UNDICI FUNZIONI IMPORTANTI CHE UN FIREWALL DEVE GARANTIRE

Non limitarsi a bloccare le minacce di rete
ma proteggere, gestire e controllare il traffico
delle applicazioni

SONICWALL®

Indice

SONICWALL®

I firewall crescono

I firewall tradizionali che utilizzano la tecnica SPI (Stateful Packet Inspection) si concentrano sul blocco delle minacce a livello di rete, valutando le porte e i protocolli utilizzati dal traffico a livello di rete. Gli ultimi firewall di prossima generazione (NGFW) utilizzano l'ispezione profonda dei pacchetti per effettuare la scansione dell'intero payload dei pacchetti con funzioni di prevenzione avanzata delle intrusioni, antimalware, filtraggio dei contenuti e anti-spam. Molte applicazioni vengono rese disponibili attraverso le comuni porte web sharing e i protocolli HTTP o HTTPS, il che non consente ai firewall tradizionali di vedere queste applicazioni e di prioritizzare il traffico produttivo e sicuro rispetto a quello improduttivo e insicuro. I firewall di prossima generazione forniscono indicazioni sulle applicazioni stesse, mettendo a disposizione degli specialisti delle reti un'importante capacità di discernimento.

Con la proliferazione del cloud computing e delle tecnologie Web 2.0 i firewall si trovano a dover affrontare un'ulteriore sfida: il controllo delle applicazioni.

SONICWALL®

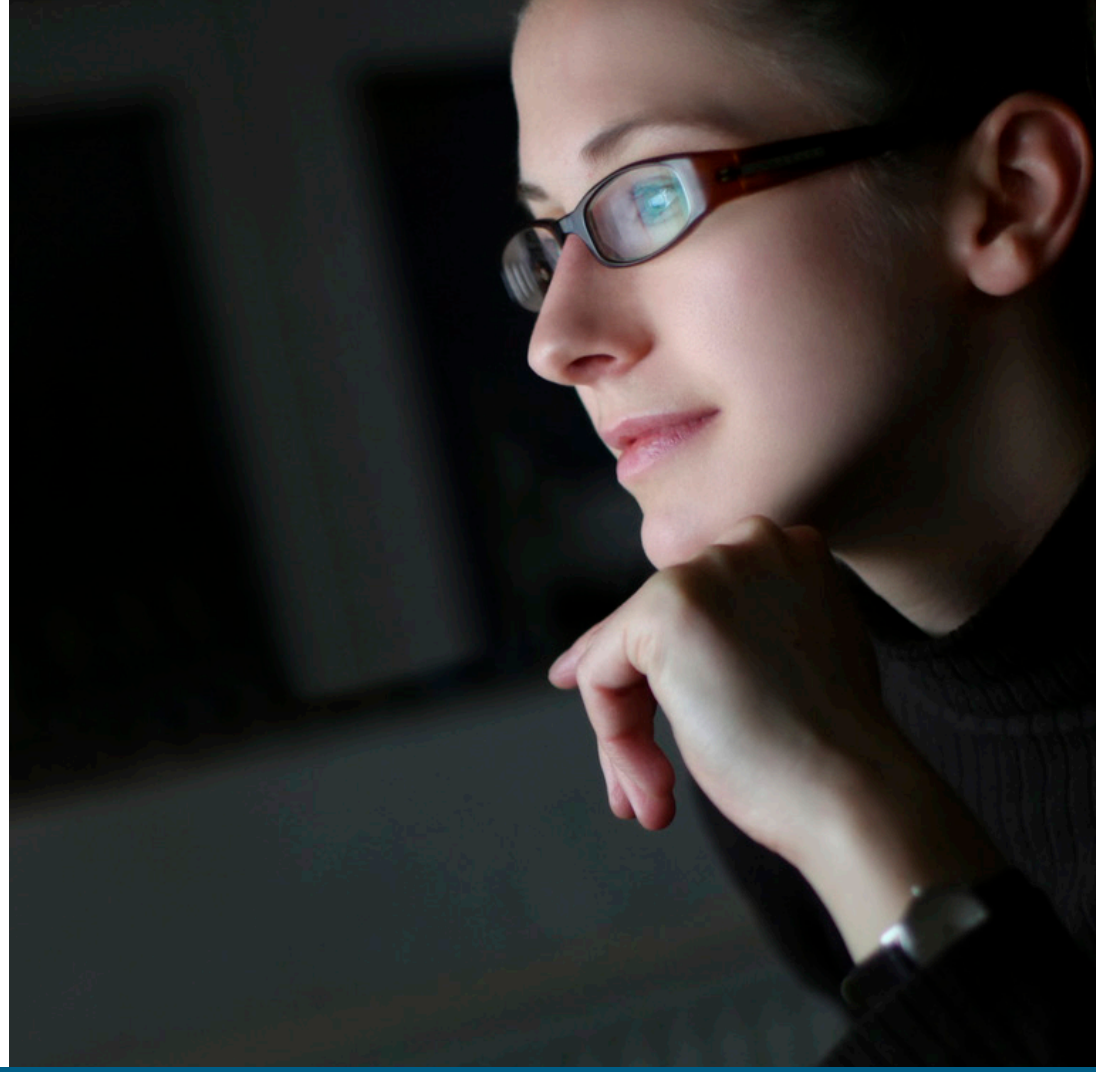
Che cosa fa SonicWall Application Intelligence and Control?

