SONICWALL GLOBAL MANAGEMENT SYSTEM

Umfassendes Sicherheitsmanagement, Monitoring und Reporting sowie umfangreiche Analysen

Eine effiziente Sicherheitsmanagement-strategie 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
- Operationalisierung von Firewalls an Remote-Standorten und Zweigniederlassungen in vier einfachen Schritten mit vollautomatischer Implementierung
- Zentrale Bereitstellung, Verwaltung und Überwachung der SD-WAN-Implementierung, -Konnektivität und -Performance
- HIPAA-, SOX- und PCI-Berichte für interne und externe Auditoren
- Schnelle und einfache Implementierung als Software, virtuelle Appliance oder Cloud-Lösung – jeweils 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

- Handeln Sie schnell, fördern Sie Zusammenarbeit und Kommunikation und sorgen Sie für eine bessere Verfügbarkeit von Wissen im gemeinsamen Sicherheitsframework.
- Treffen Sie fundierte Entscheidungen zu Sicherheitsregeln auf Basis zeitkritischer und konsolidierter Bedrohungsinformationen für eine effizientere Sicherheit.

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

Workflow-Automatisierung

Durch die native Workflow-Automatisierung hilft das GMS-System Organisationen dabei, die Anforderungen verschiedener gesetzlicher Vorgaben wie PCI, HIPPA und DSGVO an das Auditing und die Verwaltung von Regeländerungen an der Firewall einzuhalten. Es ermöglicht Regeländerungen durch den Einsatz konsequenter Verfahren beim Konfigurieren, Abgleichen, Validieren, Prüfen und Freigeben von Firewall-Regeln vor der Implementierung. Die Freigabegruppen sind flexibel und erlauben die Einhaltung verschiedener Autorisierungs- und Auditverfahren in unterschiedlichen Organisationen. Bei der Workflow-Automatisierung werden freigegebene Sicherheitsregeln programmseitig implementiert, um die operative Effizienz zu verbessern, Risiken zu mindern und Fehler zu vermeiden.

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.

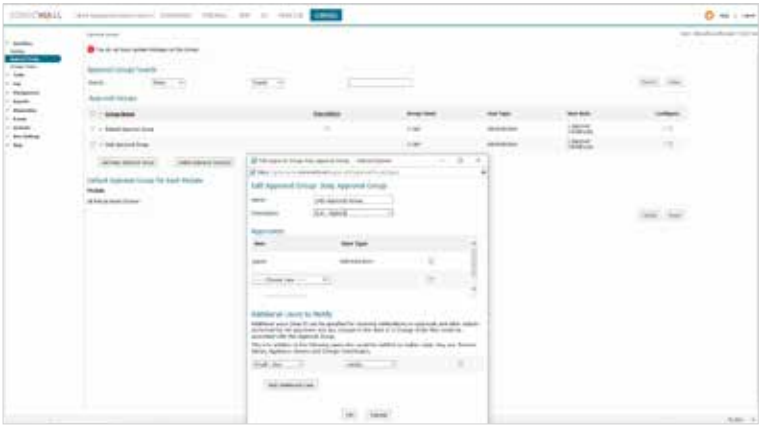
4. IMPLEMENTIERUNG

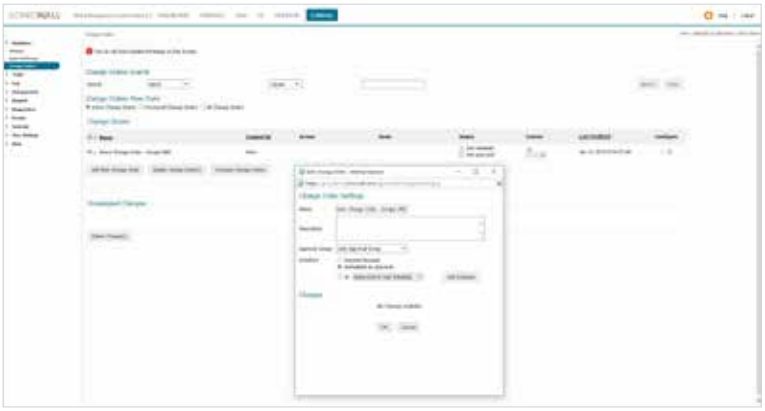
GMS implementiert die Regeländerungen sofort oder **nach einem festen Zeitplan**.

