

Symantec™ Gateway Security

Umfassender Gateway-Schutz mit einer vollständig integrierten und einfach zu verwaltenden Sicherheits-Appliance

Symantec Gateway Security ist eine integrierte Appliance für den Gateway-Schutz, die Sicherheitsverstöße direkt am Gateway zwischen dem Internet und Unternehmensnetzwerken oder zwischen einzelnen Netzwerksegmenten verhindert. Die einfach installierbare und zu verwaltende Appliance integriert fünf wesentliche Sicherheitsfunktionen – Firewall, Virenschutz, Intrusion Detection, Content-Filtering und VPN (Virtual Private Network) – in einer einzigen Lösung und bietet daher optimalen Schutz vor den neuen "komplexen" Formen der Bedrohung. Aufgrund dieser diversen Funktionen stellt Symantec Gateway Security Appliance zudem eine äußerst kosteneffiziente Sicherheitslösung dar. Durch die optimale Zusammenarbeit aller Sicherheitsfunktionen werden nicht nur die Kosten für den Erwerb, die Installation und die Verwaltung separater Komponenten gesenkt, auch die Sicherheitsverwaltung wird entscheidend erleichtert. Symantec Raptor™ Management Console sorgt für eine benutzerfreundliche Handhabung: Alle Sicherheitsfunktionen lassen sich vor Ort oder per Fernverwaltung über die intuitive Benutzeroberfläche der Konsole konfigurieren und verwalten. Durch eine gemeinsame Berichtsstruktur für alle Funktionen ist auch die Analyse und Auswertung der Sicherheitsdaten kein Problem.



> **Vollständig integrierte Lösung für einen umfassenden Schutz aller Netzwerkebenen**

Alle vorkonfigurierten und vorinstallierten Sicherheitstechnologien der Symantec Gateway Security-Appliance funktionieren wie eine einzige Software. Damit eignet sich die Appliance optimal zur Abwehr der heutigen "komplexen" Gefahren wie CodeRed und Nimda, denen allen eines gemeinsam ist: Für ihre Angriffe setzen sie jeweils äußerst vielfältige Methoden ein, wie beispielsweise das Verwenden unterschiedlicher Protokolle. Um sie zuverlässig zu stoppen, ist es erforderlich, ihnen ebenfalls mit einer koordinierten technischen Intervention an mehreren Fronten zu begegnen. Symantec Gateway Security sorgt für diese zuverlässige Sicherheit, denn von außen eingehende Daten durchlaufen eine Reihe von strengsten Sicherheitsprüfungen. Auf diese Weise werden Bedrohungen abgewehrt, bevor sie überhaupt das interne System erreichen.

Intrusion-Detection-Agenten arbeiten mit der leistungsstarken Symantec Gateway Security-Firewall zusammen und überprüfen den Internet- und E-Mail-Verkehr auf bekannte Angriffssignaturen. Beim Auftreten von Sicherheitsverstößen werden sofort entsprechende Gegenmaßnahmen eingeleitet, beispielsweise indem Pakete von verdächtigen IP-Adressen blockiert werden. Mit Hilfe spezieller Prüfverfahren der Application Proxy-Technologie, Paketfilterung und Checks des Network Circuit analysiert die Firewall-Engine das gesamte Internet-Paket, um verdächtige Syntax, ungewöhnliche Zeichen, ungültige Befehle und andere Funktionen aufzuspüren, die von Sicherheitsbedrohungen häufig innerhalb von Netzwerkprotokollen missbraucht werden. Der gesamte Internet-, E-Mail- und FTP-Datenverkehr muss Symantec's Multi-Thread-Virenprüf-Engine und Richtlinienfilter passieren. Infizierte Dateien werden gestoppt und repariert. Symantec Gateway Security enthält darüber hinaus Funktionen zum Blockieren von Webinhalten sowie VPN-Funktionalität, die mit den fortschrittlichsten Sicherheitstechnologien (beispielsweise dem neuesten AES-Verschlüsselungsalgorithmus) arbeiten. Diese Funktionen sorgen für zusätzliche Kontrolle und eine Reduktion der Kommunikationskosten und Netzwerkbelastung. Alle Programme sind auf dem neuesten Stand der Technik, vielfach prämiert und in puncto Funktionalität richtungweisend.

