



- **Gestione centralizzata della sicurezza e delle policy**
- **Configurazione e deployment per reti VPN**
- **Monitoraggio attivo con allarme in tempo reale**
- **Logging centralizzato**
- **Implementazione come software, hardware o appliance virtuale**
- **Reporting intelligente e visualizzazione delle attività**
- **Gestione offline**
- **Gestione semplificata delle licenze**
- **Supporto SNMP**
- **Numerose opzioni d'integrazione**

SonicWALL® Global Management System (GMS) è uno strumento flessibile, potente e intuitivo che consente ad aziende di qualsiasi dimensione, ambienti distribuiti e service provider di gestire tutte le appliance SonicWALL da una postazione centrale, implementando con estrema rapidità le policy di sicurezza. SonicWALL GMS™ offre funzioni di monitoraggio centralizzato in tempo reale e report dettagliati sulle policy e sulla conformità alle normative.

L'intuitiva interfaccia utente basata sul Web di SonicWALL GMS consente di controllare il ciclo di vita completo di migliaia di appliance e servizi firewall, anti-spam, di accesso remoto sicuro e backup/ripristino di SonicWALL, dalla configurazione iniziale a complesse modifiche delle policy fino agli aggiornamenti remoti. Per le imprese, la possibilità di amministrare l'intera rete aziendale da un'unica interfaccia di gestione significa ridurre i tempi di amministrazione, le complessità d'uso e il costo totale di proprietà (TCO). I service provider possono beneficiare delle sue capacità di gestione multiaziendale per consolidare, raggruppare e classificare migliaia di appliance dei clienti e le relative policy di sicurezza. Grazie all'architettura di reporting integrata, gli amministratori possono personalizzare e pianificare i report in base alle esigenze specifiche di clienti gestiti o dirigenti o in conformità alle normative di sicurezza vigenti a livello dei singoli reparti aziendali. SonicWALL GMS può essere implementato con flessibilità come applicazione software su server Windows® di terzi, come appliance SonicWALL E-Class UMA (Universal Management Appliance) o come appliance virtuale di SonicWALL GMS in un ambiente VMware®.

Caratteristiche e vantaggi

Gestione centralizzata della sicurezza e delle policy tramite uno strumento flessibile, potente e intuitivo che consente di gestire e monitorare ambienti di rete distribuiti e impostare policy da una postazione centrale. Gli amministratori possono così creare, distribuire e applicare svariate policy di servizio e di sicurezza per migliaia di appliance firewall, anti-spam, di accesso remoto sicuro e backup/ripristino di SonicWALL.

Le sofisticate funzionalità di **configurazione e deployment per reti VPN** consentono alle aziende distribuite di ridurre il carico di lavoro, i costi e le complessità normalmente associate alla creazione e manutenzione di policy aziendali, connettività VPN e configurazione della rete. I service provider possono consolidare e raggruppare le policy di sicurezza relative a migliaia di clienti, ottimizzando così il rispetto degli accordi sui livelli di servizio (SLA).

Il **monitoraggio attivo dei dispositivi con segnalazione di allarme in tempo reale** permette agli amministratori di adottare misure preventive e reagire immediatamente in caso di avaria delle unità.

Il **logging centralizzato** fornisce un quadro generale da cui è possibile consolidare gli eventi di sicurezza e i log di migliaia di appliance o effettuare analisi dettagliate sull'uso della rete.

Implementazione flessibile come **software** (installabile nell'infrastruttura esistente), **hardware** (utilizzando un'appliance con sistema operativo hardened ad alte prestazioni) o come **appliance virtuale** (sfruttando le risorse di calcolo condivise per ottimizzare l'utilizzo, semplificare la migrazione e ridurre i costi di capitale).

Il **reporting intelligente e la visualizzazione delle attività** forniscono una visione completa e report grafici su firewall SonicWALL, accesso remoto sicuro e dispositivi di backup e ripristino, offrendo una maggiore visibilità sui trend di utilizzo delle applicazioni e sugli eventi di sicurezza. Grazie ai report personalizzabili con il logo e i colori aziendali, le imprese possono rafforzare la propria immagine di brand presso utenti e clienti.

