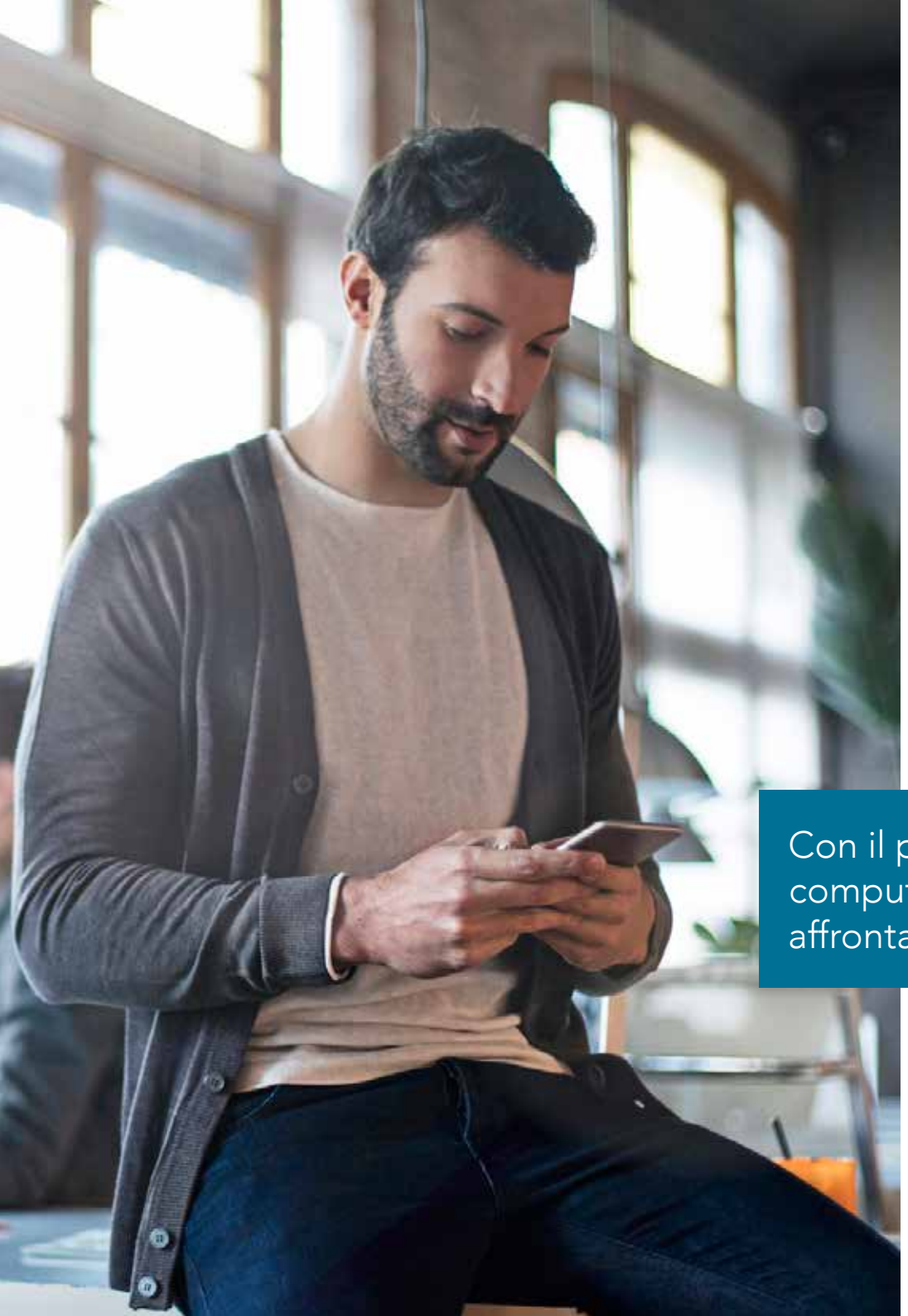
11 funzioni utili che il vostro firewall dovrebbe avere

Espandete la protezione oltre il blocco delle minacce di rete per proteggere, gestire e controllare il traffico delle applicazioni

