FORTINET

Productguide

Real Time Network Protection

2014|2015

- Next Generation Firewalling
- UTM-Appliances
- E-Mail Security
- Web Application und Web Server Security
- Cloud Security
- Virtualisierung und Security

Oberberg Online

Inhalt

Das ist Fortinet

HISTORIE

Fortinet wurde im Jahre 2000 von Ken und Michael Xie gegründet - mit der Vision, Echtzeit-Sicherheitslösungen für Netzwerke zu entwickeln. Bereits 2002 wurden die ersten Produkte der bis heute überaus erfolgreichen FortiGate-Serie auf den Markt gebracht. Heute betreut Fortinet weltweit weit über 100.000 Kunden mit ca. 1.500 Mitarbeitern und ca. 8.000 Vertriebspartnern. Fortinet wird von führenden Marktanalysten wie Gartner als Unternehmen mit dem höchstem Potenzial angesehen und kann sich seit vielen Jahren als Nr. 1 im UTM-Security-Markt bezeichnen (Quelle: IDC).

PORTFOLIO

Fortinet entwickelt Multi-Threat-Sicherheitssysteme für Unternehmen aller Größenordnungen, Rechenzentrumsbetreiber, Carrier und Service-Provider. Die Lösungen beinhalten Sicherheits-Module wie Firewall, VPN (IPsec und SSL), Antivirus, Intrusion Prevention, URL-Filter, Applikationskontrolle, Bandbreitenmanagement, Data Loss Prevention, WAN-Optimierung, Anti-Spyware, Anti-Spam uvm. Mit dieser Kombination aus verschiedenen Engines, die äußerst flexibel in beliebiger Kombination, einzeln oder auch virtualisiert implementiert werden können, schützen die Appliances vor bekannten Bedrohungen ebenso wie vor bisher nicht analysierten, versteckten Angriffen. Speziell entwickelte ASICs (anwendungsspezifische Prozessoren) beschleunigen gezielt einzelne Prozesse und garantieren so Security in Echtzeit.

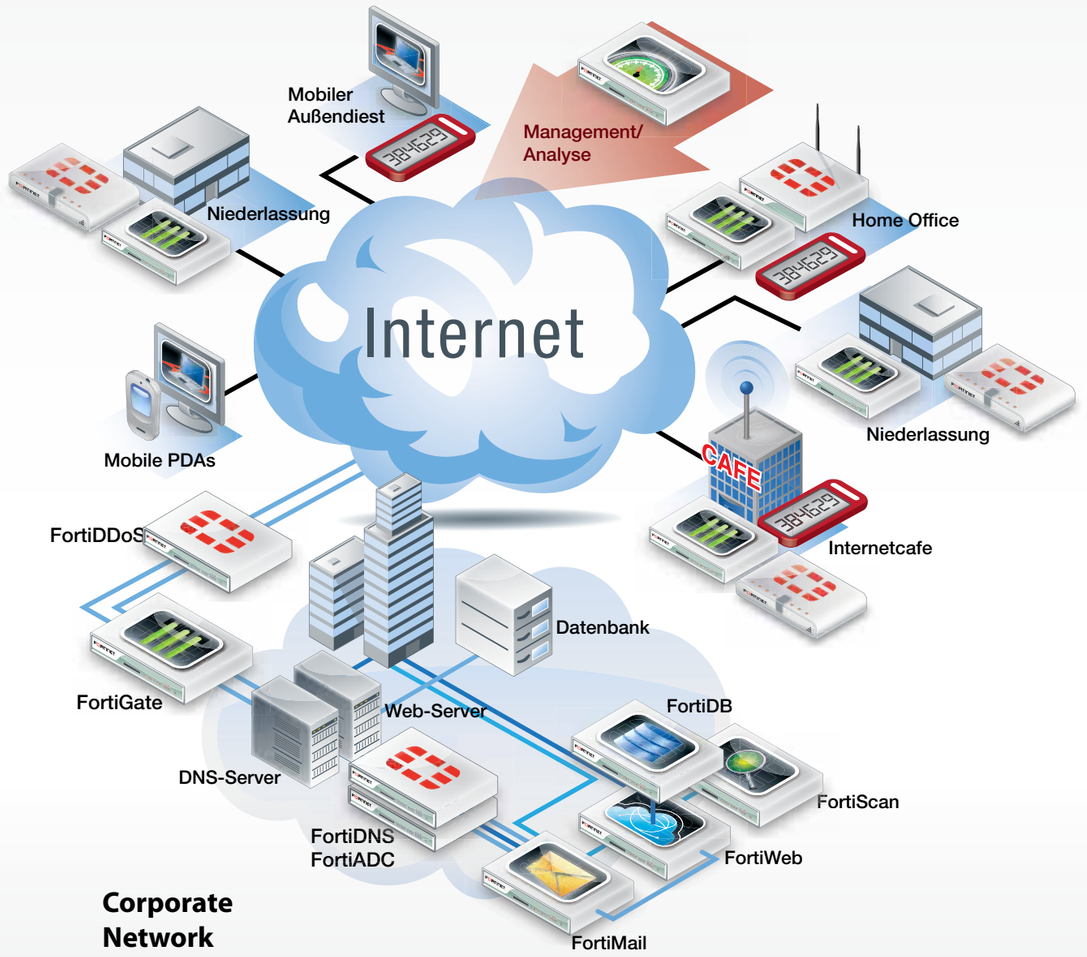
Alle FortiGate Appliances basieren auf dem leistungsfähigen und spezialisierten Security-Betriebssystem FortiOS, einer Fortinet-eigenen Entwicklung. Dieses Betriebssystem ist modular und somit kontinuierlich und im Rahmen normaler Software-Updates erweiterbar. Neben den FortiGate Appliances bietet Fortinet auch E-Mail-AntiSpam/AntiVirus-Lösungen (FortiMail), Endpoint-Security (FortiClient), voll integriertes zentralisiertes Management, Erfassung und Reporting (FortiManager und FortiAnalyzer). FortiDB ist für die Datenbanksicherheit verantwortlich und mit FortiWeb werden Webapplikationen und Webserver effizient geschützt. Mit FortiAuthenticator besteht die Möglichkeit der zentralen 2-Faktor-Authentifizierung, FortiScan bietet Vulnerability und Patch Management und unterstützt Unternehmen beim Erfüllen von Compliancevorgaben.

FortiBalancer und FortiCache optimieren die Lastverteilung über Webserver und in Content Delivery Netzwerken (CDN). Flexible und hochsichere WLAN-Umgebungen können mit den Thin Access Points FortiAP und den in die FortiGate Serie integrierten WLAN-Controllern realisiert werden. FortiGuard Subscription Dienste werden von einem weltweit operierenden Team aus Security-Spezialisten entwickelt und aktualisiert und gewährleisten, dass Updates als Reaktion auf aktuelle und künftige Sicherheitsbedrohungen in Echtzeit zur Verfügung stehen.

Ken Xie, Gründer und CEO von Fortinet

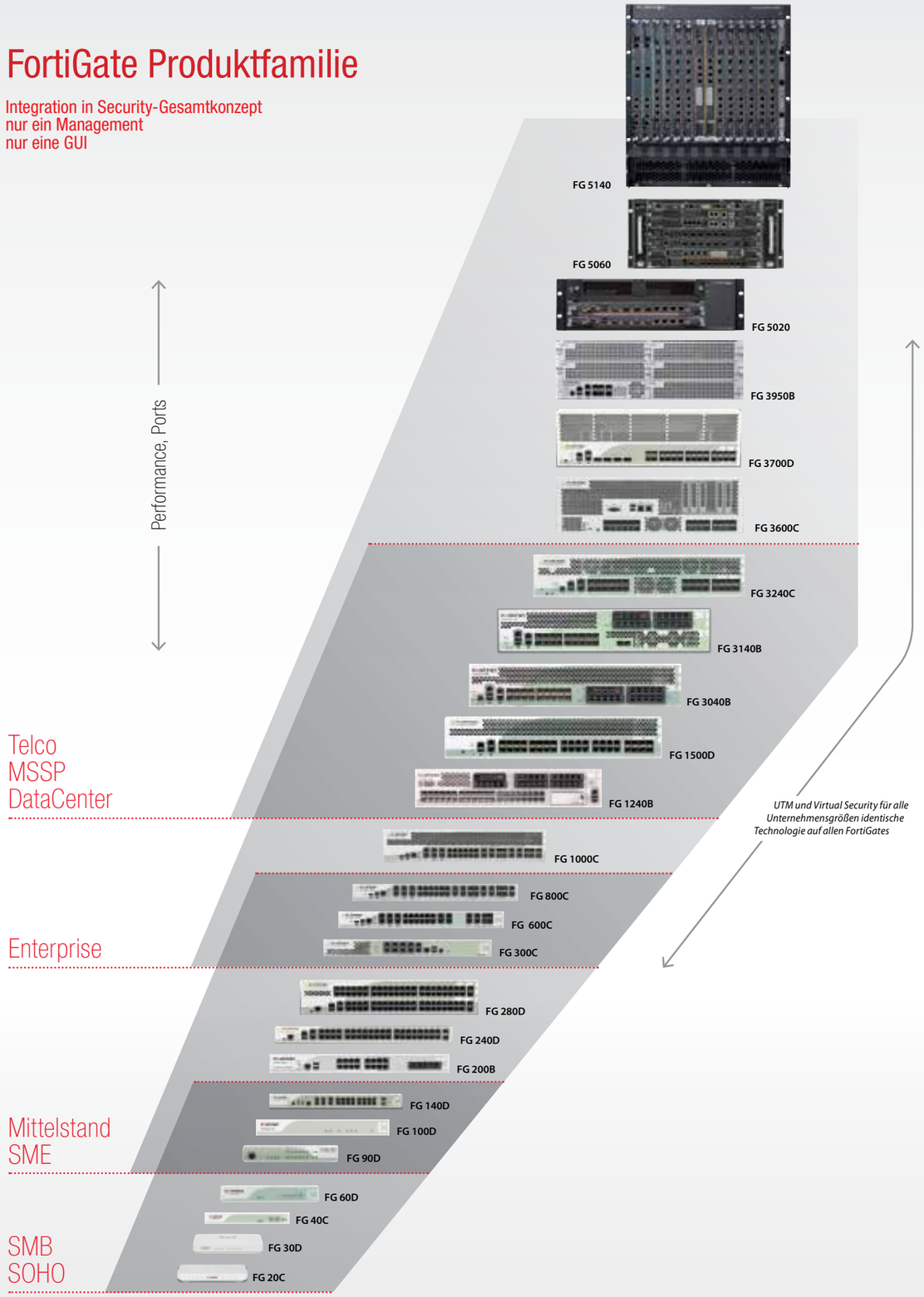
Das Konzept

Die Flexibilität der verschiedenen Fortinet-Lösungen und der ausschließliche Fokus auf IT-Sicherheit ermöglichen Unternehmen aller Größenordnungen die Implementierung durchgängiger, höchst leistungsfähiger und kostenoptimierter Security-Infrastrukturen. End-to-End-Security wird mit Fortinet-Produkte unkompliziert und kostengünstig realisierbar - in einzelnen, überschaubaren Projekt-Etappen, oder durch eine vollständige Migration mit vielen auf umfangreiche Rollouts abgestimmten Tools. Das Schaubild verdeutlicht die unterschiedlichen Einsatzmöglichkeiten, die von hochkomplexen Rechenzentren mit oder ohne Managed Services über kleine und große Unternehmens-Filialen, Home-Office-Absicherung, Mobile Security bis hin zu Remote-Access-Lösungen, Mail-Absicherung und Schutz von Web-Anwendungen reichen, um nur einige wenige zu nennen.



