SONICWALL

SONICWALL GLOBAL MANAGEMENT SYSTEM

Umfassendes Sicherheitsmanagement, Monitoring und Reporting sowie umfangreiche Analysen

Eine effiziente Sicherheitsmanagementstrategie setzt ein tiefes Verständnis der Sicherheitsumgebung voraus, um Regeln besser koordinieren und die Entscheidungsfindung optimieren zu können. Organisationen, die keine unternehmensweite Perspektive über ihr Sicherheitskonzept haben, laufen oft Gefahr, Opfer von vermeidbaren Cyberangriffen und Compliance-Verstößen zu werden. Berichtsdaten in unterschiedlichen Formaten sowie die Nutzung unterschiedlicher Tools auf verschiedenen Plattformen machen Sicherheitsanalysen und das Reporting aus operativer Sicht ineffizient. Für Organisationen ist es so noch schwerer, Sicherheitsrisiken schnell zu erkennen und darauf zu reagieren. Um diese Probleme zu lösen, ist ein systematischer Ansatz für die Verwaltung der Netzwerksicherheit gefragt.

Genau hier kommt das SonicWall Global Management System (GMS) ins Spiel. GMS integriert Verwaltung und Überwachung, Analysen, Forensikfunktionen und Audit-Reporting und bildet so die Grundlage für eine effiziente Security-Governance-, Compliance- und Risikomanagementstrategie. Die funktionsreiche GMS-Plattform bietet verteilten Unternehmen, Serviceprovidern und anderen Organisationen einen reibungslosen, ganzheitlichen Ansatz, um alle betrieblichen Aspekte ihrer Sicherheitsumgebung zusammenzuführen. Mit GMS können Sicherheitsteams denkbar einfach die Firewalls, drahtlosen Access-Points und Lösungen für E-Mail-Sicherheit und einen sicheren mobilen Zugriff von SonicWall sowie Netzwerk-Switches anderer Anbieter verwalten. Das alles erfolgt über einen verwalteten und prüffähigen Workstream-Prozess, um alle Sicherheits-, Compliance- und Verfügbarkeitsanforderungen des Netzwerks sicherzustellen. Unter anderem bietet GMS zentralisierte Richtlinienverwaltung und -durchsetzung, Echtzeit-Ereignisüberwachung, granulare Datenanalysen und Berichte sowie Audit-Trails über eine einheitliche Verwaltungsplattform.

Vorteile:

- Einrichtung eines einheitlichen Sicherheitsprogramms für Security-Governance, Compliance und Risikomanagement
- Einheitlicher und auditierbarer Ansatz für Sicherheitskoordination, forensische Funktionen, Analysen und Reporting
- Risikoreduzierung und schnelle Reaktion auf Sicherheitsvorfälle
- Unternehmensweite Sicht auf das Sicherheitsökosystem
- Automatisierung von Workflows und Einhaltung von Sicherheitsprozessen
- HIPAA-, SOX- und PCI-Berichte für interne und externe Auditoren
- Schnelle und einfache Implementierung als Software, virtuelle Appliance oder Cloud-Lösung – alle zu geringen Kosten

ZENTRALE VERWALTUNG

- Schaffen Sie eine einfache Lösung für umfassendes Sicherheitsmanagement, Analyseberichte und Compliance und vereinheitlichen Sie Ihr Netzwerksicherheitsprogramm.
- Sie können Workflows automatisieren und abgleichen, um eine komplett aufeinander abgestimmte Security-Governance-, Compliance- und Risikomanagementstrategie zu erstellen.

COMPLIANCE

- Regulierungsbehörden und Auditoren profitieren von automatischen PCI-, HIPAA- und SOX-Sicherheitsberichten.
- Sie können jegliche Kombination auditierbarer Netzwerksicherheitsdaten anpassen und sich so in Richtung spezifischer Compliance-Vorgaben entwickeln.

RISIKOMANAGEMENT

- Regulierungsbehörden und Auditoren profitieren von automatischen PCI-, HIPAA- und SOX-Sicherheitsberichten.
- Sie können jegliche Kombination auditierbarer Netzwerksicherheitsdaten anpassen und sich so in Richtung spezifischer Compliance-Vorgaben entwickeln.

GMS bietet einen ganzheitlichen Ansatz für Security-Governance, Compliance und Risikomanagement.

Mithilfe von Prozessen zur Workflow-Automatisierung können Unternehmen mit GMS zudem auch ihre Changemanagement-Anforderungen erfüllen. Durch das Workflow-Feature lässt sich ein strenger Prozess für die Konfiguration, den Vergleich, die Validierung, die Prüfung und die Genehmigung von Regeln vor der Implementierung durchsetzen. Auf diese Weise werden die Richtigkeit und Einhaltung von Regeländerungen sichergestellt. Die Freigabegruppen sind flexibel und erlauben die Einhaltung unternehmenseigener Sicherheitsregeln, während sie gleichzeitig Risiken und Fehler reduzieren, die Effizienz verbessern und hocheffektive Sicherheitsmechanismen ermöglichen. Mithilfe der GMS-Workflow-Automatisierung und Auditierung von Regeländerungen können Unternehmen geeignete Firewall-Regeln flexibel und zuversichtlich zur richtigen Zeit und in Übereinstimmung mit entsprechenden Compliance-Vorgaben implementieren.

GMS bietet einen ganzheitlichen Ansatz für Security-Governance, Compliance und Risikomanagement.