SONICWALL™

Sommario

SONICWALL™



Il firewall cresce

I firewall tradizionali con ispezione Stateful Packet mirano a bloccare le minacce a livello di rete valutando le porte e i protocolli utilizzati dal traffico a livello di rete. I più recenti firewall di nuova generazione (NGFW) utilizzano la *deep packet inspection* per scansionare il payload dell'intero pacchetto per fornire una prevenzione avanzata delle intrusioni, antimalware, filtraggio dei contenuti e anti-spam. Molte applicazioni vengono fornite tramite Web e condividono porte comuni e protocolli HTTP o HTTPS. In questo modo, i firewall tradizionali sono praticamente ciechi nei confronti di queste applicazioni e non possono dare priorità al traffico produttivo e sicuro rispetto a quello improduttivo e potenzialmente insicuro. I firewall di nuova generazione permettono di ottenere informazioni sulle applicazioni stesse, offrendo una capacità fondamentale per i professionisti della rete.

Con il proliferare di tecnologie come il cloud computing e il Web 2.0, i firewall si trovano ora ad affrontare una nuova sfida: il controllo delle applicazioni.

SONICWALL™

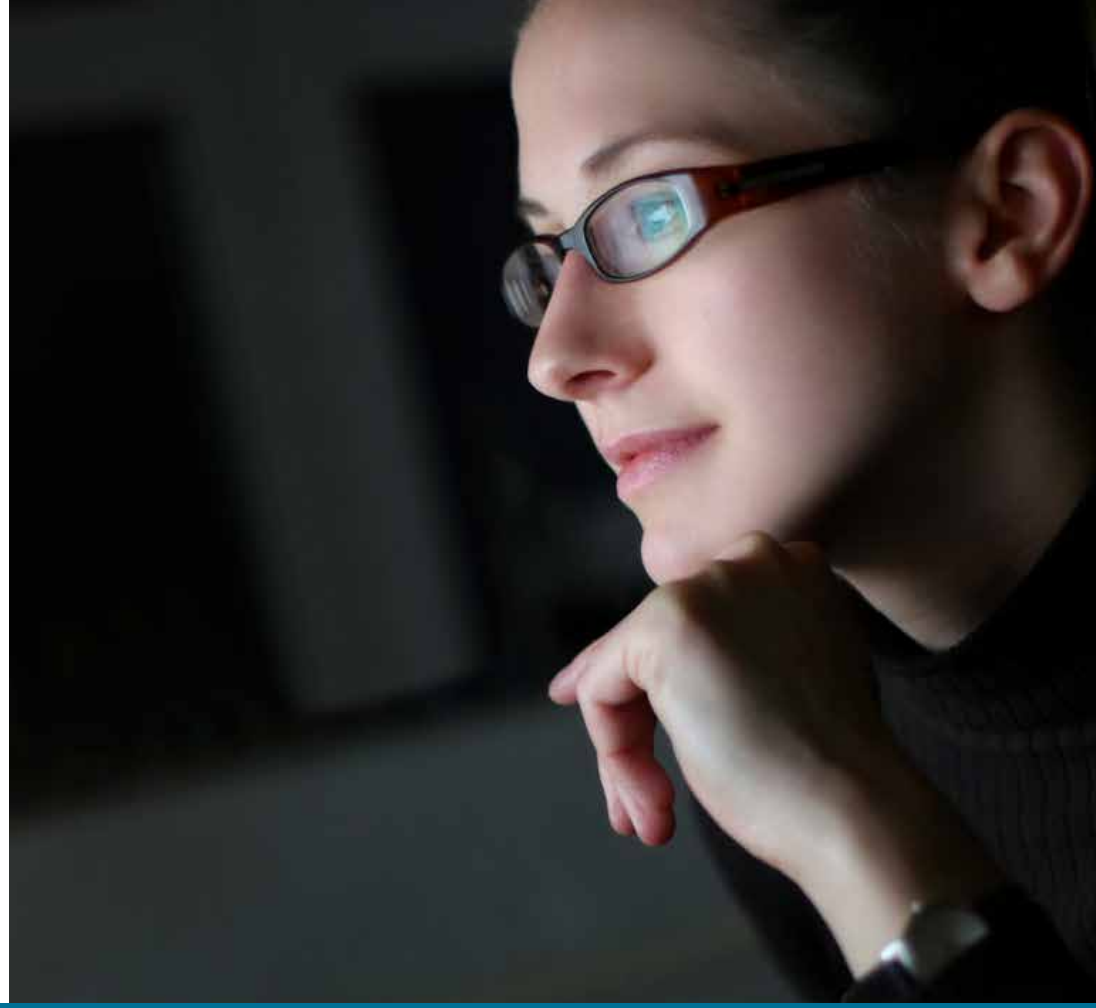
Che cosa fa SonicWall Application Intelligence and Control?