I firewall SonicWall consentono di identificare e controllare tutte le applicazioni in uso sulla rete. Questo ulteriore controllo migliora la conformità e la prevenzione delle perdite di dati identificando le applicazioni sulla base delle loro segnature univoche anziché in base alle porte o ai protocolli. Ciò si ottiene visualizzando il traffico delle applicazioni per determinare i modelli d'uso e definendo di conseguenza politiche granulari per applicazioni, utenti e persino gruppi di utenti, come pure l'ora del giorno e altre variabili per un controllo flessibile in grado di soddisfare qualsiasi esigenza di rete.

Assegnare la larghezza di banda per applicazioni mission-critical o sensibili alla latenza.

Come funziona SonicWall Application Intelligence and Control?

Utilizzando un ampio database di segnature di applicazioni in costante crescita aggiornato automaticamente SonicWall identifica le applicazioni sulla base del loro "DNA" anziché attraverso attributi meno univoci come la porta di origine, quella di destinazione o il tipo di protocollo. Ad esempio, è possibile autorizzare la messaggistica istantanea ma bloccare il trasferimento dei file o consentire l'accesso a Facebook ma bloccare quello ai giochi. Questi controlli sono disponibili anche per tutto il traffico crittografato TLS/SSL, che dev'essere verificato esattamente come le connessioni non crittografate. Inoltre è possibile visualizzare agevolmente i risultati dei controlli, con la conseguente possibilità di regolare di precisione l'uso delle applicazioni e ottimizzare la larghezza di banda di rete.



Controllare le categorie delle applicazioni, le singole applicazioni e le loro funzioni specifiche.

La visualizzazione delle applicazioni consente di “vedere”, prima di definire la politica, quali browser vengono utilizzati.

La prima chicca:

Controllare le applicazioni consentite in rete

Ci si deve accertare che tutti i dipendenti utilizzino l’ultima versione di Internet Explorer. Lo scopo è garantire che tutti i dipendenti che avviano IE9 o IE10 vengano automaticamente reindirizzati al sito per il download di IE11 e venga impedito loro l’accesso a qualsiasi altro sito. Le possibili soluzioni sono:

- Controllare fisicamente tutti i sistemi tutti i giorni per quanto riguarda la versione del browser
- Scrivere uno script personalizzato per controllare automaticamente le versioni del browser
- Definire una politica tramite SonicWall Application Intelligence and Control, e non pensarci più

Definire una politica per reindirizzare gli utenti di IE9 o IE10 sul sito per scaricare l’ultima versione di IE e bloccare l’accesso a IE9 e IE10

1. L’engine DPI (Deep Packet Inspection) verifica User Agent = IE 9.0 o User Agent = IE 10.0 nell’header HTTP
2. La politica reindirizza gli utenti IE9 e IE10 al sito per scaricare IE11, impedendo a IE9 e IE10 l’accesso ad altri siti

SONICWALL®

La seconda chicca:

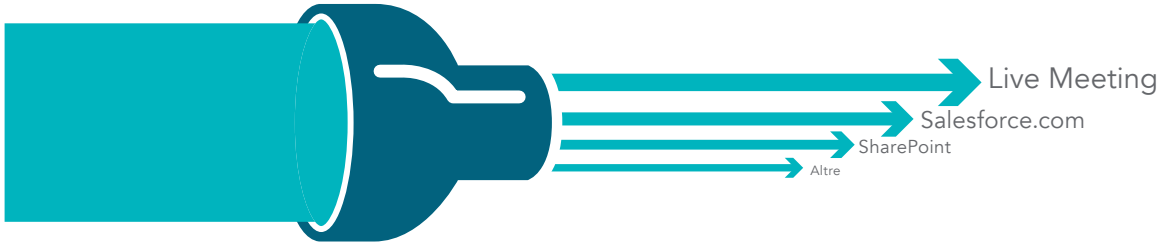
Gestire la larghezza di banda per le applicazioni critiche

Molte applicazioni critiche, come Live Meeting, Salesforce.com® e SharePoint®, sono basate sul cloud, o girano su reti disperse geograficamente. Garantire che tali applicazioni abbiano priorità rispetto alla navigazione web improduttiva migliora la produttività delle imprese.

Definire una politica per assegnare in via prioritaria la larghezza di banda all'applicazione Live Meeting

1. L'engine DPI verifica la segnatura o il nome delle applicazioni
2. Assegnare all'applicazione Live Meeting una larghezza di banda maggiore in via prioritaria

La priorità delle applicazioni può essere basata sulla data (considerare la priorità a fine trimestre per le applicazioni di vendita).



SONICWALL®

La terza chicca:

Bloccare le applicazioni peer-to-peer

Le applicazioni peer-to-peer (P2P) improduttive come BitTorrent vengono spesso utilizzate per scaricare copie senza licenza di filmati protetti da copyright, e possono consumare rapidamente la larghezza di banda o trasmettere malware. Tuttavia la creazione di nuove applicazioni P2P, o anche semplici cambiamenti (ad esempio i numeri delle versioni) alle applicazioni P2P esistenti hanno luogo costantemente, per cui diventa difficile bloccare manualmente le singole applicazioni P2P.

SonicWall aggiorna continuamente il database d'intelligence e di controllo con l'aggiunta di nuove applicazioni non appena si rendono disponibili. È quindi possibile definire semplicemente una politica per bloccare da quel momento in poi tutte le applicazioni P2P.

Definire una politica per impedire l'uso delle applicazioni P2P

1. L'engine DPI utilizza le segnature delle applicazioni P2P predefinite dall'elenco delle segnature delle applicazioni
2. Scegliere le applicazioni P2P dall'elenco delle segnature predefinite
3. Applicare la politica a tutti gli utenti
4. Bloccare le applicazioni P2P mediante limitazioni basate sulla larghezza di banda e sul tempo

Elenco delle segnature delle applicazioni

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

+

Elenco delle segnature delle applicazioni

Aggiornamenti SonicWall ricevuti ed applicati

=

Elenco delle segnature delle applicazioni

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

I risultati

- È possibile gestire e controllare le applicazioni P2P
- Non è necessario sprecare tempo ad aggiornare le regole delle segnature IPS

La quarta chicca:

Bloccare i componenti improduttivi delle applicazioni

Le applicazioni social come Facebook, Instagram e YouTube sono diventate nuovi canali di comunicazione utilizzati dalle persone e dalle aziende. Bloccare tutte le applicazioni social può essere controproduttivo, però si può controllare come vengono usate sul posto di lavoro.

Ad esempio, è possibile consentire al personale di marketing di aggiornare la pagina Facebook aziendale, ma non di giocare su Facebook a Texas HoldEm Poker o Candy Crush Saga. Con l'intelligence e il controllo delle applicazioni è possibile definire una politica che consenta l'accesso a Facebook, ma blocchi i giochi.

Definire una politica per consentire l'accesso a Facebook ma non ai giochi

1. Selezionare "Tutti" gli utenti
2. Selezionare "Applicazioni giochi Facebook" come categoria
3. Definire una singola regola per "Bloccare" a tutti gli utenti l'accesso ai giochi di Facebook

È anche possibile consentire la chat, bloccando i trasferimenti di file in chat.