1. KONFIGURATION UND VERGLEICH

GMS konfiguriert **Anforderungen zur Regeländerung** und **markiert Abweichungen farblich** für einen klaren Vergleich.

2. VALIDIERUNG

GMS **prüft die Integrität der Regellogik**.

3. PRÜFUNG UND GENEHMIGUNG

GMS sendet eine E-Mail an Reviewer und **protokolliert den Audit-Trail (Genehmigung/ Ablehnung)** der Regel.

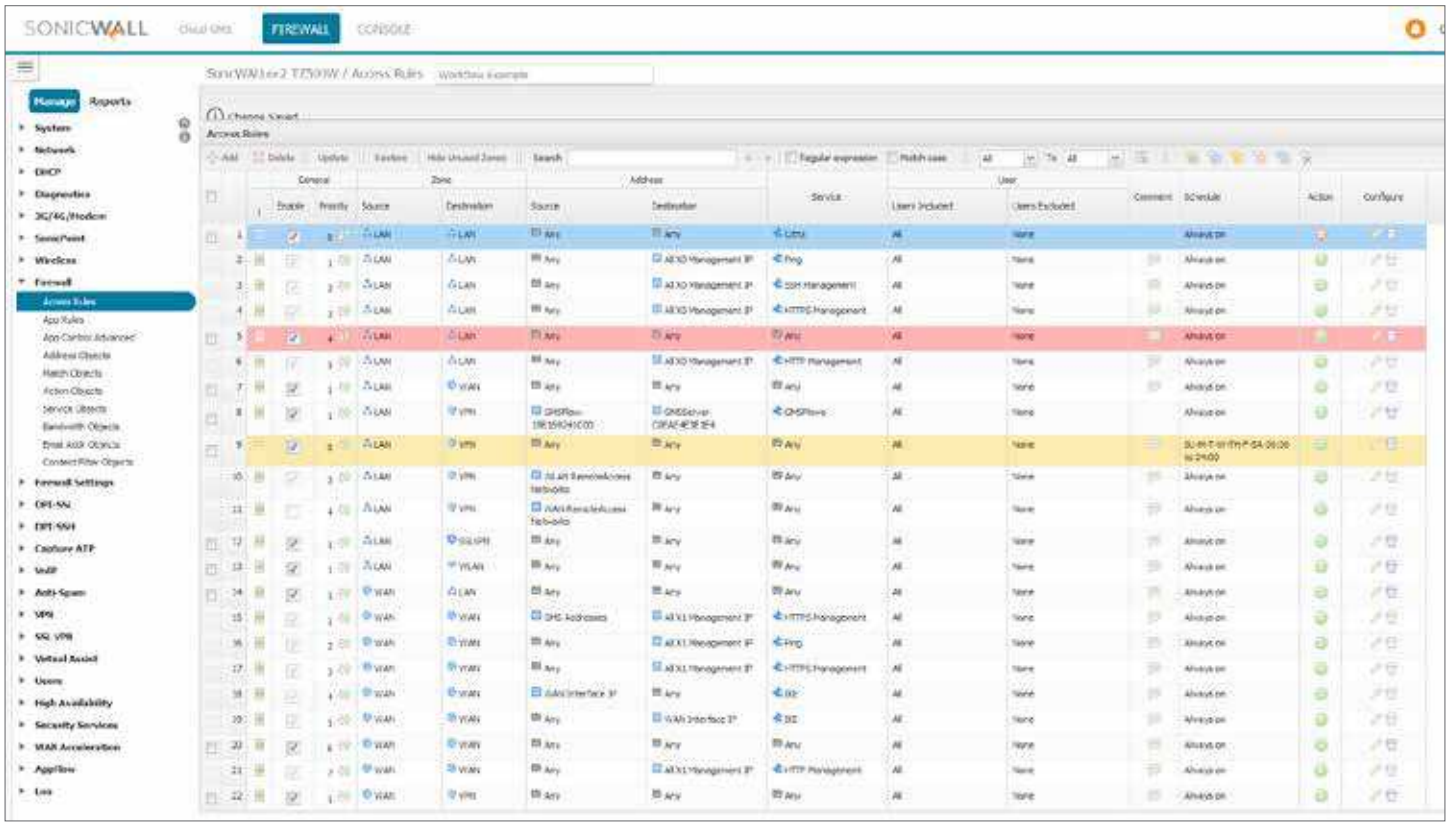
4. IMPLEMENTIERUNG

GMS implementiert die Regeländerungen sofort oder **nach einem festen Zeitplan**.

5. AUDIT

Die Änderungsprotokolle ermöglichen eine genaue **Prüfung** der Regeln und akkurate **Compliance**-Daten.

