



SonicWALL Global Management System

GESTIONE BASATA SU POLICY

Soluzione di gestione e monitoraggio centralizzato della rete

- **Gestione centralizzata della sicurezza e delle policy**
- **Configurazione e deployment per reti VPN**
- **Monitoraggio attivo con allarme in tempo reale**
- **Logging centralizzato**
- **Reporting intelligente e visualizzazione delle attività**
- **Gestione offline**
- **Gestione semplificata delle licenze**
- **Supporto SNMP**

SonicWALL® Global Management System (GMS) è uno strumento flessibile, potente e intuitivo che consente ad aziende distribuite 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 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 multaziendale 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.

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 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 sul livello 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.

Il **reporting intelligente e la visualizzazione delle attività** forniscono una visione completa e report grafici sui dispositivi di sicurezza e sulle attività degli utenti, offrendo una maggiore visibilità sui trend di utilizzo 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.

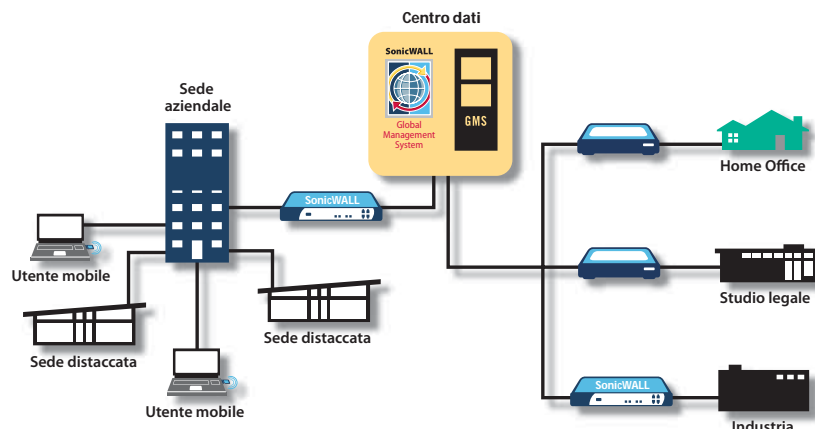
La **gestione semplificata delle licenze** offre una console unica per archiviare, monitorare e aggiornare i dati di licenza delle appliance SonicWALL gestite, semplificando la gestione della sicurezza e dei servizi in abbonamento.

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.

Specifiche tecniche

SonicWALL Global Management System

Soluzione completa di gestione della sicurezza per imprese e service provider



SonicWALL GMS edizione Standard Software (licenza 10 nodi)
01-SSC-3363
SonicWALL GMS edizione Standard Software (licenza 25 nodi)
01-SSC-3311
SonicWALL Comprehensive GMS Supporto base 8x5 (10 nodi)
01-SSC-3355
SonicWALL Comprehensive GMS Supporto base 8x5 (25 nodi)
01-SSC-3370
SonicWALL Comprehensive GMS Supporto base 24x7 (10 nodi)
01-SSC-3353
SonicWALL Comprehensive GMS Supporto base 24x7 (25 nodi)
01-SSC-3374



SonicWALL GMS consente agli amministratori di creare con semplicità policy di sicurezza per i dispositivi 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, come ad es. il controllo degli accessi ai siti web, e degli eventi di sicurezza delle appliance SonicWALL gestite.

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 2000 Server (SP4), Windows 2000 Professional (SP4), Windows XP Professional (SP2), Windows 2003 Server (SP1), Sun*: Solaris 8

Hardware per impiego singolo

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

Ambiente SPARC*: (minimo) processore UltraSPARC III da 1,593 GHz, memoria 2 GB e due drive da 146 GB

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
Ambiente SPARC*: (minimo) processore UltraSPARC III da 1,593 GHz, memoria 1 GB e due drive da 146 GB

Server database Ambiente x86: (minimo) processore Intel a doppia CPU da 3 GHz, 2 GB di RAM e 300 GB di spazio su disco
Ambiente SPARC*: (minimo) processore UltraSPARC III da 1,593 GHz, memoria 2 GB e due drive da 146 GB

Gateway GMS

Appliance SonicWALL della serie PRO con versione firmware min. 6.3.1.2, SonicOS Standard 2.0 o SonicOS Enhanced 2.0 e appliance di sicurezza SonicWALL per la sicurezza della rete basate su VPN¹

Database

Ambiente Microsoft*: Microsoft SQL Server 2000 (SP4) e Microsoft SQL Server 2005 (SP1) su Windows 2000 Server (SP4) o 2003 Server (SP1)

Ambiente Oracle*: Oracle 9.2.0.1 edizioni Standard ed Enterprise su Windows XP Professional (SP2), Windows 2000 Server (SP4), Windows 2003 Server (SP1) o Solaris 8

Java

Driver Java Database Connectivity (JDBC) - compatibilità JDBC 2.0 tipo 3 o 4,² Plug-in Java, versione 1.5 o successiva

Appliance SonicWALL supportate e gestibili da GMS

Appliance di sicurezza SonicWALL serie TZ e serie PRO³, appliance SonicWALL CSM e SonicWALL SSL-VPN

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

Browser

Microsoft* Internet Explorer 6.0
Mozilla Firefox 1.5 o successiva

Firmware supportato

Appliance di sicurezza SonicWALL: firmware SonicWALL 6.1.2.0 o successiva, SonicOS Standard 1.0 o successiva, SonicOS Enhanced 2.0 o successiva.

Appliance SonicWALL CSM: SonicWALL 1.0 o successiva

Appliance SonicWALL SSL-VPN: firmware SonicWALL SSL-VPN 1.5.0.3 o successiva

¹ Il gateway GMS deve disporre come minimo di un'appliance di sicurezza SonicWALL PRO 2040 o superiore.

² Il driver JDBC viene installato da GMS solo per SQL-Server. I prodotti Oracle vengono forniti con il driver JDBC. Prestare particolare attenzione durante l'installazione del database Oracle.

³ I modelli legacy SonicWALL XPRS/XPRS2, SonicWALL SOHO2, SonicWALL Tele2 e SonicWALL Pro/Pro-VX non sono supportati.

Italia / Supporto

Numero verde: 800.909.106

Telefono: +31 (0) 411.617.814

E-mail: sales_support-europe@sonicwall.com

Italia / U ci

Telefono: +39.333.273.55.18

E-mail: italy@sonicwall.com