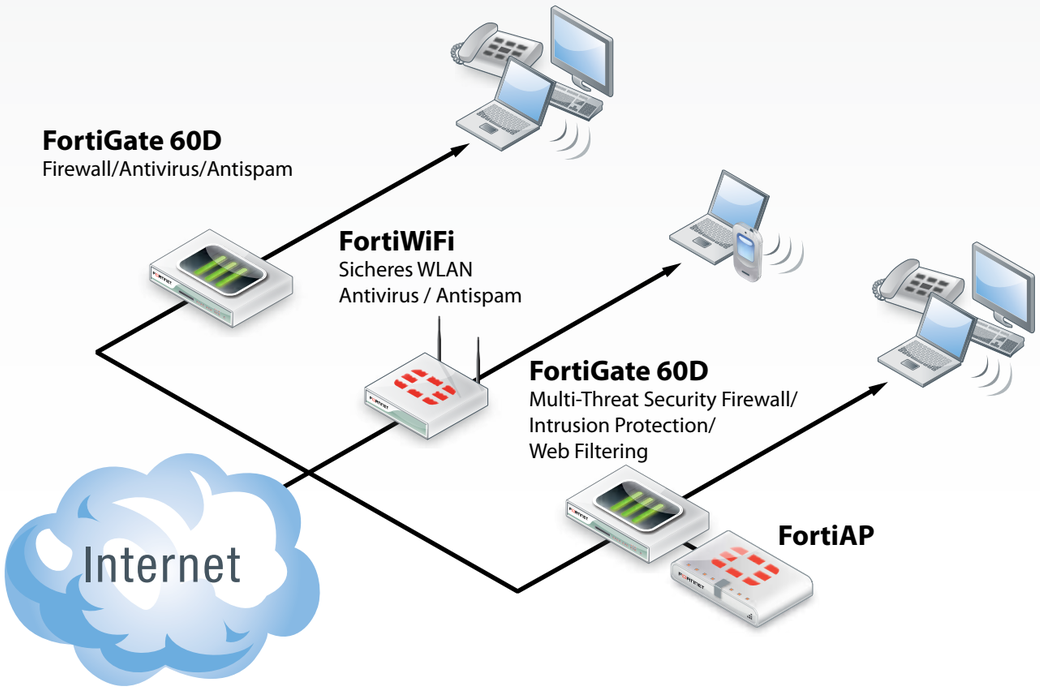
FortiGate Produktfamilie

Integration in Security-Gesamtkonzept
nur ein Management
nur eine GUI



Fortinet für KMU und Mittelstand

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



Fortinet in Enterprise-Umgebungen

Große Unternehmen sehen sich zunehmend komplexen Bedrohungen ausgesetzt. Die ständig wachsende Zahl von heterogenen Endgeräten, der rasante Anstieg der im Unternehmen eingesetzten Anwendungen, Virtualisierung und Cloud Computing, die Nutzung von privaten Endgeräten im Unternehmen (bring your own device / BYOD), Social Media, Streaming Applikationen, Konsolidierungsbestrebungen und Kostendruck, die Bereitstellung von Services von überall und zu jeder Zeit, gesetzliche oder branchenspezifische Auflagen - dies sind nur einige der Themen, die Security in Unternehmen zu einer täglich komplexer werdenden Herausforderung machen. FortiGate Appliances bieten einen konsolidierten, kostenoptimierten und zugleich höchst leistungsfähigen Lösungsansatz. Die Integration verschiedenster Security-Module, eine durchgängige Produktpalette für das zentrale Rechenzentrum bis hin zum Home Office und den mobilen Anwender, zentrales Management auch für viele 1000 Systeme, eine einheitliche Benutzerführung sowie gleicher Funktionsumfang auf allen Plattformen sind nur einige der Besonderheiten, die diese Produktlinie zur bevorzugten Sicherheitslösung zahlreicher weltweit agierende Konzerne gemacht hat. So verlassen sich große Carrier, Service Provider, Rechenzentrumsbetreiber und ein Großteil der Fortune500-Unternehmen auf Fortinet-Sicherheit.

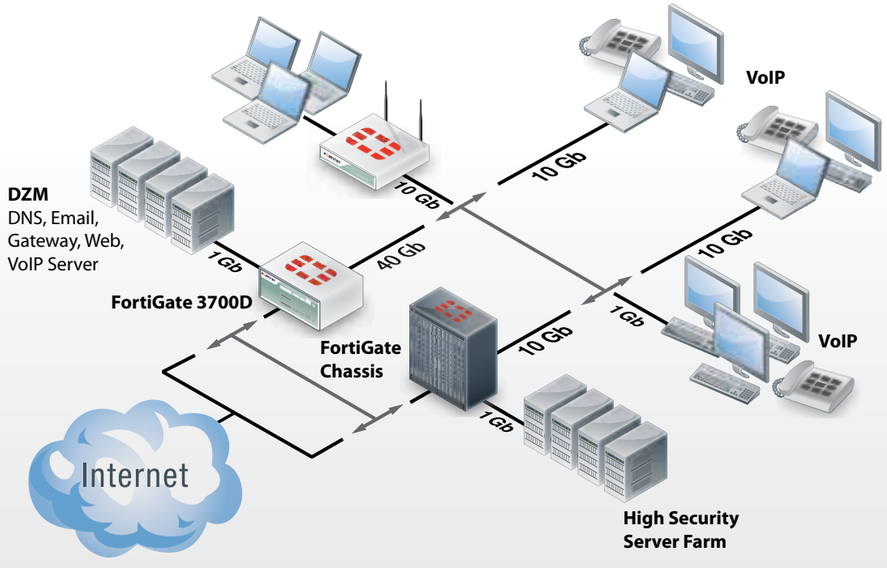
Fortinet FortiGate-Systeme bieten Unternehmen auf Enterprise-Level die folgenden Vorteile:

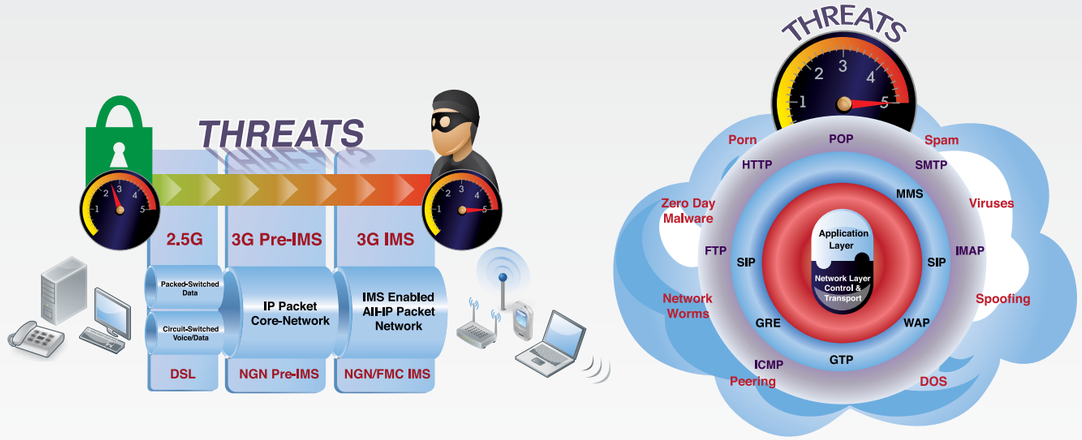
- *Führende, von den ICSA-Labs zertifizierte Funktionalität für Unternehmensnetze jeder Größe, gleich ob drahtgebunden oder drahtlos, in Kombination mit Multi-Gigabit-Durchsatz für Antivirus-Gateways, IPS, VPN und Firewalls uvm.*
- *TransparenterFunktionsmodus, der die Fortinet-Sicherheitstechnik nahtlos mit existierenden Security-Produkten im Unternehmen zusammenarbeiten lässt*
- *Eine Auswahl führender Sicherheitsfeatures für Netzwerke, beschleunigt durch FortiASICs und durch die zum Patent angemeldete CPRL-Technologie*
- *Ein skalierbares Sicherheitssystem, verwaltet über ein einheitliches Management-Interface für Unternehmen jeder Größe*
- *User-unabhängiges Lizenzierungsmodell*
- *FortiGuard Subscription Services für Applikationskontrolle, Antivirus, IPS, Web-Filter, Schwachstellenmangement und Antispam bieten Updates in Echtzeit und den branchenweit besten Netzwerkschutz*

Die Kernvorteile der Fortinet Security Solution Suite:

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

SECURED CORPORATE NETWORK





Fortinet für Carrier

Sicherheit für Pre-IMS- und IMS-Infrastrukturen

REVOLUTION DER SERVICES – EVOLUTION DER NETZWERKE

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

FORTINET SECURITY SOLUTION SUITE

Es ist eine extrem komplexe Aufgabe, IP-Infrastrukturen zu sichern. Sicherheitsbedrohungen sind nicht statisch. Erfolgreicher Schutz setzt eine lückenlose Sammlung von Werkzeugen voraus, mit der sich bekannte Bedrohungen ausschalten und unbekannte Cyber-Angriffe bekämpfen lassen. Die Tools müssen außerdem revisionssichere Informationen in Echtzeit liefern und in der Lage sein, für zukünftige Herausforderungen zu skalieren und sich weiter zu entwickeln. Fortinet stellt eine komplette Suite an Sicherheitslösungen für Carrier zur Verfügung. Die Produkte basieren auf netzwerk- und anwendungsorientierten ASIC-Security-Echtzeit-Engines, die durch Software-Module für spezifische Schutzanforderungen ergänzt werden. FortiCarrier konsolidiert auf einer Plattform neun Sicherheitsfunktionen und ist derzeit das einzige, vollständig virtualisierte Angebot. Mit FortiGate adressiert der Marktführer für Unified Threat Management die Sicherheitsaspekte dreier Trends – Netzkonvergenz bei Daten, Sprache, Video und Mobile Content, Sicherheitsrisiken in der Mobilfunkkommunikation, sowie Security-as-a-Service – und erleichtert Carriern und Service Providern die Einführung Cloud-basierter Security Services.

Mit FortiCarrier können Kunden bei den Investitions- und Betriebskosten für die Sicherheit ihrer Netzwerke sparen und zudem das Geschäftsmodell der Managed Security Services einführen. Die aktuellen Modelle FortiCarrier-3810A und FortiCarrier-5001A-DW integrieren das Betriebssystem FortiCarrier 5.0, das mit spezifischen Funktionen auf den Bedarf von Service Providern zugeschnitten ist.

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

END-TO-END SECURITY

Unübertroffene Performance und umfangreicher Schutz

FortiGate

Die schnellste Firewall der Welt

Next Generation Firewalling (NGFW) und
Unified Threat Management (UTM)

FortiGate Serie

FortiGate

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 Bedrohungen durch Viren, Würmer, Exploits, Spyware oder neuartigen sog. Blended 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 Firewall sind fest integrierter Bestandteil aller FortiGate Appliances.