5. AUDIT

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

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





Partner Enabled Services
Brauchen Sie Hilfe bei der Planung, Implementierung oder Optimierung Ihrer SonicWall-Lösung? Unsere SonicWall Advanced Services Partner bieten Ihnen erstklassige Professional Services. Weitere Infos erhalten Sie unter www.sonicwall.com/PES.

Vollautomatische Implementierung

Die vollautomatische Implementierung ist als Service in GMS integriert und vereinfacht und beschleunigt den Bereitstellungsprozess für SonicWall-Firewalls in Niederlassungen und Remote-Standorten. Der Prozess erfordert einen minimalen Eingriff durch die Benutzer und ist vollständig automatisiert, sodass eine große Anzahl von Firewalls in vier einfachen Bereitstellungsschritten in Betrieb genommen werden kann. Dadurch werden Zeitaufwand, Kosten und Komplexität der Installation und Konfiguration erheblich reduziert, während Sicherheit und Konnektivität umgehend und automatisch gewährleistet sind.

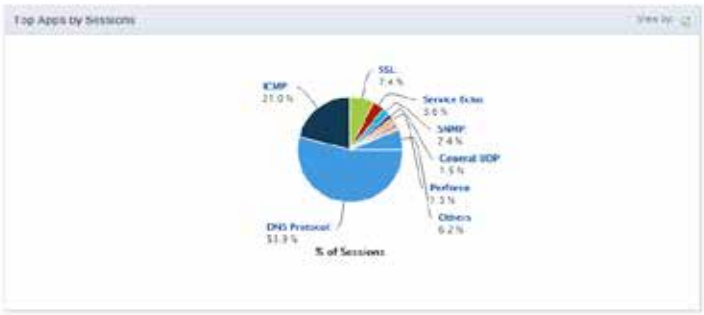
SCHRITT 1	**FIREWALL REGISTRIEREN** Die neue Firewall wird mit der zugewiesenen Seriennummer und dem Authentifizierungscode in MySonicWall registriert.
SCHRITT 2	**FIREWALL VERBINDEN** Die Firewall wird über das mitgelieferte Ethernetkabel mit dem Netzwerk verbunden.
SCHRITT 3	**FIREWALL EINSCHALTEN** Die Firewall wird mit dem Netzkabel an das Stromnetz angeschlossen und eingeschaltet. Das Gerät erhält eine vom DHCP-Server automatisch zugewiesene WAN-IP. Sobald die Verbindung hergestellt wurde, wird das Gerät automatisch erkannt, authentifiziert und im Capture Security Center hinzugefügt. Alle Lizenzen und Konfigurationen werden mit MySonicWall und License Manager synchronisiert.
SCHRITT 4	**FIREWALL VERWALTEN** Das Gerät ist jetzt betriebsbereit und kann über die cloudbasierte zentrale Verwaltungskonsole von Capture Security Center verwaltet werden. Dies umfasst Firmware-Upgrades, Sicherheitspatches und Konfigurationsänderungen auf Gruppenebene.

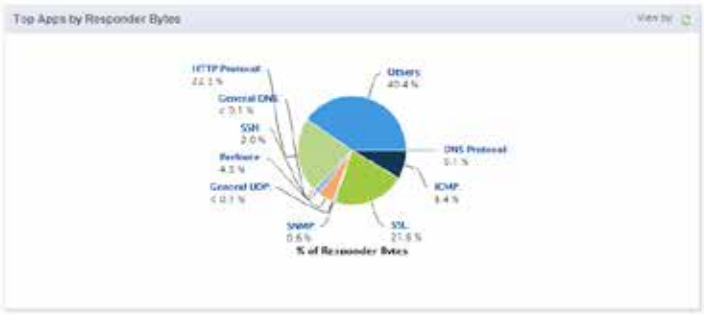
Vollautomatische Bereitstellung: Inbetriebnahme der Firewall in vier einfachen Schritten

