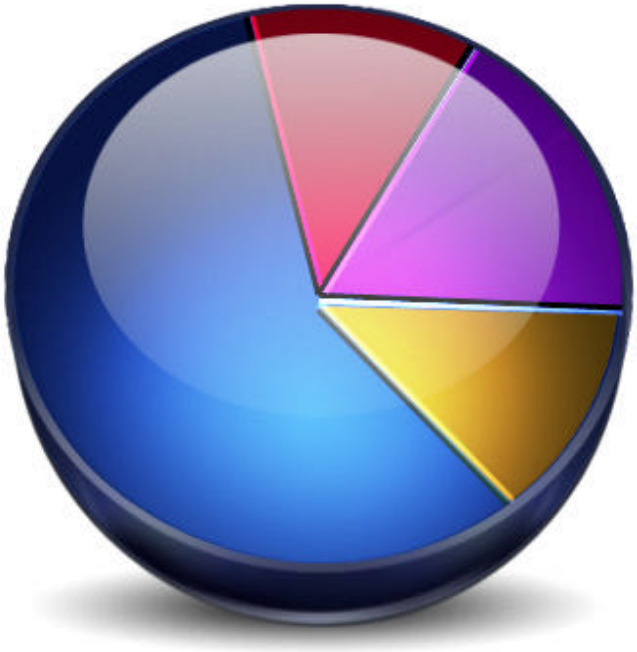

SONICWALL

Reporting

Table of Contents

OVERVIEW OF SONICWALL REPORTING 3

CATEGORIE DI REPORT_CATEGORIES OF REPORTS 4

PANORAMICA DEI REPORT DI RIEPILOGO SONICWALL 6

REPORT DI RIEPILOGO DELLE AUTENTICAZIONI 6
REPORT DI RIEPILOGO DELLO STATO 6
REPORT DI RIEPILOGO DELLA LARGHEZZA DI BANDA 6
REPORT DI RIEPILOGO DEL ROI 6
REPORT DI RIEPILOGO DEI SERVIZI 7
REPORT DI RIEPILOGO DELL'UTILIZZO DELLA VPN 7
REPORT DI RIEPILOGO DELL'UTILIZZO DEL WEB 7
REPORT DI RIEPILOGO DEL TEMPO DI NAVIGAZIONE 7
REPORT DI RIEPILOGO DEL FILTRAGGIO WEB 8
REPORT DI RIEPILOGO FTP 8
REPORT DI RIEPILOGO DELLA POSTA ELETTRONICA 8
REPORT DI RIEPILOGO DEGLI ATTACCHI 9
REPORT DI RIEPILOGO DEGLI ATTACCHI VIRUS 9
REPORT DI RIEPILOGO DELLA PREVENZIONE INTRUSIONI 9

EXECUTIVE SUMMARY OF REPORTS 10

FOR JANUARY 15, 2007 10
Authentication Summary 10
Status Summary 10
Bandwidth Summary 10
ROI Summary 11
Services Summary 11
VPN Summary 11
Web Usage Summary 11
Browse Time Summary 11
FTP Summary 12
Mail Summary 12
Attack Summary 12
Virus Attack Summary 12
Intrusion Prevention Summary 12

SAMPLE SONICWALL REPORT 10-42

Overview of SonicWALL Reporting

Il monitoraggio di attività ed eventi critici della rete – come ad esempio minacce alla sicurezza, uso improprio delle risorse Web e un consumo eccessivo della larghezza di banda disponibile – è un componente essenziale per qualsiasi rete moderna. Le soluzioni di reporting SonicWALL si integrano alla perfezione con i dispositivi SonicWALL per la sicurezza in Internet, fornendo report dettagliati e completi sulle diverse attività svolte in rete. SonicWALL GMS™ e ViewPoint™ rappresentano un salto di qualità decisivo nel reporting di rete.

Entrambe le soluzioni GMS (Global Management System) e ViewPoint consentono agli amministratori IT di creare riepiloghi dinamici, cronologici e in tempo reale basati sul robusto modulo di reporting SonicWALL, offrendo così la massima visibilità sullo stato della rete. Grazie ai report sulla conformità che possono essere personalizzati ed esportati in diversi formati, le aziende e i service provider possono sfruttare le potenti capacità del reporting SonicWALL per capire come viene utilizzata la propria rete, tenere traccia degli eventi che hanno minacciato la rete e analizzare le tendenze di utilizzo. Gli amministratori possono inoltre monitorare gli accessi alla rete, potenziare la sicurezza e prevedere le esigenze future in termini di larghezza di banda.

