SONICWALL GLOBAL MANAGEMENT SYSTEM

Soluzione completa di analisi, reporting, monitoraggio e gestione della sicurezza

Una strategia vincente di gestione della sicurezza richiede una profonda comprensione dell'ambiente di sicurezza per favorire un miglior coordinamento delle policy e decisioni migliori. Spesso, la mancanza di una visione globale della struttura di sicurezza aziendale espone le organizzazioni al rischio di attacchi informatici e violazioni della conformità che sarebbero prevenibili. L'uso di numerosi strumenti su piattaforme diverse e di formati di dati differenti per la creazione dei report rende inefficienti le funzioni di analisi e reportistica di sicurezza. Ciò compromette ulteriormente la capacità dell'azienda di riconoscere rapidamente i rischi di sicurezza e reagire. Per superare queste criticità le aziende devono adottare un approccio sistematico alla gestione degli ambienti di sicurezza di rete.

Il SonicWall Global Management System (GMS) consente di risolvere tutte queste problematiche. GMS integra funzioni di gestione, monitoraggio, analisi anche forense e creazione di rapporti di controllo. Queste funzionalità costituiscono la base di una strategia di governance della sicurezza, conformità e gestione del rischio. La piattaforma GMS, con la sua vasta gamma di funzioni, offre ad imprese distribuite, fornitori di servizi e altre organizzazioni un approccio fluido e olistico per consolidare tutti gli aspetti operativi del proprio ambiente di sicurezza. Grazie a GMS i team addetti alla sicurezza possono gestire con facilità le soluzioni SonicWall come firewall, punti di accesso wireless, sicurezza e-mail, soluzioni per l'accesso mobile protetto e switch di rete di altri fornitori. Questo processo viene realizzato attraverso un flusso di lavoro governato e verificabile che garantisce l'efficienza, la sicurezza e la conformità della rete. GMS include funzioni di gestione e applicazione centralizzata delle policy, monitoraggio degli eventi in tempo reale, analisi granulare dei dati e creazione dei relativi report, audit trail e altro ancora, il tutto in una piattaforma di gestione unificata.

Vantaggi:

- Creazione di un programma unificato di governance della sicurezza, conformità e gestione del rischio
- Approccio coerente e verificabile all'orchestrazione della sicurezza, all'analisi forense e alla creazione di rapporti
- Riduzione del rischio e risposta tempestiva agli eventi di sicurezza
- Visione d'insieme dell'intero ecosistema di sicurezza aziendale
- Automazione dei flussi di lavoro e conformità delle procedure di sicurezza
- Creazione di rapporti conformi a HIPAA, SOX e PCI per revisori interni ed esterni
- Installazione semplice e veloce, a scelta come software, appliance virtuale o nel cloud – il tutto a un costo ridotto.

CONTROLLO CENTRALIZZATO

- Una soluzione semplice e completa di gestione della sicurezza, reporting analitico e conformità per unificare il programma di protezione della rete
- Automazione e correlazione dei flussi di lavoro per creare una strategia coordinata di governance della sicurezza, conformità e gestione del rischio

CONFORMITÀ

- I report automatici di sicurezza conformi a PCI, HIPAA e SOX aiutano a soddisfare i requisiti degli organismi di regolamentazione e controllo
- Personalizzazione di combinazioni di dati di sicurezza verificabili per agevolare il percorso verso specifiche norme di conformità

GESTIONE DEL RISCHIO

- I report automatici di sicurezza conformi a PCI, HIPAA e SOX aiutano a soddisfare i requisiti degli organismi di regolamentazione e controllo
- Personalizzazione di combinazioni di dati di sicurezza verificabili per agevolare il percorso verso specifiche norme di conformità

GMS offre un approccio olistico alla governance della sicurezza, alla conformità e alla gestione del rischio

GMS soddisfa i requisiti di gestione delle modifiche delle imprese attraverso processi e procedure di automazione dei flussi di lavoro. La funzione di workflow garantisce la correttezza e la conformità delle modifiche alle policy mediante un rigoroso processo di configurazione, comparazione, convalida, revisione e approvazione delle policy prima della loro implementazione. I gruppi di approvazione flessibili consentono di rispettare le politiche di sicurezza aziendali e, al tempo stesso, riducono il rischio e gli errori, incrementano l'efficienza e assicurano un'elevata efficacia in termini di sicurezza. Grazie all'automazione dei flussi di lavoro e al controllo delle modifiche alle policy, GMS offre alle imprese maggiore agilità e la sicurezza di applicare le policy del firewall in modo corretto, nel momento giusto e nel rispetto delle normative di conformità.

