

~~1110~~ funzioni utili che il vostro firewall dovrebbe avere

Molto più del semplice blocco delle minacce alla rete –
protezione, gestione e controllo del traffico delle applicazioni

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Il firewall si evolve	1
Cosa fa SonicWALL Application Intelligence and Control?	2
Come funziona SonicWALL Application Intelligence	3
1 ^a funzione utile: controllo delle applicazioni consentite in rete	4
2 ^a funzione utile: gestione della larghezza di banda per le applicazioni strategiche	5
3 ^a funzione utile: blocco delle applicazioni peer-to-peer	6
4 ^a funzione utile: blocco dei componenti improduttivi delle applicazioni	7
5 ^a funzione utile: visualizzazione del traffico delle applicazioni	8
6 ^a funzione utile: gestione della larghezza di banda per un gruppo di utenti	9
7 ^a funzione utile: blocco dei virus prima che entrino nella rete	10
8 ^a funzione utile: identificazione delle connessioni in base al paese	11
9 ^a funzione utile: prevenzione di fughe di dati tramite la posta elettronica	12
10 ^a funzione utile: prevenzione di fughe di dati tramite Web Mail	13
11 ^a funzione utile: gestione della larghezza di banda per lo streaming audio e video	14
Somma delle funzionalità	15

Il firewall si evolve

I tradizionali firewall con stateful packet inspection bloccano essenzialmente le minacce a livello di rete monitorando le porte e i protocolli utilizzati dal traffico che transita a livello di rete. I recenti firewall di nuova generazione utilizzano l'ispezione approfondita dei pacchetti (deep packet inspection) per scansionare l'intero payload dei pacchetti,

Con la proliferazione di tecnologie di cloud computing e Web 2.0, i firewall devono ora affrontare una nuova sfida: il controllo delle applicazioni.

fornendo prevenzione avanzata contro le intrusioni, filtraggio dei contenuti e funzionalità anti-malware e anti-spam. Molte applicazioni vengono fornite via Web attraverso porte e protocolli HTTP o HTTPS comuni. In tal modo i firewall tradizionali non sono in grado di rilevare queste applicazioni e neppure di distinguere il traffico produttivo e sicuro rispetto al traffico non produttivo e potenzialmente non sicuro. I firewall di nuova generazione offrono una visione dettagliata delle applicazioni stesse, fornendo uno strumento d'importanza strategica ai professionisti della rete.

Cosa fa SonicWALL Application Intelligence and Control?

I firewall SonicWALL® consentono di identificare e monitorare gli applicativi utilizzati nella rete aziendale. Questo controllo aggiuntivo aumenta la conformità alle normative e migliora la prevenzione delle fughe di dati grazie alla possibilità di identificare le applicazioni in base alle loro firme digitali specifiche piuttosto che alle porte o ai protocolli.

SonicWALL Application Intelligence, Control and Visualization può assegnare maggiore larghezza di banda alle applicazioni mission-critical o sensibili ai ritardi, limitando al contempo l'uso di applicazioni che possono ridurre la produttività, come ad esempio giochi online o streaming video.

A tale scopo viene visualizzato il traffico delle applicazioni per determinare i modelli di utilizzo e, sulla base di queste informazioni, creare policy granulari per applicazioni, utenti o anche gruppi di utenti oppure basate su fasce orarie o altre variabili, fornendo uno strumento di controllo flessibile e adattabile a qualsiasi esigenza di rete.



Come funziona SonicWALL Application Intelligence and Control?

SonicWALL attinge a un ampio database di signature di applicazioni, in continua crescita e aggiornato automaticamente, per identificare le applicazioni in base al loro "DNA" piuttosto che ad attributi generici quali la porta sorgente, la porta di destinazione o il tipo di protocollo.

SonicWALL permette di controllare non solo intere categorie di applicazioni o singoli applicativi, ma anche funzionalità specifiche all'interno delle applicazioni, con la possibilità di bloccarle o di limitarne la larghezza di banda.

Ad esempio, un amministratore può decidere di consentire la messaggistica istantanea ma bloccarne il trasferimento di file, oppure di consentire l'accesso a Facebook ma bloccare l'accesso ai giochi basati su Facebook. Questi controlli sono disponibili anche per l'intero traffico SSL, che deve essere ispezionato così come le connessioni non criptate. I risultati dei controlli, visualizzabili con la massima semplicità, consentono di migliorare l'uso delle applicazioni e ottimizzare l'ampiezza di banda della rete.

