Compumatica
SECURE NETWORKS

Technisches

WhitePaper

CompuWall

Die High-Level-Firewall für Behörden und Unternehmen

Compumatica secure networks

DAS *COMPUWALL* FIREWALL-SYSTEM

Die *CompuWall* ist eine Application Level Firewall mit Web-Management, die speziell zur Absicherung kleiner und mittlerer Netzwerke entworfen wurde.

Sie sichert den Übergang verschiedener Netzsegmente, indem sie die Netze de facto physikalisch von einander trennt.

Fehlbedienung wird durch den in die Praxis umgesetzten Grundsatz faktisch ausgeschlossen.

„Alles was nicht explizit erlaubt wird,
ist grundsätzlich verboten.“

Die *CompuWall* vereint ihren sehr hohen Sicherheitsstandard mit hoher Performance und leichter Bedienung.

Somit eignet sie sich insbesonders für kleine bis mittlere Organisationen, aber durchaus auch für Netzübergänge größerer Organisationen, bei denen Teile der Infrastruktur unabhängig von der zentralen IT-Infrastruktur abgesichert werden sollen.

Besonderes Augenmerk wurde auf

- die **Sicherheit,**
- die **Stabilität** und
- den **Datendurchsatz**

der jeweiligen Anwendungen gelegt.

Diese Konstellation bietet das höchste Sicherheitsniveau aller Firewall-Architekturen!

Insbesondere unterscheidet es sich deutlich vom Konzept der „Stateful Inspection“.

SICHERHEITSMECHANISMEN

- **Zugriffskontrolle auf Netzwerkebene**
  Nur zugelassene Verbindungen können aufgebaut werden.
- **Zugriffskontrolle auf Benutzerebene**
  Nur authentisierte Benutzer erlangen Zugriff auf einzelne Systeme/Systemgruppen.
- **Administration von Zugriffsrechten**
  Der Zugang ist nur möglich, wenn die Protokolle und Dienste durch den Administrator definiert und zugelassen werden.
- **Kontrolle auf Applikationsebene**
  Die Benutzer können nur die notwendigen Kommandos der für ihre Arbeiten wichtigen Dienste (wie z.B. HTTP oder FTP) nutzen. Kommandos, die missbraucht werden könnten, stehen somit erst gar nicht zur Verfügung. Zudem können die Dateninhalte (auch HTTPS) an zentraler Stelle auf schädliche Inhalte überprüft werden.
- **Isolation der Dienstprogramme**
  Alle Dienste werden gezwungen spezielle Proxy-Applikationen zu nutzen. Jeder Proxy arbeitet dabei mit eingeschränkten Rechten in einem isolierten Bereich des Betriebssystems.
- **Beweissicherung, Log-Analyse und Alarmierung**
  Alle sicherheitsrelevanten Ereignisse können aufgezeichnet und analysiert werden oder führen zusätzlich zu einer Alarmierung.
- **Schutz der internen Netzwerkstrukturen**
  Die Kenntnis der Kommunikationsbeziehungen erleichtert die Arbeit eines potentiellen Angreifers. Geheimhaltung der zu schützenden Netzwerkstrukturen ist deshalb ein wichtiger Bestandteil der Sicherheitsstrategie.
- **Verschlüsselte Administration**
  Der Management-Zugriff erfolgt vollständig verschlüsselt,

entweder über HTTPS (zusätzlich geschützt durch ein Client-Zertifikat) oder per SSH.

KONZEPT DER HIGH-LEVEL-*COMPUWALL*

Durch die intuitiv zu bedienende Management-Oberfläche werden dem Administrator der Einstieg und die Konfiguration der *CompuWall* erleichtert.

Die *CompuWall* zeichnet sich insbesondere durch folgende Kriterien aus:

- **Rundumschutz durch eXtended Unified Threat Management (XTM)**
- **Sehr hoher Sicherheitsstandard**
- **Schnelle Inbetriebnahme**
- **Einfache und intuitive Bedienung**
- **Strukturierte Regelübersicht**
- **Detaillierte Zustandsmeldungen und Berichte**

Die *CompuWall* basiert auf einem sicherheitsoptimierten Linux-Betriebssystem, dem *CryptoBastion* OS, das von Grund auf für die Anwendung als uneinnehmbares Firewall-System entwickelt wurde.

Bereits seit Beginn der 90er Jahre wurde stets das gleiche solide Grundkonzept beibehalten, um eine Vielzahl von Sicherheitsfunktionen erweitert und stetig optimiert.

