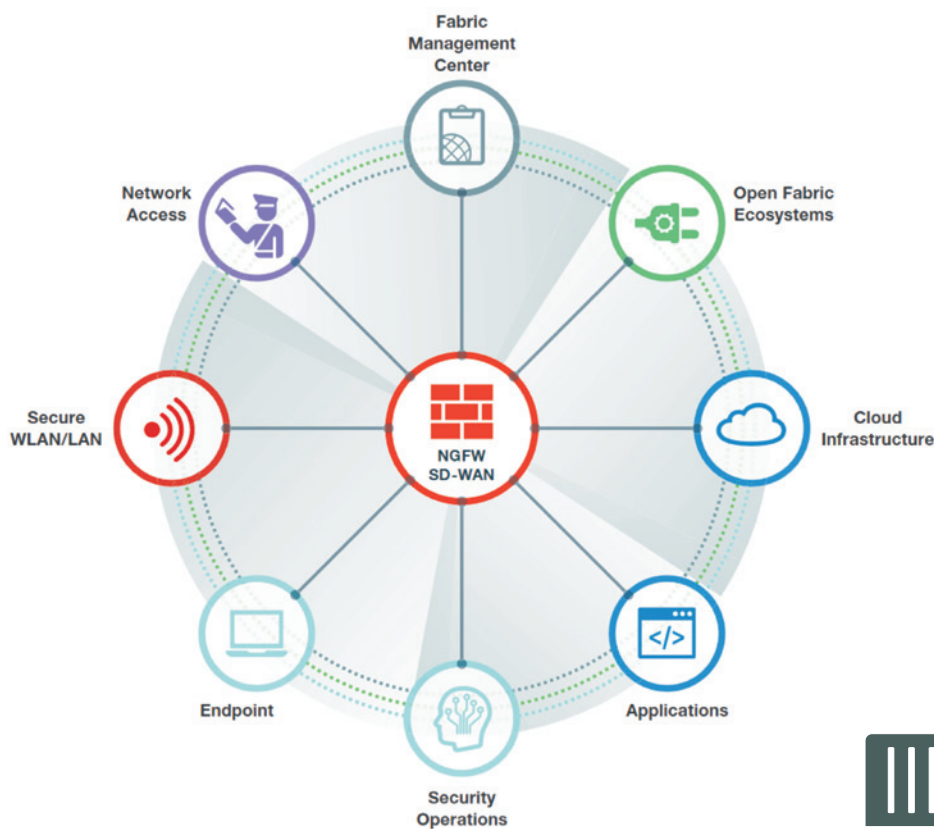


Secure Networks

Fortinet Solutions from Professionals

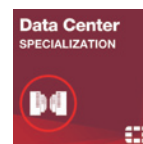


IT-Union GmbH & Co. KG

BUSINESS IT-SOLUTIONS

■ Warum IT-Union?

- **Seit 2003 Partner von FORTINET**
- **Managed Service & 24x7 Support**
- **Schnelle Reaktionszeiten & hohe Flexibilität**
- **25+ Jahre Erfahrung & tiefgreifendes Know-how**
- **15+ zertifizierte System-Ingenieure in DACH (NSE 4-8)**



■ Nutzen Sie unser Wissen und unsere Erfahrung

Die Mitglieder der IT-Union GmbH & Co. KG gehören zu den ältesten und höchst zertifizierten FORTINET-Partnern in Deutschland. Seit 2003 beraten, installieren und betreuen wir Netzwerke mit Produkten und Lösungen dieses Herstellers. Die IT-Union unterstützt Sie u. a. mit 15 zertifizierten System-Ingenieuren (NSE 4-8) kompetent und branchenübergreifend in Projekten mit unterschiedlichster Größenordnung und Komplexität. Das Servicecenter unserer Gruppe bietet Ihnen hierbei individuelle Konzepte inkl. 24x7 Service, flankiert durch ein eigenes Servicelager. Die IT-Union ist Mitglied im europäischen FORTINET 361° Security Forum.

■ IT-Union

Die IT-Union GmbH & Co. KG (ITU) wurde 2008 als Systemhausverbund gegründet und ist ein gemeinsames Tochterunternehmen von den Gesellschaftern BMA networks (Hamburg), GORDION (Troisdorf), INDASYS (Stuttgart) und VINTIN (Schweinfurt). Mit weiteren Büros in Kiel, Fulda und Malters (CH) verfügt die ITU derzeit über sieben Standorte. Die ITU betreut branchenübergreifend Kunden, von Enterprise bis Carrier, und bietet Lösungen mit Fokus auf die Themen:

- **Analyzing**
- **Outsourcing**
- **IT-Sicherheit**
- **Datennetzwerktechnik**
- **Managed- / Cloud-Services**
- **Triple-Play Metronetzwerke**



IT-UNION – SECURE NETWORKS

Die Mitglieder der IT-Union sind bereits seit den frühen 90er Jahren am Markt und verfügen allesamt über ein tiefes Know-how im Bereich der IT. Durch die langjährige Erfahrung unserer Spezialisten in Kombination mit einem über-regionalen sowie flexiblen Service- und Support ist die ITU ein idealer Partner rund um das Thema IT – sowohl für öffentliche Auftraggeber und Organisationen, als auch für Unternehmen in jeglicher Größe.



Unser Fokus

Wir bieten Ihnen langjährige Erfahrung, tiefgreifendes Know-how und hohe Flexibilität, insbesondere zu folgenden Schwerpunkt-Themen:

Datennetzwerktechnik

- Wireless LAN
- Loadbalancing
- WLAN Suite Survey
- IPv4 zu IPv6 Migration
- Triple Play – Metronetze
- Analysen für LAN / WLAN
- Routing, VPN, u.v.m. – WAN
- Server, Storage, Virtualisierung
- RZ-Infrastruktur, Switching, u.v.m. – LAN

IT-Sicherheit und Datenschutz

- Sandboxing
- VPN, SSL, SD-WAN
- Datenschutzconsulting
- Email-, Web- und IoT-Security
- SSO, Authentifizierung, NAC
- Firewalling, Content Security, u.v.m.
- Security Information & Event Mgmt. (SIEM)

Outsourcing, Managed / Cloud-Services

- BPO, Outtasking
- Training und Zertifizierungen
- Systemadministration, Monitoring, u.v.m.
- 24x7-Services (SLA, Spare Parts, u.v.m.)
- Hybride Infrastrukturen u.a. AWS und Azure

NORD

Kiel

BMA networks GmbH
Preetzer Chaussee 55
24222 Schwentinental

Telefon 0431 97449 0
Email vertrieb.ki@it-union.eu

Hamburg

BMA networks GmbH
Albert-Einstein-Ring 5
Arelia-Haus, 22761 Hamburg

Telefon 0431 97449 0
Email vertrieb.hh@it-union.eu

MITTE

Köln

GORDION
Data Systems Technology GmbH
Mottmannstraße 13
53842 Troisdorf

Telefon 02241 4904 0
Email vertrieb.kln@it-union.eu

Schweinfurt

VINTIN GmbH
Felix-Wankel-Straße 4
97526 Sennfeld

Telefon 09721 67594 10
Email vertrieb.sw@it-union.eu

Fulda

VINTIN GmbH
Rangstraße 39
36043 Fulda

Telefon 0661 2503859 0
Email vertrieb.fd@it-union.eu

SÜD

Stuttgart

indasys connectivity GmbH
Leitzstraße 4c
70469 Stuttgart

Telefon 0711 896659 115
Email vertrieb.st@it-union.eu

CH

Malters

VINTIN GmbH
Bahnhofstrasse 7
CH-6102 Malters

Telefon +41 41 5600067
Email vertrieb.ch@it-union.eu



Inhaltsverzeichnis

Das ist Fortinet

■ Überblick	5
■ Fortinet Security Fabric	6
■ Sicherheit: FortiGuard Labs bietet schnelleren und effektiveren Schutz	7
■ Leistung: FortiASICs steigern die Leistung deutlich	7
■ Einfachheit: FortiOS ermöglicht Konsolidierung und Vereinfachung der Sicherheit	7
■ Hochleistungs-Lösungen	8
■ Mittlere Lösungen	8
■ Einstiegslösungen	8
■ FortiGate – High Performance Next Generation Firewalling	9
■ FortiOS – Das Sicherheits-Betriebssystem der FortiGate-Serie	10

Die Module im einzelnen:

■ FortiGate Firewall	11
■ FortiGate VPN	11
■ FortiGate Intrusion Prevention Systeme (IPS)	12
■ FortiGate (D)DoS Abwehr	13
■ FortiGate Applikationskontrolle	13
■ FortiGate AntiVirus	15
■ FortiGate Web-Filter	16
■ FortiGate Secure WLAN	16
■ FortiGate Mobile Security und BYOD (Bring Your Own Device)	18
■ FortiGate Client Reputation	18
■ FortiGate Virtuelle Instanzen	19
■ FortiGate 2-Faktor-Authentifizierung mit FortiToken	20
■ FortiGate Data Loss Prevention	21
■ FortiGate WAN-Optimierung	21
■ FortiGate AntiSpam	22
■ FortiGate SSL-Inspection	22
■ FortiGate Bandbreiten-Management	22
■ FortiGate Layer 2 und Layer 3 Routing	22
■ FortiGate Netzwerkzugriffskontrolle (NAC)	23
■ FortiGate VoIP und SIP Security	23
■ FortiGate IPv6 Security	24
■ FortiGuard Services - globale und lokale Sicherheitsupdates	26

■ FortiSIEM Security Information & Event Management	27
■ FortiManager	28
■ FortiAnalyzer	29
■ FortiAP – Sichere WLAN Infrastruktur mit den Access Points FortiAP	30
■ FortiToken	32
■ FortiAuthenticator – Zentraler AAA-Server	34
■ FortiClient Endpoint Security	35
■ FortiEDR - Real-Time Endpoint Protection, Detection & Automated Response	36
■ FortiSandbox	38
■ FortiMail	40
■ FortiWeb Web Application Firewall	41
■ FortiDDoS Abwehr von DDoS-Angriffen bis auf Applikationsebene	42
■ SCADA	43
■ FortinetVM Fortinet-Lösungen auch für VM-Systeme	44

Fortinet Produktmatrix	45–47
-------------------------------	--------------

Copyright 2020 Fortinet und IT-Union GmbH & Co. KG.
Änderungen und Irrtümer vorbehalten. Alle Rechte vorbehalten. Alle Logos, Marken, Firmennamen und Produktdesigns gehören ihren jeweiligen Eigentümern.

FORTINET®

Fortinet wurde im Jahr 2000 von Ken Xie, dem Gründer und ehemaligen Präsidenten und CEO von NetScreen gegründet. Ein starkes Management-Team mit großer Erfahrung in Sachen Netzwerksicherheit führt heute das Unternehmen.

Gründungsjahr: 2000

Erste Produktveröffentlichung:
Mai 2002

Börsengang: November 2009

NASDAQ: FTNT

Unternehmenszentrale:
Sunnyvale, California

Mitarbeiter: mehr als 7.700

Umsatz 2019: 2,16 Mrd. US-Dollar

Umsatz Quartal 2/2020:
616 Mio. US-Dollar

Anzahl verkaufter Produkte:
mehr als 5,9 Millionen

Kunden:
mehr als 465.000

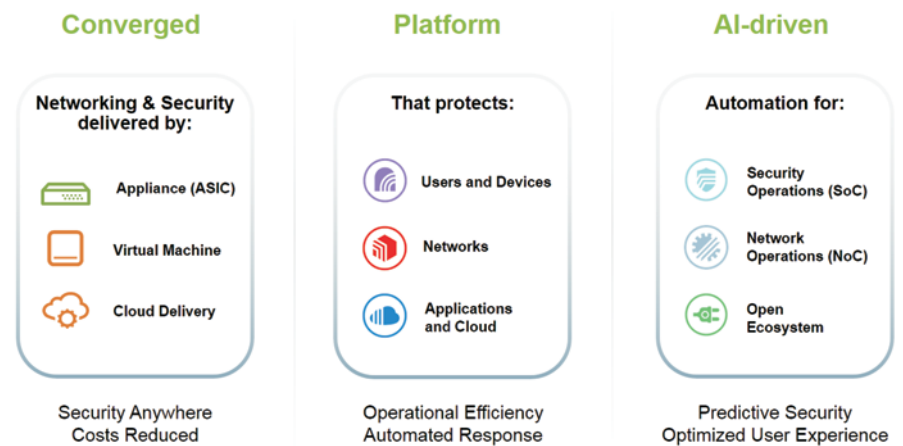
Patente:
682 erteilte Patente
195 angemeldete Patente

■ Überblick

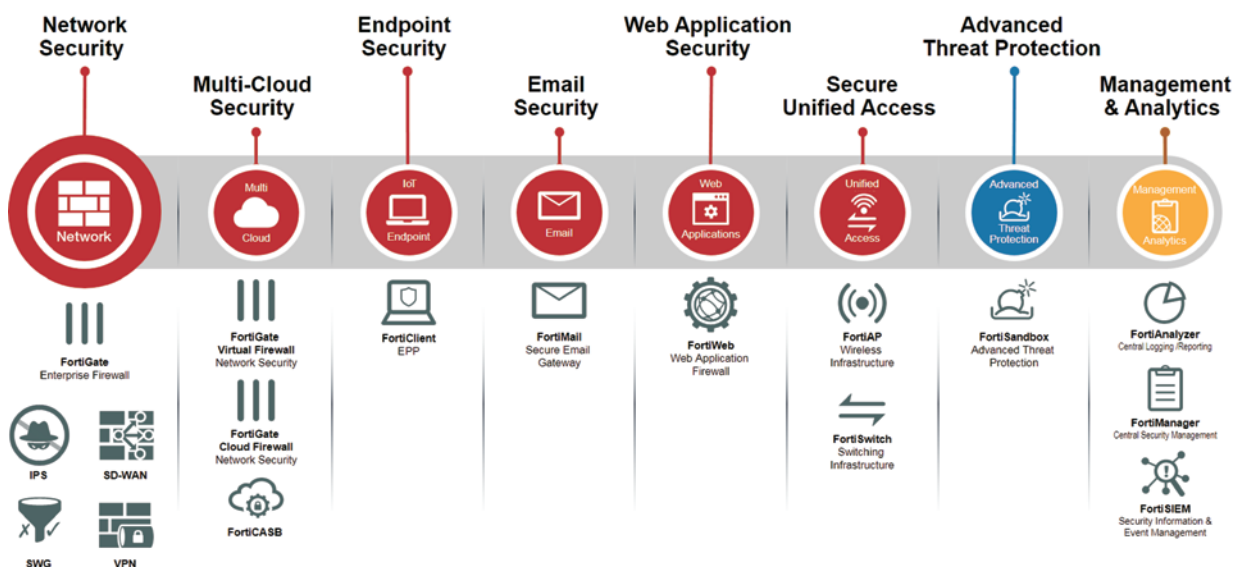
Die Mission von Fortinet ist es, innovativste und leistungsstärkste Netzwerk-Sicherheitsplattformen zu bieten und Ihre IT-Infrastruktur zu vereinfachen.

- Wir sind ein führender globaler Anbieter von Netzwerk-Sicherheitslösungen für Betreiber, Datenzentren, Unternehmen und verteilte Niederlassungen.
- Durch ständige Innovation unserer speziell angepassten ASICs, Hardwaresysteme, Netzwerksoftware, Verwaltungsmöglichkeiten und Sicherheitsforschung haben wir einen großen, schnell wachsenden und hochzufriedenen Kundenstamm und konnten Umsätze und Marktanteil ständig erhöhen.

Technologische Vision: Fortinet Security Fabric



Fortinet End-to-End Protection



■ Fortinet Security Fabric

Die weitreichende Digitalisierung sorgt fortlaufend für Umstrukturierungen in Unternehmen, während technologische Trends wie das Internet der Dinge (IoT) und Cloud Computing die Grenzen von Netzwerken verschwimmen lassen. Bei all diesen Veränderungen verlassen sich viele Anwender leider weiterhin auf Sicherheitsstrategien, die vor Jahrzehnten entwickelt wurden und die sich stetig beschleunigenden Geschäftsabläufe von heute nicht mehr ausreichend unterstützen können. Dies ist kein lokal begrenztes oder branchenspezifisches Problem, sodass die Sicherheitsbedenken und Herausforderungen weltweit doch ziemlich ähnlich sind, auch wenn sich die Infrastrukturen selbst stark voneinander unterscheiden.

Eine zeitgemäße, effektive Security-Strategie stellt sich den Herausforderungen des digitalen Markts und der entsprechenden neuen IT-Infrastrukturen von Unternehmen, indem sie klassische unabhängige Systeme in einer einzigen Architektur mit fünf kritischen und voneinander abhängigen Faktoren vereint – Skalierbarkeit, Sichtbarkeit, Sicherheit, Proaktivität und Offenheit.

■ Skalierbarkeit

Um Bedrohungen in den grenzenlosen Netzwerken von heute zu erkennen und abzufangen, muss eine Security Fabric nicht nur dynamisch skalierbar sein, um die Volumen- und Performance-Anforderungen zu erfüllen, sie muss sich auch zu den Netzwerkgrenzen hin skalieren, um einen nahtlosen, allgegenwärtigen Schutz zu gewährleisten.

■ Sichtbarkeit

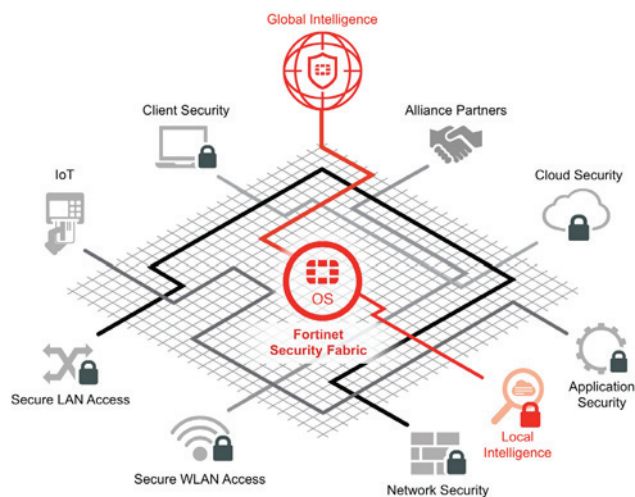
Da eine Fabric als einzelne Entität arbeitet, bietet sie umfassende Informationen über alle Geräte, Benutzer, Inhalte und Daten, die in und aus dem Netzwerk fließen, sowie Informationen über Muster im Datenverkehr. Das sorgt für geringere Komplexität und spart Kosten, während gleichzeitig die Verwaltungseffizienz gesteigert wird.

■ Offenheit

Damit Unternehmenskunden ihre bestehenden Infrastrukturen und Sicherheitsinvestitionen weiterhin nutzen können, sollte eine Security Fabric in zahlreiche Lösungen von Drittanbietern integriert werden. Fortinet arbeitet eng mit seinen weltweiten Allianzpartnern und der IT-Branche an der Entwicklung von offenen APIs in der gesamten Fabric. Damit haben Unternehmen die Flexibilität, die Lösungen gemeinsam mit bestehenden oder neuen Sicherheitstechnologien zu nutzen und so maximalen Schutz zu erhalten.

■ Proaktivität

Mit Advanced Threat Protection-Technologien werden umfassende Analysen des Datenverkehrs durchgeführt und Informationen über lokale Bedrohungen dynamisch erstellt, die an Bedrohungsforscher übertragen werden können, um automatische Updates des gesamten Systems in Echtzeit durchzuführen. Diese umfassenden Informationen in Kombinationen mit fortschrittlichen, skalierbaren und schnellen Analysen führen zu einer proaktiven Sicherheitsarchitektur mit der Möglichkeit, Bedrohungen schnell zu erkennen und zu bekämpfen.



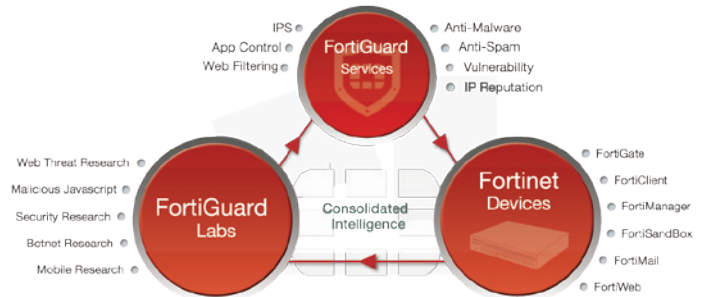
■ Sicherheit

Die universelle Transparenz einer Infrastruktur, wie gerade beschrieben, ist in der heutigen Bedrohungslandschaft grundlegend für die Sicherheit. Das Fortinet Sicherheitsbetriebssystem (FortiOS) fungiert als „Single-Pane-of-Glass“ in unserer Security Fabric.

■ Sicherheit:

FortiGuard Labs bietet schnelleren und effektiveren Schutz

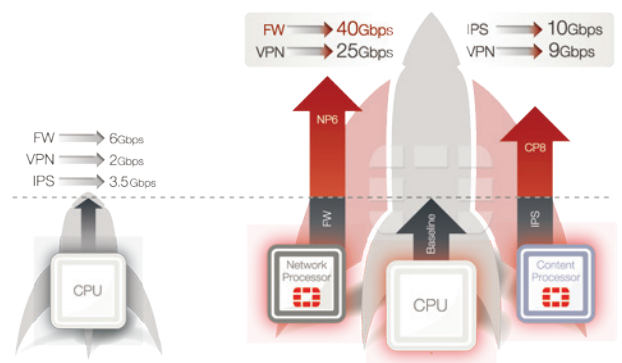
- Unser großes Forschungsteam für globale Bedrohungen erkennt neue Gefahren und entwickelt Schutzangebote für eine Vielzahl interner konsolidierter Sicherheitslösungen.
- Updates werden rund um die Uhr sofort geliefert.
- Der Schutz von FortiGuard wurde in unabhängigen Tests für hocheffektiv gegen aktuelle Bedrohungen befunden.



■ Leistung:

FortiASICs steigern die Leistung deutlich

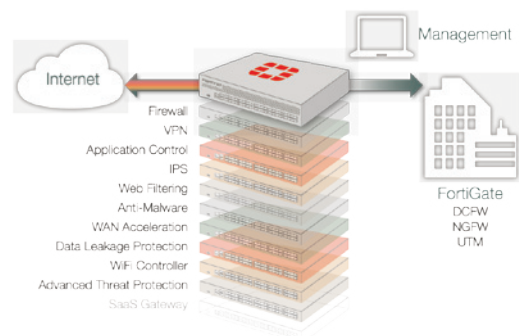
- Wichtige Netzwerk- und Contentverarbeitungsfunktionen werden von der CPU auf maßgeschneiderte FortiASICs geladen, um Leistung und Skalierbarkeit deutlich zu erhöhen.
- Unsere spezielle ASIC-Architektur bietet die beste Performance bei Netzwerksicherheitslösungen auf dem Markt, verhindert Engpässe und ermöglicht Kunden, den wachsenden Bandbreitenanforderungen nachzukommen.