GMS-Workflow-Automatisierung: fünf Schritte für eine fehlerfreie Regelverwaltung



SONICWALL

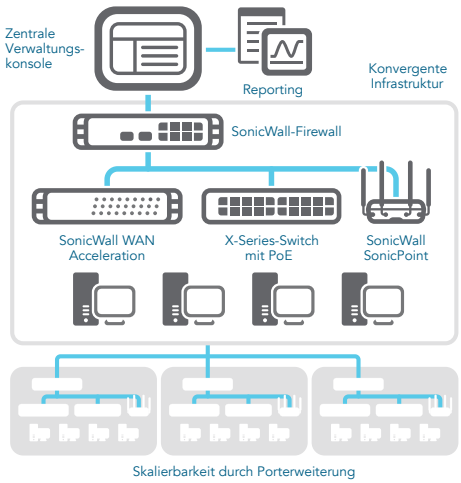
Sicherheitsmanagement- und Überwachungsfeatures	
Funktion	Beschreibung
Zentrales Sicherheits- und Netzwerkmanagement	Unterstützt Administratoren bei der Implementierung, Verwaltung und Überwachung einer verteilten Netzwerksicherheitsumgebung.
Föderierte Regelkonfiguration	Einfache, zentrale Regeldefinition für Tausende SonicWall-Firewalls, drahtlose Access-Points, E-Mail-Sicherheitsfunktionen, Secure-Remote-Access-Geräte und Switches.
Change-Order-Management und Workflow	Durch dieses Feature lässt sich ein Prozess für die Konfiguration, den Vergleich, die Validierung, die Prüfung und die Genehmigung von Regeln vor der Implementierung durchsetzen. Auf diese Weise werden die Richtigkeit und Einhaltung von Regeländerungen sichergestellt. Die Freigabegruppen lassen sich benutzerdefiniert konfigurieren, um die Einhaltung unternehmenseigener Sicherheitsregeln zu gewährleisten. Alle Regeländerungen sind in einer nachprüfbaren Form protokolliert, um sicherzustellen, dass die Firewall gesetzliche Vorgaben erfüllt. Sämtliche granularen Details zu allen Änderungen werden chronologisch gespeichert und helfen bei der Compliance, beim Audit-Trailing und bei der Fehlerbehebung.
Effiziente VPN-Implementierung und -Konfiguration	Vereinfacht die Bereitstellung von VPN-Konnektivität und konsolidiert Tausende von Sicherheitsregeln.
Offline-Management	Ermöglicht zeitgesteuerte Konfigurationsarbeiten und Firmware-Updates bei verwalteten Appliances, um Ausfallzeiten zu reduzieren.
Effiziente Lizenzverwaltung	Vereinfacht die Appliance-Verwaltung über eine einheitliche Konsole sowie die Verwaltung von Security- und Support-Lizenz-Subskriptionen.
Umfassendes Dashboard	Das Dashboard umfasst personalisierbare Widgets, geografische Karten und benutzerorientierte Reporting-Funktionen.
Aktive Überwachung von Geräten und Alarmierung	Echtzeit-Alarme mit integrierten Überwachungsfunktionen und einfache Troubleshooting-Prozesse ermöglichen es Administratoren, Präventivmaßnahmen zu ergreifen und eine umgehende Problembehebung zu veranlassen.
SNMP-Unterstützung	Bietet leistungsstarke Echtzeit-Traps für alle Transmission Control Protocol/Internet Protocol (TCP/IP)- und SNMP-fähigen Geräte und -Anwendungen. Damit lassen sich Fehler bei kritischen Ereignissen im Netzwerk schnell lokalisieren und beheben.
Anwendungsvisualisierung und Application-Intelligence	Historische und Echtzeitberichte zeigen, welche Anwendungen von welchen Usern genutzt werden. Die Berichte bieten intuitive Filter- und Drill-down-Funktionen und sind komplett personalisierbar.
Vielfältige Integrationsmöglichkeiten	API(Application Programming Interface)-Schnittstelle für Webservices, CLI(Command Line Interface)-Unterstützung für die meisten Funktionen und SNMP-Trap-Unterstützung für Serviceprovider und Unternehmen.
Verwaltung von Switches der Dell Networking X-Series	Die Switches der Dell X-Series lassen sich jetzt ganz unkompliziert mit TZ-, NSA- und SuperMassive-Firewalls verwalten. Dabei erfolgt die Verwaltung für die gesamte Netzwerksicherheitsinfrastruktur über eine einzige Konsole.
Sicherheitsberichte und -analysen	
Funktion	Beschreibung
Botnet-Bericht	Vier Berichtstypen: Versuche, Ziele, Initiatoren und Zeitverlauf. Sie enthalten Informationen zum Angriffsvektor wie etwa Botnet-ID, IP-Adressen, Länder, Hosts, Ports, Schnittstellen, Initiator/Ziel, Quelle/Ziel und Benutzer.
Geo-IP-Bericht	Bietet Informationen zum blockierten Datenverkehr basierend auf dem Herkunftsland oder dem Zielort des Datenverkehrs. Vier Berichtstypen: Versuche, Ziele, Initiatoren und Zeitverlauf. Sie enthalten Informationen zum Angriffsvektor wie etwa Botnet-ID, IP-Adressen, Länder, Hosts, Ports, Schnittstellen, Initiator/Ziel, Quelle/Ziel und Benutzer.
Bericht zur MAC-Adresse	Hier wird die Media Access Control (MAC)-Adresse auf der Berichtsseite angezeigt. Gerätespezifische Informationen (Initiator MAC und Responder MAC) werden in fünf Berichtstypen dargestellt: • Datennutzung > Initiatoren • Datennutzung > Responder • Datennutzung > Details • Benutzeraktivitäten > Details • Webaktivitäten > Initiatoren