I firewall SonicWall consentono di identificare e controllare tutte le applicazioni utilizzate sulla rete. Questo controllo aggiuntivo migliora la conformità e la prevenzione delle fughe di dati identificando le applicazioni sulla base delle loro firme uniche anziché su porte o protocolli. A tal fine, viene visualizzato il traffico delle applicazioni per determinare modelli di utilizzo e quindi creare policy granulari per applicazioni, utenti o addirittura gruppi di utenti, nonché in base all'ora del giorno e ad altre variabili, per un controllo flessibile che può adattarsi a qualsiasi requisito della rete.

Allocazione di larghezza di banda per applicazioni strategiche o a bassa latenza.

Come funziona SonicWall Application Intelligence and Control?

Utilizzando un database di firme applicative vasto e costantemente aggiornato, SonicWall individua le applicazioni basate sul loro «DNA» anziché su attributi meno univoci, come la porta di origine, la porta di destinazione o il tipo di protocollo. Ad esempio, è possibile far passare l'instant messaging, ma bloccare il trasferimento dei file, oppure consentire l'accesso a Facebook, ma impedire l'accesso a giochi basati su Facebook. Questi controlli sono disponibili per tutto il traffico crittografato SSL, che deve essere ispezionato al pari delle connessioni non crittografate. Inoltre è possibile visualizzare facilmente i risultati dei controlli, potendo quindi affinare l'utilizzo delle applicazioni e ottimizzare la larghezza di banda della rete.



Controllo delle categorie di applicazioni, di singole applicazioni e di caratteristiche specifiche delle applicazioni.

La visualizzazione delle applicazioni consente di «vedere» quali browser vengono utilizzati prima di creare la policy.

La 1ª funzione utile:

Controllare le applicazioni ammesse sulla rete

Un esempio può essere la verifica che tutti i dipendenti utilizzino l'ultima versione di Internet Explorer. L'obiettivo è assicurarsi che tutti i dipendenti che avviano IE9 o IE10 siano automaticamente reindirizzati al sito di download di IE11 e non possano accedere ad altro sul Web. Le soluzioni possibili sono:

- Verificare fisicamente ogni sistema, ogni giorno, per accertarsi della versione del browser Web
- Scrivere uno script personalizzato per controllare automaticamente le versioni del browser
- Impostare una policy con SonicWall Application Intelligence and Control e smettere di preoccuparsi

Creare una policy per reindirizzare gli utenti di IE9 o IE10 al download del browser IE e bloccare l'accesso a Internet da IE9 o IE10

1. Il motore Deep Packet Inspection (DPI) cerca lo User Agent = IE 9.0 o lo User Agent = IE 10.0 nell'intestazione HTTP
2. La policy reindirizza gli utenti di IE9 o IE10 al sito di download di IE11, bloccando l'accesso da IE9 o IE10 a qualsiasi altro sito Web

SONICWALL™

La 2ª funzione utile:

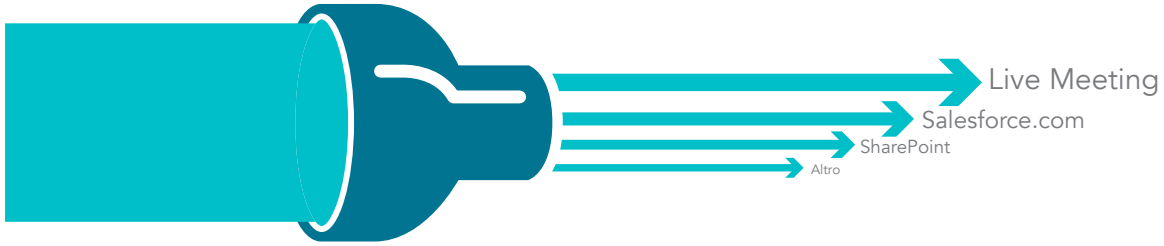
Gestire la larghezza di banda delle applicazioni strategiche

Molte applicazioni strategiche, come Live Meeting, Salesforce.com® e SharePoint®, sono basate su cloud o girano su reti disperse geograficamente. Garantire che queste applicazioni abbiano la precedenza rispetto alla navigazione Web non produttiva migliora la produttività aziendale.

