

The logo features the word "FORTINET" in a bold, black, sans-serif font. The letter "O" is replaced by a red square icon with a white grid pattern. A registered trademark symbol (®) is located at the end of the word.

**FORTINET®**

Real Time Network Protection

## Inhalt

Umfassende Sicherheitslösungen .....	02
Fortinet Security – Das Konzept .....	03
Das ist Fortinet .....	03
FortiGate Produktfamilie (Übersicht) .....	04
<b>FortiGate</b> .....	04
Fortinet Firewall .....	05
Fortinet VPN .....	06-07
Fortinet IPS .....	07-08
Fortinet AntiVirus .....	08
Fortinet AntiSpam .....	08
Fortinet WebFiltering .....	09-10
Fortinet Wireless LAN Security .....	10-11
Fortinet Voice Over IP .....	12
Application Control .....	12-13
Data Leakage Prevention .....	13
WAN-Optimierung .....	13
SSL-Inspection .....	13
Virtualisierung von IT-Sicherheit .....	14
Fortinet für KMU und Mittelstand .....	15
Fortinet in Enterprise-Umgebungen .....	15-16
Fortinet für Carrier .....	17
<b>Technische Daten</b> .....	18-19
FortiWiFi Voice-80C .....	20
FortiAP-220A .....	21
FortiMail™ – Email Security .....	22
FortiAnalyzer – zentralisiertes Reporting .....	22
FortiManager – zentralisiertes Management .....	23
FortiClient – Endpoint Security .....	23
FortClient Host Security .....	24
FortiDB – Datenbank Security .....	24-25
FortiWeb – Applikation Firewall .....	25
FortiScan – Vulnerability Management .....	25
FortiSwitch .....	26
Ihr Vorteil: Das Wick Hill Service Programm .....	27
UTM Marktführerschaft · Industrie Zertifizierungen · Industrie Auszeichnungen · Kontakt .....	28

## Umfassende Sicherheitslösungen

*Fortinets vielfach ausgezeichnete FortiGate™ Serie mit ASIC-beschleunigtem Unified Threat Management (UTM) Netzwerksicherheitssystem schützt kosteneffizient gegen aktuelle und entstehende Netzwerk- und Content Level Bedrohungen.*

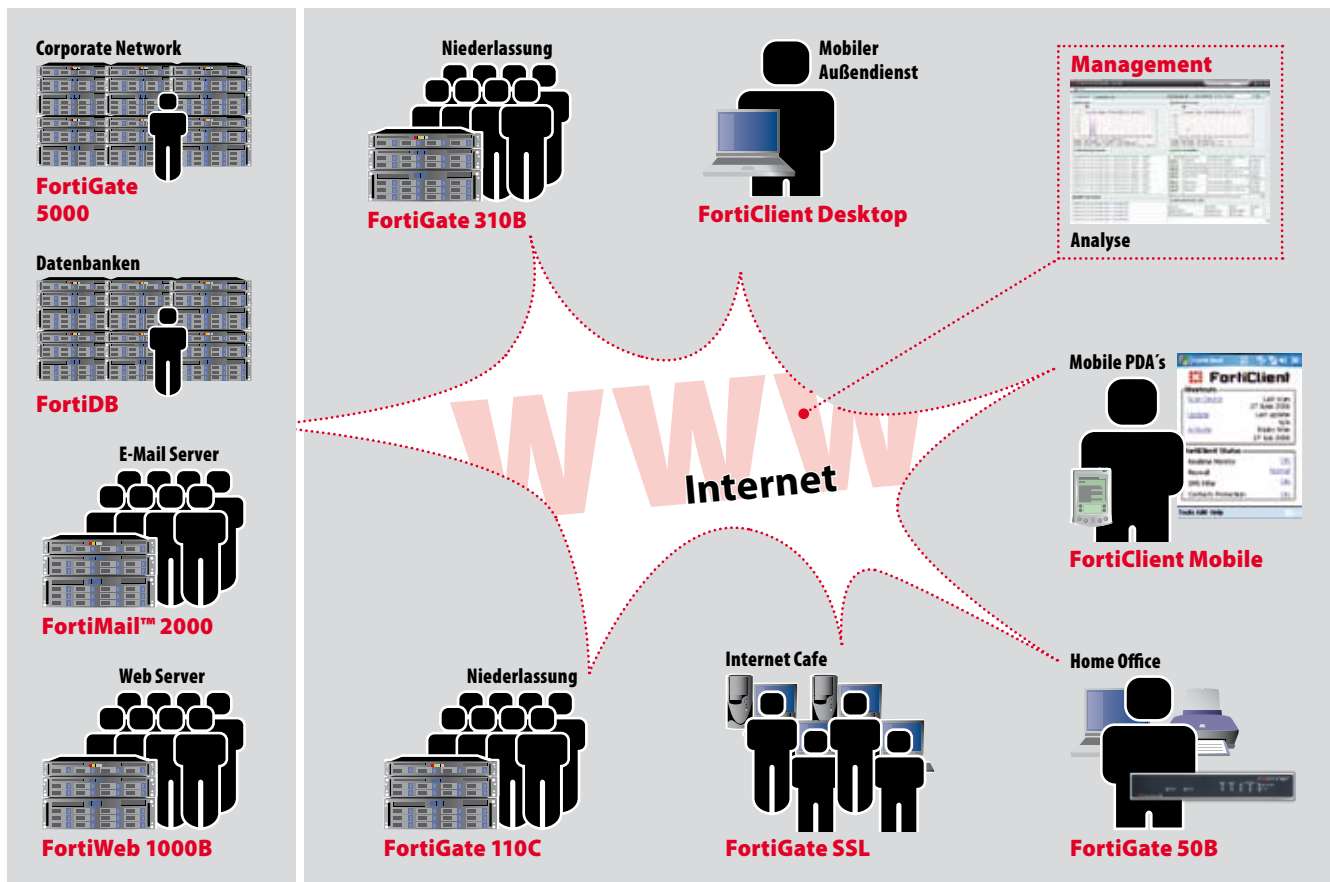
*FortiGate Lösungen ermitteln und eliminieren komplexe Sicherheitsbedrohungen wie Viren, Würmer, Trojaner, unpassenden Web-Content und ähnliche Bedrohungen in Echtzeit ohne die Leistung des Netzwerks zu beeinträchtigen.*

Fortinet bietet eine umfassende Palette mit voll integrierten Sicherheits- und Netzwerkfunktionen, einschließlich Antivirus-Systemen, Anti-Spyware, Firewall, Virtual Private Networking (VPN), Intrusion Detection & Prevention (IDP), Web-Filtering, Anti-Spam und Traffic-Optimierung. Neben den FortiGate Netzwerklösungen bietet Fortinet auch FortiMail™ eMail-Messaging-Sicherheitsanwendungen und FortiClient™ Endpoint Security Software für Personal Computer und mobile Smartphones.

FortiManager™ und FortiAnalyzer™ Lösungen ermöglichen voll integriertes zentralisiertes Management, Erfassung und Reporting bei allen Produkten. FortiDB™ ist für die Datenbanksicherheit verantwortlich und mit FortiWeb™ werden Webapplikationen geschützt. FortiScan™ bietet Vulnerability und Patch Management und unterstützt Unternehmen beim Erfüllen von Compliancevorgaben.

FortiGuard™ Subscription Dienste werden von einem weltweit operierenden Team aus Security-Spezialisten gewährleistet, das rasche Lösungen als Reaktion auf aktuelle und entstehende Sicherheitsbedrohungen entwickelt; Echtzeit-Updates für Antivirus, Anti-Spyware, Intrusion Prevention, Web-Filtering und Anti-Spam werden automatisch mittels dem globalen Verteilungsnetzwerk an die Fortinet-Produkte gepusht.

## Fortinet Security – Das Konzept



## Das ist Fortinet

Fortinet wurde im Jahre 2000 von Ken Xie, dem Gründer und früheren CEO von NetScreen, gegründet. Ken hat es sich zum Ziel gesetzt, Echtzeit-Sicherheitslösungen für Netzwerke zu entwickeln. Heute hat Fortinet dieses Ziel durch die Entwicklung einer eigenen ASIC-Architektur erreicht und wird von führenden Marktanalysten wie Gartner als die Firma mit dem größten Potential für die Zukunft angesehen.

Fortinet entwickelt Multi-Threat-Sicherheitssysteme für Unternehmen und Service-Provider. Die Lösungen umfassen Applikationen wie Firewall, Antivirus, Intrusion Prevention, VPN und Anti-Spyware bis hin zu Anti-Spam. Mit dieser Kombination, die komplett oder in Auswahl implementiert werden kann, schützen die Appliances vor bekannten Bedrohungen ebenso wie vor bisher nicht analysierten, versteckten Angriffen. Der ASIC beschleunigt die Geräte, die sich für Unternehmen und Niederlassungen jeglicher Größe eignen. Die Lösungen von Fortinet haben weltweit Preise errungen und wurden als einzige Sicherheitsprodukte bereits acht mal durch die ICSA in den Kategorien Firewall, Antivirus, IPSec, SSL, IPS, Anti virus auf Client-Ebene, Cleaning und Anti-Spyware ausgezeichnet.

Alle FortiGate Antivirus Firewalls basieren auf dem zur Zeit einzigartigen FortiASIC™ Content Processing Chip und dem leistungsfähigen und sicheren FortiOS™ Betriebssystem. Diese ASIC-basierte Architektur analysiert Netzwerk Inhalte in Echtzeit, und hält somit Gefahren direkt am Eingang zum Firmennetzwerk ab. FortiGate Systeme sind weltweit die einzigen, die von der ICSA für Antivirus, IPSec, Firewall and Intrusion Detection zertifiziert sind und bieten so den höchsten Grad an verfügbarer Sicherheit. Fortinet Firewalls werden häufig auch komplementär zu anderen Firewalls im Transparent-Modus eingesetzt und sorgen so in bereits bestehenden Sicherheitsarchitekturen für zusätzliche Absicherung.

### Warum Fortinet?

- einheitliche Benutzeroberfläche und zentrales Management
- unlimitierte Benutzeranzahl (einfachstes Lizenzmodell)
- ASIC Prozessoren die Ihr Netzwerk in Echtzeit schützen (keine Performanceverlust)
- Mehr als 500 Techniker weltweit die ständig für neu auftkommende Viren, Angriffe, Spam etc. Patches schreiben um Ihr Netzwerk permanent zu schützen
- Hardware, Software und Services sind ausschließlich Eigenentwicklungen von Fortinet (keine Dritthersteller)
- Bedrohungsszenarien richten sich nicht nach Unternehmensgrößen, deshalb bieten alle FortiGates denselben Funktionsumfang und eine einheitliche Bedienungs Oberfläche

## FortiGate Produktfamilie

Integration in Security-Gesamtkonzept  
nur ein Management  
nur eine GUI

UTM und Virtual Security für alle  
Unternehmensgrößen identische  
Technologie auf allen FortiGates

Performance, Ports, Features



FG 5140



FG 5050



FG 5020



FG 3810A



FG 3016B



FG 1240B



FG 620B



FG 310B



FG 110C



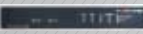
FG 200B



FG 80C



FG 60C\*



FG 50B



FG 30B

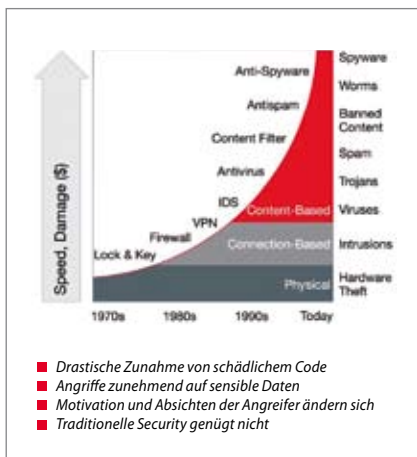
Enterprise

Mittelstand  
SME

\* verfügbar ab  
voraussichtlich  
Q2/2010

SMB | SOHO

Unternehmensgröße



## FortiGate



FORTINET bietet mit den Produktfamilie „FortiGate“ eine ganze Palette von mehrfach ausgezeichneten Appliances für den Schutz Ihres Netzwerks. Die FortiGate Systeme schützen Ihre Daten zuverlässig vor Netzwerk- und Contentlevel basierten Bedrohungen. Hier spielen die selbstentwickelten ASIC Prozessoren eine große Rolle, die die Dienste und Sicherheitsfunktionen der FortiGate enorm beschleunigen können. Somit lassen sich Bedrohungen durch Viren, Würmer, Exploits, Spyware effektiv bekämpfen - und das in Echtzeit! Weitere Funktionen wie URL-Kategoriefilter, IPSec- und SSL-VPN, Bandbreiten-steuerung und selbstverständlich eine marktführende Firewall sind fest integrierter Bestandteil aller FortiGate Appliances die nicht per Benutzer lizenziert werden.

Bedrohungsszenarien richten sich nicht nach Unternehmensgrößen, und so bieten alle FortiGate Appliances denselben Funktionsumfang und dieselbe Bedienung per grafischer Oberfläche oder CLI (command line Interface).

Auch kleinere Unternehmen profitieren so von FORTINETs Erfahrung aus Großprojekten und lassen sich bei sehr gutem Preis-Leistungsverhältnis mit einem hervorragenden Schutz bei außergewöhnlicher Flexibilität absichern.

## FortiGate Funktionen:



Firewall (Details dazu Seite 05)



Wireless LAN Security (Details dazu Seite 10)



VPN (Details dazu Seite 06)



Voice over IP (Details dazu Seite 12)



IPS/IDP (Details dazu Seite 07)



Application Control (Details dazu Seite 12)



AntiVirus (Details dazu Seite 08)



Data Leakage Protection (Details dazu Seite 13)



AntiSpam (Details dazu Seite 08)



WAN-Optimierung (Details dazu Seite 13)



Webfiltering (Details dazu Seite 09)



SSL Inspection (Details dazu Seite 13)



## Fortinet Firewall



Die branchenführenden FortiGate Security Systeme von Fortinet bieten unerreichte integrierte Security-Ressourcen, Benutzerfreundlichkeit und ein optimales Preis-Leistungsverhältnis. Zusammen mit der zustandsorientierten Firewall verwendet das FortiGate System eine Vielzahl an integrierten Sicherheitsmechanismen, um so aktuelle, komplexe Angriffe, wie SoBig und Netsky, zu identifizieren und daran zu hindern, dass sie die zu schützenden Netzwerke infizieren. Hinzu kommt, dass Fortinets skalierbare Produktreihe FortiGate-Modelle anbietet, um jede Netzwerkgröße mit wichtigen Security Leistungsmerkmalen auszustatten, wie Stateful Firewall, VPN, Anti-Virus, IPS, Web Content Filtering, Anti-Spam und Traffic Shaping, die bei allen Modellen zur Verfügung stehen.

### MSSP Managed Firewall Service

MSSPs konzentrieren sich vermehrt auf Fortinets branchenführende FortiGate Security Systeme für eine effiziente und kostengünstige Bereitstellung von integrierten Security-Diensten für Kunden. Fortinets Security-Zonen und Virtual Domains bieten eine perfekte Plattform, auf der ein verwalteter Security-Dienst entwickelt werden kann. Mit dem zentralisierten Management von Fortinets FortiManager und dem zentralisierten Reporting Server von Fortinets FortiAnalyzer™ können MSSPs jetzt ihre Instandhaltungs- und Bereitstellungskosten reduzieren, indem sie ein einziges Bedienfeld für die Verwaltung und die unkomplizierte Implementierung von Tausenden von FortiGate Systemen verwenden.

### SOHO DSL/Kabel Implementierung

Fortinets unkompliziert zu implementierenden und zu verwaltenden Sicherheitssysteme bieten außergewöhnlichen Wert und Performance für die Sicherung eines Netzwerkes im Home Office- und Kleinunternehmensbereich. FortiGate Installationsassistenten ermöglichen Installationen, die innerhalb von wenigen Minuten vorgenommen und in Betrieb genommen werden können. ►

### Die wichtigsten Leistungsmerkmale der Firewall:

- ASIC-beschleunigte Hardware und speziell entwickeltes sicheres OS
- Security auf Anwendungsebene
- virtuelle Security Domains und Security-Zonen
- unternehmensgetestete hohe Verfügbarkeit
- Security-Zonen und standardbasierte Konfiguration
- VoIP-fähige Gateways unterstützen H.323, SIP und SCCP Protokolle
- Dynamische Routing-Protokolle; RIP, OSPF, BGP und PIM
- Detaillierte Erfassung und Reporting

## Firewall für Unternehmen und dezentrale Niederlassungen

FortiGate Firewalls erfüllen die Anforderungen von Unternehmen hinsichtlich Skalierbarkeit, Performance und Zuverlässigkeit. Optimierte Security Ressourcen, wie integriertes Anti-Virus, IPS Anti-Spam und URL Filtering, hohe Verfügbarkeit, Wire-Speed-Performance und Security-Zonen sind in allen FortiGate-Modellen verfügbar. Darüber hinaus bietet Fortinets breite Palette an FortiGate-Modellen ein Modul, das sich an jede Netzwerkgröße anpasst, während Fortinets FortiManager™ System eine einzige Schnittstelle für das zentrale Management und die einfache Implementierung von Hunderten von FortiGate-Systemen vorsieht.