Le soluzioni di reporting SonicWALL:

- mostrano il consumo di banda per ogni servizio o indirizzo IP
- identificano eventuali utilizzi impropri del Web
- forniscono report dettagliati sugli attacchi subiti
- registrano e aggregano gli errori di sistema e della rete
- segnalano eventi e problemi relativi alla rete VPN
- offrono un riepilogo del traffico verso un determinato sito Web
- forniscono log giornalieri con tutti gli eventi per ogni firewall

Le soluzioni di reporting SonicWALL offrono una maggiore visibilità nel complesso mondo di attività digitali gestito dalle appliance di sicurezza SonicWALL. Il presente documento offre una panoramica esauriente sui report di riepilogo SonicWALL, completata da un report completo a titolo di esempio.

Vi invitiamo quindi a dare uno “sguardo in profondità” al mondo del reporting SonicWALL.

Categorie di report

Di seguito sono elencate le categorie di report disponibili nella famiglia di soluzioni per il reporting SonicWALL:

- Login Reports
  - User Login
  - Admin Login
  - Failed Login
- Status Reports
  - Status Summary
- Bandwidth Reports
  - Bandwidth Summary
  - Bandwidth Top Users
- ROI Reports
  - ROI Summary
  - ROI Top Users
- Service Reports
  - Services Summary
- VPN Reports
  - VPN Summary
  - VPN Top Users
  - VPN By Policy
  - VPN By Policy Hourly
  - VPN By Service
- Web Usage Reports
  - Web Usage Summary
  - Web Usage Top Sites
  - Web Usage Top Users
  - Web Usage By User
  - Web Usage By Category
  - Web Usage By Site
- Browse Time Reports
  - Browse Time Summary
  - Browse Time Top Users
  - Browse Time By User
- Web Filter Reports
  - Web Filter Summary
  - Web Filter Top Sites
  - Web Filter Top Users
  - Web Filter By User, By Site
  - Web Filter By Category
- FTP Reports
  - FTP Usage Summary
  - FTP Usage Top Users

- Mail Reports
    - Mail Usage Summary
    - Mail Usage Top Users
- Attacks Reports
    - Attacks Summary
    - Attacks By Category
    - Attacks Errors
- Virus Attacks Reports
    - Virus Attacks Summary
    - Virus Attacks Top Viruses
- Spyware Reports
    - Spyware Summary
    - Spyware By Category
- Intrusions Reports
    - Intrusions Summary
    - Intrusions By Category

Panoramica dei report di riepilogo SonicWALL

Report di riepilogo delle autenticazioni

I report sui login di autenticazione mostrano i login effettuati con successo da utenti e amministratori e i tentativi di login falliti di utenti e amministratori. Ad esempio, il report sui login degli utenti contiene il nominativo di tutti gli utenti che hanno effettuato l'accesso all'appliance SonicWALL (ad es. in un determinato giorno) per eludere il filtraggio dei contenuti o per accedere in remoto alle risorse della rete locale. Il report sui login degli amministratori elenca gli accessi effettuati da un amministratore in un determinato giorno. Questo report è utile per identificare tentativi di abuso e di gestione non autorizzata di un dispositivo SonicWALL.

Report di riepilogo dello stato

I report di stato visualizzano il numero di ore in cui uno o più dispositivi SonicWALL sono rimasti online e in funzione durante un periodo di tempo specificato. In base a queste informazioni, un amministratore può localizzare con esattezza i punti in cui si è verificato un problema all'interno della rete o, ad esempio, identificare un dispositivo SonicWALL con problemi di connettività causati dalla rete interna o dal fornitore di accesso a Internet (ISP). Per un provider di servizi gestiti, questo report è estremamente utile per documentare a un cliente gestito il rispetto degli accordi sui livelli di servizio (SLA) garantiti.

Report di riepilogo della larghezza di banda

I report sulla larghezza di banda indicano la quantità di dati trasmessi attraverso una o più appliance SonicWALL e rappresentano quindi lo strumento ideale per analizzare il consumo della larghezza di banda a livello globale. Gli amministratori IT possono vedere quanta banda è stata utilizzata in una determinata ora o giornata, o in un periodo di giorni, e quali sono gli utenti che impegnano maggiormente la banda. Sulla base di queste informazioni, un'azienda può valutare quali strategie sono più adeguate per la propria rete. Se ad esempio occorre una maggiore larghezza di banda, l'azienda può rinnovare le proprie apparecchiature di rete o aumentare la banda disponibile per l'accesso a Internet dalla rete aziendale o, più semplicemente, limitare l'utilizzo della banda a pochi dipendenti selezionati.