Creazione di una policy per dare più priorità alla larghezza di banda per l'applicazione Live Meeting

1. Il motore Deep Packet Inspection cerca la firma dell'applicazione o il nome dell'applicazione
2. Assegnare una priorità più alta per la larghezza di banda all'applicazione Live Meeting

La priorità dell'applicazione può essere basata sulla data; basti pensare alla priorità di fine trimestre per le applicazioni di vendita.



SONICWALL™

La 3ª funzione utile:

Bloccare le applicazioni peer-to-peer (P2P)

Le applicazioni peer-to-peer (P2P) non produttive, come BitTorrent, sono spesso utilizzate per scaricare versioni non autorizzate di prodotti protetti da copyright e possono rapidamente consumare larghezza di banda o trasmettere malware. Tuttavia, vengono continuamente create nuove applicazioni P2P o semplicemente modificate le applicazioni P2P già esistenti (ad es. i numeri di versione), quindi è difficile bloccare manualmente ogni singola applicazione P2P.

SonicWall aggiorna costantemente il database di Application Intelligence and Control aggiungendo nuove applicazioni P2P non appena sono disponibili. Ora è possibile creare semplicemente una policy per bloccare tutte le applicazioni P2P che si presentano.

Creazione di una policy per bloccare l'utilizzo di applicazioni P2P

1. Il motore Deep Packet Inspection utilizza firme di applicazioni P2P predefinite prese dall'elenco delle firme delle applicazioni
2. Scegliere le applicazioni P2P nell'elenco delle firme predefinite
3. Applicare la policy a tutti gli utenti
4. Bloccare le applicazioni P2P per mezzo della larghezza di banda e le restrizioni a tempo

Elenco delle firme delle applicazioni

BitTorrent-6.1
BitTorrent-6.0.3
BitTorrent-6.0.2
BitTorrent-6.0.1
… e altre centinaia

\+

Elenco delle firme delle applicazioni

Gli aggiornamenti da SonicWall vengono ricevuti e applicati

=

Elenco delle firme delle applicazioni

BitTorrent-6.1.1
BitTorrent-6.1
BitTorrent-6.0.3
BitTorrent-6.0.2
… e altre centinaia

Il risultato

- Possibilità di gestire e controllare le applicazioni P2P
- Nessuna necessità di passare tempo ad aggiornare le regole delle firme IPS

SONICWALL™

La 4ª funzione utile:

Bloccare i componenti improduttivi delle applicazioni

Le applicazioni dei social network come Facebook, Instagram e YouTube sono diventate nuovi canali di comunicazione per individui e per aziende. Sebbene possa essere controproducente bloccare tutte le applicazioni di social networking, è possibile controllare come possono essere utilizzate sul posto di lavoro.

Ad esempio, è possibile lasciare che il personale di marketing aggiorni la pagina Facebook dell'azienda, senza permettere loro di giocare su Facebook con Candy Crush o Mafia Wars. Con Application Intelligence and Control è possibile creare una policy per consentire l'accesso a Facebook, pur bloccando i giochi.

Creazione di una policy per consentire l'accesso a Facebook, ma bloccando i giochi su Facebook

1. Selezionare «Tutti gli utenti»
2. Selezionare la categoria «Applicazioni di gioco su Facebook»
3. Creare una singola regola per «Bloccare» l'accesso ai giochi su Facebook

È possibile consentire le chat, bloccando però i trasferimenti di file all'interno della chat.