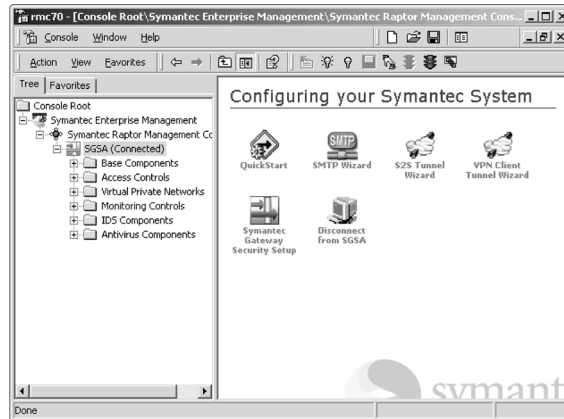
Um sich vor sämtlichen potenziellen Bedrohungen und den daraus resultierenden unterschiedlichen Angriffsformen zu schützen, benötigen Unternehmen eine vollständig integrierte Sicherheitslösung. Mit einer Kombination aus Sicherheitsprüfungen und fortlaufendem System-Hardening sorgt Symantec Gateway Security für den Schutz des Gateways auf allen Ebenen. Die Appliance kontrolliert und überwacht den gesamten Datenverkehr auf Würmer, Viren, bösartigen Code, unbefugte Zugriffsversuche, Denial-of-Service-Attacken sowie "komplexe" Formen der Bedrohung wie beispielsweise CodeRed und Nimda. Damit alle Sicherheitsfunktionen jederzeit auf dem neuesten Stand und somit wirksam sind, werden integrierte Updates für Virendefinitionen und Angriffssignaturen automatisch über die Symantec LiveUpdate™-Funktion an alle notwendigen Technologiebereiche verteilt.

DIE VORTEILE

- > Umfassender Gateway-Schutz mit einer einfach zu verwaltenden Appliance, die speziell für die Anforderungen von kleineren und mittleren Unternehmen, sowie deren Niederlassungen entwickelt wurde
- > Schutz vor den neuesten Bedrohungen mit fünf vollständig integrierten Sicherheitstechnologien
- > Überwachung und Kontrolle des gesamten Internet-Datenverkehrs mit einer unternehmensweiten ICESA-zertifizierten Firewall, die die AES-, 3DES- und DES-Verschlüsselungsstandards unterstützt
- > Sichere Verbindungen mit standortfernen Büros und Telearbeitern über ein integriertes IPSec-kompatibles und ICESA-zertifiziertes ProxySecured VPN
- > Innovative Prüfverfahren für den E-Mail- und Internet-Datenverkehr sowie proaktive E-Mail-Blockierung zur Abwehr aller Arten von Gefahren am Gateway (beispielsweise Viren, Würmer und vielfältige "komplexe" Formen der Bedrohung wie Nimda und CodeRed)
- > Benachrichtigung des System-Administrators über Scans und Zugriffsversuche mit Hilfe der integrierten Intrusion-Detection-Funktionen
- > Durchsetzung der Unternehmensrichtlinien für die Internet-Nutzung mit Hilfe integrierter Funktionen zur Filterung und Blockierung von Webinhalten
- > Einfache Verwaltung durch eine gemeinsame Managementkonsole mit einer grafischen Benutzeroberfläche für alle Sicherheitsfunktionen
- > Automatische Sicherheits-Updates in einem einzigen integrierten Paket über LiveUpdate™
- > Skalierbarkeit und optimale Leistung durch integrierte Funktionen für die Hochverfügbarkeit und Lastverteilung
- > Unterstützt von Symantec Security Response, dem weltweit führenden Forschungs- und Unterstützungsteam für Internet-Sicherheit

➤ Zentrale Steuerung über eine einzige Managementkonsole

Mit Hilfe intelligenter Setup-Assistenten lässt sich die Symantec Gateway Security-Appliance in nur wenigen Minuten installieren und konfigurieren. Alle Daten, die über E-Mail, Internet oder Datei-Übertragungen das Netzwerk durch das Internet-Gateway erreichen oder verlassen, werden zuverlässig geschützt. Mit der Symantec Raptor™ Management Console werden alle Sicherheitsfunktionen über eine einzige Managementkonsole zentral verwaltet und überwacht. Sicherheitsrichtlinien und -regeln lassen sich für jede Appliance einfach konfigurieren und ändern. Dabei ist es völlig unwesentlich, ob sich die Appliance vor Ort oder an weit entfernten Standorten befindet. Die intuitive Benutzeroberfläche der Konsole unterstützt System-Administratoren bei der Erstellung und Konfiguration von Regeln. Sicherheits-Patches lassen sich problemlos per Remotezugriff installieren. Die Konfiguration von Sicherheitsrichtlinien für Benutzer und Benutzergruppen ist ebenfalls mit nur geringem Aufwand verbunden. Dank der zentralen Steuerung lässt sich auch die Verteilung der Updates effizient verwalten. Umfangreiche Benachrichtigungs-, Protokoll- und Berichtsfunktionen ermöglichen die Erstellung benutzerdefinierter Analysen und Trendberichten zu den Sessions. Die Vorteile dieser zentralen Verwaltung aller wichtigen Sicherheitsfunktionen: schnelle Installationen, einfache Verwaltung sowie eine strikte und effektive Überwachung des gesamten Unternehmensnetzwerks.