■ Einfachheit:

FortiOS ermöglicht Konsolidierung und Vereinfachung der Sicherheit

- IT-Manager können einheitliche Grundsätze für alle Sicherheitslösungen schaffen und so schnellere, robustere Systeme mit weniger Verwaltungsaufwand entwickeln.
- Unsere integrierte Plattform bietet die Flexibilität, um Ressourcen dorthin zu verlagern, wo Sie sie brauchen. Sie erhalten eine einfachere und wartungsärmere Infrastruktur.



■ Hochleistungs-Lösungen

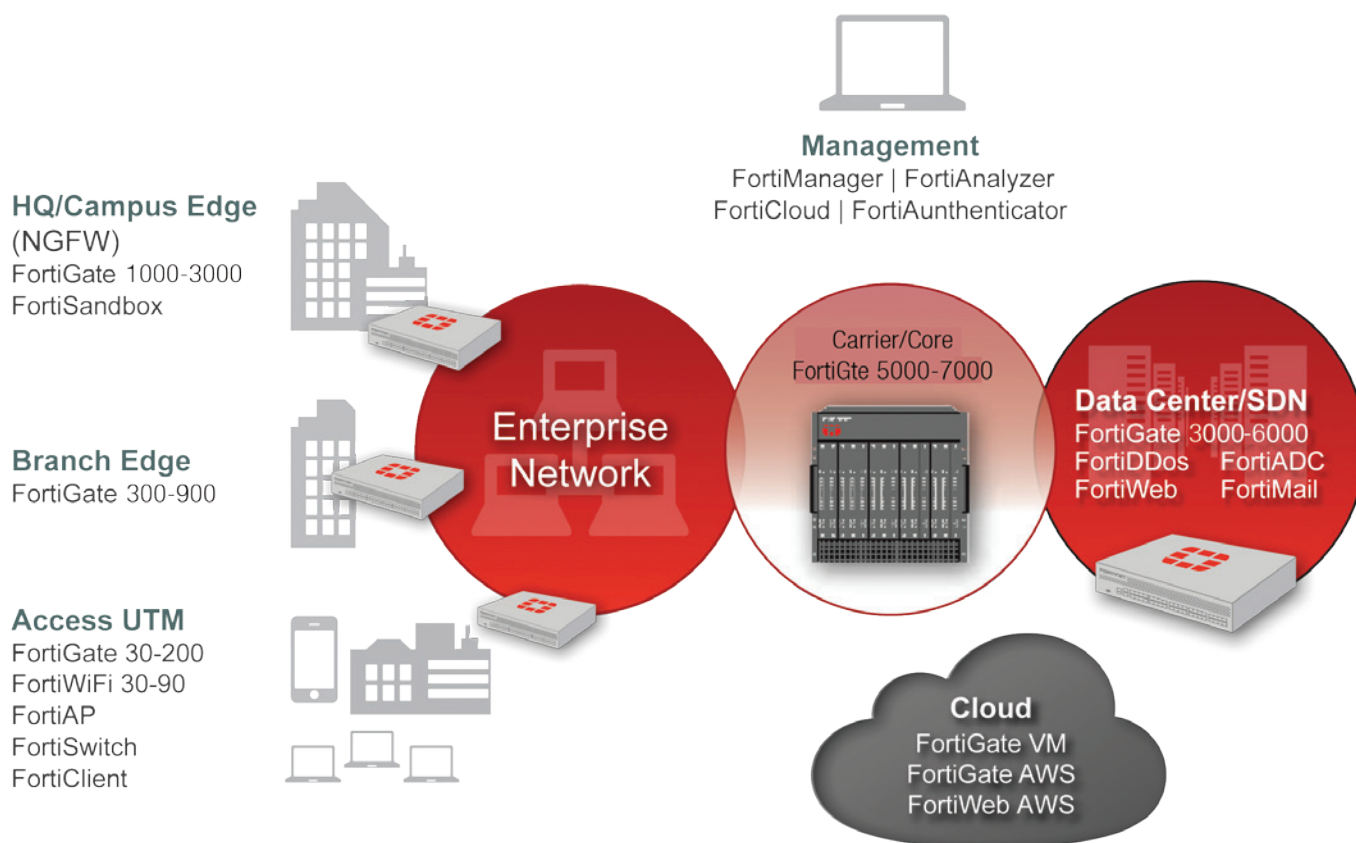
Die branchenführenden Hochleistungs-Sicherheitsplattformen von Fortinet bieten eine Next Generation Firewall (NGFW) mit außerordentlichem Datendurchlauf, äußerst niedriger Latenz und Multi-Vektor-Schutz, die sie zur idealen Lösung für anspruchsvollste Netzwerkkumgebungen in Unternehmen macht.

■ Mittlere Lösungen

Mit unserem Sortiment an bewährten Hochleistungs-Sicherheitsplattformen finden Sie die richtige Balance zwischen Leistung und Preis für Ihre Anforderungen. Fortinet bietet mehr Modelle und Sicherheitstechnologie-Optionen als jeder andere Anbieter auf dem Markt.

■ Einstiegslösungen

Sie benötigen umfassenden Unternehmensschutz für Ihre kleinsten Niederlassungen, Vertretungen, Ausrüstung am Kundenstandort und Einzelhandelsnetzwerke? FortiWiFi™ Geräte bietet den Vorteil, dass sie als „Thick Access Point“ fungieren und drahtlose Funktionen, mit denen Sie Ihren gesamten Traffic überwachen mit und ohne Kabel überwachen und steuern können. So vermeiden Sie die Kosten und potentiellen Sicherheitslücken eines separaten drahtlosen Netzwerks. Die optionale Power-Over-Ethernet (PoE)-Unterstützung der Einstiegslösungen von FortiGate beschleunigt und vereinfacht den Einsatz eines voll integrierten kabellosen Netzwerks.



■ FortiGate – High Performance Next Generation Firewalling

FortiGate Module

Fortinet bietet mit der Produktfamilie „FortiGate“ eine ganze Palette von mehrfach ausgezeichneten Appliances für den Schutz von Netzwerken und Applikationen. Die FortiGate Systeme schützen Daten zuverlässig und in Echtzeit vor Netzwerk- und Content-basierenden Bedrohungen.

Hier spielen die von Fortinet entwickelten ASIC Prozessoren eine entscheidende Rolle, die die vielfältigen Dienste und Sicherheitsfunktionen der FortiGate Appliances enorm beschleunigen. Somit lassen sich Bedro-

hungen durch Viren, Würmer, Exploits, Spyware oder neuartige Blended Threats und Advanced Persistent Threats, also Kombinationen aus den genannten Angriffsmustern, effektiv bekämpfen – und das in Echtzeit!

Weitere Funktionen wie umfangreiche und komfortable Applikationskontrolle, URL-Filter, IPSec- und SSL-VPN, Bandbreitenmanagement, WLAN-Controller, integrierte 2-Faktor-Authentifizierung und selbstverständlich eine marktführende und hochperformante Firewall sind fest integrierter Bestandteil aller FortiGate Appliances.

High-End NGFW

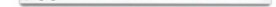
- Firewall-Appliances mit bis zu 300+ Gbit/s und Gehäuse-Durchsatz von mehr als 1 Tbit/s.
- Integrierte High Speed 40/100 GbE Anschlüsse sowie eine hohe 10 GbE Anschlussdichte
- Konsolidierte Sicherheitsfunktionen mit Empfehlung von NSS Labs bieten erstklassigen Schutz
- Hochverfügbarkeit und Virtual-Domain-Support für mandantenfähige Umgebungen
- Intuitive Verwaltungsschnittstelle bietet umfassende und detaillierte Transparenz und Kontrolle



FG 7000 Serie



FG 6000 Serie



FG 2000 Serie

Mid-Range NGFW

- Bis zu 52 Gbit/s – bestes Preis-Leistungs-Verhältnis für Firewalls seiner Klasse
- 5-mal schneller als jede andere NGFW-Plattform in der Branche
- Integrierte 10 GbE-Ports zum Schutz interner Hochgeschwindigkeitssegmentierungen
- Von NSS Labs „empfohlene“ NGFW und NGIPS – bietet hervorragenden Schutz
- Zentralisierte Verwaltungskonsolle für unvergleichliche Transparenz und Kontrolle



FG 900 Serie



FG 500 Serie

Entry-Level NGFW

- Bis zu 4 Gbit/s Firewall-Durchsatz - ideal für kleine und mittelständische Unternehmen oder Außenstellen
- Erstklassiger, von NSS Labs, Virus Bulletin und AV-Comparatives geprüfter Schutz
- Zuverlässige Security Appliances in kompakter lüfterlosen Bauform
- Integrierter WLAN-Controller für einen leistungsstarken Zugang sowie kabelgebundene und drahtlose Sicherheit mit zentralisiertem Management



FG 90 Serie



FG 60 Serie

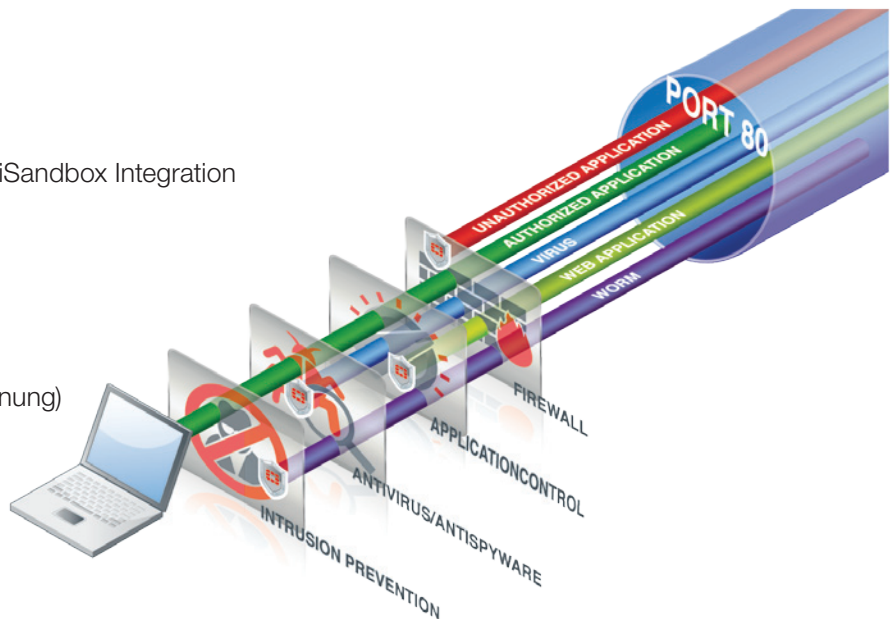


FortiOS – Das Sicherheits-Betriebssystem der FortiGate Serie

Das Betriebssystem aller FortiGate Systeme, FortiOS, bietet eine Vielzahl von Modulen, mit denen Unternehmen ihre Infrastruktur komfortabel und flexibel absichern können. FortiOS ist modular angelegt und kann mit späteren Updates im Rahmen eines bestehenden Service-Vertrages einfach um neue Funktionen erweitert werden – ohne zusätzliche Kosten!

FortiOS – und damit jede FortiGate Appliance – beinhaltet folgende Funktionen:

- Firewall
- VPN
- AV
- IPS
- Advanced Threat Protection mit FortiSandbox Integration
- Applikationskontrolle
- URL-Filter
- Integrierter WLAN-Controller
- Integrierter Switch-Controller
- Mobile Security & BYOD (Client Reputation, Device/OS-Erkennung)
- WAN-Optimierung, Web-Cache & Explicit Proxy
- Authentifizierung via integriertem Token-Server
- Bandbreitenkontrolle
- IPv6-Support
- Data Loss Prevention
- SSL Inspection
- Smart Policies und Identity Based Policies
- Routing
- VLANs
- Virtuelle Instanzen (VDOMs)
- Endpoint Control – Integration FortiClient
- Skalierbares Security Management (optional via FortiManager)
- Umfangreiches Reporting und Troubleshooting (erweiterbar durch FortiCloud und FortiAnalyzer)
- FortiView – Monitoring und Troubleshooting “out of the box”





Die Module im einzelnen:

■ FortiGate Firewall

Die branchenführenden FortiGate Security-Systeme bieten unerreichte integrierte Security-Ressourcen, Benutzerfreundlichkeit und ein optimales Preis-Leistungsverhältnis. Zusammen mit der Stateful-Inspection-Firewall verwendet das FortiGate System eine Vielzahl an integrierten Sicherheitsmechanismen, um vor aktuellen und komplexen Angriffen, wie Stuxnet und Duqu effektiv zu schützen.

Das Herzstück aller FortiGate Modelle ist die schnellste Firewall der Welt (Quelle: Breaking Point). Firewall-Regelwerke kontrollieren sämtliche Daten, die eine FortiGate Appliance zu passieren versuchen – zwischen FortiGate Interfaces, Zonen oder VLAN-Sub-interfaces. Solche Regelwerke enthalten Anweisungen, ob und wie einzelne Verbindungen akzeptiert oder Pakete weitergeleitet werden.

Bei Eintreffen einer Verbindungsanfrage werden z. B. Quell- und Zieladresse und der Dienst (Port Nummer) analysiert, um die anwendbaren Firewall-Regeln zu identifizieren. Dabei können u. U. viele verschiedene Instruktionen zur Anwendung kommen – neben obligatorischen Anweisungen wie dem Akzeptieren oder Verwerfen von Datenpaketen können optionale Instruktionen wie Loggen, Zuweisung von Bandbreite oder Authentifizierung greifen. Sämtliche anderen Sicherheitsmodule (z. B. AntiVirus, IPS, Applikationskontrolle, URL-Filter usw.) werden abhängig von diesem zentralen Firewall-Regelwerk gesteuert.

■ FortiGate VPN

Virtual Private Networks (VPN) ermöglichen die sichere, verschlüsselte Verbindung zu privaten Unternehmensnetzwerken und -ressourcen. So kann z.B. ein Anwender von seinem Home Office oder von unterwegs per VPN mittels einer verschlüsselten Verbindung auf das zentrale Netzwerk zugreifen. VPN-Verbindungen können nicht von unauthorisierten Dritten ausgelesen oder

manipuliert werden und ein Zugriff auf sensible Informationen wird so verhindert.

Fortinet bietet VPN-Optionen, sowohl mittels seiner FortiGate Appliances, als auch über die in die FortiClient integrierte Funktionalität. Mittels zweier FortiGates (oder auch standard-konformen Drittanbietern) können auf diese Weise auch viele verschiedene Standorte sicher über ein VPN miteinander verbunden werden.

Hub and Spoke 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 Bandbreiten-Management-Funktionen ermöglichen, dass VoIP-Traffic auch bei einer VPN-Verbindung priorisiert wird.

SSL oder IPsec?

In den vergangenen Jahren haben sich zwei Standards für verschlüsselte Verbindungen etabliert: IPsec VPNs und SSL VPNs. Während IPsec VPNs primär in sog. site-2-site-Verbindungen und zentral gemanagten mobilen Endgeräten zum Einsatz kommen, haben sich SSL-VPNs vorwiegend in sog. clientless (z.B. Internet-Cafe) Umgebungen etabliert.

IPsec VPN bietet sich an für klassische Layer3-basierende Anwendungen, bei denen eine verschlüsselte Verbindung zwischen zwei Geräten aufgebaut wird. SSL VPN bietet Vorzüge im Bereich der Web-Anwendungen, bei denen zwischen Web-Server und Web-Browser eine sichere (SSL-verschlüsselte) Verbindung etabliert wird.

Fortinet unterstützt in höchst komfortabler Weise beide Standards und eine Vielzahl von Optionen zur individu-

ellen Konfiguration und Administration. Auf FortiGate Systemen können IPsec und SSL-VPN-Verbindungen auch gleichzeitig zum Einsatz kommen.

VPN-Services für MSSPs

Mit Fortinet können MSSPs einen hochsicheren VPN-Dienst bereitstellen, indem sie die integrierte VPN-Engine mit den übrigen UTM-Modulen verknüpfen. So kann ein- und ausgehender Traffic in Echtzeit auf Malware untersucht und erst dann freigegeben werden,

um die Verbreitung von Schadsoftware innerhalb eines Unternehmens-VPN zu verhindern.

Ein weiteres Plus ist, dass Fortinets flexible VPN-Architektur die Interoperabilität mit allen standardbasierten IPSec VPN-Gateways zulässt. Unabhängig vom VPN Device, das der Kunde verwendet, gewährleistet das zentral implementierte FortiGate System Malware-freien VPN Traffic.

■ FortiGate Intrusion Prevention Systeme (IPS)

Intrusion Prevention Systeme bieten Schutz gegen bekannte und zukünftige Bedrohungen auf Netzwerkebene. Zusätzlich zur Signatur-basierten Erkennung wird eine Anomalie-basierte Erkennung durchgeführt. Das System generiert einen Alarm, wenn Daten einem speziellen Profil eines Angriffsverhaltens entsprechen. Dieses Verhalten wird dann analysiert, um die Evolution von Bedrohungen zu erkennen und neue Signaturen entwickeln zu können, die dann wiederum Bestandteil der FortiGuard-Services werden.

Implementierung von IPS

Das in die FortiGate Appliances integrierte Hochleistungs-IPS-Modul kann entweder als Standalone-Device oder als Bestandteil einer Multifunktions-Firewall (UTM) sowie an Netzwerk-Perimeter (Übergang zwischen internem und externem Netzwerk) als auch im internen Netz agieren. So können sowohl protokoll- oder anwendungsbasierende Angriffe von außen als auch die Ausbreitung von derartigen Schädlingen im internen Netzwerk (die z. B. über mobile Endgeräte oder Datenträger ins Unternehmen gelangt sind) erkannt und verhindert werden.

IPS für die Zentrale und Niederlassungen

Fortinets flexible Architektur und skalierbare Produktreihe berücksichtigt Implementierungen im zentralen Netzwerkbereich zum Schutz vor externen und internen Angriffen ebenso wie die Absicherung von Niederlassungen jeder Größenordnung. Dies wird durch die identische IPS-Funktionalität auf allen FortiGate Appliances erreicht. In Verbindung mit FortiManager und FortiAnalyzer können so größte und hochkomplexe VPN-Infrastrukturen flexibel, einfach, kostengünstig und auch mandantenfähig realisiert werden.

One-Armed IDS (Sniffer)

Als Ergänzung ist es möglich, sog. Sniffer-Policies zu erstellen, mit denen eine FortiGate als „one-armed“ Intrusion Detection System fungiert, also nicht in den Datenstrom eingreift, sondern diesen nur mitliest. Dabei wird der Datenverkehr auf Übereinstimmungen mit bereits konfigurierten IPS-Sensoren und Applikationslisten untersucht. Bei einem Treffer wird dieser gelogged und die eingehenden Daten abgewiesen. Auf diese Weise ist es möglich, den Datenverkehr zu untersuchen ohne die einzelnen Datenpakete zu verarbeiten.



■ Fortigate (D)DoS-Abwehr

Typische Firewall-Systeme sind in der Lage, DoS- und DDoS-Angriffe zu erkennen, und sofern diese nur eine geringe Bandbreite belegen, auch abzuwehren. Dabei wird jedoch die CPU des Firewall-Systems stark belastet, da jedes angreifende Paket mithilfe einer Firewall-Regel bearbeitet werden muss. Fortinet bietet in seinen FortiGate Systemen ein mehrstufiges Abwehrmodell, welches die vorhandenen Ressourcen der Appliance deutlich entlastet.

DoS-Sensor

Mithilfe eines sogenannten DoS-Sensors können DoS-Angriffe bereits erkannt werden, bevor klassische Firewall-Regeln greifen. Der DoS-Sensor, der viele verschiedene Typen von Netzwerk-Anomalien erkennen kann, unterscheidet zwischen angreifenden und erlaubten Daten. Erlaubte Daten werden an das Regelwerk der Firewall übergeben, Pakete die als DoS-Angriff gewertet werden, werden entsprechend der im DoS-Sensor hinterlegten Konfiguration behandelt. Nachgeschaltete Intelligenz in einem FortiGate System, wie etwa die IPS Engine, bietet darüber hinaus weitere Möglichkeiten zur Erkennung von DoS- und DDoS-Angriffen auf höheren Netzwerkschichten.

■ FortiGate Applikationskontrolle

Die Vielfalt von Applikationen nimmt kontinuierlich und zum Teil sogar drastisch zu – verstärkt durch den Trend, dass Enterprise-Applikationen zunehmend in Richtung Web-Plattformen migrieren und Web 2.0 mit einer Vielzahl von einfachen und vielfach privat genutzten Anwendungen (Webmail, Instant Messaging, Social Media wie Twitter und Facebook usw.) den Administratoren das Leben erschwert.