Bedrohungsszenarien richten sich nicht nach Unternehmensgrößen, und so bieten alle FortiGate Appliances nahezu denselben Funktionsumfang und dieselbe Bedienung per grafischer Oberfläche oder CLI (command line Interface). Die User-unabhängige Lizenzierung aller Module vereinfacht das Netzwerk-Design, ermöglicht Kostentransparenz und den flexiblen Einsatz der Produkte.

Auch kleinere Unternehmen profitieren so von Fortinets Erfahrung aus Großprojekten und können so bei sehr gutem Preis-Leistungsverhältnis mit einem hervorragenden Schutz bei außergewöhnlicher Flexibilität Ihre Netzwerke und Daten absichern. FortiGate Funktionen:

- *Endgeräte- und Betriebssystem-Erkennung*
- *Client Reputation*
- *Identity Centric Policies*
- *Firewall*
- *VPN*
- *IPS/IDP*
- *Applikationskontrolle*
- *AntiVirus (Proxy-, Flow- und Cloud-based)*
- *WLAN Controller*
- *URL-Filter*
- *Schwachstellenmanagement*
- *Network Access Control (NAC)*
- *2-Faktor-Authentifizierung*
- *10 virtuelle Instanzen „onboard“*
- *Voice over IP*
- *IPv6-Security*
- *Data Leakage Protection*
- *Bandbreitenmanagement*
- *Layer2&3-Routing*
- *WAN-Optimierung*
- *SSL Inspection*
- *umfangreiches Reporting*
- *Switch-Controller*
- *umfangreicher IPv6-Support*

FortiGate Firewall

DAS HERZSTÜCK DER APPLIANCE

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, 01/2012). Firewall-Regelwerke kontrollieren sämtliche Daten, die eine FortiGate Appliance zu passieren versuchen - zwischen FortiGate-Interfaces, Zonen oder VLAN-Subinterfaces. 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.

MANAGED FIREWALL SERVICE

Managed Security Service Provider (MSSPs) konzentrieren sich vermehrt auf Fortinets branchenführende FortiGate Security Systeme, um eine effiziente und kostengünstige Bereitstellung von integrierten Security-Diensten für Kunden anbieten zu können. Die Flexibilität von Fortinets Security-Zonen und mandantenfähigen Virtual Domains bieten eine perfekte Plattform, auf der ein verwalteter Security-Dienst entwickelt werden kann. In Verbindung mit dem zentralisierten Management von Fortinets FortiManager und dem zentralisierten Reporting Server von Fortinets FortiAnalyzer können MSSPs ihre Instandhaltungs- und Bereitstellungskosten deutlich reduzieren. Eine einzige Benutzeroberfläche für die ebenfalls mandantenfähige Verwaltung, Analyse, Konfiguration und die unkomplizierte Implementierung von Tausenden von FortiGate Systemen tragen weiter zur Kostensenkung bei.

REMOTE ACCESS IN FILIALEN UND HOME OFFICES

Durch höchst einfache Konfiguration, Installations-Wizzards, umfangreichen RollOut-Support und Konvertierungstools sind Fortinet-Appliances ideal für kleine Niederlassungen, Filialisten und Home-Office-Umgebungen geeignet. Auch der Austausch von Geräten in derartigen Umgebungen wird durch einfachste Installation per gesichertem USB-Stick gewährleistet.

FortiGate Firewall Highlights

- *EAL4+ und ICSA-Labs Certified (Enterprise Firewall)*
- *Identity/Application-Based Policy*
- *IPv6 Support (NAT / Transparent mode)*
- *Granulare Per-Policy Protection Profile*
- *NAT, PAT, Transparent (Bridge)*
- *Routing Mode (RIP, OSPF, BGP, Multicast)*

Weitere Features

- *Policy-Based NAT*
- *Virtual Domains (NAT/Transparent mode)*
- *VLAN Tagging (802.1Q)*
- *Group-based Authentication & Scheduling*
- *SIP/H.323 /SCCP NAT Traversal*
- *WINS Support*
- *Explicit Proxy Support (Citrix/TS etc.)*
- *VoIP Security (SIP Firewall / RTP Pinholing)*
- *Vulnerability Management*

FortiGate VPN

Virtual Private Networks (VPN) ermöglichen die sichere, verschlüsselte Verbindung zu privaten Unternehmensnetzwerken und -resourcen. 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 können auf diese Weise auch viele verschiedene Standorte sicher über ein VPN miteinander verbunden werden.

HUB-AND-SPOKE VPN FÜR UNTERNEHMEN

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

SSL ODER IPSEC?

In den vergangen 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 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 Verbindung etabliert wird. Fortinet unterstützt in höchst komfortabler Weise beide Standards und eine Vielzahl von Optionen zur individuellen Konfiguration und Administration. Auf FortiGate-Systemen können IPsec und SSL-VPN-Verbindungen auch gleichzeitig zum Einsatz kommen.

VPN SERVICES FÜR MSSPS

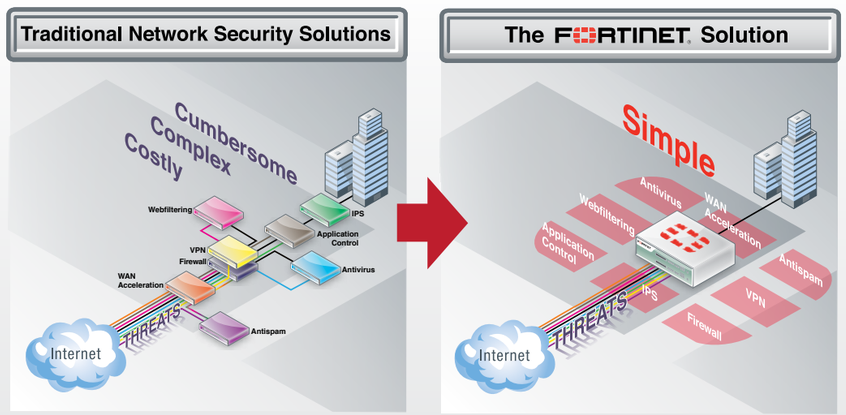
Mit Fortinet können MSSPs einen hochsicheren VPN-Dienst bereitstellen, indem sie die integrierte VPN-Engine mit den übrigen UTM-Modulen verknüpfen. So kann ein- und ausgehender Traffic in Echtzeit auf Malware untersucht und erst dann freigegeben werden, um die Verbreitung von Schadsoftware innerhalb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

- *ICSA Labs Certified (IPSec/SSL-TLS)*
- *PPTP, IPSec, and L2TP + IPSec Support*
- *SSL-VPN Concentrator (incl. iPhone client support)*
- *DES, 3DES, and AES Encryption Support*
- *Automatische IPSec Konfiguration*
- *Hub and Spoke VPN Support*

Weitere Features

- *SHA-1/MD5 Authentifizierung*
- *PPTP, L2TP, VPN Client Pass Through*
- *IKE Certificate Authentifizierung (v1 & v2)*
- *IPSec NAT Traversal*
- *Dead Peer Detection*
- *RSA SecurID Support*
- *SSL Single Sign-On Bookmarks*
- *SSL 2-Faktor Authentifizierung*
- *LDAP Gruppen Authentifizierung (SSL)*



FortiGate IPS

Intrusion Prevention Systeme (IPS) 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) agieren - und sowohl am Netzwerk-Perimeter (Übergang zwischen internem und externem Netzwerk) als auch im internen Netz. 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 und kostengünstig - und auch mandantenfähig - realisiert werden.

HIGH PERFORMANCE DOS-PREVENTION FÜR SERVICE PROVIDER

Der speziell entwickelte SP2-ASIC von Fortinet, der in ausgewählten FortiGate-Modellen integriert ist, stellt zusätzliche Beschleunigung der IPS-Funktionalität direkt am Interface zur Verfügung. Dies gewährleistet insbesondere bei Denial-of-Service-Angriffen eine effiziente Abwehr, ohne die Performance der zentralen Security-Module und damit der gesamten Appliance zu beeinträchtigen.
In modularen FortiGate-Appliances können zu diesem Zweck sog. Security Processing Module nachgerüstet werden, die mit dem neuen SP2-Chip ausgestattet sind. So kann (bei Bedarf auch erst im Nachhinein) die IPS-Performance einer Appliance signifikant gesteigert 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. 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 oder 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 belastet, da jedes angreifende Paket mithilfe einer Firewallregel 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 Firewallregeln greifen. Der DoS-Sensor, der zwölf 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, bieten darüber hinaus weitere Intelligenz zu Erkennung von DoS- und DDoS-Angriffen auf höheren Netzwerkschichten.

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

FortiGate IPS Highlights

- *ICSA Labs Certified (NIPS)*
- *Schutz vor über 3000 Threats*
- *Protokoll Anomalie Support*
- *Support kundenspezifischer Signaturen*
- *Automatische IPS Database Updates*
- *IPv6 Support*
- *Skalierbar von Home Office bis Multi-Gigabit Rechenzentrum IPS*

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 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 ZU 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, 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 Applikationskontrolle Highlights

- *Erkennung und Kontrolle von über 2000 Applikationen*
- *Traffic-Shaping (pro Applikation)*
- *Facebook Applikations- und Kategorie-Kontrolle*
- *Erkennung und Kontrolle einzelner Anwendungs-Services*
- *Einrichtung von Zeitfenstern oder -Konten pro User*
- *Kombination mit anderen integrierten UTM-Modulen (z.B. AV, IPS, URL-Filter, DLP usw.)*
- *Kontrolle weitverbreiteter Anwendungen unabhängig von Port oder Protokoll: Facebook, KaZaa, ICQ, Gnutella, BitTorrent, MySpace, WinNY, Skype, Edonkey*

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 genannten 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 PEFORMANCE 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 Fortinet kontinuierlich unter den Top5 AntiVirus-Anbietern.

FortiGate AntiVirus Highlights

- *ICSA Labs Certified (Gateway Antivirus)*
- *Incl. Antispyware und Worm Prevention*
- *Protokolle: HTTP/HTTPS SMTP/SMTPS, POP3/POP3S IMAP/IMAPS, FTP, viele IM Protokolle*
- *Flow-Based Antivirus Scanning Modus*
- *Automatische "Push" Content Updates*
- *File Quarantäne Support*
- *IPv6 Support*

Weitere Features

- *skalierbare Performance und ASIC-beschleunigt*
- *Prüfung von VPN (IPSec und SSL) Content*
- *bi-direktionales Content Filtering*
- *komprimierter Dateiformat-Support: tar, gzip, rar, lzh, iha, cab, arj, zip, bzip2, upx, msc, fsg, und aspack*
- *zentralisiertes Management und Reporting für Tausende von FortiGate-Systemen*
- *Implementierung in Transparent, NAT und Route-Modus*
- *AV-Datenbanken: Standard, Extended, Extreme, Flow*

FortiGate WebFiltering

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. Flow basierende 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.