La quinta chicca:

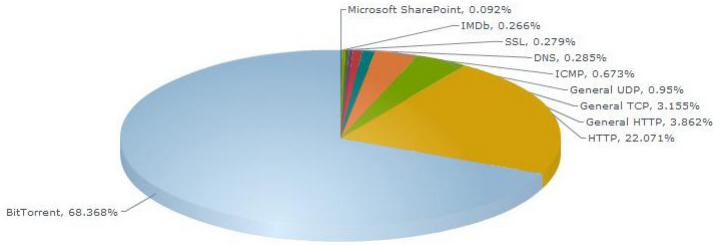
Visualizzare il traffico delle applicazioni

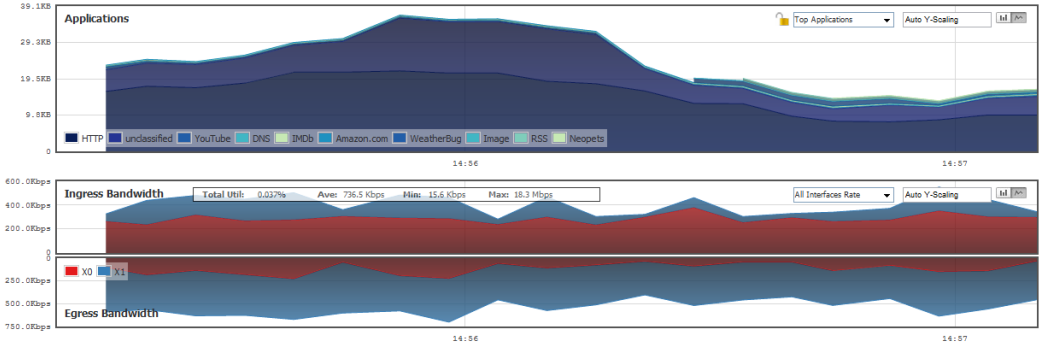
Che cosa sta succedendo alla rete? Chi è che consuma la larghezza di banda? Perché la rete è diventata lenta? Vi siete mai posti queste domande? È possibile utilizzare una combinazione di strumenti per cercare di dare una risposta, ma è un processo che richiede tempo, e può comunque fornire indicazioni solo a cose fatte. Grazie alla visualizzazione del traffico delle applicazioni in tempo reale di SonicWall è possibile rispondere a queste domande istantaneamente, diagnosticare rapidamente i problemi, individuare l'uso di rete non conforme, definire apposite politiche ed apprezzarne immediatamente l'efficacia.

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

1. Visualizzare i grafici in tempo reale del traffico di tutte le applicazioni
2. Visualizzare i grafici in tempo reale della larghezza di banda in ingresso e in uscita
3. Visualizzare i grafici in tempo reale dei siti visitati e l'attività di tutti gli utenti
4. Definire filtri propri per ottenere le informazioni di maggiore interesse

La visualizzazione consente agli amministratori di avere un riscontro immediato sui flussi di traffico in rete.





SONICWALL®

La sesta chicca:

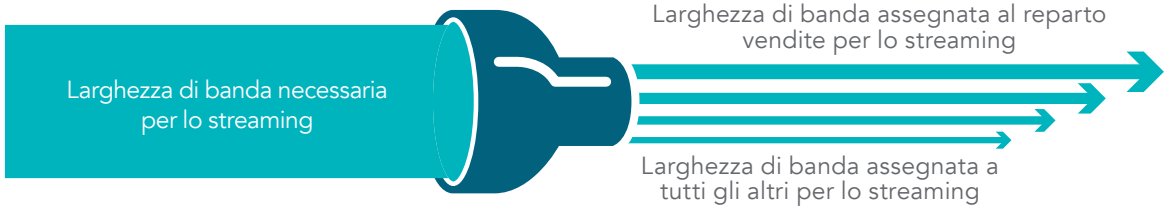
Gestire la larghezza di banda per singoli gruppi di utenti

Che cosa fate se il vostro CEO si lamenta che i video dei notiziari che vuole guardare tutte le mattine vanno a singhiozzo e non vengono riprodotti correttamente? Fatti i debiti controlli, stabilite che il problema ha a che fare con la politica aziendale di gestione della larghezza di banda attuata per tutti i filmati in streaming. Era facile limitare la larghezza di banda per tutti, ma adesso c'è un modo migliore, la gestione della larghezza di banda basata sui gruppi.