La 5ª funzione utile:

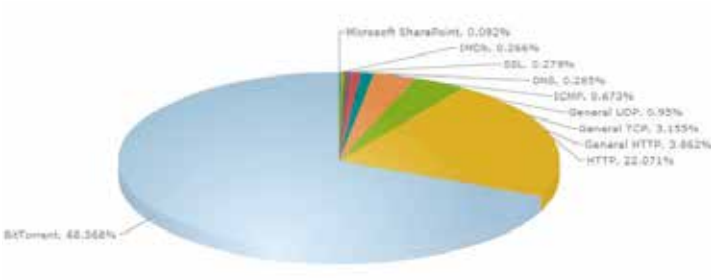
Visualizzazione del traffico delle applicazioni

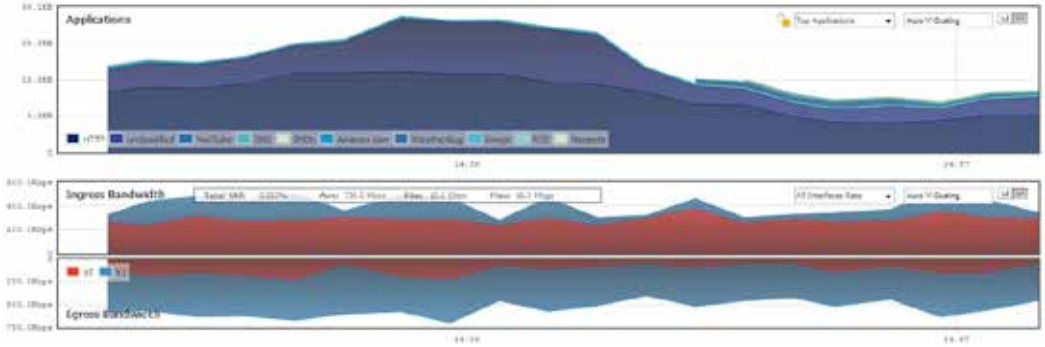
Cosa sta succedendo sulla mia rete? Chi sta sprecando la mia banda? Perché la mia rete è così lenta? Vi siete mai posti una di queste domande? Potreste utilizzare una combinazione di strumenti separati per tentare di avere le risposte, ma questo processo richiede tempo e non fa altro che fornire informazioni dopo che i fatti sono già successi. Con la visualizzazione del traffico delle applicazioni in tempo reale di SonicWall, potete rispondere a queste domande immediatamente, diagnosticare rapidamente le problematiche, rilevare un utilizzo non conforme della rete, creare policy appropriate e verificare immediatamente l'efficacia di queste policy.

Visualizzazione di tutto il traffico in tempo reale accedendo all'Application Flow Monitor

1. Visualizzazione di grafici in tempo reale di tutto il traffico delle applicazioni
2. Visualizzazione di grafici in tempo reale della larghezza di banda in ingresso e uscita
3. Visualizzazione di grafici in tempo reale dei siti Web visitati e di tutte le attività degli utenti
4. Creazione di filtri personalizzati per ottenere le informazioni più rilevanti

La visualizzazione fornisce agli amministratori un feedback istantaneo sui flussi di traffico sulla rete.





SONICWALL

La 6ª funzione utile:

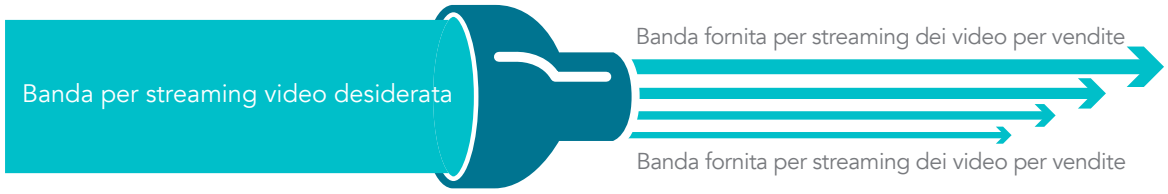
Gestione della larghezza di banda per un gruppo di utenti

Cosa fare se il CEO si lamenta del fatto che i filmati sulle notizie aziendali che vuole guardare ogni mattina scattano e non vengono riprodotti correttamente? In seguito a un'indagine, si rileva che la causa è una policy di gestione della larghezza di banda a livello aziendale che è stata implementata per tutti i video in streaming? Una soluzione potrebbe essere ridurre le restrizioni della larghezza di banda per tutti, ma oggi è disponibile una risposta migliore: la gestione della larghezza di banda in base ai gruppi.

Creazione di una policy per escludere i membri della dirigenza dalla gestione della larghezza di banda dei video in streaming

1. Selezionare il gruppo di dirigenti importato dal proprio server LDAP
2. Il motore Deep Packet Inspection utilizza firme di applicazioni per video in streaming predefinite prese dall'elenco delle firme delle applicazioni
3. Applicare la restrizione sulla larghezza di banda al traffico con tale intestazione

Molte aziende hanno riscontrato che i dipendenti preferiscono avere un accesso completo al Web, anche se dispongono di una larghezza di banda ridotta per i siti non produttivi.