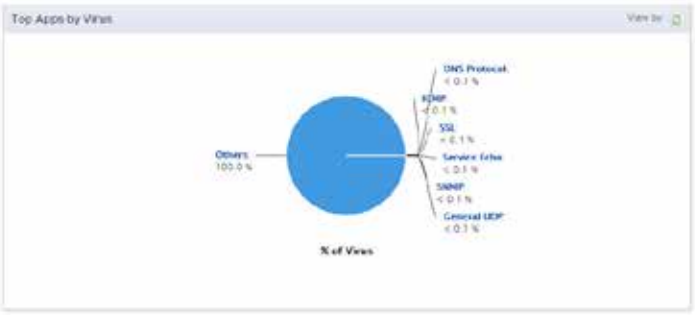
Reporting

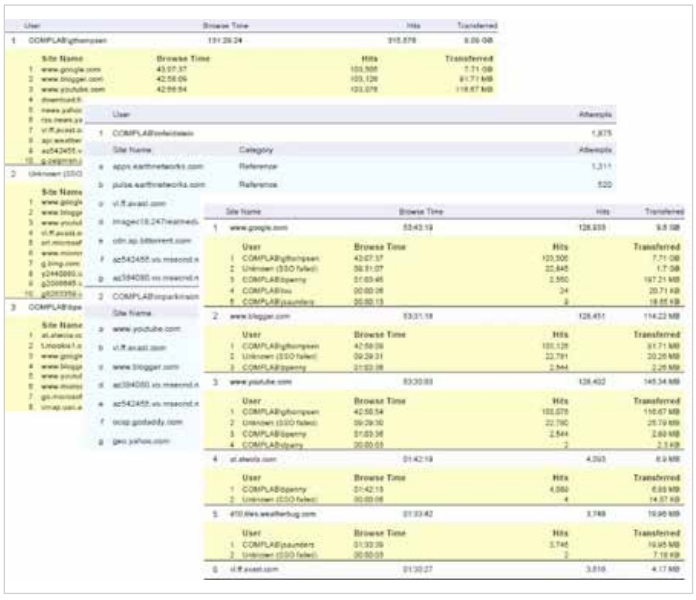
Das Capture Security Center bietet neben mehr als 140 vordefinierten Berichten auch die Möglichkeit, individuelle Berichte zu erstellen und dabei die auditierbaren Daten beliebig zu kombinieren. So können die gewünschten Anwendungsfälle durchgespielt werden. Die Ergebnisse umfassen einen Gesamt- und Detailüberblick über Netzwerkereignisse, Benutzeraktivitäten, Bedrohungen, Prozess- und Performanceprobleme, Sicherheitseffektivität, Risiken und Sicherheitslücken, Compliance-Readiness und sogar Post-mortem-Analysen. In sämtliche Berichte fließt der kollektive Input aus vielen Jahren Zusammenarbeit zwischen SonicWall und seinen Partnern ein. Dies liefert Organisationen äußerst detaillierte Einblicke, Anwendungsmöglichkeiten und Kenntnisse zu den Syslog- undIPFIX-/NetFlow-Daten, die zum Nachverfolgen, Messen und Durchführen effektiver Netzwerk- und Sicherheitsprozesse erforderlich sind.

Intuitive grafische Berichte vereinfachen die Überwachung verwalteter Appliances. Mit Nutzungsdaten für einen bestimmten Zeitbereich, Initiator, Responder oder Service können Administratoren Verkehrsanomalien einfach erkennen. Sie können außerdem Berichte in eine Microsoft® Excel®-Tabelle oder PDF-Datei exportieren oder direkt an einen Drucker weiterleiten, um regelmäßige Geschäftsanalysen durchzuführen.









