SonicWALL® Scrutinizer

GESTIONE E REPORTING

Tool di reporting, visualizzazione e analisi del traffico applicativo

- **Analisi e report granulari**
- **Risoluzione avanzata dei problemi**
- **Potente visualizzazione**
- **Analisi forense ottimizzata**
- **Analisi SonicWALL del traffico delle applicazioni**
- **Supporto di terze parti**
- **Allarmi personalizzabili**
- **Gestione flessibile**

Le organizzazioni sono sempre più sotto pressione per massimizzare la produttività, ottimizzare gli investimenti di capitale e abbattere i costi (inclusi gli abbonamenti mensili ai servizi Internet). Allo stesso tempo il traffico di applicazioni non aziendali come Web 2.0 e social media aumenta in maniera esponenziale, a scapito della larghezza di banda disponibile e della produttività. I tool di reporting e monitoraggio obsoleti offrono una certa visibilità sulle porte e i protocolli in uso, ma non riescono a fornire una visione globale del traffico applicativo in transito attraverso firewall, router e switch e non sono in grado di rilevare minacce provenienti da host infetti all'interno della rete. I fornitori di servizi gestiti (MSP, Managed Service Provider) e i rivenditori a valore aggiunto (VAR, Value Added Reseller) hanno inoltre la necessità di dimostrare ai propri clienti il valore dei servizi offerti e, al contempo, monitorare i costi e il tempo impiegato per gestire i singoli account.

SonicWALL® Scrutinizer è un tool di reporting, visualizzazione e analisi del traffico di applicazioni multi-vendor che permette di misurare le prestazioni attuali e storiche della rete e correggerne in tempo reale eventuali problemi, aumentando così la produttività di aziende e fornitori di servizi. Scrutinizer supporta un'ampia gamma di router, switch e firewall e svariati protocolli di reporting dei flussi di dati.

Scrutinizer supporta i dispositivi di rete dei principali vendor. In combinazione con un firewall di nuova generazione di SonicWALL offre tuttavia prestazioni eccellenti. Scrutinizer fornisce una comprensione senza precedenti delle analisi del traffico delle applicazioni esportate dai firewall SonicWALL tramite IPFIX o NetFlow. Scrutinizer è in grado di identificare le principali comunicazioni tra applicazioni e client nonché le applicazioni e i flussi, protocolli, utenti, domini, paesi e sottoreti maggiormente utilizzati. Sebbene altri produttori di firewall forniscano il supporto per NetFlow o IPFIX, solo SonicWALL offre un'analisi così dettagliata del traffico delle applicazioni.

Scrutinizer genera report automatici sul monitoraggio proattivo di jitter/latenze, analisi approfondita del traffico delle applicazioni, allarmi in caso di comportamenti sospetti e dashboard personalizzabili. Scrutinizer offre inoltre report storici e avanzati, gestione basata sui ruoli, analisi avanzate, allarmi di soglia[1] e tante altre funzioni speciali per MSP e ISP[2].

Caratteristiche e vantaggi

Analisi e report granulari con visualizzazione semplificata dei principali host, protocolli, porte, applicazioni, traffico e comunicazioni client/applicazioni per tutti i dispositivi e i settori della rete. Le opzioni di analisi flessibile consentono di visualizzare i trend di utilizzo in bit, byte, pacchetti o percentuale di larghezza di banda totale consumata. Scrutinizer supporta sia IPFIX che Flexible NetFlow, per la creazione di modelli di report personalizzabili, e può memorizzare tutti i dati di flusso per un periodo di tempo indefinito.

Risoluzione avanzata dei problemi grazie a IPFIX, che offre funzioni più dettagliate per risolvere problemi come colli di bottiglia, latenza, jitter, timeout attivo, principali comunicazioni tra client e applicazioni, flussi più frequenti degli host, volume degli host, volume di coppie di indirizzi, indirizzi MAC, VLAN e domini più utilizzati.