1ª funzione utile: controllo delle applicazioni consentite in rete



IE 8.0

Supponiamo che nella vostra azienda tutti i dipendenti debbano usare la versione più recente di Internet Explorer. La vostra missione consiste nel garantire che tutti i dipendenti che lanciano IE6 o IE7 vengano automaticamente reindirizzati al sito di download di IE8, senza poter accedere a nessun altro sito Web. Le vostre possibili soluzioni sono:

- Controllare fisicamente quale versione di browser è installata su ogni singola macchina
- Scrivere uno script personalizzato per controllare automaticamente le versioni dei browser
- Impostare una policy con SonicWALL Application Intelligence and Control – e non pensarci più



IE 7.0

Creare una policy per reindirizzare gli utenti con IE6 o IE7 al sito di download della versione più recente del browser, bloccando l'accesso a Internet per gli utenti con IE6 o IE7

1. Il motore Deep Packet Inspection (DPI) ricerca l'agente utente = IE 6.0 o l'agente utente = IE 7.0 nell'intestazione HTTP
2. La policy reindirizza gli utenti con le versioni IE6 o IE7 al sito di download di IE8, bloccando al contempo l'accesso a qualsiasi altro sito Web per i browser IE6 o IE7

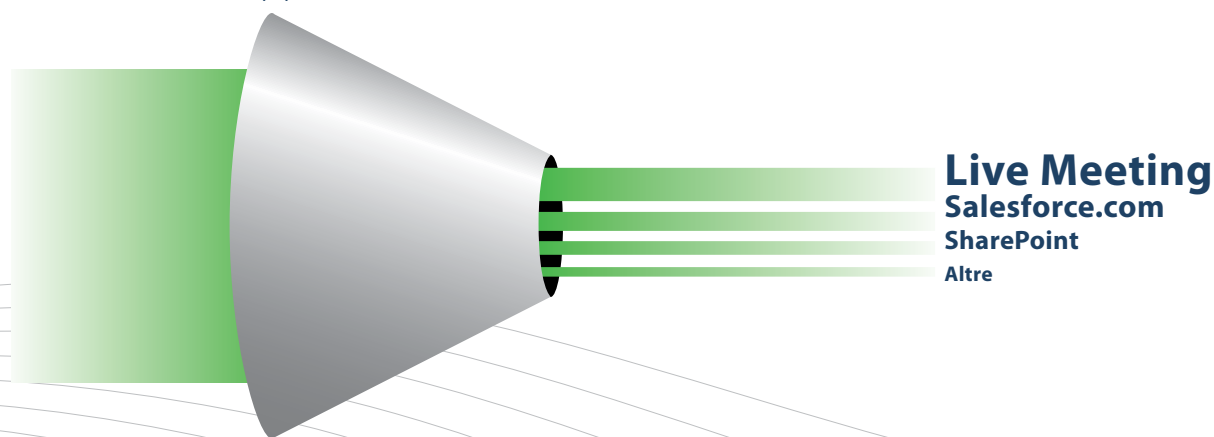
La visualizzazione delle applicazioni consente di stabilire quali versioni browser vengono utilizzate prima di creare la policy.

2^a funzione utile: gestione della larghezza di banda per le applicazioni strategiche

Molte applicazioni mission-critical, come ad esempio Live Meeting, Salesforce.com® e SharePoint®, sono basate su cloud oppure girano su reti geograficamente distribuite. Garantendo la priorità a queste applicazioni rispetto alla navigazione Web improduttiva è possibile migliorare la produttività aziendale.

Creare una policy per dare priorità di banda all'applicazione Live Meeting

1. Il motore Deep Packet Inspection (DPI) ricerca la firma dell'applicazione o il nome dell'applicazione
2. Assegnare all'applicazione Live Meeting una priorità di banda maggiore rispetto alle altre applicazioni



***La priorità di un'applicazione è impostabile
anche in base alla data
(ad esempio priorità alle applicazioni di vendita a fine trimestre)***

3ª funzione utile: blocco delle applicazioni peer-to-peer

Le applicazioni peer-to-peer (P2P) improduttive, quali BitTorrent, vengono spesso utilizzate per scaricare versioni illegali di contenuti multimediali protetti da copyright e possono rapidamente consumare moltissima larghezza di banda e veicolare malware. Poiché in continuazione vengono create nuove applicazioni P2P o apportate semplici modifiche (ad es. i numeri di versione) a quelle esistenti, bloccare manualmente ogni singola applicazione P2P è alquanto difficile.