## Implementierungen für Einzelhandelsunternehmen mit Multi-Speicherung

**FortiGate Sicherheitssysteme** bieten Einzelhandelskunden eine kosteneffiziente Lösung, die ihre speziellen Geschäftsanforderungen erfüllen, und war mittels der Sicherung von Anwendungen wie POS (Point of Sale), Bestandsanwendungen und Online-Finanztransaktionen, während Fortinets ASIC-basierendes, speziell entwickeltes Design die Zuverlässigkeit und Anwendungssicherheit bietet, die Einzelhandelsunternehmen benötigen, um kostenintensive Netzwerkausfallzeiten zu vermeiden. Darüber hinaus bieten alle FortiGate Modelle ein Modul, das sich an jede Netzwerkgröße anpasst, während der FortiManager ein einzige Schnittstelle für das zentrale FortiGate System vorsieht, die Verwaltung und den Schutz mehrerer Standorte in eine betriebsbereite Lösung.

### Die wichtigsten Leistungsmerkmale von VPN:

- ASIC-beschleunigtes VPN
- IKE: Pre-shared Key, X.509 Certs, Manual Keys
- intensive Anwenderauthentifizierung, RADIUS, LDAP, Local Database, SecureID, X-Auth Support für IPSec Clients
- IPSec, SSL, L2TP, und PPTP
- VPN content inspection - Antivirus, IPS, URL Filtering
- Hub-and-spoke Konfiguration
- FIPS 140-2 Zertifizierung
- Traffic-Modellierung misst dem Traffic mittels VPNs eine höhere Priorität bei.



## Fortinet VPN

SW

Fortinets optimierte VPN Lösungen erfüllen die Anforderungen bezüglich Preis-Leistungsverhältnis von Unternehmen jeder Größe. Fortinets VPN bietet sichere und kostengünstige Alternativen zu teuren Frame-Relais-Kreisläufen mit Niedrigbandbreite für die Verbindung von mehreren Niederlassungen im offenen Internet. Das zentralisierte VPN Management von FortiManager™ bietet die Möglichkeit, Hunderte von FortiGate Systemen von einem einzigen Bedienfeld aus zu verwalten. In enger Verknüpfung mit Fortinets Anwendungssicherheitschutz, Firewall, Anti-Virus, Web Filtering und IPS bietet Fortinet die sicherste VPN Lösung, die heute auf dem Markt erhältlich ist.

## VPN für dezentrale Niederlassungen des Unternehmens und Partner-Extranet

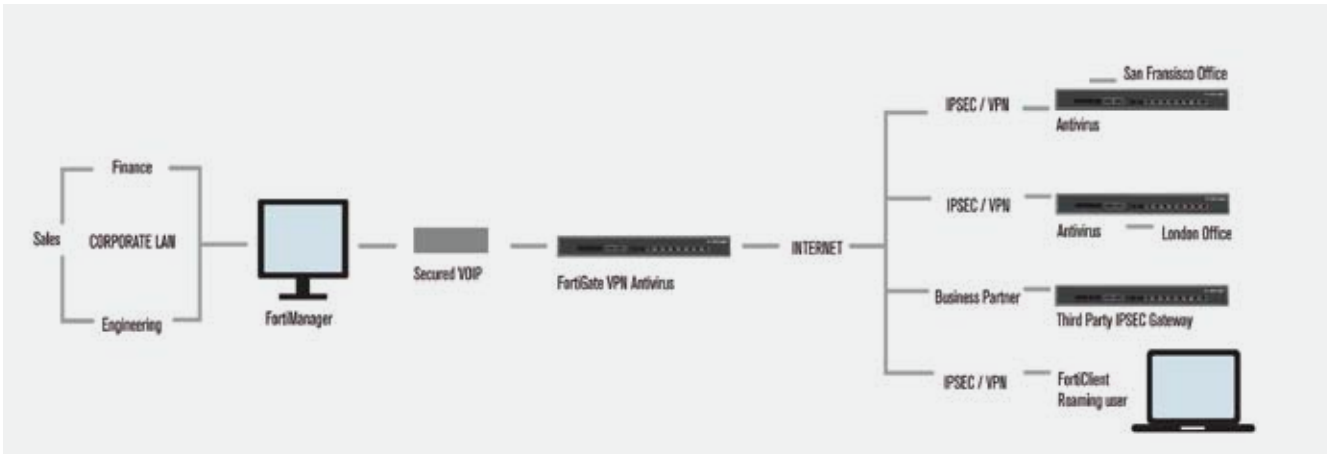
Bei einer parallelen Implementierung zu einer bestehenden Firewall beendet ein FortiGate VPN Gateway VPNs von dezentralen Niederlassungen und Extranet-Partnern, die einen begrenzten Zugang zu DMZ-Servern fordern. Dank der in den FortiGate Systemen integrierten Sicherheitsmerkmale kann der Administrator präzise umrissene Sicherheitsstandards konfigurieren und so den Zugang auf Ressourcen im gemeinsamen LAN und DMZ kontrollieren.

## Hub-and-Spoke VPN für Unternehmen

Hub-and-Spoke VPN Konfigurationen ermöglichen, dass mehrere Fernstandorte miteinander verbunden werden können, ohne dass dabei spezielle Verbindungen für jeden Standort notwendig sind. Eine ideale Anwendung für diese Konzeption ist, den VoIP-Traffic über VPNs zu transportieren, um so die Gebühren für Ferngespräche zu verringern. Fortinets Traffic-Modellierungs-Funktionen ermöglichen, dass VoIP-Traffic Priorität auch bei einer VPN Verbindung erhält.

## Remote Access (IPSec und SSL) für Unternehmen

Ideal für Roaming-Nutzer, wie dezentrales Verkaufspersonal, das Zugriff auf Ressourcen des gemeinsamen LAN, wie E-Mail- und Intranet-Ressourcen, benötigt. Fortinet bietet sowohl sicheren IPSec Client (FortiClient™) als auch Client-freien SSL VPN für wichtigen Zugriff auf Bereiche, in denen IPSec durch eine Firewall blockiert sein könnte. Strenge Authentifizierung ist zwingend, damit Anwender sichere VPN Sitzungen einrichten können.



### MSSP: Virenfrei verwalteter VPN Service

Um von Fortinets integriertem Anti-Virusschutz zu profitieren, können MSSPs den branchenweit sichersten VPN Dienst bereitstellen, indem sie Fortinets optimierte Anti-Virusmaschine aktivieren, um eingehenden und ausgehenden VPN Traffic zu blockieren, der Viren, Würmer, Trojaner, Spyware und anderen schädlichen Content enthält, um den Ausbruch von Viren zu vermeiden, welche sich von Niederlassung zu Niederlassung verbreiten. Ein weiteres Plus ist, dass Fortinets flexible VPN Architektur die Interoperabilität mit den meisten IPSec VPN Gateways zulässt. Unabhängig vom VPN CPE, den der Kunde verwendet, gewährleistet das im Kern implementierte FortiGate System virenfreien VPN Traffic.



## Fortinet IPS



Fortinet bietet eine skalierbare und leicht zu implementierende Reihe von FortiGate IPS Security Systemen, die nahtlos am Netzwerkrand installiert oder als eine IPS-Lösung im Zentrum des Netzwerks implementiert werden kann, um so elementare Unternehmensanwendungen vor externen sowie internen Angriffen zu schützen. Darüber hinaus können Security-Administratoren mit den SOHO- und SME FortiGate-Modellen von Fortinet jetzt kosteneffizient das gleiche IPS-Schutzniveau in dezentralen Niederlassungen implementieren, welches in der Vergangenheit nur für den Hauptsitz des Unternehmens zur Verfügung stand. Durch die enge Integration von branchenführenden Security-Technologien, IPS, Anti-Virus, Anti-Spam, Web Filtering, VPN und Stateful Firewall bietet Fortinet unerreichte Sicherheit für Unternehmen und Service Provider zur Bekämpfung von komplexen gemischten Bedrohungen, bei denen mehrere Methoden angewendet werden, um Hosts zu infizieren und sich selbst auszubreiten.

### IPS-Implementierung

Das FortiGate™ IPS System, das zusammen mit einer bestehenden Firewall installiert wird, wird in den Traffic-Pfad implementiert, der eingehende und ausgehende Pakete nach schädlichem und missgebildetem Content durchforstet. Die hochpräzise IPS-Maschine und die hochverfügbare (HA) Konfiguration des FortiGate Systems gewährleistet maximale Verfügbarkeit der Netzwerkressourcen.

### IPS im zentralen Netzwerkbereich und für dezentrale Niederlassungen

**Fortinets flexible Architektur** und skalierbare Produktreihe berücksichtigt Implementierungen im zentralen Netzwerkbereich zum Schutz vor externen und internen Angriffen, wohingegen die umfangreiche Produktreihe des FortiGate Systems Security-Administratoren in die Lage versetzt, kosteneffizient IPS-Schutz in kleineren dezentralen Niederlassungen zu implementieren. FortiManager™ zentralisiertes Management bietet eine einzige Bedienfeld-Schnittstelle zur Verwaltung von Tausenden von FortiGate Systemen.

#### Die wichtigsten Leistungsmerkmale von IPS:

- ASIC-basierte Hardware-Entwicklung für Multi-Gigabit Durchsatz
- Automatische Updates für IPS Signaturen und Scanning-Maschinen
- benutzerdefinierte Kunden-IPS-Signaturen
- Prüfung von VPN (IPSec und SSL) Content
- bi-direktionales IPS Content Filtering
- Signatur- und Protokoll-Anomalie-Maschinen
- Detaillierte Erfassung und Reporting
- Unterstützung von mehr als 50 Protokollen und Anwendungen

### Die wichtigsten Leistungsmerkmale von AntiVirus:

- skalierbare Performance und Modelle von SOHO für Multi-Gigabit, Anti-Virus Schutz
- ASIC-basierte Hardwareentwicklung
- automatische Updates von Anti-Virus-Signaturen
- prüft SMTP, POP3, IMAP, FTP, HTTP und Instant Messenger Protokolle
- Prüfung von VPN (IPSec und SSL) Content
- bi-direktionales Content Filtering
- komprimierter Dateiformat-Support: tar, gzip, rar, lzh, iha, cab, arj, zip, bzip2, upx, msc, fsg, und aspack
- zentralisiertes Management und Reporting für Hunderte von FortiGate-Systemen
- implementiert in Transparent, NAT und Route-Modi



## Fortinet AntiVirus

**SW**

Fortinets optimierte Anti-Virus-Technologie verwendet eine Kombination aus Signatur- und heuristischen Detektionsmodulen und bietet so vielschichtigen Echtzeitschutz gegen zahlreiche Angriffsformen auf den Desktop und das Netzwerk-Gateway. Extrem hohe System-Performance wird durch die Verwendung des integrierten FortiASIC Content-Prozessors (CP) zusammen mit Fortinets patentierter Technologie, bekannt unter der Bezeichnung CPRL oder Content Pattern Recognition Language, erreicht, die dem beschleunigten Scannen von Virusdateien und der Heuristik/Anomalie-Erkennung dienen.

### MSSP Core Network Security

Wird im Kernbereich von Großunternehmen oder Service Providern implementiert, um in E-Mails, im Web und im FTP Traffic enthaltene Viren daran zu hindern, in das Netzwerk einzudringen oder es zu verlassen. Die Nutzung von standardbasiertem Routing oder Content-Switching kann eine messbare Multi-Gigabit-Performance bieten, indem ein bestimmter Traffic für ein erweitertes Scanning an eine FortiGate Sicherheitsanwendung umgeleitet wird. Eine solche Konfiguration eliminiert zudem viele interne Implementierungsprobleme.

### DMZ Schutz

Wird implementiert, um offenes Internet, FTP- und E-Mail-Server, die in DMZ-Segmenten Ihrer bestehenden Firewall implementiert sind, zu schützen. Fortinets Advanced Anti-Virus-Technologie ermittelt und blockiert Virusinfektionen zu einem Bruchteil der Kosten einer herkömmlichen Server-Software, ohne die Server-Performance durch aufwändiges Viren-Scanning zu beeinträchtigen.

### Ausbruchseindämmung

Die Best-of-Breed-Security-Systeme von FortiGate werden als Teil einer mehrschichtigen Security-Entwicklung implementiert und bieten anwendungsbezogenen Schutz gegen Content-basierte Bedrohungen, die die Gateway-Firewall umgehen könnten.

### Rahmenschutz

Ein einziges FortiGate Security System, das als Netzwerk Security Gateway implementiert wird, kann mehrere DMZ-Ports zusammen mit dem Unternehmensnetzwerk vor Viren und anderen Content-basierten Angriffen schützen. Fortinets Sicherheitszonen und Virtual-Domain-Funktionen bieten Unternehmen, die mehrere Netzwerke schützen müssen, niedrigere Gesamtbetriebskosten.



## Fortinet AntiSpam

**SW**

Fortinets™ System ist die optimale Lösung für Unternehmenskunden und bietet eine Fülle von zuverlässigen und hochleistungsfähigen Funktionen, um Spam-Nachrichten und ihre schädlichen Anhänge zu ermitteln, zu markieren, unter Quarantäne zu stellen und zu blockieren. Eine rasche Installation bei niedriger Gesamtinstandhaltung, in Kombination mit Fortinets preisgekrönter Verwaltungsschnittstelle, gewährleisten hohe Benutzerfreundlichkeit bei niedrigen Gesamtbetriebskosten, was FortiMail™-Anwendungen heute zu den leistungsstärksten und kostengünstigsten E-Mail-Security-Systemen für Unternehmen macht.

## Mittelständisches Unternehmen

Durch die Verwendung von FortiMails™ integrierter Anti-Spam- und Anti-Virus-Security können kleinere Unternehmen kosteneffizient Spam bekämpfen, ohne zusätzliche Server einzurichten. Alles, was das Unternehmen benötigt, um von FortiGuards™ On-Demand-Diensten samt sechs zusätzlichen Anti-Spam-Funktionen zu profitieren, ist die Aktivierung der entsprechenden Optionen in der FortiMail™-Anwendung. Fortinets Anti-Spam- und Anti-Virus Subscription Dienste pro Funktionseinheit sind deutlich günstiger als Angebote von anderen Anbietern, die ihre Dienste auf einer Anwenderbasis lizenzieren.

## Großunternehmen mit mehrfachen Mailrelais

FortiMail™-Anwendungen bieten optimierten Anti-Spam-Schutz für Großunternehmen mit mehreren Mail-Servern. Die Implementierung mehrerer FortiMail™-Anwendungen als Mail-Übermittlungsagenten vergrößert die E-Mail-Performance für Unternehmen mit hohem Mailaufkommen. Die Verwendung von DNS MX gewichteten Warteschleifen bietet Redundanz, wobei eine Verlangsamung und ein Belastungsausgleich des Spam- und Anti-Virus-Scanning bei einem Betrieb im Gateway-Modus berücksichtigt wird.