Den Kern des Systems bilden die mit viel Erfahrung entwickelten Proxy-Applikationen.

Die *CompuWall* ist in der Lage drei verschiedene Verbindungsmodi zu konfigurieren, die auch miteinander gekoppelt werden können:

- **nicht** transparente Verbindungen**,**
- **einseitig** transparente Verbindungen und
- **beidseitig (doppelt)** transparente Verbindungen

Diese Flexibilität ermöglicht eine mühelose Konzeption und problemlose Integration des Application Gateways in beliebige Netzwerkinfrastrukturen.

CompuWall – Features und deren Nutzen

Dienstprogramme

Die *CompuWall* bietet Ihnen das volle Spektrum an Funktionalität, um Netzwerkübergänge einer oder mehrerer Organisation(en) abzusichern.

Um den hohen Sicherheitsanforderungen Ihres Netzwerkes gerecht zu werden, wurden spezielle, performanceoptimierte Proxies für die folgenden Protokolle entwickelt:

OpenVPN Tunnel

Der OpenVPN-Zugang ermöglicht die problemlose Kopplung externer Telearbeitsplätze und Mobilfunkgeräte an das betriebseigene Intranet oder einfachen und sicheren Site-to-Site-Zugriff innerhalb des Unternehmens.

Clientsoftware ist für folgende Betriebssysteme kostenfrei erhältlich: Linux, Windows, MAC OS, iOS, Android, PocketPC.

IPsec

Remote-Zugriff VPN-Lösung für iOS-Geräte

- Realisiert durch strongSwan unter Verwendung von IKEv1 und doppelter Authentifzierung (RSA & Xauth)
- Unterstützung von NAT-Traversal und Split-Tunneling
- Kann mit dem eingebauten Cisco IPsec VPN-Client in iOS-Geräten zusammenarbeiten

HTTP/HTTPS [AntiVIRUS]

Zugriff auf das World Wide Web mit der Möglichkeit zur Filterung auf Applikationsebene (ClamAV, KasperskyAV®).

URL-Filter

Basierend auf kategorisierten Blacklisten, konfigurierbar anhand von Domainnamen, URL-Fragmenten oder regulären Ausdrücken innerhalb der URL (zusätzliche Whitelist für vertrauenswürdige URLs).

Phishing- und Malwareschutz

Basierend auf Google Safebrowsing Blacklisten, inklusive automatischer Updates.

SSL Decrypter

Integrierte Lösung zum Schutz vor Viren und schadhaftem Code innerhalb des HTTPS-Datenstroms

Content Filter	Ermöglicht die Filterung von Java, JavaScript und ActiveX-Elementen (Microsoft Silverlight, Adobe Flash und anderer eingebetteter Inhalt) und Cookies.
User-Agent Blacklist/Filter	Anfragen der ausgewählten Web-Clients werden geblockt.
FTP [AntiVIRUS]	Datei-Download/-Upload mit der Möglichkeit einzelne FTP-Kommandos zu filtern.
TELNET	Administrationszugriff auf externe Server mit der Möglichkeit diese Sitzungen zu protokollieren (AUDIT).
ESMTP [AntiVIRUS/ AntiSPAM]	Schutz beim Senden und Empfangen von E-Mails durch strikte Trennung der notwendigen Prozesse. Zusätzliche Filterung von ESMTP-Kommandos und Optionen möglich.
POP3 [AntiVIRUS/ AntiSPAM]	Abholen von E-Mails von externen/internen E-Mailservern.
NNTP	Zugriff auf Newsgruppen.
NET8	Proxy für Oracle Datenbankzugriffe.
RTSP	Real Time Streaming – Multimedia Proxy.
TCPR	Relay für TCP-basierte Anwendungen.
UDPR	Relay für UDP-basierte Anwendungen.
DNS	Ermöglicht die Vorwärts-/Rückwärtsauflösung über Netzwerkgrenzen hinweg.
PING	Test der Erreichbarkeit einzelner Endgeräte.
MGNTP	Ermöglicht die Verwaltung der *Compumatica CryptoGuard VPN* Geräte über eine *CompuWall* hinweg. (dient zusätzlich dem Schutz vor Phishing).
Reverse Proxy	Integrierter Schutz der internen Server bzw. Server-Farmen innerhalb einer DMZ.
MIME Filter	Ermöglicht die Filterung verschiedener MIME-Typen.