Potenti strumenti di visualizzazione con le principali interfacce di tutti i router, switch e firewall per visualizzare il traffico applicativo attuale (in tempo reale) o archiviato mediante grafici interattivi, tabelle e Google® Maps, un'innovativa vista a matrice per visualizzare i campi di flusso e mappe di rete con i dati dei flussi rilevanti.

Analisi forense ottimizzata per rilevare e segnalare applicazioni non autorizzate, traffico dannoso, host Internet infetti, violazioni del numero di sequenza del flusso, DNS cache poisoning, indirizzi IP e server DHCP/di posta elettronica non autorizzati, scansione delle porte, traffico multicast eccessivo, HTTP hijacking e attacchi DDOS.

L'**analisi SonicWALL del traffico delle applicazioni** è una soluzione unica nel suo genere che combina un avanzato firewall di nuova generazione con il software Scrutinizer. Il firewall trasmette i dati IPFIX in tempo reale all'applicazione di analisi del traffico, con cui l'amministratore può esaminare i dati di utilizzo in base ad applicazioni o utenti, analizzare i dati di periodi differenti e altro ancora. Il supporto per NetFlow o IPFIX viene fornito anche da altri vendor di firewall, ma solo SonicWALL offre un'analisi così dettagliata del traffico delle applicazioni.

Il **supporto di terze parti** garantisce la compatibilità con centinaia di router, switch e firewall di altri fornitori, offrendo la possibilità di monitorare migliaia di interfacce simultaneamente.

Gli **allarmi personalizzabili** sono attivabili in caso di utilizzo delle interfacce, flussi incompleti, attività illecite e deterioramento della qualità voce e video, con possibilità di visualizzare quanti altri allarmi sono stati provocati da un host.

Le funzionalità di **gestione flessibile** offrono dashboard personalizzabili in base all'account di login e autorizzazioni basate su gruppi o sul login per accedere ai flussi di determinate interfacce di router, switch e firewall. I provider di servizi gestiti (MSP) possono facilmente modificare i fogli di stile per adattarli al brand aziendale.

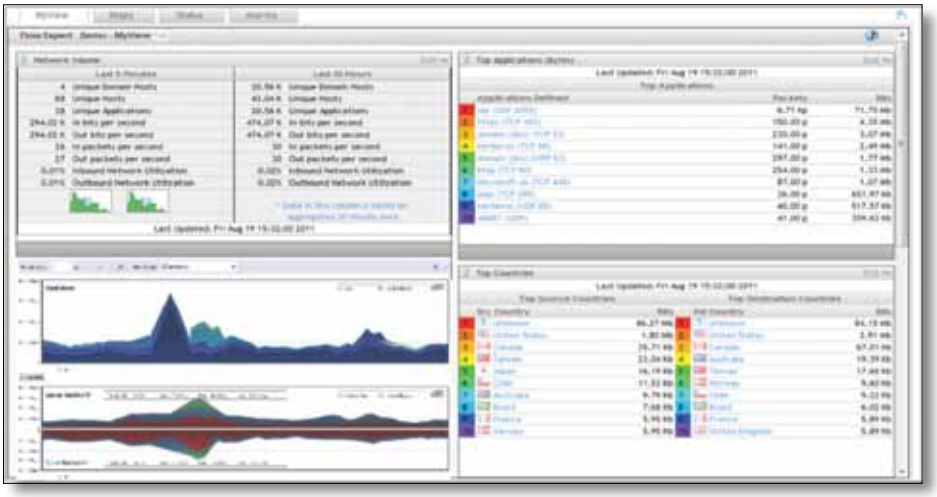
[1] Questa funzionalità richiede il modulo Flow Analytics
[2] Disponibile nel modulo Service Provider