### Die wichtigsten Leistungsmerkmale von AntiSpam:

- *hochleistungsfähige, bewährte Anwendung mit konfigurierbarer RAID-Speicherung*
- *FortiGuard Antispam nutzt mehrere Spam-Detektionsmethoden*
- *kosteneffiziente Anti-Virus- und Anti-Spam-Subscription pro Funktionseinheit*
- *FortiGuard Anti-Spam bietet eine einfache Installation*
- *uneingeschränkte E-Mail-Server-Leistungsfähigkeit*
- *Dreifachmodusfunktionalität, Gateway, Transparent, Server*
- *integriertes branchenführendes Anti-Virus-Scanning*
- *Detaillierte Erfassung und maßgeschneidertes Reporting*



## Fortinet WebFiltering

SW

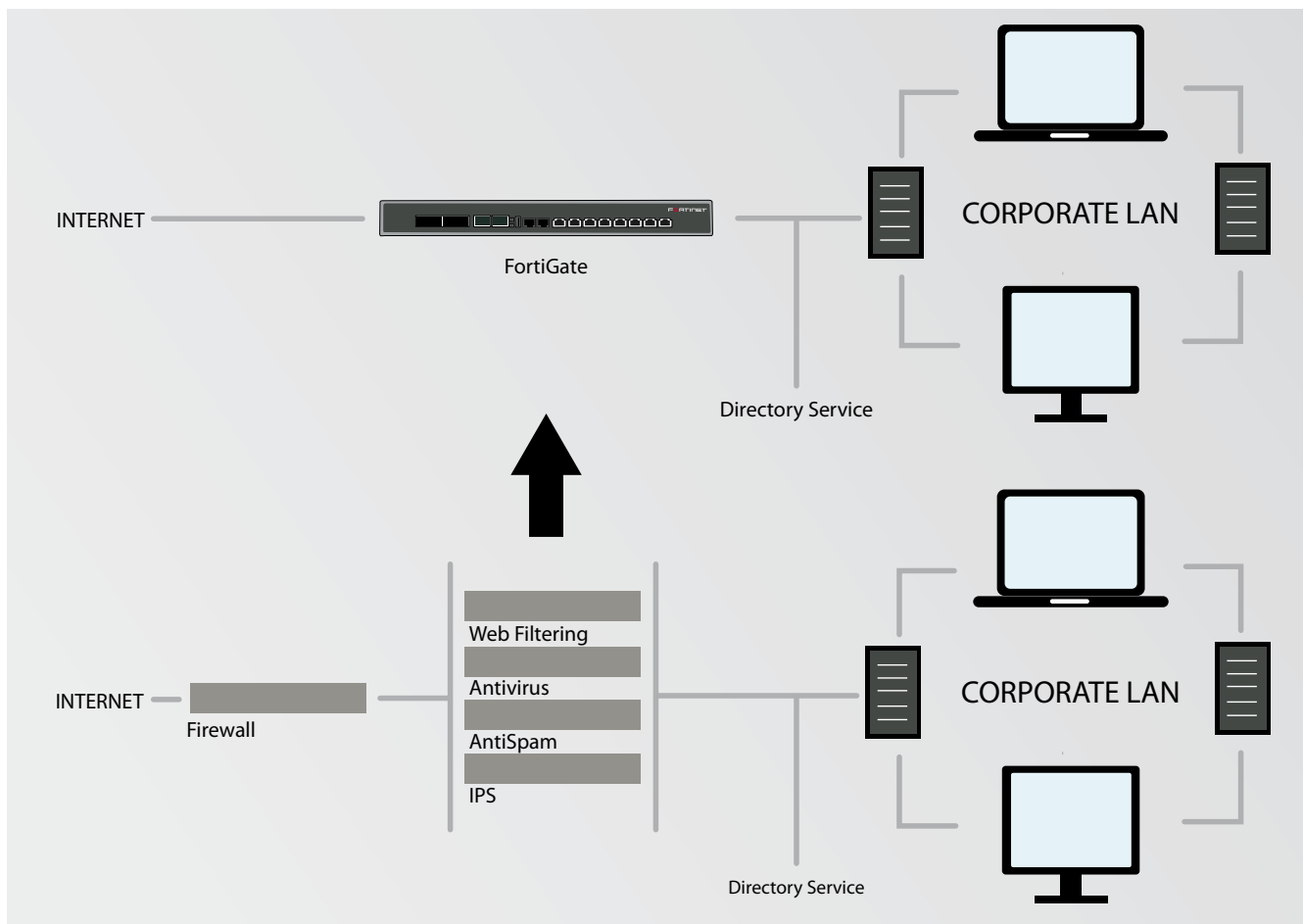
Die Nutzung des Internets ist zu einem wesentlichen Bestandteil für die Führung eines Unternehmens geworden, doch hat eine unangemessene Internetnutzung zu niedrigerer Produktivität, unangemessener Nutzung von Unternehmensressourcen, Störmanövern, gesetzlicher Haftung und Personalproblemen geführt. Fortinets FortiGuard Web Filtering Service reguliert und bietet wertvolle Einsicht in alle Internetaktivitäten und ermöglicht es dem Kunden so, neue gesetzliche Bestimmungen, Personal- & Internetnutzungsgrundsätze für Unternehmen zu erfüllen. Fortinet ist ein Mitglied der Internet Watch Foundation in Großbritannien, eine Organisation, die potenziell illegalen Online-Content bekämpft und den Zugang zu sexuellem Kindesmissbrauch verhindert. Fortinets Web Filtering Lösungen sind darüber hinaus CIPA-zertifiziert. Das Children's Internet Protection Act (CIPA) ist ein Bundesgesetz, das im Dezember 2000 vom amerikanischen Kongress verabschiedet wurde, um Problemen hinsichtlich des Zugangs auf das Internet und andere Informationen in Schulen und Bibliotheken entgegenzusteuern.

## Web Filtering für Klein- und mittelständische Unternehmen

Heute suchen viele Klein- und mittelständische Unternehmen nach MSSPs, die eine umfassende Lösung für ihre Network-Security-Anforderungen bieten. MSSPs können Fortinets Web Filtering Technologien einsetzen, um Web Filtering Ressourcen für Klein- und mittelständische Unternehmen bereitzustellen, die den Zugang zu unangemessenen Internetseiten kontrollieren wollen, welche Unternehmen dem Risiko einer potenziellen Haftung aussetzen, welche die Netzwerksicherheit beeinträchtigen und wertvolle Netzwerkbandbreite in Anspruch nehmen.

## CIPA zertifiziertes Web Filtering für Bibliotheken

Um die Internet-Filtering-Anforderungen der CIPA zu erfüllen, können Bibliotheken Fortinets branchenführenden, die Bestimmungen der CIPA erfüllenden FortiGuard Web Filtering Dienst gezielt nutzen. Anders als Web Filtering Produkte von anderen Anbietern, welche die Installation eines Einzelservers erfordern, ist die Implementierung von FortiGuard Web Filtering so einfach wie die Implementierung dieser Anwendung auf dem FortiGate System. ►



### Web Filtering für Unternehmen

Fortinets branchenführender FortiGuard Web Filtering Service bietet Unternehmen jeder Größe eine unkompliziert zu implementierende und kosteneffiziente Lösung zur Kontrolle des Zugriffs auf unangemessene Internetseiten, die für Unternehmen Material darstellen, für das sie potenziell haftbar gemacht werden können, die Netzwerksicherheit beeinträchtigen und wertvolle Netzwerkbandbreite in Anspruch nehmen. FortiGuard Web Filtering unterhält die größte URL-Datenbank der IT-Industrie mit mehr als 30 Millionen bewerteten Internetseiten, 76 Kategorien und 6 Bewertungsklassen. Als Teil der Datenbank kann FortiGuard den Zugriff auf Internetseiten blockieren, die ein Sicherheitsrisiko darstellen, wie P2P-, Phishing- und Spyware-Internetseiten. Darüber hinaus bietet das Subscription-Modell pro Funktionseinheit von Fortinet deutlich niedrigere Kosten als andere Anbieter, die für Web Filtering Lizenzen pro Anwender anbieten.

### K-12 CIPA zertifiziertes Web Filtering

Schulen implementieren FortiGuard Web Filtering, um CIPA-Anforderungen hinsichtlich der Filterung von unangemessener Internetnutzung zu erfüllen. Dank FortiGuards branchenführender Web Filtering Datenbank und sehr präzise kategorisierter Bewertungen können Administratoren außergewöhnlich gut sehr spezifische Internetzugangsstandards für unterschiedliche Nutzergruppen anwenden.



## Fortinet Wireless LAN Security



FortiGate Security Systeme bieten eine umfassende Reihe an Funktionen, mit denen die höchsten Anforderungen bei der Implementierung von Wi-

reless LANs erfüllt werden. FortiGate Systeme können in Verbindung mit Wireless Access Points von jedem Anbieter implementiert und dazu verwendet werden, Content-basierte Bedrohungen aus E-Mail- und Internet-Traffic, wie Viren, Würmer, Intrusionen, ungemessener Internet Content, in verbesserter Echtzeit zu ermitteln und zu eliminieren, ohne dabei die Performance des Netzwerkes zu beeinträchtigen. Neben der Bereitstellung von anwendungsbezogenem Schutz bieten die FortiGate Systeme umfassende netzwerkbezogene Dienste, wie Firewall, VPN, Intrusion Detection und Traffic-Modellierung, welche einen vollständigen Netzwerkschutz-Service mittels spezieller, leicht zu verwaltender Plattformen bieten. Insbesondere VPN Verschlüsselungs-, Anwender-Authentifizierungs- und Dateiverzeichnis-Integrations-Leistungsmerkmale der FortiGate Systeme ermöglichen eine Eindämmung von Sicherheitslücken von WLAN-Produkten der jetzigen Generation und bieten eine vollständige Nachrüstung für jede WLAN-Implementierung.

## WLAN Support

Die neue Serie von Fortinet eigenen Thin Access Points (FortiAP) in Verbindung mit einer Vielzahl von Wireless Controllern (nahezu allezu FortiGate Appliances ab FortiOS 4.1.) bietet High-Performance Netzwerkzugänge mit integrierter Content-Security.

Durch die Kombination eines Wireless Controllers mit einer FortiGate Plattform (größer als Modell FG50x) wird das Sicherheitsniveau des kabelgebundenen LANs automatisch auf die WLAN-Umgebung übertragen. Der gesamte WLAN-Traffic wird so identitäts-basierend über die UTM-Engines der FortiGate Appliance geleitet und dort entsprechend analysiert und es werden nur autorisierte Verbindungen zugelassen. Durch diese Integration ist es möglich von einer einzigen Konsole aus den Netzwerkzugang zu überwachen, Regelwerke einfach und schnell up-zudaten und den Datenverkehr und die Einhaltung von Compliance-Regeln kontinuierlich zu überwachen. Da jede FortiGate Appliance (größer als Modell FG50x) ab FortiOS 4.1. über diese Wireless-Controller Funktionalität verfügt, können bereits bestehende Gateways durch ein einfaches Betriebssystem-Update um dieses Feature erweitert werden – die Anschaffung einer zusätzlichen Plattform mit einer eigenen Administrations-Oberfläche entfällt.

Durch die hohe Performance und große Reichweite der neuen FortiAP-Serie ist der Aufbau einer hochsicheren und leistungsstarken WLAN-Infrastruktur einfach und kostengünstig möglich. In vielen Anwendungsszenarien erübrigt sich unter Umständen sogar das Installieren einer Verkabelung bis zum Arbeitsplatz, da die Durchsatzraten der WLAN-Lösung vielfach äquivalent hoch sind.

## Zu den weiteren Eigenschaften dieser Produktlinie gehören:

- Erkennung und Reporting von nicht erlaubten Access Points (sog. Rogue APs)
- granulare Endpoint-Kontrolle
- Standard-Reports, die für Audits nutzbar sind
- 802.11n Support (parallel zu a/b/g) basierend auf 2x2 Multiple-In/Multiple-Out (MIMO) Technologie
- Volle Integration in das umfangreiche UTM-Feature-Set einer FortiGate-Appliance
- Spannungsversorgung des FortiAP über das LAN-Kabel (POE-Funktion, nur bei FortiAP 210-Serie)

## Fortinet löst die wichtigsten Probleme

- Sicherheitsprobleme mit WLAN-Implementierung
- Kein systemeigener Support zur Aktivierung eines Wireless Access Point zur Unterscheidung des WLAN NIC eines Angestellten von dem eines freundlichen Besuchers oder eines böswilligen Eindringlings
- Begrenzter Support für Dateiverzeichnisintegration.
- Kein systembezogener Support für Authentifizierung von Terminals
- Lücken in der WEP-Verschlüsselung
- Content-basierende Angriffe, wie Virus Scanning, Sript Filtering und Intrusion Detection/Intrusion Prevention
- Kein systemeigener Support für QoS zur Gewährleistung einer angemessenen Zuteilung von gemeinsam verwendeter Wireless-Bandbreite

### Sicherheitsproblem mit WLAN-Implementierung

Kein systemeigener Support zur Aktivierung eines Wireless Access Point zur Unterscheidung des WLAN NIC eines Angestellten von dem eines freundlichen Besuchers oder eines böswilligen Eindringlings

Begrenzter Support für Dateiverzeichnisintegration

Kein systembezogener Support für Authentifizierung von Terminals

Lücken in der WEP-Verschlüsselung

Content-basierende Angriffe, wie Virus Scanning, Sript Filtering und Intrusion Detection/Intrusion Prevention

Kein systemeigener Support für QoS zur Gewährleistung einer angemessenen Zuteilung von gemeinsam verwendeter Wireless-Bandbreite

### Wird durch die FortiGate Plattform aufgegriffen

Authentifizierung auf Anwenderebene und Anwender/Gruppen-Standards, welche z. B. Angestellte in die Lage versetzen, Zugang zu bestimmten Datenressourcen und –diensten zu erhalten, bietet Internetzugang für Gäste ausschließlich für E-Mail- und Internetzugang, verweigert Eindringlingen diesen Dienst jedoch.

Anwender-Authentifizierung mittels interner Datenbank, Radius Server oder LDAP-Verzeichnis.

IP/MAC Einbindung für die Aktivierung der physischen Authentifizierung von Zugangsterminals.

Starke Verschlüsselung einschließlich WPA-2 und Authentifizierung von Wireless Links, welche IPSec VPN mit einer Auswahl an Triple-DES oder AES-Verschlüsselung verwenden, und SHA1 oder MD5 für Authentifizierung auf Paketebene.

Intrusion Detection und Intrusion Prevention, Anti-Virus/Anti-Spyware und Web Content Filtering von Wireless Traffic.

Standard-basierte Traffic-Modellierung für die Zuteilung von Bandbreite basierend auf Anwenderidentität und Anwendungstyp.

**FortiOS**

*In FortiOS 4.2., dem Security-Betriebssystem aller FortiGate-Lösungen, wurden viele der bisher nur im FortiOS-Carrier verfügbaren VoIP-Security Funktionen für das gesamte Portfolio der FortiGate-Modelle integriert. Dazu zählen u.a. SIP Header Conformance Check (Prüfung einer SIP Nachricht auf Unregelmäßigkeiten), SIP Message Rate Limitation (per Methode), SIP NAT IP Address Speicherung, Multiple RTP Endpoint Support, SIP Hosted NAT Traversal, SIP HA Failover sowie Deep SIP Message Inspection (Syntax Check einer SIP Nachricht). Außerdem wurde eine Stateful SCTP Firewall implementiert.*



**Fortinet Voice Over IP**



Aufgrund der zunehmenden Implementierung von VoIP stehen sowohl Unternehmen als auch Service Provider vor der Herausforderung, Telefoniedienste hochverfügbar und in der gewohnte „analoge“ Qualität bereitstellen zu müssen. Ist es bei vielen Standardanwendungen unproblematisch, wenn deren Antwortzeiten im Millisekunden- oder sogar Sekundenbereich variieren, ist dies bei Sprache völlig inakzeptabel, da dies zu einer deutlich spürbaren Qualitätsminderung (=Unverständlichkeit) führt. Quality of Service (QoS) für VoIP ist damit eine der großen Herausforderungen. Ein Aspekt von QoS ist aber auch die generelle Verfügbarkeit – welche durch die Nutzung von IP-basierender Infrastruktur den dort seit langem bekannten Sicherheitsbedrohungen ausgesetzt und damit gefährdet ist. Daher ist es wichtig, bereits vorhandene IT-Security-Infrastruktur dahingehend zu prüfen, ob sie sich auch zum Schutz von VoIP-Diensten eignet – und ggf. entsprechende Erweiterungen oder sogar einen Ersatz zu planen.

Ein sicherheitsrelevanter Aspekt bei VoIP-Diensten ist die Tatsache, dass während eines VoIP-Telefonats Ports dynamisch geöffnet und geschlossen werden – dies wird von vielen Standard-Firewalls nicht unterstützt, weshalb für VoIP oft ein großer Port-Bereich standardmäßig geöffnet ist (um diesen Dienst überhaupt nutzen zu können) und somit Angreifern das leichte Eindringen ins Unternehmensnetz ermöglicht.

Die **Fortinet VoIP Firewall** erkennt anhand des überprüften SIP-Verkehrs, welche Ports für den Sprachverkehr dynamisch geöffnet werden sollen und wann sie wieder geschlossen werden müssen. Dieser dynamische Prozess unterstützt auch NAT (auf IP, SIP, SDP und RTP). Viele Kunden arbeiten inzwischen mit Fortinets FortiGate Anti-Virus Firewalls, um den Video-, Daten- und Voice-Traffic vor verbreiteten Echtzeit-Traffic-Problemen zu schützen, darunter: Registrierungsentführung, Server-Imitation, Nachrichtenfälschungen, Sitzungsabbrüche und Dienstverweigerungen (DOS). Ein weiterer Vorteil von FortiGate-Lösungen für Videokonferenzen ist, dass die bereitgestellte Sicherheit für die Endanwender transparent ist. Es besteht keine Notwendigkeit, Änderungen in den Video-Systemen vorzunehmen.