Daraus ergeben sich neue Herausforderungen für die IT-Sicherheit, da vielen dieser Anwendungen neue Sicherheitslücken innewohnen, die herkömmliche Abwehrmaßnahmen umgehen können. Desweiteren stehen IT-Verantwortliche vor dem Problem, die Produktivität der Mitarbeiter trotz derartiger oft zeitintensiver Applikationen (Chat, Games usw.) zu erhalten und die Zuverlässigkeit der Infrastruktur zu bewahren, obwohl

Hardware basierte DoS-Abwehr

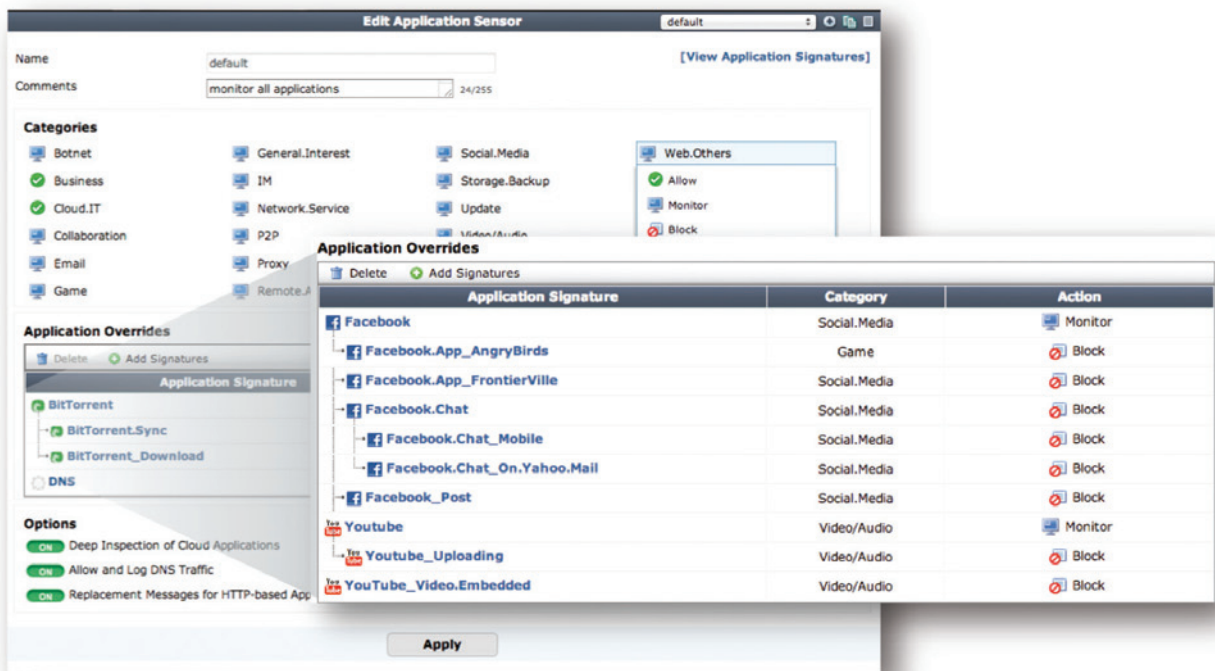
Mithilfe der Fortinet ASICs SP2 oder SP3, die in einigen größeren FortiGate Appliances sowie Erweiterungsmodulen integriert sind, kann mittels der dort vorhandenen Proxyfunktionalität eine TCP SYN Flood Attacke erkannt und abgewehrt werden, ohne die restliche Appliance-Architektur nennenswert zu belasten. Durch die im SP3 integrierten Load Balancer-Funktionen ist es sogar möglich, hochperformante DDoS-Abwehr parallel zur ebenso leistungsfähigen IPS-Funktionalität zu betreiben, indem die Daten entsprechend auf weitere interne Module bzw. Prozessoren (ASICs) verteilt werden.

In modularen FortiGate Appliances können zu diesem Zweck sog. Security Processing-Module nachgerüstet werden, die mit den neuen SP2/SP3-Chips ausgestattet sind. So kann (bei Bedarf auch erst im Nachhinein) die IPS-Performance einer Appliance signifikant gesteigert werden.

diese Anwendungen oft eine sehr hohe Bandbreite benötigen (Video/Audio-Downloads oder -Streaming). Zunehmend spielt auch die Einhaltung von Compliance-Regularien eine Rolle, die weitere Anforderungen an IT-Abteilungen stellt.

Arbeitsweise

Applikationskontrolle stellt ein Werkzeug zur Verfügung, das Administratoren in die Lage versetzt, gezielt auf einzelne Applikationen einzuwirken – auch dann, wenn diese Non-Standard Ports verwenden oder erlaubte Protokolle als Tunnel nutzen. Als Teil einer Multi-Layer-Security-Architektur ermöglicht Applikationskontrolle eine granulare Steuerung des Anwendungsverhalten und beeinflusst so im positiven Sinne die Bandbreite, Performance, Stabilität und Zuverlässigkeit sowie die Compliance der IT-Infrastruktur.



Vorteile gegenüber herkömmlichen Methoden

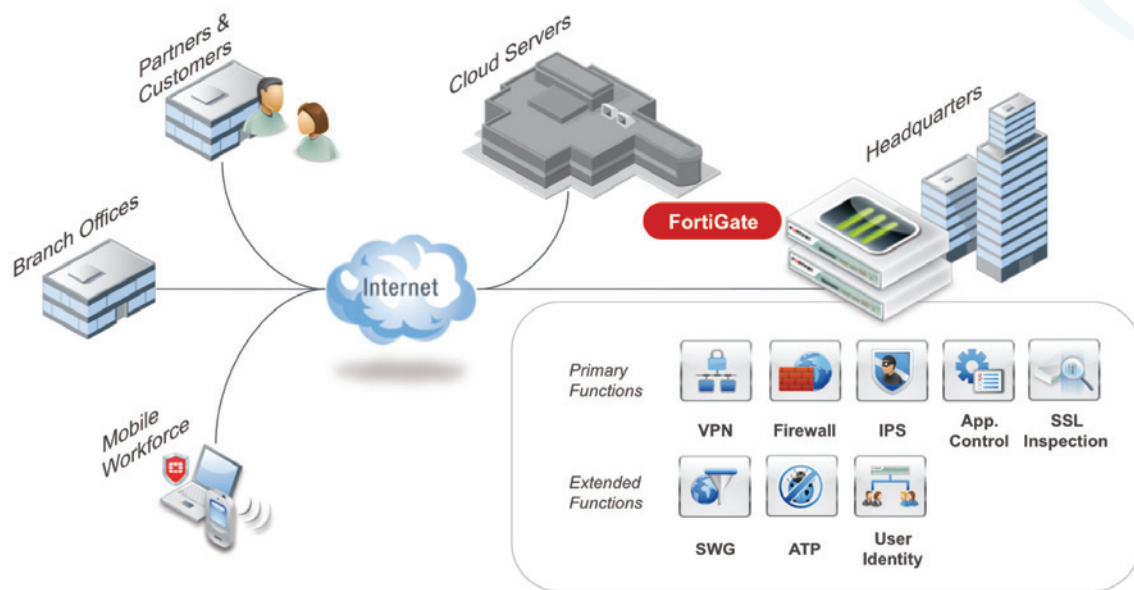
Eine herkömmliche Firewall kontrolliert den Datenstrom basierend auf Port- bzw. Service-Kontrollmechanismen. Applikations-Kontrolle setzt auf dynamische Untersuchung der Daten und ermöglicht überdies die Anwendung weiterer Kontrollen, wie etwa Bandbreitenvergabe pro Applikation oder Zeitfenster bzw. -konten für deren Nutzung. Weiterhin kann sogar innerhalb von Applikationen ein Teil der Funktionalität eingeschränkt werden, z. B. die Nutzung von Facebook bei gleichzeitigem Unterbinden von Facebook Chat, oder das Nutzen von Google.Docs, oder 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. Die maximale Nutzbarkeit von Applikationen wird so bei minimalem Risiko erzielt. Derartige Regeln zur Nutzung können bis auf Anwenderebene und selbstverständlich auch geräte- oder abteilungsbezogen erstellt werden.

Integration als Mehrwert

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.



■ FortiGate AntiVirus

Das Antivirus-Modul vereint eine Reihe von Features, die verhindern, dass ungewollte oder potenziell gefährliche Dateien in das Netzwerk gelangen. Diese Features arbeiten auf unterschiedliche Weise, wie etwa das Prüfen der Dateigröße, des Namens, des Dateityps, oder des Vorhandenseins eines Virus oder einer Grayware Signatur. Dabei haben alle Antivirus-Mechanismen gleichzeitig Zugriff auf den Datenverkehr, wodurch sichergestellt ist, dass viele Operationen nahezu gleichzeitig erfolgen können. Dies erhöht die Performance der Antivirus-Engine erheblich.

Proxy-, Flow- oder Cloud-basierter AntiVirus

Zusätzlich zu drei Proxy-basierenden Antivirus-Datenbanken beinhaltet FortiOS außerdem eine hoch performante flow-basierende Antivirus-Option. Diese ermöglicht es, Dateien jeder Größe zu scannen, ohne die Performance merklich zu beeinträchtigen. Überdies ist es möglich, komprimierte Dateien zu analysieren um auch versteckte Threats zu erkennen. Durch die Flexibilität, zwischen den Antivirus-Engines wählen zu können, ist es möglich, die ideale Ausgewogenheit zwischen Performance und Security individuell an die Umgebung anzupassen.

Ab FortiOS 5 steht darüber hinaus eine Cloud-basierte AV-Engine zur Verfügung. Diese ergänzt die zuvor ge-

nannten Engines und bietet zusätzliches Sandboxing. So können – ohne die Performance der FortiGate zu beeinträchtigen – Dateien in der Cloud analysiert und ihre Gefährlichkeit in einer sog. Sandbox geprüft werden.

High Performance AntiVirus

Fortinets optimierte Anti-Virus-Technologie verwendet eine Kombination aus Signatur- und heuristischen Detektionsmodulen und bietet so vielschichtigen Echtzeitschutz gegen zahlreiche Angriffsformen. 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.

AntiVirus Techniken

Abhängig vom erforderlichen Schutzniveau können unterschiedliche Instanzen aktiviert werden, die eingehende Daten auf Malware untersuchen. Dabei wird unterschieden zwischen Pattern Scan, Grayware Scan und einer heuristischen Analyse. Während die ersten beiden Verfahren auf bekannte Virus-Definitionen untersuchen, ist es möglich, mit Letzterer auch Mutationen bekannter Viren oder gänzlich neue Viren-Signaturen zu erkennen.

Echtzeit Updates

Die Effizienz einer Antivirus-Lösung wird nicht nur an ihrem Durchsatz oder an der Erkennungsrate, sondern auch an der Geschwindigkeit, in der Signatur-Updates eintreffen, gemessen. Über das FortiGuard Distribution Network (FDN) werden diese Informationen kontinuierlich aktualisiert und in Echtzeit bereitgestellt. Dieser Vorgang erfolgt automatisch und erfordert keinen Eingriff des Administrators. Im Vergleich rangiert die Fortinet AV-Engine kontinuierlich unter den Top5 AntiVirus-Anbietern.

Advanced Threat Protection – Integration in FortiSandbox

Moderne, hochgradig komplexe und „hartnäckige“ Malware ist nicht selten so programmiert, dass sie Wege

zu finden versucht, vorhandene Abwehrmechanismen wie Firewall, AV, IPS usw. zu umgehen. An dieser Stelle greifen weitere Erkennungsmethoden und die Integration einer FortiGate mit Fortinets Sandbox-Technologie. Verdächtig wirkende Daten werden – bevor sie ins Unternehmensnetz gelangen können, an eine FortiSandbox weitergeleitet. Dort werden sie in einer isolierten Umgebung zur Ausführung gebracht und auf ihre Wirkung untersucht.

Sollte dabei ein schadhaftes Verhalten erkannt werden, werden die Daten blockiert und das Ergebnis der Analyse an die Fortinet Labs gesendet, die daraufhin neue Signaturen entwickeln und bereitstellen. Weitere Informationen zu Fortinets Sandbox-Lösungen finden Sie im gleichnamigen Kapitel in dieser Broschüre.

■ FortiGate Web-Filter

Unerlaubtes Internet-Surfen und die Verwendung von webbasierenden Anwendungen resultieren häufig in Produktivitätsverlust, hoher Netzwerklast, Infizierung mit Malware und Datenverlusten. Web Filtering kontrolliert den Zugriff auf webbasierte Anwendungen wie Instant Messaging, Peer-to-Peer File Sharing und Streaming-Applikationen. Gleichzeitig werden Phishing Sites und Blended Threats blockiert. Überdies können Botnet Befehle und Fast Flux File Downloads blockiert werden. Flowbasierende Web Filtering Optionen sind ebenfalls verfügbar.

Arbeitsweise

Das Fortinet WebFilter-Modul besteht aus drei interagierenden Komponenten: dem URL-Filter, dem Web Content Filter und dem FortiGuard Webfilter Service. Der URL-Filter verwendet URLs und URL Patterns, um Webseiten zu blockieren. Der Web Content Filter blockiert Webseiten, die bestimmte Wörter oder Patterns

enthalten, die individuell spezifiziert werden können. Fortinets FortiGuard Web Filtering Service reguliert und bietet wertvolle Einsicht in alle Internetaktivitäten und ermöglicht es dem Kunden so, neue gesetzliche oder interne Bestimmungen und Vorschriften einzuhalten.

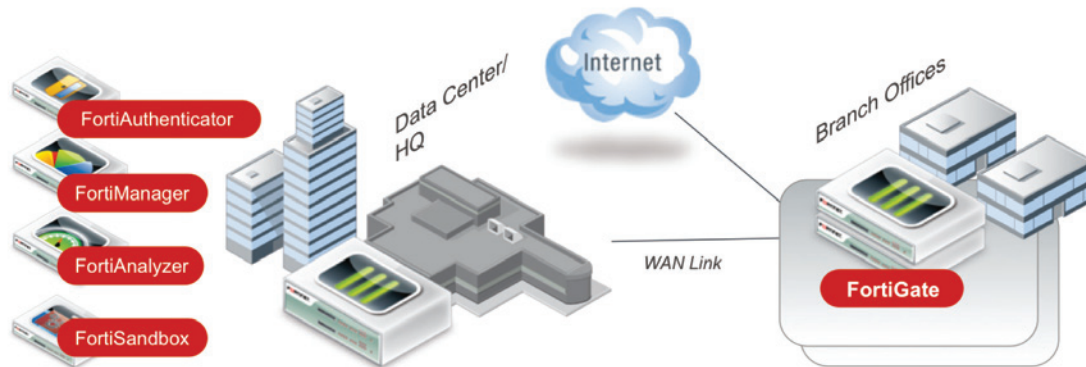
Jugendschutz

Fortinet ist ein Mitglied der Internet Watch Foundation in Großbritannien, eine Organisation, die potenziell illegalen Online-Content bekämpft und den Zugang zu kinderpornografischen Websites verhindert. Fortinets Web Filtering Lösungen sind darüber hinaus CIPA-zertifiziert. Das Children's Internet Protection Act (CIPA) ist ein US-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.

■ FortiGate Secure WLAN

FortiGate Security-Systeme bieten eine umfassende Reihe an Funktionen, mit denen die höchsten Anforderungen bei der Implementierung von Wireless LANs erfüllt werden. FortiGate Systeme können in Verbindung

mit Wireless Access Points (FortiAP) implementiert und dazu verwendet werden, Content-basierte Bedrohungen aus E-Mail- und Internet-Traffic, wie Viren, Würmer, Intrusionen, unangemessenen Internet Content, in



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 Bandbreitenmanagement, 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.

Die umfangreiche Serie von Fortinet-eigenen Thin Access Points (FortiAP) in Verbindung mit einer Vielzahl von Wireless Controllern (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 FG30B) wird das Sicherheitsniveau des kabelgebundenen LANs automatisch auf die WLAN Umgebung übertragen.

Der gesamte WLAN-Traffic wird so Identitäts-basiert 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 prüfen.

Return on Investment

Da jede FortiGate Appliance (ab FG40C) ab FortiOS 4.3. 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.

Access Points für alle Anwendungen

FortiAPs stehen für alle denkbaren Anwendungen zur Verfügung. Indoor, Outdoor, Remote Access Points sowie umfangreiches Zubehör wie z.B. verschiedene Antennen finden sich im entsprechenden Kapitel dieser Broschüre.

■ FortiGate Mobile Security und BYOD (Bring Your Own Device)

Die drastische Zunahme von mobilen Endgeräten, die z. T. auch Privateigentum der Nutzer sind, stellt Unternehmen vor eine neue Dimension an Herausforderungen: Kontrolle über Geräte, auf die aufgrund der Gesetzeslage kein, oder nur ein stark beschränkter und vor allem reglementierter Zugriff möglich ist. Aber auch, wenn die Endgeräte Unternehmenseigentum sind, ist eine sichere Kontrolle oft nur bedingt möglich (z. B. bietet das iOS der Apple-Welt kaum Möglichkeiten, Security-Software zu installieren). Hier müssen zentrale Mechanismen die dezentrale Sicherheit schaffen.

■ FortiGate Client Reputation

Nicht nur in BYOD-Umgebungen, sondern in jedem Unternehmen ist es wichtig, frühzeitig zu erkennen, welche User bewusst oder unbewusst die IT-Sicherheit gefährden. Dies kann durch Nutzung unerlaubter Software, Surfen auf gefährlichen Webseiten oder Download von infizierten Dateien (Bilder, PDFs, Audio, Video) erfolgen – aber auch durch die unbemerkte Infektion durch Zombie-Code, der das Endgerät zum Teil eines Botnets macht.

Die neue FortiOS Client Reputation Funktionalität erlaubt es, Usern individuelle Nutzungsprofile zuzuweisen, diese regelmäßig auf Abweichungen zu scannen und so eine Nutzer-ScoreCard anzulegen. Diese dient

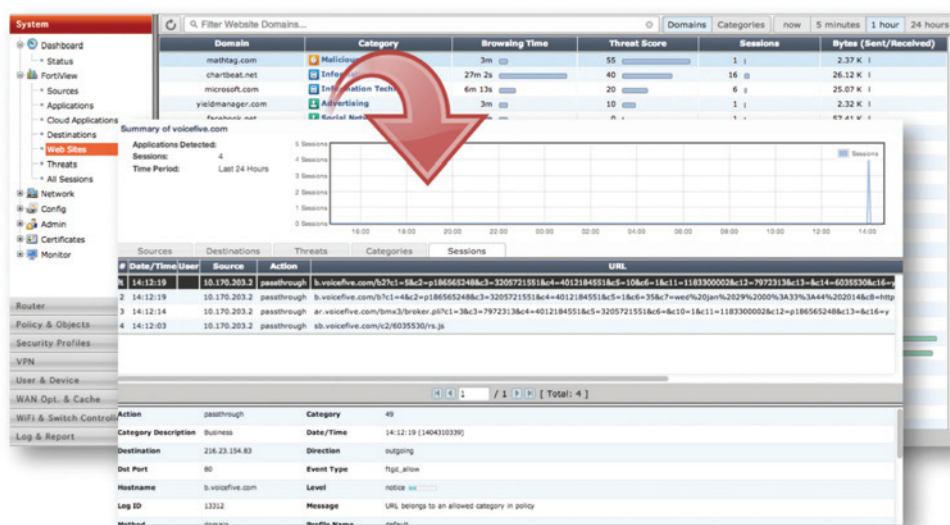
Device- und OS-Erkennung

Ab FortiOS 5 stellen alle FortiGate Appliances umfangreiche Funktionen für diesen Zweck bereit. So können anhand spezieller Parameter die Endgeräte (Typ & Hersteller) sowie die installierten Betriebssysteme (Typ & Release) erkannt werden. In Verbindung mit geographischer Ortsbestimmung, User-Erkennung und -Authentifizierung und ggf. weiterer Eckdaten (Zeit, Datenmenge, Ressourcen etc.) sind so individuelle Regelwerke möglich, die in Abhängigkeit dieser Rahmenparameter herangezogen werden können.

wiederum als Basis für Regelwerke, die in Abhängigkeit des User-Scores adaptiert werden können bzw. Alarme auslösen.

FortiGate Monitoring und Troubleshooting mit FortiView

Mit FortiView, einem ab FortiOS 5.2. verfügbaren integrierten Tool zum Monitoring und Troubleshooting, ist es nunmehr möglich, schnell und einfach die Events einer FortiGate zu visualisieren und die Fehlersuche deutlich zu vereinfachen. Detaillierte Logs bieten tiefen Einblick in Sessions einer FortiGate, umfangreiche Reports optimieren und erleichtern die vorausschauende Netzwerkplanung.



■ FortiGate Virtuelle Instanzen

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, aufwändiger Wartung und Bedienung, komplizierter Verwaltung von Service-Verträgen, Stromverbrauch und mangelhafter Flexibilität entstehen würden. Darüber hinaus benötigen immer mehr Unternehmen heterogene Security-Dienste für einzelne Teile ihrer Infrastruktur, also unterschiedliche Funktionen für verschiedene Abteilungen.

Virtuelle Domänen (VDOMs)

Mit der standardisierten und integrierten Virtualisierungsfunktion – sogenannten virtuellen Domänen (VDOMs) – können sämtliche Funktionen einer FortiGate Appliance 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 FortiGate Modellen sind 10 VDOMs möglich und ab Werk ohne zusätzliche Kosten vorhanden. Ab der 1000er Serie sind mit zusätzlichen Lizenzen weitere VDOMs pro FortiGate möglich. Neben vielen äußerst

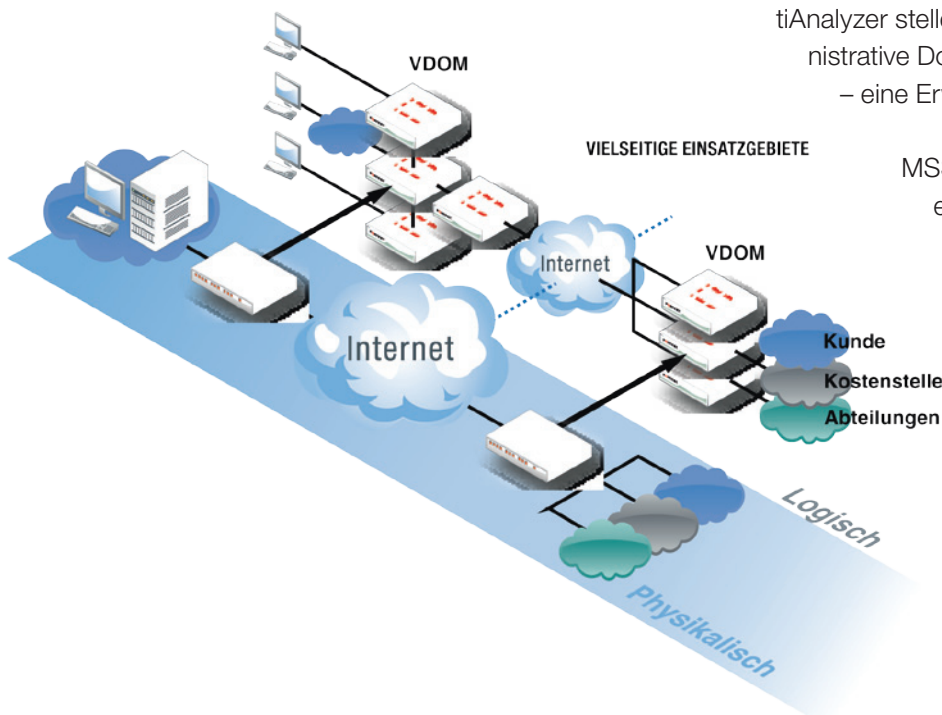
flexiblen Konfigurations-Optionen reduziert der Einsatz von VDOMs auch den Platz- und Strombedarf. So können z.B. mit einer einzigen FG600C bis zu 10 kleinere FortiGates (z.B. FG40C oder FG60D) ersetzt werden – ein deutlicher Platzvorteil und bis zu 18.000 kWh Stromersparnis pro Jahr.

