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.

SonicWall Global Management System (GMS) consente di risolvere tutte queste problematiche. GMS integra funzioni di gestione, monitoraggio, analisi anche forense e reporting 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 reporting
- 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
- Implementazione zero-touch per rendere operativi i firewall di uffici remoti e filiali in quattro semplici passaggi
- Provisioning, gestione e monitoraggio centralizzati per implementazione, connettività e prestazioni dell'SD-WAN
- Reporting 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

- Maggiore agilità per favorire la collaborazione, la comunicazione e il trasferimento di conoscenze all'interno dell'infrastruttura di sicurezza condivisa
- Decisioni informate sulle policy di sicurezza, basate su informazioni sulle minacce tempestive e consolidate, per un maggiore livello di efficienza della sicurezza

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

Automazione dei flussi di lavoro

Mediante l'automazione dei flussi di lavoro, GMS aiuta a conformare le attività di sicurezza ai requisiti di controllo e gestione delle modifiche delle policy dei firewall previsti da varie normative quali PCI, HIPAA e GDPR. Consente la modifica delle policy del firewall mediante una serie di rigorose procedure di configurazione, comparazione, convalida, revisione e approvazione delle policy prima della loro implementazione. I gruppi di approvazione sono flessibili per consentire la conformità alle varie procedure di autorizzazione e controllo previste da diversi tipi di organizzazioni. L'automazione dei flussi di lavoro applica in modo programmatico le policy di sicurezza approvate per migliorare l'efficienza operativa, ridurre al minimo i rischi ed eliminare gli errori.

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

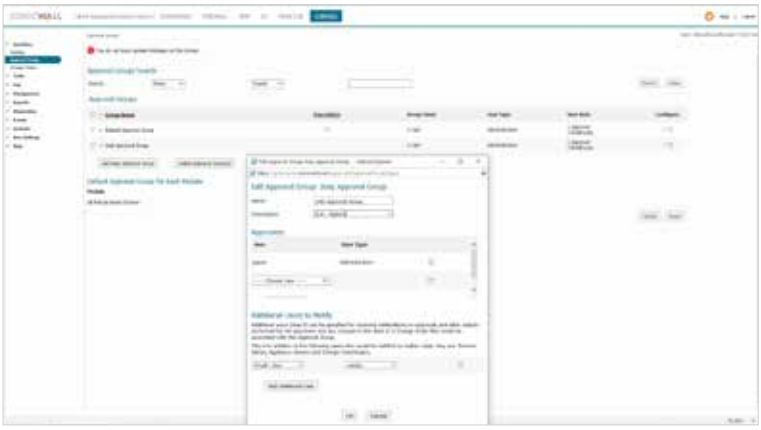
4. IMPLEMENTAZIONE

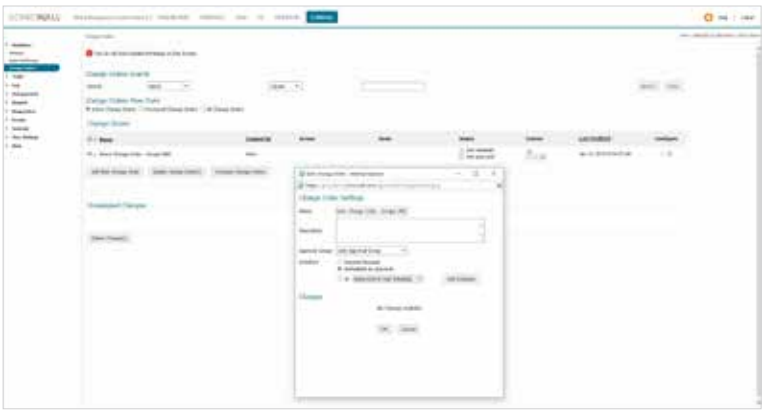
GMS implementa le modifiche alle policy immediatamente o **in modo pianificato**

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





Partner Enabled Services
Serve aiuto per pianificare, ottimizzare o implementare una soluzione SonicWall? Gli Advanced Services Partner di SonicWall sono qualificati per fornire servizi professionali di altissimo livello. Per maggiori informazioni: www.sonicwall.com/PES.