La **gestione offline** consente di effettuare le configurazioni pianificate e/o gli aggiornamenti del firmware per le appliance in modalità offline, riducendo al minimo i tempi di fermo per utenti e clienti.

La **gestione semplificata delle licenze** offre una console unica per archiviare, monitorare e aggiornare i dati di licenza delle appliance SonicWALL gestite, semplificando la gestione della sicurezza e dei servizi in abbonamento.

Il **supporto SNMP** fornisce un potente meccanismo di allerta in tempo reale, per tutti i dispositivi basati su TCP/IP e SNMP, che permette di individuare e risolvere prontamente gli eventi critici della rete.

Le **numerose opzioni d'integrazione** includono un'interfaccia di programmazione delle applicazioni (API) per i servizi Web, il supporto CLI per la maggior parte delle funzioni e il supporto per trap SNMP. I fornitori di servizi e le aziende possono utilizzare queste opzioni per integrare il GMS nel loro sistema di automazione, gestione e monitoraggio dei servizi professionali e in altri applicativi aziendali.

Specifiche tecniche



SonicWALL Global Management System

Soluzione completa di gestione della sicurezza per imprese e service provider

SonicWALL GMS Standard Edition

SonicWALL GMS, licenza software

per 10 nodi

01-SSC-3363

SonicWALL GMS, licenza software

per 25 nodi

01-SSC-3311

SonicWALL GMS, upgrade software

per 1 nodo

01-SSC-7662

SonicWALL GMS, upgrade software

per 5 nodi

01-SSC-3350

SonicWALL GMS, upgrade software

per 10 nodi

01-SSC-7664

SonicWALL GMS, upgrade software

per 25 nodi

01-SSC-3301

SonicWALL GMS, upgrade software

per 100 nodi

01-SSC-3303

SonicWALL GMS, upgrade software

per 250 nodi

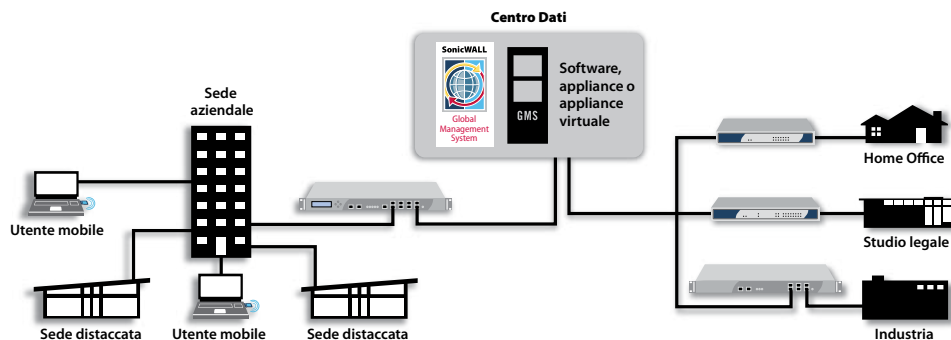
01-SSC-3304

SonicWALL GMS, upgrade software

per 1.000 nodi

01-SSC-3306

Per una panoramica dei prodotti supportati visitare il sito www.sonicwall.com/us/products/6030.html



SonicWALL GMS consente agli amministratori di creare con semplicità policy di sicurezza per le appliance SonicWALL e di applicarle a livello globale, individuale o di gruppo.



SonicWALL GMS permette di generare svariati report storici e informativi per offrire un quadro dei trend di utilizzo - ad es. per sapere quali siti Web sono stati visitati e da quali utenti - e degli eventi di sicurezza delle appliance SonicWALL gestite.