Die Fortinet VoIP Firewallfunktionen werden von führenden Europäischen Service Providern und Enterprise Unternehmen eingesetzt, um deren VoIP Verkehre zu schützen. Hierbei ist die Reaktionsgeschwindigkeit ein elementarer Bestandteil, um auch neue und noch unbekannte Angriffe durch Signaturen innerhalb von wenigen Minuten abzuwehren. Durch eine genaue Überprüfung der VoIP Protokolle und eine gute Lastabwehr wird ein effektiver Schutzmechanismus aufgebaut.

**Beispielszenarien für die Bedeutung einer Integration von Applikations-Kontrolle in ein Multi-Layer-Security System:**

Applikations-Kontrolle und AntiVirus Auch wenn Applikations-Kontrolle Anwendungen erkennt und deren Nutzung reglementiert, so können infizierte Webseiten, Würmer, die via Instant Messaging/Chat übertragen werden, schädliche Files, die per File Transfer ins Unternehmen gelangen oder sonstige Schwachstellen in den Anwendungen selbst nur dann sinnvoll bekämpft werden, wenn zusätzlich ein integriertes AntiVirus-Modul diese Malware zuverlässig erkennen kann. ►



**Application Control**

**Mehr als nur Security: Applikations-Kontrolle**

Applikations-Kontrolle überwindet all diese Beschränkungen und Probleme, in dem es Mittel bereitstellt, die Applikationen erkennen und deren Nutzung im Detail kontrollieren können – auch dann, wenn diese non-standard Ports verwenden oder über gängige oder auch weniger gängige Protokolle getunnelt werden. Dies geschieht durch die Analyse des applikations-spezifischen Paket-Verhaltens, sowie eines umfangreichen Protokoll-Decodings. Eine herkömmliche Firewall kontrolliert den Datenstrom basierend auf Port- bzw. Service-Kontrollmechanismen. Applikations-Kontrolle setzt auf dynamische Untersuchung der Daten und ermöglicht überdies die Anwendung weiterer Kontrollen, wie etwa Bandbreitenvergabe pro Applikation oder Zeitfenster bzw. -konten für deren Nutzung. Überdies kann sogar innerhalb von Applikationen ein Teil der Funktionalität eingeschränkt werden, z.B. die Nutzung von Facebook, aber das Unterbinden von Facebook Chat oder das Nutzen von Google.Docs, aber das Unterbinden von Google.Talk.

Applikations-Kontrolle ergänzt somit die Funktionalität von Firewall- und IPS-Mechanismen um eine granulare Steuerung von Anwendungen und Protokollen. Somit wird die maximale

Nutzbarkeit von Applikationen bei minimalem Risiko erzielt. Derartige Regeln zur Nutzung können bis auf Anwenderebene und selbstverständlich auch Geräte- oder Abteilungsbezogen erstellt werden.

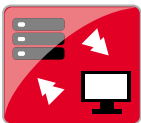
Es ist wichtig, Applikations-Kontrolle nicht als isolierten Bestandteil der IT-Sicherheit zu verstehen, denn dies führt zu einem reaktiven Ansatz der Security-Strategie. Vielmehr ergänzt es sinnvoll die vorhandenen Abwehrmechanismen wie z.B. Firewall, VPN, AntiVirus, IPS und Web Filter und idealerweise integriert es sich in diese. Unternehmen leiden zunehmend an der – nicht nur in IT-Security-Umgebungen – häufig anzutreffenden viel zu heterogen gewachsenen Struktur, die auf sog. Point-Solutions, also Nischen-Lösungen basieren. Diese integrieren sich nur bedingt oder gar nicht, sind aufgrund der Vielfalt schwierig in der Administration – und erhöhen oft unbemerkt die Betriebskosten eines Unternehmens in beträchtlicher Weise. Als unangenehmen Nebeneffekt beeinflussen solche oft seriell in einen Datenstrom eingebrachten Lösungen auch die Gesamt-Performance des Netzwerks negativ, da durch diese Vorgehensweise Pakete oft mehrfach analysiert werden – oder im schlimmsten Fall sogar Paketinformationen für eine sinnvolle Analyse gar nicht mehr zur Verfügung stehen.

Applikations-Kontrolle und Web Filter stellen eine sinnvolle Schutzmaßnahme gegen klassische und gewollte Webseiten und deren Inhalte dar. Applikationen, die über zulässige Webseiten oder Web Proxies getunnelt oder umgeleitet werden, können jedoch hier nicht erkannt werden – die Integration mit Applikations-Kontrolle ist unumgänglich.



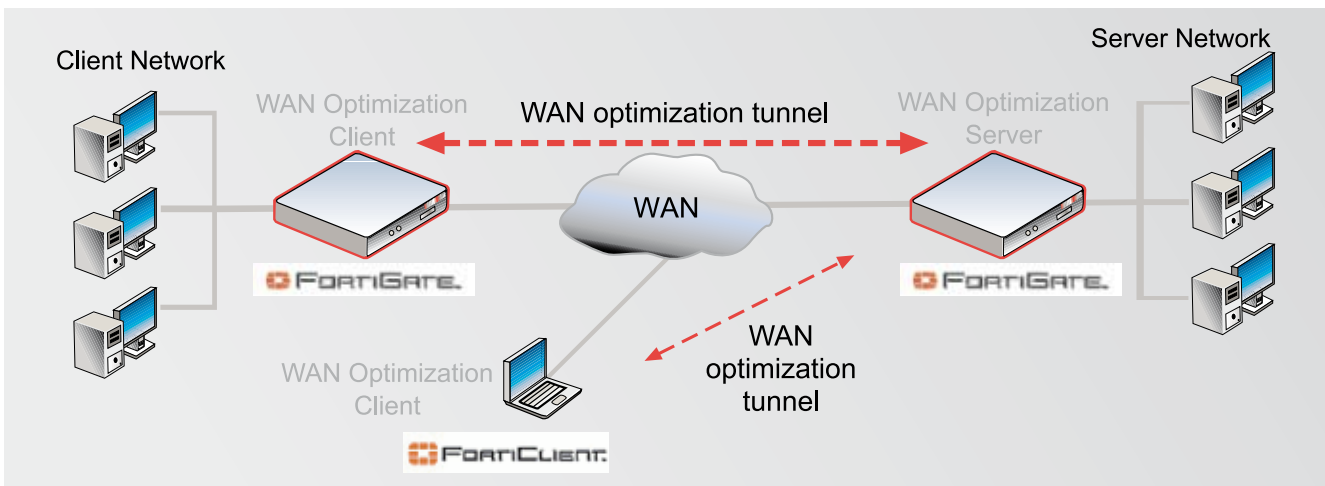
## Data Leakage Prevention

hilft bei Identifizierung und Schutz vertraulicher Informationen außerhalb der Netzwerkgrenzen, ist auf jede Applikation anwendbar und greift auch bei verschlüsseltem Datenverkehr. Data Leakage Prevention kann so konfiguriert werden, dass Kontrollpfade für Daten und Dateien eingerichtet und damit gesetzliche Richtlinien eingehalten werden.



## WAN-Optimierung

beschleunigt den WAN-Zugriff auf Applikationen und stellt zugleich die Multi-Threat-Security sicher. Der Service sorgt für mehr Performance, Produktivität und Einsparungen bei Datenübertragungsmengen, Bandbreitenbedarf, Serverressourcen und Netzwerkkosten. Der Einsatz der WAN-Optimierung setzt FortiGate-Modelle mit lokalem Speicher voraus.

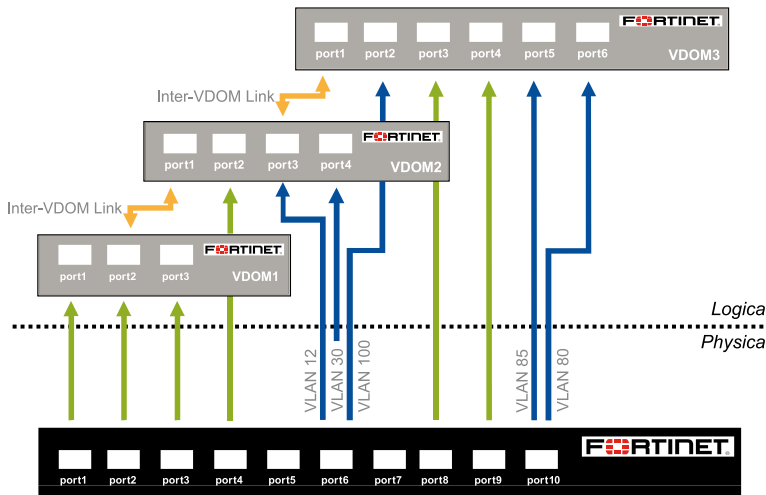


## SSL-Inspection

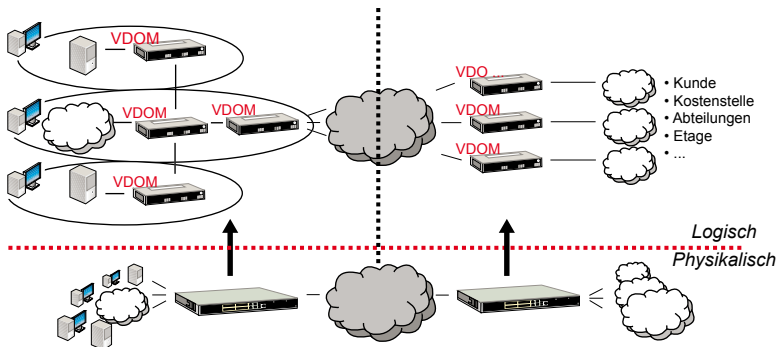
verbessert den Schutz und die Richtlinienkontrolle für verschlüsselten Datenverkehr. Dabei werden verdeckte Kommunikationsdaten überprüft, der Schutz für Web- und Applikationsserver erhöht und der Einblick in den Netzwerkverkehr verbessert

## Virtualisierung von IT-Sicherheit

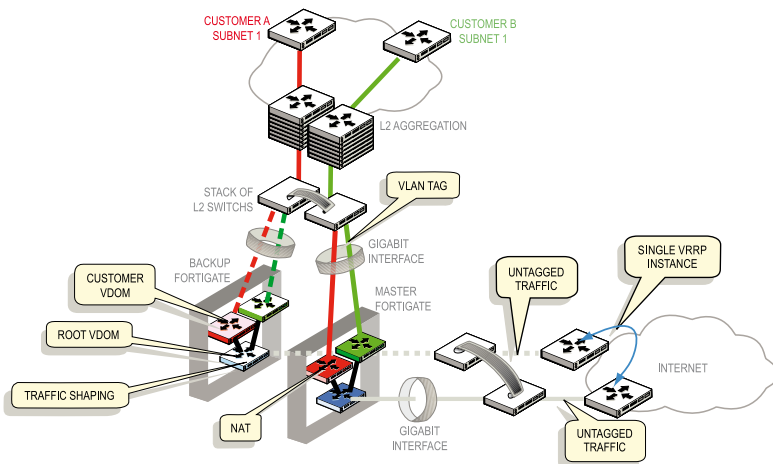
### Flexible Port-Zuweisung



### Vielfältige Einsatzgebiete



### Hochverfügbarkeit



Die Konsolidierung unterschiedlicher IT-Security-Dienste auf einer einzigen Hardware-Plattform kann durch deren Virtualisierung optimal ergänzt werden. So lassen sich Kosten senken, die sonst aufgrund von hohem Platzbedarf, aufwendiger Wartung und Bedienung, komplizierter Verwaltung von Service-Verträgen, Stromverbrauch und mangelhafter Flexibilität entstehen. Darüber hinaus benötigen immer mehr Unternehmen heterogene Security-Dienste für einzelne Teile ihrer Infrastruktur, also unterschiedliche Funktionen für verschiedene Abteilungen.

Mit der standardisierten und integrierten Virtualisierungsfunktion – sogenannte virtuelle Domänen (VDOMs) – können sämtliche Funktionen des FortiGate auch als virtuelle Einheit abgebildet werden. Daraus ergibt sich die Möglichkeit, dass einzelne Abteilungen oder Kunden mehrere oder auch nur bestimmte Funktionen wie Firewall, AV- oder IPS-Dienste nutzen können. Die Verwaltung läuft dabei auf ein und derselben Appliance. Bei allen Modellen bis zur 1xxxer Serie sind 10 VDOMs möglich, mit zusätzlichen Lizenzen sind sogar bis zu 250 VDOMs realisierbar.

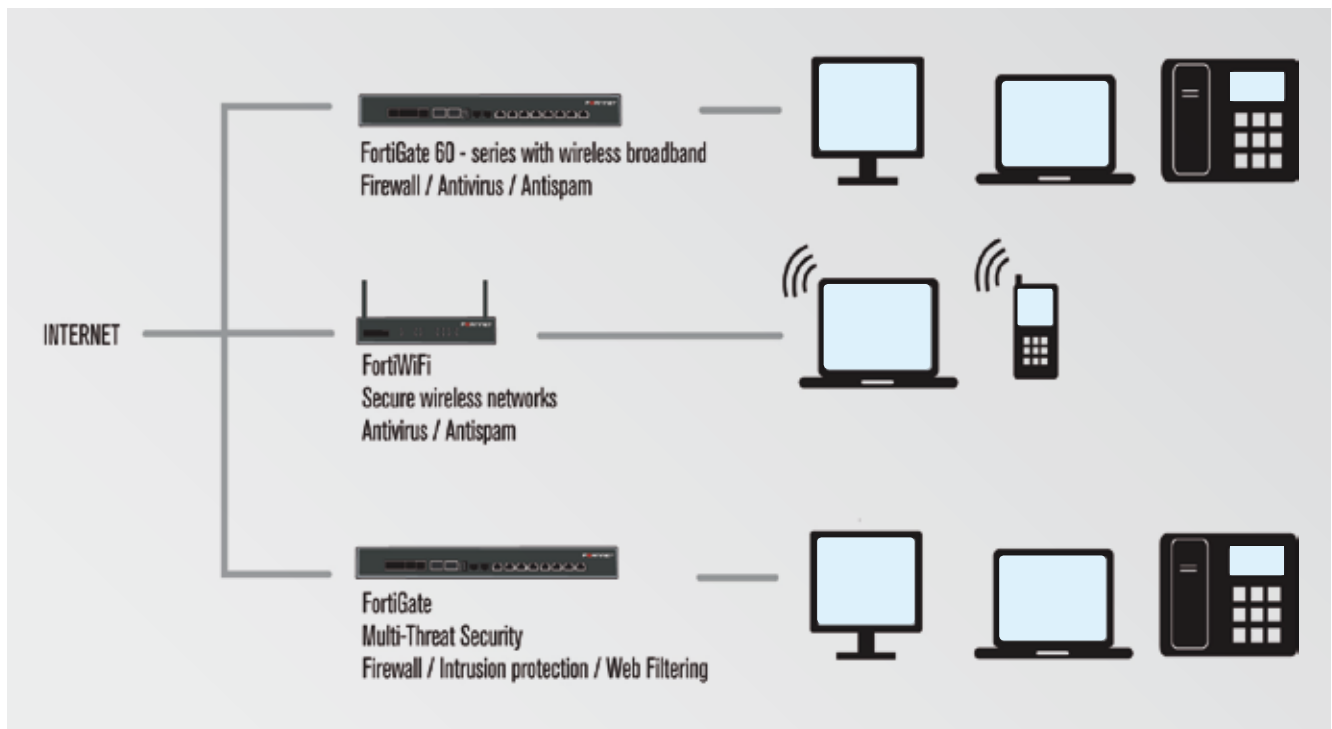
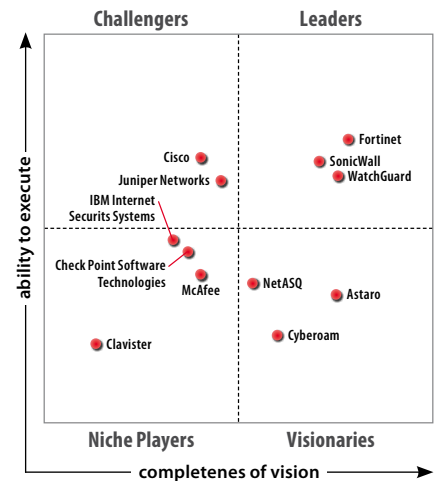
In Verbindung mit FortiManager und FortiAnalyzer können extrem flexible Management- und Reporting-Funktionen mandantenfähig abgebildet und entweder durch den Kunden, die Abteilung oder den Dienstleister verwaltet werden. Sowohl FortiManager als auch FortiAnalyzer stellen diese Funktionalitäten bereits standardmäßig bereit, eine Erweiterung ist hier nicht erforderlich.