GMS offre un approccio olistico alla governance della sicurezza, alla conformità e alla gestione del rischio

1. CONFIGURAZIONE E CONFRONTO

GMS configura gli **ordini di modifica** delle policy e le differenze in base a **codici colore** per offrire confronti chiari

2. CONVALIDA

GMS esegue una **convalida** dell'integrità della logica delle **policy**

3. REVISIONE E APPROVAZIONE

GMS invia e-mail ai revisori e registra un **audit trail di approvazione/ disapprovazione** delle policy

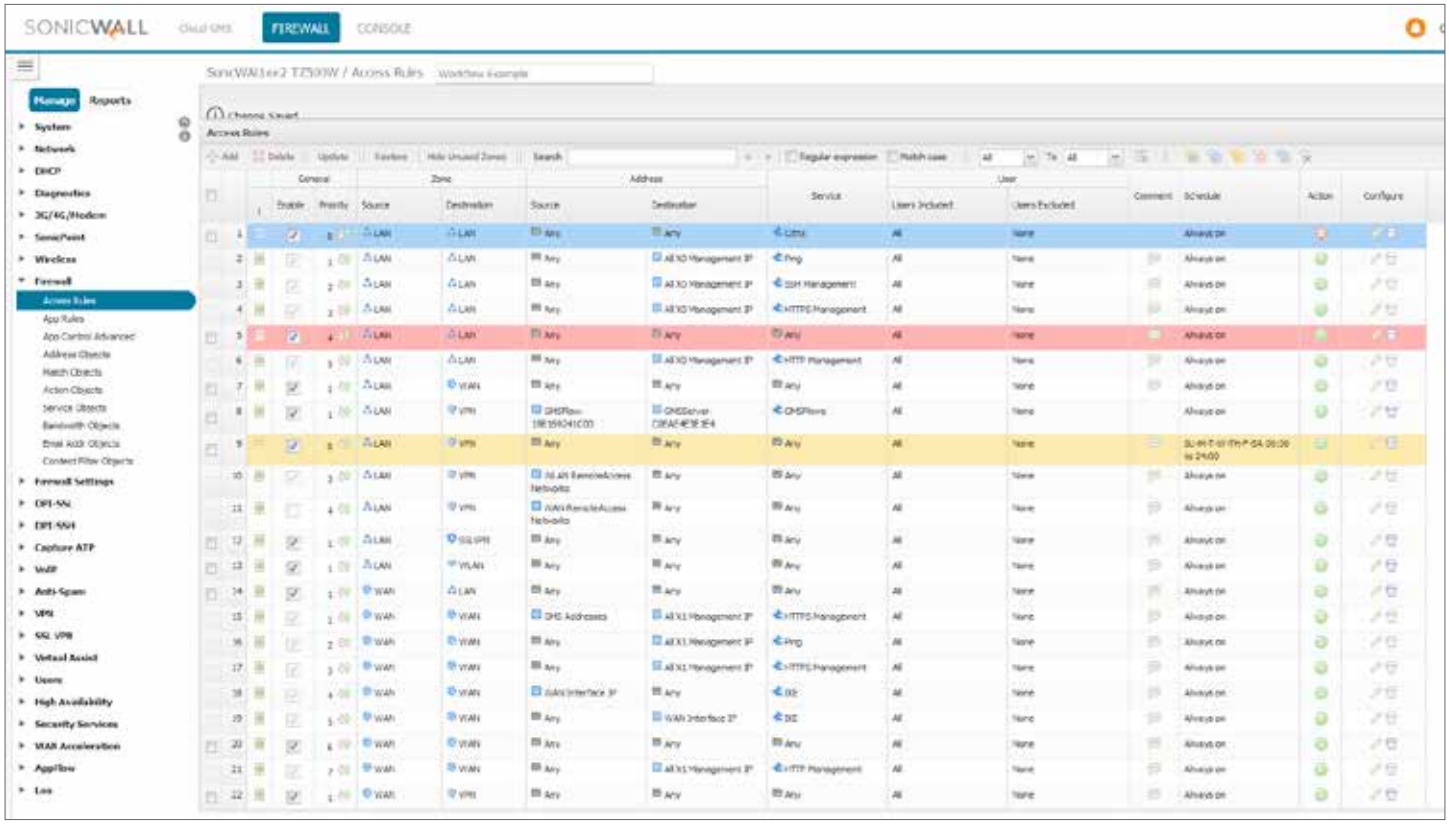
4. IMPLEMENTAZIONE

GMS implementa le modifiche alle policy immediatamente o **in modo pianificato**

5. CONTROLLO

I registri dei cambiamenti consentono un **controllo** accurato delle policy e dati di **conformità** esatti

Automazione dei flussi di lavoro GMS: cinque passi per una perfetta gestione delle policy