SonicWALL aggiorna continuamente il database per il controllo intelligente delle applicazioni, aggiungendo nuove applicazioni P2P appena sono disponibili. A questo punto è possibile creare una semplice policy per bloccare tutte le applicazioni P2P d'ora in poi.

Creare una policy per bloccare l'uso di applicazioni P2P

1. Il motore Deep Packet Inspection (DPI) utilizza le firme predefinite delle applicazioni P2P riportate nella lista delle firme delle applicazioni
2. Scegliere le applicazioni P2P dalla lista di firme predefinite
3. Applicare la policy a tutti gli utenti
4. Bloccare le applicazioni P2P applicando restrizioni alla larghezza di banda e alle fasce orarie consentite



4^a funzione utile: blocco dei componenti improduttivi delle applicazioni

Le applicazioni di social networking quali Facebook, Twitter e YouTube sono diventate nuovi canali di comunicazione sia per le singole persone che per le aziende. Mentre un blocco di tutte le applicazioni di social networking potrebbe essere controproducente, si può decidere di controllare come vengono utilizzate sul posto di lavoro.

Ad esempio si può permettere al personale del reparto marketing di aggiornare la pagina Facebook aziendale ma non di giocare a giochi di Facebook come Farmville o Mafia Wars. Con il controllo intelligente delle applicazioni è possibile creare una policy per consentire l'accesso a Facebook ma bloccare Farmville.



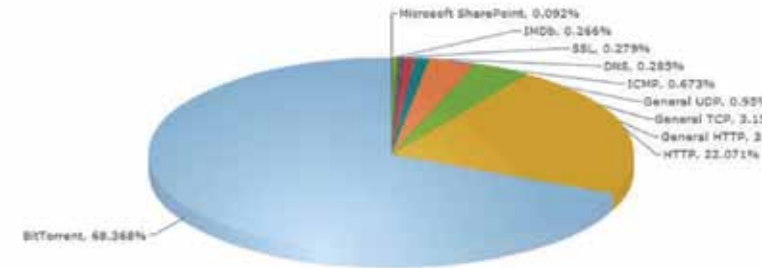
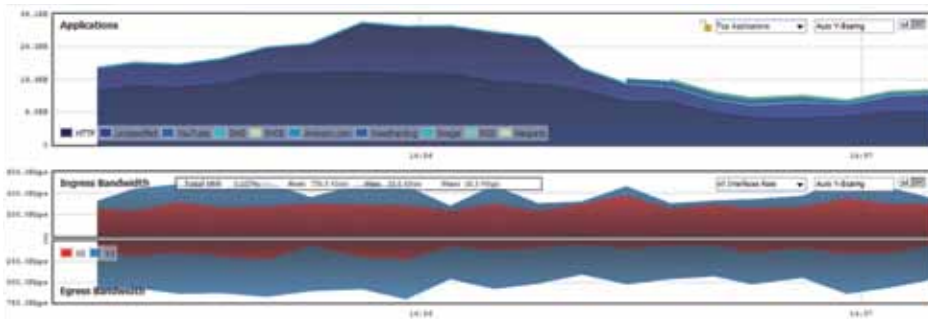
Creare una policy per consentire l'accesso a Facebook, bloccando però i giochi di Facebook

1. Selezionare "Tutti" gli utenti
2. Selezionare le applicazioni di gioco di Facebook come categoria
3. Creare un'unica regola per "Bloccare" l'accesso ai giochi di Facebook per tutti gli utenti

***È anche possibile consentire le chat
ma bloccare il trasferimento di file durante le chat.***

5ª funzione utile: visualizzazione del traffico delle applicazioni

Cosa succede nella mia rete? Chi sta sprecando la larghezza di banda disponibile? Perché la mia rete è così lenta? Vi siete mai posti una di queste domande? Per ottenere una risposta è possibile utilizzare una combinazione di strumenti separati, ma questo processo richiede tempo e fornisce solo informazioni successive ai fatti. La visualizzazione in tempo reale del traffico delle applicazioni di SonicWALL fornisce una risposta immediata a queste domande, con la possibilità di diagnosticare rapidamente i problemi, rilevare l'utilizzo non conforme della rete, creare policy adeguate e verificare immediatamente l'efficacia di queste policy.



Visualizzare tutto il traffico in tempo reale tramite Application Flow Monitor

1. Visualizzare grafici in tempo reale sul traffico di tutte le applicazioni
2. Visualizzare grafici in tempo reale sulla larghezza di banda in ingresso e in uscita
3. Visualizzare grafici in tempo reale sui siti Web visitati e su tutte le attività degli utenti
4. Creare filtri personalizzati per ottenere le informazioni più rilevanti

La visualizzazione delle applicazioni fornisce agli amministratori un feedback immediato sui flussi di traffico della rete.