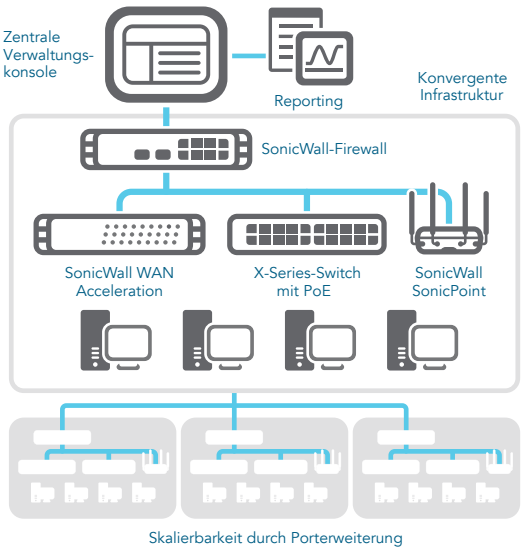
SONICWALL®

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.
Vollautomatische Bereitstellung	Einfachere und schnellere Remote-Implementierung von SonicWall-Firewalls über die Cloud. Automatische Durchsetzung von Regeln, Durchführung von Firmware-Upgrades und Synchronisierung von Lizenzen.
SD-WAN-Bereitstellung	Einfache zentrale Bereitstellung, Verwaltung und Überwachung der SD-WAN-Implementierung und -Konnektivität über verteilte Unternehmensumgebungen hinweg
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.
Unterstützung für geschlossene Netzwerke	Implementieren Sie GMS in geschlossenen Umgebungen wie etwa stark geschützten staatlichen Netzwerken. Alle Lizenzschlüssel und Signaturdateien der SonicWall-Back-End-Services werden gebündelt, verschlüsselt und sicher an das lokale Dateisystem übertragen, wo GMS darauf zugreifen und anschließend die nötigen Updates hochladen und an sämtliche verwalteten Sicherheitsappliances weiterleiten kann.
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.

Sicherheitsberichte und -analysen (Fortsetzung)	
Funktion	Beschreibung
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
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.
Authentifizierungssicherheit	
Funktion	Beschreibung
Kontosperrung	Die Richtlinien für die Kontosperrung sorgen dafür, dass ein GMS-Benutzerkonto deaktiviert wird, wenn in einem bestimmten Zeitraum das Passwort mehrfach falsch eingegeben wird. Dies reduziert die Wahrscheinlichkeit, dass Angreifer Benutzerpasswörter erraten und unerlaubt auf geschützte Ressourcen und Daten im Netzwerk zugreifen.
Passwortkomplexität	Die Richtlinie für die Passwortkomplexität legt wichtige Mindestvoraussetzungen für ein sicheres Passwort für die Anmeldung im GMS-System und den Zugriff darauf fest.
Administratorzugriff auf bestimmte Adressbereiche	Kunden können den Administratorzugriff auf bestimmte IP-Adressbereiche steuern.