## Fortinet für KMU und Mittelstand

Netzwerkbedrohungen unterscheiden nicht nach Unternehmensgröße. Filialen und kleinere Firmen sind den gleichen Risiken ausgesetzt wie große Unternehmen. KMUs fordern allerdings schlüsselfertige Sicherheitslösungen, die keine allzu hohen Kosten verursachen, aber trotzdem umfassenden Schutz bieten. Fortinet hält hier marktführende Unified-Threat-Management-Appliances bereit, die alle notwendigen Sicherheitsfunktionen für den Schutz eines Unternehmens zusammenführen – darunter Antivirus, Firewall, VPN, Intrusion Prevention, Webfilter, Antispam, Antispyware und Traffic Shaping. Die einfach zu implementierenden und leicht zu verwaltenden Systeme sind hervorragend für KMUs und Filialen geeignet und bieten im Rahmen einer modernen Security-Plattform außergewöhnliche Flexibilität und hervorragenden Schutz bei einem sehr guten Preis-Leistungsverhältnis. Zahlreiche Filialen, KMUs und SOHOs weltweit setzen Fortinet FortiGate-Systeme ein.

**Fortinet-FortiGate-Systeme weisen die folgenden Vorteile für den Einsatz in Filialen, bei KMUs und SOHOs auf:**

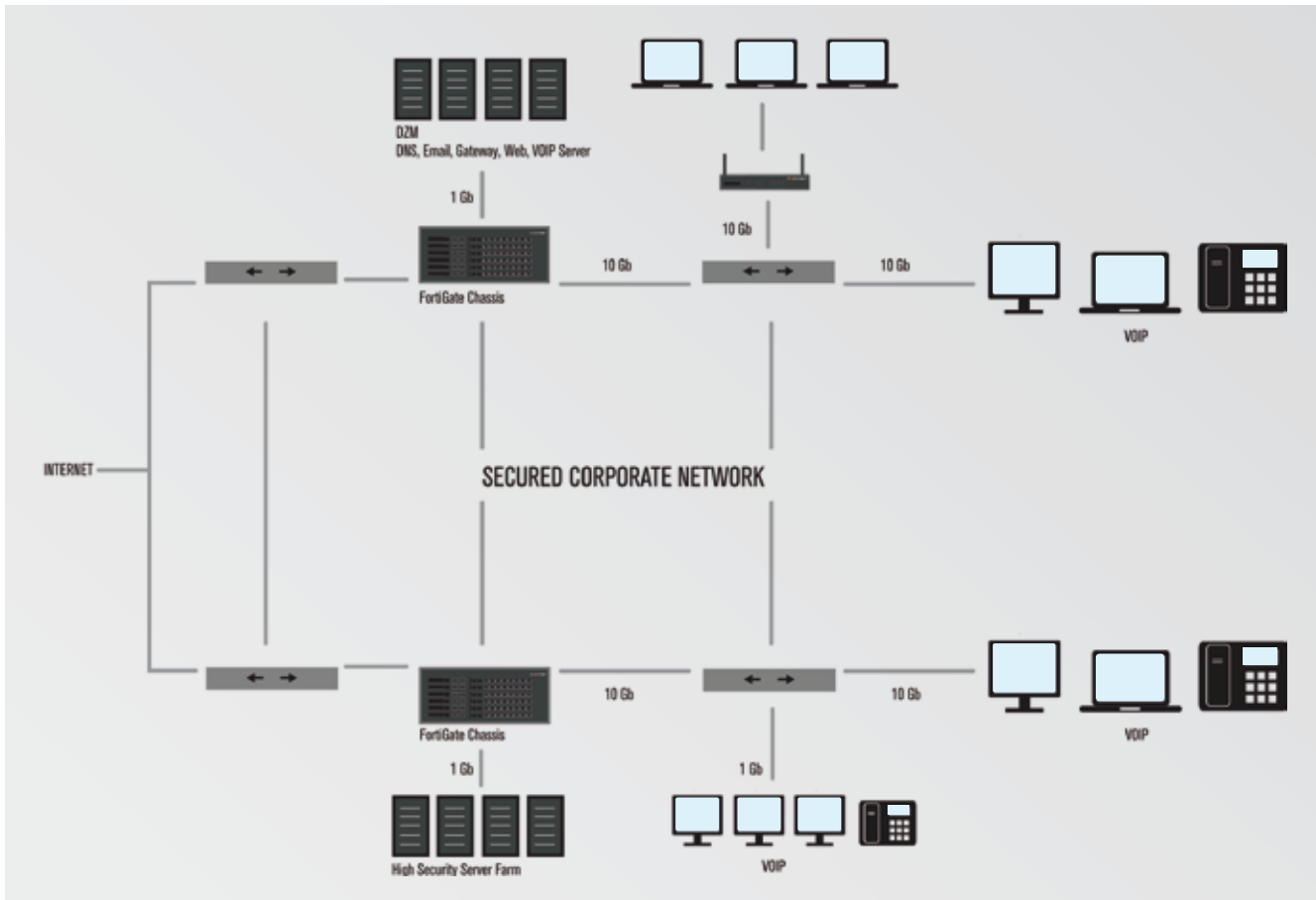
- Marktführende Unified-Threat-Management-Funktionalität (UTM)
- ICSA-zertifizierte Sicherheit auf Enterprise-Niveau zu einem vergleichsweise kleinen Preis
- Preiswert und gleichzeitig leicht zu implementieren und zu verwalten



## Fortinet in Enterprise-Umgebungen

**Viele Unternehmen** haben heute erkannt, dass eine einzige Verteidigungslinie nicht mehr ausreicht, um höherwertige E-Commerce-Transaktionen, geistiges Eigentum und den Datenaustausch mit Partnern zu schützen. Eine gründliche Abwehrstrategie ist notwendig, um die Kompromittierung der Firmennetze mithilfe einer Kombination neuer Techniken und Ansätze zu verhindern.

Ein Unternehmen kann FortiGate-Systeme von Fortinet dazu einsetzen, eine ganze Reihe von Bedrohungen aufzuspüren, zu blockieren, in Logs festzuhalten und vollständig zu eliminieren. FortiGate bekämpft unter anderem ungeeignete Webinhalte, Spam und Spyware. ▶



**Unternehmen jeder Größe** profitieren von Fortinet-Produkten im Einsatz gegen zunehmende netzwerkgestützte Attacken, deren Gefahr auch von der ständigen Verschiebung des Netzwerkperimeters herrührt.

**Heutige Firmennetze** wachsen intern durch drahtlose Verbindungen. Sie erstrecken sich auf mobile Anwender auf Dienstreisen. Sie erweitern sich nach außen um Partner-Extranets und nach innen um Intranets für die Mitarbeiter. Zusammen mit existierenden Host-gestützten Antivirus-Systemen, einfachen Firewalls oder separaten IPS-Systemen erweitern die Produkte von Fortinet dramatisch die Fähigkeit eines Unternehmens, Bedrohungen dynamisch abzuwehren und einen gründlichen und wirksamen Schutz aufzubauen.

### Fortinet FortiGate-Systeme bieten Unternehmen auf Enterprise-Level die folgenden Vorteile:

- **Führende, von den ICSA-Labs zertifizierte Funktionalität** für Unternehmensnetze jeder Größe, gleich ob drahtgebunden oder drahtlos, in Kombination mit Multi-Gigabit-Durchsatz für Antivirus-Gateways, IPS, VPN und Firewalls.
- **Transparenter Funktionsmodus**, der die Fortinet-Sicherheitstechnik nahtlos mit existierenden Security-Produkten im Unternehmen zusammenarbeiten lässt.
- **Eine Auswahl führender Sicherheitsfeatures für Netzwerke**, beschleunigt durch FortiASIC und durch die zum Patent angemeldete CPRL-Technologie.
- **Ein skalierbares Sicherheitssystem**, verwaltet über ein einheitliches Management-Interface für Unternehmen jeder Größe. Die Zahl der angeschlossenen Clients am Hauptsitz oder in Filialen spielt keine Rolle.
- **Ein attraktives Pro-Box-Lizenzierungsmodell** löst das kostentreibende Pro-User-Lizenzierungsmodell ab, das der Wettbewerb häufig anbietet. Pro-User-Lizenzierung kann das jährliche operative Budget in einer Höhe belasten, die vier- bis fünfmal dem Anschaffungspreis für die Systeme entspricht.
- **FortiGuard Subscription Services** für Antivirus, IPS, Web-Filter und Antispam bieten Updates in Echtzeit und den branchenweit besten Netzwerkschutz.

# Fortinet für Carrier

Sicherheit für Pre-IMS- und IMS-Infrastrukturen

## Revolution der Services – Evolution der Netzwerke

Carrier mit drahtlosen und drahtgebundenen Diensten erleben ein explosives Umsatzwachstum auf der Basis von IP-gestützten Services wie Breitband-Access, Multimedia Messaging, Voice over IP (VoIP), Video Services und kombinierten Multimedia-Diensten. Der Wettbewerbsdruck ist enorm. Es geht dabei um Kundenbindung, die Kontrolle über die Wertschöpfungskette und darum, Kapitalbindung und operative Ausgaben zu begrenzen. Um die aktuellen Chancen und Herausforderungen optimal zu adressieren, richten die Carrier IP-gestützte Netzwerke und Applikation-Service-Netze ein. Für den wirtschaftlichen Erfolg dieser Bemühungen ist es unbedingt notwendig, dazu das passende Risikomanagement einzuführen.

## Fortinet Security Solution Suite

Es ist eine extrem komplexe Aufgabe, IP-Infrastrukturen zu sichern. Sicherheitsbedrohungen sind nicht statisch. Erfolgreicher Schutz setzt eine lückenlose Sammlung von Werkzeugen voraus, mit der sich bekannte Bedrohungen ausschalten und unbekannte Cyber-Angriffe bekämpfen lassen. Die Tools müssen außerdem revisionssichere Informationen in Echtzeit liefern und in der Lage sein, für zukünftige Herausforderungen zu skalieren und sich weiter zu entwickeln. Fortinet stellt eine komplette Suite an Sicherheitslösungen für Carrier zur Verfügung. Die Produkte basieren auf netzwerk- und anwendungsorientierten ASIC-Security-Echtzeit-Engines, die durch Software-Module für spezifische Schutzanforderungen ergänzt werden.

**FortiCarrier** konsolidiert auf einer Plattform neun Sicherheitsfunktionen und ist derzeit das einzige, vollständig virtualisierte Angebot. Mit FortiGate adressiert der Marktführer für Unified Threat Management die Sicherheitsaspekte dreier Trends - Netzkonvergenz bei Daten, Sprache, Video und Mobile Content, Sicherheitsrisiken in der Mobilfunkkommunikation und Security-as-a-Service - und erleichtert Carriern und Service Providern die Einführung Cloud-basierter Security Services.

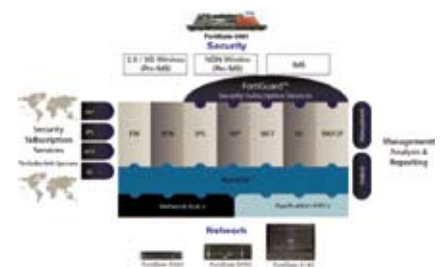
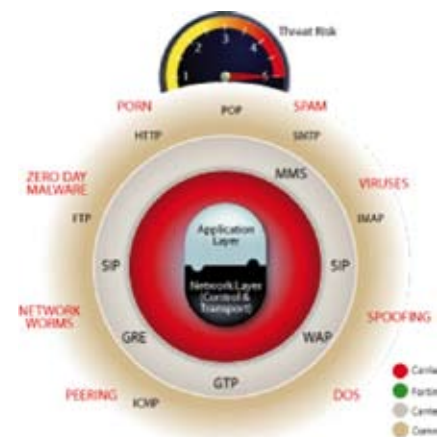
Mit FortiCarrier können Kunden bei den Investitions- und Betriebskosten für die Sicherheit ihrer Netzwerke sparen und zudem das Geschäftsmodell der Managed Security Services einführen. Die aktuellen Modelle FortiCarrier-3810A und FortiCarrier-5001A-DW integrieren das Betriebssystem FortiCarrier 4.0, das mit spezifischen Funktionen auf den Bedarf von Service Providern zugeschnitten ist:

**Dynamische Security-Profile** sorgen für die automatische Zuweisung von Security-Richtlinien für einzelne Benutzer, so dass Service Provider den manuellen Konfigurationsaufwand für die unterschiedlichen Security-Richtlinien ihrer Kunden reduzieren und Betriebskosten senken können. Ein wichtiger Vorteil, da Managed Security Services die Managementkomplexität erhöhen können. Mit Session Initiation Protocol (SIP) Security schützt Fortinet Sprachanrufe, die im Zuge der Konvergenz von Sprachnetzen und IP-Netzen über das Internet laufen. FortiOS Carrier enthält eine SIP-Firewall, die sich nahtlos in den Fortinet Intrusion Prevention Service integriert und Sprachinfrastrukturen gegen lückenhaften Datenverkehr und bösartige Bedrohungen absichert. Mobile Security ist in FortiOS Carrier mit gleich drei Features abgedeckt: Antivirus und Antispam für Multimedia Messaging Service (MMS), Filtern von Handyinhalten zur Durchsetzung von Nutzungsrichtlinien sowie eine GPRS Tunneling Protocol-Firewall mit 3GPP-Kompatibilität. In Kombination schützen diese Features die Infrastruktur des Mobilfunkanbieters ebenso wie die Endgeräte.

**Die FortiOS Carrier Software ist kostenlos**, sofern für die betriebene Hardware ein laufender FortiCare-Support-Vertrag besteht.

## Die Kernvorteile der Fortinet Security Solution Suite:

- Ultra-Hochleistungs-ATCA-Plattformen für Zuverlässigkeit, Skalierbarkeit und anwenderfreundliches Management
- Modulare Softwarearchitektur, die eine schnelle Ergänzung und Aktualisierung der Sicherheitsfunktionen erlaubt – immer passend zu den aktuellen Sicherheitsanforderungen
- Umfassende Security-Subscription-Services – einzelne Dienste lassen sich abonnieren
- Leistungsfähige Management- und Analyse-Appliances für zentrale Steuerung und umfassende Reports



## Technische Daten



### MSSP AND LARGE ENTERPRISE SYSTEMS

Features	FortiGate-5140 Chassis	FortiGate-5050 Chassis	FortiGate-5020 Chassis	FortiGate-5001A -SW / -DW Blade (with AMC)	FortiGate-5005FA2	FortiGate-5001SX and FortiGate-5001FA2
Firewall Throughput (512 Byte)	Up to 182 Gbps	Up to 65 Gbps	Up to 26 Gbps	2 Gbps (6-22 Gbps)	5 Gbps	4 Gbps
IPSec VPN Throughput	Up to 98 Gbps	Up to 35 Gbps	Up to 14 Gbps	800 Mbps (4-9 Gbps)	800 Mbps	600 Mbps
Concurrent Sessions	Up to 28 M	Up to 10 M	Up to 4 M	2 M	1.2 M	1.2 M
Sessions Per Sec	Up to 700 K	Up to 250 K	Up to 100 K	50 K	30 K	20 K
Antivirus Throughput	Up to 7 Gbps	Up to 2.5 Gbps	Up to 1 Gbps	500 Mbps	300 Mbps	250 Mbps
Intrusion Prevention Throughput	Up to 56 Gbps	Up to 20 Gbps	Up to 8 Gbps	2 Gbps	3 Gbps	2 Gbps
Number of VDOMs	Up to 3.500	Up to 1.250	Up to 500	Up to 250	Up to 250	Up to 250
Network Interfaces	See modules below	See modules below	See modules below	2 GbE 10/100/1000 port and Double- or Single-Width AMC slot. Supports 10GbE modules.	6 GbE SFP ports and 2 FortiASIC-accelerated SFP ports	5001SX: 4-GbE SFP, 4-GbE 10/100/1000 5001FA2: 2 GbE SFP, 4 GbE 10/100/1000, and 2 FortiASIC-accelerated SFP ports
Chassis Slots / Max Security Blades	14 / 14	5 / 5	2 / 2			
Power Source	2	DC / AC	AC			
Recommended Security Blades	14 / 14	4	2			
Max Fabric Blades	DC/AC	2	0			
Recommended Security Blades	12	3 or 4	2			
Max Fabric Blades	2	2	0			