Anwendungsbereiche

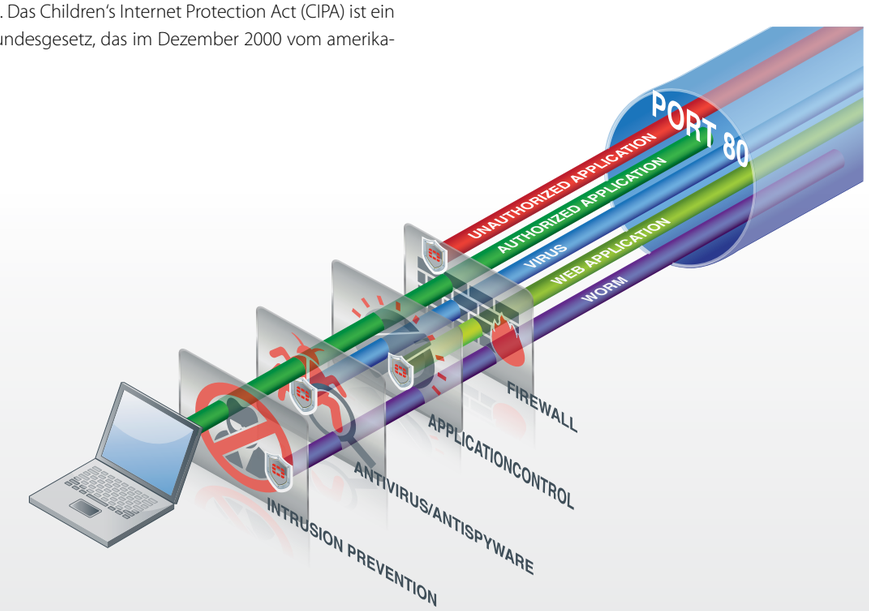
- *Steigerung der Produktivität*
- *Erhöhung der verfügbaren Bandbreite*
- *Verhinderung von Datenverlust oder Veröffentlichung von vertraulichen Informationen über Chat-Seiten, nicht erlaubte und nicht kontrollierte Web-Mail Systeme, Instant Messaging und Peer-2-Peer File Sharing*
- *Reduzierung der Bedrohung durch schädliche Webseiten (Phishing, Pharming, Malware, Spyware, Grayware, Streaming Media uvm.)*
- *Einhaltung rechtlicher Bestimmungen (z.B. Copyright) beim Download von Dateien*

FortiGate WebFilter Highlights

- *76 Content Kategorien*
- *über 2 Milliarden Web Seiten kategorisiert*
- *HTTP/HTTPS Filtering*
- *Kundenspezifisches Black/White-Listing*
- *Web Filtering Time-Based Quota*

Weitere Features

- *URL/Keyword/Phrase Block*
- *URL/Category Exempt blockiert Java Applets, Cookies, Active X*
- *MIME Content Header Filtering*
- *IPv6 Support*
- *Flow-based Web Filtering*



FortiGate Wireless LAN

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.

INTEGRIERTER WLAN CONTROLLER

Die neue 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 authorisierte 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.

FortiGate WLAN Highlights

- *Integrierter WLAN-Controller*
- *Bereitstellung von kundenspezifischen Captive Portals für sichere Anmeldung (auch in Verbindung mit FortiToken) und User-basierende Authentisierung gegen lokale Datenbank*
- *Integriertes öffentliches Zertifikat zur WPA-Enterprise Authentifizierung*
- *Distributed Automatic Radio Resource Provisioning (DARRP)*
- *MAC-Address Whitelisting*
- *Automatische Profilzuweisung*
- *Gastzugang-Management via „Receptionist-GUI"*
- *Wireless Mesh*

Weitere Features

- *Erkennung, Reporting und Unterdrückung von nicht erlaubten Access Points (sog. Rogue APs)*
- *Granulare Endpoint-Kontrolle*
- *Standard-Reports, die für Audits nutzbar sind*
- *Support von 802.11ac, n, g, b, a*
- *Basierend auf 2x2 Multiple-In/Multiple-Out (MIMO) Technologie*
- *Volle Integration in das umfangreiche UTM-Feature-Set einer FortiGate-Appliance*
- *Applikations- und/oder User-abhängiges Bandbreitenmanagement*
- *Spannungsversorgung des FortiAP über das LAN-Kabel (POE-Funktion, nur bei FortiAP 210-Serie)*
- *Indoor- und Outdoor-Access Points verfügbar*
- *Planungshilfe mit FortiPlanner*

FortiGate 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 augrund 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.

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, Resourcen etc.) sind so individuelle Regelwerke möglich, die in Abhängigkeit dieser Rahmenparameter herangezogen werden können.

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

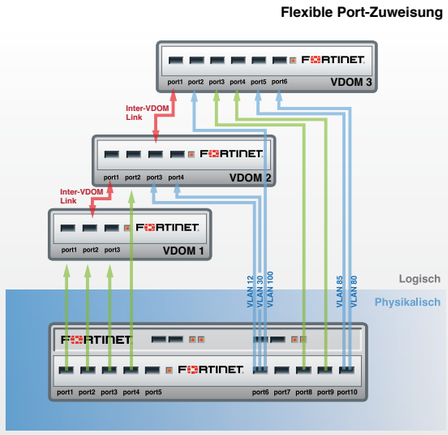
FortiGate und Virtualisierung

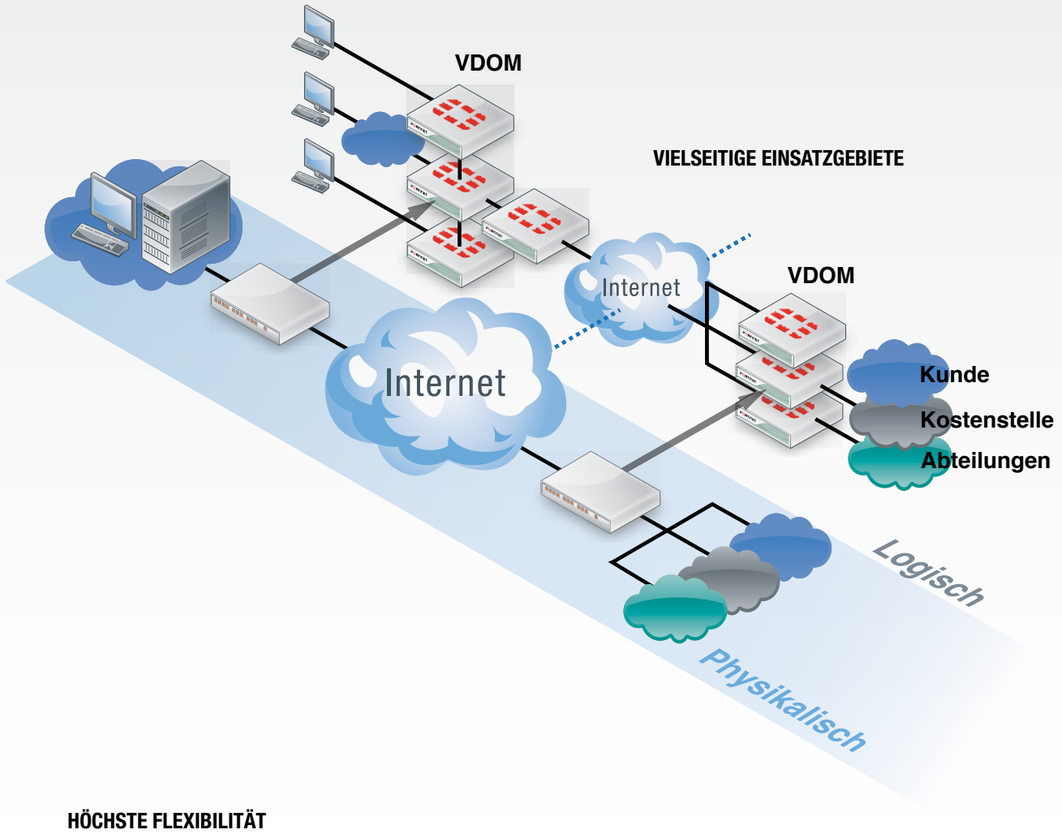
Die Konsolidierung unterschiedlicher IT- Security-Dienste auf einer einzigen Hardware-Plattform kann durch deren Virtualisierung optimal ergänzt werden. So lassen sich Kosten senken, die sonst aufgrund von hohem Platzbedarf, aufwändiger Wartung und Bedienung, komplizierter Verwaltung von Service-Verträgen, Stromverbrauch und mangelhafter Flexibilität entstehen. 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 Modellen bis zur 600er Serie sind 10 VDOMs möglich und ab Werk ohne zusätzliche Kosten vorhanden. Ab der 1000er Serie sind mit zusätzlichen Lizenzen weitere VDOMs pro FortiGate möglich, in den 5000er Chassis-Systemen sind sogar bis zu 250 VDOMs realisierbar. 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. FG50B oder FG60C) ersetzt werden - ein deutlicher Platzvorteil und bis zu 18.000 kWh Stromersparnis pro Jahr.

Flexible Port-Zuweisung





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 Virtual Security Highlights

- *Reduzierung von Platz, Kosten und Stromverbrauch*
- *Auch auf kleinen FortiGate Modellen verfügbar*
- *Maximale Flexibilität durch beliebige Kombination von virtuellen Diensten auf einer Appliance*
- *Individuelle Managed Services in Organisationen oder für MSSPs*
- *Mandantenfähigkeit*
- *Skalierbarkeit*
- *Erweiterbarkeit (ab 1000er Serie)*
- *Large Scale Security Services*

FortiGate 2-Faktor-Authentifizierung und 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 erlangen können. 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-BASIERTE 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 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 Authentifizierung Highlights

- *Flexible Auswahl unterschiedlicher Authentifizierungsmethoden*
- *Integrierte CA*
- *Integrierter Authentifizierungs-Server*
- *2-Faktor-Authentifizierung mittels FortiToken, E-Mail oder SMS*
- *LDAP, RADIUS und TACAS+ Support*
- *X.509 Support*

Weitere Features

- *Windows Active Directory und NTLM und Novel eDirectory Support*
- *Fortinet Single Sign On*
- *Fortinet OneTimePasswort Software für Smartphones*
- *Identity Based Policies*
- *Dynamische User-Profile*
- *Lokale Datenbank*
- *Xauth over RADIUS für IPSEC VPN*
- *RSA SecurID Support*
- *LDAP Group Support*

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, SMPTPS), 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 Data Loss Prevention (DLP) Highlights

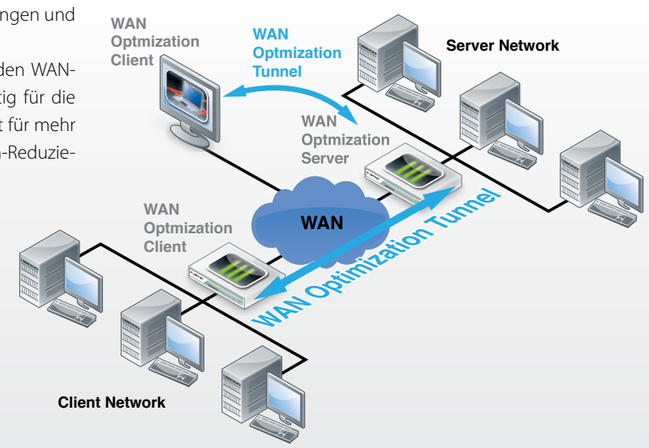
- *Identifizierung und Kontrolle von sensiblen Daten „in Bewegung"*
- *Integrierte Pattern Datenbank*
- *RegEx-based Matching Engine für kundenspezifische Pattern*
- *Konfigurierbare Aktionen (block/log)*
- *Kundenspezifische Pattern*
- *Support von IM, HTTP/ HTTPS uvm.*
- *Unterstützt viele populäre File Typen*
- *Internationaler Zeichensatz wird unterstützt*
- *Document Fingerprinting*
- *Flow-Based DLP Scanning Mode*

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 WAN-Zugriff 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 bereits, die die benötigte Bandbreite drastisch - um bis zu 80% - reduzieren können.