SONICWALL™

La 7ª funzione utile:

Blocco degli attacchi ransomware e delle violazioni

La sicurezza di rete deve avere la massima priorità dal punto di vista di qualsiasi amministratore IT. L'abilità di bloccare attacchi come i ransomware e le violazioni veicolati da malware e da tentativi di intrusione evita di esporre l'organizzazione a grandi rischi e permette di risparmiare risorse potenzialmente sprecate. I servizi di sicurezza SonicWall, che girano sull'architettura ad alte prestazioni e a bassissima latenza dei firewall di nuova generazione di SonicWall, sono in grado di bloccare milioni di minacce note e ancora ignote evitando che penetrino nella rete, ancora prima che diventino un pericolo per la vostra organizzazione. SonicWall Capture estende le funzionalità di prevenzione delle minacce del firewall attraverso il rilevamento e la prevenzione di attacchi sconosciuti e zero-day per mezzo di un servizio di sandboxing basato sul cloud e multi-engine.

Bloccate attacchi e intrusioni del malware prima che entrino nella vostra rete!

SONICWALL™

L'8ª funzione utile:

Identificazione delle connessioni per Paese

Una connessione verso un IP in un paese straniero proveniente da una filiale locale dell'azienda o da una succursale è semplicemente una connessione benigna di qualcuno che sta navigando su Internet oppure si tratta di un'attività botnet? È possibile utilizzare l'analisi intelligente delle applicazioni come potente strumento di analisi forense per identificare esattamente cosa sta succedendo sulla rete e la provenienza di un'attività.

Visualizzazione delle connessioni per Paese o creazione di filtri per Paesi specifici

1. Verificare quali applicazioni si collegano a IP in altri Paesi
2. Controllare quali utenti e quali computer si collegano a IP in altri Paesi
3. Creare filtri per limitare il traffico verso i Paesi specificati, con liste di esclusione

Una volta che si conosce la risposta alla domanda, è possibile parlare con l'utente, ispezionare la macchina su cui si trova l'indirizzo IP problematico oppure abilitare una utility di acquisizione dei pacchetti sul firewall per analizzare esattamente cosa stia passando su tale connessione. Utilizzando SonicWall Application Intelligence and Control è possibile identificare e affrontare problemi di cui altrimenti si potrebbe non essere a conoscenza.

La 9ª funzione utile:

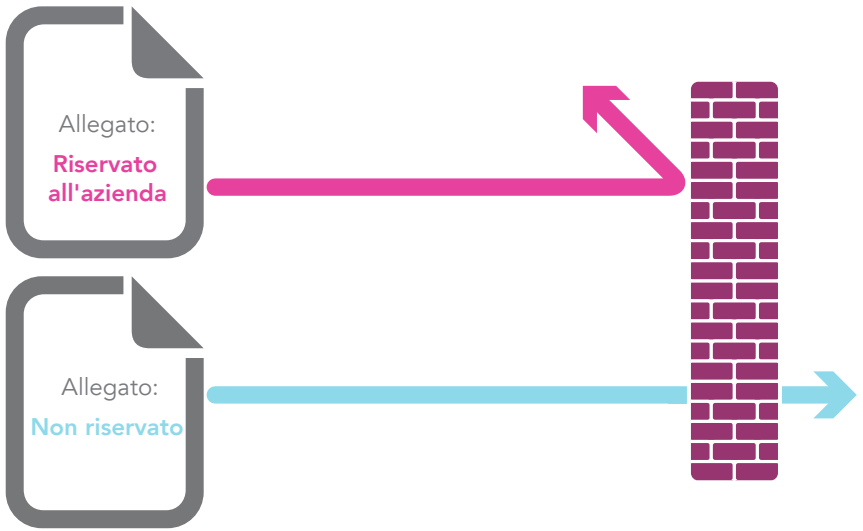
Prevenzione delle fughe di dati via e-mail

In alcune aziende, le e-mail in uscita non passano nel sistema di protezione e-mail oppure tale sistema non controlla il contenuto degli allegati e-mail. In entrambi i casi, gli allegati «riservati all'azienda» possono uscire facilmente dall'azienda. Poiché il traffico di rete in uscita attraversa il firewall, è possibile rilevare e bloccare questi «dati in fuga».