Sicherheitsberichte und -analysen (Fortsetzung)	
Funktion	Beschreibung
Capture ATP-Bericht	Dank detaillierter Bedrohungsinformationen kann man gezielt auf eine Bedrohung oder Infizierung reagieren.
HIPPA-, PCI- und SOX-Berichte	Vordefinierte PCI-, HIPAA- und SOX-Berichtsvorlagen für Security-Compliance-Audits.
Berichte zu unberechtigten drahtlosen Access-Points	Die Berichte enthalten Informationen zu allen genutzten Drahtlosgeräten sowie zu unautorisiertem Verhalten aus Ad-hoc- oder Peer-to-Peer-Networking zwischen Hosts und zufälligen Verbindungen für Benutzer, die sich mit benachbarten unautorisierten Netzwerken verbinden.
Datenstromanalyse und -berichte	Datenstromberichts-Agent für Analyse- und Nutzungsdaten zum Anwendungsverkehr mittels IPFIX- oder NetFlow-Protokolle, um die Echtzeitüberwachung bzw. historische Überwachung zu ermöglichen. Bietet eine wirksame und effiziente Oberfläche für die visuelle Echtzeitüberwachung des Netzwerks. Administratoren können so Anwendungen und Websites mit hohem Bandbreitenbedarf identifizieren, die Anwendungsnutzung der jeweiligen User beobachten sowie Angriffe und Bedrohungen im Netzwerk antizipieren. • Ein Real-Time-Viewer mit Personalisierung mittels Drag-and-drop • Ein Real-Time-Report-Bildschirm inklusive Filterung mit nur einem Klick • Ein Top-Flows-Dashboard inklusive „Anzeige nach“-Schaltflächen mit nur einem Klick • Ein Flow-Reports-Bildschirm mit fünf zusätzlichen Tabs für Datenstromattribute • Ein Flow-Analytics-Bildschirm mit leistungsstarken Funktionen für Korrelation und Pivoting • Ein Session-Viewer für einen detaillierten Drill-down einzelner Sessions und Pakete
Intelligentes Reporting und Visualisierung der Benutzeraktivitäten	Umfassende Berichte mit grafischen Elementen für SonicWall-Firewalls sowie Email Security- und Secure Mobile Access-Geräte. Detaillierter Einblick in Nutzungstrends und Security-Events. Serviceprovider profitieren von einem einheitlichen Corporate Branding.
Zentrales Logging	Zentrale Konsolidierung von Security-Events und -Protokollen für Tausende von Appliances. So können von einem zentralen Punkt aus forensische Netzwerkanalysen durchgeführt werden.
Echtzeit- und historisches Next-Generation-Syslog-Reporting	Bahnbrechende Verbesserungen der Architektur verkürzen die zeitaufwendige Zusammenfassung, sodass Berichte über eingehende Syslog-Nachrichten nahezu in Echtzeit erstellt werden können. Außerdem lassen sich Daten per Drill-down aufschlüsseln und Berichte umfassend personalisieren.
Übergreifende zeitgesteuerte Berichte	Zeitliche Steuerung von Berichten, die automatisch erstellt und über mehrere Appliances unterschiedlichen Typs hinweg an autorisierte Empfänger per E-Mail versendet werden.
Analyse des Anwendungsverkehrs	Organisationen profitieren von aussagekräftigen Daten zum Anwendungsverkehr, zur Bandbreitennutzung und zu Sicherheitsbedrohungen. Gleichzeitig stehen leistungsstarke Troubleshooting- und Forensik-Funktionen zur Verfügung.

Skalierbare, verteilte Architektur

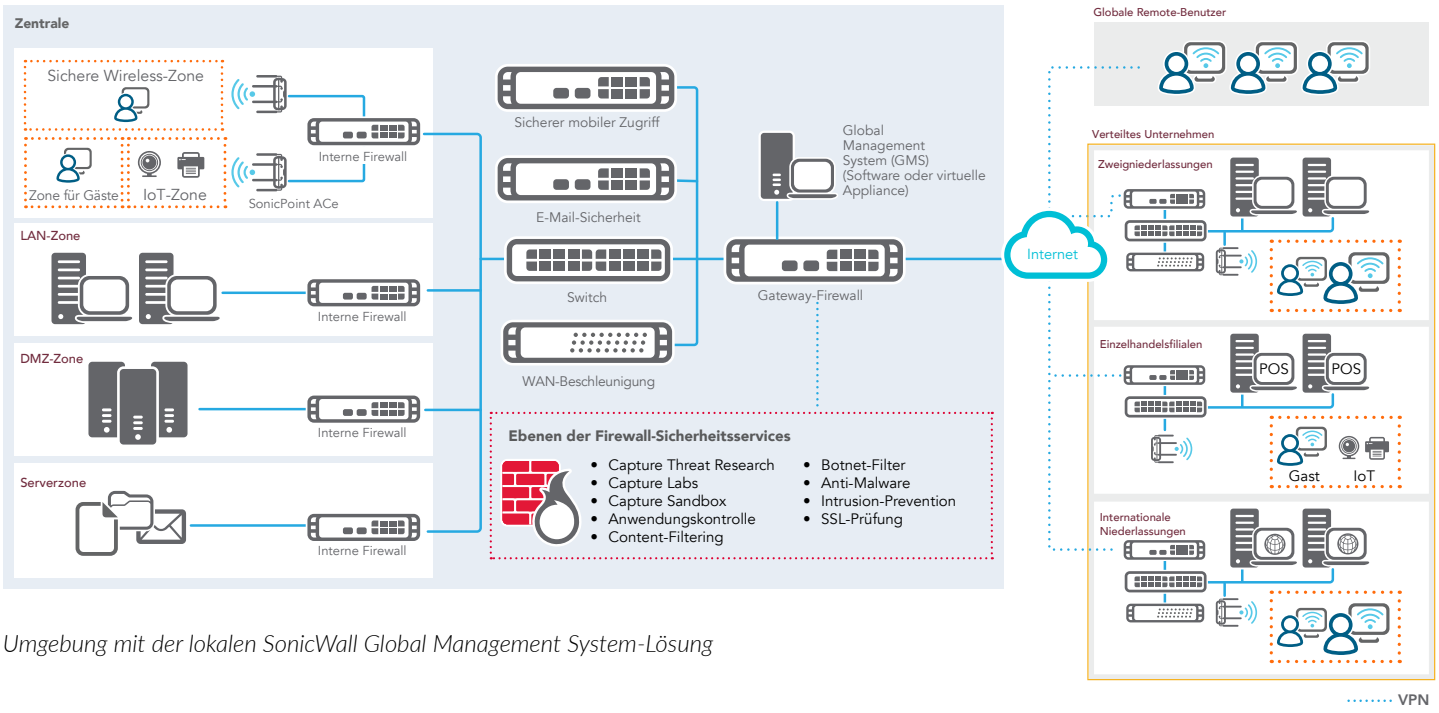
Herzstück von GMS ist eine verteilte Architektur, die eine endlose Systemskalierbarkeit ermöglicht. Eine einzige GMS-Instanz kann die Transparenz und Kontrolle über Tausende GMS-verwalteter Netzwerksicherheitsgeräte erhöhen – egal wo sich diese befinden. Aus Sicht der Benutzererfahrung bietet das universelle GMS-Dashboard modernste Design- und Nutzungskonzepte für die Benutzeroberfläche, die gemeinsam konsistente Workflows über das gesamte Sicherheitsökosystem hinweg ermöglichen.