SONICWALL

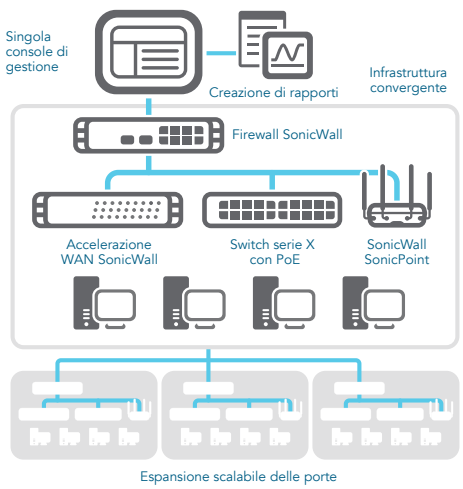
Funzionalità di monitoraggio e gestione della sicurezza	
Funzionalità	Descrizione
Gestione centralizzata della sicurezza e della rete	Aiuta gli amministratori a implementare, gestire e monitorare un ambiente di rete distribuito.
Configurazione di policy federate	Semplice configurazione delle policy per migliaia di firewall SonicWall, punti di accesso wireless, dispositivi di sicurezza e-mail e accesso remoto sicuro e switch da una postazione centralizzata.
Gestione degli ordini di modifica e flusso di lavoro	La correttezza e la conformità delle modifiche alle policy vengono garantite mediante un processo di configurazione, comparazione, convalida, revisione e approvazione delle policy prima della loro implementazione. I gruppi di approvazione sono configurabili dagli utenti per assicurare la conformità alle policy di sicurezza aziendale. Tutte le modifiche alle policy vengono registrate in un formato verificabile, garantendo così la conformità del firewall ai requisiti normativi. Tutti i dettagli granulari di ogni modifica effettuata sono registrati in ordine cronologico per facilitare il rispetto della conformità, gli audit trail e la risoluzione di problemi.
Configurazione e implementazione VPN avanzate	Semplificano la creazione di connessioni VPN e consolidano migliaia di policy di sicurezza.
Gestione offline	Consente di pianificare le configurazioni e gli aggiornamenti del firmware per le appliance gestite, riducendo al minimo i tempi di fermo.
Gestione semplificata delle licenze	Semplifica la gestione delle appliance attraverso un'unica console e la gestione della protezione e dei servizi in abbonamento.
Dashboard universale	Widget personalizzabili, mappe geografiche e report basati sugli utenti.
Monitoraggio e notifica per i dispositivi attivi	Notifiche in tempo reale con funzioni di monitoraggio integrate per semplificare la risoluzione dei problemi e consentire agli amministratori di adottare misure preventive e fornire rimedi immediati.
Supporto SNMP	Le notifiche trap avanzate in tempo reale per tutti i dispositivi e le applicazioni abilitati per TCP/IP (Transmission Control Protocol/Internet Protocol) e SNMP potenziano la risoluzione dei problemi grazie alla rapida identificazione e reazione agli eventi critici della rete.
Visualizzazione e intelligence delle applicazioni	Rapporti in tempo reale e storici sulle applicazioni in uso e sugli utenti che le utilizzano. I rapporti sono completamente personalizzabili con intuitive funzioni di filtraggio e drill-down.
Numerose opzioni di integrazione	Interfaccia di programmazione delle applicazioni (API) per i servizi Web, supporto per interfaccia a riga di comando (CLI) per la maggior parte delle funzioni e supporto per trap SNMP sia per aziende che per fornitori di servizi.
Gestione di switch Dell Networking serie X	Gli switch della serie X di Dell possono essere gestiti facilmente con i firewall delle serie TZ, NSA e SuperMassive, offrendo una gestione unificata dell'intera infrastruttura di sicurezza della rete.
Creazione di rapporti e analisi di sicurezza	
Funzionalità	Descrizione
Rapporti Botnet	Sono disponibili quattro tipi di rapporto (tentativi, obiettivi, iniziatori e cronologia), contenenti informazioni di contesto sui vettori di attacco come ID delle botnet, indirizzi IP, paesi, host, porte, interfacce, iniziatore/obiettivo, origine/destinazione e utente.
Rapporto GeoIP	Contiene informazioni sul traffico bloccato basate sul Paese di origine o di destinazione del traffico. Sono disponibili quattro tipi di rapporto (tentativi, obiettivi, iniziatori e cronologia), contenenti informazioni di contesto sui vettori di attacco come ID delle botnet, indirizzi IP, paesi, host, porte, interfacce, iniziatore/obiettivo, origine/destinazione e utente.
Rapporto sull'indirizzo MAC	Nella pagina del rapporto viene visualizzato l'indirizzo MAC (Media Access Control), oltre a informazioni specifiche del dispositivo (MAC dell'iniziatore e del risponditore). Sono disponibili cinque tipi di rapporto: • Utilizzo dati > Iniziatori • Utilizzo dati > Risponditori • Utilizzo dati > Dettagli • Attività utente > Dettagli • Attività Web > Iniziatori