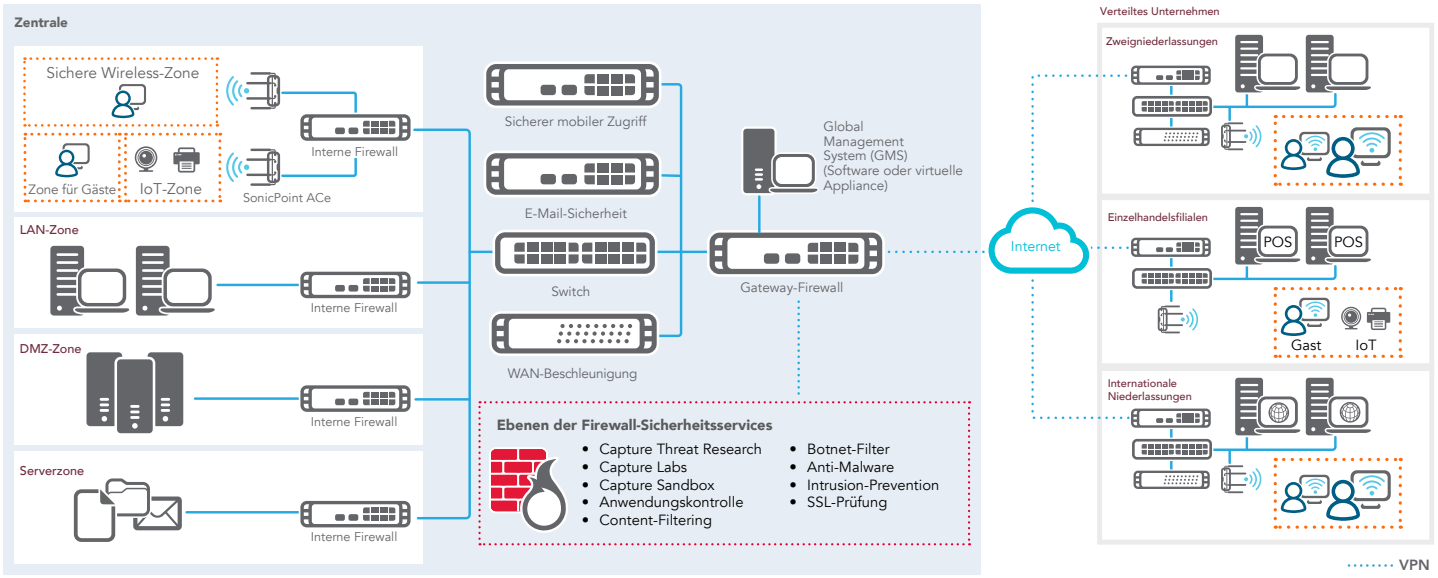
Skalierbare, verteilte Architektur

GMS ist eine lokale Lösung, die sich als Software oder virtuelle Appliance implementieren lässt. Das Herzstück von GMS ist eine verteilte Architektur, die eine endlose Systemverfügbarkeit- und -skalierbarkeit ermöglicht. Eine einzige GMS-Instanz kann die Transparenz und Kontrolle über Tausende GMS-verwalteter Netzwerksicherheitsgeräte erhöhen – egal wo sich diese befinden. Kunden profitieren mit GMS von hoch interaktiven, einheitlichen Dashboards mit Echtzeit-Überwachung, Reporting und Analysedaten, die intelligente Entscheidungen zu Sicherheitsregeln sowie Zusammenarbeit, Kommunikation und Wissen innerhalb des gemeinsamen Sicherheitsframeworks unterstützen. Mit einer unternehmensweiten Sicht auf die Sicherheitsumgebung und Echtzeit-Sicherheitsdaten für die zuständigen Mitarbeiter können Organisationen geeignete Aktionen für Sicherheitsregeln und -kontrollen durchführen, um ein stärkeres adaptives Sicherheitskonzept zu erhalten.



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.



Umgebung mit der lokalen SonicWall Global Management System-Lösung

Die Funktionen im Überblick

Reporting

- Große Auswahl an grafischen Berichten
- Compliance-Reporting
- Personalisierbares Reporting mit Drill-down-Funktionen
- Zentrales Logging
- Sammelberichte zu verschiedenen Bedrohungen
- Reporting zu Benutzern
- Berichte zur Anwendungsnutzung
- Detailliertes Reporting zu Services
- Neues Abwehrkonzept gegen Angriffe
- Bandbreiten- und Serviceberichte pro Schnittstelle
- Reporting für SonicWall-Firewall-Appliances
- Reporting für SonicWall-SRA-SSL-VPN-Appliances
- Universelle zeitgesteuerte Berichte
- Syslog- und IPFIX-Reporting der nächsten Generation
- Flexibles und granulares Reporting nahezu in Echtzeit
- Reporting zur genutzten Bandbreite pro User
- Reporting zu Client-VPN-Aktivitäten
- Detaillierte Zusammenfassung der Services über VPN-Bericht
- Reporting zu unberechtigten drahtlosen Access-Points
- Reporting zur SRA SMB Web Application Firewall (WAF)

Verwaltung

- Ortsunabhängiger Zugriff
- Warnmeldungen und Benachrichtigungen
- Diagnosetools
- Mehrere gleichzeitige Benutzersitzungen
- Offline-Management und Scheduling
- Verwaltung von Firewall-Sicherheitsregeln
- Verwaltung von VPN-Sicherheitsregeln
- Verwaltung von E-Mail-Sicherheitsregeln
- Verwaltung von SSL-VPN-Regeln und Regeln für einen sicheren Remote-Zugriff
- Verwaltung der Security-Mehrwertdienste
- Definition von Regelvorlagen auf Gruppenebene
- Regelreplikation von einem Gerät auf eine Gerätegruppe
- Regelreplikation von der Gruppenebene auf ein einzelnes Gerät
- Redundanz und Hochverfügbarkeit
- Provisioning-Management
- Skalierbare und verteilte Architektur
- Dynamische Verwaltungssichten
- Einheitlicher Lizenzmanager
- Befehlszeilenschnittstelle (CLI)
- API (Application Programming Interface)-Schnittstelle für Webservices
- Rollenbasierte Verwaltung (Benutzer, Gruppen)
- Umfassendes Dashboard
- Back-up von Einstellungsdateien für Firewall-Appliances
- SD-WAN
- Vollautomatische Bereitstellung
- Unterstützung für geschlossene Netzwerke
- Firewall-Sandwich-Unterstützung