Definire una politica per escludere i membri della dirigenza dalla gestione della larghezza di banda per i filmati in streaming

1. Scegliere il gruppo dei dirigenti importato dal server LDAP
2. L'engine DPI utilizza le segnature delle applicazioni di streaming predefinite dall'elenco delle segnature delle applicazioni
3. Applicare la limitazione della larghezza di banda al traffico che presenta quell'header

Molte aziende hanno riscontrato che i dipendenti sono più contenti se viene consentito loro l'accesso completo al web, anche se è stata ridotta la larghezza di banda per i siti improduttivi.



SONICWALL

La settima chicca:

Bloccare le violazioni e gli attacchi ransomware

La sicurezza delle reti dev'essere la prima preoccupazione degli amministratori dei sistemi informatici. La capacità di bloccare gli attacchi tipo ransomware e le violazioni effettuate tramite malware e i tentativi d'intrusione evita alle aziende grossi rischi e fa risparmiare risorse che andrebbero altrimenti sprecate. I servizi di sicurezza di SonicWall, che girano sull'architettura di prestazioni elevate a latenza ultrabassa dei firewall SonicWall di prossima generazione, sono in grado d'impedire l'accesso alla rete di milioni di minacce note e non, prima che possano provocare danni all'organizzazione. SonicWall Capture estende le capacità di prevenzione delle minacce del firewall individuando e prevenendo gli attacchi sconosciuti e zero giorni tramite un servizio di sandboxing multi-engine basato sul cloud.

Bloccate gli attacchi di malware e le intrusioni prima che possano entrare in rete!

SONICWALL®

L'ottava chicca:

Identificare le connessioni in base al paese

Una connessione ad un IP di un paese estero dal vostro ufficio periferico locale o da una filiale è solo una connessione benigna di qualcuno che sta navigando in Internet o è un'attività di botnet? È possibile utilizzare la funzione di identificazione del traffico in base al paese di GeoIP per identificare e controllare il traffico di rete verso o da determinati paesi per proteggersi dagli attacchi di origine nota o sospetta della minaccia, o per indagare il traffico sospetto proveniente dalla rete.

Visualizzare le connessioni in base al paese o definire filtri specifici per i singoli paesi

1. Verificare quali applicazioni si stanno collegando ad IP di altri paesi
2. Guardare quali utenti e quali computer si stanno collegando ad IP di altri paesi
3. Definire dei filtri per limitare il traffico verso determinati paesi tramite elenchi di esclusione

Una volta trovata la risposta è possibile parlare con l'utente, controllare la macchina con l'indirizzo IP che non rispetta le regole, o attivare un'utility di cattura dei pacchetti sul firewall per analizzare esattamente che cosa passa su quella connessione. Grazie alla funzione di identificazione del traffico in base al paese GeoIP di SonicWall è possibile identificare e risolvere problemi di cui prima non si era neppure a conoscenza.

La nona chicca:

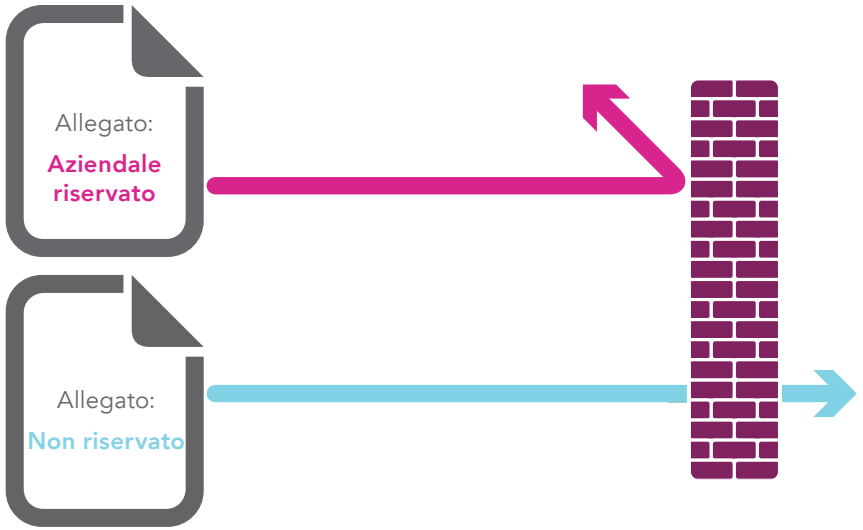
Prevenire le perdite di dati via email

In alcune aziende le email in uscita non passano attraverso il sistema di sicurezza della posta elettronica, o il sistema non verifica il contenuto degli allegati. In entrambi i casi possono uscire dall'azienda allegati riservati. Poiché il traffico di rete in uscita passa attraverso il firewall, è possibile individuare e bloccare questi dati quando sono in movimento.

Definire una politica per bloccare gli allegati alle email contenenti la filigrana "Aziendale riservato"

L'engine DPI verifica:

1. Il contenuto delle email = "Aziendale riservato" e
2. Il contenuto delle email = "Aziendale proprietario" e
3. Il contenuto delle email = "Privato proprietario" etc.



SONICWALL®

La decima chicca:

Prevenire le perdite di dati via webmail

Immaginiamo che la protezione antispam esistente sia in grado di rilevare e bloccare un normale messaggio in uscita contenente informazioni “aziendali riservate”. Ma che cosa succede se un dipendente utilizza un servizio di posta elettronica come Yahoo® o Gmail® per inviare informazioni “aziendali riservate”?

Definire una politica per bloccare gli allegati “aziendali riservati” nel traffico web

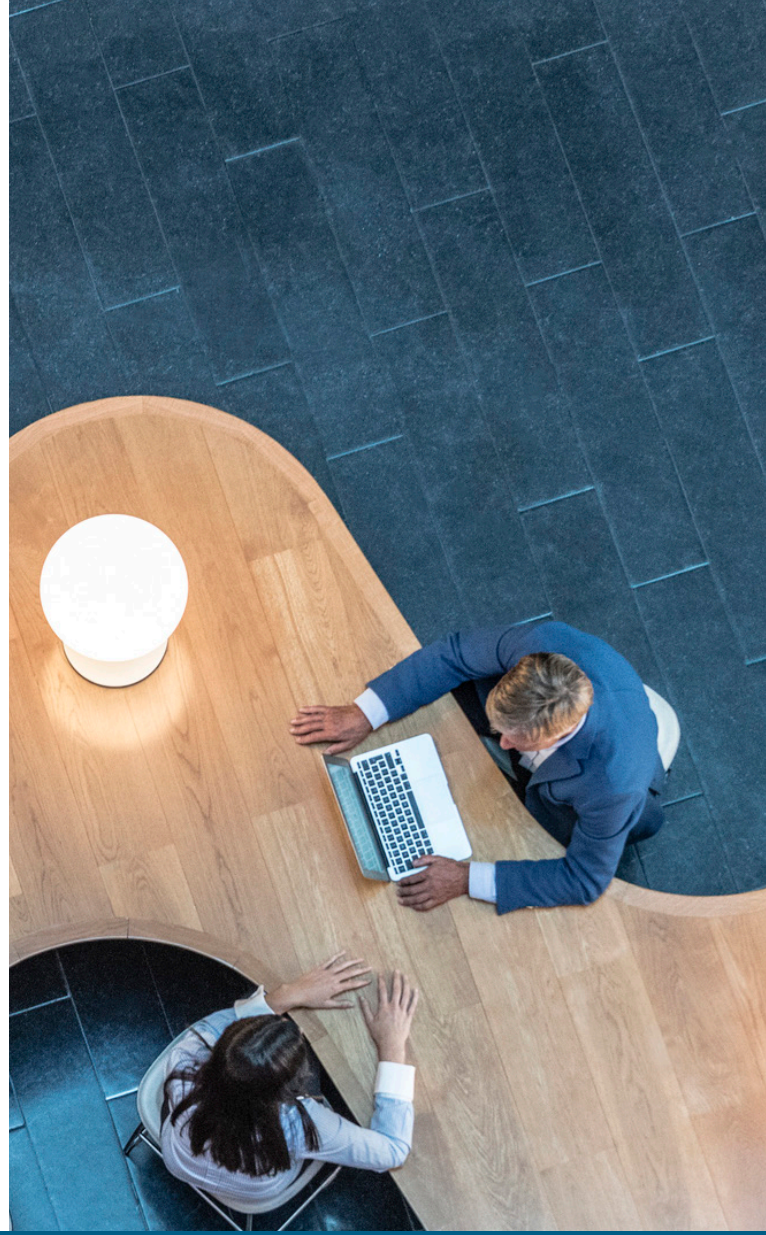
1. L’engine DPI verifica la presenza di informazioni “aziendali riservate” nei file trasferiti via http o https
2. Bloccare il messaggio e notificare al mittente che si tratta di informazioni “aziendali riservate”