Implementazione zero-touch

GMS integra il servizio Zero-Touch Deployment, che semplifica e velocizza il processo di provisioning dei firewall SonicWall presso sedi remote e filiali. Il processo richiede un intervento minimo da parte dell'utente ed è completamente automatizzato per rendere operativi i firewall su vasta scala in quattro semplici passaggi. Ciò riduce significativamente il tempo, i costi e la complessità associati all'installazione e alla configurazione, mentre la protezione e la connettività vengono applicate in modo immediato e automatico.

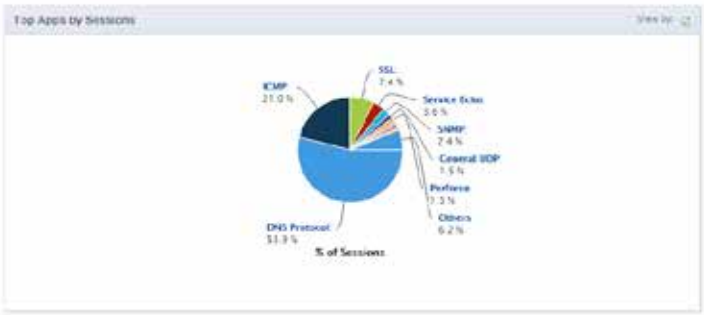
FASE 1	**REGISTRAZIONE DEL FIREWALL** Registrare il nuovo firewall in MySonicWall utilizzando il numero di serie e il codice di autenticazione assegnati.
FASE 2	**CONNESSIONE DEL FIREWALL** Collegare il firewall alla rete utilizzando il cavo Ethernet fornito in dotazione all'unità.
FASE 3	**ACCENSIONE DEL FIREWALL** Accendere il firewall dopo aver collegato il cavo di alimentazione e averlo inserito in una presa a muro standard. Alle unità viene automaticamente assegnato un IP WAN tramite il server DHCP. Una volta stabilità la connettività, l'unità viene automaticamente rilevata, autenticata e aggiunta al Capture Security Center e tutte le licenze e configurazioni vengono sincronizzate con MySonicWall e License Manager.
FASE 4	**GESTIONE DEL FIREWALL** L'unità è ora operativa e gestita tramite la console di gestione centrale basata su cloud di Capture Security Center, che si occupa degli aggiornamenti del firmware, delle patch di sicurezza e delle modifiche alla configurazione a livello di gruppo.

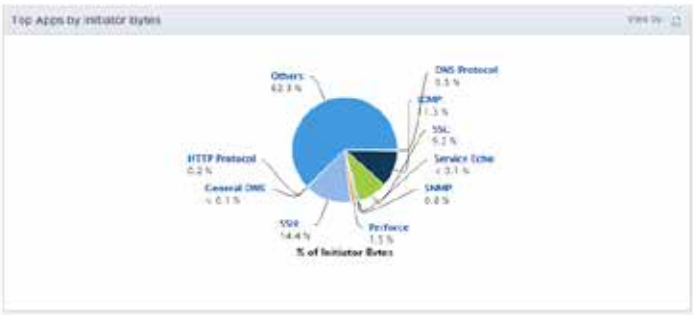
Implementazione zero-touch: quattro semplici passaggi per rendere operativo il firewall