GMS ist eine lokale Lösung, die sich als Software oder virtuelle Appliance implementieren lässt. Alternativ gibt es das SonicWall Cloud Global Management System (Cloud GMS), eine Cloud-basierte Security-Management- und Reporting-Plattform, die Prozesse rund um das Sicherheitsmanagement beschleunigt und vereinfacht und gleichzeitig die Flexibilität von Services verbessert – all das zu geringen Subskriptionskosten.

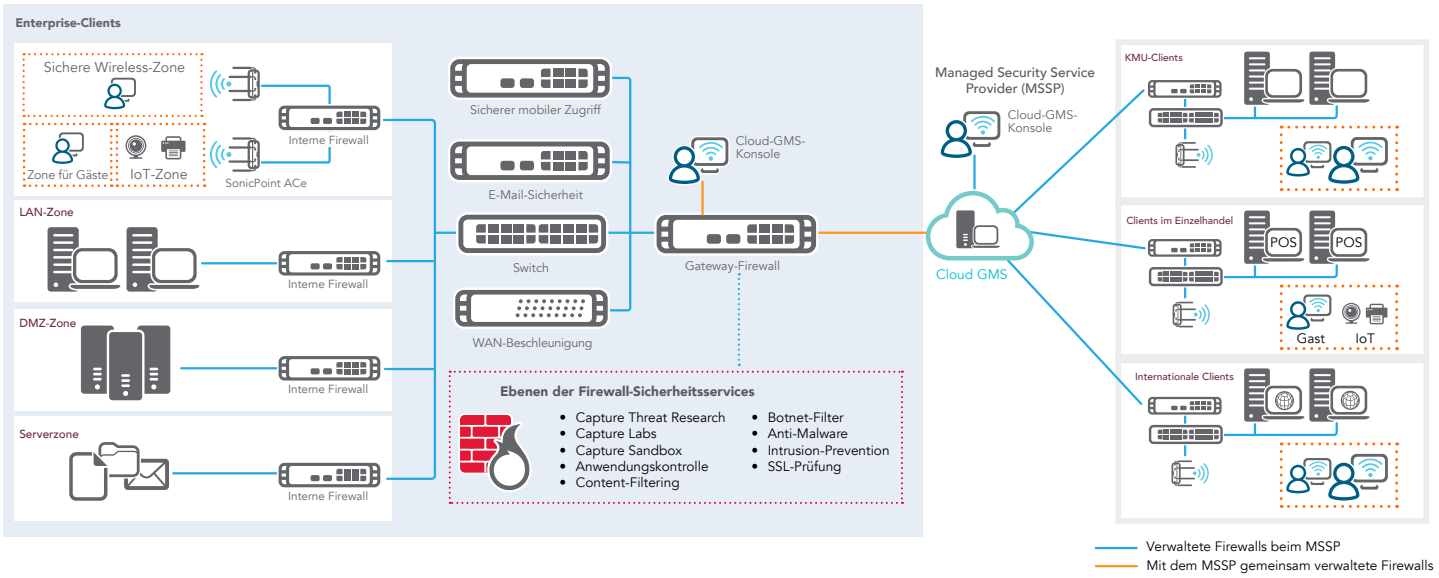


SonicWall Global Management System (GMS)

Die lokale GMS-Lösung bietet eine umfassende und skalierbare Security-Management-, Analyse- und Reporting-Plattform für verteilte Unternehmen und Datencenter, während sich Cloud GMS ideal für Serviceprovider (also MSPs und MSSPs) eignet.