Report di riepilogo del ROI

I report sul ritorno dell'investimento (ROI) mostrano il costo totale legato alla larghezza di banda utilizzata (in megabyte), cioè trasferita attraverso una o più appliance SonicWALL. I report sul ROI sono lo strumento ideale per verificare il costo totale derivante dal consumo di banda nella propria rete. Gli amministratori possono generare report sul ROI per una determinata ora o giornata, o per un periodo di giorni. Inoltre hanno la possibilità di capire quali sono gli utenti che impegnano

maggiormente la banda e quale percentuale del costo totale è attribuibile a ognuno di questi utenti.

Analogamente ai report sulla larghezza di banda, anche queste informazioni possono essere utilizzate per valutare nuove strategie aziendali come ad esempio un aumento della banda disponibile, l'aggiornamento delle apparecchiature esistenti, l'ottimizzazione della tecnologia WAN o una semplice limitazione dell'accesso a Internet mediante appositi strumenti di limitazione della larghezza di banda.

Report di riepilogo dei servizi

I report sui servizi forniscono informazioni sulla quantità di dati trasmessi da ogni servizio attraverso una determinata appliance SonicWALL. I report sui servizi sono particolarmente utili per identificare un utilizzo improprio della larghezza di banda o anche per valutare la necessità di nuove policy per la rete. Se ad esempio viene rilevato un picco nel consumo di banda, un amministratore di rete può consultare il report e capire se la causa è dovuta al normale accesso al Web, a un utente che utilizza il server FTP per trasferire file di grandi dimensioni, a un tentativo di attacco DoS (Denial of Service) o agli altri servizi esistenti.

Report di riepilogo dell'utilizzo della VPN

I report sull'utilizzo della VPN forniscono informazioni sulla percentuale di utilizzo della VPN attraverso una o più appliance SonicWALL. Questi report consentono di visualizzare l'utilizzo della VPN in una determinata ora o giornata, o in un periodo di giorni, e di vedere quali sono gli utenti che fanno un maggiore utilizzo dei tunnel VPN. I report generici sull'utilizzo della larghezza di banda non forniscono sempre un quadro esauriente del consumo di banda in una rete. Se invece viene rilevato un traffico VPN elevato, un'azienda può decidere di aumentare la propria connettività a Internet, implementare dispositivi di ottimizzazione della WAN o riconfigurare la rete VPN per migliorare l'instradamento del traffico dati nei tunnel site-to-site.

Report di riepilogo dell'utilizzo del Web

Il report sull'utilizzo del Web contiene informazioni sulla larghezza di banda HTTP elaborata da un dispositivo SonicWALL per ogni ora di un giorno specifico. I report sull'utilizzo del Web consentono di verificare quanta banda è stata utilizzata per navigare in Internet nell'arco di un'ora, di una giornata o di un periodo di giorni specifico. Gli amministratori possono vedere quali utenti impegnano maggiormente la larghezza di banda per navigare nel Web e quali sono i siti più richiesti e visitati dai dipendenti. Questo tipo di report permette alle aziende di valutare la produttività dei propri dipendenti.

Report di riepilogo del tempo di navigazione

I report sul tempo di navigazione mostrano la quantità di tempo trascorso a navigare in Internet attraverso una o più appliance SonicWALL. Gli amministratori possono verificare il tempo di navigazione in Internet per una determinata ora o giornata, o per un periodo di giorni specifico, e vedere quali sono gli utenti che navigano

maggiormente nel Web, con la relativa percentuale di tempo per ogni utente calcolata sulle ore totali di navigazione. Mediante queste informazioni, un'azienda può individuare con maggiore chiarezza le strategie da adottare. Se ad esempio occorre ridurre le spese associate al consumo di banda, il manager IT può generare dei report sul tempo di navigazione per sapere quanto tempo viene trascorso a navigare in Internet visitando siti Web non correlati alla funzione professionale di un determinato dipendente.

Report di riepilogo del filtraggio Web

Il report sul filtraggio Web mostra il numero di tentativi di accesso a siti bloccati, in un determinato giorno, utilizzando una o più appliance SonicWALL. Questi report includono i nomi dei siti Web bloccati in base alla lista di filtraggio dei contenuti, a parole chiave personalizzate e ai nomi di dominio. I report sul filtraggio Web possono essere utilizzati per controllare i tentativi di accesso a siti bloccati in una determinata ora, giornata o periodo di giorni. Gli amministratori possono inoltre vedere quali sono gli utenti che tentano più spesso di accedere a siti bloccati e quali sono i siti più richiesti fra quelli bloccati.