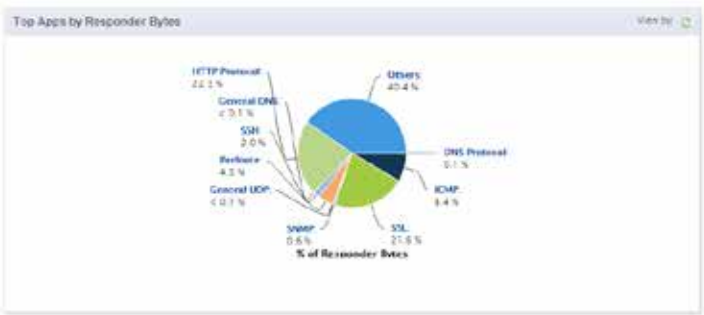
Reportistica

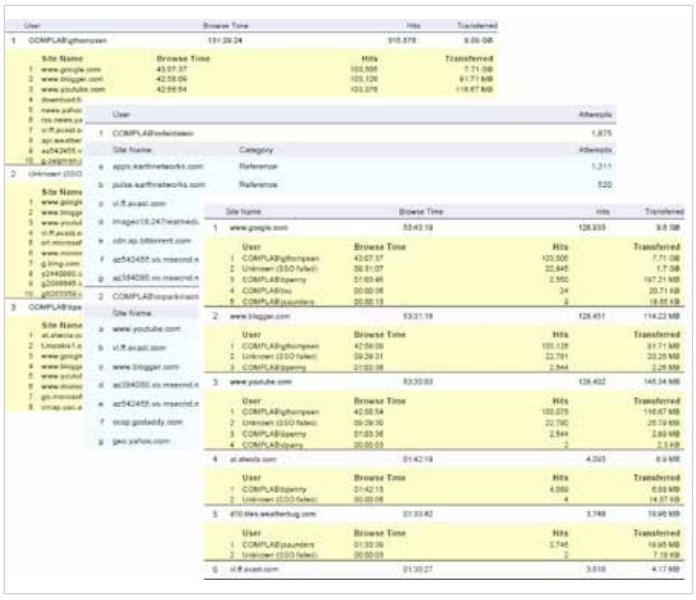
Capture Security Center offre più di 140 report predefiniti e la flessibilità di creare report personalizzati utilizzando una qualsiasi combinazione di dati verificabili per acquisire i risultati di vari casi d'uso. Questi risultati includono un quadro generale e informazioni dettagliate su eventi di rete, attività degli utenti, minacce, problemi operativi e a livello di performance, efficacia della sicurezza, rischi e lacune di sicurezza, preparazione alla conformità e analisi a posteriori. Ogni report è progettato sulla base degli input collettivi ricevuti da clienti e partner di SonicWall nell'arco di numerosi anni. Ciò fornisce maggiore granularità, contesto e conoscenza dei dati Syslog e IPFIX/NetFlow necessari per monitorare, misurare e garantire un funzionamento efficace della rete e delle misure di sicurezza.

Gli intuitivi report grafici semplificano il monitoraggio dei dispositivi gestiti. Gli amministratori possono facilmente rilevare eventuali anomalie del traffico esaminando i dati di utilizzo in base a finestre di tempo, origine, destinazione o servizi specifici. Inoltre possono esportare i report in fogli di calcolo Microsoft® Excel®, in file PDF o direttamente verso una stampante per le normali revisioni aziendali.