### MSSP AND LARGE ENTERPRISE SYSTEMS

Features	FortiSwitch-5003A Switch Fabric Blade	FortiSwitch-5003 Switch Fabric Blade	FortiController-5208 Load Balancing Fabric Blade
Firewall Throughput (512 Byte)	Delivers high availability 10GbE switching for FortiGate-5140 and -5050 chassis. Each FortiGate-5001A requires a 10GbE Rear Transition Module (RTM) for switching across the backplane fabric.	Delivers high availability switching across the high-speed chassis backplane fabric.	Delivers high-bandwidth load balancing for antivirus and intrusion prevention applications.
IPSec VPN Throughput			
Concurrent Sessions			
Sessions Per Sec			
Antivirus Throughput			
Intrusion Prevention Throughput			
Number of VDOMs			
Network Interfaces	9-10GbE SFP+, 2-GbE 10/100/100 (Mgmt)	3-GbE 10/100/1000, 1-GbE 10/100/1000 (Mgmt)	2-10GbE XFP, 8-GbE SFP, 1-GbE 10/100/1000 (Mgmt)
Chassis Slots / Max Security Blades		RTM-XB2 or RTM-XD2: 10 GbE Rear Transition Module for FG-5000 Series	
Power Source			
Recommended Security Blades			
Max Fabric Blades			
Recommended Security Blades			
Max Fabric Blades			

### EXPANSION MODULES

<b>Advanced Mezzanine Card (AMC) Modules</b>	[Double-Width (DW) Modules:] • ADM-XD4: 4-port 10GbE FortiASIC Module • ADM-XB2: 2-port 10GbE FortiASIC Module • ADM-XE2: 2-port 10GbE Security Processing Module • ADM-FB8: 8-port GbE FortiASIC Module • ADM-FE8: 8-port GbE Security Processing Module [Single-Width (SW) Modules:] • ASM-FB4: 4-port GbE FortiASIC Module • ASM-CE4: 4-port GbE Security Processing Module • ASM-S08: 80 GB Hard Disk Storage Module • ASM-CX4: 4-port GbE TX By-Pass Module • ASMFx2: 2-port GbE SX By-Pass Module • ASM-ET4: 4-port T1/E1 WAN Module
<b>Fortinet Mezzanine Card (FMC) Modules</b>	• FMC-XD2: 2-port 20GbE SFP Firewall Acceleration Module • FMC-XG2: 2-port 20GbE IPS Acceleration Module

## Technische Daten

ENTERPRISE APPLIANCES						
Features	FortiGate-3950B /-3951B (with FMC)	FortiGate-3810A (with AMC)	FortiGate-3600A (with AMC)	FortiGate-3016B (with AMC)	FortiGate-1240B (with AMC)	FortiGate-800 /-800F
Firewall Throughput (512 Byte)	20 Gbps (120 Gbps)	7 Gbps (55 Gbps)	6 Gbps (10 Gbps)	16 Gbps (20 Gbps)	40 Gbps (44 Gbps)	1 Gbps
IPSec VPN Throughput	8 Gbps (48 Gbps)	1 Gbps (23 Gbps)	800 Mbps (3.8 Gbps)	12 Gbps (15 Gbps)	16 Gbps (18.5 Gbps)	200 Mbps
Concurrent Sessions	10 M	2 M	1.1 M	1.1 M	2 M	800 K
Sessions Per Sec	175 K	40 K	40 K	25 K	100 K	10 K
Antivirus Throughput	1.5 Gbps	500 Mbps	400 Mbps	300 Mbps	900 Mbps	150 Mbps
Intrusion Prevention Throughput	(More than 10 Gbps)	4 Gbps	3 Gbps	2 Gbps	1.5 Gbps	600 Mbps
10/100 Interface	0	0	0	0	0	4
GbE Interface	2	8	8	2	16	4 / 0-800F
SFP Interface	4	2	2	16	24	0 / 4-800F
SFP+ Interface (10GbE)	2 (10/12)	0	0	0	0	0
Modular Expansion Slots	5 / 4 FMC	2 SW and 2 DW AMC	1 SW AMC	1 SW AMC	1 SW AMC and 6 FSM	No
Switch / LAN Interface	0	0	0	0	0	0
Hot-Swappable Power Supplies	Yes	Yes	Yes	Yes	Yes	No
VDOMs (Max)	Up to 250	Up to 250	Up to 250	Up to 250	Up to 25	10

ENTERPRISE APPLIANCES							
Features	FortiGate-620B /-620B-DC (with AMC)	FortiGate-500A	FortiGate-400A	FortiGate-310B /-310B-DC FortiGate-311B (with AMC)	FortiGate-300A	FortiGate-200B /-200B-POE	FortiGate-224B /-200A
Firewall Throughput (512 Byte)	16 Gbps (20 Gbps)	600 Mbps	500 Mbps	8 Gbps (12 Gbps)	400 Mbps	5 Gbps	150 Mbps
IPSec VPN Throughput	12 Gbps (15 Gbps)	150 Mbps	140 Mbps	6 Gbps (9 Gbps)	120 Mbps	2.5 Gbps	70 Mbps
Concurrent Sessions	1 M	500 K	500 K	600 K	400 K	500 K	400 K
Sessions Per Sec	25 K	10 K	10 K	20 K	10 K	15 K	4 K
Antivirus Throughput	350 Mbps	120 Mbps	100 Mbps	160 Mbps	70 Mbps	95 Mbps	30 Mbps
Intrusion Prevention Throughput	1 Gbps	400 Mbps	300 Mbps	800 Mbps	200 Mbps	500 Mbps	100 Mbps
10/100 Interface	0	8	4	0	4	8	26 / 8
GbE Interface	20	2	2	10	2	8	0 / 2
SFP Interface	0	0	0	0	0	0	0
SFP+ Interface (10GbE)	0	0	0	0	0	0	0
Modular Expansion Slots	1 SW AMC	No	No	1 SW AMC 64GB (311B)	No	No	No
Switch / LAN Interface	0	4	0	0	0	8	24 / 4
Hot-Swappable Power Supplies	Opt. Ext. Red. AC Power	No	No	Opt. (310B) Yes (311B)	No	No	No
VDOMs (Max)	10	10	10	10	10	10	10

SMB/ROBO/SOHO APPLIANCES								
Features	FortiGate-110C / -111C	FortiGate Voice-80C	FortiWiFi Voice-80CS	FortiGate-82C	FortiGate-80C / -80CM FortiWiFi-80CM / -81CM	FortiGate-60C FortiWiFi-60C	FortiGate-50B / -51B FortiWiFi-50B	FortiGate/ WiFi-30B
Firewall Throughput (512 Byte)	500 Mbps	500 Mbps	500 Mbps	350 Mbps	350 Mbps	1 Gbps	50 Mbps	30 Mbps
IPSec VPN Throughput	100 Mbps	100 Mbps	100 Mbps	80 Mbps	80 Mbps	70 Mbps	48 Mbps	5 Mbps
Concurrent Sessions	400 K	400 K	400 K	100 K	5 K	80 K	25 K	5K
Sessions Per Sec	10 K	10 K	10 K	5 K	50 Mbps	3 K	2 K	1K
Antivirus Throughput	65 Mbps	65 Mbps	65 Mbps	50 Mbps	100 Mbps	20 Mbps	19 Mbps	5 Mbps
Intrusion Prevention Throughput	200 Mbps	200 Mbps	200 Mbps	100 Mbps	6 / 1 FE DMZ	60 Mbps	30 Mbps	10 Mbps
Switch/LAN Interfaces	8 FE	8 FE	6 / 1 FE DMZ	0	2 GbE	5 GbE / 1 FE DMZ	3 FE	3 / 4 FE
WAN Interfaces	2 GbE	2 GbE	2 GbE	4 GbE	FW-80CM/ 81CM	2 FE	2 FE	1 FE
Wireless Interfaces	No	No	802.11 a/b/g/n	No	WiFi a/b/g/n	FW-60C a/b/g/n	FW-50B WiFi b/g	FW-30B WiFi b/g
Other Interfaces	USB, COM, 32 GB SSD(111C)	4 FXO, Concurrent Calls: 20	Concurrent Calls: 20	1TB Storage & 3 open slots	ExpressCard Slot, Modem (80/81CM), 32 GB SSD (81CM)	ExpressCard Slot, SD Slot include 4 GB card, 1 USB-A and 1 USB-B port, POE-Powered (FW-60C)	POE-Powered (FortiWiFi), USB, COM, 32GB SSD (51B)	USB, COM
VDOMs (Max)	10	10	10	10	10	10	10	0



## FortiWiFi Voice-80C

All-in-One: UTM-Security und Telefonanlage



### Integriertes Business Gateway

Die FortiWiFi Voice-80C ist eine multifunktionale Multi-Layer Security-Plattform, die kleine und mittlere Unternehmens-Standorte mit einer nahezu vollständigen IT-Infrastruktur ausstattet. Sie kombiniert die Funktionalität einer umfassenden Mutli-Threat Appliance mit der eines VoIP-Gateways, einer Telefonanlage, eines Routers sowie der eines Switches in einem einzigen Gerät. Sämtliche Funktionen werden über eine einzige Benutzeroberfläche administriert, wodurch eine hohe Benutzerfreundlichkeit und hohe Effizienz erreicht werden.

Damit wird die FortiWiFi Voice-80C den Anforderungen der Unternehmen gerecht, mehr Funktionalität und Sicherheit mit geringem Kostenaufwand zu erzielen.

### Umfassender Schutz vor Angriffen

Die FortiWiFi Voice-80C bietet umfassenden Schutz gegen alle Arten von Angriffen, insbesondere den neueren Ausprägungen wie z.B. Blended Threats, einer Kombination aus unterschiedlichen „klassischen“ Bedrohungen. Erreicht wird dieses hohe Sicherheitsniveau durch Fortinets außergewöhnlich umfassendes Security-Technologiespektrum:

- Firewall
- VPN (SSL und IPsec)
- Dynamisches Routing
- AntiVirus/AntiMalware
- URL-Filter
- AntiSpam
- Applikationskontrolle
- Intrusion Prevention (IPS)
- Data Loss Prevention (DLP)
- Endpoint Security (NAC)
- SSL Inspection

### Flexibilität

Die acht Ports der FortiWiFi Voice-80C bieten erlauben das flexible Einrichten verschiedener Sicherheits-Zonen für verschiedene Abteilungen, Anwender, Geräte oder Zugangsmethoden. Der integrierte FortiASIC Content Prozessor sorgt für die nötige Performance bei rechenintensiven Security-Checks, wie etwa bei AntiVirus oder AntiSpam – so beeinträchtigt die FortiWiFi Voice-80C in keiner Weise die Performance der Netzwerk-Infrastruktur. Die integrierte WLAN-Option ermöglicht überdies die flexible Anbindung mobiler Endgeräte über das Funkverbindungen. Durch die Integration in die Security-Engines ist auf diese Weise auch die Sicherheit in diesem sonst sehr unsicheren Infrastrukturbereich gewährleistet.

### Zertifizierungen

Die vier ICSA-Labs zertifizierten Inspection-Technologien stellen sicher, dass Anwender höchste Sicherheit erhalten und geltende Compliance-Regeln wie etwas PCI DSS eingehalten werden. ICSA Labs bietet allgemein anerkannte und unabhängige Zertifizierungen für End-User und Großunternehmen.

### Integrierte Telefonanlage

Die VoIP-basierende integrierte Telefonanlage bietet alle Funktionen, die in einer typischen Büroumgebung erforderlich sind. Es können bis zu 50 Rufnummern verwaltet und bis zu 20 Anrufe parallel geführt werden. Konferenzschaltungen, Anrufweiterleitungen und ein flexibler Anrufbeantworter sind nur einige der vielen möglichen Optionen. Als Endgeräte können die von Fortinet angebotenen SIP-Phones FortiFone-100 oder andere handelsübliche SIP-Endgeräte oder –SoftClients zum Einsatz kommen.

Die Anbindung der FortiWiFi Voice-80C an eine zentrale VoIP-TK erfolgt via SIP-Trunk, alternativ ist über einen separat erforderlichen Adapter die Anbindung an einen lokalen Telefonanbieter möglich.



## FortiAP-220A

Sicherer WLAN Zugang für Unternehmen



Fortified Wireless Space

Fortinet ist bekannt für Sicherheitslösungen, die umfassenden und höchsten Schutz sowohl für kabelgebundene wie kabellose (Wireless) Netzwerke bieten. Die neue Serie von Thin Access Points in Verbindung mit einer Vielzahl von Wireless Controllern bietet High-Performance Netzwerkzugänge mit integrierter Content-Security.

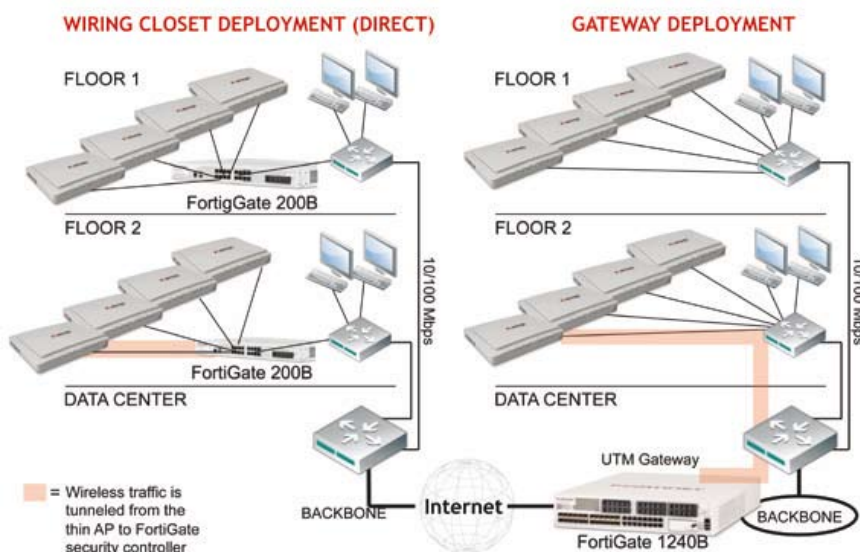
Durch die Kombination eines Wireless Controllers mit einer FortiGate Plattform (größer als Modell FG50x) wird das Sicherheitsniveau des kabelgebundenen LANs automatisch auf die WLAN-Umgebung übertragen. Der gesamte WLAN-Traffic wird so identitäts-basierend über die UTM-Engines der FortiGate Appliance geleitet und dort entsprechend analysiert und es werden nur autorisierte Verbindungen zugelassen. Durch diese Integration ist es möglich von einer einzigen Konsole aus den Netzwerkzugang zu überwachen, Regelwerke einfach und schnell upzudaten und den Datenverkehr und die Einhaltung von Compliance-Regeln kontinuierlich zu überwachen. Da jede FortiGate Appliance (größer als Modell FG50x) ab FortiOS 4.1. über diese Wireless-Controller Funktionalität verfügt, können bereits bestehende Gateways durch ein einfaches Betriebssystem-Update um dieses Feature erweitert werden – die Anschaffung einer zusätzlichen Plattform mit einer eigenen Administrations-Oberfläche entfällt.

Durch die hohe Performance und große Reichweite der neuen FortiAP-Serie ist der Aufbau einer hochsicheren und leistungsstarken WLAN-Infrastruktur einfach und kostengünstig möglich. In vielen Anwendungsszenarien erübrigt sich unter Umständen sogar das Installieren einer Verkabelung bis zum Arbeitsplatz, da die Durchsatzraten der WLAN-Lösung vielfach äquivalent hoch sind.



### Zu den weiteren Eigenschaften dieser Produktlinie gehören:

- Erkennung und Reporting von nicht erlaubten Access Points (sog. Rogue APs)
- granulare Endpoint-Kontrolle
- Standard-Reports, die für Audits nutzbar sind
- 802.11n Support (parallel zu a/b/g) basierend auf 2x2 Multiple-In/Multiple-Out (MIMO) Technologie
- Volle Integration in das umfangreiche UTM-Feature-Set einer FortiGate-Appliance
- Spannungsversorgung des FortiAP über das LAN-Kabel (POE-Funktion, nur bei FortiAP 210-Serie)





## FortiMail™ – Email Security



Fortinets FortiMail™ System bietet eine Fülle von zuverlässigen und hochleistungsfähigen Funktionen, um Spam-Nachrichten und ihre schädlichen Anhänge zu ermitteln, zu markieren, unter Quarantäne zu stellen und zu blockieren. Eine rasche Installation bei niedriger Gesamtinstandhaltung in Kombination mit Fortinets preisgekrönter Verwaltungsschnittstelle gewährleisten hohe Benutzerfreundlichkeit bei niedrigen Gesamtbetriebskosten, was die FortiMail™ zu den leistungsstärksten und kostengünstigsten E-Mail-Security-Systemen am Markt macht. Durch die Verwendung von FortiMails integrierter Anti-Spam- und Anti-Virus-Security können kleinere Unternehmen kosteneffizient Spam bekämpfen, ohne zusätzliche Server einzurichten..