FortiGate WAN Optimierung Highlights

- *Bi-Directional / Gateway to Client/Gateway*
- *Integriertes Caching und Protokoll Optimierung*
- *Beschleunigt CIFS/ FTP/ MAPI/ HTTP/ HTTPS/ Generic TCP*
- *Erfordert FortiGate mit SSD oder Festplatte*



FortiGate Anti Spam

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

FortiGate AntiSpam Highlights

- *SMTP/SMTPS, POP3/POP3S, IMAP/IMAPS Support*
- *Real-Time Blacklist/Open Relay Database Server*
- *MIME Header Check*
- *Keyword/Phrase Filtering*
- *IP Address Blacklist/Exempt List*
- *Automatische Echtzeit-Updates vom FortiGuard Netzwerk*

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 Bandbreiten-Management Highlights

- *Policy-based Bandbreiten-Management*
- *Application-based und Per-IP Bandbreiten-Management*
- *Differentiated Services (DiffServ) Support*
- *Garantierte/ Maximale/ Priorisierte Bandbreite*
- *Bandbreiten-Management Shaping via Accounting oder Quoten*

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 Routing Highlights

- *Multiple WAN Link Support*
- *PPPoE Support*
- *DHCP Client/Server*
- *Policy-Based Routing*
- *Dynamisches Routing für IPv4 (RIP, OSPF, IS-IS, BGP & Multicast Protocols)*
- *Dynamisches Routing für IPv6 (RIP, OSPF, & BGP)*
- *Multi-Zone Support*

Weitere Features

- *Routing zwischen Zonen*
- *Routing zwischen Virtual LANs (VLANs)*
- *Multi-Link Aggregation (802.3ad)*
- *IPv6 Support (Firewall, DNS, Transparent Mode, SIP,Dynamic Routing, Admin Access, Management)*
- *VRRP und Link Failure Control*
- *sFlow Client*

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 Schwachstellen-Management

Mittels der in die meisten FortiGate Appliances integrierten Schwachstellen-Management Option ist es möglich, Server und Workstations im Netzwerk auf Schwachstellen zu scannen. Diese Scans können automatisch oder manuell erfolgen. Die Ergebnisse sind sowohl über die Benutzeroberfläche der FortiGate als auch über einen ins Netzwerk integrierten FortiAnalyzer darstellbar. Dabei kann ein FortiAnalyzer die Ergebnisse vieler FortiGates sammeln und korrelieren.
Für eine Schwachstellen-Analyse werden zunächst die zu scannenden Assets definiert bzw. automatisch erkannt. Anschließend kann basierend auf einer umfangreichen Sammlung von Schwachstellen-Tests ein Netzwerk-Scan durchgeführt werden. Dabei sind auch kundenspezifische Analysen möglich. Die Ergebnisse können im Detail oder nach Kategorie, Priorität, in Abhängigkeit vom Betriebssystem oder nach individuellen Kriterien zusammengefasst dargestellt werden.

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 Videokonferenzen 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 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 VoIP Security Highlights

- *SIP Header Conformance Check (Prüfung einer SIP Nachricht auf Unregelmäßigkeiten)*
- *RTP PIN-Holing*
- *SIP Message Rate Limitation (per Methode)*
- *SIP NAT*
- *IP Address Speicherung*
- *Multiple RTP*

Weitere Features

- *Endpoint Support*
- *SIP Hosted NAT Traversal*
- *SIP HA Failover*
- *Deep SIP Message Inspection (Syntax Check einer SIP Nachricht)*
- *Stateful SIP dialog tracking*
- *Stateful SCTP Firewall*
- *Hochverfügbarkeits-Funktionen (HA)*
- *Geographische Redundanz*
- *Umfassendes Logging und Reporting*

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 effzienter 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 Infrastrutkur 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 IPv6-Security Highlights

- *Statisches und dynamisches Routing (RIPv6, BGP4+, and OSPFv3)*
- *DNS*
- *Network Interface Addressing*
- *Routing access lists und Prefix Lists*
- *IPv6 tunnel over IPv4, IPv4 tunnel over IPv6*
- *Security Policies*
- *Authentifizierung*

Weitere Features

- *IPv6 over SCTP*
- *Packet und Network Sniffing*
- *IPsec VPN*
- *SSL VPNs*
- *UTM Security*
- *NAT/Route und Transparent Mode*
- *Logging und Reporting*
- *SNMP*
- *Virtual IPs und Gruppen*
- *IPv6 spezifisches Troubleshooting wie z.B. „ping6"*

WLAN Access Points FortiAP

SICHERE WLAN INFRASTRUKTUR

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 FG50x) 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 authorisierte 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 FG50x) ab FortiOS 4.1. über diese Wireless-Controller Funktionalität verfügt, können bereits bestehende Gateways durch ein einfaches Betriebssystem-Update um dieses Feature erweitert werden – die Anschaffung einer zusätzlichen Plattform mit einer eigenen Administrations-Oberfläche entfällt.

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

Die Thin WLAN Access Point Serie FortiAP umfasst Modelle für jeden Anwendungsbereich, sowohl Indoor als auch Outdoor.

Zu den weiteren Eigenschaften dieser Produktlinie gehören:

- *Erkennung und Reporting von nicht erlaubten Access Points (sog. Rogue APs)*
- *Mobile Access Points*
- *Granulare Endpoint-Kontrolle*
- *Standard-Reports, die für Audits nutzbar sind*
- *802.11n Support (parallel zu a/b/g) basierend auf 2x2 Multiple-In/Multiple-Out (MIMO) Technologie*
- *Einrichtung kundenspezifischer Captive Portals (LogIn-Seiten) mit 2-Faktor (Token) Support*
- *Volle Integration in das umfangreiche UTM-Feature-Set einer FortiGate-Appliance*
- *Spannungsversorgung des FortiAP über das LAN-Kabel möglich (PoE)*
- *Automatic Radio Resource Provisioning (ARRP) für optimierten Durchsatz*
- *Receptionist GUI für die Vergabe von WLAN Vouchers (ab FOS 4.3. special built)*
- *Integration in FortiManager und FortiAnalyzer für zentrales Management und Reporting*
- *FortiPlanner Software für einfache Planung von WLAN-Infrastrukturen*
- *Wireless Mesh*
- *Local Breakout*
- *Access Point Load Balancing*
- *Kostenlose FortiPlanner Planungs-Software*

FortiAP Highlights

- *Kostengünstige Indoor- und Outdoor Lösungen*
- *Zentrales Management über FortiGate oder FortiWiFi WLAN-Controller*
- *Rogue-Access Point Erkennung und Unterdrückung*
- *Gleichzeitiges Security-Monitoring und Client-Services-Bereitstellung*
- *Gast-Management mit Voucher-Druck*
- *Fast Roaming*

Weitere Features

- *PCI DSS Compliance Support*
- *Layer 7 (Application) Qualtiy of Service Optionen*
- *PoE-fähig*
- *ARRP Support*
- *Integration in FortiManager und FortiAnalyzer*

FortiAP Produktfamilie

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 authorisierte 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

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 starkt vereinfacht.

FORTITOKEN 300

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 Fortinet-Token-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 beispielweise für Admin-Accounts.

FortiToken Highlights

- *Geringe Anschaffungskosten*
- *Lebenslange Lizenz*
- *Skalierbar*
- *Nutzung vorhandener FortiGate-Systeme als Authentifizierung-Server*
- *Vereinfachtes Management durch zentrale Token-Verwaltung in FortiGuard*
- *Integration in FortiClient*
- *Robustes Gehäuse*
- *Manipulationsicher*

FortiAuthenticator

ZENTRALER AAA-SERVER

Der FortiAuthenticator dient als zentrale Instanz für das User Identity Management. Es werden 2-Faktor-Authentifizierung, Identitäts-Verifikation und Netzwerkzugriffskontrolle (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 SINGLES SIGN ON (FSSO)

Fortinet Singles 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.

FortiAuthenticator Highlights

- *Zentrales Management von Nutzerinformationen*
- *Vereinfachung von Authentifizierung-Prozess*
- *Zusätzliche Flexibilität für FortiToken Anwendungen*
- *Erhöhte Sicherheit durch 2-Faktor-Authentifizierung*
- *3rd Party Integration via RADIUS und LDAP*

Weitere Features

- *FortiGate identitätsbasierende Regelwerke Integration in Active Directory*
- *Erweitertes Fortinet Single Sing On (FSSO)*
- *Self-Provisioning Portal*
- *Lokales webbasierendes Management-Interface*
- *Command Line Management-Interface (CLI)*
- *Zentrales Management, Analyse und Report via FortiManager und FortiAnalyzer*

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 Highlights*

- *Integrierter VPN-Client (SSL und IPsec)*
- *Applikationskontrolle*
- *AntiVirus*
- *Web Filter*
- *WAN-Optimierung*
- *Schwachstellenmanagement*
- *Umfangreicher OS Support (Windows, MacOS, iOS, Android)*
- *Client Zertifikat Support*
- *Zentrales Mangement*
- *Zentrales Endpoint Logging*
- *Konfigurations-Bereitstellung*
- *Policy Compliance Enforcement*
- *Windows AD SSO Agent*

**Je nach Betriebssystem und Lizenzierung sind nicht alle Features verfügbar.*

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 administrieren. 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.

FortiSandbox

Mithilfe der leistungsstarken Sicherheits-Appliance 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 Verteidigunslinie – 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 ebenso verdächtige oder High-Risk-Dateien in E-Mails identifizieren und sie zur weiteren Untersuchung an die FortiSandbox weiterleiten.

DIE FORTISANDBOX AUF EINEN BLICK:

Die FortiSandbox-3000D lässt sich standalone in vorhandene Netzwerke integrieren, ohne weitere Konfigurationen ändern zu müssen. Alternativ ermöglicht die Lösung eine Ergänzung von Fortinets FortiGate- und FortiMail-Plattformen, um deren Erkennungsmechanismen weiter zur 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.

Die wichtigsten Funktionen der FortiSandbox:

- *Dynamische Antimalware- und Updates-/Cloud-Abfrage: Erhält Updates von FortiGuard Labs und kann Anfragen in Echtzeit dorthin zurücksenden. Hierdurch lassen sich bereits vorhandene und auch zukünftige Bedrohungen sofort und intelligent aufdecken.*
- *Code-Emulation: Bietet verschlankte Sandbox-Inspektion in Echtzeit. Erkannt wird hierbei auch Malware, die Sandboxen gezielt umgeht oder die sich nur mit speziellen Software-Versionen ausführen lässt.*
- *Vollständige virtuelle Umgebung: Stellt ein in sich geschlossenes Laufzeitumfeld zur Verfügung, um Risiken oder verdächtigen Code zu analysieren und dessen gesamten Lebenszyklus zu untersuchen.*
- *Verbesserter Überblick: Ermöglicht umfassende Einsicht in zahlreiche Netzwerk-, System- und Dateiaktivitäten kategorisiert nach Risiko, um so die Reaktionszeiten bei Sicherheitsvorfällen zu verkürzen.*
- *Callback-Ermittlung: Überprüft Netzwerk-Traffic auf Anfragen für den Besuch manipulierter Seiten, die Kommunikation mit C&C-Servern und andere Aktivitäten, die auf eine Gefährdung hinweisen.*
- *Manuelle Analyse: Ermöglicht es Sicherheitsadministratoren, Malware-Samples manuell und ohne gesonderte Appliance hochzuladen, um virtuelles Sandboxing durchzuführen.*
- *Optionale Übermittlung an FortiGuard: Tracer-Berichte, kompromittierte Dateien und andere Informationen lassen sich an FortiGuard Labs übermitteln, um von dort Handlungsempfehlungen sowie Inline-Updates zu erhalten.*

EMAIL SECURITY

Effektiver Schutz vor E-Mail-Viren und SPAM

FortiMail

Eine der schnellsten und leistungsfähigsten Appliance-Serien für Messaging-Security

User-unabhängige Lizenzierung, High-Speed, granulare Konfiguration, Schutz auch vor ausgehendem SPAM, 3 Betriebsmodi, auch als Mail-Server verwendbar

FortiMail

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. Insbesondere 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 IDENTIY BASED ENCRYPTION (NUTZER-ABHÄNGIGE 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.