6ª funzione utile: gestione della larghezza di banda per un gruppo di utenti

Il vostro direttore si lamenta del fatto che i video di notizie finanziarie che vuole guardare ogni mattina sono lenti e non funzionano correttamente. Dopo una breve verifica, scoprite che il problema è causato da una policy di gestione della larghezza di banda che avete applicato per limitare lo streaming video di tutti gli utenti. A questo punto potreste ridurre le limitazioni alla banda per tutti gli utenti, oppure - ancor meglio - utilizzare la gestione della larghezza di banda basata sui gruppi.

Creare una policy per escludere lo staff dirigenziale dalla gestione della banda per lo streaming video

1. Scegliere il gruppo di dirigenti importato dal server LDAP
2. Il motore Deep Packet Inspection (DPI) utilizza le firme predefinite delle applicazioni di streaming video dalla lista delle firme delle applicazioni
3. Applicare la limitazione della larghezza di banda al traffico contenente quell'intestazione

Larghezza di banda desiderata per flussi video

Larghezza di banda fornita al reparto vendite

Larghezza di banda fornita agli altri utenti

Molte aziende hanno scoperto che i loro dipendenti preferiscono avere pieno accesso al Web, pur disponendo di una larghezza di banda ridotta per i siti improduttivi.

7ª funzione utile: blocco dei virus prima che entrino nella rete

La protezione della rete è uno degli obiettivi prioritari di qualsiasi amministratore IT. La capacità di bloccare minacce malware come virus, spyware, keylogger, Trojan e tentativi d'intrusione in rete a livello del gateway protegge l'azienda da rischi maggiori e impedisce un inutile spreco di risorse.

***Bloccare virus, spyware e altro malware
a livello gateway
prima che possano entrare nella rete!***



I servizi di protezione SonicWALL, basati sull'architettura ad alte prestazioni e bassissima latenza dei firewall SonicWALL di nuova generazione, sono in grado di neutralizzare milioni di minacce prima che possano entrare nella rete e trasformarsi in una minaccia per i vostri utenti. Se un utente collega un laptop infetto alla rete, i firewall di nuova generazione di SonicWALL riescono a bloccare la propagazione del malware all'interno di quel reparto e nel resto dell'azienda.

8ª funzione utile: identificazione delle connessioni in base al paese

La connessione a un IP di un paese straniero realizzata dall'ufficio accanto al vostro o da una sede distaccata è una connessione innocua di un utente che sta navigando in rete oppure un'attività botnet? In questi casi il controllo intelligente delle applicazioni offre potenti strumenti di analisi per identificare esattamente tutto ciò che accade nella vostra rete.

Visualizzare le connessioni in base al paese o creare filtri specifici per paese

1. Controllare quali applicazioni si connettono a IP di altri paesi
2. Vedere quali utenti e quali computer si connettono a IP di altri paesi
3. Creare filtri per limitare il traffico verso paesi specifici, liberamente selezionabili, con liste di esclusione



Una volta ottenute le informazioni desiderate potete decidere se parlare con l'utente, ispezionare la macchina che si connette a un indirizzo IP non consentito oppure attivare un'utilità di cattura dei pacchetti sul firewall per analizzare con esattezza cosa succede in una determinata connessione. Il controllo intelligente delle applicazioni consente di identificare e risolvere problemi di cui altrimenti non si verrebbe a conoscenza.

9ª funzione utile: prevenzione di fughe di dati tramite la posta elettronica

In alcune aziende, i messaggi e-mail in uscita non passano attraverso il sistema di protezione e-mail aziendale, oppure quel sistema non controlla il contenuto degli allegati. In entrambi i casi, gli allegati con informazioni confidenziali possono uscire senza problemi dalla rete aziendale. Se invece il traffico in uscita dalla rete passa attraverso il firewall, avete la possibilità di identificare e bloccare questi "dati in movimento".

Creare una policy per bloccare gli allegati e-mail contenenti il watermark "Confidenziale"

Il motore Deep Packet Inspection (DPI) ricerca:

1. contenuto e-mail = "Confidenziale" e
2. contenuto e-mail = "Proprietà dell'azienda" e
3. contenuto e-mail = "Proprietà privata", ecc.



10ª funzione utile: prevenzione di fughe di dati tramite Web Mail

Supponiamo che la protezione anti-spam esistente sia in grado di rilevare e bloccare un normale messaggio e-mail in uscita contenente informazioni confidenziali dell'azienda. Ma cosa succede se un dipendente utilizza un servizio di WebMail come Yahoo® o Gmail® per inviare all'esterno informazioni di tipo riservato o confidenziale?