Höchste Flexibilität

VDOMS ermöglichen nicht nur individuelle Security-Service-Konfigurationen innerhalb von Unternehmen oder für MSSPs. Sie bieten weitere Vorteile, wie z.B. die optimierte Lastverteilung innerhalb eines Clusters, in dem auf einem Cluster-Member z. B. die Firewall im Primary- und die AV-Engine im StandBy-Modus ausgeführt wird – und im anderen Cluster-Member entsprechend umgekehrt. So wird die Performance beider Appliances optimal genutzt und trotzdem eine Hochverfügbarkeit gewährleistet. Ebenso kann auf diese Weise ein Cluster entsprechend skaliert werden, ohne dass Geräte ausgetauscht werden müssten.

Mandantenfähige Security Services

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, sog. Administrative Domains (ADOMs), standardmäßig bereit – eine Erweiterung ist hier nicht erforderlich.



MSSPs können auf diese Weise sehr einfach und kostengünstig maßgeschneiderte Security Services anbieten.

Dabei kann jede einzelne VDOM individuell und völlig unabhängig mit dem vollen Funktionsumfang einer FortiGate konfiguriert werden. Änderungen sind ebenso einfach und schnell – und vor allem ohne Unterbrechung der Services möglich. Ebenso kann eine Inter-VDOM-Kommunikation etabliert werden, wenn dies aus Kundensicht oder für administrative Zwecke erforderlich sein sollte.

■ FortiGate 2-Faktor-Authentifizierung mit FortiToken

Bei der Authentifizierung handelt es sich um die Bestätigung der Identität von Personen oder Instanzen. Im Zusammenhang mit Unternehmensnetzwerken müssen die Identitäten von Nutzern oder Computern definiert und kontrolliert werden, um sicherzustellen, dass nur autorisierte Instanzen Zugriff auf das Netzwerk bekommen.

Fortinet Systeme unterstützen Netzwerk Zugangskontrolle (NAC) und können so Firewall-Regeln und VPN-Dienste einzelnen Usern dediziert zuweisen. Eine FortiGate Appliance unterstützt drei unterschiedliche Authentifizierung-Methoden: Passwort-Authentifizierung für Personen, Zertifikat-basierende Authentifizierung für Host-Computer oder Endpoints, sowie 2-Faktor-Authentifizierung für zusätzliche Sicherheit über normale Passwörter hinaus.

Lokale Passwortauthentifizierung

Die einfachste Möglichkeit der Authentifizierung basiert auf User-Accounts, die bereits lokal auf einer FortiGate Appliance gespeichert sind. Über die Möglichkeit, einen User-Account vorübergehend abzuschalten, ist es möglich, den Netzwerkzugang zu unterbinden, ohne den Account zu löschen. Lokale User-Accounts sind eine gute Methode für kleinere FortiGate Installationen. Sobald mehrere FortiGate Appliances zum Einsatz kommen, die mit denselben Accounts arbeiten, ist die Verwendung externer Authentifizierungsserver empfehlenswert, um die Account-Verwaltung und -Konfiguration zu vereinfachen.

Server-basierter Passwortauthentifizierung

Die Nutzung von externen LDAP, RADIUS oder TACACS+ Authentifizierungs-Servern ist immer dann wünschenswert, wenn mehrere FortiGate Appliances dieselben Anwender authentifizieren müssen, oder wenn eine FortiGate in ein Netzwerk integriert wird, das bereits einen Authentifizierungsserver beinhaltet.

Single Sign On mittels FSAE

„Single (user) Sign On“ bedeutet, dass sich Anwender nur einmal anmelden müssen, um auf unterschiedliche Netzwerkressourcen zugreifen zu können. Die Fortinet

Server Authentication Extension (FSAE) bietet u.a. Single Sign On Möglichkeiten für:

- Microsoft Windows Netzwerke mit Active Directory oder NTLM Authentifizierung
- Novell Netzwerke mit eDirectory
- Zertifikat-basierte Authentifizierung

Ein RSA X.509 Server Zertifikat ist eine kleine Datei, die von einer Certificate Authority (CA) ausgegeben wird, die entweder auf einem Computer oder auf einer FortiGate Appliance installiert ist, um sich selbst gegenüber anderen Geräten innerhalb des Netzwerks zu authentifizieren. Wenn sich nun eine Instanz im Netzwerk mittels eines Zertifikates authentifiziert, kann die andere Instanz prüfen, ob dieses Zertifikat von der CA ausgegeben wurde. Die Identifizierung ist daher so vertrauenswürdig, wie die CA, die das Zertifikat ausgegeben hat. Zum Schutz gegen modifizierte oder missbräuchlich genutzte Zertifikate ist es möglich, diese von der CA zurückrufen zu lassen.

2-Faktor Authentifizierung

Optional und zur Erhöhung der Sicherheit kann ein User aufgefordert werden, zusätzlich zu bekannten Informationen (Usernamen und Passwort) einen speziellen Besitz (FortiToken oder Zertifikate) zu dokumentieren. Bei einem FortiToken handelt es sich um einen Code Generator, der für die Authentifizierung einen einmaligen Code generiert. Wenn dieses Feature aktiviert ist, muss der Anwender zusätzlich zu Username und Passwort diesen Code eingeben.

Die FortiGate Appliance verifiziert dann den Code des FortiToken in Kombination mit Usernamen und Passwort. Diese Form der Authentifizierung kann z.B. für den Aufbau einer VPN-Verbindung, für den Administration-Zugang oder die Nutzung eines WLAN-Portals verwendet werden. Als weitere Optionen für diese Art der Authentifizierung stehen der Versand einer E-Mail oder einer SMS an den sich anmeldenden User zur Verfügung. In diesem Fall müssen die darin enthaltenen Codes zusätzlich zur Anmeldung eingegeben werden.

■ FortiGate Data Loss Prevention

Der ungewollte oder mit krimineller Energie gezielte Versand sensibler Daten erzeugt nicht nur hohe Kosten, sondern kann auch das Image eines Unternehmens stark beschädigen. Data Loss Prevention (oder DLP) bezeichnet ein System oder eine Software, die zuvor definierte vertrauliche Daten identifiziert, monitort und deren unerwünschten Versand verhindert.

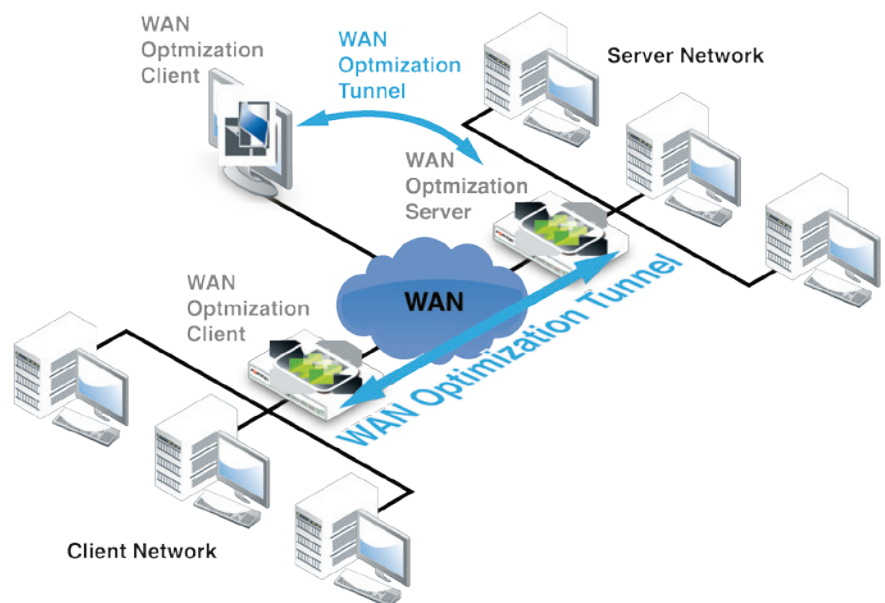
Die in FortiOS integrierten DLP Features beinhalten Finger Printing von Dokumenten oder deren Quellen, verschiedene Inspektionsmodi, erweitertes Pattern Matching sowie Datenarchivierung. Nahezu sämtliche

Inhalte können analysiert werden, darunter auch HTTP, HTTPS, FTP, FTPS, E-Mail (POP3, POP3S, IMAP, IMPS, SMTP, SMTPS), NNTP und Instant Messaging (AIM, ICQ, MSN und Yahoo!) Protokolle.

Hierbei können Textvergleiche ebenso wie erweitertes Pattern Matching mittels Wildcards oder Perl-Ausdrücken erfolgen. Zum Beispiel kann durch voreingestellte Pattern der Versand oder Empfang von Kreditkartennummern erkannt, gemeldet und/oder blockiert werden.

■ FortiGate WAN-Optimierung

Bedingt durch die Zentralisierung von Applikationen oder Serverfarmen ebenso wie die verstärkte Nutzung von Cloud Services rückt das Thema Bandbreite auf WAN-Verbindungen verstärkt in den Mittelpunkt. Häufig sind gerade kleinere Niederlassungen nicht mit hoher Bandbreite angebunden. Applikationen, die ursprünglich für die Nutzung in lokalen Netzwerken entwickelt wurden, werden in die Cloud verschoben und verursachen nun eine drastische Zunahme des Datenverkehrs auf den WAN-Verbindungen.



Anwendungen wie Windows File Sharing (CIFS), E-Mail (MAPI) und viele andere Applikationen erreichen auf diese Weise bei weitem nicht mehr die Performance, die sie in lokalen Netzwerken auszeichnen. Das Ergebnis sind häufig Produktivitätsverlust, kostspielige Netzwerk-Upgrades, teurere WAN-Verbindungen und eine höhere Belastung des IT-Personals.

Die FortiOS WAN-Optimierung beschleunigt den WANZugriff auf Applikationen und sorgt gleichzeitig

für die Sicherheit der Verbindungen. Der Service sorgt für mehr Performance, Produktivität und Bandbreiten-Reduzierung, verbesserte Server-Ressourcen und geringere Netzwerkkosten. Mit Protokolloptimierung, Byte Caching, Web & File Caching sowie SSL-Beschleunigung stehen verschiedene Tools bereit, die die benötigte Bandbreite drastisch – um bis zu 80% – reduzieren können.

■ FortiGate AntiSpam

Fortinet Anti Spam-Technologie bietet umfangreiche Möglichkeiten Spam Mails zu erkennen und zu blockieren. In gleicher Weise werden schadhafte Mail-Anhänge zuverlässig erkannt, um Angriffe von SpamBots und kompromittierten Systemen abzuwehren. FortiGate und FortiWifi-Plattformen bieten integrierte AntiSpam Funktionalität als Teil ihrer Multi Layer Schutzmechanismen. Diese werden durch kontinuierliche FortiGuard Update Services aktualisiert.

Die in FortiGate Systemen integrierte AntiSpam-Technologie kann – je nach Infrastruktur und Datenaufkommen, insbesondere bei kleineren Unternehmen eine völlig ausreichende Spam-Abwehr darstellen. Mails werden hier zwar nicht quarantänisiert (diese Funktion und viele andere bieten FortiMail Systeme – s. dazu entsprechendes Kapitel in dieser Broschüre), aber mit einer bereits sehr hohen Erkennungsrate aufgrund von Reputations-Analyse geblockt und belasten damit die internen Mail-Server nicht.

■ FortiGate SSL-Inspection

Verbindungen zwischen Webapplikationen und Web-Browsern bedienen sich häufig der SSL Verschlüsselung. Dies erhöht die Sicherheit der Datenübertragung, verhindert jedoch, dass die Security Module eine Analyse der eintreffenden Daten vornehmen können. Eine FortiGate Appliance ist in der Lage, eine SSL

Verbindung zu terminieren, die Daten zu entschlüsseln, zu analysieren und anschließend eine gesicherte SSL Verbindung zum Client aufzubauen. So ist gewährleistet, dass sowohl eintreffende als auch ausgehende Daten den Sicherheitsansprüchen des Unternehmens genügen.

■ FortiGate Bandbreiten-Management

Viele Anwendungen wie E-Mail, Video- und Audio-Streaming, Voice over IP, FTP und die zunehmende Nutzung von Webapplikationen in der Cloud lassen den Bandbreitebedarf extrem in die Höhe schnellen. In Spitzenzeiten genügt dann die zur Verfügung stehende Bandbreite nicht mehr, um alle Anwendungen adäquat zu bedienen. Die Folge sind drastische Leistungseinbrüche oder sogar der Abbruch von Verbindungen. Insbesondere bei Sprachübertragung sind jedoch derartige Aussetzer nicht akzeptabel.

Die in FortiOS integrierten Mechanismen bieten vielfältige Optionen Anwendungen zu privatisieren, ihnen Bandbreite zu garantieren oder diese zu limitieren. So kann für einzelne Applikationen Quality of Service (QoS) gewährleistet werden. Insbesondere in Verbindung mit der integrierten Applikationskontrolle und den sog. Identity Based Policies (userspezifische Regelwerke) ist es möglich, die Nutzung von Anwendungen sehr filigran zu kontrollieren.

■ FortiGate Layer 2 und Layer 3 Routing

Jede FortiGate Appliance verfügt über eine leistungsfähige Routing Engine. Damit sind sowohl statische wie auch dynamische Routing Konzepte realisierbar. Mittels dieser Optionen ist z. B. Load Balancing, regelabhängiges Routing, oder Routing im transparenten Modus

möglich. Es werden die gängigen Routingprotokolle wie z.B. RIP, BGP oder OSPF unterstützt. Insbesondere in komplexen VPN Umgebungen ist eine leistungsfähige Routing Engine zwingend erforderlich.



■ FortiGate Netzwerkzugriffskontrolle (NAC)

Die häufigen Veränderungen in Unternehmensnetzwerken – bedingt durch Umzüge, den Wechsel von Endgeräten und die Nutzung von Mobile Devices – machen es erforderlich, dass eine Zugriffskontrolle erfolgt. Dabei wird geprüft, ob auf dem Endgerät definierbare Sicherheits- und andere Anwendungen installiert sind. Zum Beispiel kann festgestellt werden, ob auf dem Endgerät ein FortiClient in seiner aktuellsten Version läuft. Ebenso wird geprüft, ob zwingend erforderliche Anwendungen auf dem Endgerät verfügbar sind.

Endpoints, die diese Prüfung nicht bestehen, werden entweder auf eine Website umgeleitet, wo ggf. die erforderliche Software heruntergeladen werden kann, oder sie werden in Quarantäne gestellt. Via SNMP kann die FortiGate auch mit einem Switch kommunizieren und diesen veranlassen, den zugehörigen Port zu deaktivieren.

■ FortiGate VoIP und SIP Security

Aufgrund der zunehmenden Implementierung von VoIP stehen sowohl Unternehmen als auch Service Provider vor der Herausforderung, Telefoniedienste hochverfügbar und in der gewohnten „analogen“ 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 Datenverkehrs, 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 Systemen, um Video-, Daten- und Voice-Traffic vor weitverbreiteten Echtzeit-Traffic-Problemen zu schützen, darunter: Session Hijacking, Server-Imitation, Nachrichten-Modifizierungen, Sitzungsabbrüche und Denial-of-Service Angriffen (DoS).

Ein weiterer Vorteil von FortiGate Lösungen für Video-Konferenzen ist, dass die bereitgestellte Sicherheit für die Endanwender transparent bleibt. Es besteht keine Notwendigkeit, Änderungen in den Video-Systemen vorzunehmen.

Schutz von Unified Communication und NGN/IMS Netzwerken

Ab FortiOS 4.2. bieten FortiGate Appliances eine Vielzahl von Carrier-grade Schutzmechanismen für SIP-Daten. Einige sind im Folgenden aufgeführt:

Deep SIP Message Inspection analysiert die Header Syntax für SIP und SDP. Bei Erkennung von Syntax-Verletzungen können entsprechende Gegenmaßnahmen konfiguriert werden, u.a. automatische SIP-Antwort-Nachrichten, um den SIP-Server zu entlasten. Die Methodik bietet u.a. Schutz vor weitverbreiteten SIP Fuzzing Angriffen.

SIP Message Rate Begrenzung erlaubt die Begrenzung der Anzahl von SIP Nachrichten pro SIP Request Methodik. So können DoS-Angriffe auf SIP-Server verhindert werden.

RTP Pin-Holing leitet nur solche RTP/RTCP Pakete weiter, die mit der individuellen Session Beschreibung des zugeordneten SIP-Dialogs konform sind. Nach Beendigung eines SIP-Dialogs schließt die FortiGate die sog. Pin-Hole automatisch. RTP/RTCP Pin-Holing wird

von FortiASICs unterstützt, so dass eine größtmögliche Durchsatzrate bei äußerst geringem Jitter erzielt wird.

Stateful SIP Dialog Tracking FortiOS analysiert SIP Nachrichten und schützt so vor ungewollten oder unerlaubten SIP Paketen, die nicht dem zugeordneten SIP-Dialog entsprechen. So ist es z. B. möglich, schadhafte SIP BYE-Nachrichten zu erkennen und zu blockieren, die nicht in den Kontext des entsprechenden SIP Dialogs passen.

■ FortiGate IPv6 Security

Seit der Vergabe der letzten IPv4-Adresse in 2010 gewinnt IPv6 zunehmend an Bedeutung auch in kleineren Unternehmen. Haben Carrier und einige größere Unternehmen bereits eine vollständige oder partielle Umstellung durchgeführt, wird durch die Einführung neuer Services, die künftig nur noch via IPv6-Adressierung erreichbar sein werden, der Druck hinsichtlich einer Migration von IPv4 nach IPv6 zunehmend ansteigen.

IPv6 bietet viele Features, die über Jahre bei IPv4 vermisst wurden: Limitierung bei der Anzahl der verfügbaren Adressen, faire Verteilung von Adressen, integrierte Quality of Service (QoS) Funktionen, bessere Multimedia-Unterstützung und verbessertes Handling von fragmentierten Daten. IPv6 verfügt über 128-Bit-Adressen (IPv4: 32-Bit) und eliminiert dadurch voraussichtlich die Notwendigkeit von NAT, da pro Person weltweit ca. 1 Milliarde IP-Adressen zur Verfügung stehen.

IPv4 und IPv6 – gemischte Welten

Durch die sich über mehrere Jahre erstreckende Umstellungsphase werden IT-Infrastruktur-Komponenten über lange Sicht beide Welten – also IPv4 und IPv6 – unterstützen müssen. Dies stellt viele der vorhandenen Komponenten, insbesondere Routing- und Security-Instanzen, vor große Herausforderungen.

Bei der Umstellung und Migration auf IPv6 stellt sich daher die Frage zum richtigen Umgang mit Malware. IPv6 bietet Malware Autoren mehr Möglichkeiten, ihren Schadcode stärker zu verbreiten, als mit IPv4. Ein trivialer Grund sind die IPv6 Stacks, mit denen es wenig Praxiserfahrung gibt. Den IPv4 Stacks liegen

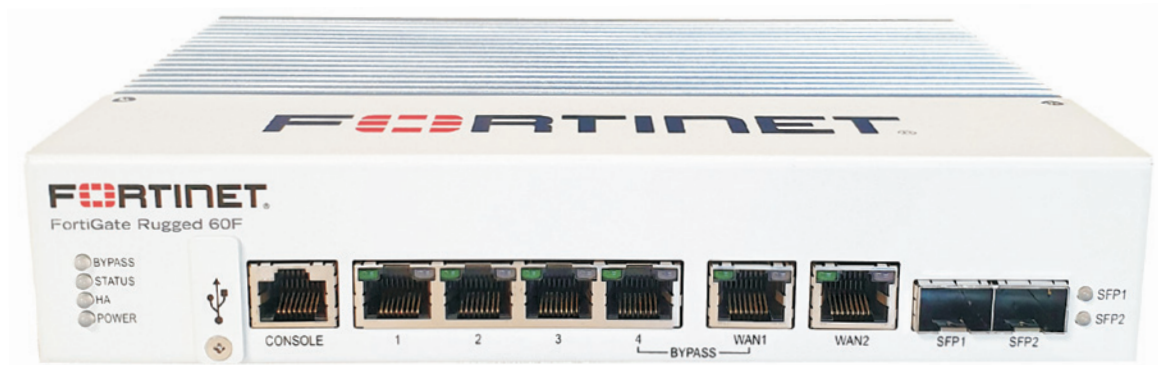
Dekaden an Erfahrung zugrunde, und trotzdem finden sich in diesen immer noch diverse Schwachstellen. IPv6 Stacks in Betriebssystemen oder in Programmen gehen weitgehend jungfräulich in den harten Internet-Alltag. Bereits heute gibt es schon über hundert bekannte Schwachstellen in diversen IPv6 Protokollstacks und Implementierungen.

IPv6 Malware

Fast alle IPv4-basierten Exploits sind auch IPv6 fähig. Das bedeutet, dass Virenschreiber im ersten Schritt nichts oder nur wenig anpassen müssen, damit ein Exploit auch IPv6 fähig ist. Sie können jedoch zusätzliche Mechanismen von IPv6 nutzen, um sich noch stärker, noch unbemerkter und damit effizienter zu verbreiten.

Ähnliches gilt für einen Wurm. „I Love You“ nutzt Email zur Weiterverteilung, hier ist keine Anpassung notwendig. Wohingegen „Conficker“ sich selbsttätig über eine Schwachstelle in Windows über IPv4 verbreitet, aber über eine Anpassung auch IPv6 tauglich gemacht werden kann.

Hackertools für IPv6 sind bereits seit Jahren im Umlauf. IPv6 Tunneldienste bergen ein hohes Risiko unbemerkt Daten an bestehenden Sicherheitslösungen vorbei zu schleusen. Malware kann zum Beispiel unbemerkt IPv6 auf einem Host aktivieren, einen IPv6 Tunneldienst starten und diesen Pfad nach außen öffnen. Ein klassisches Beispiel ist hier Teredo. Damit ließe sich nicht einfach nur IPv6 durch eine bestehende IPv4 NAT Firewall tunneln, sondern die IPv6 Adresse dieses Hosts wäre auch grundsätzlich von außen erreichbar.