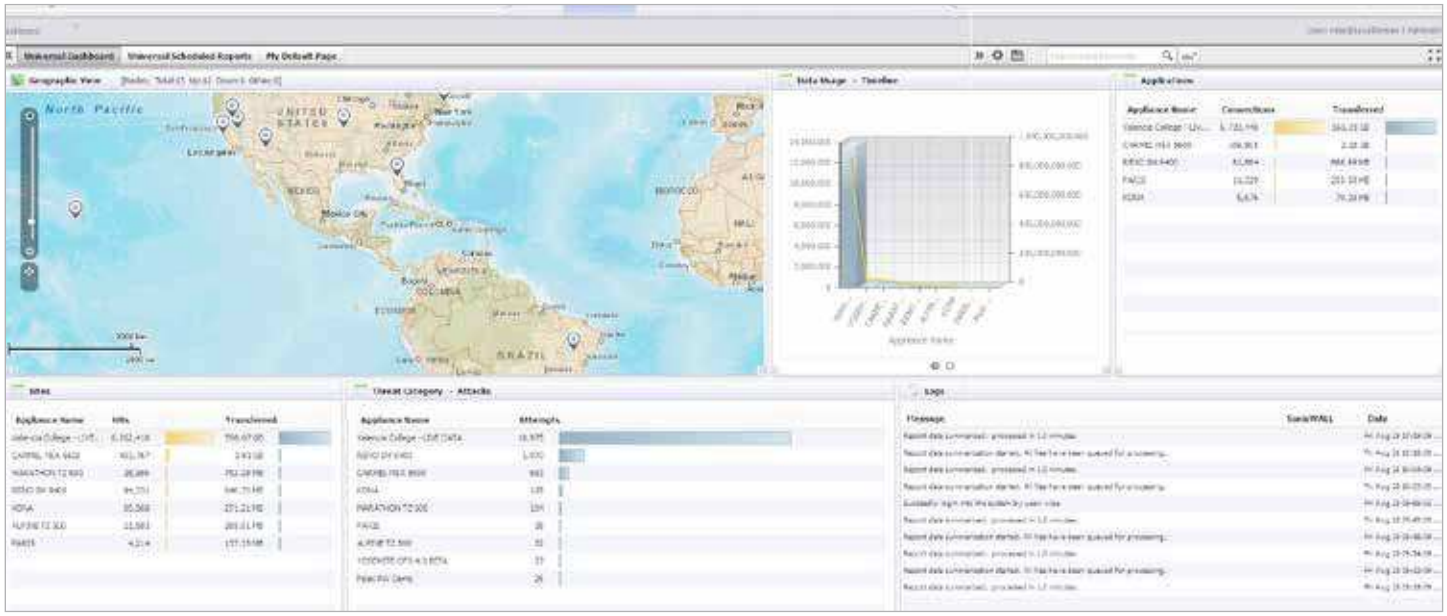


Umgebung mit der lokalen SonicWall Global Management System-Lösung

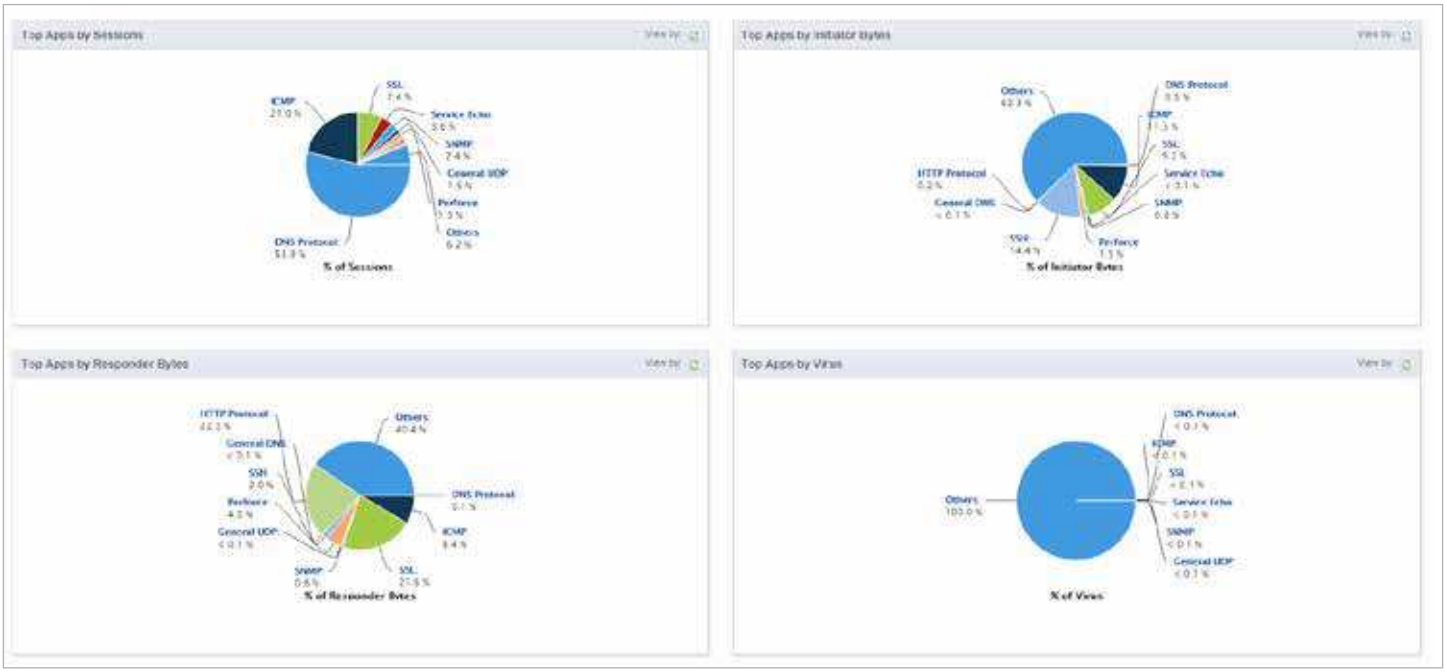


Umgebung mit der Cloud-basierten SonicWall Global Management System-Lösung

Kontextsensitive Dashboards bieten vielfältige informative Widgets, wie geografische Karten, Syslog-Berichte, Bandbreitenübersichten, Auflistungen der am häufigsten besuchten Websites oder der für bestimmte Benutzer relevantesten Daten.



Intuitive grafische Berichte vereinfachen die Überwachung verwalteter Appliances. Nutzungsdaten für einen bestimmten Zeitbereich, Initiator, Responder oder Service ermöglichen eine einfache Erkennung von Verkehrsanomalien. Sie können Berichte in ein Microsoft® Excel®-Spreadsheet oder in eine PDF-Datei exportieren oder direkt an einen Drucker weiterleiten.



S = Standard
N = Nicht verfügbar

Die Funktionen im Überblick			
Lösung		GMS (lokal)	GMS (Cloud)
	Reporting	S	S
	Regel-Verwaltung	S	S
	Überwachung	S	S
Implementierungsoptionen			
	Als virtuelle Appliance implementierbar	S	Cloud
	Als Softwareanwendung implementierbar	S	Cloud
	Zu Verwaltungs- und Reporting-Zwecken in einem IPv6-Netzwerk implementierbar	S	S
Reporting			
	Große Auswahl an grafischen Berichten	S	S
	Compliance-Reporting	S	N
	Personalisierbares Reporting mit Drill-down-Funktionen	S	S
	Zentrales Logging	S	S
	Sammelberichte zu verschiedenen Bedrohungen	S	S
	Benutzerbasiertes Reporting	S	S
	Berichte zur Anwendungsnutzung	S	S
	Neues Abwehrkonzept gegen Angriffe	S	S
	Bandbreiten- und Serviceberichte pro Schnittstelle	S	S
	Reporting für SonicWall-UTM-Firewall-Appliances	S	S
	Reporting für SonicWall-SRA-SSL-VPN-Appliances	S	N
	Universelle zeitgesteuerte Berichte	S	N
	Next-Generation-Berichtsfunktionen	Syslog und IPFIX	IPFIX
	Flexibles und granulares Reporting nahezu in Echtzeit	S	S
	Reporting zu Benutzern	S	S
	Reporting zur genutzten Bandbreite pro User	S	S
	Detailliertes Reporting zu Services	S	S
	Reporting zu Client-VPN-Aktivitäten	S	N
	Detailliertere Zusammenfassung der Services über VPN-Bericht	S	N