➤ Eine skalierbare Lösung für kleine und große Unternehmen

Die Symantec Gateway Security-Appliance ist in drei Ausführungen erhältlich und eignet sich für Unternehmen mit 50 bis 1000 Netzwerkknoten. Aufgrund der in jedem Modell vorinstallierten Hochverfügbarkeits- und Lastverteilungslösungen (optionales Feature) gewährleistet die Appliance einen maximalen Durchsatz, zuverlässige Systemverfügbarkeit und hohe Skalierbarkeit. In Netzwerken mit bis zu 5000 oder mehr Knoten mit höheren Durchsatzraten können bis zu acht Appliances zu einem Cluster zusammengefasst werden, um Hochverfügbarkeit und System-Failover zu gewährleisten.

➤ Erstklassiger Service und Support

Die Symantec Gateway Security-Appliance ist eine vollständig integrierte Sicherheitslösung, bei der alle Komponenten und damit auch der Service und die weltweite technische Unterstützung für alle Sicherheitsfunktionen aus einer Hand stammen. Die Symantec Security Response-Experten stehen rund um die Uhr bereit und können im Notfall innerhalb weniger Stunden aktuelle Bedrohungen identifizieren und den Unternehmen mit Symantecs exklusiver LiveUpdate™-Funktion umgehend neue Signaturen zustellen. LiveUpdate hält jede integrierte Sicherheitsfunktion automatisch auf dem neuesten Stand, indem es die neuesten Virendefinitionen, Angriffssignaturen und Sicherheits-Patches in einem einzigen, selbstinstallierenden Update-Paket verteilt. Dadurch lassen sich weitere Sicherheitszwischenfälle sehr leicht in den Griff bekommen. Da die Installation und Verteilung automatisch erfolgt, ist auch keinerlei Verwaltungsaufwand notwendig.

Beim Kauf der Symantec Gateway Security-Appliance erhalten Unternehmen ein Jahr lang Gold Support. Zu den Leistungen dieses Programms gehören: technische Unterstützung, Virendefinitions-, Angriffssignatur- und Content-Filtering-Updates sowie eine Austauschvereinbarung bei nachgewiesenen Hardware-Problemen.

> **Umfassender Schutz mit einer einfach zu verwaltenden Appliance**

Die Symantec™ Gateway Security-Appliance ist eine einfach zu verwaltende Lösung für den Gateway-Schutz, die zahlreiche Sicherheitsfunktionen integriert:

- **ICSA-ZERTIFIZIERTE UNTERNEHMENS-FIREWALL** Die speziellen Prüfverfahren der Application Proxy- Technologie ermöglichen die Konfiguration von Richtlinien für die Überwachung und Kontrolle des gesamten Netzwerkverkehrs und sorgen für den Schutz der Unternehmens-/Internet-Schnittstelle, der unternehmenseigenen Intranets, der privaten Subnetze und Niederlassungen. Die einzigartige Hybridarchitektur gewährleistet Sicherheit und hohe Geschwindigkeit. Symantec Gateway Security prüft den Datenverkehr, indem es den vom Server initiierten ausgehenden HTTP-Datenverkehr, der nicht die RFC-Standards erfüllt, blockiert. Mit der Anwendung der Best-Fit-Regel wird gleichzeitig verhindert, dass versehentlich Schwachstellen entstehen. ICSA-, IPsec- und Firewall-Zertifizierungen gewährleisten die Einhaltung der höchsten Sicherheits- und Interoperabilitätsanforderungen.
- **INTEGRIERTES IPSEC-KOMPATIBLES UND ICSA-ZERTIFIZIERTES PROXYSECURED VPN** Die integrierte VPN-Technologie ermöglicht sichere Verbindungen zwischen Unternehmenssitz, reisenden Mitarbeitern und Geschäftspartnern. Der Datenverkehr wird dabei nicht nur auf Netzwerkebene, sondern auch auf der Anwendungsebene überwacht. Bei der Verbindungsherstellung werden folgende Verschlüsselungsstandards unterstützt: Advanced Encryption Standard (AES), 3DES (Triple Data Encryption Standard: 168-Bit-Schlüssel) und DES (Data Encryption Standard: 56-Bit-Schlüssel). Unter Einsatz von IKE und PKI sowie verschiedener Authentifizierungstechnologien wie z. B. Digital Certificates bietet die Symantec Gateway Security-Appliance optionale Unterstützung für starke Authentifizierung. Unterstützt werden Authentifizierungsmethoden wie Windows NT® Domain Login, S/Key, SecurID und X.509-Zertifikate. Zudem bietet Symantec Enterprise VPN Support für Authentifizierungsprotokolle wie TACACS+, RADIUS und LDAP (diese Protokolle sind ebenfalls für die Firewallfunktionen verfügbar).
- **PRÜFUNG DES E-MAIL- UND INTERNET-VERKEHRS** Unter Einsatz modernster Symantec-Technologien prüft die Symantec Gateway Security-Appliance den E-Mail- und Internet-Verkehr (SMTP, HTTP und FTP) direkt am Gateway. Trojanische Pferde und Nimda-ähnliche Viren und Würmer werden gestoppt, bevor sie das Netzwerk infizieren können.
- **MARKTFÜHRENDER VIRENSCHUTZ** Die innovativen Virenschutztechnologien von Symantec, darunter die erweiterbare NAVEX™ Prüf-Engine und die heuristische Bloodhound™-Technologie, sorgen für umfassenden Schutz an allen anfälligen Netzwerk-Gateways. Böartige Viren, die über E-Mail, Internet oder Dateiübertragungen das Netzwerk erreichen, werden automatisch erkannt und beseitigt.
- **PROAKTIVE E-MAIL-BLOCKIERUNG** Die Symantec Gateway Security-Appliance blockiert E-Mail-Nachrichten nach Betreffzeile, Anhangsname oder Nachrichtengröße. Bei flächendeckenden Virenausbrüchen, für die häufig eine gemeinsame Betreffzeile oder andere gemeinsame Merkmale typisch sind, bietet diese Funktion demnach einen aktiven Schutz.
- **FILTERUNG VON WEBINHALTEN ("CONTENT FILTERING")** Die integrierten Funktionen zum Filtern von Webinhalten unterbinden unerwünschtes Surfen am Arbeitsplatz. Durch die Kontrolle des Zugriffs auf URLs und Newsgruppen gemäß den jeweiligen Anforderungen und Richtlinien eines Unternehmens wird dieses geschützt und eine übermäßige Belastung des Netzwerks vermieden.
- **INTRUSION DETECTION** Intrusion-Detection-Technologien benachrichtigen Administratoren bei einem Angriffsversuch auf das Netzwerk. Mehr als 80 Angriffssignaturen werden eingesetzt, um Versuche, bei denen beispielsweise Traversal-Schwachstellen missbraucht, Port-Scans durchgeführt oder DoS-Angriffe gestartet werden, zu blockieren oder abzuwehren. Agenten zur Schwachstellenanalyse erkennen darüber hinaus unzureichende Sicherheitseinstellungen, nicht benötigte Services sowie Patches, die nicht installiert sind. Dieser Schutz lässt sich automatisch über LiveUpdate™ mit den neuesten Angriffssignaturen aktualisieren. Umfangreiche Benachrichtigungs-, Protokoll- und Berichts-Tools ermöglichen die Erstellung benutzerdefinierter Analysen des Netzwerkverkehrs und der Netzwerknutzung.

Die Symantec Gateway Security-Appliance kann problemlos mit anderen Sicherheitsprodukten von Symantec integriert werden. So können in einem Unternehmen umfassende Sicherheitslösungen implementiert werden, die alle Bereiche des Netzwerks – vom Internet-Gateway bis hin zur Desktop-Ebene – schützen.