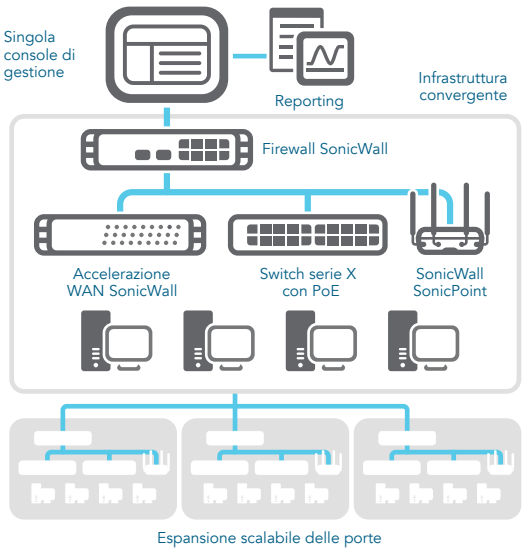
SONICWALL®

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 console 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.
Zero-Touch Deployment	Semplifica e velocizza l'implementazione e il provisioning dei firewall SonicWall in remoto attraverso il cloud. Distribuisce automaticamente le policy, esegue gli aggiornamenti del firmware e sincronizza le licenze.
Provisioning SD-WAN	Provisioning, gestione e monitoraggio semplici e centralizzati dell'implementazione e della connettività SD-WAN in ambienti aziendali distribuiti.
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	Report in tempo reale e storici sulle applicazioni in uso e sugli utenti che le utilizzano. I report 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.
Supporto di reti chiuse	GMS è installabile in ambienti chiusi, come le reti governative ad elevata protezione. Tutti le chiavi di licenza e i file con le firme dei servizi backend di SonicWall sono compressi, crittografati e trasferiti al file system locale, dove GMS può accedere, caricare e inviare gli aggiornamenti necessari a tutte le appliance di sicurezza gestite.
Reporting e analisi di sicurezza	
Funzionalità	Descrizione
Report Botnet	Sono disponibili quattro tipi di report (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.
Report GeoIP	Contiene informazioni sul traffico bloccato basate sul Paese di origine o di destinazione del traffico. Sono disponibili quattro tipi di report (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.

Reporting e analisi di sicurezza (continuazione)	
Funzionalità	Descrizione
Report sull'indirizzo MAC	Nella pagina del report 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 report: • Utilizzo dati > Iniziatori • Utilizzo dati > Risponditori • Utilizzo dati > Dettagli • Attività utente > Dettagli • Attività Web > Iniziatori
Report Capture ATP	Questo report mostra informazioni dettagliate sul comportamento delle minacce per reagire a una minaccia o ad un'infezione.
Report conformi a HIPAA, PCI e SOX	I modelli di report predefiniti, conformi ai requisiti PCI, HIPAA e SOX, consentono di soddisfare i controlli di conformità della sicurezza.
Reporting 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 report 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 con drag-and-drop personalizzabile • Schermata con report in tempo reale e filtraggio con un semplice clic • Dashboard sui flussi principali con pulsanti per la visualizzazione in base a categorie • Schermata con report 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.
Report 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.
Report 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.
Report 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.
Sicurezza dell'autenticazione	
Funzionalità	Descrizione
Blocco degli account	Il criterio di blocco degli account disabilita un account utente di GMS se vengono inserite password errate dopo un numero specificato di tentativi consentiti entro un periodo di tempo definito. Ciò impedisce ai criminali informatici di indovinare le password degli utenti e riduce la possibilità che un attacco riuscito possa ottenere l'accesso non autorizzato a risorse e dati protetti della rete.
Complessità delle password	Il criterio di complessità delle password stabilisce le linee guida minime ritenute importanti per creare una password efficace di login e accesso al sistema GMS.
Accesso amministrativo a intervalli di indirizzi specifici	I clienti hanno la possibilità di controllare l'accesso amministrativo a intervalli di indirizzi IP specifici.

