



SonicWALL Application Intelligence, Control and Visualization

FIREWALL

Controllo granulare intelligente e visualizzazione in tempo reale delle applicazioni

Per gli amministratori IT può essere una vera e propria sfida garantire l'uso efficace di soluzioni aziendali mission-critical e, al tempo stesso, contrastare l'utilizzo di applicazioni inutili e spesso pericolose da parte dei dipendenti. Le applicazioni d'importanza strategica richiedono la massima priorità nell'utilizzo della banda disponibile, mentre quelle di social media e gaming devono essere limitate nell'accesso alla banda o completamente bloccate. I firewall con ispezione Stateful Packet utilizzati in molte aziende controllano le porte e i protocolli, ma non sono in grado di risolvere questo problema in quanto non riescono a identificare le applicazioni. In poche parole, i firewall con ispezione Stateful Packet non sono in grado di distinguere il traffico "buono" da quello "cattivo".

Mediante la scansione di ogni byte di ogni singolo pacchetto di tutto il traffico di rete, le soluzioni SonicWALL® garantiscono un controllo intelligente e completo delle applicazioni indipendentemente dalla porta e dal protocollo, rilevando con esattezza quali applicazioni vengono utilizzate e chi ne fa uso. I firewall SonicWALL di nuova generazione utilizzano un database di signature delle minacce in continua espansione, in grado di rilevare migliaia di applicazioni e milioni di minacce malware, per proteggere la rete in modo automatico e trasparente. Questa soluzione rileva ed elimina malware, intrusioni, fughe di dati e violazioni delle policy prima che questi possano causare danni alla rete aziendale o ai suoi utenti.

SonicWALL Application Intelligence and Control offre potenti strumenti di gestione e maggiore facilità d'uso agli amministratori IT, permettendogli di mantenere un controllo granulare delle applicazioni e degli utenti. Gli amministratori possono creare con facilità policy per la gestione della larghezza di banda basate su categorie logiche predefinite (ad es. social media o gaming), singole applicazioni o anche utenti e gruppi. Man mano che vengono create nuove applicazioni, i firewall ricevono nuove signature e le policy corrispondenti vengono automaticamente aggiornate, senza necessità di lunghi e impegnativi aggiornamenti dei criteri e delle applicazioni da parte dello staff IT. L'analisi del traffico delle applicazioni consente agli amministratori di risolvere eventuali problemi di rete e reagire alle minacce con maggiore efficienza e reattività, garantendo un ritorno dell'investimento immediato. Inoltre l'analisi del traffico applicativo offre una panoramica dettagliata degli eventi e delle attività, che permette di potenziare la sicurezza e gestire l'uso della rete da parte dei dipendenti.

L'Application Intelligence and Control è disponibile in abbonamento annuale, biennale o triennale con il SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention oppure è incluso negli abbonamenti alla SonicWALL Comprehensive Gateway Security Suite per i firewall delle serie TZ 210, Network Security Appliance (NSA) ed E-Class NSA.

Caratteristiche e vantaggi

L'**analisi intelligente delle applicazioni** utilizza la tecnologia Reassembly-Free Deep Packet Inspection™ di SonicWALL per scansionare tutti i pacchetti del traffico, identificando le applicazioni in uso e gli utenti che le utilizzano. SonicWALL gestisce un database di signature per garantire la protezione trasparente e automatica delle reti.

Il **controllo delle applicazioni** consente di utilizzare policy flessibili e configurabili per limitare o bloccare applicazioni, file, indirizzi URL e allegati e-mail in base a tipo di applicazione, utente, eventi pianificati, signature personalizzabili e molto altro ancora.

La **visualizzazione delle applicazioni** fornisce grafici in tempo reale su applicazioni in uso, consumo di banda in ingresso e in uscita, utenti, siti Web attualmente visitati e altro ancora. Inoltre è possibile esportare questi stessi dati in qualsiasi analizzatore NetFlow/IPFIX per eseguire monitoraggi offline, risolvere problemi o effettuare diagnosi in base alla cronologia delle attività di rete.

L'**analisi del traffico delle applicazioni** fornisce un'analisi in tempo reale e cronologica dei dati trasmessi attraverso il firewall, incluse le attività delle applicazioni per ogni utente.

La **prevenzione delle fughe di dati** monitorizza e blocca la trasmissione di dati sensibili mediante upload su server FTP, come allegati con servizi di Webmail personale quali Hotmail® o Gmail®, o tramite la posta elettronica aziendale (SMTP e POP3).

La **gestione della larghezza di banda a livello di applicazione** garantisce la qualità del servizio (QoS) assegnando livelli di throughput dedicati ad applicazioni mission-critical o a gruppi di utenti in fasce di orario specifiche.

Gli **aggiornamenti automatici delle signature** semplificano l'amministrazione e garantiscono che la rete sia sempre protetta contro le minacce più attuali.