ERWEITERTE FUNKTIONEN – XTM – EXTENDED THREAT MANAGEMENT

- Detaillierte Reporting-Funktionalität für OpenVPN-, E-Mail- und Web-Traffic (exportierbar als PDF-Datei).
- Einfach zu konfigurierender, auf kategorisierten Blacklisten basierender URL-Filtermechanismus für

HTTP(S)-Verbindungen. Die verwendeten Listen sind kompatibel zu den Formaten, die auch von Squidguard/DansGuardian verwendet werden. Ausnahmeregeln können in einer zusätzlichen Whitelist spezifiziert werden.

- IP-Blackholing: Es kann eine Liste von IP-Adressen spezifiziert werden, zu denen jeglicher Netzwerkverkehr untersagt werden soll. Alle davon betroffenen Netzwerkpakete werden verworfen.
- Einfacher, zertifikatsbasierter IPsec-/OpenVPN-Zugang für Telearbeiter und/oder Standortkopplungen. Die CompuWall kann somit mühelos als VPN-Gateway konfiguriert werden.
- Integrierte AntiVIRUS-Erkennung für die Protokolle HTTP(S), FTP, ESMTP und POP3 durch ClamAV und/oder Kaspersky® kavd (inklusive automatischer Updates der Virendatenbanken).
- AntiSPAM-Schutz für die Protokolle ESMTP und POP3 durch SpamAssassin und Realtime Blacklists (RBL).
- Phishing- und Malwareschutz, basierend auf Google Safe Browsing Blacklisten.
- Host-IDS mittels AIDE (Advanced Intrusion Detection Environment), zur Überprüfung der Integrität der Systemdateien und -verzeichnisse.
- Hochverfügbarkeit (Active/Active oder Active/Passive) durch den Einsatz von Heartbeat Version 2, auch für transparente Verbindungen.
- Benutzerauthentifikation, global für mehrere Dienste oder sessionabhängig, mittels Passwort, SKey oder Hardwaretoken, MAS (Mobile Authentication Service), LDAP oder RADIUS-Authentifikation möglich.
- Protokollierung und Alarmierung von sicherheitsrelevanten Ereignissen per E-Mail (auch zu einem entfernten Log-Server per syslog Protokoll möglich). Die Log-Daten können exportiert oder zeit- bzw. volumenabhängig automatisch gelöscht werden.

- Einfache Installation von Updates und Patches über die graphische Oberfläche.
- Reporting: Die Auslastung einzelner Systemparameter wird erfasst und pro Tag, Woche bzw. Monat graphisch dargestellt.
- Die Überwachung der Systemressourcen wird durch SNMP v3 ermöglicht.
- IP Masquerading: Durch die Application Gateway Technologie von *Compumatica* ist Ihr internes Netzwerk von außen unsichtbar.
- Unterstützung für Demilitarisierte Zonen (DMZ): Durch den Einsatz von drei oder mehr Netzwerkinterfaces können beliebige Netzsegmente gebildet werden, um z.B. öffentliche Server zu schützen.
- Integriertes Backup in verschlüsselter Form (AES 256).
- Zeitsynchronisation mit einem beliebigen NTP-Zeitserver.
- Zugriff auf die Kommandozeile per Javascript-ssh-Terminal.
- Einfache Lizenzierung per USB Token; sowohl für temporäre als auch für permanente Lizenzen.
- Die Firewall-Software verfügt über einen minimalen Befehlssatz. Zusätzliche, ggf. zur Administration erforderliche Werkzeuge, werden auf einer separaten CDROM zur Verfügung gestellt.
- Extrem einfache Installation und Konfiguration der initialen Netzwerkeinstellungen.
- LTS Linux Kernel 3.4.x (32-/64-bit Unterstützung).

MANAGEMENT VIA WEB BROWSER

Die *CompuWall* wird über einen Browser administriert. Damit haben Sie die Möglichkeit, einfach und schnell von überall Zugriff auf die Administrationsoberfläche Ihrer Firewall zu erlangen.

Dieser Zugang wird mit Hilfe von SSL-Verschlüsselung (Client-Zertifikat) und zusätzlicher Authentifikation des Administrators abgesichert. Ein unberechtigter Zugriff auf Ihre *CompuWall* ist somit ausgeschlossen!

Nach erfolgreichem Login bietet Ihnen Ihr Browser eine intuitiv und unkompliziert zu bedienende, graphische Benutzeroberfläche. Alle Menüs sind klar und übersichtlich strukturiert, sodass alle Sicherheitsfunktionen komfortabel administriert und überwacht werden können.