Creazione di rapporti e analisi di sicurezza (continuazione)	
Funzionalità	Descrizione
Rapporto Capture ATP	Questo rapporto mostra informazioni dettagliate sul comportamento delle minacce per reagire a una minaccia o ad un'infezione.
Rapporti conformi a HIPPA, PCI e SOX	I modelli di report predefiniti, conformi ai requisiti PCI, HIPAA e SOX, consentono di soddisfare i controlli di conformità della sicurezza.
Rapporti su punti di accesso wireless non autorizzati	Visualizzazione di tutti i dispositivi wireless in uso e di comportamenti malevoli da connessioni di rete ad hoc o peer-to-peer tra gli host e associazioni accidentali per gli utenti che si collegano a reti vicine non autorizzate.
Analisi e rapporti sui flussi	La creazione di report sui flussi per l'analisi del traffico delle applicazioni e i dati di utilizzo tramite i protocolli IPFIX o NetFlow consente un monitoraggio in tempo reale e cronologico. Gli amministratori dispongono così di una potente interfaccia per monitorare visivamente la propria rete in tempo reale, con la capacità di identificare le applicazioni e i siti web che richiedono più larghezza di banda, visualizzare l'utilizzo delle applicazioni per ogni utente e anticipare gli attacchi e le minacce diretti alla rete. • Visualizzatore in tempo reale personalizzabile con funzioni drag-and-drop • Schermata con rapporti in tempo reale e filtraggio con un semplice clic • Dashboard sui flussi principali con pulsanti per la visualizzazione in base a categorie • Schermata con rapporti sui flussi, con cinque schede aggiuntive sugli attributi dei flussi • Schermata di analisi dei flussi con potenti funzioni di correlazione e pivoting • Visualizzatore di sessioni per analisi drill-down approfondite di singole sessioni e pacchetti.
Rapporti intelligenti e visualizzazione delle attività	Gestione completa e creazione di report grafici per i firewall, le soluzioni di sicurezza e-mail e i dispositivi di accesso mobile sicuro SonicWall. Offre maggiore visibilità sui trend di utilizzo e gli eventi relativi alla sicurezza, rafforzando l'immagine di brand per i fornitori di servizi.
Sistema di logging centralizzato	Un unico strumento centralizzato per consolidare gli eventi di sicurezza e i log di migliaia di appliance o effettuare analisi forensi della rete.
Rapporti in tempo reale o storici basati su syslog di nuova generazione	La rivoluzionaria architettura potenziata semplifica il laborioso processo di riepilogo dei dati, fornendo report quasi in tempo reale sui messaggi syslog in arrivo, con la possibilità di eseguire analisi drill-down dei dati e personalizzare ampiamente i report.
Rapporti pianificati universali	Creazione automatica di report pianificati per diverse appliance di vario tipo, che vengono poi inviati per e-mail a destinatari autorizzati.
Analisi del traffico delle applicazioni	Questa opzione offre all'azienda informazioni dettagliate sul traffico delle applicazioni, sull'uso della larghezza di banda e sulle minacce alla sicurezza, oltre a potenti funzioni di risoluzione dei problemi e analisi forense.

Architettura scalabile distribuita

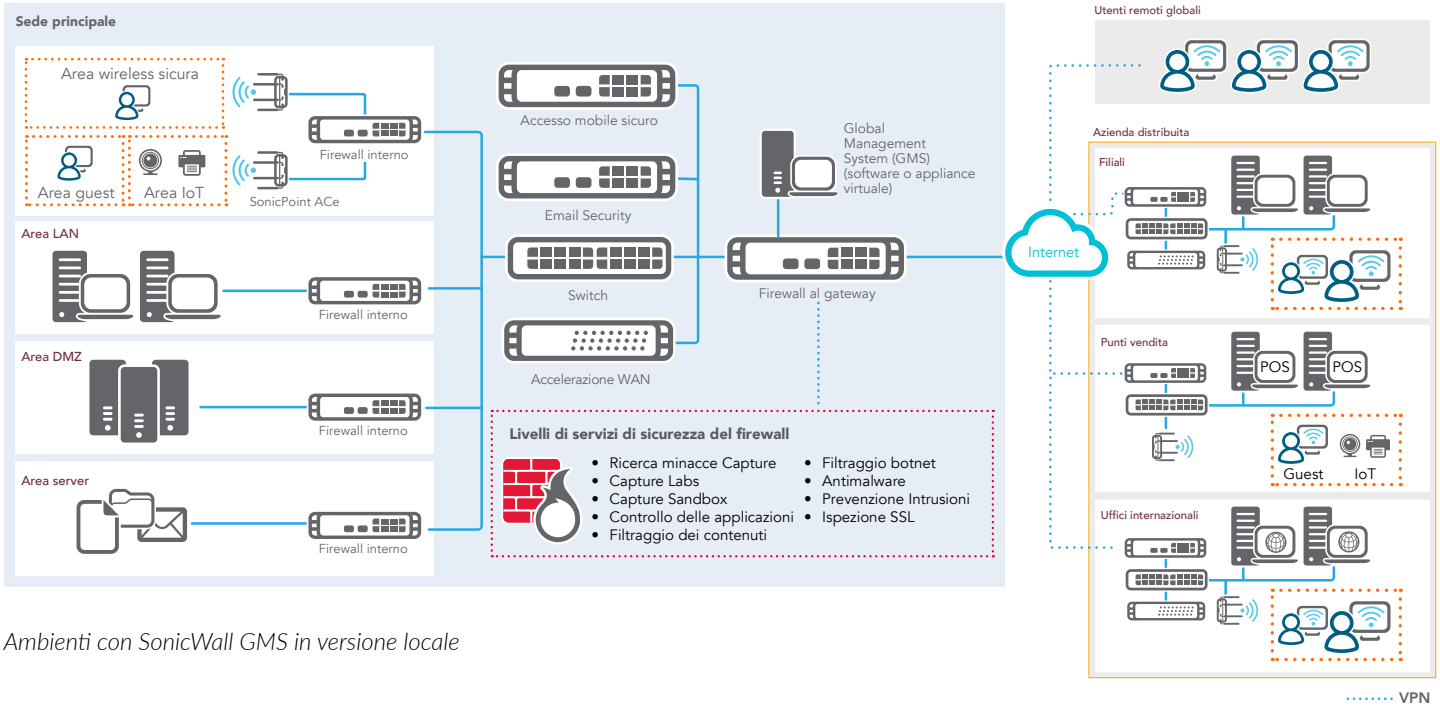
Il sistema GMS è basato su un'architettura distribuita che favorisce la scalabilità illimitata del sistema. Una singola istanza di GMS può fornire visibilità e controllo su migliaia di dispositivi di sicurezza gestiti della propria rete, a prescindere dalla loro posizione. A livello di esperienza utente, il dashboard universale di GMS utilizza un'interfaccia utente e principi di usabilità all'avanguardia che insieme garantiscono flussi di lavoro coerenti per tutti gli operatori nell'intero ecosistema di sicurezza.