Überwachung

IPFIX-Datenströme in Echtzeit

SNMP-Unterstützung

Aktive Überwachung von Geräten und Alarmierung

SNMP-Relay-Verwaltung

Überwachung des VPN- und Firewall-Status

Live-Syslog-Überwachung und Warnmeldungen

Authentifizierungssicherheit

Kontosperrung

Passwortkomplexität

Administratorzugriff auf bestimmte Adressbereiche

Mindestsystemanforderungen

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

Betriebssystem

- 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:
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)

Für die Verwaltung mit GMS unterstützte SonicWall Appliances

- SonicWall-Netzwerksicherheitsappliances: Appliances der SuperMassive E10000 und 9000 Series, E-Class NSA, NS*a* Series und TZ Series
- Virtuelle SonicWall-Netzwerksicherheitsappliances: NSv Series
- SonicWall Secure Mobile Access (SMA)-Appliances: SMA Series und E-Class SRA
- SonicWall Email Security-Appliances
- Alle TCP-/IP- und SNMP-Geräte und -Anwendungen für aktive Überwachung

Global Management System (GMS) – Bestellinformationen	
Produkt	Artikelnummer
SONICWALL GMS SOFTWARE-LIZENZ (5 NODES)	01-SSC-3311
SONICWALL GMS SOFTWARE-LIZENZ (10 NODES)	01-SSC-7662
SONICWALL GMS SOFTWARE-LIZENZ (25 NODES)	01-SSC-3350
SONICWALL GMS SOFTWARE-UPGRADE (1 NODE)	01-SSC-7664
SONICWALL GMS SOFTWARE-UPGRADE (5 NODES)	01-SSC-3301
SONICWALL GMS SOFTWARE-UPGRADE (10 NODES)	01-SSC-3303
SONICWALL GMS SOFTWARE-UPGRADE (25 NODES)	01-SSC-3304
SONICWALL GMS SOFTWARE-UPGRADE (100 NODES)	01-SSC-3306
SONICWALL GMS SOFTWARE-UPGRADE (250 NODES)	01-SSC-0424
SONICWALL GMS SOFTWARE-UPGRADE (1000 NODES)	01-SSC-7675
SONICWALL GMS CHANGE MANAGEMENT AND WORKFLOW	01-SSC-6524
SONICWALL GMS E-CLASS 24/7-SOFTWARE-SUPPORT FÜR 1 NODE (1 JAHR)	01-SSC-6514
SONICWALL GMS E-CLASS 24/7-SOFTWARE-SUPPORT FÜR 5 NODES (1 JAHR)	01-SSC-3334
SONICWALL GMS E-CLASS 24/7-SOFTWARE-SUPPORT FÜR 10 NODES (1 JAHR)	01-SSC-3336
SONICWALL GMS E-CLASS 24/7-SOFTWARE-SUPPORT FÜR 25 NODES (1 JAHR)	01-SSC-3337
SONICWALL GMS E-CLASS 24/7-SOFTWARE-SUPPORT FÜR 100 NODES (1 JAHR)	01-SSC-3338
SONICWALL GMS E-CLASS 24/7-SOFTWARE-SUPPORT FÜR 250 NODES (1 JAHR)	01-SSC-6524
SONICWALL GMS E-CLASS 24/7-SOFTWARE-SUPPORT FÜR 1000 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 27 Jahren bekämpft SonicWall Cyberkriminalität, um kleinen, mittleren und großen Unternehmen weltweit Schutz zu bieten. Mit unseren Produkten und Partnern können wir eine automatisierte Echtzeitlösung zur Erkennung und Prävention von Sicherheitslücken für die individuellen Anforderungen von mehr als 500.000 Organisationen in über 215 Ländern und Regionen bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können. Für weitere Informationen besuchen Sie www.sonicwall.com oder folgen uns auf Twitter, LinkedIn, Facebook und Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, Kalifornien
95035, USA
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

DataSheet-SonicWallGlobalManagementSystem-US-VG-MKTG4042