GO

Da: goodguy@your_company.com
A: goodguy@partner.com
Oggetto: Approvazione cartellino presenze Giacomo
Approvo il tuo cartellino presenze per questa settimana. Giuseppe

STOP

Da: badguy@your_company.com
A: badguy@competitor.com
Oggetto: Piano di sviluppo del progetto
Ecco il piano di sviluppo
Gen 09 – Versione 7.0
Questo è un documento **aziendale riservato**



Lo stesso si può fare anche per il contenuto basato su FTP.

L'undicesima chicca:

Gestire la larghezza di banda per lo streaming audio e video

Accedere ai filmati in streaming da siti come YouTube.com può essere utile, ma spesso se ne abusa. Bloccare questi siti può essere una soluzione, ma un approccio preferibile è limitare la larghezza di banda totale assegnata allo streaming, indipendentemente dalla sua provenienza. Lo stesso vale anche per i siti di streaming audio, come le stazioni radio musicali online ed i servizi di streaming musicale come Spotify ed Apple Music. Questo traffico non proviene necessariamente da siti noti, ma può anche essere ospitato nei blog. Pertanto l'obiettivo è identificare questo tipo di traffico per quello che è, anziché in base alla sua provenienza. L'engine DPI a questo proposito è il massimo.

Definire una politica per limitare lo streaming audio e lo streaming video servendosi di un elenco di segnature predefinito

1. Selezionare Streaming Video e Streaming Audio come categorie di applicazione
2. Impostare la larghezza di banda da assegnare ad esse (es., 10%)
3. Definire una regola per limitare al 10% per tutti il consumo di ampiezza di banda per lo Streaming Video e lo Streaming Audio (eventualmente escludendo gruppi di determinati reparti, come quelli che si occupano di formazione)
4. Facoltativamente programmare l'attivazione della regola durante il normale orario di lavoro, ma non in quello del pranzo o dopo le 18.
5. Verificare l'efficacia della nuova politica tramite la visualizzazione in tempo reale accedendo all'Application Flow Monitor

SONICWALL®

Se si sommano tutte queste funzioni

Piattaforma di presentazioni elevate
+ DPI
+ Prevenzione delle intrusioni
+ Controllo, intelligence e visualizzazione in tempo reale delle applicazioni

---

Firewall SonicWall di prossima generazione

Sicurezza, prestazioni e controllo

SONICWALL®

Chi siamo

SonicWall è attiva nel settore della lotta al cibercrimine da più di 27 anni a difesa delle PMI, delle grandi aziende e delle multinazionali in ogni parte del mondo. Grazie ad un attento abbinamento di prodotti e partner, abbiamo realizzato una soluzione di rilevazione e prevenzione automatica delle violazioni in tempo reale, calibrata sulle specifiche esigenze di oltre 500.000 organizzazioni in più di 215 paesi e territori, che consente ai nostri clienti di lavorare di più con maggiore tranquillità. Per ulteriori informazioni visitare www.sonicwall.com o seguirci su Twitter, LinkedIn, Facebook e Instagram.

Per chiarimenti riguardanti il potenziale utilizzo di questo materiale rivolgersi a:

SonicWall Inc.
1033 McCarthy Boulevard
Milpitas, CA 95035

Per ulteriori informazioni consultare il nostro sito web.
www.sonicwall.com

Ebook-11CoolThings-Firewall-US-VG-MKTG5084

SONICWALL