GMS è una soluzione utilizzabile in locale come software o come appliance virtuale. In alternativa è disponibile SonicWall Cloud Global Management System (Cloud GMS), una piattaforma di reporting e gestione della sicurezza distribuita via cloud che accelera e semplifica le attività di gestione della sicurezza aumentando al contempo l'agilità dei servizi – il tutto a un basso costo di abbonamento.

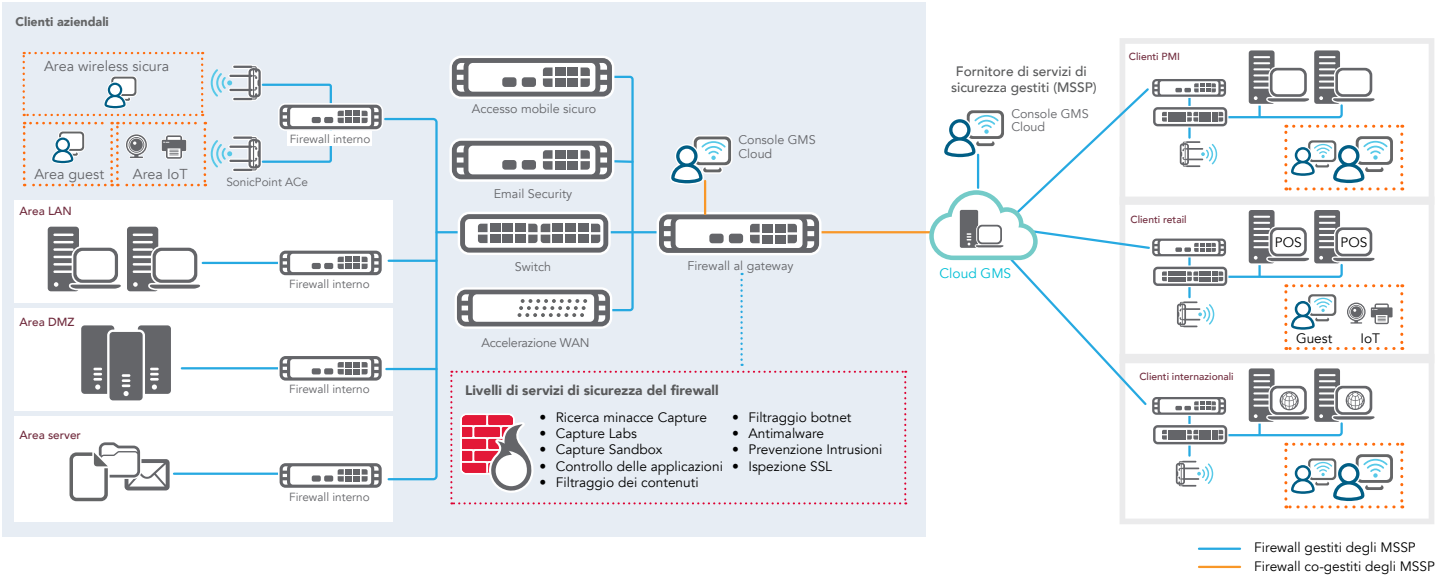


SonicWall Global Management System (GMS)

GMS in versione locale (on-premise) è una piattaforma di gestione, analisi e reporting completa e scalabile per imprese e data center distribuiti, mentre Cloud GMS è la soluzione ideale per fornitori di servizi (cioè MSP e MSSP).