Report di riepilogo FTP

I report sull'utilizzo FTP forniscono informazioni sulla percentuale di utilizzo del server FTP attraverso una o più appliance SonicWALL. Questi report sono indicati per monitorare il consumo di banda FTP in una determinata ora, giornata o periodo di giorni, con la possibilità di identificare gli utenti che impegnano maggiormente la larghezza di banda FTP.

I report generici sull'utilizzo della larghezza di banda non forniscono sempre un quadro completo del consumo di banda in una rete. Se invece viene rilevato un traffico FTP intenso, ad esempio durante le ore di punta, un'azienda può considerare un aumento della larghezza di banda disponibile oppure rinnovare i propri apparati di rete, adottare misure interne per evitare che il traffico dati si concentri nelle ore di punta o chiedere ai propri dipendenti di comprimere i file di grandi dimensioni prima di trasmetterli.

Report di riepilogo della posta elettronica

I report sull'utilizzo della posta elettronica forniscono informazioni sul traffico e-mail realizzato attraverso una o più appliance SonicWALL. L'amministratore IT può vedere quanta banda è stata utilizzata per il traffico e-mail in una determinata ora o giornata, o in un periodo di giorni specifico, e quali utenti occupano maggiormente la banda disponibile per inviare o ricevere e-mail. I report sull'utilizzo della posta elettronica includono il traffico SMTP, POP3 e IMAP. Mentre i report generici sull'utilizzo della banda non forniscono sempre un quadro completo del consumo di banda in una rete, mediante questi report un'azienda può rilevare ad esempio un traffico e-mail intenso durante le ore di punta e decidere di aumentare la banda disponibile o di utilizzare maggiormente servizi di Web mail in un ambiente di hosting gestito, oppure di limitare le dimensioni degli allegati per il traffico SMTP.

Report di riepilogo degli attacchi

I report sugli attacchi mostrano il numero di attacchi indirizzati o inoltrati attraverso una o più appliance SonicWALL, come ad esempio attacchi di tipo DoS (Denial of Service) o tramite pacchetti sonda, tentativi d'intrusione e qualsiasi altra attività maligna diretta all'appliance SonicWALL o ai computer della rete LAN o DMZ. Come per ogni ambiente di rete distribuito, SonicWALL consiglia di adottare un approccio multilivello per garantire la massima protezione della rete. Grazie ai report riepilogativi sugli attacchi subiti, gli amministratori di rete possono verificare quanti e quali attacchi sono stati neutralizzati mediante le appliance SonicWALL, valutando così l'efficacia dei dispositivi di protezione installati sul perimetro della rete aziendale.

Report di riepilogo degli attacchi virus

I report sugli attacchi virus mostrano il numero di attacchi virus indirizzati o inoltrati attraverso una o più appliance SonicWALL. Analogamente al report di riepilogo degli attacchi, anche il report sui virus illustra l'efficacia dell'appliance SonicWALL nel neutralizzare gli attacchi virus prima che possano penetrare nella rete aziendale.

Report di riepilogo della prevenzione intrusioni

I report creati dal servizio IPS (Intrusion Prevention Service) indicano il numero di tentativi d'intrusione che si sono verificati in un determinato periodo di tempo. Questi report sono un'ulteriore dimostrazione delle potenti capacità della tecnologia d'ispezione deep packet di SonicWALL.

Executive Summary of Reports

For January 15, 2007

This Executive Summary of Reports highlights key findings in various network, usage, services and security reports.

Use this report to help do the following:

- Evaluate the effectiveness of and compliance of your Internet usage policy
- Document the time and bandwidth impact of Web browsing on your IT operations
- Identify Web-based services that reduce the effectiveness of or circumvent installed security measures
- Help understand how your organization is using and consuming its Internet resources

Below is a summary of the key findings in this daily report for ACME, Inc.:

Authentication Summary

Five or more repeated attempts within a 15-minute time period are highlighted in your report. There were ten (10) recorded user logins for this particular report day. Tommy Nguyen made 6 attempts into the network and Art King made 2. The rest of the user logins were single attempts. Further investigation should be made into identifying any misuse and/or unauthorized management of your SonicWALL appliance.

Status Summary

We have recorded that your SonicWALL unit has been up 100% of the time and there have been no service disruptions for this report date. This is in alignment your Service Level Agreement (SLA) set forth with your managed services contract.