L'**ispezione Deep Packet per il traffico SSL** estende la protezione al traffico SSL crittografato con funzioni avanzate di conformità, filtraggio dei contenuti e prevenzione delle fughe di dati, eliminando un altro possibile vettore di malware. Il traffico crittografato viene decifrato, ispezionato e quindi nuovamente crittografato in modo assolutamente trasparente per l'utente, con possibilità di configurazione per le connessioni sia in entrata che in uscita.*

*01-SSC-8680 DPI SSL, licenza di aggiornamento per NSA 220 e superiori.

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

- **Analisi intelligente delle applicazioni**
- **Controllo delle applicazioni**
- **Visualizzazione delle applicazioni**
- **Suite di analisi del traffico delle applicazioni**
- **Prevenzione delle fughe di dati**
- **Gestione della larghezza di banda a livello di applicazione**
- **Aggiornamenti e notifiche automatici**
- **Ispezione Deep Packet per il traffico SSL**

Firewall di nuova generazione con analisi intelligente, controllo e visualizzazione delle applicazioni

Identificazione

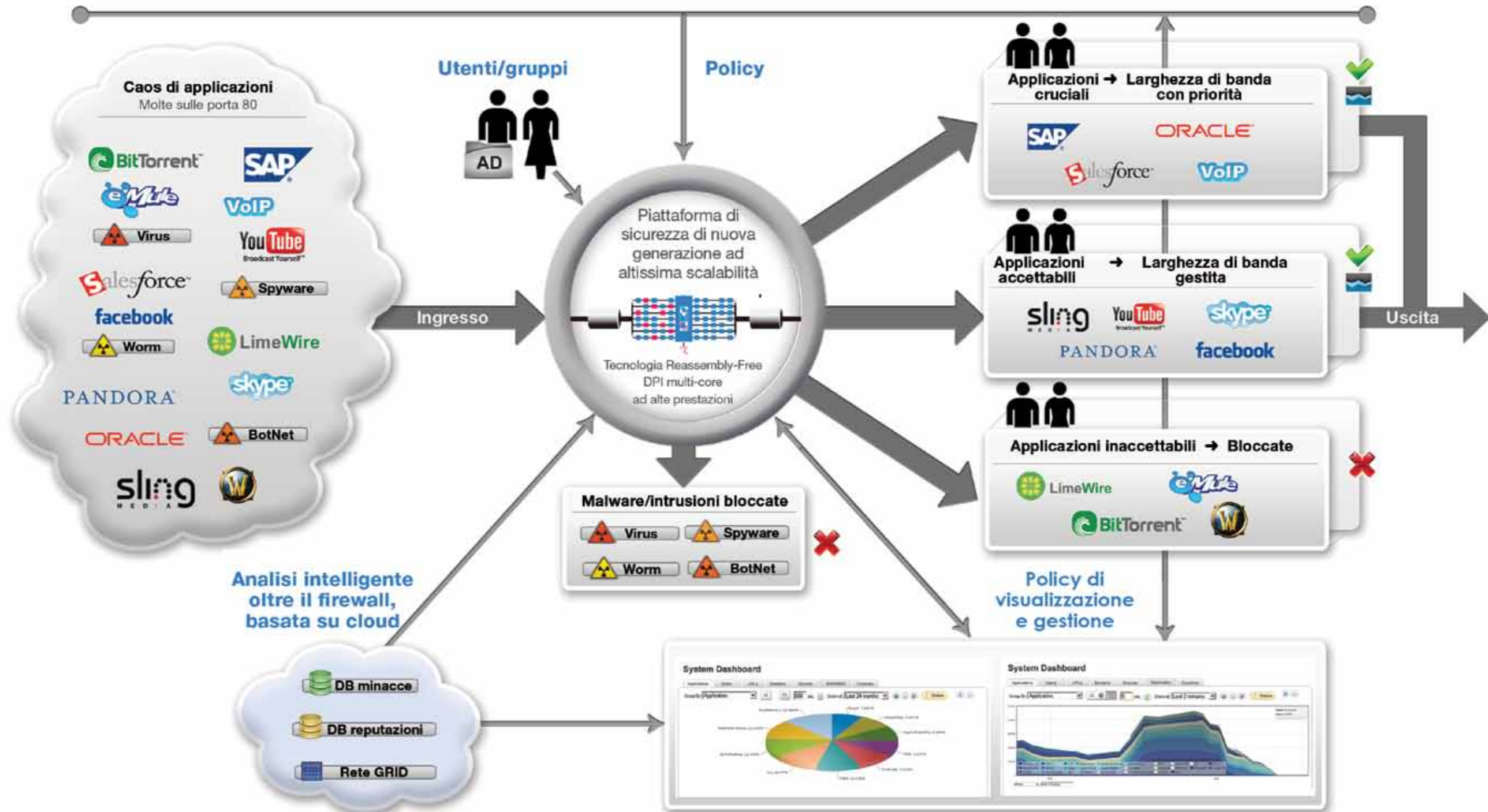
- Per applicazione
 - non per porta e protocollo
- Per utente/gruppo
 - non per IP
- Per ispezione dei contenuti
 - non per nome dei file