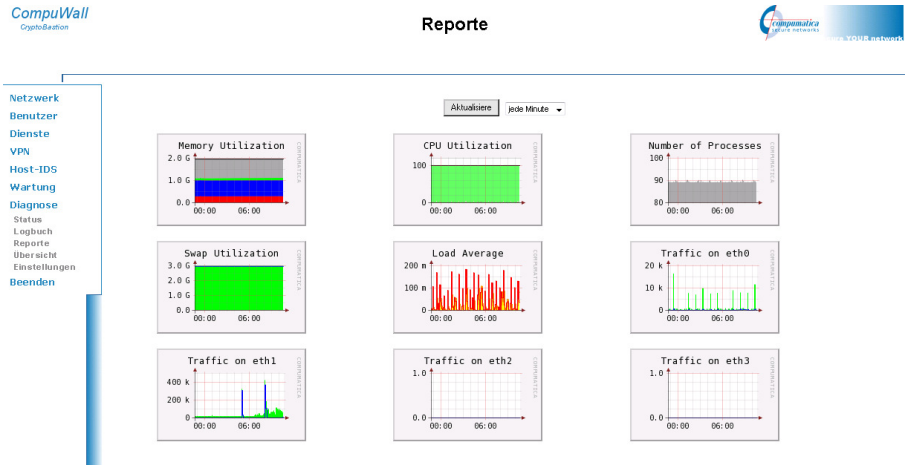
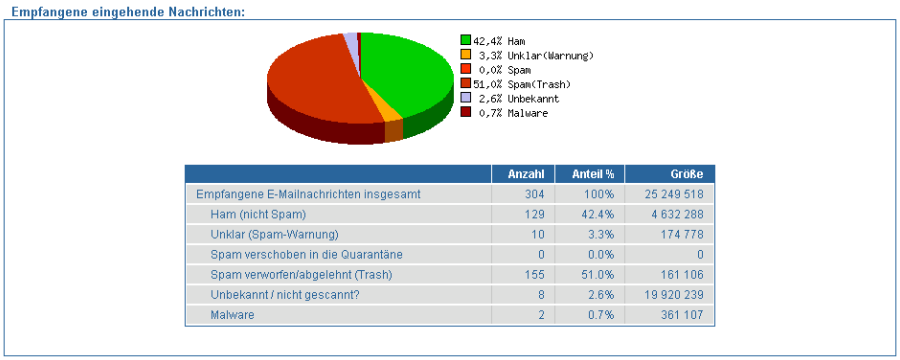


Abbildung 1: Screenshot der *CompuWall*-Benutzeroberfläche



	Anzahl	Anteil %	Größe
Empfangene E-Mailnachrichten insgesamt	304	100%	25 249 518
Ham (nicht Spam)	129	42.4%	4 632 288
Unklar (Spam-Warnung)	10	3.3%	174 778
Spam verschoben in die Quarantäne	0	0.0%	0
Spam verworfen/abgelehnt (Trash)	155	51.0%	161 106
Unbekannt / nicht gescannt?	8	2.6%	19 920 239
Malware	2	0.7%	361 107

Abbildung 2: Screenshot einer *Spam-Statistik*

Ablehnungsstatistik

SMTP-Verbindungen (Incoming)							
604							
Abgelehnt							
Sender IP-Adresse			Sender		Empfänger		
74			95		134		
Regel	DNS	RBL	Regel	DNS	Regel	DNS	RAV
0	0	74	59	36	1	0	133

Empfangene / Übertragene E-Mailnachrichten (Datenvolumen)						
304 (24 657.7 kB)						
Empfang abgelehnt			Angenommene			
155			149			
unvollständig	Malware	Spam (Trash)	Spam	Malware	Unknown	Ham
0	0	155	0	2	18	129

Quarantäne	Gesendete (inbound)
2 (352.6 kB)	149 (24 500.4 kB)