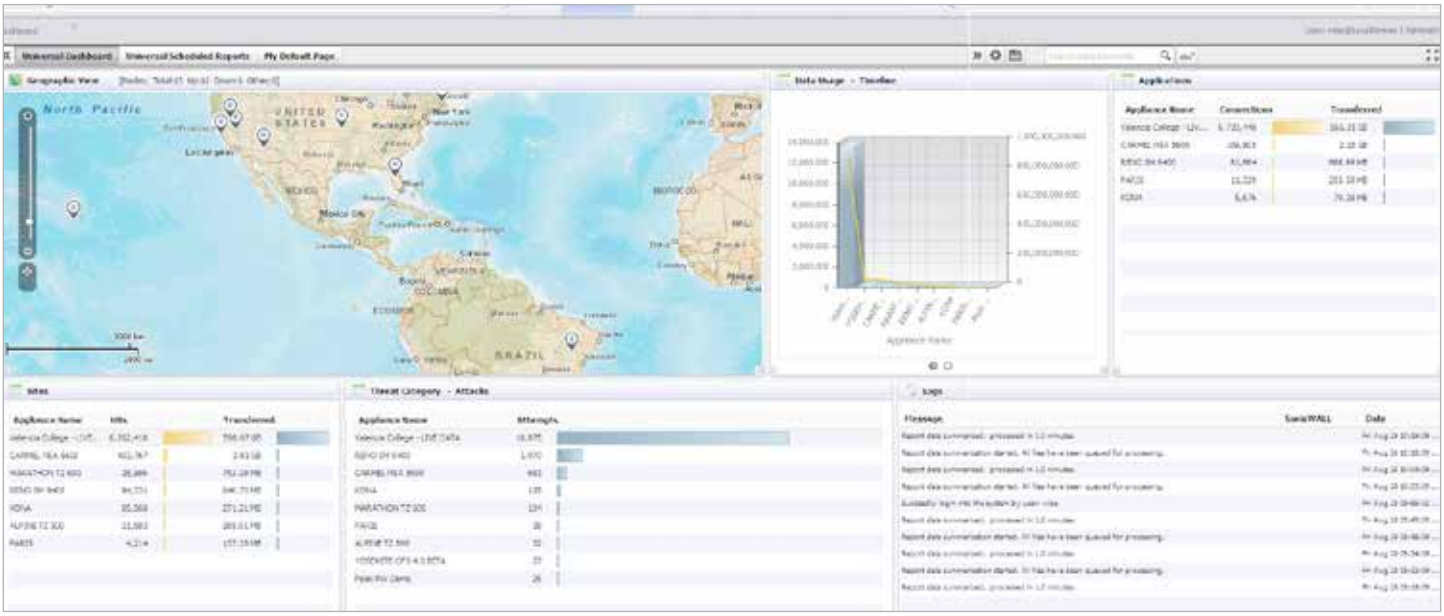
Ambienti con SonicWall GMS in versione locale



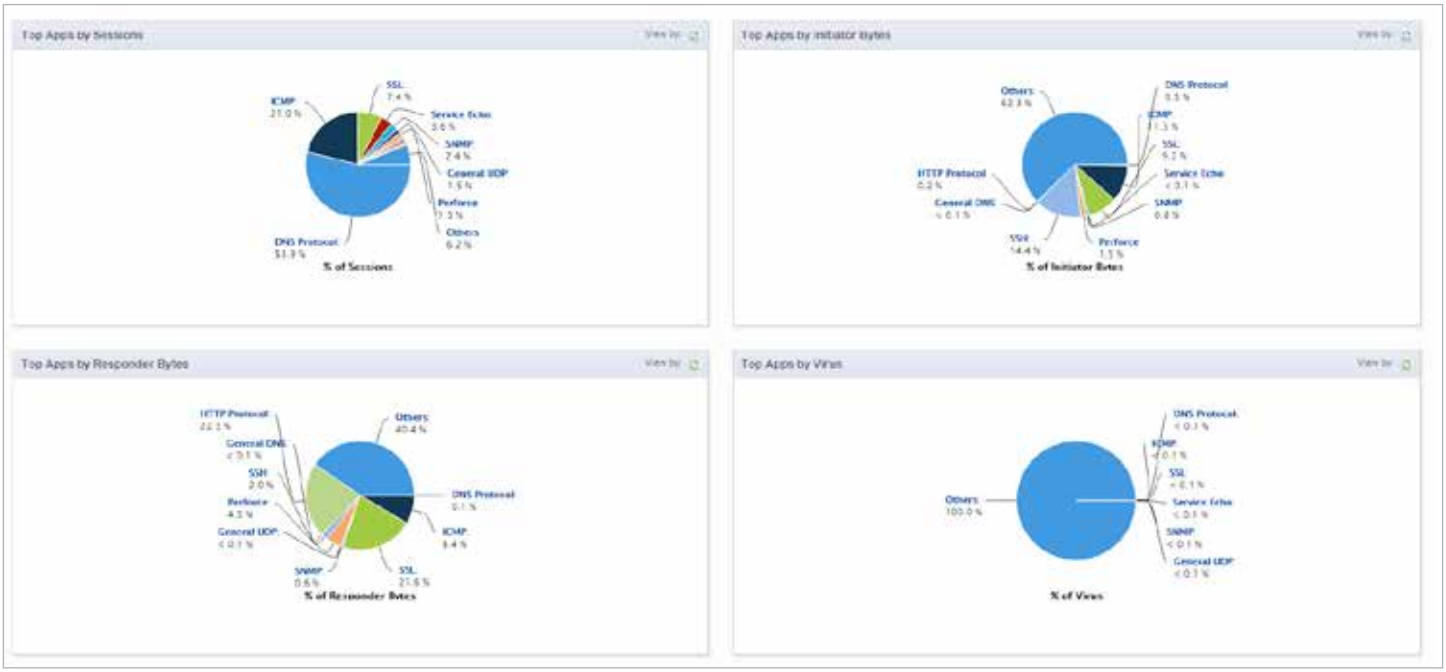
Ambienti con SonicWall GMS basato sul cloud

