Piattaforma SonicOS

L'architettura SonicOS rappresenta il cuore di tutti i firewall SonicWall, dal SuperMassive™ 9800 ai dispositivi TZ SOHO. SonicOS utilizza la tecnologia d'ispezione approfondita dei pacchetti (deep packet inspection) in combinazione con microprocessori di sicurezza multi-core dedicati per fornire efficaci funzioni di prevenzione delle violazioni, identificazione e controllo delle applicazioni con visualizzazione in tempo reale, connettività VPN (Virtual Private Networking) ad alta velocità e altre solide funzionalità di sicurezza.

Funzionalità firewall

Motore Reassembly-Free Deep Packet Inspection (RFDPI)	
Funzionalità	Descrizione
Reassembly-Free Deep Packet Inspection (RFDPI)	Si tratta di un motore di ispezione proprietario, brevettato e ad alte prestazioni, 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 che 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, riducendo notevolmente la latenza dell'ispezione DPI e correlando tutte le informazioni sulle minacce in un'unica architettura.
Firewall e connettività di rete	
Funzionalità	Descrizione
API per la gestione delle minacce	Consente al firewall di ricevere e utilizzare flussi di intelligence proprietari, OEM o di terze parti, per contrastare minacce zero-day, attacchi malicious insider, credenziali compromesse, ransomware e minacce persistenti avanzate.
Ispezione Stateful Packet	Tutto il traffico della rete viene ispezionato, esaminato e reso conforme alle policy di accesso del firewall.
Alta disponibilità/clustering	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	I firewall possono essere installati 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.

Firewall e connettività di rete (cont.)	
Funzionalità	Descrizione
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 Dell serie X 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	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 guest di utilizzare le credenziali dei propri servizi di social network come Facebook, Twitter o Google+ per registrarsi e accedere a Internet e ad altri servizi guest attraverso la rete wireless host, la LAN o zone DMZ utilizzando l'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 creazione di rapporti	
Funzionalità	Descrizione
Global Management System (GMS)[1]	Con SonicWall GMS è possibile monitorare diverse appliance SonicWall, configurarle e creare rapporti per mezzo di un'unica interfaccia intuitiva che riduce la complessità e i costi gestionali.
Gestione avanzata con un unico dispositivo	I server cloud di SonicWall ospitano un database sempre aggiornato di oltre 17 milioni di firme sulle minacce, che viene consultato per potenziare le funzionalità del database di firme integrato e assicurare alle opzioni RFDPI una copertura estesa delle minacce.
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.
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 site-to-site tra i firewall SonicWall, garantendo l'applicazione istantanea e automatica della sicurezza e della connettività.
VPN per una connettività Site-to-Site	La rete VPN IPSec ad alte prestazioni consente di utilizzare i dispositivi della serie SuperMassive come concentratori di VPN per migliaia di utenti privati, filiali o altri siti di grandi dimensioni.
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 e-mail, file, computer, siti Intranet e applicazioni da un'ampia serie di piattaforme.
Gateway VPN ridondante	Se si usano più WAN, è possibile configurare una VPN primaria e secondaria per un failover e un failback automatici di 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, eliminando così il filtraggio indesiderato di indirizzi IP a causa di classificazioni errate.
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.

Servizi in abbonamento per la prevenzione delle violazioni

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 all'identificazione	Per impedire l'ingresso di file potenzialmente dannosi nella rete, i file inviati al cloud per l'analisi possono essere trattenuti al gateway finché non viene determinata la loro natura.
Analisi di un'ampia varietà di file	Supporta l'analisi di un'ampia gamma di tipi di file, tra cui programmi eseguibili (PE), DLL, documenti PDF e 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 signature viene inviata immediatamente ai firewall con abbonamento al servizio SonicWall Capture, 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.
Prevenzione delle minacce crittografate	
Funzionalità	Descrizione
Ispezione e decrittografia SSL	Il traffico SSL/TLS crittografato viene immediatamente decrittografato e analizzato senza l'uso di proxy per individuare malware, intrusioni e perdite di dati, e vengono applicate policy per il controllo di contenuti, URL e applicazioni che proteggono dalle minacce nascoste nel traffico SSL crittografato. L'opzione è inclusa negli abbonamenti di sicurezza di tutti i modelli, tranne SOHO. Per quest'ultimo è venduta come licenza a parte.
Ispezione DPI-SSH	L'ispezione approfondita dei pacchetti del protocollo SSH (DPI-SSH) decripta e ispeziona i dati che attraversano i tunnel SSH, per prevenire attacchi basati su 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.
Anomalia/abuso di 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 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 impediscono l'ingresso non rilevato delle minacce nella rete, grazie all'uso di tecniche di evasione nei livelli da 2 a 7.
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	I server cloud di SonicWall ospitano un database sempre aggiornato con decine di milioni di firme sulle minacce, che viene consultato per potenziare le funzionalità del database di firme integrato e assicurare alle opzioni RFDPI una copertura estesa delle minacce.
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.