IPv6 Security

Es wird offensichtlich, dass klassische, IPv4-basierte Schutzmechanismen in IPv6 oder gemischten Umgebungen keinen ausreichenden Schutz mehr bieten können. Ebenfalls liegt auf der Hand, dass ein reines „IPv6-ready“-Zertifikat genau in Augenschein genommen werden muss: Nicht jede einzelne Security-Instanz in einer UTM- oder NGFW-Appliance ist automatisch damit erfasst; vielmehr gilt es, die einzelnen Module auf ihre IPv6-Fähigkeit zu prüfen.

Durch seine jahrelange enge Kooperation mit Carriern und Service Providern, die im Bereich IPv6 zu den sog. „Early Adoptern“ gehören und deren Infrastruktur bereits in großen Teilen IPv6-fähig ist, hat Fortinet umfangreiche Erfahrungen in diesem Segment sammeln können. Darauf ist es auch zurückzuführen, dass FortiGate Lösungen bereits heute eine Vielzahl von IPv6-Security-Features bieten und bedenkenlos in eine zu migrierende Umgebung integriert werden können – bzw. eine Migration bei bereits vorhandenen FortiGate Appliances in puncto Security problemlos ist.

FortiGate Ruggedized – die Lösung für Industrie und Produktions-Umgebungen

Industrielle Kontrollsysteme werden mit immer mehr gezielten Angriffen konfrontiert und sind besonders an

fällig für Angriffe mit dem Potential, weitläufige Ausfälle zu verursachen. Traditionelle Sicherheitssysteme sind für Büro-Umfelder gedacht. Das FortiGateRugged-60D ist eine auf die Industrie spezialisierte, komplette Sicherheitslösung, die speziellen Schutz für essentielle Industrienetzwerke gegen schädliche Angriffe bietet.

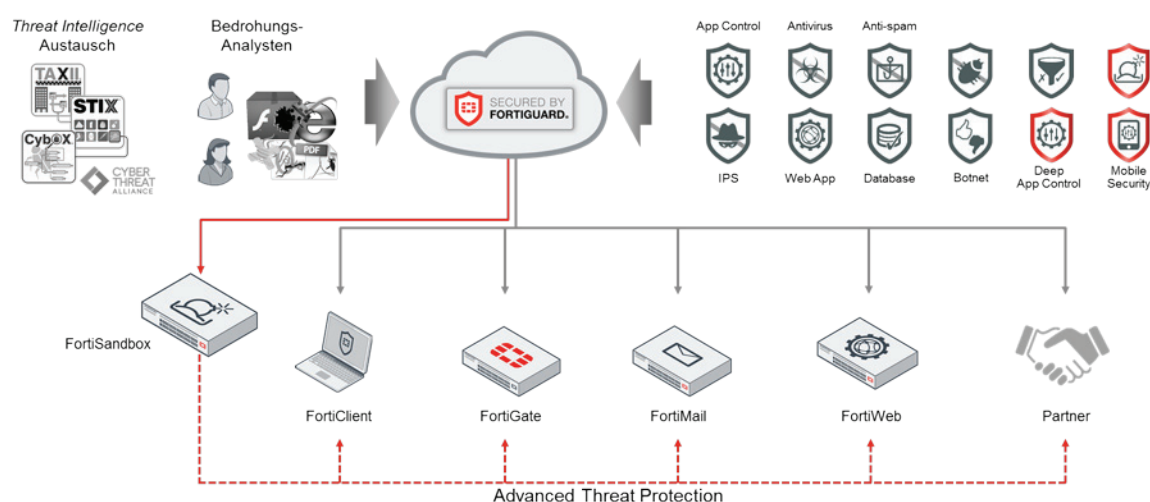
Ruggedized Protection for Harsh Environments

FortiGateRugged-60D erfüllt die Leistungsziele und Zuverlässigkeitsstandards für den Betrieb im anspruchsvollen Umfeld der Schaltstation. Es wurde für den zuverlässigen Einsatz unter schweren elektrischen und umweltlichen Bedingungen entwickelt, einschließlich großer Elektro- oder Funkinterferenzen und vieler Temperaturbereiche.

Industrial Network Security FortiOS bietet auf der Ruggedized-Plattform spezifischen Schutz für industrielle Netzwerke unter Einsatz von Sicherheitstechnologien wie Antivirus & IPS, während der Update-Dienst und das Team von Bedrohungsexperten von FortiGuard Echtzeitschutz bieten, um die neusten Angriffe ohne Intervention des Administrators zu identifizieren.

■ FortiGuard Services – globale und lokale Sicherheitsupdates:

Für einen optimalen Schutz und den perfekten Einsatz Ihrer FortiGate Firewall-Lösung benötigen Sie unseren FortiGuard Service. Diesen erhalten Sie in einzelnen Modulen (ab FortiGate 100D Serie) oder in fertigen Bündeln kombiniert mit FortiCare 24x7 Services. Hier stehen zwei Möglichkeiten zur Auswahl, entweder das UTM Bundle oder das alle Module beinhaltende Enterprise Bundle.



Die FortiGuard Lab liefern schnellen und effektiven Schutz rund um die Uhr. Unser großes Forschungsteam in den 4 über den Globus verteilten Forschungseinrichtungen erkennt neue Gefahren und entwickelt effektive Pattern, Subscriptions und Listings für die einzelnen Sicherheitsmodule auf der FortiGate. Aber auch für die anderen Fortinet Sicherheitslösungen. Unabhängige Test haben dies in der Vergangenheit mehrfach bestätigt.

FortiGuard Subscription Service	UTM Bundle	Enterprise Bundle
NGFW (IPS & Application Control)	✓	✓
AntiVirus incl. Botnet IP & Domain Reputation DB	✓	✓
Web Filtering	✓	✓
AntiSpam	✓	✓
FortiSandbox Cloud		✓
Mobile Security (Mobile AV DB)		✓

Ab FortiOS 5.4.2 oder höher.

■ FortiSIEM

FortiSIEM bietet Organisationen eine umfassende, ganzheitliche und skalierbare Sicherheits- und Event Management-Lösung vom IoT bis zur Cloud. Die Lösung verfügt über patentierte Analysefunktionen, die für eine strenge Einhaltung der Netzwerksicherheit, Leistung und Konformitätsstandards sorgen – all das über ein zentrales Dashboard.

Einheitliche NOC- und SOC-Analyse (patentierte Technologie)

Fortinet hat eine Architektur entwickelt, die einheitliche und korrelierte Analysen basierend auf unterschiedlichen Informationsquellen wie Logs, Leistungsmetriken, SNMP-Traps, Sicherheitswarnungen und Konfigurationsänderungen ermöglicht. FortiSIEM nimmt die, herkömmlich isoliert voneinander überwachten, Analysen aus SOC und NOC und führt diese Daten zu einer ganzheitlicheren Ansicht der in der Organisation verfügbaren Gefahrendaten zusammen. Jede Information wird in ein Ereignis umgewandelt, das zunächst analysiert und dann in eine ereignisbasierte Analyse-Engine für Echtzeitsuchen, Regeln, Dashboards und Ad-hoc-Abfragen geladen wird.

Verteilte Ereigniskorrelation in Echtzeit (patentierte Technologie)

Fortinet ist der einzige Anbieter mit einer verteilten Ereigniskorrelations-Engine. Komplexe Ereignismuster können in Echtzeit mit minimaler Verzögerung erkannt werden. Dank dieses patentierten Algorithmus kann FortiSIEM eine Vielzahl von Regeln bei gleichbleibend hohen Ereignisraten in Echtzeit verarbeiten, was zu wesentlich kürzeren Erkennungszeiträumen führt.

In Echtzeit-automatisierte Infrastrukturerkennung und Anwendungserkennungs-Engine (CMDB)

Fortinet hat eine intelligente Infrastruktur und Anwendungserkennungs-Engine entwickelt, die in der Lage ist die Topologie der physischen, wie auch der virtuellen Infrastruktur vor Ort sowie in Public oder Private Clouds zu ermitteln und zuzuordnen. Hierzu sind lediglich Anmeldedaten erforderlich, ohne vorherige Kenntnisse, worum es sich bei dem Gerät oder der Anwendung handelt.

Große Unternehmen und verwaltete Service Provider – „mandantenfähige Architektur“

Fortinet stellt eine äußerst flexible und mandantenfähige Architektur bereit, die es Unternehmen und Service Providern ermöglicht, eine große Zahl von physischen/logischen Domänen und überlagernden Systemen und Netzwerken von einer einzelnen Konsole aus zu verwalten.

Dynamische Zuordnung der Benutzeridentität

Fortinet hat eine dynamische Methode zur Zuordnung der Benutzeridentität entwickelt. Zunächst werden Benutzer und ihre Rollen anhand von lokalen Quellen identifiziert. Gleichzeitig wird eine neue Netzwerkidentität anhand wichtiger Netzwerkereignisse, wie etwa Firewall-Ereignissen, Active Directory-Anmeldungen, VPN-Anmeldungen, WLAN-Anmeldungen, Host Agent-Registrierungsprotokollen usw. erkannt. Schließlich erstellt FortiSIEM durch das Kombinieren von Benutzeridentität, Netzwerkidentität und Geoidentität in einer verteilten In-Memory-Echtzeitdatenbank einen dynamischen Audit-Trail zur Benutzeridentität.

Flexibles und schnelles, benutzerdefiniertes Framework zur syntaktischen Analyse (patentierte Technologie)

Fortinet hat eine XML-basierte Sprache zur syntaktischen Analyse von Ereignissen entwickelt. Sie entspricht funktional einer hohen Programmiersprache und ist leicht zu verändern. Sie kann jedoch zur Laufzeit kompiliert werden, wodurch sie äußerst effizient ist. Alle FortiSIEM-Parser übertreffen mithilfe dieser Lösung das Angebot der meisten Mitbewerber und können Daten bei mehr als 10.000 EPS (Ereignisse pro Sekunde) pro Knoten verarbeiten.



■ FortiManager

Zentralisiertes Management

FortiManager Appliances stellen eine Vielzahl von notwendigen und hilfreichen Tools zur Verfügung, mit denen eine Fortinet-basierende Sicherheits-Infrastruktur optimal und effektiv administriert und kontrolliert werden kann. So sind die Verwaltung, das RollOut, Updates oder die zentrale Konfiguration von bis zu vielen tausend Fortinet-Appliances und FortiClients einfach, übersichtlich und kostengünstig realisierbar.

FortiManager Appliances reduzieren drastisch Verwaltungskosten und vereinfachen Prozesse. Die Erkennung von Geräten, das Gruppen-Management, Auditing-Möglichkeiten sowie umfangreiche Funktionen, mittels derer komplexe VPN-Umgebungen verwaltet werden können, sind nur einige wenige der zahlreichen Features dieser Appliance-Serie. In Verbindung mit den FortiAnalyzer Lösungen für Logging und Reporting stehen äußerst leistungsfähige zentrale Management-Instanzen für jede Unternehmensgröße zur Verfügung.

Mandantenfähigkeit

Da die FortiManager Appliance-Serie auf bis zu mehrere tausend Geräte und Clients skaliert, stehen integrierte mandantenfähige Management-Domänen zur Verfügung. Diese sog. ADOMs (Administrative Domains) bieten maximale Flexibilität bei der Verwaltung von unternehmensinternen Abteilungen, unabhängigen Unternehmensbereichen oder für das Management vieler tausend verschiedener Kunden. Durch zusätzliche und optionale globale ADOMs sind weitere zentrale Administration-Features verfügbar die gleichermaßen für große Unternehmen wie für Service Provider hochinteressant sind.

Hierarchische Objektdatenbank

Die Erstellung von Templates zur Gerätekonfiguration ermöglichen das schnelle Einbinden und Konfigurieren einer Fortinet-Appliance. Jede DOM verfügt über eine gemeinsame Objektdatenbank, auf die alle Geräte und Policies zugreifen können. So sind identische oder ähnliche Konfigurationen innerhalb einer Gruppe sehr einfach zu erstellen. Mittels der optionalen Global Policy Add-Ons können

übergreifende Regelwerke und globale Datenbanken, die für alle FortiOS im System zur Verfügung stehen, erstellt werden.

Lokales Security Content Hosting

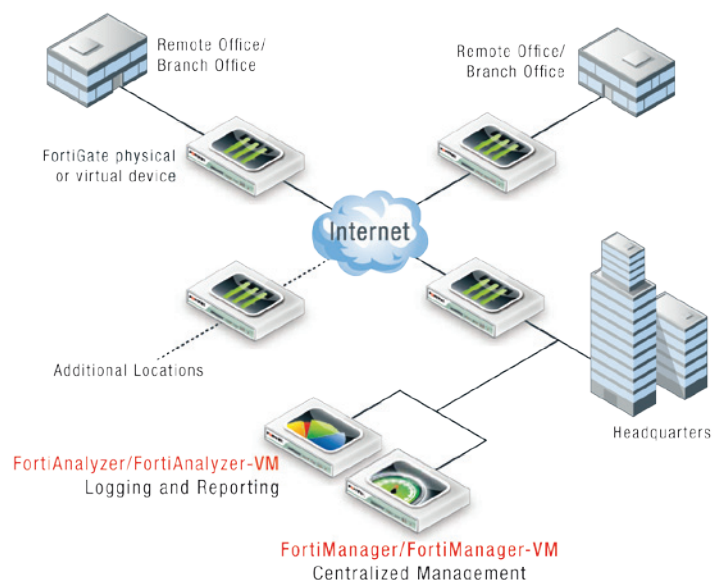
Die Option, Security Updates lokal bereitzustellen, bietet Administratoren bessere Kontrollmöglichkeiten über Updates und reduziert und verbessert Antwortzeiten für Rating Datenbanken. So können Antivirus-, Intrusion Prevention-, Schwachstellenmanagement-, Web Filtering- und Anti-Spam-Updates lokal zur Verfügung gestellt werden.

Vereinheitlichtes Managementmodell

Ein optimierter und einheitlicher Work-Flow ermöglicht die einfache Konfiguration mehrerer verschiedener Management-Komponenten via ADOM. Dazu stehen Objekte und dynamische Objekte, Import- und VPN-Wizards, VDOM-Synchronisation, Geräte-Übersichten und GUI-basierende Skripte zur Verfügung.

FortiManager XML API

Die FortiManager XML-API ist eine Web-Service-Schnittstelle, die der Automatisierung von Managementprozessen dient. Kunden einer privaten oder öffentlichen Cloud können so z.B. in ein Provisioning-System integriert werden. Außerdem können FortiGate Systeme über ein Web-Service-Interface konfiguriert werden.





■ 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 EMail-Daten können archiviert und ausgewertet werden. Zusätzlich können geographisch und chronologisch verteilte Securitydaten zentral gesammelt, korreliert und analysiert werden.

Umfangreiches Reporting

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.

Auf diese Weise können sich Unternehmen jeder Größenordnung einen einfachen und konsolidierten Überblick über ihre Security-Situation verschaffen. Durch eine Vielzahl von voreingestellten und kunden-spezifischen Reports werden Unternehmen ebenfalls bei ihren Compliance-Bestrebungen unterstützt.

Schwachstellenmanagement

Die FortiAnalyzer Systeme bieten sehr umfangreiche Scan-Möglichkeiten, die es erlauben, sämtliche Endgeräte in einem Netzwerk zu erkennen und zu priorisieren, Schwachstellen zu katalogisieren, Ports zu erstellen und Listen mit Handlungsempfehlungen auszugeben. Unternehmen, die PCI DSS Compliance nachweisen müssen, können auf voreingestellte Schwachstellen-Scans und -Reports zurückgreifen.

Wesentliche Funktionen:

- **UTM- & Trafficberichte**
Analysieren Sie regelmäßig Ihr Sicherheitsprofil und Ihre Traffic-/Bandweitenmuster mit einem neuen gemeinsamen UTM-/Trafficbericht.

- **Integrierte Berichtsvorlagen**
Nutzen Sie die anpassbaren PDF-Vorlagen für bunte, umfassende und grafische Netzwerksicherheits- und Nutzungsberichte.
- **Import/Export von Vorlagen**
Exportieren Sie nach dem Erstellen eines Berichts die Konfiguration auf einen anderen FortiAnalyzer oder ADOM und bearbeiten Sie sie.
- **Ereignisverwaltung**
Überwachen Sie wichtige Ereignisse mit einmaligen Analysemöglichkeiten für potentiell anomales Verhalten, um sie dem IT-Administrator vorzulegen.
- **Drill-Downs**
Grafische Echtzeitdarstellungen der Traffic-, Web-, E-Mail- und Bedrohungsaktivitäten.

Alarmierung

- Umfassende Alarmeinstellung
- Auslösung nach Schwere, bestimmten Ereignissen, Aktionen und Zielen
- Festlegung verschiedener Schwellen für die Anzahl von Ereignissen in einem bestimmten Zeitraum
- Anzeige und Suche vergangener Alarme
- Benachrichtigung per E-Mail/SNMP oder Erstellung eines Syslog-Ereignisses

Log Viewer

- Anzeige von vergangenen oder Echtzeit-Protokollen
- Auswahl aus Traffic, Ereignis oder UTM-Protokollen
- Suche nach Gerät, ADOM oder im Ganzen
- Protokollfilter und Suchmöglichkeiten
- Gezielte Untersuchung mit Protokolldetails
- Intuitive Icons für Länder, Anwendungen, etc.

DLP-Archivierung

- Untersuchung von DLP-Content-Archiven
- Unterstützte Archivtypen u. A.: E-Mail, HTTP, FTP, IM
- Archivtext anzeigen oder Dateien herunterladen

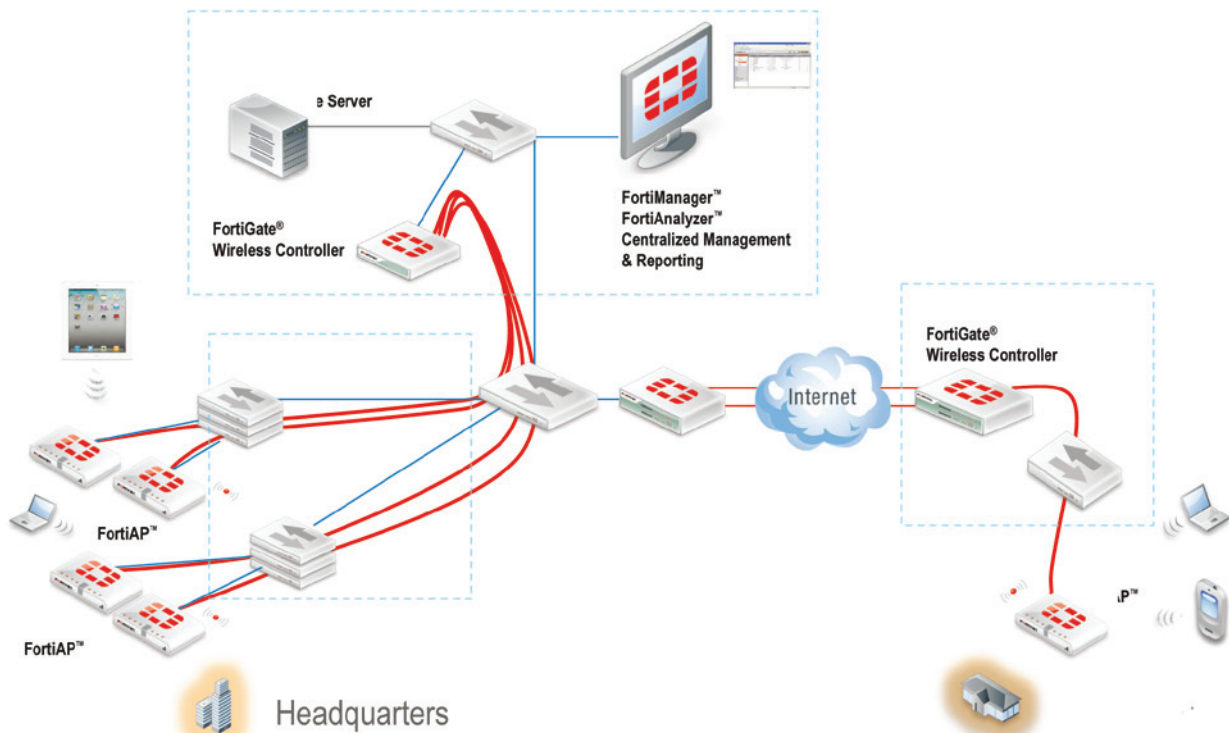
■ FortiAP – Sichere WLAN Infrastruktur mit den Access Points FortiAP

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 in jeder FortiGate Appliance bietet High-Performance Netzwerkzugänge mit integrierter Content-Security. Durch die Kombination eines Wireless Controllers mit einer FortiGate Plattform (größer als Modell FG30B) wird das Sicherheitsniveau des kabelgebundenen LANs automatisch auf die WLAN-Umgebung übertragen.

Der gesamte WLAN-Traffic wird so identitätsbasiert 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 prüfen.

Da jede FortiGate Appliance (größer als Modell FG30B) 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. Die Thin WLAN Access Point Serie FortiAP umfasst Modelle für jeden Anwendungsbereich, sowohl Indoor als auch Outdoor.





Voucher-Erstellung für Gastzugänge

Mittels einer integrierten sog. Receptionist-GUI können auf einfache Weise Vouchers für den WLAN-Zugang erstellt und ausgedruckt werden. Die Zugänge können z.B. zeitlich beschränkt werden, gleichzeitig für eine Gruppe von Personen erstellt und komfortabel verwaltet werden.

Remote Access Points und Local Break Out

Mobile Mitarbeiter, Teleworker sowie Niederlassungen eines Unternehmens benötigen ebenfalls WLAN. Dieses muss denselben Sicherheitsanforderungen der

Zentrale genügen und auch von dieser managebar sein. Mittels der FortiGate und FortiAP Integration ist beides möglich. Überdies kann Traffic auch über einen sog. Local Break Out in der jeweiligen Niederlassung verbleiben und muss nicht zwingend – je nach Regelwerk – über die Zentrale geroutet werden.

Remote Access Points stellen darüberhinaus eine elegante, kleine und kostengünstige Möglichkeit dar, kleine Home-Offices oder mobile Mitarbeiter sehr schnell und einfach an die Zentrale anzubinden und über eine CAPWAP-Verbindung eine verschlüsselte Verbindung dorthin zu etablieren.



■ FortiToken

Einmal-Passwort für starke Authentifizierung

Mit dem FortiToken 200 können Unternehmen leistungsfähige aber dennoch preiswerte und einfache starke 2-Faktor-Authentifizierung einführen. Dabei handelt es sich um Einmal-Passwort-Token (auch One-Time-Passwort/OTP), mit dem Unternehmenszugänge gesichert werden können, die bisher auf schwache 1-Faktor-Authentifizierung (z.B. statische Passwörter) ausgelegt sind.