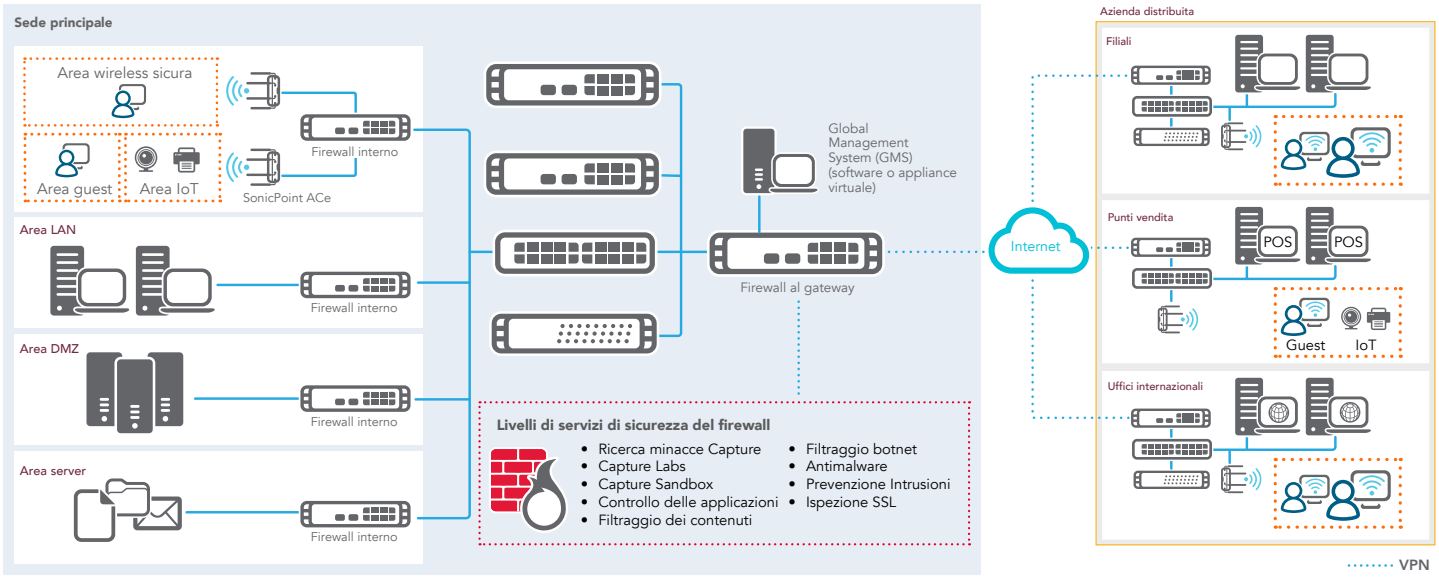
Architettura scalabile distribuita

GMS è una soluzione utilizzabile in locale come software o come appliance virtuale. Il sistema GMS è basato su un'architettura distribuita che favorisce la disponibilità e 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. Per il cliente ciò si traduce in dashboard universali altamente interattive con numerosi controlli in tempo reale, report e dati analitici per aiutarlo a prendere decisioni informate sulle politiche di sicurezza, favorendo la collaborazione, la comunicazione e il trasferimento di conoscenze nell'infrastruttura di sicurezza condivisa. Una visione globale dell'ambiente di sicurezza aziendale e la condivisione di informazioni sulla sicurezza in tempo reale con le persone giuste in azienda consentono di creare policy e controlli di sicurezza accurati, contribuendo così a realizzare una strategia di protezione più solida e adattiva.



SonicWall Global Management System (GMS)

GMS on-premise è una piattaforma di gestione, analisi e reportistica completa e scalabile per imprese e data center distribuiti.



Ambienti con SonicWall GMS in versione locale

SONICWALL®

Riepilogo delle funzionalità

Reporting

- Ampia serie di report grafici
- Reporting sulla conformità
- Reporting personalizzabili con funzioni drill-down
- Sistema di logging centralizzato
- Reporting su minacce multiple
- Reporting incentrati sull'utente
- Reporting sull'utilizzo delle applicazioni
- Reporting granulari sui servizi
- Nuovi strumenti di intelligence per gli attacchi
- Report su larghezza di banda e servizi per ogni interfaccia
- Reporting per le appliance SonicWall
- Reporting per appliance VPN SSL SRA SonicWall
- Report pianificati universali
- Reporting Syslog e IPFIX di nuova generazione
- Reporting quasi in tempo reale flessibili e granulari
- Reporting sulla larghezza di banda per utente
- Reporting sull'attività VPN del client
- Riepilogo dettagliato del report sui servizi tramite VPN
- Reporting su punti di accesso wireless non autorizzati
- Reporting sui firewall per applicazioni Web (WAF) SRA per le PMI

Gestione

- Accesso ubiquitario
- Avvisi e notifiche
- Strumenti di diagnostica
- Varie sessioni utente simultanee
- Gestione e pianificazione offline
- Gestione delle policy di sicurezza dei firewall
- Gestione delle policy di sicurezza VPN
- Gestione delle policy di sicurezza e-mail
- Gestione delle policy di accesso remoto sicuro/VPN SSL
- Gestione dei servizi di sicurezza a valore aggiunto
- Definizione di modelli di policy a livello di gruppi
- Replica delle policy da un dispositivo a un gruppo di dispositivi
- Replica delle policy dal livello di gruppo a un singolo dispositivo
- Ridondanza ed elevata disponibilità
- Gestione del provisioning
- Architettura scalabile e distribuita
- Viste di gestione dinamica
- Gestione unificata delle licenze
- CLI (Command Line Interface)
- Interfaccia di programmazione delle applicazioni (API) per i servizi Web
- Gestione basata sui ruoli (utenti, gruppi)
- Dashboard universale
- Backup dei file di preferenze per le appliance firewall
- SD-WAN
- Implementazione zero-touch
- Supporto di reti chiuse
- Supporto di firewall sandwich