Creazione di una policy per bloccare gli allegati e-mail che contengono il watermark «riservato all'azienda»

Il motore Deep Packet Inspection va alla ricerca di:

1. Contenuto e-mail = «Riservato all'azienda» e
2. Contenuto e-mail = «Proprietà dell'azienda» e
3. Contenuto e-mail = «Proprietà privata», ecc.



SONICWALL™

La 10ª funzione utile:

Prevenzione delle fughe di dati tramite webmail

Ipotizziamo che l'attuale protezione antispam sia in grado di rilevare e bloccare una normale e-mail in uscita contenente l'informazione «riservato all'azienda». Ma cosa succede se un dipendente utilizza un servizio di webmail, come Yahoo® o Gmail®, per inviare informazioni «riservate all'azienda»?

Creazione di una policy per bloccare gli allegati «riservati all'azienda» nel traffico

1. Il motore Deep Packet Inspection va alla ricerca di «riservato all'azienda» su file trasferiti tramite http o https
2. Bloccare i messaggi e inviare una notifica al mittente che il messaggio è «riservato all'azienda»

OK

Da: bravoragazzo@vostra_azienda.com
A: bravoragazzo@partner.com
Oggetto: Approvazione cartellino Mario
Il tuo cartellino per questo mese è stato approvato. Carlo

STOP

Da: cattivapersona@tua_azienda.com
A: cattivapersona@concorrente.com
Oggetto: Road map di progetto
Ecco la road map
Gennaio 09 – Release 7.0
Questo documento è **Riservato all'azienda**

Anche per i contenuti basati su FTP.

L'11ª funzione utile:

Gestione della larghezza di banda per audio e video in streaming

A volte è utile accedere a video in streaming da siti come YouTube.com, ma spesso gli utenti ne abusano. Bloccare questi siti potrebbe funzionare, ma è preferibile un approccio che limiti la larghezza di banda totale concessa ai video in streaming, a prescindere dalla loro provenienza. Lo stesso vale per i siti di streaming audio, come le stazioni radio musicali on-line e i servizi di musica in streaming come Spotify ed Apple Music. Non è detto che questo traffico provenga da siti ben noti, ma può essere anche ospitato su blog. Pertanto, l'obiettivo è identificare questo traffico per ciò che è, anziché in base alla sua origine. La Deep Packet Inspection svolge egregiamente questo compito.

Creazione di una policy per limitare lo streaming di audio e video in base all'elenco di firme predefinite

1. Selezionare Video in streaming e Audio in streaming come categorie di applicazioni
2. Impostare la quantità di larghezza di banda che si desidera allocare a queste categorie di applicazioni (ad es. 10%)
3. Creare una regola che obblighi le categorie di Video in streaming e Audio in streaming a consumare al massimo il 10% della larghezza di banda per tutti (escludendo eventualmente i gruppi di particolari reparti, ad esempio quelli nel gruppo di formazione)
4. Come opzione, pianificare la regola in modo che abbia effetto durante gli orari di lavoro standard, ma non durante la pausa pranzo o dopo le 18:00.
5. Confermare l'efficacia della nuova policy con una visualizzazione in tempo reale accedendo all'Application Flow Monitor

SONICWALL™

Riepilogo delle funzionalità combinate

Piattaforma ad alte prestazioni
+ Ispezione deep packet
+ Prevenzione delle intrusioni
+ Controllo intelligente e visualizzazione delle applicazioni

Firewall di nuova generazione SonicWall

Prestazioni, protezione e controllo delle applicazioni

SONICWALL™

Informazioni su SonicWall

Da oltre 25 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 difesa informatica in tempo reale ottimizzata per le specifiche esigenze di oltre 500.000 aziende internazionali in più di 150 paesi, per consentire loro di fare più affari con maggior sicurezza.

Per qualsiasi domanda sul potenziale utilizzo di questo materiale, contattare

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Per maggiori informazioni, consultare il nostro sito web.
www.sonicwall.com

Ebook-11CoolThings-Firewall-US-KS-26242

SONICWALL™