Abbildung 3: Screenshot einer SMTP-*Ablehnungsstatistik*

TECHNISCHE SPEZIFIKATION

CRYPTOBASTION: COMPUWALL

Software / Operating System	Speziell gesichertes und gehärtetes Linux OS, basierend auf Kernel 3.4	
Hardware	Linux-basierende Server-Hardware mit folgender Minimalausstattung: VGA-Grafikkarte, 2 Netzwerkkarten, CDROM/DVD-Laufwerk, Festplatte > 8GB, serielle Schnittstelle, USB-Slot(s)	
Application Gateway	Single- oder Multi-homed	
Netzwerkschnittstellen	Gigabit- und/oder Fast-Ethernet (bis zu 10 Netzwerkkarten), Unterstützung von VLAN-Tagging	
Virtual Private Network	OpenVPN-Zugang mit Benutzer-Zertifikaten und/oder Site-to-Site, IPsec	
Proxies	AntiVIRUS:	HTTP(S), FTP, ESMTP, POP3
	AntiSPAM:	ESMTP, POP3
	transparent oder nicht-transparent:	HTTP(S), FTP, POP3, RTSP, TELNET, NNTP, PING
	nicht-transparent:	HTTPS Decrypter, ESMTP, NET8, MGNTP, DNS
Generische Relays	transparent oder nicht-transparent: TCPR, UDPR doppelt transparent: TCPR, UDPR	
Authentisierungssystem	Local Authentication System: Passwort, Einmal-Passwort (SKey), Mobile Authentication Service (MAS), IDENTD Remote Authentication System: LDAP, RADIUS	
Intrusion Detection	Host Intrusion Detection System mittels AIDE	

Datendurchsatz[1]	httpp[2]	ohne Proxy: ca. 880 Mbps (direkte Verbindung) mit Proxy: ca. 400 Mbps (LS[3]: ca. 700 Mbps) mit SSL: ca. 70 Mbps (LS: ca. 120 Mbps)
	tcpr[4]	ohne Relay: ca. 930 Mbps (direkte Verbindung) mit Relay: ca. 880 Mbps (LS: ca. 920 Mbps)
Hochverfügbarkeit	Jeweils zwei redundante Gateways im Aktiv – Aktiv (Loadsharing) oder Aktiv – Passiv (Hot Standby) Modus, basierend auf Heartbeat Version 2	
Lizenzierung	USB-Token	

[1] Der Durchsatz wurde mit Hilfe folgender Hardwarekomponenten in einem Gigabit-Netzwerk ermittelt: Client: Dual XEON 3.2GHz; Bastion: Quad Core XEON 1.6GHz, 2GB RAM; Server: Dual XEON 3.2GHz

[2] Gemessen im Mixed Mode (Paketgrößen: 0.5kB, 5kB, 50kB, 500kB und 5MB) mit 100 parallelen Client-Threads

[3] LS bezeichnet hier den Loadsharing Modus über zwei Gateways mit identischen Hardwarespezifikationen

[4] Gemessen 2007 mittels iperf -P100 (Anzahl paralleler Client-Threads)

COMPUWALL – ANWENDUNGSBEISPIELE

Die *CompuWall* eignet sich besonders für folgende Anwendungen:

- Anbindung kleiner und mittlerer Organisationen an das Internet
- Anbindung von Filialen oder Tochterunternehmen an zentrale Firmennetze
- Absicherung von Teilbereichen in großen Netzen
- Spezielle Anbindungen an bestehende Netze (z.B. Remote Access) und Mobilfunkgeräte

ANBINDUNG AN DAS INTERNET

Dies ist die Kernanwendung von Firewallsystemen. Hier ist die *CompuWall* auf kleine und mittlere Netze zugeschnitten. Sie integriert alle notwendigen Funktionen in einem Gerät und lässt sich leicht von einem beliebigen PC administrieren.

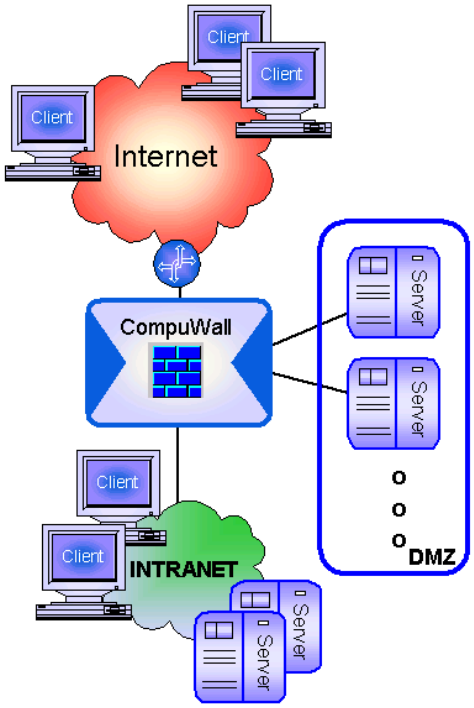


Abbildung 4: Anbindung der *CompuWall* an das Internet

ANBINDUNG VON FILIALEN AN EIN ZENTRALES FIRMENNETZ

Viele Organisationen verfügen bereits über eine zentrale Enterprise Firewall und möchten nun ihre Zweigniederlassungen an die Zentrale anbinden. Zu diesem Zweck benötigt man eine sichere und überschaubare Firewalllösung.