➤ Maximale Sicherheit und Optimierung der Sicherheitsinvestition

Die Symantec™ Gateway Security-Appliance integriert moderne Sicherheitsfunktionen hinter einer einzigen Managementkonsole und gewährleistet die nahtlose Zusammenarbeit der einzelnen Technologien. Die Appliance bietet damit eine Lösung, die einerseits die Sicherheit im Unternehmen erhöht und einfach zu verwalten ist, andererseits aber auch die Netzwerkleistung und die Investitionen im Sicherheitsbereich optimiert.

VERGLEICH DER DREI VON SYMANTEC ANGEBOTENEN APPLIANCE-MODELLE

MODELLE	5110	5200	5300
Maximaler Durchsatz	bis zu 40 MBit/s	bis zu 90 MBit/s	bis zu 90 MBit/s
Durchschnittlicher Durchsatz	12 MBit/s (8 T1)	40 MBit/s (T3)	40 MBit/s (T3)
Einfache Installation und Verwaltung	Ja	Ja	Ja
Supportleistungen	1 Jahr Gold Support im Paket enthalten	1 Jahr Gold Support im Paket enthalten	1 Jahr Gold Support im Paket enthalten
Empfohlene Netzwerkgröße	bis zu 50 Knoten	bis zu 250 Knoten	bis zu 1000 Knoten
Remote-to-Site VPN	Option	Option	Option
Site-to-Site VPN	Standard	Standard	Standard
Hochverfügbarkeit und Lastverteilung	Option	Option	Option
Firewall	Full Inspection	Full Inspection	Full Inspection
Virenschutz	Carrier Class-Virenschutz	Carrier Class-Virenschutz	Carrier Class-Virenschutz
Intrusion Detection	"Pass-through"-Technologie	"Pass-through"-Technologie	"Pass-through"-Technologie
Content-Filtering	URL	URL	URL
PHYSIKALISCHE DATEN			
Gewicht:	4,2 kg	10,7 kg	10,7 kg
Abmessungen (in cm):	43,2B x 31,8T x 4,5H	44,5B x 57,8T x 4,5H	44,5B x 57,8T x 4,5H
HARDWARE			
Ethernet-Ports	4 unabhängige 10/100 BaseT-Netzwerk- Schnittstellen	4 unabhängige 10/100 BaseT-Netzwerk- Schnittstellen	4 unabhängige 10/100 BaseT-Netzwerk- Schnittstellen
Serielle Ports	2 Ports	2 Ports	2 Ports
UPS (Unterbrechungsfreie Stromversorgung)	UPS-Unterstützung	UPS-Unterstützung	UPS-Unterstützung
LCD (Flüssigkristalldisplay)	LCD-Anzeige für einfache Installation und Verwaltung	LCD-Anzeige für einfache Installation und Verwaltung	LCD-Anzeige für einfache Installation und Verwaltung
Anforderungen an die Stromversorgung	100 - 240 V, 50/60 Hz	100 - 240 V, 50/60 Hz	100 - 240 V, 50/60 Hz
Durchschnittlicher Stromverbrauch	50 Watt	100 Watt	100 Watt
Max. Stromverbrauch	60 Watt	130 Watt	130 Watt

GATEWAY-SICHERHEIT BILDET EINEN WICHTIGEN BESTANDTEIL DER SYMANTEC ENTERPRISE SECURITY-LÖSUNGEN. SYMANTEC ENTERPRISE SECURITY VERBINDET ERSTKLASSIGE TECHNOLOGIEN, UMFASSENDE SERVICES UND GLOBALE REAKTIONSTEAMS FÜR IHRE UNTERNEHMENSICHERHEIT.



SYSTEMANFORDERUNGEN MANAGEMENTKONSOLE

- Windows® NT oder 2000
- Prozessor ab Pentium® III 300 MHz
- 128 MB RAM (Minimum)

WORLD HEADQUARTERS:
20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
001-408-253 9600
001-800-441 7234

DEUTSCHLAND:
Symantec (Deutschland) GmbH
Kaiserswerther Str. 115
D - 40880 Ratingen
Tel.: +49 (0) 69-6641 0315
E-Mail:
enterprise.deutsch@symantec.com

ÖSTERREICH:
Symantec GmbH
Wipplingerstraße 34
A - 1010 Wien
Tel.: +43 (0)1- 50137-5020
E-Mail: enterprise.deutsch@symantec.com

SCHWEIZ:
Symantec Switzerland AG
Grindelstrasse 6
CH - 8303 Bassersdorf
Tel.: +41 (0) 1-838 49 00
Fax: +41 (0) 1-838 49 01
E-Mail: infoline@symantec.com