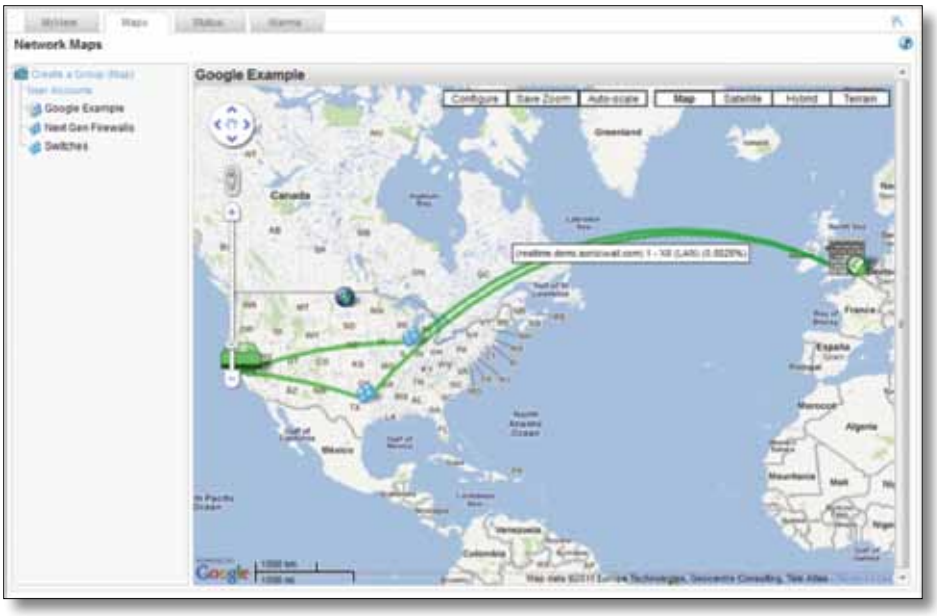
SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Dashboard personalizzabile

Il dashboard utente personalizzabile offre una visione rapida e dettagliata delle prestazioni della rete. È possibile creare cruscotti per ogni utente per avere una visione semplice e dettagliata delle applicazioni maggiormente utilizzate o del volume di rete o per visualizzare mashup personalizzati rilevanti per un determinato utente.





Google Maps

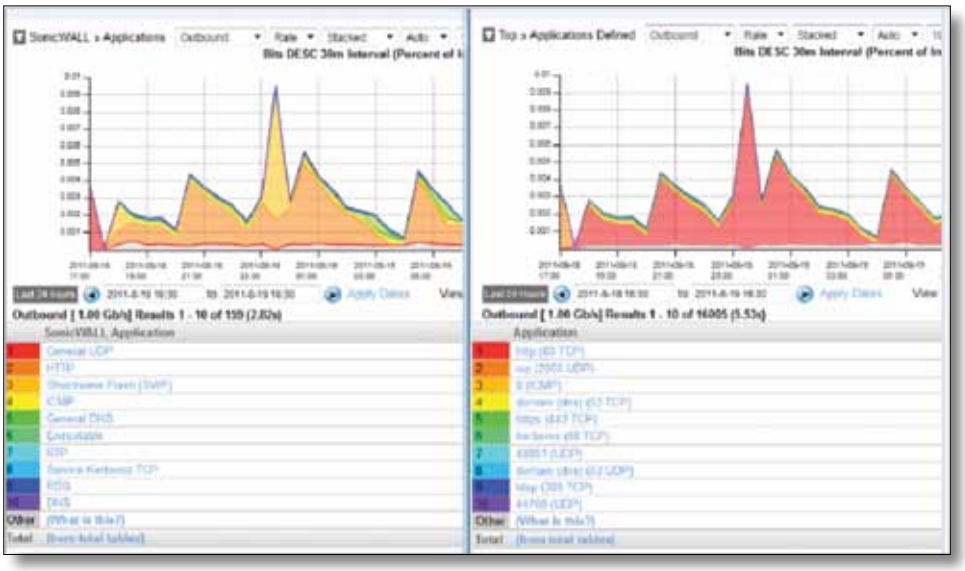
L'integrazione di Google Maps offre una vista completa dell'intera rete, anche a livello globale! I collegamenti sono evidenziati a colori e visualizzati in base allo stato attuale, agevolando così la risoluzione dei problemi.