Die Hersteller von Enterprise Firewalls preisen zwar an, dass man mit ihren Produkten die Firewalls der Zweigniederlassungen mitverwalten kann. Dies ist aber oft in der Praxis nicht umsetzbar – z.B. wenn die Zweigniederlassung eine eigenständige Netzwerkadministration hat.

In diesen Fällen ist die *CompuWall* die ideale Wahl für die Zweigniederlassung.

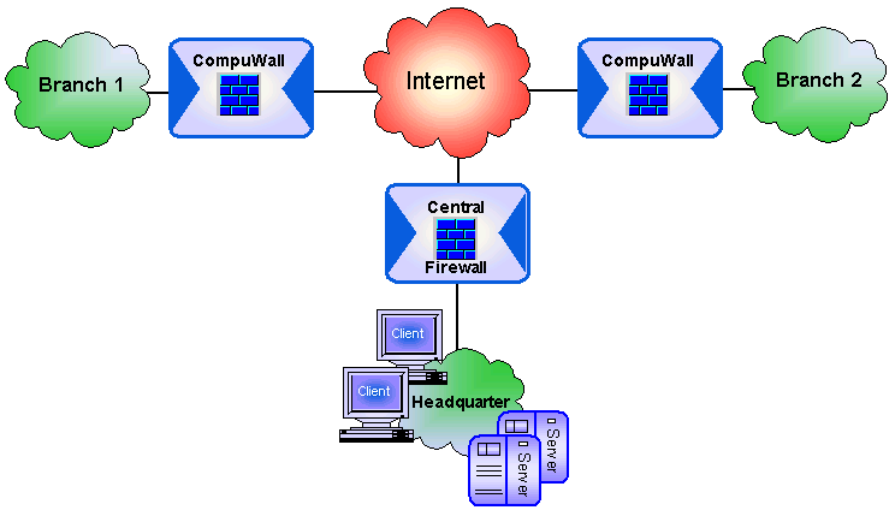


Abbildung 5: Anbindung von Filialen an ein zentrales Firmennetz

ABSICHERUNG VON ABTEILUNGSNETZEN

Viele Organisationen haben bereits eine zentrale Enterprise Firewall und wollen nun bestimmte interne Abteilungen wie z.B. Vorstand oder Personalabteilung innerhalb ihres internen Netzes schützen. Hierfür kann die zentrale Firewall nicht verwendet werden, da sie das gesamte Firmennetz physikalisch vom Internet trennt, nicht aber das Netz des Vorstandes vom restlichen Firmennetz.

Für die Absicherung des Vorstandsnetzes gegenüber dem restlichen Firmennetz reicht eine kleine Firewall, die einfach zu administrieren ist. Die *CompuWall* ist hierfür die optimale Wahl.

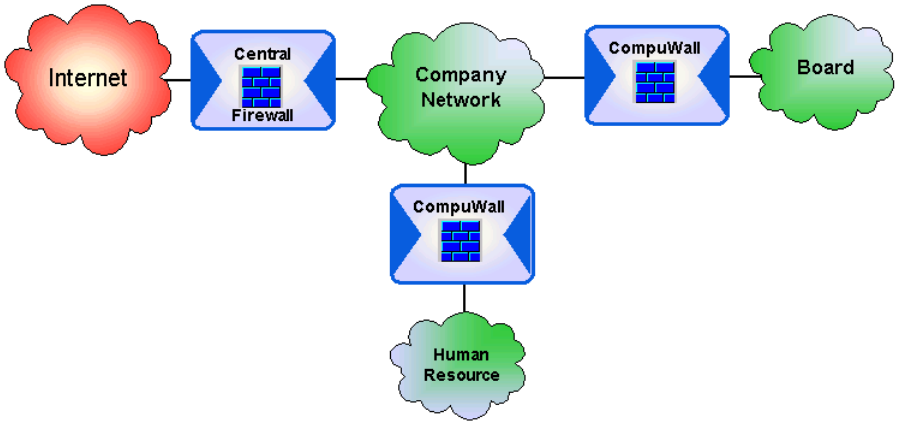


Abbildung 6: Absicherung eines Abteilungsnetzes mit Hilfe der *CompuWall*

ABSICHERUNG VON REMOTE-ZUGÄNGEN

Nicht immer bietet die zentrale Enterprise Firewall die notwendige Flexibilität, um dort einen Remote-Zugang aus einem externen Netz zu realisieren. Getrennte Verantwortlichkeiten innerhalb einer Organisation können eine weitere Ursache sein, warum ein solcher Zugang separat abgesichert werden muss.