Categorizzazione

- Per applicazione
- Per categoria di applicazioni
- Per destinazione
- Per contenuto
- Per utente/gruppo

Controllo

- Prioritizzazione applicazioni per policy
- Gestione applicazioni per policy
- Blocco applicazioni per policy
- Rilevazione e blocco del malware
- Rilevazione e prevenzione di tentativi di intrusione



Specifiche tecniche



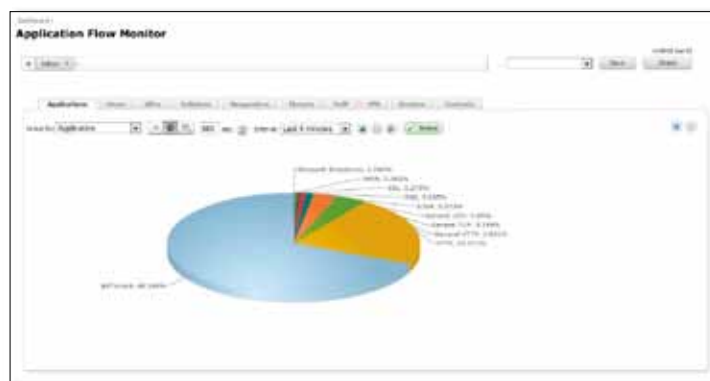
Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention, and Application Intelligence and Control Service

NSA E7500 (1 anno)
01-SSC-6130
NSA E6500 (1 anno)
01-SSC-6131
NSA E5500 (1 anno)
01-SSC-6132
NSA 5000 (1 anno)
01-SSC-6159
NSA 4500 (1 anno)
01-SSC-6133
NSA 3500 (1 anno)
01-SSC-6134
NSA 2400 (1 anno)
01-SSC-6135
Serie NSA 250M (1 anno)
01-SSC-4570
Serie NSA 220 (1 anno)
01-SSC-4612
Serie TZ 210 (1 anno)
01-SSC-6165

Sono disponibili anche servizi in abbonamento pluriennali. Per consultare i codici della linea completa di appliance di sicurezza di rete SonicWALL, visitare il sito www.sonicwall.com.

Visualizzazione delle applicazioni

I grafici in tempo reale per applicazioni, banda in ingresso e in uscita, siti Web visitati e tutte le attività degli utenti consentono agli amministratori di modificare i criteri di utilizzo delle applicazioni per conformarli alle policy di rete.



Funzionalità

- Application Intelligence**
- Scansiona e identifica tutto il traffico indipendentemente dalle porte o dai protocolli, offrendo un controllo completo
 - Prevenzione delle fughe di dati con stringhe di testo definite per utente
 - Gestione della banda a livello di applicazioni in base a un ampio database di signature in continua espansione e a potenti funzioni di creazione delle policy
 - Funzioni Log Only / Log and Block predefinite o impostabili per determinate azioni, messaggi utente personalizzabili, esclusione DPI e gestione della larghezza di banda
 - Ispezione Deep Packet del traffico incanalato tramite protocolli SSL crittografati

- Database di signature**
- Database aggiornato dinamicamente con migliaia di signature per applicazioni e basate sui contenuti

- Logging e analisi del traffico applicativo**
- Reporting avanzato di nuova generazione basato su syslog
 - Analisi del traffico delle applicazioni tramite Analyzer, Scrutinizer o Global Management System di SonicWALL
 - Netflow/IPFIX con registrazione delle estensioni per una maggiore semplicità di analisi e visualizzazione del traffico

- Scalabilità**
- Capacità di scansione simultanea di grandi quantità di file in download di dimensioni illimitate

Per ulteriori informazioni sulla suite di servizi di sicurezza SonicWALL a valore aggiunto, tra cui Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service, Application Intelligence and Control, Comprehensive Anti-Spam Service, Enforced Client Anti-Virus and Anti-Spyware o Content Filtering Service, visitate il nostro sito all'indirizzo <http://www.sonicwall.com>.



SonicWALL Italy
T + 39.010.7407851
Italy@sonicwall.com
Contatti Supporto SonicWALL
www.sonicwall.com/emea/4724.html

Linea di soluzioni di sicurezza dinamica SonicWALL

 SICUREZZA DI RETE	 ACCESSO REMOTO SICURO	 SICUREZZA WEB / E-MAIL	 BACKUP E RECOVERY	 GESTIONE BASATA SU POLICY
---	---	--	---	---

SONICWALL
DYNAMIC SECURITY FOR THE GLOBAL NETWORK™