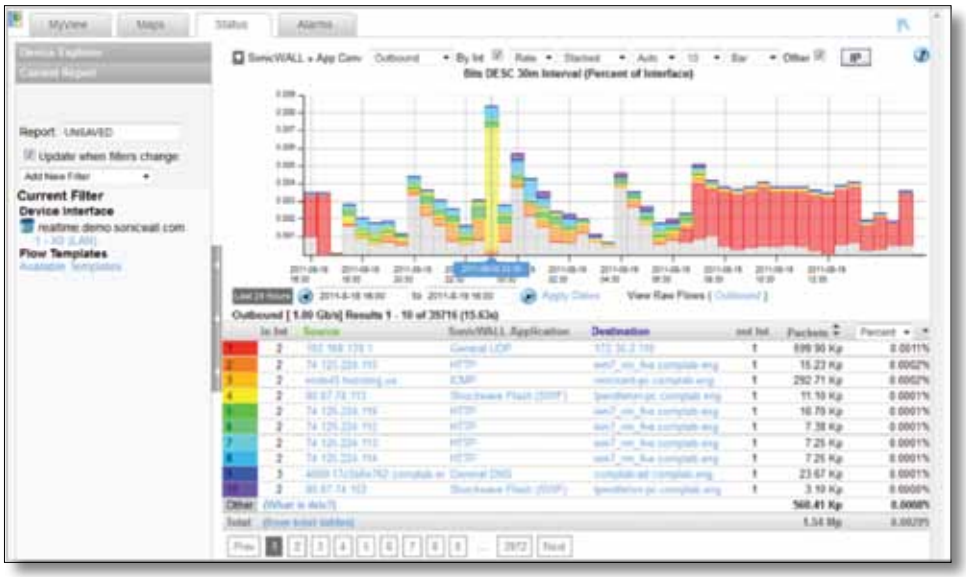
Vista a matrice

L'innovativa vista a "matrice" offre una potente visualizzazione delle comunicazioni tra applicazioni e client in tutta la rete. Le connessioni host-to-host sono facilmente rilevabili in quanto vengono visualizzate nel momento in cui vengono create.

Modelli SonicWALL

I modelli SonicWALL personalizzabili offrono un ulteriore livello di granularità per l'analisi dettagliata del traffico che attraversa la rete. A sinistra: SonicWALL IPFIX con modelli. A destra: tradizionale analisi del traffico delle applicazioni.



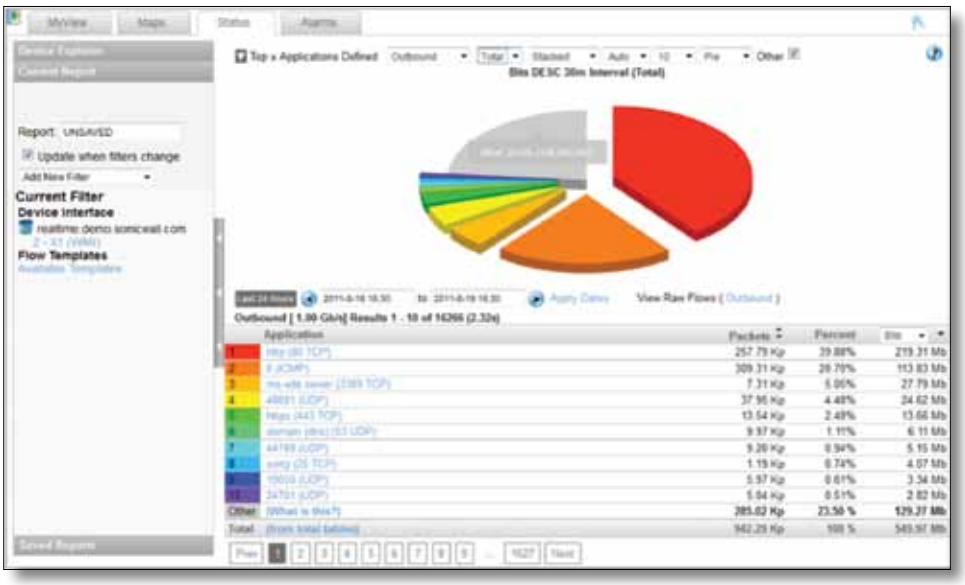


Comunicazioni tra applicazioni e client

Il traffico delle applicazioni può essere frammentato in intervalli di tempo specifici per identificare i picchi di utilizzo. Le statistiche sull'uso delle applicazioni offrono una visione chiara e dettagliata delle prestazioni della rete.