Hierfür bietet sich die *CompuWall* als eigenständige Lösung mit hohem Sicherheitsstandard an.

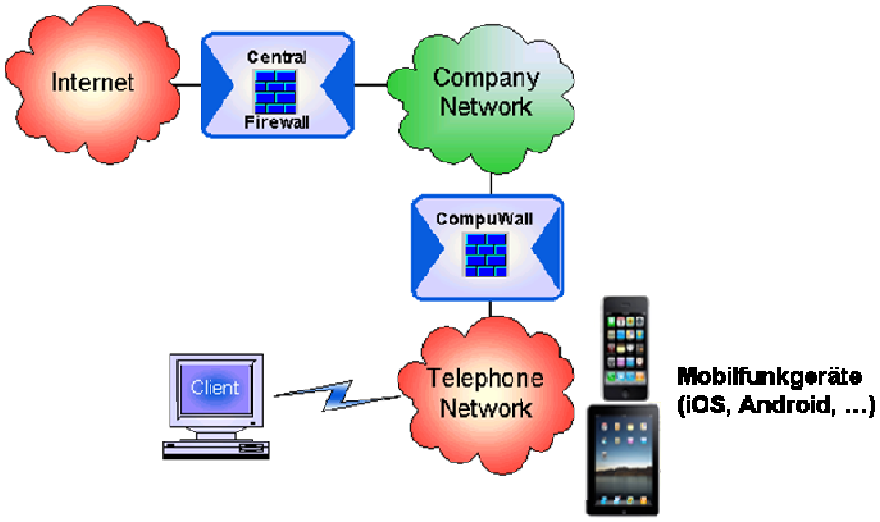


Abbildung 7: Absicherung von Remote-Zugängen mit Hilfe der *CompuWall*

VORTEILE DER *COMPUWALL*

Maximale Sicherheit und maximaler Schutz, Turn-Key-Solution, XTM

- Wir bieten Ihnen eine umfassende, an Ihr Sicherheitskonzept angepasste Firewall-Umgebung (XTM – eXtended Unified Threat Managament mit AntiVIRUS, AntiSPAM und Host-IDS).
- Keine Sicherheitsrisiken durch eine fehlerhafte Konfiguration des Betriebssystems. Die Routingfunktionalität wurde aus dem Betriebssystemkernel entfernt:
  Keine virtuelle, sondern reale Netztrennung!
- Optional kann das *CompuWall*-System durch zertifizierte *CryptoGuard VPN* Geräte erweitert werden. Diese Erweiterung bietet Ihnen die zusätzliche Möglichkeit der Paketfilterung auf verschiedenen Netzwerkebenen und zudem sichere und schnelle Verschlüsselung der Datenpakete zwischen verschiedenen Standorten.

Hohe Performance, Stabilität, Hochverfügbarkeit

- Die Optimierung der Firewall-Software garantiert einen sehr hohen Datendurchsatz der Proxies auf Applikationsebene.
- Die *CryptoBastions*-Software, egal ob als *CompuWall* oder *CryptoWall*, gilt als praxiserprobt und überzeugt durch langjährige Stabilität und Zuverlässigkeit.
- Die integrierte Hochverfügbarkeitslösung kann auf die speziellen Anforderungen der jeweiligen Systemumgebung angepasst werden.
- Keine Lizenzbeschränkung im Hinblick auf die Anzahl der Benutzer oder Netzwerkverbindungen.
- Keine zusätzlichen Kosten für das Betriebssystem und andere Softwarekomponenten.

Flexibel, modular, zukunftsorientiert

- Die *CompuWall*-Lösung wurde modular designed und kann somit einfach in eine bestehende Netzwerkstruktur integriert werden.
- Änderungen der Topologie oder der Regelstrukturen können schnell und einfach nachvollzogen werden.
- Die voranschreitende Entwicklung neuer Features, die RFC-Konformität der Dienste und die ständige Aktualisierung der Betriebssystemparameter garantieren Ihnen, dass Ihr Sicherheitssystem stets auf dem letzten Stand der Technik ist.