FortiMail Highlights

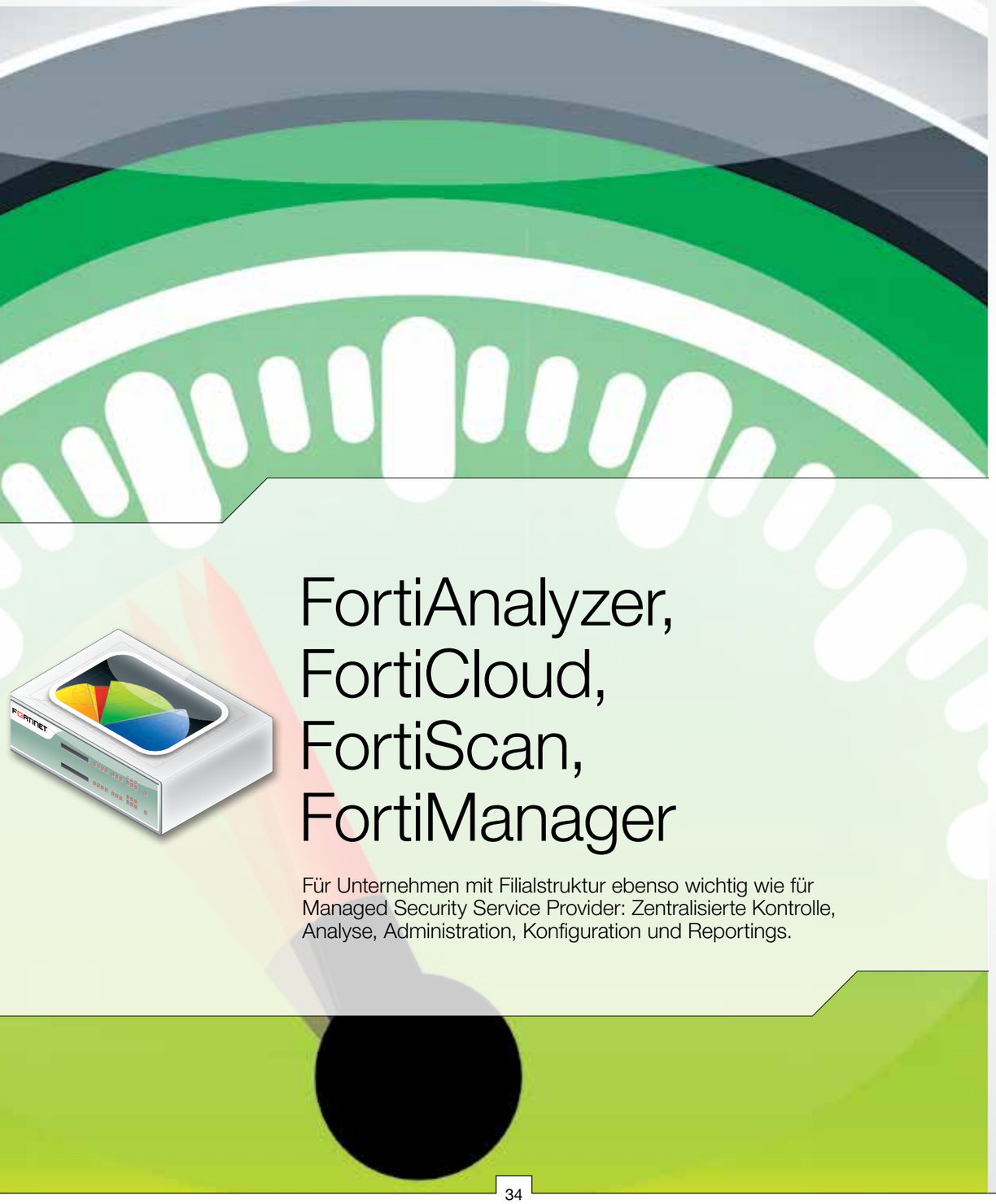
- *Multiple Email Domain Support*
- *High Availability (HA) Support*
- *SMTP Mail Gateway für bestehende Email Server*
- *Integriertes Policy-Based Email Routing und Queue Management*
- *Outbound Mail Relay für verbesserte Mail Security*
- *Granular Layered Detection Policies für Spam, Viren, Adressen, IP Adressen oder Domains*
- *Per User Antivirus und Antispam Scanning mittels LDAP Attributen auf Per Policy (Domain) Basis*

Weitere Features

- *LDAP-Based Email Routing*
- *Quarantined Message Access mit WebMail and POP3*
- *Tägliche Quarantäne Berichte*
- *Policy-Based Archiving von Inbound und Outbound Nachrichten mit Backup Support für Remote Storage*
- *Mail Queue Support für verzögerte und unzustellbare E-Mails*
- *SMTP Authentication Support via LDAP, RADIUS, POP3 or IMAP*
- *Per User Automatic White List*
- *SNMP Support*
- *Local Sender Reputation*
- *Dynamic DNS (DDNS)*
- *Greylist Database Persistence*
- *Sender Policy Framework (SPF)*
- *DomainKeys*
- *DomainKeys Identified Mail (DKIM)*
- *Fragmented Message Blocking*
- *Integration in FortiManager & FortiAnalyzer*
- *uvm.*

ZENTRALES MANAGEMENT & REPORTING

Völlige Kontrolle über das Unternehmens-Netzwerk



FortiAnalyzer, FortiCloud, FortiScan, FortiManager

Für Unternehmen mit Filialstruktur ebenso wichtig wie für Managed Security Service Provider: Zentralisierte Kontrolle, Analyse, Administration, Konfiguration und Reportings.

FortiAnalyzer

ZENTRALISIERTES REPORTING

Die FortiAnalyzer-Produktfamilie bietet Echtzeit-Netzwerk-Logging-, Analyse- und Reporting-Funktionen in Form einer Appliance, die auf sichere Weise Log-Daten von Fortinet-Geräten und auch von Produkten anderer Hersteller zusammenführen. Sämtliche Informationen über Traffic, Events, Viren, Angriffe, Web-Inhalte und E-Mail-Daten können archiviert und 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 kundenspezifischen 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.

FortiAnalyzer Highlights

- *Log Analyse & Reporting*
- *Über 300 voreingestellte Reports*
- *Kundenspezifisches Reporting*
- *Mandantenfähigkeit*
- *NetzwerkAnalyse*
- *Zentrale Quarantäne*
- *DLP Archivierung*
- *Forensische Analsye*
- *Real-Time-Log-Viewer*
- *Schwachstellen- und Compliance-Management*
- *Graphisches Reporting*
- *Granulare Informationen über das Netzwerk*
- *3rd-Party Integration*
- *Integration in FortiManager*
- *Uvm.*

FortiAnalyzer

FortiCloud

Mit FortiCloud stellt Fortinet einen gehosteten Security-Management- und Log-Analyse-Service zur Verfügung, der FortiGate und FortiWifi Appliances unterstützt. FortiCloud bietet zentrales Reporting, Traffic-Analyse, Konfigurations-Management sowie Log-Speicherung ohne die Notwendigkeit zusätzlicher Hard- und Software.

Durch einfaches Hinzufügen über einen kostenlosen Account können FortiGate-Appliances auf diese Weise einfach administriert und ausgewertet werden. Bei einem größeren Speicherbedarf als 1GB pro Appliance kann der jeweilige Geräte-Account individuell und kostengünstig um weitere Kapazität (200GB) ergänzt werden. Gespeichert werden können Traffic-Verlauf, System Events sowie Web-, Applikations- und Security-Events.

FORTICLOUD BESTANDTEILE

DASHBOARD
System- und Log-Widgets inkl. Echtzeit-Monitor

LOG VIEWER
Echtzeit Log-Übersicht mit Filtern auf alle kritischen Vorkommnisse oder unklare Ereignisse

DRILLDOWN ANALYSIS
User- und Netzwerk-Aktivitäts-Analysen zur granularen Visualisierung aller Aktionen

REPORT GENERATOR
Erstellung von kundenspezifischen oder vorkonfigurierten Reports in verschiedenen Formaten (inkl. PDF), um z.B. Compliance nachzuweisen oder bestimmte Netzwerk-Verhaltensweisen zu dokumentieren.

DEVICE MANAGEMENT
Management von Software Updates und Standardisierung über das gesamte Netzwerk

Highlights

- *Einfaches zentrales Management*
- *Verkehrs- und Applikations-Visualisierung*
- *Sichere, gehostete Log-Speicherung*
- *Echtzeit-Monitoring und -Alarmierung*
- *Kundenspezifisches oder vorkonfiguriertes Reporting*
- *Verkehrsanalyse*
- *Konfigurations-Management*
- *konsistente Backups und Upgrades*
- *Jahreslizenz pro 200G-Speicherpaket – keine weitere Kosten für Service etc.*

FortiScan

FortiScan
Vulnerability Management

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

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

FortiManager

FortiManager

ZENTRALISIERTES MANAGEMENT VON FORTINET-SECURED NETZWERKEN
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, dass 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 (Adminitrative 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 AddOns können übergreifende Regelwerke und globale Datenbanken, die für alle FortiOS im System zur Verfügung stehen, erstellt werden.

LOKALES SECURITY CONTENT HOSTING
Die Optionen, 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 WorkFlow 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.

