%, non condensante			

[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. Il test viene eseguito con più flussi attraverso varie coppie di porte. Rilevazione throughput di prevenzione delle minacce con Gateway AV, Anti-Spyware, IPS e Application Control attivati. [3] Rilevazione throughput VPN mediante traffico UDP con pacchetti di 1.280 byte. [4] Valido per SuperMassive 9200, 9400 e 9600. È stata presentata domanda di certificazione UC APL per SuperMassive 9800. [5] Supportato su SonicOS 6.1 e 6.2. [6] Ogni 125.000 connessioni DPI ridotte, il numero di connessioni DPI SSL disponibili aumenta di 750. *Uso futuro. Tutte le specifiche, le funzioni e le informazioni sulla disponibilità sono soggette a modifiche.

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
CONTRATTO ASSISTENZA E SICUREZZA SUPERMASSIVE 9200	**SKU**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Firewall management and reporting, Shadow IT Visibility, and 24x7 Support for SuperMassive 9200 (1 anno)	01-SSC-1570
Capture Advanced Threat Protection for SuperMassive 9200 (1 anno)	01-SSC-1575
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention, Content Filtering with Support for 9200 (1 anno)	01-SSC-4172
Intrusion Prevention, Anti-Malware, CloudAV, Application Intelligence, Control and Visualization for SuperMassive 9200 (1 anno)	01-SSC-4202
Content Filtering Premium Business Edition for 9200 (1 anno)	01-SSC-4184
Platinum Support for the SuperMassive 9200 (1 anno)	01-SSC-4178
CONTRATTO ASSISTENZA E SICUREZZA SUPERMASSIVE 9400	**SKU**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Firewall management and reporting, Shadow IT Visibility, and 24x7 Support for SuperMassive 9400 (1 anno)	01-SSC-1580
Capture Advanced Threat Protection for SuperMassive 9400 (1 anno)	01-SSC-1585
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention, Content Filtering with Support for 9400 (1 anno)	01-SSC-4136
Intrusion Prevention, Anti-Malware, CloudAV, Application Intelligence, Control and Visualization for SuperMassive 9400 (1 anno)	01-SSC-4166
Content Filtering Premium Business Edition for 9400 (1 anno)	01-SSC-4148
Platinum Support for the SuperMassive 9400 (1 anno)	01-SSC-4142
CONTRATTO ASSISTENZA E SICUREZZA SUPERMASSIVE 9600	**SKU**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Firewall management and reporting, Shadow IT Visibility, and 24x7 Support for SuperMassive 9600 (1 anno)	01-SSC-1590
Capture Advanced Threat Protection for SuperMassive 9600 (1 anno)	01-SSC-1595
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention, Content Filtering with Support for 9600 (1 anno)	01-SSC-4100
Intrusion Prevention, Anti-Malware, CloudAV, Application Intelligence, Control and Visualization for SuperMassive 9600 (1 anno)	01-SSC-4130
Content Filtering Premium Business Edition for 9600 (1 anno)	01-SSC-4112
Platinum Support for the SuperMassive 9600 (1 anno)	01-SSC-4106
CONTRATTO ASSISTENZA E SICUREZZA SUPERMASSIVE 9800	**SKU**
Advanced Gateway Security Suite – Capture ATP, Threat Prevention, Firewall management and reporting, Shadow IT Visibility, and 24x7 Support for SuperMassive 9800 (1 anno)	01-SSC-1183
Capture Advanced Threat Protection for SuperMassive 9800 (1 anno)	01-SSC-1188
Comprehensive Gateway Security Suite: Application Intelligence, Threat Prevention, Content Filtering with Support for 9800 (1 anno)	01-SSC-0809
Intrusion Prevention, Anti-Malware, CloudAV, Application Intelligence, Control and Visualization for SuperMassive 9800 (1 anno)	01-SSC-0827
Content Filtering Premium Business Edition for 9800 (1 anno)	01-SSC-0821
Gold 24x7 Support for the SuperMassive 9800 (1 anno)	01-SSC-0815
MODULI E ACCESSORI*	**SKU**
SonicWall SuperMassive 9800 Series system fan FRU	01-SSC-0204
SonicWall SuperMassive 9800 Series power supply AC FRU	01-SSC-0203
SonicWall SuperMassive 9000 Series system fan FRU	01-SSC-3876
SonicWall SuperMassive 9000 Series power supply AC FRU	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-LX SFP	01-SSC-9790
Modulo in rame 1000BASE-T SFP	01-SSC-9791
GESTIONE E REPORTISTICA	**SKU**
SonicWall GMS 10-node software license	01-SSC-3363
SonicWall GMS E-Class 24x7 Software Support for 10 nodes (1 anno)	01-SSC-6514
SonicWall Scrutinizer virtual appliance with Flow Analytics Module software license for up to 5 nodes (comprende un anno di 24x7 Software Support)	01-SSC-3443
SonicWall Scrutinizer with Flow Analytics Module software license for up to 5 nodes (comprende un anno di 24x7 Software Support)	01-SSC-4002
SonicWall Scrutinizer Advanced Reporting Module software license for up to 5 nodes (comprende un anno di 24x7 Software Support)	01-SSC-3773

**Per l'elenco completo dei moduli SFP e SFP+ supportati rivolgersi a un centro assistenza SonicWall.*

SonicWall

SonicWall fornisce soluzioni di cybersecurity illimitata per l'era iperdistribuita in una realtà lavorativa in cui tutto è all'insegna del telelavoro, della mobilità e della mancanza di sicurezza. Conoscendo l'ignoto, offrendo una visibilità in tempo reale e rendendo possibili economie innovative, SonicWall colma le lacune di cybersecurity per aziende, enti pubblici e PMI in ogni parte del mondo. Per ulteriori informazioni visitare www.sonicwall.com

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

Datasheet-SuperMassive-US-COG-2465