SONICWALL®

I dashboard sensibili al contesto visualizzano diversi widget informativi, come ad es. mappe geografiche, rapporti basati su syslog, riepiloghi della larghezza di banda, siti Web più visitati oppure i dati più rilevanti per determinati utenti.



Gli intuitivi report grafici semplificano il monitoraggio dei dispositivi gestiti. Eventuali anomalie del traffico sono facilmente rilevabili esaminando i dati di utilizzo in base a finestre di tempo, origini, destinazioni o servizi specifici. I report possono essere esportati in fogli di calcolo Microsoft® Excel®, in file PDF o direttamente verso una stampante.



SONICWALL®

S = standard
N = non disponibile

Riepilogo delle funzionalità			
Soluzione		GMS (On-Premise)	GMS (Cloud)
	Creazione di rapporti	S	S
	Gestione delle policy	S	S
	Monitoraggio	S	S
Opzioni di installazione			
	Installabile come appliance virtuale	S	Cloud
	Installabile come applicazione software	S	Cloud
	Installabile per la gestione e la creazione di rapporti in una rete IPv6	S	S
Creazione di rapporti			
	Ampia serie di rapporti grafici	S	S
	Creazione di rapporti sulla conformità	S	N
	Creazione di rapporti personalizzabili con funzioni drill-down	S	S
	Sistema di logging centralizzato	S	S
	Creazione di rapporti su minacce multiple	S	S
	Creazione di rapporti basati sugli utenti	S	S
	Creazione di rapporti sull'utilizzo delle applicazioni	S	S
	Nuovi strumenti di intelligence per gli attacchi	S	S
	Rapporto su larghezza di banda e servizi per ogni interfaccia	S	S
	Creazione di rapporti per firewall UTM SonicWall	S	S
	Creazione di rapporti per appliance VPN SSL SRA SonicWall	S	N
	Rapporti pianificati universali	S	N
	Creazione di rapporti di nuova generazione	Syslog e IPFIX	IPFIX
	Creazione di rapporti quasi in tempo reale flessibili e granulari	S	S
	Creazione di rapporti incentrati sull'utente	S	S
	Creazione di rapporti sulla larghezza di banda per utente	S	S
	Creazione di rapporti più granulari sui servizi	S	S
	Creazione di rapporti sull'attività VPN del client	S	N
	Riepilogo più dettagliato del report sui servizi tramite VPN	S	N
	Creazione di rapporti su su punti di accesso wireless non autorizzati	S	N
	Creazione di rapporti sui firewall per applicazioni Web (WAF) SRA per le PMI	S	N
Gestione			
	Accesso ubiquitario	S	S
	Avvisi e notifiche	S	S
	Strumenti di diagnostica	S	S
	Varie sessioni utente simultanee	S	S
	Gestione e pianificazione offline	S	S
	Gestione delle policy di sicurezza dei firewall	S	S
	Gestione delle policy di sicurezza VPN	S	S
	Gestione delle policy di sicurezza e-mail	S	N
	Gestione delle policy di accesso remoto sicuro/VPN SSL	S	N
	Gestione dei servizi di sicurezza a valore aggiunto	S	S

S = standard
N = non disponibile

Riepilogo delle funzionalità			
Soluzione		GMS (On-Premise)	GMS (Cloud)
Gestione (continuazione)			
	Definizione di modelli di policy a livello di gruppi	S	S
	Replica delle policy da un dispositivo a un gruppo di dispositivi	S	S
	Replica delle policy dal livello di gruppo a un singolo dispositivo	S	S
	Ridondanza ed elevata disponibilità	S	S
	Gestione del provisioning	S	S
	Architettura scalabile e distribuita	S	S
	Viste di gestione dinamica	S	S
	Gestione unificata delle licenze	S	S
	CLI (Command Line Interface)	S	N
	Interfaccia di programmazione delle applicazioni (API) per i servizi Web	S	N
	Gestione basata sui ruoli (utenti, gruppi)	S	S
	Dashboard universale	S	N
	Backup dei file di preferenze per le appliance firewall	S	S
Monitoraggio			
	Flussi di dati IPFIX in tempo reale	S	S
	Supporto SNMP	S	N
	Monitoraggio e avvisi per i dispositivi attivi	S	S
	Gestione relay SNMP	S	N
	Monitoraggio stato VPN e firewall	S	S
	Monitoraggio e avvisi syslog in tempo reale	S	N

Requisiti minimi di sistema

Di seguito sono riportati i requisiti minimi previsti per il sistema SonicWall GMS relativamente a sistema operativo, database, driver, hardware e appliance SonicWall supportate:

Sistema operativo[1]

Windows Server 2016

Windows Server 2012 standard a 64 bit

Windows Server 2012 R2 standard a 64 bit (versioni in lingua inglese e giapponese)

Windows Server 2012 R2 Datacenter

Requisiti hardware

Utilizzare il Calcolatore di capacità GMS per determinare i requisiti hardware per la propria implementazione.