Monitoraggio

Flussi di dati IPFIX in tempo reale

Supporto SNMP

Monitoraggio e avvisi per i dispositivi attivi

Gestione relay SNMP

Monitoraggio stato VPN e firewall

Monitoraggio e avvisi syslog in tempo reale

Sicurezza dell'autenticazione

Blocco degli account

Complessità delle password

Accesso amministrativo a intervalli di indirizzi specifici

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

- 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:
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)

Appliance SonicWall supportate e gestibili da GMS

- Appliance di sicurezza di rete SonicWall: serie SuperMassive E10000 e 9000, E-Class NSA, NSa e TZ Series
- Appliance di sicurezza di rete SonicWall virtuali: serie NSv
- Appliance SonicWall Secure Mobile Access (SMA): serie SMA ed E-Class SRA
- Appliance SonicWall Email Security
- Tutti i dispositivi basati su TCP/IP e SNMP e applicazioni per il monitoraggio attivo

Informazioni per ordinare Global Management System (GMS)	
Prodotto	SKU
SONICWALL GMS, LICENZA SOFTWARE, 5 NODI	01-SSC-3311
SONICWALL GMS, LICENZA SOFTWARE, 10 NODI	01-SSC-7662
SONICWALL GMS, LICENZA SOFTWARE, 25 NODI	01-SSC-3350
SONICWALL GMS, UPGRADE SOFTWARE, 1 NODO	01-SSC-7664
SONICWALL GMS, UPGRADE SOFTWARE, 5 NODI	01-SSC-3301
SONICWALL GMS, UPGRADE SOFTWARE, 10 NODI	01-SSC-3303
SONICWALL GMS, UPGRADE SOFTWARE, 25 NODI	01-SSC-3304
SONICWALL GMS, UPGRADE SOFTWARE, 100 NODI	01-SSC-3306
SONICWALL GMS, UPGRADE SOFTWARE, 250 NODI	01-SSC-0424
SONICWALL GMS, UPGRADE SOFTWARE, 1000 NODI	01-SSC-7675
SONICWALL GMS, GESTIONE MODIFICHE E FLUSSI DI LAVORO	01-SSC-6524
SONICWALL GMS, SUPPORTO SOFTWARE E-CLASS 24X7 PER 1 NODO (1 ANNO)	01-SSC-6514
SONICWALL GMS, SUPPORTO SOFTWARE E-CLASS 24X7 PER 5 NODI (1 ANNO)	01-SSC-3334
SONICWALL GMS, SUPPORTO SOFTWARE E-CLASS 24X7 PER 10 NODI (1 ANNO)	01-SSC-3336
SONICWALL GMS, SUPPORTO SOFTWARE E-CLASS 24X7 PER 25 NODI (1 ANNO)	01-SSC-3337
SONICWALL GMS, SUPPORTO SOFTWARE E-CLASS 24X7 PER 100 NODI (1 ANNO)	01-SSC-3338
SONICWALL GMS, SUPPORTO SOFTWARE E-CLASS 24X7 PER 250 NODI (1 ANNO)	01-SSC-6524
SONICWALL GMS, SUPPORTO SOFTWARE E-CLASS 24X7 PER 1000 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 27 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 rilevamento e prevenzione automatizzata delle violazioni in tempo reale ottimizzata per le esigenze specifiche di oltre 500.000 organizzazioni in più di 215 paesi e regioni, per consentire loro di fare più affari con maggior sicurezza. Per maggiori informazioni visita **www.sonicwall.com** o seguici su Twitter, LinkedIn, Facebook e Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

DataSheet-SonicWallGlobalManagementSystem-US-VG-MKTG4042