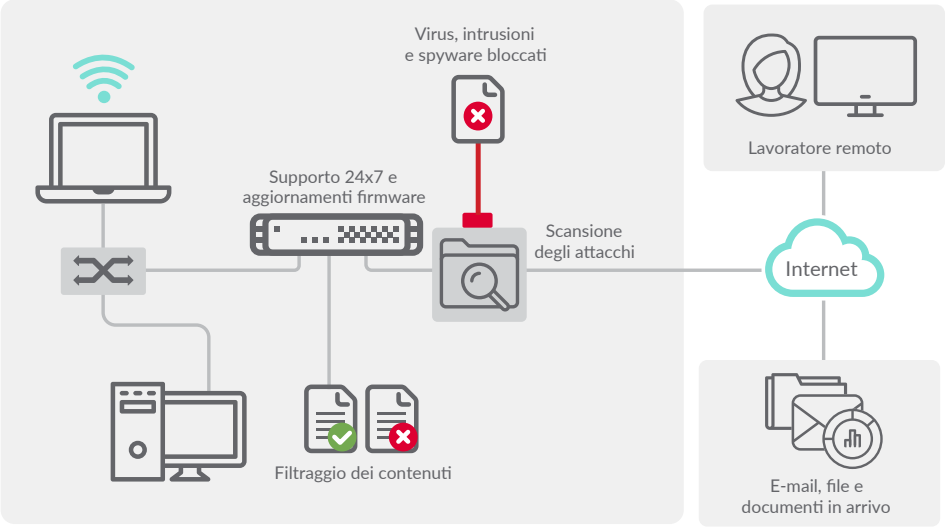
Advanced Gateway Security Suite

Protezione completa della rete in un singolo pacchetto integrato

La protezione di rete è un tema complesso, ma ciò non significa che proteggere la propria rete da minacce note e sconosciute sia necessariamente difficile. SonicWall Advanced Gateway Security Suite (AGSS) elimina il problema di dover scegliere tra diversi servizi di protezione aggiuntivi, in quanto tutte le funzionalità di sicurezza necessarie a garantire una protezione totale sono integrate in un solo e conveniente pacchetto.

Disponibile su tutti i firewall fisici e virtuali, inclusi i firewall delle serie NS*sp*, NS*a*, TZ e NS*v*, SonicWall AGSS protegge la rete da attacchi zero-day, virus, intrusioni, botnet, spyware, Trojan, worm e altri attacchi dannosi. I file sospetti vengono esaminati a livello del gateway, in una sandbox multilivello basata sul cloud, proteggendo così la rete da minacce sconosciute. Appena vengono identificate nuove minacce, e spesso prima che i produttori di software rilascino le patch corrispondenti, i firewall SonicWall e il database Capture Cloud vengono automaticamente aggiornati con nuove firme per garantire una protezione efficace dalle minacce. Tutti i firewall SonicWall integrano il brevettato motore Reassembly-Free Deep Packet Inspection®, che analizza il traffico alla ricerca di svariati tipi di applicazioni e protocolli e garantisce una protezione totale, 24 ore su 24, da attacchi interni ed esterni e da vulnerabilità delle applicazioni. La soluzione SonicWall offre inoltre gli strumenti necessari per applicare policy sull'uso di Internet e controllare l'accesso interno a contenuti web inappropriati, improduttivi e potenzialmente illegali grazie al filtraggio completo dei contenuti. Questo potente pacchetto di servizi include anche il supporto tecnico 24x7, aggiornamenti firmware specifici e la sostituzione dell'hardware.