FortiManager Highlights

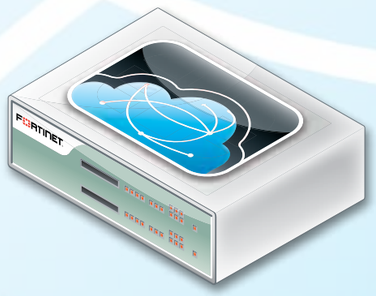
- *Zentrales Update-und Konfiguration-Management*
- *Support von vielen tausend Geräten und Clients*
- *Hierarchische Objektdatenbank*
- *Automatisiertes Provisioning*
- *Rollen-basierte Administration*
- *Web-Portal SDK*

Weitere Features

- *XML API*
- *Integration mit FortiAnalyzer*
- *Automatische Geräteerkennung*
- *zentrales Management komplexer VPN-Netzwerke*
- *Netzwerk-und Security-Monitoring*
- *Support von FortiGate, FortiClient, FortiMail, FortiSwitch, FortiAuthenticator und FortiAnalyzer Lösungen*

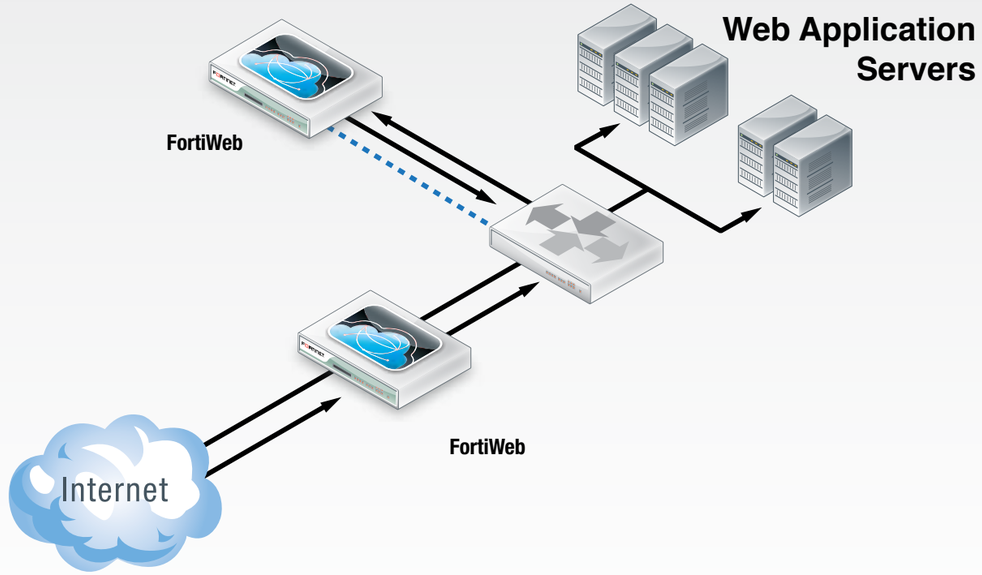
APPLICATION SECURITY

Schutz von Web-Applikationen, DNS-Servern, Datenbanken und DDoS-Abwehr



FortiWeb, FortiDDoS FortiDNS, FortiDB

Effektiver Schutz von Web-Anwendungen wie Portalen und Shops, Load Balancing und Beschleunigung von Transaktionen, Schutz von Datenbanken und DNS-Servern sowie Abwehr von hochvolumigen und Applikationsbasierenden DDoS-Angriffen



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.

WEB SERVICES UND „NORMALE“ FIREWALLS

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

FortiWeb Highlights

- *ICSA WAF zertifiziert*
- *DoS Schutz auf Netzwerk und Application Layer*
- *User Verhaltens-Analyse*
- *User-unabhängige Lizenzierung*
- *Geo-IP Analyse*
- *Schutz gegen OWASP Top10*
- *Schwachstellen-Management von Web-Applikationen*

Weitere Features

- *Beschleunigung kritischer Web-Anwendungen*
- *Unterstützung bei PCI DSS 6.6 Compliance Anforderungen*
- *Flexible Einsatzmöglichkeiten durch Inline, Transparent- oder Reverse-Proxy und Offline Sniffer*
- *Schnelles Setup durch Auto-Learn Security Profiling, Policy Wizzard und voreingestellte Policies*
- *Anti Web Defacement*
- *Data Loss Prevention*
- *Application Load Balancing*
- *SSL Offloading*
- *Data Compression*

FortiDB
Datenbank Security

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

FortiDDoS
DDoS-Angriffe erfolgreich abwehren

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 Attacken als auch DDoS-Angriffen auf Applikationsebene. Diese Angriffe legen ganze Webseiten still, 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 in-house 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 APPLIANCE 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 Latenzzeiten (weniger als 26 µs) garantieren. So ist die Verfügbarkeit von kritischen Systemen, Servern und Anwendungen auch bei DDoS-Angriffen 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 Netzwerkverkehrsanalyse 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-Attacken, 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.

FortiDDoS Highlights

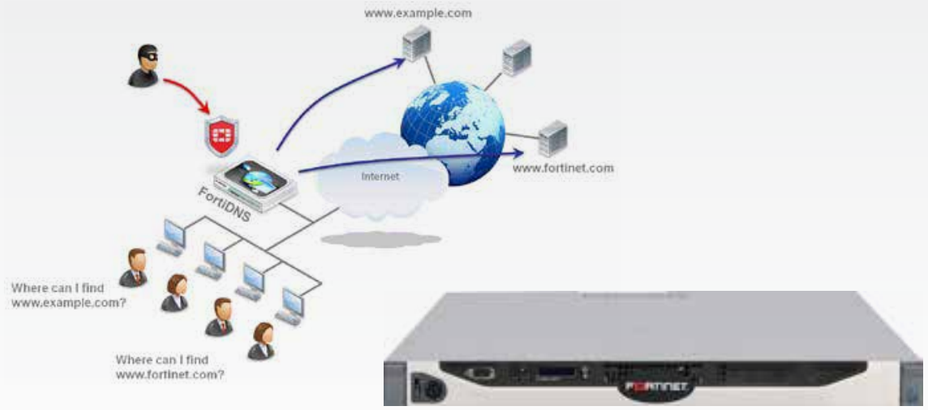
- *Hochleistungsfähige, hardware-basierte DDoS-Erkennung und Entschärfung*
- *Virtuelle Netzwerkpartitionen für parallele Absicherung von Segmenten mit unterschiedlichen Anforderungen*
- *Auto-Learning reduziert den Administrationsaufwand erheblich und passt Policies in Abhängigkeit des Verhaltens automatisch an*
- *Traffic-Baselining erkennt „natürliches“ Wachstum und reduziert False-Positives*
- *Granulares Reporting und Langzeitanalyse Verbesserung die Sichtbarkeit von Angriffen und die Effektivität der Schutzmaßnahmen*
- *Transparente Integration ohne zusätzliche IP- oder MAC-Adressen*
- *Mehrfache Schwellwerte verbessern die Erkennung von Abweichung und reduzieren die Reaktionszeit*

Weitere Features

- *Country Code/IP-Adress Filter (Geo-Location Schutz)*
- *Bogon (Bogus IP) Filter, Access Control Listen*
- *Packet Flood Reduzierung / Protokoll Verifikation*
- *Stateful Packet Inspection, Out-of-State Filter*
- *Granulare Layer 3, 4 Filter*
- *Application Layer Filter, Get und Resource Flood Filter*
- *Algorithmische Filter*
- *Heuristische Filter*

FortiDNS

DNS Server effektiv schützen



DNS-SICHERHEIT - EIN MUSS

Domain Name System (DNS), die Methodik, um Domänen-Namen in IP-Adressen von Geräten (z.B. Servern) zu übersetzen, wird oft als „Lebenselixier" des Internet bezeichnet. Ohne DNS könnten keine E-Mails versendet werden, würden keine Webseiten gefunden und jeglicher Internetzugang wäre unmöglich. Im Falle der Kompromittierung eines DNS-Systems wären Unternehmen angreifbar und User-Zugriffe auf Webseiten könnten leicht auf schädliche Inhalte umgeleitet werden. DNS ist eins der kritischsten, aber häufig am wenigsten beachteten Elemente, die kontinuierliche Geschäftsprozesse gewährleisten.

Das Problem mit DNS ist seine Komplexität, die Anfälligkeit für Fehlkonfiguration und die Notwendigkeit, es via Command Line Interface zu bedienen. FortiDNS wurde von Grund auf dahingehend entwickelt, als hoch-sicheres DNS Caching System herkömmliche Lösungen zu ersetzen. Durch seine zu 100 % grafische Benutzeroberfläche werden Konfigurationsfehler nahezu ausgeschlossen.

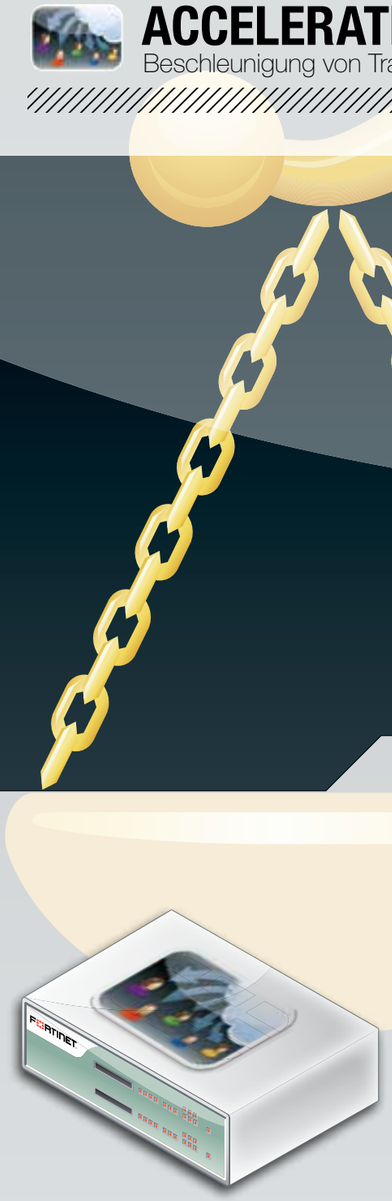
SICHERHEIT IM FOKUS

Wie auch bei anderen Fortinet Lösungen, wird Sicherheit bei FortiDNS großgeschrieben. Um dies zu erreichen, ist Fortinet eine Technologie-Partnerschaft mit Nominum, einem der führenden Anbieter von DNS-Lösungen, eingegangen. Entwickelt von Fortinet und "Powered by Nominum" steht für signifikante Verbesserung der Sicherheit im DNS-Umfeld. Dazu zählen z.B.:

LAYER	MASSNAHME	AUSWIRKUNG
Abschreckung	zufällige Transaktions-Ids (QID)	reduziert die Wahrscheinlichkeit eines erfolgreichen Angriffs
	zufälliger UDP Source Port	
	zufällige Cases (Query Namen)	
Abwehr	Erkennen & Abwehren (D&D)	reduziert die Geschwindigkeit eines Angriffs um den Faktor 100
	Erkennung von Spoofed Responses und Umschalten auf TCP	
	z.B. schaltet 0x20-Fehler auf TCP um	
Widerstandsfähigkeit	Erkennen von unverlangten Antworten	verhindert das Einbringen eines „Fake Records"
Mängelbeseitigung	Benachrichtigung und Reporting inkl. aller TCP Transaktionen (auch 0x20 und D&D)	isoliert Angreifer und leitet Gegenmaßnahmen ein

ACCELERATION SERVICES

Beschleunigung von Transaktionen, intelligentes LoadBalacing und VideoCaching



FortiADC, FortiCache

Intelligentes und hochperformantes Loadbalancing von Web-Transaktionen und -Request sowie effektives Caching von Video-Streams in z.B. CDNs