Bandwidth Summary

This report shows your company has exchanged 82.917 Mbytes of data between the local network and the Internet for the given report period. The hourly consumption graph shows the times that the network is under the least, average, and maximum load.

ROI Summary

Your Return on Investment (ROI) report illustrates that 24.596 Mbytes of bandwidth was consumed through your SonicWALL appliance resulting in a net cost of $0.246 (factoring the cost of your monthly Internet charges) for the given report period. Also, between the hours of 01:00 – 02:00 and 13:00 – 14:00 your SonicWALL appliance recorded a surge of Internet traffic. Your top bandwidth user on this particular day was Sanjay Sawney with 46.587% of they day's total Internet traffic. Further investigation may be required in order to make sure there are no spyware/adware applications on this user's machine and if this employee is adhering to your company's Internet usage policy.

Services Summary

Your Services Summary Report shows that 76.632% of your Internet traffic comes from TCP/HTTP traffic for this particular daily report. This amounts to 59.769 Mbytes and 10,952 events.

VPN Summary

VPN usage accounted for 2.914 Mbytes of Internet traffic resulting in 4,247 events. A peak surge of VPN traffic occurred between 21:00 - 22:00, which accounted for 9.292% of the daily VPN traffic. Services running over TCP port 1886 accounted for 33.117% of the overall daily traffic resulting in 0.855 Mbytes and 92 Events. Dolph Smith accounted for 39.405% of the overall VPN traffic. This amount of VPN traffic was normal given the typical Internet traffic on your network.

Web Usage Summary

Web usage accounted for 61.296 Mbytes of traffic resulting in 11,291 events. A peak surge of Web Usage occurred between 07:00 – 08:00, which accounted for 7.178% of Web usage traffic. The most frequently visited Web usage category was "Information Technology/Computers" and accounted for 39.751%. The top visited website was www.hotmail.com and accounted for 45.736% of traffic. The top user of the Web is Sanjay Sawney who accounted for 45.080%. Further investigation may be required to investigate appropriate usage of the company's internet services.

Browse Time Summary

Browse Time accounted for 00:09:27 of time spent browsing the Internet. A peak surge of browse time occurred between 11:00 – 12:00, which accounted for 5.820% of total Browse Time traffic. The user spending the most time browsing on this day was Sanjay Sawney who accounted for 53.673% of all browse time. Further investigation may be required to investigate appropriate usage of the company's internet services.

FTP Summary

FTP usage amounted to 2.790 Mbytes of traffic. A peak surge of FTP services occurred between 14:00 – 15:00, which accounted for 92.542% of the day's FTP traffic. The top FTP user was Sanjay Sawney who used 68.131% of the total FTP bandwidth. Since the aggregate amount of FTP traffic is small, further investigation is not warranted.

Mail Summary

Mail usage for SMTP, POP3 and IMAP traffic accounted for 0.281 Mbytes of traffic. A peak surge of mail usage occurred between 19:00 – 20:00, which accounted for 18.002% of all mail traffic. The top mail user was Greg Etemad who accounted for 45.151% of all mail traffic. Further investigation may be required to investigate appropriate usage of the company's mail services.

Attack Summary

The account summary report shows that 157 attacks were attempted on your company's network on this particular report day. 6.369% of these attacks occurred between the hours of 11:00 – 12:00. 88.535% of attacks were IP Spoof attacks coming from source IP addresses 64.220.173.243 and 7.1.1.10. Your SonicWALL appliance is dynamically updated with new signatures everyday to thwart such attacks. However, further investigation of these attacks may be warranted.

Virus Attack Summary

The Virus Attack report shows that 211 attacks were launched against your company's network on this particular report day. 65.403% of the attacks occurred between the hours of 14:00 – 15:00. 26.066% of virus attacks were "Nesky.Gen-2(Worm)" attacks coming from source IP address 63.198.213.253. Your SonicWALL appliance is dynamically updated with new signatures everyday to thwart such attacks. However, further investigation of these attacks may be warranted.

Intrusion Prevention Summary

The Intrusion Prevention Service (IPS) report shows 548 IPS attacks were launched against your company's network on this particular report day. 61.314% of the attacks occurred between the hours of 14:00 – 15:00. 23.443% of the attacks were coming from an internal rogue machine with IP address 192.168.169.180. Further investigation is required to identify this machine and uncover the nature of these IPS probes. Your SonicWALL appliance is dynamically updated with new signatures everyday to thwart such attacks. However, further investigation of these attacks may be warranted.