Vantaggi:

- Soluzione di sicurezza completa per la rete
- Protezione antivirus e antispyware al gateway con certificazione ICSA
- Tecnologia IPS all'avanguardia
- Controllo e intelligence delle applicazioni
- Filtraggio dei contenuti
- Supporto 24x7 con aggiornamenti firmware e sostituzione dell'hardware
- Sandbox di rete multi-engine con SonicWall RTDMI
- Gestione unificata via cloud

Advanced Gateway Security Suite
NS*sp* 12800 (1 anno) 01-SSC-6591
NS*sp* 12400 (1 anno) 01-SSC-6588
NS*a* 9650 (1 anno) 01-SSC-2036
NS*a* 9450 (1 anno) 01-SSC-0414
NS*a* 9250 (1 anno) 01-SSC-0038
NS*a* 6650 (1 anno) 01-SSC-8761
NS*a* 5650 (1 anno) 01-SSC-3674
NS*a* 4650 (1 anno) 01-SSC-3493
NS*a* 3650 (1 anno) 01-SSC-3451
NS*a* 2650 (1 anno) 01-SSC-1783
Serie TZ600 (1 anno) 01-SSC-1460
Serie TZ500 (1 anno) 01-SSC-1450
Serie TZ400 (1 anno) 01-SSC-1440
Serie TZ300 (1 anno) 01-SSC-1430
NS*v* 1600 (1 anno) 01-SSC-5787
NS*v* 800 (1 anno) 01-SSC-5737
NS*v* 400(1 anno) 01-SSC-5681
NS*v* 300 (1 anno) 01-SSC-5584
NS*v* 200 (1 anno) 01-SSC-5306
NS*v* 100 (1 anno) 01-SSC-5219
NS*v* 50 (1 anno) 01-SSC-5194
NS*v* 25 (1 anno) 01-SSC-5165
NS*v* 10 (1 anno) 01-SSC-5008
Sono disponibili anche SKU per più anni.
Per consultare i codici SKU della linea completa di firewall SonicWall, visitare il sito www.sonicwall.com

SonicWall Advanced Gateway Security Suite comprende le opzioni seguenti:

- Abbonamento ai servizi Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Application Intelligence and Control
- Abbonamento al Content Filtering Service (CFS)
- Abbonamento al supporto 24x7
- Abbonamento al servizio Capture Advanced Threat Protection (ATP)
- Abbonamento a Capture Security Center Lite

Caratteristiche e vantaggi

Soluzione di sicurezza completa per la rete che include tutte le funzionalità necessarie a proteggersi da minacce quali ransomware, virus, spyware, worm, Trojan, adware, keylogger, malicious mobile code (MMC) e altre applicazioni e contenuti web pericolosi.

Il servizio Capture Advanced Threat Protection (ATP) rivoluziona i sistemi di rilevamento delle minacce avanzate con una soluzione sandbox multi-engine basata sul cloud che blocca gli attacchi sconosciuti e zero-day a livello del gateway e con funzioni di riparazione automatica.

Capture ATP utilizza la tecnologia Real-Time Deep Memory Inspection (RTDMI) di SonicWall per rilevare e bloccare il malware che non mostra un comportamento dannoso o che nasconde le proprie armi mediante la crittografia. Forzando il malware a rivelare i propri strumenti di attacco in memoria, il motore RTDMI rileva e blocca proattivamente minacce zero-day comuni e malware sconosciuto utilizzando in modo accurato tecniche di ispezione in tempo reale basate sulla memoria.

La protezione antivirus e antispyware al gateway con certificazione ICSA abbina l'anti-malware basato sulla rete a un database nel cloud contenente decine di milioni di firme malware, fornendo una protezione approfondita contro le moderne minacce avanzate.

La tecnologia IPS all'avanguardia protegge da worm, Trojan, vulnerabilità software e altre intrusioni mediante l'analisi di tutto il traffico di rete per rilevare pattern dannosi o anomali, aumentando così l'affidabilità e le prestazioni della rete.

Application Intelligence and Control è un insieme di policy granulari specifiche per applicazione che consente agli amministratori di controllare e gestire gli applicativi (aziendali e non) tramite la classificazione delle applicazioni e l'applicazione di criteri.