Mit dem FortiToken können Administratoren sowohl mobile als auch unternehmensinterne Anwender in ein erweitertes Sicherheitskonzept einbeziehen. Dabei ist das FortiToken Teil der umfangreichen Produktstrategie zur Multi-Faktor-Authentifizierung, mit der sichergestellt wird, dass nur noch autorisierte Personen Zugang zu unternehmenskritischen Daten erhalten.

Nutzen der vorhandenen Fortinet-Appliances

Jede FortiGate Appliance bietet ab FortiOS 4.3. die Möglichkeit der 2-Faktor-Authentifizierung. Ein externer und nicht selten kostenintensiver Server sowie kostspielige Token mit Jahreslizenzen können so entfallen. Die zeitbasierenden FortiToken bieten starke Authentifizierung für IPsec VPN, SSL VPN, WLAN Captive Portals und FortiGate Administrator Login. Dabei ist das Token ständig mit der FortiGate zeitsynchronisiert.

FortiGuard Schlüsselmanagement

Das FortiGuard Center sorgt für ein sicheres und komfortables Schlüsselmanagement. Nach Registrierung der Token-S/N an der FortiGate verteilt das FortiGuard Security Center die zugehörigen Schlüssel über eine Cloud-basierende sichere Infrastruktur an die jeweiligen FortiGates. Wenn es eine identitätsbasierende Regel erfordert, ist eine FortiGate so in der Lage, das 6-stellige Token-Passwort gegen seine eigene Datenbank zu verifizieren.

Integration mit FortiAuthenticator

In Verbindung mit dem FortiAuthenticator kann die Nutzung des FortiTokens sehr einfach auf komplexere FortiGate Umgebungen sowie auf 3rd-Party-Systeme erweitert werden. Nähere Informationen finden sich im separaten Kapitel zum FortiAuthenticator in dieser Broschüre.

Standards und AAA Server Kompatibilität

Das FortiToken ist kompatibel mit herkömmlichen lokalen und Remote-Access-Servern inklusive Active Directory, LDAP und RADIUS. Die FortiGate verwaltet somit gleichzeitig sowohl die Backend-Kommunikation mit diesen Servern als auch die 2-Faktor-Authentifizierung mit dem Anwender. In Kombination mit einer FortiGate entspricht das FortiToken dem OATH Standard.

Widerstandsfähiges Design

Das FortiToken wird in einem manipulationssicheren Gehäuse ausgeliefert und der veränderungsresistente interne Speicher verhindert Manipulationen am dynamischen Passwort-Generator.



FortiToken 200CD

Mit FortiToken 200CD, bei dem die Token-Seeds auf den Servern der FortiGuard Labs sicher hinterlegt sind, bietet Fortinet eine Option, die Kunden diese Seeds auf einer verschlüsselten CD bereitstellt. Somit hat der Anwender die Möglichkeit, diese Token-Keys in eigener Verantwortung sicher zu verwahren und die Mehrfachnutzung (ein Token auf mehreren FortiGates) wird stark vereinfacht.

FortiToken 300 – USB-SmartCard Token

Für besonders sichere Umgebungen bietet sich das FortiToken 300, eine USB-SmartCard-Token für PKI-Infrastrukturen an. Es bietet OneTime-Passwords und Verschlüsselung über einen Hardware-Chip in Verbindung mit einer Client-Software. Letztere ist für Windows, Linux und MacOS verfügbar. Es werden Microsoft CAPI und PKCS#11 APIs unterstützt. Die Lizenz ist – wie auch bei den übrigen FortinetToken Lösungen, eine Einmal-Lizenz, so dass keine weiteren Kosten entstehen.



FortiToken Mobile

Ergänzend zu den Hardware-Token ist es mit dem FortiToken Mobile möglich, iOS und Android-Geräte als Token zu nutzen. Diese OATH-kompatible Lösung bietet ein zeitbasiertes OneTime-Passwort-Verfahren und entbindet den User von der Nutzung eines zusätzlichen Geräts (HW-Token). Durch ein dynamisches Generieren der Token-Seeds sowie dessen verschlüsselte Übertragung und Speicherung ist dieses Verfahren deutlich sicherer als vergleichbare Methoden.

Das FortiToken Mobile ist mit den FortiGate Appliances ebenso nutzbar wie mit der Authentifizierungs-Lösung FortiAuthenticator und somit universell einsetzbar. Es basiert auf einer Einmal-Lizenz, die eine wiederholte Lizenzierung überflüssig macht und somit Kosten spart. Jede FortiGate Appliance ab FOS5 bietet die kostenlose Nutzung von zwei FortiToken Mobile beispielsweise für Admin-Accounts.



■ FortiAuthenticator – Zentraler AAA-Server

Der FortiAuthenticator dient als zentrale Instanz für das User Identity Management. Es werden 2-Faktor-Authentifizierung, Identitäts-Verifikation und Netzwerk-zugriffskontrolle (NAC) unterstützt.

Durch den Support von LDAP und RADIUS und die Integration des Fortinet Single Sign On Features der FortiGate Serie in Active Directory stehen umfangreiche Funktionen zur Zugriffskontrolle der Anwender zur Verfügung. FortiAuthenticator ermöglicht die zentrale Zugriffssteuerung auf FortiGate und 3rd-Party-Systeme, VPN-Zugänge und Webseiten.

Zwei Faktor Authentifizierung

Der FortiAuthenticator erweitert die 2-Faktor-Authentifizierung mittels Token auf Umgebungen mit vielen verteilten FortiGate Appliance und 3rd-Party-Lösungen, die RADIUS oder LDAP-Authentifizierung unterstützen.

Die im FortiAuthenticator gespeicherten Informationen zur Benutzeridentität in Verbindung mit den Authentifizierungs- Informationen des FortiToken stellen sicher, dass nur autorisierte Anwender Zugang zu sensiblen Unternehmensdaten erlangen. Neben zusätzlicher Sicherheit unterstützt diese Vorgehensweise Unternehmen bei der Einhaltung von Compliance-Vorgaben oder anderen Regularien.

Vereinfachtes Management und Benutzerfreundlichkeit

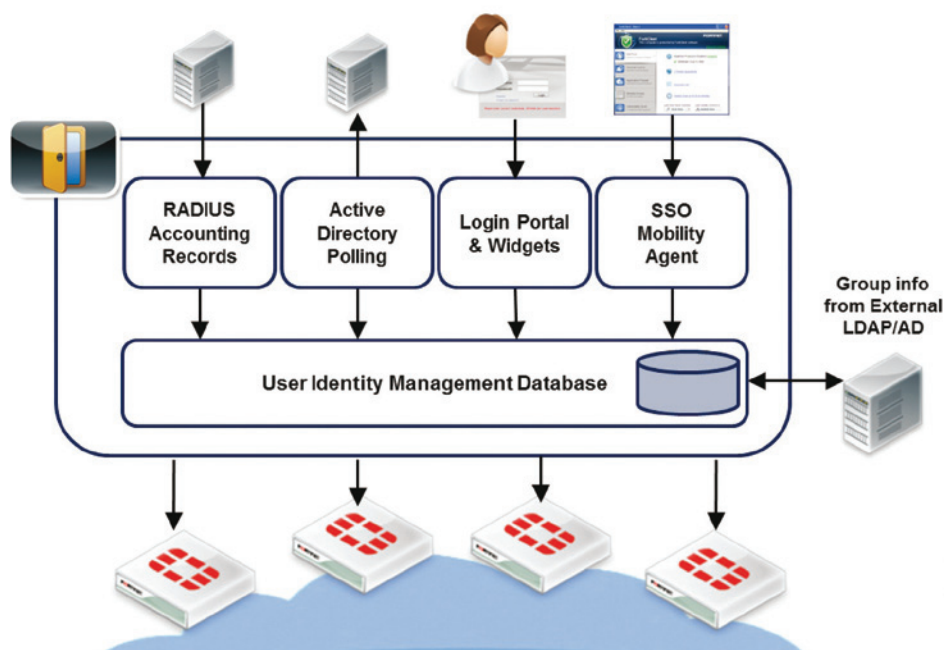
Durch die Bereitstellung sämtlicher erforderlicher Dienste sowie die Speicherung aller Benutzerdaten auf einem einzigen System, werden die Kosten für sichere Nutzer-Authentifizierung deutlich gesenkt.

Der FortiAuthenticator ist in wenigen Minuten betriebsbereit und wurde speziell zur Vereinfachung von Authentifizierungs-Prozessen entwickelt. Dies schließt die Integration in bereits vorhandene Authentifizierungs-Datenbanken ebenso ein, wie die reibungslose Token-Initialisierung.

Eine weitere Arbeitserleichterung bietet das Self-Service-Portal, über welches Anwender ihre Zugangsdaten anfordern können, wenn sie ihr Token verloren oder vergessen haben.

Fortinet Single Sign On (FSSO)

Fortinet Single Sign On (FSSO) steigert die Benutzerfreundlichkeit, indem es die Anzahl der erforderlichen LogIns deutlich reduziert. Die Integration von FSSO in Active Directory ermöglicht die Konfiguration und Nutzung von identitätsbasierten Regelwerken, um Netzwerk- und Datenzugriff in Abhängigkeit von Gruppenzugehörigkeiten festzulegen.





■ FortiClient Endpoint Security

Personal Computer (PCs), Desktops und Laptops ermöglichen den Anwendern den Zugang zu Unternehmensapplikationen und vertraulichen Daten – vom internen Netzwerk ebenso wie von unterwegs. Während sich die Produktivität verbessert, erhöht der Zugriff von außen gleichzeitig das Sicherheitsrisiko für die interne Netzwerkinfrastruktur. Die Rechner sind sogenannten „Blended Threats“ ausgesetzt, also Angriffen, die sich gleichzeitig verschiedener Mechanismen bedienen, wie z. B. Viren, Trojaner, Würmer, Spyware, Keylogger, Botnetzen, Spam und Internet-Attacken.

Während Netzwerk-Sicherheitsarchitekturen verschiedene Segmente voneinander isolieren, können sich PCs, die sich innerhalb eines Subnetzes befinden, durchaus gegenseitig infizieren. Anwender verstoßen oft unabsichtlich gegen die Sicherheitsrichtlinien, in dem sie tragbare Speichermedien (USB Sticks, MP3-Player, Kameras, mobile Festplatten) einsetzen, nicht darauf achten, ob ihr Virenschutz auf dem aktuellen Stand ist oder sogar die Personal Firewall ausschalten.

Anwender, die auf Webseiten mit unangemessenen oder schädlichen Inhalten zugreifen, gefährden die Integrität des Netzwerks, beeinflussen die Produktivität negativ, verursachen Sicherheitsrisiken und lösen unter Umständen rechtliche Auseinandersetzungen aus.

Während Sicherheitstechnologien, wie z. B. AntiVirus Software, einen bestimmten Angriffspunkt schützen und somit nur für bestimmte Angriffsarten zur Verfügung stehen, versagen diese Methoden bei „Blended Threats“ und sind auch nicht in der Lage, Zugangsrichtlinien umzusetzen.

FortiClient Security Suite

Der neue FortiClient in seiner aktuellen Version 5 konsolidiert die bisher verfügbaren Varianten und erweitert seinen Einsatzbereich auf zusätzliche Plattformen, darunter auch die gängigsten mobilen Betriebssysteme iOS und Android. Dadurch – und durch eine Vielzahl weiterer Funktionen – ist sein Einsatz auch in heterogenen und BYOD-(Bring Your Own Device) Umgebungen möglich.

Seine einzeln aktivierbaren Sicherheits-Engines reichen von einer leistungsstarken AntiVirus-Einheit über WebFilter bis hin zu VPN-Clients und Schwachstellen-Management-Funktionen. In Verbindung mit einer FortiGate kann der FortiClient zentral administriert und überwacht werden; ebenfalls ist auf diese Weise ein lokales Logging und Auswerten der Client-Daten möglich.

Einfachste und kostengünstige Lizenzierung

In der Standalone-Version ist der FortiClient – inkl. aller Updates – kostenlos unter www.forticlient.com zum Download verfügbar. Diese Option ermöglicht es kleinen Unternehmen und auch Privatpersonen, ihre Endgeräte effektiv zu sichern und überdies kostengünstige VPN-Verbindungen zu einer zentralen FortiGate bereitzustellen.

Größere Unternehmen mit den Anforderungen, ihre Endgeräte zentral zu administrieren, zu updaten und zu überwachen, können mithilfe einer FortiGate Appliance die FortiClients zentral verwalten. Auf diese Weise können unterschiedliche Profile erstellt und ausgerollt werden, auch in Abhängigkeit von der aktuellen Netzwerk-Verbindung („on-net/off-net“).

Ebenso können die Logdaten der Clients zentral gesammelt und ausgewertet werden. Pro FortiGate Appliance sind 10 FortiClients kostenfrei integrier- und managebar. Bei weiteren Clients ist der Erwerb einer permanenten Einmallizenz erforderlich.

FortiEDR

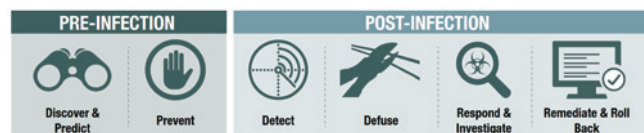
Erweiterter, automatisierter Endpunkt-Schutz mit Bedrohungserkennung und Response-Maßnahmen

Überblick

Komplexe Angriffe können Endgeräte in wenigen Minuten – wenn nicht Sekunden – infizieren. EDR-Tools (Endpoint Detection and Response) der ersten Generation sind dagegen machtlos. Aus mehreren Gründen: Sie erfordern eine manuelle Alert-Sichtung & -Reaktion und erzeugen so viele Indikatoren, dass bereits überlastete Security-Teams von einer Flut von Sicherheitswarnungen überrollt werden. Auch steigen durch veraltete EDR-Tools die Security-Operations-Kosten und Prozesse können so langsam werden, dass das Geschäft darunter leidet.

FortiEDR bietet einen intelligenten Echtzeit-Bedrohungsschutz, der Endgeräte vor und nach einer Infektion schützt. Die Lösung reduziert proaktiv die Angriffsfläche und verhindert Malware-Infektionen. Potenzielle Bedrohungen werden in Echtzeit erkannt und entschärft. Zudem lassen sich Incident Response und Fehlerbehebung mit anpassbaren Playbooks automatisieren. FortiEDR unterstützt Sie dabei, Sicherheitsverletzungen automatisch und effizient in Echtzeit zu unterbinden, ohne Ihr Security-Team mit einer Flut von Fehlalarmen zu überlasten oder den Geschäftsbetrieb zu stören.

Mit automatisierten EDR-Funktionen für die Bedrohungssuche und Incident Response greift der Schutz sofort: Mit FortiEDR gibt es keine zeitliche Verzögerung zwischen Reaktions- und Verweilzeit – und auch kein zu spätes oder ausbleibendes Reagieren auf Sicherheitswarnungen. Zudem schützt FortiEDR Systeme dank seiner Security-Parität unterschiedlichste Betriebssysteme auf Workstations, Servern und virtuellen Maschinen, einschließlich älterer Betriebssysteme und eingebetteter Systeme.



Erkennung mit proaktiver Risikominderung der Angriffsfläche

- Entdecken und kontrollieren von Rogue- (d. h. ungeschützte oder nicht verwaltete Geräte) und IoT-Geräten
- Nachverfolgen von Anwendungen und Bewertungen
- Erkennen und Schließen von System- & Anwendungsschwachstellen mit virtuellem Patching
- Reduktion von Angriffsflächen mit risikobasierten, proaktiven Richtlinien

Next-Generation-Antivirus (NGAV)

- Kernelbasierter NGAV-Schutz mit maschinellem Lernen
- Anreicherung der Ergebnisse mit Bedrohungsdaten aus Echtzeit-Feeds von einer ständig aktualisierten Cloud-Datenbank
- Offline-Schutz für Endgeräte, die nicht mit dem Netzwerk verbunden sind
- Gerätesteuerung über USB

Automatisierter Echtzeit-Schutz

- Auf Betriebssysteme abgestimmte Bedrohungserkennung, die verdeckte, eingeschleuste Angriffe mit hoher Präzision ausspürt – einschließlich speicherbasierter und „Living Off The Land“-Angriffe
- Schließen von Sicherheitslücken in Echtzeit und Eliminieren der Verweildauer von Bedrohungen
- Analyse der gesamten Log-History
- Schutz vor Ransomware-Verschlüsselung und Manipulationen von Dateien und Registry
- Kontinuierliche Validierung der Bedrohungsklassifizierung
- Weniger Fehlalarme und keine Flut von Sicherheitswarnungen, damit keine Alerts übersehen werden



Reaktion mittels anpassbarer Playbooks

- Automatisierte Klassifizierung von Vorfällen
- Standardisierte Incident-Response - Verfahren mit Playbook-Automatisierung
- Optimieren von Security-Ressourcen mit automatisierten Incident-Response-Aktionen (Entfernen von Dateien, Beenden bössartiger Prozesse, Rücknahme dauerhafter Änderungen, Informieren von Benutzern, Ticket-Erstellung, Isolieren von Anwendungen und Geräten, etc.)
- Kontextbasierte Reaktion auf Vorfälle mithilfe einer Klassifizierung von Vorfällen und Angriffsziele (z.B. Endgeräte-Gruppen)
- Vollständige Transparenz über die Angriffsketten und bössartigen Änderungen mittels patentiertem Code-Tracing
- Automatisierte Bereinigung und Rollback von bössartigen Änderungen ohne Beeinträchtigung der Systemverfügbarkeit
- Optionaler MDR-Dienst (Managed Detection und Response) als SOC-Ergänzung

Geführte Benutzeroberfläche mit Datenanreicherung

- Automatisierte Untersuchung mit minimalen Störungen für Endanwender
- Automatische Threat-Entschärfung und -Blockierung
- Patentierte Code-Tracing-Technologie für vollständige Transparenz über Angriffsketten und Stacks
- Aufbewahren von Speicher-Snapshots bei In-Memory-Angriffen für die Suche nach speicherbasierten Bedrohungen
- Geführte Benutzeroberfläche mit verständlichen Erklärungen mit Angabe des zugehörigen MITRE-Attack-Frameworks sowie des nächsten logischen Schritts für die forensische Untersuchung

Security-Fabric-Integration

FortiEDR nutzt die Architektur der Security Fabric und funktioniert integriert mit vielen Security-Fabric-Komponenten wie FortiGate, FortiSandbox, FortiNAC oder FortiSIEM.

Management-, Architektur- und Plattform-Unterstützung

Die integrierte Management-Konsole bietet Funktionen zur Verhinderung, Erkennung und Reaktion auf Bedrohungen und Sicherheitsvorfälle. Erweiterte REST-APIs sind für alle Konsolen-Aktionen und weitere Funktionalität verfügbar.

Offline-Security: Schutz und Erkennung erfolgen beim Endpunkt, damit auch nicht verbundene Endgeräte sicher sind.

Native Cloud-Infrastruktur: FortiEDR bietet ein mandantenfähiges Management in der Cloud. Die Lösung kann nativ in der Cloud, hybrid oder On-Premises bereitgestellt werden. Auch Air-Gapped-Umgebungen werden unterstützt.

Schlanker Endpunkt-Agent: FortiEDR beansprucht weniger als 1 % der CPU-Leistung, höchstens 120 MB RAM und 20 MB Festplattenspeicher und belastet den Netzwerk-Traffic minimal.

Unterstützte Betriebssysteme: FortiEDR unterstützt Windows-, MacOS- und Linux-Betriebssysteme und bietet außerdem einen Offline-Schutz.

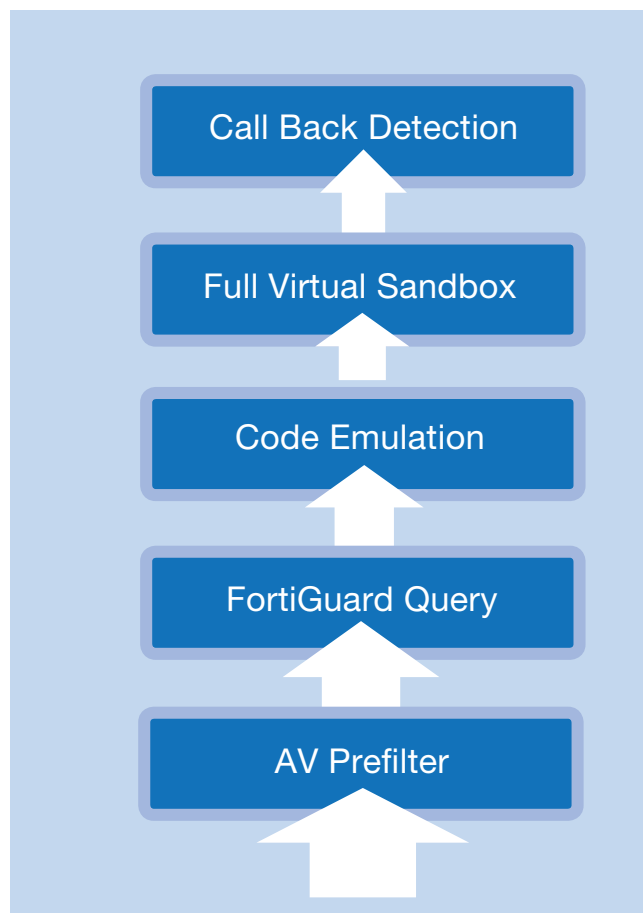
■ FortiSandbox

Mithilfe der leistungsstarken Sicherheits-Appliance (die auch als VM-Lösung verfügbar ist) FortiSandbox können Unternehmen und Behörden hochgefährliche Angriffe wie zum Beispiel Advanced Persistent Threats (APTs) zuverlässiger erkennen und verhindern. APTs sind zielgerichtete und besonders effektive Cyber-Attacken auf IT-Infrastrukturen und vertrauliche Daten, die zumeist über einen längeren Zeitraum ausgeführt werden.