Prevenzione delle minacce (cont.)	
Funzionalità	Descrizione
Ispezione bidirezionale dei TCP primari	Il motore RFDPI esegue l'analisi bidirezionale dei flussi TCP primari su tutte le porte per rilevare e prevenire le minacce in ingresso e in uscita.
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 alla ricerca di malware, anche se non sono eseguiti in porte standard note.
Controllo e intelligence delle applicazioni[1]	
Funzionalità	Descrizione
Controllo delle applicazioni	Verifica delle applicazioni o di singole funzionalità rilevate dal motore RFDPI a fronte di un database in crescita, contenente migliaia di firme di applicazioni. Questo controllo potenzia la sicurezza e la produttività della rete.
Identificazione di applicazioni personalizzate	Per verificare le applicazioni personalizzate è possibile creare firme basate su schemi o parametri specifici, che risultano univoci per un'applicazione nelle relative comunicazioni di rete. Ciò consente di acquisire maggiore controllo sulla rete.
Gestione della larghezza di banda delle applicazioni	Questa opzione regola in modo granulare la larghezza di banda disponibile e la assegna alle applicazioni (o categorie di applicazioni) più importanti, bloccando il traffico delle applicazioni superflue.
Visualizzazione del traffico integrata/esterna	Identifica l'utilizzo della larghezza di banda e analizza il comportamento della rete, visualizzando in tempo reale il traffico delle applicazioni direttamente sul dispositivo e generando rapporti sul traffico applicativo per analisi esterne tramite NetFlow/IPFix.
Controllo granulare	Questa opzione consente di controllare le applicazioni o 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/servizi Terminal/Citrix.
Filtraggio dei contenuti[1]	
Funzionalità	Descrizione
Filtraggio dei contenuti interno/esterno	Questa funzionalità utilizza il Content Filtering Service per applicare policy relative a un utilizzo accettabile e bloccare l'accesso ai siti Web che contengono informazioni o immagini inopportune o di ostacolo alla produttività.
Content Filtering Client	Consente di applicare policy che bloccano contenuti Internet specifici per i dispositivi Windows, Mac OS, Android e Chrome situati all'esterno del perimetro del firewall.
Controlli granulari	Mediante combinazioni di categorie è possibile 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	Le funzionalità del firewall sono utilizzate come primo livello di difesa presso il perimetro, insieme alla protezione degli endpoint che impedisce l'ingresso di virus nella rete attraverso notebook, unità USB e altri sistemi non protetti.
Opzione di applicazione automatizzata	Questa opzione verifica che in tutti i computer con accesso alla rete sia installata e attiva la versione più recente delle firme antivirus e antispyware. In questo modo si eliminano i costi normalmente legati alla gestione degli antivirus e degli antispyware sui computer desktop.
Opzione di installazione automatizzata	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.
Protezione antispyware	Grazie all'opzione di protezione avanzata contro gli spyware, è possibile eseguire scansioni e bloccare l'installazione di una serie completa di programmi spyware su desktop e notebook prima che vengano trasmessi dati riservati. Questo potenzia le prestazioni e la sicurezza dei computer desktop.

[1] Richiede un abbonamento aggiuntivo

Riepilogo delle funzionalità di SonicOS

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 per la gestione delle minacce

Ispezione e decrittografia SSL/SSH[2]

- Deep Packet Inspection per TLS/SSL/SSH
- Inclusione/esclusione di oggetti, gruppi o nomi 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
- Capacità di blocco automatico

Prevenzione delle intrusioni[2]

- Scansione basata sulle firme
- Aggiornamenti automatici delle firme
- Motore di ispezione bidirezionale
- Funzionalità per regole IPS granulari
- Identificazione tramite 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 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 rapporti sulle applicazioni tramite NetFlow/IPFIX
- Tracciamento delle attività degli utenti (SSO)
- Database completo di firme delle applicazioni

Filtraggio dei contenuti Web[2]

- Filtraggio degli URL
- Tecnologia antiproxy
- Blocco in base a parole chiave
- Categorie di classificazione CFS per la gestione della larghezza di banda
- 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 VPN ridondante
- Mobile Connect per iOS, Mac OS X, Windows, Chrome, Android e Kindle Fire
- VPN basata sul routing (RIP/OSPF/BGP)

Connettività di rete

- PortShield
- Frame Jumbo
- Indagine del percorso MTU
- Registrazione avanzata
- VLAN trunking
- Mirroring delle porte (non su TZ e NSA 2600)
- QoS livello 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)

VoIP

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

Gestione e monitoraggio

- GUI Web
- CLI (Command Line Interface)
- SNMPv2/v3
- Gestione e creazione di rapporti centralizzate con il SonicWall Global Management System (GMS)[2]
- Accesso
- Esportazione per Netflow/IPFix
- Backup della configurazione basato sul cloud
- Piattaforma analitica di sicurezza BlueCoat
- Visualizzazione della larghezza di banda e delle applicazioni
- Gestione IPv4 e IPv6
- Creazione immediata di rapporti (Scrutinizer)
- Display di gestione LCD
- Gestione di switch Dell serie X[1]

Wireless

- MU-MIMO
- Tool di pianificazione wireless
- Cambio automatico di banda
- Beamforming
- Equità di accesso alla rete (AirTime fairness)
- Estensore MiFi
- Quote cicliche guest

Wireless integrato (solo TZ Series)

- Dual-band (2,4 GHz e 5 GHz)
- Standard wireless 802.11 a/b/g/n/ac
- Rilevamento e prevenzione delle intrusioni wireless
- Servizi guest wireless
- Messaggistica hotspot leggera
- Segmentazione dei punti di accesso virtuali
- Captive portal
- ACL cloud

[1] *Non supportato su SonicOS 6.2.7.7*
[2] *Richiede un abbonamento aggiuntivo.*

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, CA 95054
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

© 2017 SonicWall Inc. TUTTI I DIRITTI RISERVATI. SonicWall è un marchio o marchio registrato di SonicWall Inc. e/o delle sue affiliate negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi e marchi registrati appartengono ai rispettivi proprietari.

Datasheet-SonicOSplatform-US-VG-MKTG480