Il filtraggio dei contenuti risolve le problematiche di sicurezza, protezione e produttività grazie alla possibilità di applicare regole per l'utilizzo di Internet e bloccare l'accesso a contenuti web dannosi e improduttivi.

Il supporto 24x7 con aggiornamenti firmware e sostituzione dell'hardware protegge l'azienda e l'investimento nella tecnologia SonicWall attraverso aggiornamenti firmware specifici, assistenza tecnica competente, sostituzione tempestiva dell'hardware in caso di guasti e strumenti di auto-assistenza elettronici.

Capture Security Center Lite consente di gestire l'implementazione SonicWall e di eseguire il backup/ripristino delle preferenze dei firewall da un'unica console basata su cloud.

I servizi AGSS in breve

Sandbox multi-engine, Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, Application Intelligence and Control

- Il motore antivirus a livello gateway rileva in tempo reale virus, worm, Trojan e altre minacce provenienti da Internet.
- La protezione antispyware dinamica blocca l'installazione di spyware dannosi e interrompe le comunicazioni spyware esistenti.
- La potente prevenzione delle intrusioni protegge da svariate minacce basate sulla rete tra cui worm, Trojan e altri codici dannosi.
- Il servizio di controllo e intelligence delle applicazioni consente di

classificare le applicazioni e applicare policy.

- Il database delle firme aggiornato dinamicamente assicura una protezione continua dalle minacce.
- La sandbox multi-engine con RTDMI previene minacce sconosciute come attacchi zero-day e ransomware.

Capture Advanced Threat Protection (Capture ATP)

- Blocca gli attacchi zero-day prima che entrino nella rete.
- Distribuisce rapidamente le firme di riparazione alle altre appliance di sicurezza di rete.
- Crea una protezione avanzata contro le minacce in continua evoluzione.
- Analizza un'ampia gamma di tipi di file.

Content Filtering Service (CFS)

- Il filtraggio completo dei contenuti fornisce un controllo personalizzabile sugli accessi interni a contenuti web inappropriati, improduttivi e potenzialmente illegali.
- Le valutazioni dei siti web memorizzate nella cache locale dei firewall SonicWall garantiscono tempi di risposta praticamente immediati per i siti visitati di frequente.
- L'architettura di valutazione ad aggiornamento dinamico confronta tutti i siti web richiesti dagli utenti con un database nel cloud contenente milioni di URL, indirizzi IP e domini e compara ogni valutazione con i criteri impostati a livello locale.

Content Filtering Client

- Blocca il malware in modo rapido e accurato con la tecnologia Real-Time Deep Memory Inspection (RTDMI).
- Estende la sicurezza e la produttività ai dispositivi utilizzati all'esterno del perimetro del firewall, applicando criteri per l'utilizzo di Internet tramite il SonicWall Content Filtering Client. Disponibile come servizio in abbonamento separato per dispositivi Windows, Mac OS e Chrome.

Supporto 24x7

- Gli aggiornamenti software e firmware mantengono aggiornata la soluzione e quindi anche il sistema di protezione della rete.
- Accesso al supporto tecnico per telefono e via web, 24 ore su 24, per ottenere assistenza in fase di configurazione e nella risoluzione dei problemi.
- Sostituzione dell'hardware in caso di guasto.
- Abbonamento annuale ai bollettini di servizio SonicWall e accesso a tool di supporto elettronici e gruppi di discussione con moderatore.

Capture Security Center Lite*

- Portale basato su cloud
- Gestione da un'unica console
- Backup e ripristino delle preferenze dei firewall

Per ulteriori informazioni su SonicWall Advanced Gateway Security Suite, visitare www.sonicwall.com.

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.

*Per le serie SuperMassive 9000, NS*a* 9250/9450/9650 ed NS*sp* 12000, CSC Management è automaticamente disponibile dopo l'attivazione dell'abbonamento AGSS corrispondente

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

Datasheet-AdvancedGatewaySecuritySuite-US-VG-MKTG4091