Indicazioni relative alle applicazioni

Permette di suddividere il traffico delle applicazioni in diverse viste per analizzarlo in base a numero di pacchetti, bit, byte o percentuale del traffico totale nell'arco di un determinato intervallo di tempo.



Caratteristiche e specifiche

Implementazione consigliata

Hardware
x64 Quad Core 2 GHz
8 GB di RAM
50 GB HDD (IDE o SATA)

Sistema operativo
Windows Server 2008 a 64 bit (R2)
[tutte le edizioni]

Requisiti minimi

Hardware
x64 Dual Core 2,2 GHz
4 GB di RAM
50 GB HDD (IDE o SATA)

Sistema operativo
Windows Server 2008 a 64 bit (SP2)
[tutte le edizioni]
Windows 7 a 64 bit, Professional o Enterprise
Windows Vista a 64 bit, Professional o Enterprise

SonicWALL Scrutinizer con modulo Flow Analytics

5 nodi
01-SSC-4002

25 nodi
01-SSC-4003

illimitati
01-SSC-4004

Moduli add-on

Modulo Managed Service Provider

5 nodi
01-SSC-4515

25 nodi
01-SSC-4516

illimitati
01-SSC-4521

Modulo Cisco Advanced Reporting
01-SSC-4536

Nota: per informazioni sulle opzioni di aggiornamento dei nodi e sui codici prodotto supportati, visitare **www.sonicwall.com**