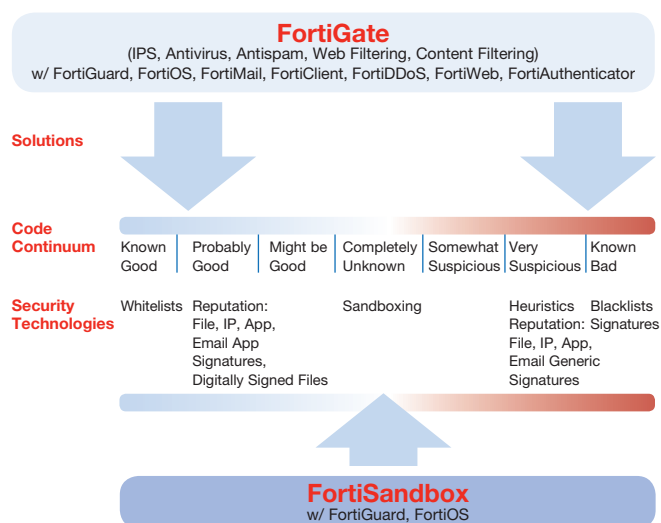
Das neue Fortinet-Angebot verbindet eine einzigartige Dual-Level-Sandbox mit der dynamischen Aufdeckung von Bedrohungen, Echtzeit-Dashboard sowie umfassenden Reporting-Funktionen in einer einzigen Anwendung, die sich sowohl in vorhandene Netzwerke als auch mit Fortinets FortiGate Next Generation Firewalls (NGFW) sowie den FortiMail E-Mail-Gateway-Appliances integrieren lässt.

Die NGFWs von Fortinet agieren als erste Verteidigungslinie – sie erkennen und minimieren Sicherheitsbedrohungen. In Kombination mit der FortiSandbox sind die Appliances in der Lage, besonders verdächtige oder risikoträchtige Dateien mit neuartigen Erkennungsmethoden zu identifizieren und zu untersuchen. Aufgrund der Ergebnisse dieser Analyse werden dann alle Schutzmechanismen – basierend auf dem gesamten Lebenszyklus der erkannten Bedrohung – aktualisiert.

Mit der neuen FortiMail Version 5.1 können Fortinet E-Mail-Gateways sowohl verdächtige als auch High-Risk-Dateien in E-Mails identifizieren und sie zur weiteren Untersuchung an die FortiSandbox weiterleiten.



Mehrstufige Arbeitsweise einer FortiSandbox

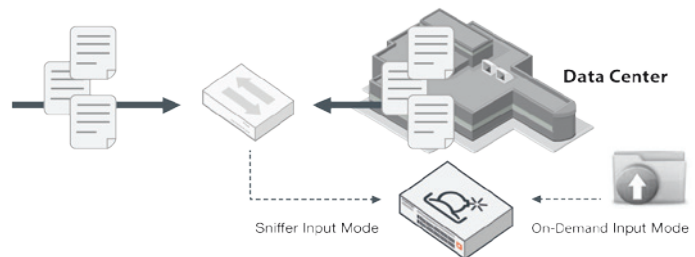


Die FortiSandbox auf einen Blick

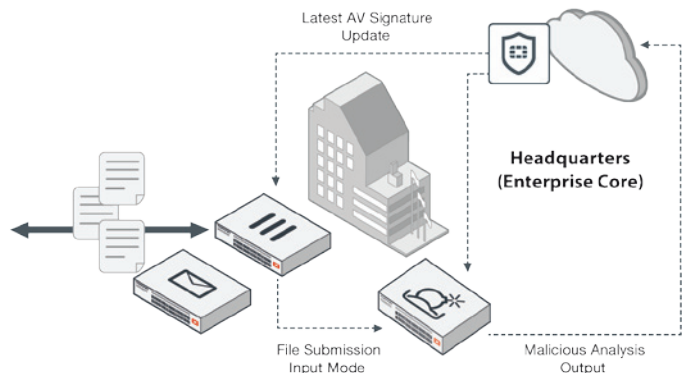
Die FortiSandbox lässt sich standalone in vorhandene Netzwerke integrieren, ohne weitere Konfigurationen vornehmen zu müssen. Alternativ ermöglicht die Lösung eine Ergänzung von Fortinets FortiGate und FortiMail Plattformen, um deren Erkennungsmechanismen weiter zu verbessern.

Getreu der Fortinet-Philosophie konsolidiert die FortiSandbox hochentwickelte Threat Detection- und Intelligence-Dienste über viele Protokolle und Funktionen hinweg in einer einzigen besonders leistungsstarken und kostengünstigen Appliance. Deren Herzstück ist eine Dual-Level Sandbox, die neuartige und komplexe Angriffsmethoden auf virtuelle Maschinen (VM) ebenso aufdeckt wie die Vielzahl immer raffinierterer Cyber-Attacken.

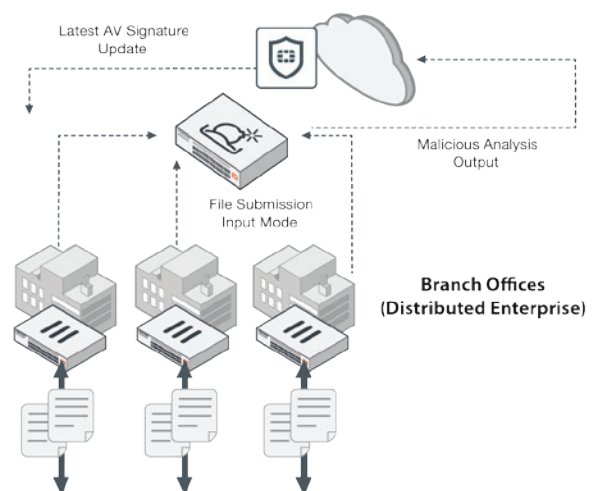
Betriebsmodus „Standalone“



Betriebsmodus „FortiGate/FortiMail Integrated“



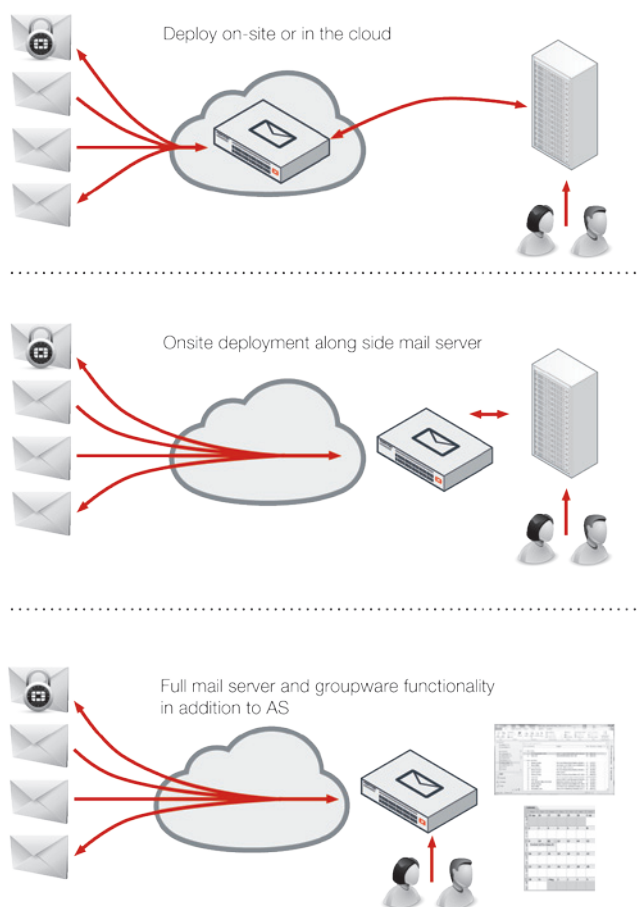
Betriebsmodus „Distributed FortiGate Integrated“



FortiMail

Email-Security

FortiMail Appliances und virtuelle Appliances bieten leistungsfähigen und umfangreichen Schutz für E-Mail-Dienste in Unternehmen jeder Größenordnung – von KMU über Carrier, Service Provider bis hin zu sehr großen Enterprise-Unternehmen. Fortinets jahrelange Erfahrung im Schutz von Netzwerken gegen Spam, Malware und andere message-basierende Angriffe spiegelt sich auch in dieser Lösung wider.



Sicherer Schutz von Mail-Systemen

FortiMail schützt E-Mail-Systeme davor, selbst zum Malware-Verteiler zu werden. Durch ihre bidirektionale Architektur schützen FortiMail Systeme Netzwerke vor eingehenden Spam-Nachrichten und Malware, bevor diese im Unternehmen Schaden anrichten können. Gleichzeitig wird verhindert, dass schadhafte ausgehende E-Mails von anderen externen Gateways zu einem Blacklisting des Unternehmens führen. Insbe-

sondere letztere Eigenschaft ist für Service Provider essenziell und höchst geschäftskritisch. FortiMail Appliances bieten High-Performance E-Mail Routing und Security durch die Verwendung von mehreren höchst genauen Anti-Spam-Filtern. In Verbindung mit Fortinets marktführenden Antivirus-&Anti-Spyware-Modulen wird höchste Sicherheit garantiert.

Verschiedene Betriebsmodi

Verschiedene Anwendungsszenarien ermöglichen zusätzliche Flexibilität beim Einsatz der Appliance. Diese kann sowohl im Gateway Modus, im Transparent Modus sowie im Server Modus betrieben werden.

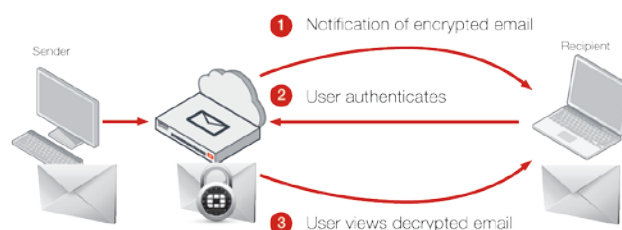
Einfaches Lizenzmodell

Das User-unabhängige Lizenzmodell garantiert niedrige Anschaffungs- und Betriebskosten und ermöglicht so eine transparente Planung.

FortiMail Identity based Encryption (nutzerabhängige Mail-Verschlüsselung)

Eine neue Funktionalität wertet die erfolgreiche und leistungsfähige Mail-Security-Appliance FortiMail noch weiter auf. Seit dem Release 4.2 der FortiMail Familie können abhängig von Nutzer (Sender) oder Mailinhalten (Wörterbücher) Mails verschlüsselt versendet werden. Dabei ist es nicht notwendig, dass auf Seiten des Senders oder des Empfänger zusätzliche Client-Software installiert wird.

Unternehmen können also kostenlos und ohne weiteren Administrationsaufwand sensible E-Mail-Kommunikation verschlüsseln und damit deutlich sicherer übertragen. Durch die sog. Identity Based Encryption werden Mails abhängig von Nutzergruppe, Nutzer oder spezifischen in der Mail enthaltenen Wörtern verschlüsselt.



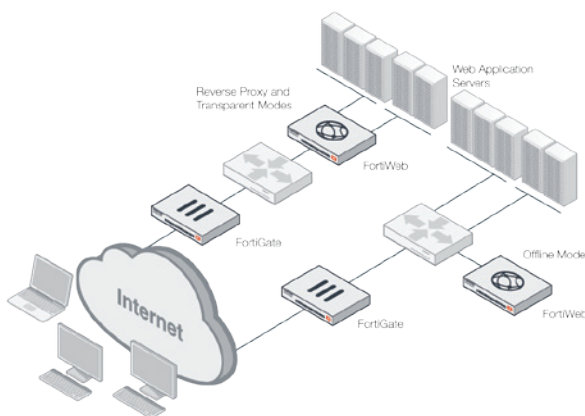
■ FortiWeb Web Application Firewall

Web-Anwendungen und Sicherheit

Web-Anwendungen nutzt nahezu jeder wie selbstverständlich – und es ist ebenso selbstverständlich, dass sie auch funktionieren. War in der Vergangenheit oft nur die Rede von E-Mail-Portalen, CRM-Portalen und ähnlichem – also reinen Business-Anwendungen für Mitarbeiter – so haben wir es inzwischen im Alltag eines jeden Internetnutzers damit zu tun. Sogenannte Provisioning-Portale werden für alle Lebensbereiche selbstverständlich.

Das Programmieren von Web-Anwendungen ist in der Regel fokussiert auf eine bestimmte Funktionalität und auf eine möglichst schnelle Verfügbarkeit, sowie geringe Kosten. Das Einbinden der notwendigen Sicherheits-Algorithmen erfordert einen mit zunehmender Komplexität der Anwendung immens steigenden Programmieraufwand – und erzeugt damit Kosten sowie eine Verzögerung der Auslieferung. Gleiches gilt für die ständigen Updates der Anwendung, die nur noch selten statisch und unverändert bleibt.

Security in eine Web-Applikation einzubinden stellt somit nicht nur eine große Herausforderung dar – es wird in den meisten Fällen schlicht vernachlässigt oder nur oberflächlich umgesetzt.



Die verschiedenen Betriebsmodi der FortiWeb

Web Services und „normale“ Firewalls

Eine normale Firewall – auch wenn sie über IPS und Applikationskontrolle verfügt – ist nicht in der Lage, Web FortiWeb Web-Application-Servers FortiWeb

Service-basierte Angriffe zu erkennen und abzuwehren. Web Services – also die den Web-Applikationen zugrundeliegenden Funktionen (die oft von mehreren Anwendungen gleichzeitig genutzt werden) – bedienen sich einer eigenen Beschreibungssprache (WSDL) und eines eigenen Protokolls (SOAP). Sowohl WSDL als auch SOAP beinhalten keinerlei Security-Mechanismen, beschreiben bzw. übertragen aber alle Parameter eines Web-Dienstes transparent.

Es liegt auf der Hand, dass Angriffe in Form von z.B. Manipulationen des Services sehr leicht möglich sind. Ein Beispiel hierfür sind sog. XDoS-Attacken, die auf nur einem einzigen System mit wenigen Byte Code erzeugt werden können, da XML rekursive Strukturen erlaubt. Mit einem simplen Eingriff ist so z.B. eine Endlosschleife „programmierbar“, die denselben Effekt erzeugt, wie ein „normaler“ DoS Angriff, für den i.d.R. mehrere tausend Systeme manipuliert und fremdgesteuert werden müssten.

Sicherheit mit FortiWeb

Die FortiWeb Produktfamilie repräsentiert eine solche integrierte Web-Security Appliance-Serie. Mit unterschiedlichen Leistungsdaten aber einheitlichem Feature-Set adressiert sie Unternehmen aller Größenordnungen, Application Service Provider (ASPs) und SaaS-Anbieter.

FortiWeb stellt neben den Modulen Web Application Firewall, XML Firewall und Web Traffic Optimizer auch ein Applikations-basiertes Load Balancing sowie einen leistungsfähigen Schwachstellenscanner bereit.

Mit der Möglichkeit des Auto-Learning ist es überdies möglich, den Traffic zu Web Anwendungen regelmäßig zu analysieren und entsprechende Security Profile automatisiert zu erstellen – ohne Eingriff in die vorhandene Netzwerkinfrastruktur oder die zu schützende Applikation.

Ein Policy Wizzard sowie voreingestellte Regelwerke erleichtern den Einsatz und die Inbetriebnahme der FortiWeb Appliances ebenso wie die verschiedenen Anwendungsszenarien als Transparent Inspection, Reverse oder True Transparent Proxy, sowie Offline.

FortiDDoS

Abwehr von DDoS-Angriffen
bis auf Applikationsebene

DDoS – keine „kleine“ Störung, sondern eine ernste Bedrohung

„Hacktivismus“ per Botnets und via Netzwerk-Test-Anwendungen haben im vergangenen Jahr drastisch zugenommen und führten zu einem starken Anstieg sowohl der Anzahl von Angriffen als auch DDoS-Angriffen auf Applikationsebene. Diese Angriffe legen ganze Webseiten lahm, indem sie die Anwendungs-Server und/oder die Internetverbindung überlasten.

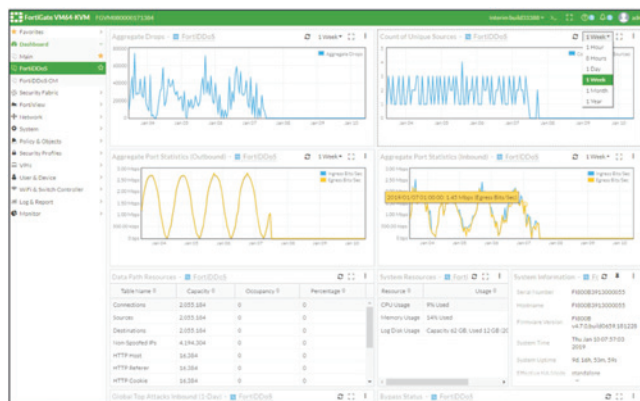
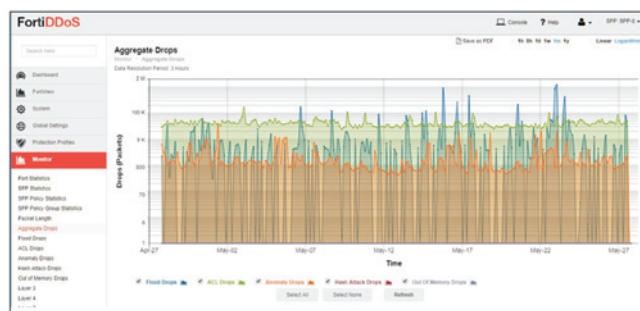
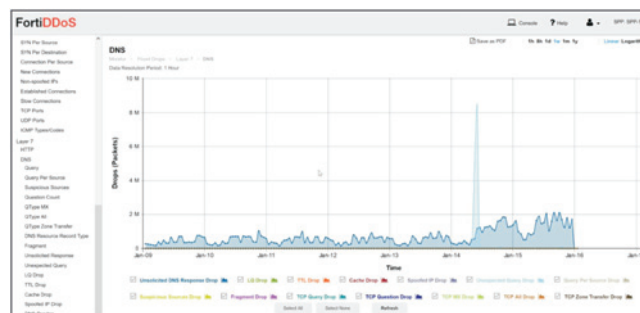
Da Unternehmen immer häufiger Software-as-a-Service (SaaS)-Angebote und andere Public-Cloud-basierte Dienste verwenden, werden DDoS-Attacken zu einem sehr ernsthaften Problem für CIOs und CSOs – und dies bereits bei der Entscheidung, ob sie Dienste überhaupt in die Cloud auslagern oder ihre Systeme und Daten weiterhin inhouse betreiben und verwalten möchten.

Die häufigsten Beweggründe für DDoS-Attacken sind heute entweder finanziell oder politisch geprägt. Finanziell motivierte Angreifer versuchen, Websitebetreiber zu erpressen, indem sie einen ersten Angriff starten und Zahlungen verlangen, die dann zukünftige Angriffe vermeiden sollen. Politisch motivierte Angreifer hingegen reagieren auf eine Aktivität des Unternehmens und stören oder unterbrechen in der Regel wichtige Geschäftsprozesse.

Motivunabhängig wirken sich Ausfallzeiten nicht nur auf die Kunden, Partner und Angestellten des Unternehmens aus, sondern können auch seine Marke und Glaubwürdigkeit stark schädigen.

FortiDDoS Appliances schützen effektiv

Die FortiDDoS Appliances wurden zum Erkennen und Abwehren von intelligenten DDoS-Attacken entwickelt und bieten somit optimalen Schutz für das Netzwerk. Die Appliances verfügen über anwendungsspezifische Chipsets (sog. ASICs), die auch hochentwickelte und hochvolumige DDoS-Angriffe blockieren und trotzdem extrem niedrige Latenz (weniger als 26 µs) garantieren.



So ist die Verfügbarkeit von kritischen Systemen, Servern und Anwendungen auch bei DDoS-Angriffen mit hoher Frequenz gewährleistet. Neben einer detaillierten Einsicht in den Netzwerkverkehr in Echtzeit sowie automatischem Schutz gegen gezielte DDoS-Attacken bieten die FortiDDoS Appliances als einzige Lösungen Netzwerk-Virtualisierung und ein automatisches und kontinuierliches Traffic-Baselining. Die Virtualisierungs-Funktion verhindert, dass Angriffe auf ein einzelnes Segment des Netzes Auswirkungen auf andere Bereiche haben.

Dies ist insbesondere für die permanente Verfügbarkeit von Systemen und Applikationen in virtualisierten Umgebungen von Rechenzentren und bei Cloud-Service-

Providern von Bedeutung. Das automatische Traffic-Baselining ermöglicht darüber hinaus die Erstellung eines Netzwerk-Verhaltensmodells, das sich fortlaufend und ohne Eingreifen des Anwenders aktualisiert und damit den Verwaltungsaufwand deutlich reduziert.

FortiDDoS Highlights

Alle FortiDDoS Appliances bieten acht virtualisierte Netzwerkpartitionen mit unabhängigen Schutz-Profilen für virtualisierte Umgebungen, eine automatische Netz-

werkverkehrsanalyse und kontextbezogene Richtlinien für Schwellwerte, um maximale Leistungsfähigkeit zu ermöglichen. Zusätzlich verfügen sie über eine Echtzeit- und eine historische Traffic-Analyse, die außergewöhnlich detaillierte Einblicke in die Top-Attacks, Top-Quellen und Top-Angreifer gewährleistet. Die FortiDDoS Produktreihe bedient sich eines neuartigen Designs für die Beseitigung typischer Leistungsengpässe, indem sichergestellt wird, dass weder CPU noch Betriebssystem Datenpakete verlangsamen.

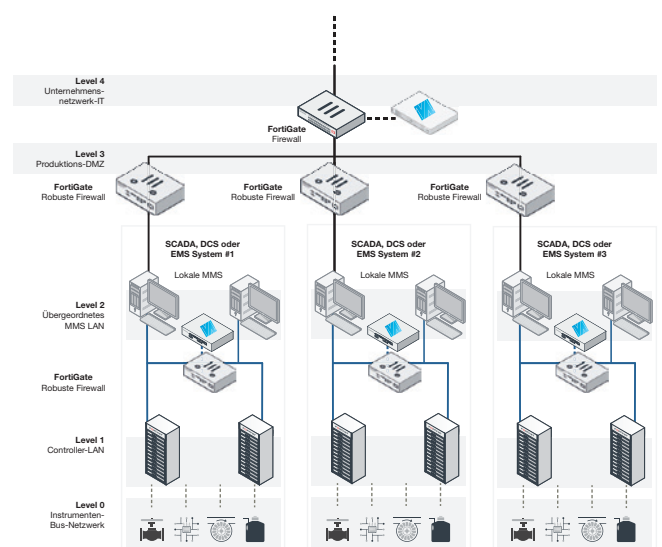
■ SCADA

Industrial Control Systems (ICS) einschließlich SCADA-Systemen (Supervisory Control and Data Acquisition) sind in den vergangenen Jahren zum Angriffsziel geworden.