Einfache, benutzerfreundliche Handhabung

- Die *CompuWall* besteht aus einem gehärteten Betriebssystem, der eigentlichen Firewall-Software und dem integrierten Management.

Zertifizierung

- Die Zertifizierung „Departementaal Vertrouwelijk“ wurde durch das NLNCSA erteilt.

CYBERSECURITY WITH A PERSONAL TOUCH

Sie können die *CompuWall* als eine fertig installierte Komplettlösung oder nur die Software von uns oder einem unserer Vertriebspartner erwerben.

Als erfahrener Anbieter von IT-Sicherheitslösungen bieten wir Ihnen ein durchdachtes und umfassendes Sicherheitskonzept, welches wir in Absprache mit Ihnen auf Ihre Sicherheitsansprüche und Ihre Security Policy zuschneiden werden.

BERATUNG IST EIN WICHTIGER BESTANDTEIL!

Wir bieten ein breites Spektrum an Dienstleistungen und Unterstützung:

- Sicherheitsstudien, Workshops
- Beratung und Konzepte
- Lieferung von Hardware und Software
- Installation
- Inbetriebnahme
- Schulung
- Wartungsverträge

Wählen Sie aus diesem Angebot die für Sie passende Lösung!

Wenn Sie weitere Informationen über die Produkte und Dienstleistungen der *Compumatica secure networks* erhalten möchten, nehmen Sie bitte Kontakt mit uns auf.

WEITERE INFORMATIONEN

KURZPROFIL:

Compumatica secure networks – zuhause in Deutschland und den Niederlanden – ist ein unabhängiges, inhabergeführtes Unternehmen, das sich ganz der Absicherung des IP-Datenverkehrs seiner Kunden verschrieben hat.

Compumatica entwickelt, produziert und implementiert Sicherheitslösungen auf höchstem Niveau für alle Arten von IP-Netzwerken und Kunden. Unsere Kunden sind sowohl kleine Organisationen mit nur wenigen inländischen Standorten, als auch internationale Unternehmen mit weltweiten Netzwerken.

Compumatica-Mitarbeiter und -Produkte erfüllen höchstmögliche Anforderungen an Zuverlässigkeit und Qualität. Die Produkte basieren auf Systemen, die nach den strengen Vorschriften des BSI (in Deutschland) und der NLNCSA (in den Niederlanden) zugelassen oder sogar zertifiziert sind. Jedes einzelne System durchläuft eine Qualitätssicherungsphase, in der es einem Langzeittest unterzogen wird. Alle *Compumatica*-Produkte sind abwärtskompatibel für zehn und mehr Jahre. Dadurch garantieren wir unseren Kunden Investitionssicherheit.

Zur Produktpalette gehören weiterhin die Geräte unserer Tochterfirma *.vantronix secure systems*, die eine einzigartige Kombination aus IPv4-IPv6-Gateway, Router, Firewall, netzwerkbasiertem Anti-Spam sowie Load Balancer basierend auf OpenBSD enthalten. *.vantronix* ist ein HP AllianceOne Partner. Der gesamte Software-Umfang ist daher auf HP-Systemen verfügbar.

Im Bereich der Mobilfunkkommunikation wird unser Angebot ergänzt durch ein umfassendes Secure Mobile Concept, das Sprachkommunikation und SMS sichert und auf die unterschiedlichen Bedürfnisse und Anforderungen der Kunden angepasst werden kann.

Unsere Kunden sind sowohl bekannte Top 500 Unternehmen, als auch Regierungsbehörden und staatliche Organisationen in verschiedenen Ländern, die mit Hilfe von *Compumatica*-Systemen ihre kritischen Daten schützen.

Als weltweit anerkannter Hersteller und Systemintegrator liefert Compumatica secure networks komplette IT-Sicherheitslösungen für Netzwerke jeder Größe.

Die Sicherheit Ihrer Daten ist unser Auftrag – *Cybersecurity with a personal touch*.

KONTAKTDATEN

Niederlande:

Compumatica secure networks BV
Oude Udenseweg 29

5405 PD Uden

Telefon +31 (0)413 334668
Fax +31 (0)413 334669

www.compumatica.com

Deutschland:

Compumatica secure networks GmbH
Monnetstraße 9

52146 Würselen

Telefon +49 (0)2405 89 24 400
Fax +49 (0)2405 89 24 410

www.compumatica.com