	Berichte zu unberechtigten drahtlosen Access-Points	S	N
	Reporting zur SRA SMB Web Application Firewall (WAF)	S	N
Verwaltung			
	Ortsunabhängiger Zugriff	S	S
	Warnmeldungen und Benachrichtigungen	S	S
	Diagnosetools	S	S
	Mehrere gleichzeitige Benutzersitzungen	S	S
	Offline-Management und Scheduling	S	S
	Verwaltung von Firewall-Sicherheitsregeln	S	S
	Verwaltung von VPN-Sicherheitsregeln	S	S
	Verwaltung von E-Mail-Sicherheitsregeln	S	N
	Verwaltung von SSL-VPN-Regeln und Regeln für einen sicheren Remote-Zugriff	S	N
	Verwaltung der Security-Mehrwertdienste	S	S

S = Standard
N = Nicht verfügbar

Die Funktionen im Überblick			
Lösung		GMS (lokal)	GMS (Cloud)
Verwaltung (Fortsetzung)			
	Definition von Regelvorlagen auf Gruppenebene	S	S
	Regelreplikation von einem Gerät auf eine Gerätegruppe	S	S
	Regelreplikation von der Gruppenebene auf ein einzelnes Gerät	S	S
	Redundanz und Hochverfügbarkeit	S	S
	Provisioning-Management	S	S
	Skalierbare und verteilte Architektur	S	S
	Dynamische Verwaltungssichten	S	S
	Einheitlicher Lizenzmanager	S	S
	Befehlszeilenschnittstelle (CLI)	S	N
	API (Application Programming Interface)-Schnittstelle für Webservices	S	N
	Rollenbasierte Verwaltung (Benutzer, Gruppen)	S	S
	Umfassendes Dashboard	S	N
	Back-up von Einstellungsdateien für Firewall-Appliances	S	S
Überwachung			
	IPFIX-Datenströme in Echtzeit	S	S
	SNMP-Unterstützung	S	N
	Aktive Überwachung von Geräten und Alarmierung	S	S
	SNMP-Relay-Verwaltung	S	N
	Überwachung des VPN- und Firewall-Status	S	S
	Live-Syslog-Überwachung und Warnmeldungen	S	N

Mindestsystemanforderungen

Nachfolgend sind die Mindestanforderungen für SonicWall GMS im Hinblick auf Betriebssystem, Datenbanken, Treibern, Hardware sowie die von SonicWall unterstützten Appliances aufgeführt:

Betriebssystem[1]

Windows Server 2016

Windows Server 2012 Standard 64 Bit

Windows Server 2012 R2 Standard 64 Bit (in englischer und japanischer Sprachfassung)

Windows Server 2012 R2 Datacenter

Hardwareanforderungen

Nutzen Sie den GMS Capacity Calculator, um die Hardwareanforderungen für Ihre Implementierung festzustellen.