	Scrutinizer gratuito	Scrutinizer con i moduli Flow Analytics	Scrutinizer con i moduli Flow Analytics e Service Provider
Capacità e visualizzazione			
Dati archiviati	Fino a 24 ore	illimitati	illimitati
In combinazione con l'archiviazione dei report fornisce una piattaforma per l'analisi dei trend	Fino a 24 ore	■	■
Elenco delle interfacce più utilizzate per tutti i router, switch e firewall	Limitato a 5 interfacce	■	■
Compatibile con i prodotti di numerosi fornitori	■	■	■
Capacità di gestire fino a 20.000 flussi al secondo con v8.X	■	■	■
Supporto di oltre 1.000 sistemi di esportazione e più di 1.000 interfacce	■	■	■
Integrazione con Google Maps	■	■	■
Reporting flessibile			
Invio pianificato di report per email		■	■
Possibilità di includere ed escludere dati mediante i filtri	■	■	■
Possibilità di rinominare i modelli per un uso futuro	■	■	■
Definizione della pagina iniziale di default per l'accesso dei clienti	■	■	■
Definizione di gruppi di applicazioni tramite campi di porte e indirizzi IP	■	■	■
Visualizzazione dei dati in bit, byte, pacchetti o in percentuale	■	■	■
Precisione fino al secondo di ricezione grazie a FlowView	■	■	■
Report per ogni interfaccia su host, protocolli e applicazioni più utilizzati, principali comunicazioni client/applicazioni e altro ancora	■	■	■
Salvataggio dei filtri per i report personalizzati		■	■
Trend sui dati in ingresso/uscita o in entrambe le direzioni simultaneamente, in tutti i report	■	■	■
Possibilità di aggiungere più interfacce per più router, switch o firewall in un unico report	■	■	■
Filtraggio in base a qualsiasi campo esportato (ad es. indirizzi MAC, VLAN, latenza, ecc.) nei modelli	■	■	■
Facile identificazione delle applicazioni più utilizzate in rete da svariati dispositivi		■	■
Report MPLS in base alle sottoreti		■	■
Report e trend sui protocolli di Microsoft® Exchange		■	■
Archiviazione di tutte le registrazioni e tutti i flussi per tutto il tempo necessario, anche per un periodo indefinito		■	■
Creazione di report basati su paesi, domini o sottoreti di maggiore utilizzo		■	■
Modelli di report specifici di SonicWALL		■	■
Soluzioni di fatturazione personalizzabili, ad es. per utilizzo eccessivo e per l'emissione delle fatture			■
Allarmi			
Allarmi per filtri memorizzati, elevata attività delle interfacce, flussi incompleti e attività illecite		■	■
Tutti i report salvati in Scrutinizer possono essere configurati con una soglia per l'attivazione di un allarme		■	■
Indice univoco per ogni allarme (segnala quanti altri allarmi ha provocato l'host)		■	■
Gli amministratori possono monitorare proattivamente la qualità del servizio (QoS) e ricevere un allarme automatico in caso di deterioramento del traffico voce/video		■	■
Risoluzione dei problemi			
Tool di risoluzione dei problemi che aiuta gli amministratori a identificare eventuali "rallentamenti" della rete	■	■	■
Analisi di latenza/jitter solo in nProbe	■	■	■
Ricerca di host o porte specifici	■	■	■
Tool di pianificazione della capacità per determinare l'utilizzo durante le ore di massimo traffico		■	■
Volume dei flussi per ogni host o volume di host univoci		■	■
Volume di coppie di indirizzi (a/da) univoci		■	■
Le statistiche IPFIX forniscono maggiori dettagli sui dati VoIP (codec, ID del chiamante, durata, origine, destinazione, ecc.)		■	■
Sicurezza			
Intervallo di tempo configurabile per la cache DNS	■	■	■
Filtraggio in base a "host-host" e "subnet-subnet"	■	■	■
Possibilità di filtrare il traffico in base ai flag TCP	■	■	■
Tracciamento del numero di sequenza del flusso, rilevamento delle tendenze dei risultati e segnalazione dei problemi	■	■	■
Rilevamento e allarme per applicazioni proibite (ad es. BitTorrent P2P, FTP, YouTube, Facebook, Skype, ecc.)		■	■
Rilevamento e allarme per traffico dannoso (ad es. worm, virus), host Internet infetti, indirizzi IP illegali, traffico multicast eccessivo, HTTP hijacking, DNS cache poisoning, server DHCP non autorizzati, attacchi DDoS, ecc.		■	■
Rilevamento e allarme per scansione: SYN, NULL, FIN, XMAS, ecc.		■	■
Amministrazione			
Dashboard MyView personalizzabili per l'accesso	■	■	■
Autorizzazioni degli utenti basate su gruppi	■	■	■
Configurazione delle autorizzazioni in base all'account di login, per accedere ai flussi di determinate interfacce di router, switch o firewall			■
Facile modifica dei fogli di stile con svariate impostazioni di default per adattare colori, font e logo e supportare le iniziative di marketing del provider di servizi			■
Protocolli supportati e altre specifiche tecniche			
Personalizzazione dei nomi delle interfacce e modifica dei nomi SNMP ifAlias di default	■	■	■
Personalizzazione della velocità dell'interfaccia (in ingresso e in uscita) con valori differenti	■	■	■
Identificazione dei nomi delle interfacce mediante NetFlow o SNMP	■	■	■
Integrazione con qualsiasi soluzione NMS di terze parti	■	■	■
Supporto LDAP	■	■	■
Rilevamento di flussi su un numero illimitato di porte UDP	■	■	■
Supporto di IPv6	■	■	■
Supporto di NetFlow v1, v5, v6, v7, v9, jFlow, sFlow (v2, v4, v5), SNMP(v1, v2, v3) e IPFIX	■	■	■
Filtro per Nexthop	■	■	■
Supporto di FnF NBAR e IPFIX nell'ispezione approfondita dei pacchetti per identificare il traffico delle applicazioni a livello 7		■	■
La risoluzione DNS diventa un processo automatizzato e costante.		■	■

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

SONICWALL®
DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

©2010 SonicWALL e il logo SonicWALL sono marchi registrati di SonicWALL, Inc. "Dynamic Security For The Global Network" è un marchio di SonicWALL, Inc. I nomi di altri prodotti qui menzionati possono essere marche e/o marchi registrati delle rispettive società. Con riserva di modifiche. 10/10 SW 1083