Creare una policy per bloccare gli allegati "Confidenziali" nel traffico Web

1. Il motore Deep Packet Inspection (DPI) ricerca la voce "Confidenziale" nei file che vengono trasferiti via http o https
2. Bloccare il messaggio e notificare al mittente che il messaggio contiene informazioni aziendali riservate o confidenziali



Da: utentecorretto@azienda.com
A: utentecorretto@partner.com
Oggetto: Approvazione orario settimanale
Il tuo orario per la prossima settimana è approvato.
Giovanni

Da: utentemalintenzionato@azienda.com
A: utentemalintenzionato@concorrenza.com
Oggetto: Piano di sviluppo del progetto
Ecco il nostro piano di sviluppo
9 Gennaio – Versione 7.0
Questo documento è riservato e **confidenziale**



Questo metodo può essere applicato anche ai contenuti basati su FTP.

11ª funzione utile: gestione della larghezza di banda per lo streaming audio e video

L'accesso allo streaming di video da siti come YouTube.com può essere utile, ma spesso si tende ad abusarne. Bloccare questi siti sarebbe possibile, ma un approccio preferibile consiste nel limitare la larghezza di banda totale assegnata allo streaming video, indipendentemente da dove proviene. Lo stesso vale per i siti di streaming audio, come le radio online e i siti che consentono di creare e ascoltare playlist musicali personalizzate. Questo traffico non proviene necessariamente da siti conosciuti e può anche essere ospitato su singoli blog. L'obiettivo consiste quindi nell'identificare questo traffico in base alla sua natura e non alla sua origine. L'ispezione Deep Packet eccelle in questo processo.



Larghezza di banda desiderata per lo streaming audio e video

Larghezza di banda fornita per lo streaming audio e video

Creare una policy per limitare lo streaming di audio e video tramite una lista di firme predefinite

1. Selezionare Streaming Video e Streaming Audio come categorie di applicazioni
2. Impostare la quantità di larghezza di banda che si desidera assegnare a queste categorie di applicazioni (ad es. 10%)
3. Creare una regola in base alla quale lo streaming video e audio può consumare al massimo il 10% della larghezza di banda per tutti gli utenti (escludendo magari gruppi specifici del personale, come quelli addetti alla formazione)
4. Inoltre si può impostare un'opzione per cui questa regola è efficace durante i normali orari di lavoro ma non durante la pausa pranzo e dopo le ore 18
5. Verificare l'efficacia della nuova policy mediante la visualizzazione in tempo reale, collegandosi ad Application Flow Monitor

Somma delle funzionalità



Piattaforma ad alte prestazioni

+ ispezione Deep Packet

+ prevenzione delle intrusioni

+ controllo intelligente e visualizzazione delle applicazioni

Firewall SonicWALL di nuova generazione

Prestazioni, protezione e controllo puntuale



Per saperne di più ...

- Scarica il whitepaper "AimPoint Group: Controllo delle applicazioni – Le 7 funzionalità indispensabili per ripristinare l'efficacia del firewall"
- Guarda il video
- Scarica la scheda tecnica

Per eventuali commenti su questo e-book o su altri e-book o whitepaper di SonicWALL, inviare un'e-mail a feedback@sonicwall.com.

Inoltra ad un amico

Profilo di SonicWALL

Guidata da una vision orientata alla sicurezza dinamica per la rete globale, SonicWALL[®] sviluppa soluzioni avanzate, intelligenti e scalabili per la sicurezza di rete e la protezione dei dati in base alle esigenze dell'azienda e alle minacce. Le soluzioni SonicWALL, implementate da aziende sia di piccole che di grandi dimensioni, sono progettate per il rilevamento e il controllo delle applicazioni, oltre che per la protezione della rete da intrusioni e attacchi malware attraverso premiati hardware, software e dispositivi virtuali. Per ulteriori informazioni, visitare il sito Web aziendale all'indirizzo www.sonicwall.com.

Linea di soluzioni di sicurezza dinamica SonicWALL



**SICUREZZA
DI RETE**



**ACCESSO
REMOTO SICURO**



**SICUREZZA
WEB / E-MAIL**



**GESTIONE BASATA
SU POLICY**



**BACKUP E
RECOVERY**

SonicWALL Italy

T + 39.010.7407851
Italy@sonicwall.com

Contatti Supporto SonicWALL

www.sonicwall.com/emea/4724.html