Requisiti per l'appliance virtuale

Hypervisor: ESXi 6.5, 6.0 o 5.5

Utilizzare il Calcolatore di capacità GMS per determinare i requisiti hardware per la propria implementazione.

Guida alla compatibilità hardware per VMware:
http://www.vmware.com/resources/compatibility/search.php

Database supportati

Database esterni: Microsoft SQL Server 2012 e 2014

In bundle con l'applicazione GMS: MySQL

Browser

Microsoft® Internet Explorer 11.0 o superiore (non usare la modalità di compatibilità)

Mozilla Firefox 37.0 o superiore

Google Chrome 42.0 o superiore

Safari (versione più recente)

Gateway GMS

Serie SonicWall SuperMassive™ E10000, SonicWall SuperMassive™ 9000, E-Class Network Security Appliance (NSA) e NSA

Appliance SonicWall supportate e gestibili da GMS

Appliance di sicurezza di rete SonicWall: serie SuperMassive E10000 e 9000, E-Class NSA, NSA e TZ®

Appliance SonicWall Secure Mobile Access (SMA): serie SMA ed E-Class SRA

Appliance SonicWall Email Security

Tutti i dispositivi abilitati per TCP/IP e SNMP e applicazioni per il monitoraggio attivo

Informazioni per ordinare Global Management System (GMS)	
Prodotto	**SKU**
SNWL CLOUD GMS, GESTIONE, FLUSSI DI LAVORO E REPORTING, LIC. PER TZ (1 ANNO)	01-SSC-3435
SNWL CLOUD GMS, GESTIONE, FLUSSI DI LAVORO E REPORTING, LIC. PER NSA (1 ANNO)	01-SSC-3879
SNWL CLOUD GMS, GESTIONE E FLUSSI DI LAVORO, LIC. PER TZ/SOHO (1 ANNO)	01-SSC-3664
SNWL CLOUD GMS, GESTIONE E FLUSSI DI LAVORO, LIC. PER NSA (1 ANNO)	01-SSC-3665
SONICWALL GMS, LICENZA SOFTWARE, 5 NODI	01-SSC-7680
SONICWALL GMS, LICENZA SOFTWARE, 10 NODI	01-SSC-3363
SONICWALL GMS, LICENZA SOFTWARE, 25 NODI	01-SSC-3311
SONICWALL GMS, UPGRADE SOFTWARE, 1 NODO	01-SSC-7662
SONICWALL GMS, UPGRADE SOFTWARE, 5 NODI	01-SSC-3350
SONICWALL GMS, UPGRADE SOFTWARE, 10 NODI	01-SSC-7664
SONICWALL GMS, UPGRADE SOFTWARE, 25 NODI	01-SSC-3301
SONICWALL GMS, UPGRADE SOFTWARE, 100 NODI	01-SSC-3303
SONICWALL GMS, UPGRADE SOFTWARE, 250 NODI	01-SSC-3304
SONICWALL GMS, UPGRADE SOFTWARE, 1000 NODI	01-SSC-3306
SONICWALL GMS, GESTIONE MODIFICHE E FLUSSI DI LAVORO	01-SSC-0424
SONICWALL GMS, SUPPORTO SOFTWARE E-CLASS 24X7 PER 1 NODO (1 ANNO)	01-SSC-7675
SONICWALL GMS, SUPPORTO SOFTWARE E-CLASS 24X7 PER 5 NODI (1 ANNO)	01-SSC-6524
SONICWALL GMS, SUPPORTO SOFTWARE E-CLASS 24X7 PER 10 NODI (1 ANNO)	01-SSC-6514
SONICWALL GMS, SUPPORTO SOFTWARE E-CLASS 24X7 PER 25 NODI (1 ANNO)	01-SSC-3334
SONICWALL GMS, SUPPORTO SOFTWARE E-CLASS 24X7 PER 100 NODI (1 ANNO)	01-SSC-3336
SONICWALL GMS, SUPPORTO SOFTWARE E-CLASS 24X7 PER 250 NODI (1 ANNO)	01-SSC-3337
SONICWALL GMS, SUPPORTO SOFTWARE E-CLASS 24X7 PER 1000 NODI (1 ANNO)	01-SSC-3338

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.

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, CA 95054
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

DataSheet-SonicWallGlobalManagementSystem-US-VG-MKTG305