Anforderungen an die virtuelle Appliance

Hypervisor: ESXi 6.5, 6.0 oder 5.5

Nutzen Sie den GMS Capacity Calculator, um die Hardwareanforderungen für Ihre Implementierung festzustellen.

VMware-Kompatibilitätsrichtlinien für Hardware:
http://www.vmware.com/resources/compatibility/search.php

Unterstützte Datenbanken

Externe Datenbanken: Microsoft SQL Server 2012 und 2014

In GMS-Anwendung integriert: MySQL

Internet-Browser

Microsoft® Internet Explorer 11.0 oder höher (nutzen Sie nicht den Kompatibilitätsmodus)

Mozilla Firefox 37.0 oder höher

Google Chrome 42.0 oder höher

Safari (neueste Version)

GMS-Gateway

SonicWall SuperMassive™ E10000 Series, SonicWall SuperMassive™ 9000 Series, E-Class Network Security Appliance (NSA) und NSA Series

Für die Verwaltung mit GMS unterstützte SonicWall Appliances

SonicWall-Netzwerksicherheitsappliances: Appliances der SuperMassive E10000 und 9000 Series sowie der E-Class NSA, NSA und TZ Series®

SonicWall Secure Mobile Access (SMA)-Appliances: SMA Series und E-Class SRA

SonicWall Email Security-Appliances

Alle TCP-/IP- und SNMP-fähigen Geräte und -Anwendungen für aktive Überwachung

Global Management System (GMS) – Bestellinformationen	
Produkt	**Artikelnummer**
SNWL CLOUD GMS MANAGEMENT WORKFLOW AND REPORTING-LIZENZ FÜR TZ (1 JAHR)	01-SSC-3435
SNWL CLOUD GMS MANAGEMENT WORKFLOW AND REPORTING-LIZENZ FÜR NSA (1 JAHR)	01-SSC-3879
SNWL CLOUD GMS MANAGEMENT AND WORKFLOW-LIZENZ FÜR TZ/SOHO (1 JAHR)	01-SSC-3664
SNWL CLOUD GMS MANAGEMENT AND WORKFLOW-LIZENZ FÜR NSA (1 JAHR)	01-SSC-3665
SONICWALL GMS SOFTWARE-LIZENZ (5 NODES)	01-SSC-7680
SONICWALL GMS SOFTWARE-LIZENZ (10 NODES)	01-SSC-3363
SONICWALL GMS SOFTWARE-LIZENZ (25 NODES)	01-SSC-3311
SONICWALL GMS SOFTWARE-UPGRADE (1 NODE)	01-SSC-7662
SONICWALL GMS SOFTWARE-UPGRADE (5 NODES)	01-SSC-3350
SONICWALL GMS SOFTWARE-UPGRADE (10 NODES)	01-SSC-7664
SONICWALL GMS SOFTWARE-UPGRADE (25 NODES)	01-SSC-3301
SONICWALL GMS SOFTWARE-UPGRADE (100 NODES)	01-SSC-3303
SONICWALL GMS SOFTWARE-UPGRADE (250 NODES)	01-SSC-3304
SONICWALL GMS SOFTWARE-UPGRADE (1000 NODES)	01-SSC-3306
SONICWALL GMS CHANGE MANAGEMENT AND WORKFLOW	01-SSC-0424
SONICWALL GMS E-CLASS 24/7-SOFTWARE-SUPPORT FÜR 1 NODE (1 JAHR)	01-SSC-7675
SONICWALL GMS E-CLASS 24/7-SOFTWARE-SUPPORT FÜR 5 NODES (1 JAHR)	01-SSC-6524
SONICWALL GMS E-CLASS 24/7-SOFTWARE-SUPPORT FÜR 10 NODES (1 JAHR)	01-SSC-6514
SONICWALL GMS E-CLASS 24/7-SOFTWARE-SUPPORT FÜR 25 NODES (1 JAHR)	01-SSC-3334
SONICWALL GMS E-CLASS 24/7-SOFTWARE-SUPPORT FÜR 100 NODES (1 JAHR)	01-SSC-3336
SONICWALL GMS E-CLASS 24/7-SOFTWARE-SUPPORT FÜR 250 NODES (1 JAHR)	01-SSC-3337
SONICWALL GMS E-CLASS 24/7-SOFTWARE-SUPPORT FÜR 1000 NODES (1 JAHR)	01-SSC-3338

Über uns

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 globalen Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

SonicWall, Inc.
5455 Great America Parkway | Santa Clara, Kalifornien 95054, USA
Weitere Information erhalten Sie auf unserer Website.
www.sonicwall.com

DataSheet-SonicWallGlobalManagementSystem-US-VG-MKTG305