### SECURE MESSAGING APPLIANCES

PRODUCT	10/100/1000 Ethernet	10/100 Ethernet	Base System Storage Capacity	RAID Storage Management	Email Domains	Policies (Domain / Sys)	Server Mode Mailboxes	Hardware Form Factor	Profiles (Domain / Sys)	Email Routing (Mgs / Hr)	Antispam (Mgs / Hr)	Redundant Power
FortiMail-5001A	2	0	80 GB	N/A	10.000	1.500 / 7.000	3.000	ATCA Blade	50 / 600	1,4 Million	1,3 Million	Yes
FortiMail-2000B	6	0	1 TB	0, 1, 5, 10, 50	5.000	1.500 / 7.000	3.000	Rack Mount (2-RU)	50 / 600	1,1 Million	1,1 Million	Yes
FortiMail-400B	4	0	500 GB	Opt - 0, 1	500	600 / 3.000	1.000	Rack Mount (1-RU)	50 / 200	264.600	234.000	No
FortiMail-100C	2	1	1 TB	N/A	50	60 / 300	200	Desktop	50 / 60	64.800	57.600	No

Bei Großunternehmen mit mehreren Mail-Servern erhöht FortiMail™ die E-Mail-Performance. Die Verwendung von DNS MX gewichteten Warteschleifen bietet Redundanz, wobei eine Verlangsamung und ein Belastungsausgleich des Spam- und Anti-Virus-Scanning bei einem Betrieb im Gateway-Modus berücksichtigt wird.

Service Provider können von FortiMails integriertem Antispam- und Anti-Viruschutz profitieren und eine zweireihige, mehrschichtige Security-Lösung schaffen. Authentifizierungsserver (LDAP, RADIUS, IDAP, POP3, SMTP, IMAP) werden zur Authentifizierung von Anwendern und Domains implementiert. Jede vom MSSP verwaltete E-Mail-Domain fließt durch FortiMail™, die pro Domain eigene Kontrollen besitzt.



## FortiAnalyzer – zentralisiertes Reporting



Die FortiAnalyzer-Produktfamilie bietet Echtzeit-Netzwerk-Logging-, Analyse- und Reporting-Funktionen in Form einer Appliance, die auf sichere Weise Log-Daten von FORTINET-Geräten und auch von Produkten anderer Hersteller zusammenführen. Sämtliche Informationen über Traffic, Events, Viren, Angriffe, Web-Inhalte und E-Mail-Daten können archiviert und kontrolliert werden. Eine umfassende Auswahl an Standardberichten gehört ebenso zum Lieferumfang wie die Möglichkeit, beliebige benutzerdefinierte Reports zu generieren. FortiAnalyzer bietet außerdem erweiterte Sicherheitsmanagement-Funktionen wie die Archivierung von Quarantäne-Dateien, Ereignis-Korrelation, Vulnerability Assessments, Traffic-Analyse und die Archivierung von E-Mail-, Webzugriffs-, Instant-Messaging- und Dateitransfer-Inhalten.



### MANAGEMENT, ANALYSIS, & REPORTING APPLIANCES

PRODUCT	10/100/1000 Ethernet	10/100 Ethernet	Base System Storage Capacity	Network Devices (Max)	FortiClient Agents (Max)	Centralized Quarantine	Number of Hard Drives	RAID Storage Management	Data Receive Rate	Log Perf. (Logs / Sec)	Recommended Device	Redundant Power
FortiAnalyzer-4000A	2	0	6 TB	2.000	No Restriction	Yes	12	0, 1, 5, 10, 50	20 Mbps	Up to 5.000	All Models	Yes
FortiAnalyzer-2000B	6	0	2 TB	2.000	No Restriction	Yes	2 (Optional - 4)	0, 1, 5, 10, 50	12 Mbps	Up to 3.000	All Models	Yes
FortiAnalyzer-1000B	4	0	1 TB	2.000	No Restriction	Yes	1 (Optional - 1)	Opt - 0, 1	4 Mbps	Up to 1.000	All Models	No
FortiAnalyzer-400B	4	0	500 GB	200	2.000	Yes	1 (Optional - 1)	Opt - 0, 1	2 Mbps	Up to 500	All Models	No
FortiAnalyzer-100C	2	1	1 TB	100	100	Yes	1	N/A	800 Kbps	Up to 200	All Models	No



## FortiManager – zentralisiertes Management

HW

Die FortiManager-Produktlinie umfasst Lösungen, mit denen sich ein zentralisiertes Managementsystem aufbauen lässt. Es integriert nahtlos die mehrstufigen Sicherheitslösungen von FORTINET und stellt so ein koordiniertes, richtliniengestütztes Provisioning, zentrale Gerätekonfiguration und Update-Management zur Verfügung. Hinzu kommen End-to-End-Netzwerk-Monitoring und Geräteüberwachung. FortiManager reduziert sowohl die Implementierungskosten als auch die Betriebskosten, die mit dem Aufbau, der Konfiguration, der Überwachung und der Wartung eines sicheren Netzwerks verbunden sind. Rollenbasiertes Management erlaubt es, mit klar definierten User-Rechten zu arbeiten und einzelnen Administratoren bestimmte Domänen oder Funktionsbereiche zuzuweisen. Device Grouping dient dazu, FORTINET-Sicherheitslösungen im Netz gruppenweise in unabhängige Verwaltungs-Domains zusammenzufassen, um den Administrationszugriff kontrollierbar zu machen und die zielgerichtete Verteilung von Richtlinien zu erleichtern. Die lokale Bereitstellung von Updates für die Bedrohungssignatur- und Filterdatenbank verringern die Reaktionszeiten auf Angriffe.

MANAGEMENT, ANALYSIS, & REPORTING APPLIANCES												
PRODUCT	10/100/1000 Ethernet	10/100 Ethernet	Base System Storage Capacity	Administration Domain	Administrative Web Portals	Web Portal Users (Max)	Local Hosted Security Content	Hardware Form Factor	Network Devices (Max)	FortiClient Devices	Model Restrictions	Redundant Power
FortiManager-5001A	2	0	80 GB	100	100	4.000	AV, IPS, VM, WF, AS	ATCA Blade	4.000	100.000	None	Yes
FortiManager-3000C	4	0	2 TB	200	100	4.000	AV, IPS, VM, WF, AS	Rack Mount (2-RU)	5.000	120.000	None	Yes
FortiManager-1000C	4	0	1 TB	50	50	500	AV, IPS, VM, WF, AS	Rack Mount (1-RU)	800	25.000	FG-5000 Series	No
FortiManager-400B	4	0	500 GB	10	10	200	AV, IPS, VM	Rack Mount (1-RU)	200	10.000	FG-5000 Series	No
FortiManager-100C	2	1	1 TB	10	10	200	AV, IPS, VM	Desktop	20	2.500	FG-5000 Series	No



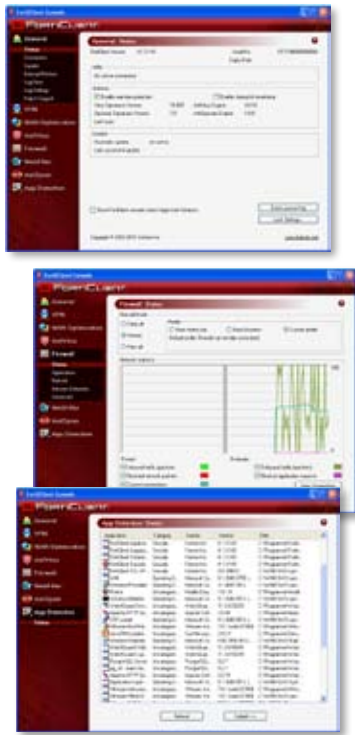
## FortiClient – Endpoint Security

SW

PCs und Laptops erlauben es heutigen Business-Anwendern, auf Unternehmensanwendungen und kritische Informationen sowohl am Arbeitsplatz als auch von unterwegs zuzugreifen. Die Verbreitung hoch mobiler Smartphones, die offene Betriebssysteme einsetzen, verspricht einen noch freizügigeren Zugriff auf Enterprise Applications und Daten. Unglücklicherweise sind alle mobilen Endgeräte Blendet Threats ausgesetzt, für die die Angreifer Viren, Spam, Spyware und Würmer verwenden. Gleichzeitig haben Anwender, die ungeeigneten und gefährlichen Web Content aufrufen und damit die Integrität ihrer Geräte untergraben, einen negativen Einfluss auf die Produktivität und verletzen die Richtlinien ihrer Unternehmen für die Nutzung von Content. Security-Agent-Technik ist für Endgeräte verfügbar, etwa in Form von Antivirus-Agenten. Sie dient zur Sicherung der Devices vor einzelnen, bestimmten Gefahren. Damit gelingt es aber nicht, einen umfassenden Schutz vor Blended Threats aufzubauen. Außerdem ist es mit dieser Agententechnik nicht möglich, Richtlinien für den Zugriff auf Inhalte durchzusetzen.

FortiClient PC und FortiClient Mobile stellen vereinheitlichte Agentenfunktionen für PCs und Smartphones zur Verfügung, darunter Personal Firewall, IPSec-VPN, Antivirus, Antispyware, Antispam und Web-Content-Filter. Der FortiClient-Agent wird auf der Basis der FortiGuard Security Subscription Services betrieben. So ist sichergestellt, dass die Devices gegen aktuelle Blended Threats umfassend geschützt sind. Die FortiClient-Agenten stellen geringe Installationsanforderungen und sind für die Betriebssysteme Microsoft Windows XP, Microsoft Vista, Windows Mobile und Symbian verfügbar

**FortiClient PC**



**FortiClient Mobile**



**FortiClient Host Security**



**Das Problem:**

PCs und Laptops erlauben es heutigen Business-Anwendern, auf Unternehmensanwendungen und kritische Informationen sowohl am Arbeitsplatz als auch von unterwegs zuzugreifen. Die Verbreitung hoch mobiler Smartphones, die offene Betriebssysteme einsetzen, verspricht einen noch freizügigeren Zugriff auf Enterprise Applications und Daten. Unglücklicherweise sind alle mobilen Endgeräte Blendet Threats ausgesetzt, für die die Angreifer Viren, Spam, Spyware und Würmer verwenden. Gleichzeitig haben Anwender, die ungeeigneten und gefährlichen Web Content aufrufen und damit die Integrität ihrer Geräte untergraben, einen negativen Einfluss auf die Produktivität und verletzen die Richtlinien ihrer Unternehmen für die Nutzung von Content. Security-Agent-Technik ist für Endgeräte verfügbar, etwa in Form von Antivirus-Agenten. Sie dient zur Sicherung der Devices vor einzelnen, bestimmten Gefahren. Damit gelingt es aber nicht, einen umfassenden Schutz vor Blended Threats aufzubauen. Außerdem ist es mit dieser Agententechnik nicht möglich, Richtlinien für den Zugriff auf Inhalte durchzusetzen.

**Die Lösung:**

FortiClient PC und FortiClient Mobile stellen vereinheitlichte Agentenfunktionen für PCs und Smartphones zur Verfügung, darunter Personal Firewall, IPSec-VPN, Antivirus, Antispyware, Antispam und Web-Content-Filter. Der FortiClient-Agent wird auf der Basis der FortiGuard Security Subscription Services betrieben. So ist sichergestellt, dass die Devices gegen aktuelle Blended Threats umfassend geschützt sind. Die FortiClient-Agenten stellen geringe Installationsanforderungen und sind für die Betriebssysteme Microsoft Windows XP, Microsoft Vista, Windows Mobile und Symbian verfügbar.

**FortiClient PC & FortiClient Mobile Kernfunktionen:**

- **Antivirus & Antispyware** – stellt umfassenden Schutz gegen Viren, Spyware, Keylogger, Trojaner, Adware und Greyware für Windows-gestützte Laptops, Desktops und Smartphones zur Verfügung. Auch Symbian-gestützte Smartphones werden unterstützt.
- **Sicheres IPSec-VPN** – stattet Windows-gestützte mobile Laptops, Desktops und Smartphones mit der Fähigkeit aus, auf Unternehmensanwendungen sicher mit DES- und 3DES-Verschlüsselung zuzugreifen.
- **Leistungsfähige Personal Firewall** – kontrolliert den Netzwerk-Traffic und setzt auf Windows-gestützten Laptops, Desktops und Smartphones und Symbian-Smartphones die jeweils angemessene Anwendungs-Zugriffskontrolle durch.
- **Starke Antispam-Funktionen** – hervorragender Spamschutz, der sich nahtlos in Microsoft Outlook für Windows sowie in SMS-Antispam für Windows und Symbian-gestützte mobile Smartphones integriert.
- **Web-Content-Filter** – setzt in Echtzeit Regeln für den Zugriff auf Web-Content durch, um Compliance zu Regularien sicherzustellen. Erhältlich für Windows-gestützte Laptops und Desktops.

- Appliance-Lösung
- Einfachste Installation und Integration
- Geringe TCO
- Einfaches Management
- Integration in Fortinet-Produkt-Familie



**FortiDB – Datenbank Security**



Den erhöhten Schutzbedarf im Datenbankbereich deckt FORTINET mit einer neuen Reihe von Security-Appliances ab, die speziell für das Vulnerability-Assessment in Datenbanken konzipiert ist. Die FortiDB ist eine automatisierte und zentralisierte Sicherheitslösung, die Datenbankapplikationen stabilisiert, indem sie potenzielle Angriffspunkte - etwa Schwachstellen in Passwörtern, Zugriffsberechtigungen und Konfigurationen - aufdeckt. Dabei setzt die Appliance Warnungen an den Systemadministrator ab und bietet Korrekturhilfen an. Die FortiDB-Produktfamilie schützt vor externem und internem Diebstahl von firmeneigenen und persönlichen Daten und erkennt auch Zugriffe scheinbar legitimer Nutzer. Allen Produkten gemeinsam sind die drei Feature-Sets 24x7 Überwachung der Datenbankaktivität, Datenbank-Audits und Vulnerability Assessment. Letzteres sorgt für die „Abhärtung“ von Datenbanken, indem Schwachstellen in Passwörtern, Zugangsberechtigungen und Konfigurationseinstellungen aufgedeckt werden.

## DATABASE SECURITY APPLIANCES

PRODUCT	10/100/1000 Ethernet	# Database Instances	Base System Storage Capacity	RAID Storage Management	Redundant Power	Database Support / Asset Agent Licenses	Repository Database Support
FortiDB-2000B	4	60	1 TB	No	Yes	DB2 UDB V8, DB2 UDB V9; Microsoft SQL Server 2000, Microsoft SQL Server 2005; Oracle 8.1.6, Oracle 8.1.7.4, Oracle 9.2.0.x, Oracle 10.2.0.x, Oracle 11.1.0.x; Sybase ASE 12.5.4, Sybase ASE 15.0.2	Apache Derby 10.x, DB2 UDB v9, Microsoft SQL Server 2005, Oracle 10gR2, PostgreSQL 8.3
FortiDB-1000B	4	30	1 TB	No	No		
FortiDB-400B	4	10	500 GB	No	No		



## FortiWeb – Applikation Firewall

HW

Die FortiWeb bietet Schutz für Web-Applikationen, Datenbanken und deren Datenverkehr anhand von Applikations- und XML-Firewall-Funktionen und beschleunigt zugleich die Anwendungen durch Lastausgleich. Zusammen mit den „FortiDB“-Produkten zur Datenbank-Security bietet die FortiWeb ein breites Security-Spektrum für Cloud Computing und andere Anwendungen im Unternehmen, bei denen vertrauliche oder persönliche Daten über Internet oder Intranet ausgetauscht werden.

**Durch XML/SSL-Offloading** mit den Forti-ASIC CP6 lässt sich eine Content-Beschleunigung erreichen, die auch die FortiGate-Security-Produkte zur Performance-Steigerung nutzen. Die Ressourcenverteilung wird ausgeglichen, indem Lasten verteilt und Content über mehrere Web-Server geroutet werden. Es besteht Übereinstimmung mit Version 1.2 der PCI-Richtlinien, weil die Web-Application-Firewall öffentlich zugänglichen Web-Applikationen vorgeschaltet ist, um webbasierte Angriffe zu erkennen und abzuwehren. Die Forti-Web- und Forti-DB-Appliances arbeiten unabhängig voneinander, lassen sich aber auch als Tandem-Sicherheitslösung einsetzen. In der Netzwerktopografie sitzt die Fortiweb-Appliance inline vor den Web-Applikationsservern, während die Forti-DB out-of-band die Datenbanken automatisch überwacht, prüft und scannt.