GMS Mobile è un'applicazione gratuita per iPhone utilizzabile dagli amministratori per connettersi in mobilità al proprio sistema GMS e ottenere una panoramica di tutti i dispositivi gestiti, controllare lo stato dei dispositivi e analizzare gli allarmi GMS in tempo reale.

Requisiti minimi di sistema

Di seguito sono riportati i requisiti minimi previsti per sistema operativo, database, driver e hardware, come pure le appliance SonicWALL supportate:

Sistema operativo

Windows Server 2003 a 32 e 64 bit (SP2), Windows Server 2008 SBS a 64 bit (R2), Windows Server 2008 Standard a 32 bit (SP2) e 64 bit (R2).

In tutti i casi descritti SonicWALL GMS funziona come applicazione a 32 bit.

Appliance virtuale

Hypervisor: VMware ESX e ESXi

Sistema operativo installato: SonicLinux hardened

Dimensioni appliance: 250 GB - 950 GB

Memoria allocata: 3 GB

Guida alla compatibilità hardware per VMware:

<http://www.vmware.com/resources/compatibility/search.php>

Hardware per impiego singolo

Ambiente x86: (minimo) processore server Intel con CPU dual-core da 3 GHz, 4 GB di RAM e 300 GB di spazio su disco

Hardware per impiego distribuito su server

Server GMS Ambiente x86: (minimo) processore Intel a CPU singola da 3 GHz, 2 GB di RAM e 300 GB di spazio su disco

Server database Ambiente x86: (minimo) processore Intel con CPU dual-core da 3 GHz, 2 GB di RAM e 300 GB di spazio su disco

Gateway GMS

Appliance SonicWALL delle serie E-Class NSA, NSA o PRO con versione firmware minima ed appliance di sicurezza basate su SonicWALL VPN¹

Database supportati

Database esterni: Microsoft SQL 2000 (SP4), Microsoft SQL 2005 a 32 e 64 bit (SP2), Microsoft SQL 2008 a 64 bit (R2)

In bundle con le applicazioni GMS: MySQL

Java

Plug-in Java, versione 1.6 o successiva

Appliance SonicWALL supportate e gestibili da GMS

Appliance di sicurezza SonicWALL: appliance delle serie E-Class NSA, NSA, PRO, TZ

Appliance SonicWALL Continuous Data Protection (CDP), SonicWALL Content Security Manager (CSM) e SonicWALL Secure Remote Access: SRA per le PMI ed E-Class SRA, appliance SonicWALL Email Security

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

Browser

Microsoft® Internet Explorer 6.0 o successivo

Mozilla Firefox 2.0 o successivo

Supportato solo sulle piattaforme Microsoft Windows

Firmware supportato

Appliance di sicurezza SonicWALL: E-Class NSA e NSA SonicOS Enhanced 5.0 o successivo

Appliance della serie SonicWALL PRO: SonicOS Enhanced 3.2 o successivo

Appliance della serie SonicWALL TZ: SonicOS Standard 3.1 o successivo e SonicOS Enhanced 3.2 o successivo

Appliance SonicWALL CDP: SonicWALL CDP 2.3 o successivo

Appliance SonicWALL CSM: SonicWALL 2.0 o successivo

Appliance SonicWALL SSL VPN: SonicWALL SRA per le PMI, firmware 2.0 o successivo, e SonicWALL Aventura E-Class SRA, firmware 9.0 o successivo

Appliance SonicWALL Email Security: firmware SonicWALL Email Security 7.0 o successivo

¹ Quando si utilizza l'opzione Management VPN Tunnel per la comunicazione sicura tra il server SonicWALL GMS e le appliance gestite tramite tunnel VPN, è necessario un gateway GMS. Il gateway GMS deve essere almeno un'appliance SonicWALL NSA (Network Security Appliance) con versione firmware min. SonicOS Enhanced 5.0 oppure un SonicWALL PRO 2040 con versione firmware min. SonicOS Enhanced 3.2. Il gateway GMS non è necessario se come metodo di gestione si utilizzano tunnel VPN esistenti o HTTPS.



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

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