Malware wie STUXNET und BlackEnergy haben ICS Schäden mit erheblichen Folgen zugefügt. Die ausschlaggebenden Fragen sind, warum dies geschieht und ob wir uns Sorgen machen müssen. Diese Angriffe sind schlichtweg ein Indikator für die Verwundbarkeit von ICS-Systemen und die potenziellen Schäden der kritischen Infrastruktur, deren Grundlage sie bilden.

ICS-Systeme wurden ursprünglich in einer Zeit entwickelt, in der operative Technologienetze (OT) noch analoge, proprietäre Systeme mit wenig bis gar keiner Verbindung zur Außenwelt waren. Ihre Sicherheit beruhte auf ihrer relativ starken Isolation. Dann wurde man sich jedoch der Vorteile gängiger Internetprotokolle sowie der einfachen und kostensparenden Nutzung von Windowsbasierten

Terminals wie MMS und SCADA Masters bewusst. Damit gerieten die in traditionellen IT-Systemen mit ihren Sicherheitsproblemen eingesetzten OT-Netzwerke auf Kollisionskurs. Der Wandel brachte zwei Hauptprobleme mit sich. Zum einen können sich ICS-Netzwerke in einer kritischen Infrastruktur keine unerwarteten Ausfälle leisten, auch nicht zu Wartungszwecken oder für einfache Updates oder Patch-Installationen. Dies macht die Windows-basierten Terminals verwundbar. Zum anderen verfügen die seriellen Protokolle von ICS-Systemen, die lediglich in TCP/IP gekapselt werden, über keinerlei eigene Sicherheitsfunktionen wie Authentifizierung oder Verschlüsselung.



FortinetVM

Fortinet-Lösungen auch für VM-Systeme

Security Lösungen für virtualisierte Umgebungen – sog. Virtual Appliances – erlauben nun auch die Integration der bekannten und umfangreichen Fortinet-Security Lösungen in kritische, virtualisierte Infrastrukturen. Darüber hinaus ermöglichen Sie die kurzfristige Bereitstellung von Security-Diensten wann und wo auch immer sie benötigt werden.

Da Unternehmen inzwischen selten eine reine hardware-basierte oder reine virtuelle Infrastruktur betreiben, ist es sinnvoll, bedarfsabhängig beide Lösungen zu integrieren. In Kombination mit den höchst leistungsfähigen Fortinet-Appliances können Unternehmen somit einen Mix aus Soft- und Hardware-basierter Security Infrastruktur implementieren. Fortinet bietet bereits seit 2004 virtualisierte Security-Lösungen an, die heute von vielen Service-Providern und Großkonzernen genutzt werden, um flexibel und mandantenfähig komplexe Sicherheits-Dienste anbieten zu können.

Mit der FortinetVM Serie erweitert Fortinet dieses Angebot für VMware und XEN Plattformen und ermöglicht noch weiterreichende Flexibilität. So können Unternehmen eine verteilte Infrastruktur sowohl hardware-basiert als auch virtualisiert nutzen und zentral mit nur einer Management-Instanz administrieren. Auch FortiManager und FortiAnalyzer sind als virtualisierte Lösungen verfügbar und integrieren sich so in ein schlüssiges Konzept.

Lösungen für MSSPs

Durch ein speziell beim FortiAnalyzer adaptiertes neues und additives Lizenzmodell können nun individuelle Security-Services seitens eines Managed Security Service Providers einfach und mit planbaren Kosten bereitgestellt werden. So kann die gesamte Infrastruktur – oder Teile derselben – auf virtuellen Systemen abgebildet werden. Bereits vorhandene Plattformen können so optimal genutzt und die benötigten Services bedarfsgerecht skaliert werden.

Virtual Appliance Support Matrix

	VMWare vSphere	Citrix Xen Server	Xen	KVM	Microsoft Hyper-V	Nutanix AHV	Amazon AWS	Microsoft Azure	Oracle OPC/OCI	Google GCP	Alibaba Aliyun
FortiGate-VM *	•	•	•	•	•	•	• / #	• / #	• / #	• / #	• / #
FortiManager-VM	•	•	•	•	•	•	• / #	•	•	•	•
FortiAnalyzer-VM	•	•	•	•	•	•	• / #	•	•	•	•
FortiWeb-VM	•	•	•	•	•	•	• / #	• / #	•	•	•
FortiWeb Manager-VM	•						•				
FortiMail-VM	•	•		•	•	•	• / #	• / #		•	
FortiAuthenticator-VM	•		•	•	•		•	•	•		
FortiADC-VM	•	•	•	•	•	•	• / #	• / #	• / #	• / #	
FortiVoice-VM	•	•		•	•		•	•			
FortiRecorder-VM	•	•		•	•		#				
FortiSandbox-VM	•			•	•	•	• / #	#			
FortiSIEM-VM	•			•	•	•	•	•			•
FortiProxy-VM	•			•							

*Available as FortiGate-VMX solution for VMware NSX environment, AzureStack and RackSpace (PAYG) # on-demand

FortiGate® Network Security Platform - *Top Selling Models Matrix

	FG/FWF-40F	FG/FWF-50E	FG/FWF-60E	FG/FWF-60F	FG-80E
Firewall Throughput (1518/512/64 byte UDP)	5 / 5 / 5 Gbps	2.5 Gbps ****	3 / 3 / 3 Gbps	10/10/6 Gbps	4 / 4 / 4 Gbps
IPsec VPN Throughput (512 byte) ¹	4.4 Gbps	90 Mbps	2 Gbps	6.5 Gbps	2.5 Gbps
IPS Throughput (Enterprise Mix) ²	1 Gbps	350 Mbps	400 Mbps	1.4 Gbps	450 Mbps
NGFW Throughput (Enterprise Mix) ^{2,4}	800 Mbps	220 Mbps	250 Mbps	1 Gbps	360 Mbps
Threat Protection Throughput (Ent. Mix) ^{2,5}	600 Mbps	160 Mbps	200 Mbps	700 Mbps	250 Mbps
Firewall Latency	4 µs	180 µs	3 µs	4 µs	3 µs
Concurrent Sessions	700,000	1.8 Million	1.3 Million	700,000	1.3 Million
New Sessions/Sec	35,000	21,000	30,000	35,000	30,000
Firewall Policies	5,000	5,000	5,000	5,000	5,000
Max G/W to G/W IPSEC Tunnels	200	200	200	200	200
Max Client to G/W IPSEC Tunnels	250	250	500	500	2,500
SSL VPN Throughput	490 Mbps	100 Mps	150 Mbps	900 Mbps	200 Mbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	200	200	200	200	200
SSL Inspection Throughput (IPS, avg. HTTPS) ³	310 Mbps	150 Mbps	135 Mbps	630 Mbps	135 Mbps
Application Control Throughput (HTTP 64K) ²	990 Mbps	450 Mbps	650 Mbps	1.8 Gbps	900 Mbps
Max FortiAPs (Total / Tunnel)	16 / 8	10 / 5	30 / 10	64 / 32	32 / 16
Max FortiSwitches	8	8	16	16	16
Max FortiTokens	500	500	500	500	500
Virtual Domains (Default/Max)	10 / 10	5 / 5	10 / 10	10 / 10	10 / 10
Interfaces	5x GE RJ45	7x GE RJ45	10x GE RJ45	10x GE RJ45	14x GE RJ45, 2x Shared Port Pairs
Local Storage	—	32 GB (51E)	128 GB (61E)	128 GB (61F)	128 GB (81E/-POE)
Power Supplies	Single AC PS	Single AC PS	Single AC PS	Single AC PS	Single AC PS
Form Factor	Desktop	Desktop	Desktop	Desktop	Desktop
Variants	WiFi, 3G4G	WiFi, Dual WiFi, Storage, LENC	WiFi, Storage, LENC, DSL, POE	WiFi, Storage	POE, Storage

	FG-80F	FG-100E	FG-100F	FG-200E	FG-400E
Firewall Throughput (1518/512/64 byte UDP)	10 / 10 / 7 Gbps	7.4 / 7.4 / 4.4 Gbps	20 / 18 / 10 Gbps	20 / 20 / 9 Gbps	32 / 32 / 24 Gbps
IPsec VPN Throughput (512 byte) ¹	6.5 Gbps	4 Gbps	11.5 Gbps	7.2 Gbps	20 Gbps
IPS Throughput (Enterprise Mix) ²	1.4 Gbps	500 Mbps	2.6 Gbps	2.2 Gbps	7.8 Gbps
NGFW Throughput (Enterprise Mix) ^{2,4}	1 Gbps	360 Mbps	1.6 Gbps	1.8 Gbps	6 Gbps
Threat Protection Throughput (Ent. Mix) ^{2,5}	900 Mbps	250 Mbps	1 Gbps	1.2 Gbps	5 Gbps
Firewall Latency	4 µs	3 µs	5 µs	3 µs	3 µs
Concurrent Sessions	1.5 Million	2 Million	1.5 Million	2 Million	4 Million
New Sessions/Sec	45,000	30,000	56,000	135,000	450,000
Firewall Policies	5,000	10,000	10,000	10,000	10,000
Max G/W to G/W IPSEC Tunnels	200	2,000	2,500	2,000	2,000
Max Client to G/W IPSEC Tunnels	2,500	10,000	16,000	10,000	50,000
SSL VPN Throughput	950 Mbps	250 Mbps	1 Gbps	900 Mbps	4.5 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	200	500	500	500	5,000
SSL Inspection Throughput (IPS, avg. HTTPS) ³	715 Mbps	130 Mbps	1 Gbps	820 Mbps	4.8 Gbps
Application Control Throughput (HTTP 64K) ²	1.8 Gbps	1 Gbps	2.2 Gbps	3.5 Gbps	12 Gbps
Max FortiAPs (Total / Tunnel)	32 / 16	64 / 32	128 / 64	256 / 128	512 / 256
Max FortiSwitches	16	24	24	64	72
Max FortiTokens	500	5,000	5,000	5,000	5,000
Virtual Domains (Default/Max)	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10
Interfaces	8x GE RJ45, 2x Shared Port Pairs	20x GE RJ45, 2x Shared Port Pairs	2x 10 GE SFP+, 18x GE RJ45, 4x Shared Port Pairs, 8x GE SFP	18x GE RJ45, 4x GE SFP	18x GE RJ45, 16x GE SFP
Local Storage	128 GB (81F)	480 GB (101E)	480 GB (101F)	480 GB (201E)	480 GB (401E)
Power Supplies	Single AC PS, dual inputs	Single AC PS, opt. Ext RPS	Dual AC PS	Single AC PS, opt. Ext RPS	Single AC PS, opt. Dual PS
Form Factor	Desktop	1 RU	1 RU	1 RU	1 RU
Variants	Bypass, Storage	POE, High Port Density	—	—	—

FortiGate® Network Security Platform - *Top Selling Models Matrix

	FG-600E	FG-1000D	FG-1100E	FG-1500D	FG-1800F
Firewall Throughput (1518/512/64 byte UDP)	36 / 36 / 27 Gbps	52 / 52 / 33 Gbps	80 / 80 / 45 Gbps	80 / 80 / 55 Gbps	198 / 197 / 140 Gbps
IPsec VPN Throughput (512 byte) ¹	20 Gbps	25 Gbps	48 Gbps	50 Gbps	55 Gbps
IPS Throughput (Enterprise Mix) ²	10 Gbps	6 Gbps	12.5 Gbps	13 Gbps	13 Gbps
NGFW Throughput (Enterprise Mix) ^{2,4}	9.5 Gbps	5 Gbps	9.8 Gbps	7 Gbps	11 Gbps
Threat Protection Throughput (Ent. Mix) ^{2,5}	7 Gbps	4 Gbps	7.1 Gbps	5 Gbps	9.1 Gbps
Firewall Latency	2 µs	3 µs	3 µs	3 µs	4 µs
Concurrent Sessions	8 Million	11 Million	8 Million	12 Million	12 Million
New Sessions/Sec	450,000	280,000	500,000	300,000	750,000
Firewall Policies	10,000	100,000	100,000	100,000	100,000
Max G/W to G/W IPSEC Tunnels	2,000	20,000	20,000	20,000	20,000
Max Client to G/W IPSEC Tunnels	50,000	100,000	100,000	100,000	100,000
SSL VPN Throughput	7 Gbps	3.6 Gbps	8.4 Gbps	4 Gbps	11 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	10,000	10,000	10,000	10,000	10,000
SSL Inspection Throughput (IPS, avg. HTTPS) ³	8 Gbps	5.0 Gbps	10.0 Gbps	5.7 Gbps	17 Gbps
Application Control Throughput (HTTP 64K) ²	15 Gbps	14 Gbps	26 Gbps	16 Gbps	34 Gbps
Max FortiAPs (Total, Tunnel)	1,024 / 512	4,096 / 2,048	4,096 / 2,048	4,096 / 2,048	4,096 / 1,024
Max FortiSwitches	96	128	196	128	196
Max FortiTokens	5,000	20,000	20,000	20,000	20,000
Virtual Domains (Default/Max)	10 / 10	10 / 250	10 / 250	10 / 250	10 / 250
Interfaces	2x 10 GE SFP+, 10x GE RJ45, 8x GE SFP	2x 10 GE SFP+, 16x GE SFP, 18x GE RJ45	2x 40GE QSFP+, 4x 25GE SFP28/10GE SFP+, 4x 10GE SFP+, 8x GE SFP, 18x GE RJ45	8x 10GE SFP+/GE SFP, 16x GE SFP, 18x GE RJ45	4x 40 GE QSFP+, 12x 25 GE SFP28/10GE SFP+, 2x10 GE SFP+, 8x GE SFP, 18x GE RJ45
Local Storage	480 GB (601E)	256 GB	960 GB (1101E)	480 GB	2 TB (1801F)
Power Supplies	Single AC PS, opt. Dual PS	Dual PS	Dual PS	Dual PS	Dual PS
Form Factor	1 RU	2 RU	2 RU	2 RU	2 RU
Variants	—	LENC	DC	10GE RJ45, LENC	—

	FG-2000E	FG-2200E	FG-3000D	FG-3300E	FG-3400E
Firewall Throughput (1518/512/64 byte UDP)	90 / 90 / 60 Gbps	158 / 155 / 100 Gbps	80 / 80 / 50 Gbps	160 / 158 / 100 Gbps	240 / 238 / 150 Gbps
IPsec VPN Throughput (512 byte) ¹	65 Gbps	98 Gbps	50 Gbps	98 Gbps	140 Gbps
IPS Throughput (Enterprise Mix) ²	11.5 Gbps	16.5 Gbps	23 Gbps	27 Gbps	44 Gbps
NGFW Throughput (Enterprise Mix) ^{2,4}	9 Gbps	13.5 Gbps	22 Gbps	23 Gbps	34 Gbps
Threat Protection Throughput (Ent. Mix) ^{2,5}	5.4 Gbps	11 Gbps	13 Gbps	17 Gbps	23 Gbps
Firewall Latency	2 µs	4 µs	3 µs	4 µs	4 µs
Concurrent Sessions	20 Million	24 Million	50 Million	50 Million	50 Million
New Sessions/Sec	500,000	500,000	400,000	460,000	460,000
Firewall Policies	100,000	100,000	200,000	200,000	200,000
Max G/W to G/W IPSEC Tunnels	20,000	20,000	40,000	40,000	40,000
Max Client to G/W IPSEC Tunnels	100,000	100,000	200,000	200,000	200,000
SSL VPN Throughput	6 Gbps	10 Gbps	8 Gbps	10 Gbps	11 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	30,000	30,000	30,000	30,000	30,000
SSL Inspection Throughput (IPS, avg. HTTPS) ³	9.4 Gbps	17 Gbps	15 Gbps	21 Gbps	30 Gbps
Application Control Throughput (HTTP 64K) ²	20 Gbps	52 Gbps	40 Gbps	70 Gbps	86 Gbps
Max FortiAPs (Total, Tunnel)	4,096 / 2,048	4,096 / 2,048	4,096 / 2,048	4,096 / 2,048	4,096 / 2,048
Max FortiSwitches	196	196	256	256	256
Max FortiTokens	20,000	20,000	20,000	20,000	20,000
Virtual Domains (Default/Max)	10 / 500	10 / 500	10 / 500	10 / 500	10 / 500
Interfaces	6x 10GE SFP+, , 34x GE RJ45	4x 40GE QSFP+, 20x 25GE SFP28/10GE SFP+, 14x GE RJ45	16x 10GE SFP+/GE SFP, 2x GE RJ45	4x 40GE QSFP+, 16x 25GE SFP28/10GE SFP+, 4x 10GE RJ45, 14x GE RJ45	4x 100GE QSFP28/40GE QSFP+, 24x 25GE SFP28/10GE SFP+/GE SFP, 2x GE RJ45
Local Storage	480 GB	2 TB (2201E)	480 GB	2 TB (3301E)	4 TB (3401E)
Power Supplies	Dual PS	Dual PS	Dual PS	Dual PS	Dual PS
Form Factor	2 RU	2 RU	2 RU	2 RU	2 RU
Variants	—	—	—	—	DC

* Featured Top selling models, for complete FortiGate offerings please visit www.fortinet.com. FortiGate virtual appliances are also available. All performance values are "up to" and vary depending on system configuration.

FortiSandbox™ Advanced Threat Prevention System

	FSA-500F	FSA-1000F-DC	FSA-2000E	FSA-3000E	FSA-VM
Sandbox Pre-Filter Throughput (Files/Hour) ¹	4,500	7,500	12,000	15,000	Hardware dependent
VM Sandboxing Throughput (Files/Hour)	120	280	480	1,120	Hardware dependent
Real-world Effective Throughput (Files/Hour)	600 ² / 360 ³	1,400 ² / 840 ³	2,400 ² / 1,440 ³	5,600 ² / 3,360 ³	Hardware dependent
Number of VMs	2 +4 optional	2 +10 optional	4 +20 optional	8 + 48 optional	4, up to 54
FortiGuard Subscription Based Security Service Option: FortiGuard Threat Intelligence (AV, IPS, Web Filtering, File Query and Sandbox Engine Update)					

¹ FortiSandbox pre-filtering is powered by FortiGuard Intelligence.

² Measured based on real-world data when both prefilter and dynamic analysis are working consecutively.

³ Measured based on real-world email traffic when both pre-filter and dynamic analysis are working consecutively.

* Based on the assumption that 1 blade will be used as master in HA-cluster mode.

FortiClient™ Advanced Endpoint Protection

	Windows	MAC OS X	Linux	Android	iOS	Chromebook
Security Fabric Components	Fabric Agent	Fabric Agent	Fabric Agent	Fabric Agent (Limited)	Fabric Agent (Limited)	Fabric Agent (Limited)
Host Security Components	AV, Anti-Exploit, Sandbox Detection, Web Filtering, App. Firewall	AV, Web Filtering, App. Firewall	AV, Sandbox Detection (Limited)	Web Filtering	Web Filtering	Web Filtering
VPN Components	IPSec, SSL VPN	IPSec, SSL VPN	SSL VPN	IPSec, SSL VPN	IPSec, SSL VPN	—
Others	Remote Logging/Reporting, WIN AD SSO Agent	Remote Logging/Reporting, WIN AD SSO Agent	—	—	Remote Logging/Reporting	Remote Logging/Reporting

FortiSIEM™ Unified Event Correlation and Risk Management Solution

	FSM-500F “COLLECTOR”	FSM-2000F “SUPERVISOR”	FSM-3500F “SUPERVISOR”
All-in-One License Capacity	N/A	Up to 500	Up to 2,000
EPS Capacity (all features enabled)	5,000	Up to 15,000	Up to 30,000

FortiAP™ Wireless Access Point

	FortiAP Series	Fortinet AP Series	FortiAP S-Series	FortiAP U-Series
Management	FortiGate-Managed, Cloud-Managed	Controller-Managed	FortiGate-Managed, Cloud-Managed	FortiGate-Managed, Cloud-Managed, Controller-Managed
Security	Via FortiGate	-	AV, IPS, AC, WF	Via FortiGate

* Frequency selection and power may be restricted to abide by regional regulatory compliance laws.

For Complete selection of FortiAPs, including remote and outdoor devices, please refer to Fortinet Wireless Solution Matrix

FortiMail™ Messaging Security Server

	FML-200F	FML-400F	FML-900F	FML-2000E	FML-3000E	FML-3200E
Email Routing* (Msg/Hr)	50,000	250,000	800,000	1.5 Mil	2.5 Mil	3.4 Mil
Performance Enterprise ATP* (Msg/Hr)	30,000	150,000	400,000	700,000	1.5 Mil	2.0 Mil
Email Domains	20	100	800	800	2,000	2,000
Server Mode Mailboxes	150	400	1,500	1,500	3,000	3,000
Storage Capacity	1x 1 TB	2x 1 TB	2x 2 TB (8 TB Max)	2x 2 TB (16 TB Max)	2x 2 TB (12 TB Max)	2x 2 TB (20 TB Max)
FortiGuard Subscription Based Security Service Options: AV, Virus Outbreak Protection, Dynamic Adult Image Analysis and Anti-spam						

* Measured based on 100KB message size, no queuing.

Virtual appliances are also available, please refer to www.fortinet.com for more information

FortiWeb™ Web Application Firewall

	FWB-100D	FWB-400E	FWB-600E	FWB-1000E	FWB-2000E	FWB-3000E	FWB-3010E	FWB-4000E
Throughput (HTTP)	25 Mbps	250 Mbps	750 Mbps	1 Gbps	2 Gbps	5 Gbps	5 Gbps	20 Gbps
Total Interfaces	4x GE RJ45	4x GE RJ45 4x GE SFP	2 (+2 bypass) x GE RJ45, 4x GE SFP	2 (+4 bypass) GE RJ45, 4x SFP GE, 2x 10GE SFP+	2x 10GE SFP+, 8x GE RJ45 Bypass, 4x GE SFP	4x 10GE SFP+, 4x GE RJ45, 4x GE RJ45 Bypass, 4x GE SFP	2 (+ 2 bypass) x 10GE SFP+, 8 x GE RJ45 Bypass, 4x GE SFP	2 (+ 2 bypass) x 10GE SFP+, 8 x GE RJ45 Bypass, 4x GE SFP
FortiGuard Subscription Based Security Service Options: WAF, AV, IP Reputation, and Credential Stuffing Defence								

Virtual appliances are also available, please refer to www.fortinet.com for more information



BMA networks

GORDION®

indasys
connectivity

VINTIN 
make IT unique

IT-Union GmbH & Co. KG

BUSINESS IT-SOLUTIONS

www.it-union.eu

KIEL — HAMBURG — KÖLN — FULDA — SCHWEINFURT — STUTTGART — MALTERS (CH)