### Schutz vor:

- Cross Site Scripting (XSS)
- SQL und OS Command Injection
- Cross Site Request Forgery
- Outbound Data Leakage
- HTTP Request Smuggling
- Buffer Overflow
- Remote File Inclusion Attacks
- Encoding Attacks
- Cookie Tampering / Poisoning
- Session Hijacking
- Broken Access Control
- Forceful Browsing / Directory Traversal / Site Recon / Google Hacking
- OWASP Top 10

## WEB SECURITY APPLIANCES

PRODUCT	10/100/1000 Ethernet	Throughput (HTTP)	Base System Storage Capacity	RAID Storage Management	Redundant Power	Max HTTP Trans / sec	Comprehensive WAF and XML Security Features	Other Features
FortiWeb-1000B	4	500 Mbps	1 TB	No	No	22.000	XML schema validation and expression limiting, WSDL Verification, Form Field Tampering Validation and others	SSL and XML encryption and co-processing, Content base Routing.
FortiWeb-400B	4	100 Mbps	500 GB	Opt - 0,1	No	10.000		
FortiDB-400B	4	10	500 GB	No	No	No		



## FortiScan – Vulnerability Management

HW

Die Appliance FortiScan bietet nicht nur Vulnerability- und Patch-Management auf Client- und Netzwerkebene, sondern unterstützt Unternehmen auch beim Erfüllen von Compliance Vorgaben. Mit einer Speicherkapazität von zwei Terrabyte und bis zu 2.000 pro Einheit unterstützten Endgeräten richtet sich diese Lösung insbesondere an mittelgroße Unternehmen. Jedoch können dank einfacher Skalierbarkeit unbegrenzt viele Endgeräte in den Scan-Prozess einbezogen werden. Das Vulnerability Management läuft als transparenter Hintergrund-Prozess und erkennt Sicherheitslücken sowie Regelverstöße im gesamten Netzwerk, also auch auf Hosts und Servern.

Während auf Netzwerk-Ebene der FortiAnalyzer die Analyseprozesse übernimmt, wird das Vulnerability Management auf Endgeräten über einen eigenen Client realisiert. Erkennung, Gerätepriorisierung und Scanning erfolgen auf Grundlage frei definierbarer Profile. Der anschließende Patch-Prozess wird um sofort anwendbare Korrekturmaßnahmen ergänzt. Netzwerk- und Security-Verantwortliche könnten Patches nicht nur installieren und verwalten, sondern auch Konfigurationen ändern und das Risiko zu schwachen Einstellungen senken, etwa durch Deaktivieren einer Applikation oder Ablehnen einer Netzwerkanfrage.



## VULNERABILITY MANAGEMENT APPLIANCES

PRODUCT	10/100/1000 Ethernet	Database Instances	Base System Storage Capacity	RAID Storage Management	Redundant Power	Database Support / Asset Agent Licenses	Repository Database Support
FortiScan-1000B	4	NA	2 TB	0, 1	No	Asset Agent Licenses - 2.000	NA

## FortiSwitch



Neue Switching Lösungen für den High Performance Computer Markt

### Next-Generation 10 GbE FortiSwitch™ sind ideale Plattform für Super-Computer und High-Speed Anwendungen sowie für Cloud Computing

„Fortinet’s FortiSwitch Produkte nutzen einzigartige Technologie, um schnellere, aber weniger komplexe Switching Lösungen zu realisieren. Es ermöglichte das Atlas Computer Cluster in Hannover zum schnellsten ethernet-basierenden Computer Cluster der Welt zu machen.“

Dr. Bruce Allen, Direktor der Abteilung "Observational Relativity and Cosmology" am Max Planck Institute für Gravitational Physics (Albert Einstein Institute)

Fortinet bietet mit der neuen „next-generation“ FortiSwitch™ Familie zwei 10 Gigabit Ethernet (GbE) High-Speed Switching Plattformen, die sich durch extrem niedrige Laufzeiten (ultra-low latency), außergewöhnlich hohe Portdichte und „verlustlose“ Skalierbarkeit auszeichnen. Das modulare FortiSwitch-1000 Chassis und der FortSwitch-500 wurden speziell für Hochleistungs-Netzwerke, wie sie von Supercomputern mit extrem rechenintensiven Anwendungen oder von Hochgeschwindigkeits-Anwendungen innerhalb von virtualisierten Server-Umgebungen und Cloud- oder Parallel-Computing Anwendungen benötigt werden, entwickelt.

Mit einer außergewöhnlich hohen Portdichte von bis zu 576 Interfaces (10 GbE) pro Chassis (10HE) kann der FortiSwitch-1000 auf bis zu mehrere tausend „non-blocking“ Ports skaliert werden, um so maximale Performance auf kleinstem Raum im Rechenzentrum zur Verfügung zu stellen. Die Einführung der FortiSwitch Produktlinie komplettiert das Angebot von Fortinet’s bestehender 10GbE Sicherheits-Infrastruktur. Fortinet stellte außerdem den FortiSwitch-100 als „Top-of-the-Rack“-Lösung Switching Plattform vor, welches ebenfalls einen Beitrag zur Kostensenkung in Rechenzentren leisten soll.

Durch die ständig steigenden Bandbreiten-Anforderungen in Rechnzentren, in denen 10GbE Verbindungen bereits die Regel sind, werden Switching-Plattformen benötigt, die sich durch höchste Performance und niedrigste Laufzeiten, vor allem aber durch geringe Abmessungen und einfache Integration hervorheben. Mit den FortiSwitch-Lösungen sind wire-speed Verbindungen bei höchster Skalierbarkeit, verbunden mit der gewohnten Einfachheit und Robustheit des Standard-Ethernet möglich. Durch Einsatz von Fortinet’s vScale™ multi-path traffic switching and dynamic congestion avoidance features wird eine quasi non-blocking Umgebung geschaffen, indem Daten in Echtzeit über den Weg mit der geringsten Laufzeit geroutet werden, und das bei Einhaltung aller Ethernet-Standards.

#### SWITCHING PLATFORMS

PRODUCT	10 GbE Ports (Max)	Through-put (Max)	Latency (Port-to-Port)	MAC Address Storage	VLAN Sup-ported	Total Link Agg Groups	Link Agg Group Size	Total Active Flows Mged	Line Cards (Max)	Fabric Cards (Max)	Management Cards (Max)	Redundant Power
FortiSwitch-1000	144	2.9 Tbps	1.6 us	16.000	4.000	72	Up to 6	144.000	12	6	2	Yes
FortiSwitch-500	24	480 Gbps	2.4 us	32.000	4.000	12	Up to 8	24.000	N/A	N/A	N/A	Yes
FortiSwitch-100	4 / 48	176 Gbps	N/A	8.000	512	6	Up to 8	N/A	N/A	N/A	N/A	No

### FortiSwitch Übersicht



Der **FortiSwitch-1000** ist vollständig redundant, modular und bietet auf 10 HE bis zu 144 Ports (10GbE). Mehrere Chassis können für maximale Skalierbarkeit verbunden werden. Der FortiSwitch-1000 ist interoperabel mit den kleineren FortiSwitch-500/100 Appliances.

Der **FortiSwitch-500** ist vollständig redundant und bietet auf 1 HE 24Ports (10GbE). Mehrere Chassis können für maximale Skalierbarkeit verbunden werden. Der FortiSwitch-500 ist interoperabel mit den FortiSwitch-1000/100 Appliances.

Der **FortiSwitch-100** ist eine 1 GbE und 10GbE Switching Plattform, konzipiert als „Top-Rack-Lösung“. Auf 1 HE bietet der FortiSwitch-100 wire speed Layer 2/3/4 Switching Features zu extrem niedrigen Kosten. In Verbindung mit den FortiSwitch-1000 oder -500 Plattformen, reduziert der FortiSwitch-100 die Gesamtkosten um ein vielfaches. Der FortiSwitch hat 48 wire speed 10/100/1000 Ports mit optionalen Uplinks (4 x 10 GbE active CX4 oder 4 x 10 GbE SFP+).

## Ihr Vorteil: Das Wick Hill Service Programm



### Support

Wick Hill hilft bei der Fehlerbehebung im laufenden Betrieb. Wir garantieren schnelle Hilfe bei Konfigurationsproblemen, Updates und Einstellungen. Über Wick Hill haben Sie den besten Draht zu den jeweiligen Ansprechpartnern auf Seite der Hersteller. Wir arbeiten sehr eng mit unseren Anbietern zusammen und können daher gezielt und effizient zugreifen. Darüber hinaus geben wir gerne Tipps & Tricks für den reibungslosen Ablauf der Installation sowie bei allen Fragen rund um das Thema Betriebssystem-Kompatibilität. Unsere technische Support-Hotline ist Montag bis Freitag von 8.30 Uhr bis 17.30 Uhr für Sie besetzt: Telefon: +49 (0)40 237301-25 E-Mail: support@wickhill.de



### Erweiterter Support

Über unsere erweiterte Support-Leistungen können Kunden direkt von unserer Installationsunterstützung profitieren. Wir unterstützen Sie beim Rollout von Appliances oder Software und führen die Softwareverteilung sowie deren -Konstellation durch.



### Consulting / Installation

Unser Team verfügt über ein großes Know-how und ist hervorragend ausgebildet. In Sachen Installation können wir Sie effizient und schnell unterstützen, gerne auch direkt vor Ort. Eine reibungslose Inbetriebnahme ist damit auch für Kunden ohne Spezialwissen oder Erfahrung kein Problem mehr. Gerne setzen wir für Sie, gemeinsam mit Resellern, einen Workshop zur Installationsunterstützung auf, der Sie Schritt-für-Schritt mit der Implementierung, der Rollout-Planung und der -Durchführung vertraut macht.



### Virtuelles Testcenter

Über unser Virtuelles Testcenter lässt sich via VPN/ SSL auf Appliances oder Serversysteme zugreifen. So können wir Szenarien für unsere Kunden nachstellen und konfigurieren. Darüber hinaus besteht die Möglichkeit, dass sich Kunden selbst mit einzelnen Geräten vertraut machen und ausprobieren können - sowohl während unserer Schulungen als auch im Rahmen unseres Testgeräteprogramms. Nutzen Sie beim Gerätetest im Virtuellen Testcenter den direkten Draht zu unseren Trainern, die Ihnen beim Erkunden von GUI oder Konfigurationsmöglichkeiten quasi virtuell zur Seite stehen.



### Schulungen / Trainings

In unseren Trainings und Schulungen vermitteln wir den Teilnehmern alle wichtigen Elemente und Besonderheiten der Produkte - in Theorie und Praxis. Hier gehen wir in die Tiefe und beschäftigen uns insbesondere mit special features, so dass die Teilnehmer das Maximum aus ihren Geräten herausholen können. Darüber hinaus besteht die Möglichkeit, innerhalb von Trainingsreihen jeweilige Zertifizierungen zu erhalten.



### Workshops

In unseren Workshops erhalten Teilnehmer einen Schnellkurs zu unseren Produkten. Anhand von Praxisübungen und -beispielen vermitteln wir fundiertes Basiswissen über Funktionalitäten und Spezifikationen. Sie erfahren in den Workshops alles über die Kompatibilität der Produkte, eine Vorstellung unseres Supportverfahrens bis hin zum Troubleshooting. Für tiefer gehendes Know-how empfehlen wir unsere Trainings.



### Webinare

Wir gestalten regelmäßig einstündige Webinare. Dabei erhalten unsere Partner nicht nur Einblicke in unser Produktportfolio und zu neuen Produktfunktionalitäten, sondern können insbesondere direkt mit uns in Kontakt treten und sich über spezielle Themen informieren. Sowohl Technik-Support als auch Vertriebsunterstützung haben einen hohen Stellenwert in unserem Service - und bieten regelmäßig zu diesen Themen Webinare an.

*Mit unseren Value-Added-Services stehen Sie immer auf der Gewinnerseite: Denn unsere Zusatzdienste wie Pre- und Post-Sales-Support, Schulungen und Marketing-Unterstützung verschaffen Ihnen als Fachhändler oder Partner echte Wettbewerbsvorteile. Unser Engagement für den Channel zeigen wir durch enge Zusammenarbeit mit Endkunden, beispielsweise bei der Suche nach dem passenden Produkt oder der richtigen Bezugsquelle. Wir verstehen uns als Bindeglied zwischen Hersteller und Fachhandel, und hinter all dem steht ein erfahrenes und hoch motiviertes Service-Team für technische Unterstützung, Training, Installation und Beratung. Fragen und Anregungen sind immer herzlich willkommen - wir stehen Ihnen jederzeit gerne zur Verfügung!*



### Wick Hill 24Plus Austauschservice

**Bieten Sie echten „Value Ad“ – mit unserem 24Plus Austauschservice!**

Mit unserem Extra-Service 24Plus können Sie gegenüber Ihrem Kunden gewährleisten, dass seine defekte Appliance innerhalb von 24 Stunden ausgetauscht wird. Im Rahmen dessen können Sie außerdem vom Service unseres Supportteams profitieren, das Ihnen dabei hilft, den Defekt zu lokalisieren. Durch das Einbinden unseres Supportteams entlasten Sie Ihren Helpdesk und sorgen für einen reibungslosen und vereinfachten Ablauf. Der 24Plus Austauschservice ist ein weiteres Werkzeug zur Kundenbindung - nutzen Sie diesen Service als zusätzliches Verkaufsargument, um sich vom Wettbewerb abzusetzen und Ihrem Kunden ein noch besseres Security-Paket anbieten zu können. Werden Sie zum Value Ad-Reseller mit unserem 24Plus Austauschservice!

*Für mehr Informationen zum 24Plus Austauschservice steht Ihnen das Wick Hill-Team gerne zur Verfügung.*

# FORTINET

## UTM Marktführerschaft

Fortinet bietet branchenweit die besten Produkte und hat die meisten Auszeichnungen der Netzwerksicherheitsbranche erhalten, einschließlich Security Product of the Year. Das Unternehmen schuf und führt den rasch wachsenden UTM-Markt weiter an. Fortinet ist der einzige Anbieter von 100% eigenen und integrierten ASIC-beschleunigten Netzwerksicherheitssystemen. Unsere Angebote zu Subscription Diensten und unsere Intelligent Systems bieten Unternehmen, MSSP und SMB und beispiellosen Wert, höchste Performance und unerreichte Funktionalität im Vergleich zu einer Einzweck-Sicherheitsanwendung oder UTM-Angeboten anderer Anbieter.

## Industrie Zertifizierungen

Lösungen von Fortinet haben die meisten Branchenzertifikate erhalten, darunter: FIPS 140-2, Common Criteria EAL4+ und verschiedene ICSA Labs Zertifizierungen, darunter SSL-TLS (VPN), IPSec, n IPS, Antivirus und Firewall. Lösungen von FortiGate sind zudem die einzigen UTM-Systeme, die von den unabhängigen NSS-Testlabors sowohl für IPS und UTM zertifiziert wurden.

## Industrie Auszeichnungen

Seit seiner Gründung berücksichtigte die Netzwerksicherheitsbranche Fortinet mit mehr als 80 Auszeichnungen, darunter Security Product of the Year und Best Integrated Security Solution. Das Unternehmen schuf und führt den rasch wachsenden UTM-Markt weiter an. Fortinet ist der einzige Anbieter von 100 % eigenen und integrierten ASIC-beschleunigten Netzwerksicherheitssystemen. Die Kombination von Sicherheitsplattformen mit Angeboten zu den FortiGuard Subscription Diensten bietet Unternehmen, Service Providern, Klein- und mittelständischen Unternehmen beispiellosen Wert, höchste Performance und unerreichte Funktionalität im Vergleich zu einer Einzweck-Sicherheitsanwendung oder UTM-Angeboten anderer Anbieter.

**Kontakt:** [www.wickhill.de](http://www.wickhill.de)



ISO 9001



COMMON CRITERIA  
EAL 4+ CERTIFIED



Wick Hill Kommunikationstechnik GmbH · Hammerbrookstraße 90 · 20097 Hamburg  
Tel.: +49 (0) 40 23 73 01-0 · Fax: +49 (0) 40 23 73 01-80 · eMail: [info@wickhill.de](mailto:info@wickhill.de)

Wick Hill Group plc: Wick Hill Limited (Woking) und Wick Hill Kommunikationstechnik GmbH (Hamburg) · Handelsregister: Hamburg B53548 · Geschäftsführer: Kenneth Ward