FortiADC

Application Level Load Balancing

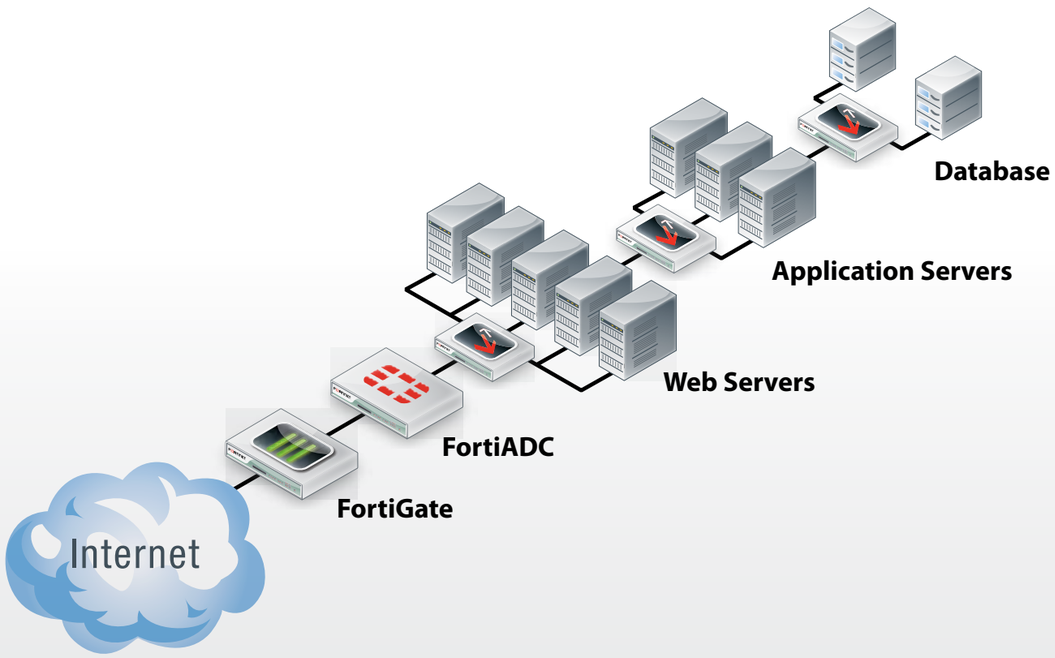
Die Parameter Verfügbarkeit, Performance und Reaktionszeit von (Web-)Anwendungen haben nicht nur zunehmend starken Einfluss auf die Akzeptanz der Nutzer, sondern bestimmen immer häufiger auch den wirtschaftlichen Erfolg von ganzen Unternehmensbereichen. Geschäftskritische Anwendungen wie Portale, Shops, CRM- oder ERP-Systeme usw. müssen daher gut und schnell funktionieren, um ihrem Zweck gerecht werden zu können. Häufig werden aber die eingangs genannten Parameter durch schlechte Programmierung der Web-Inhalte, falsch dimensionierte und somit überlastete (Web-)Server, oder unflexible Leitungsnutzung negativ beeinflusst. Abhilfe schaffen hier sogenannte Application LoadBalancing Systeme, die die Last intelligent auf die verfügbaren Server verteilen, Web-Inhalte optimieren und lokal oder sogar dezentral zwischenspeichern und weitere optimierende Funktionen übernehmen können.
Die neue Serie der FortiADC optimiert die Verfügbarkeit, das Anwendungsverhalten, die Performance sowie die Skalierbarkeit von sowohl mobilen und Cloud- als auch von Enterprise-Anwendungen. Das Design dieser Produktlinie wurde auf eine schnelle, intelligente und sichere Beschleunigung von bandbreitenlastigen und intensiv genutzten Enterprise-Anwendungen sowie Traffic-Optimierung abgestimmt. Diese Lösungen eignen sich ideal für traditionelle wie virtualisierte Rechenzentren und Cloud-Infrastrukturen in Unternehmen aller Größenordnungen.

Die FortiADC-Serie bietet folgende Funktionen:

- *Umfangreiche Layer 2-7 Load Balancing Möglichkeiten*
- *Advanced Content Routing*
- *Global Server Load Balancing*
- *SSL Offloading & Acceleration*
- *High Performance Caching*
- *TCP Acceleration*
- *IPv6 Support*

Weitere Features

- *Dynamic Compression*
- *Eine Vielzahl von Methoden zur Stabilisierung von Anwendungen*
- *Flexible „Gesundheits-Checks" für Anwendungen*
- *Unterstützung von transparentem und Proxy-Betrieb*
- *„One-Arm" und „Two-Arm" Konfigurationen*
- *Höchste Performance und optimal Skalierbarkeit*
- *Umfangreiche Managementoptionen*
- *Intelligentes und leicht zu konfigurierendes Layer 4/7 Policy- und Gruppen-Management*
- *Layer 4/7 Application Load Balancing*
- *Hochverfügbarkeits-Modus (active/passive)*
- *Konfigurierbarer Proxy-Modus (NAT) oder Transparenter-Modus pro VIP*
- *SSL Offloading*
- *IPv4 und IPv6 Firewall Regeln*
- *SynCookie-Schutz*
- *IPv6 Support*



FortiCache

ISP & Enterprise-Class Content Caching

BANDBREITE - EINE STÄNDIGE HERAUSFORDERUNG

Durch die Verlagerung der Internet-Nutzung von stationären zu mobilen Endgeräten haben sich die Nutzungsprofile ebenso drastisch verändert wie die Art und Menge der übertragenen Daten: Interaktive Webseiten, Video- und Audio-Streams und ständig größere Grafik-Dateien und Präsentationen erzeugen eine immense Last.
Carrier, Service Provider, Großunternehmen und Schulungsanbieter kämpfen gemeinsam mit demselben Problem: Bandbreite ist bereits in dem Moment verbraucht, in dem sie bereitgestellt wird. Netzwerke müssen die explosionsartig steigende Nachfrage ebenso verkraften wie Engpässe verhindert und die Funktionalität und Profitabilität aufrecht erhalten werden müssen.

KONTROLLE ÜBER DAS NETZWERK

Die FortiCache-Appliances ermöglichen eine verbesserte Netzwerk-Kontrolle durch die Möglichkeit, Inhalte zu cachen (zwischenzuspeichern) und Anwendungen massiv zu beschleunigen - und reduzieren so deren Einfluss auf die Netzwerk-Performance. Durch das Cachen von Anwendungs-Inhalten können Großunternehmen ISPs, Mobilfunk-Provider, Telcos, Universitäten und andere Ausbildungs-Netzwerke häufig genutzte Daten einfach lokal bereitstellen und den mehrfachen Download verhindern.

BANDBREITEN-REDUKTION UND APPLIKATIONS-BESCHLEUNIGUNG

Kurzzeitphänomene wie aktuelle Nachrichten, Sport-Events, Videos, Spiele uvm. treiben Bandbreite-Anforderungen kurzzeitig in ultimative Höhen – um ebenso schnell wieder zu verschwinden. Durch diese unvorhersehbare, aber extrem hohe Nachfrage können ganze Netzwerke vorübergehend zusammenbrechen und wichtige Dienste nicht mehr verfügbar sein – was nicht selten hohe Kosten verursacht. Diese Spitzenlasten zu bewältigen, ermöglicht es den zuvor genannten Unternehmen, deutlich verbesserte Services bereitzustellen und damit Kunden- und Mitarbeiterzufriedenheit, Produktivität und letztlich Profitabilität spürbar zu steigern.

FORTICACHE NETZWERKKONTROLLE

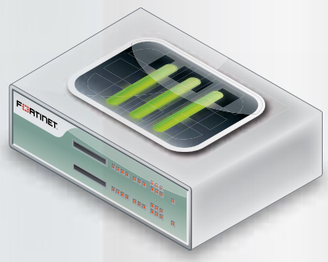
Nicht überall ist Bandbreite zu vertretbaren Kosten oder unbegrenzt verfügbar. Oft sind hier kostspielige Alternativen wie etwa Satellitenverbindungen o.ä. erforderlich, um die geforderten Dienste bereitstellen zu können. FortiCache behebt dieses Problem durch maximale Speicherung von Daten „im Netz" und reduziert so spürbar die benötigte Leitungskapazität und damit die Kosten. FortiCache „versteht" die Dateiformate von Content Delivery Networks (CDNs) wie z.B. YouTube und anderen Media-Streams, auch wenn diese Dateien mit Werbung versehen sind oder über verteilte Lokationen bereitgestellt werden.

Highlights:

- *EnterpriseClass Content Caching*
- *Video Caching*
  - *Erkennung derselben Video-ID auch bei Content von verschiedenen CDN Hosts*
  - *Vorwärts- und Rückwärtssuche in Videos*
  - *Werbungserkennung in Videos*
- *Content Delivery Network Awareness*
  - *mehr als 55 CDNs werden erkannt, weitere folgen*
- *Flow Based Web Content Filter*

VIRTUAL SECURITY

Virtualisierung von Security und Schutz virtueller Systeme



VDOMs und Fortinet VM

Virtual Security

Virtualisierung von Security-Funktionen auf jeder FortiGate (VDOM), Mandantenfähiges Management & Reporting (ADOM) und Security Appliances für VMware und XEN

Fortinet Virtual Appliances

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.

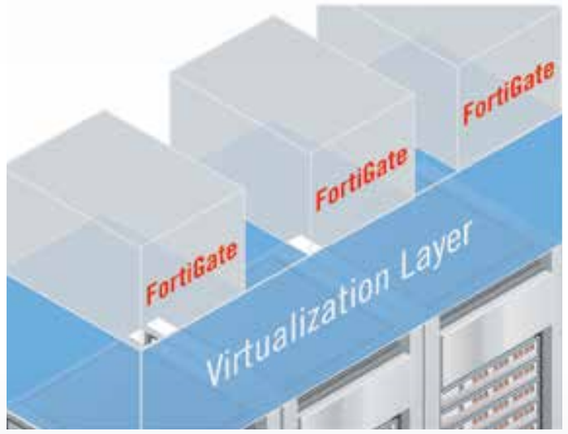
Fortinet bietet bereits seit 2004 virtualisierte Security-Lösungen an, die heute von vielen Service-Providern und Großkonzernen genutzt werden, um flexibel und mandantenfähig komplexe Sicherheits-Dienste anbieten zu können. Mit der FortinetVM Serie erweitert Fortinet dieses Angebot für VMware und XEN 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.

Folgende Fortinet-Lösungen sind bereits als virtuelle Systeme verfügbar:

- *FortiGate (NGFW/UTM-Appliance)*
- *FortiAnalyzer VM(Analyse & Reporting Tool)*
- *FortiManager (Management & Konfiguration)*
- *FortiWeb VM (Web Appliaction & XML-Firewall)*
- *FortiMailVM (Mail-Security AV/AS Lösung)*
- *FortiScanVM*

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.



Virtuelle FortiGate Appliances innerhalb einer virtuellen Infrastruktur

ZUBEHÖR

Top Rack Switching, Bypass Switches und mehr

Zubehör

FortiSwitch,
FortiCam,
FortiBridge,
PowerInjector,
Rackmount IT

FortiSwitch

FortiSwitch

GIGABIT ETHERNET SWITCHES

Fortinets FortiSwitch Gigabit Ethernet Switch Familie mit 10 Gigabit Ethernet Uplinks bietet hohe Performance und Skalierbarkeit zu einem günstigen Preis. Die FortiSwitch Plattform ist für High-Performance Computing (HPC) entwickelt worden und bietet dabei Einsatzmöglichkeiten für jede Umgebung - von Small Office bis hin zum Data Center. Die den FortiSwitches zugrundeliegende Technologie wurde zudem auch in alle HighEnd FortiGate-Systeme integriert.

FORTISWITCH 28C

Zusammen mit den FortiGate Security-Appliances ermöglicht der FortiSwitch-28C der IT die Erzeugung einer sicheren Netzwerkgrenze im Unternehmen. Geräte, die sich von außerhalb verbinden, werden zuerst identifiziert, und der Nutzer wird authentifiziert. Nach erfolgreicher Authentifizierung gelten für die Nutzung des Gerätes entsprechende, von der IT definierte Sicherheitsregeln. So entsteht eine sichere Netzwerkgrenze. Die FortiSwitch-Plattformen wurden speziell für die Anforderungen der Ethernet-Infrastruktur und Zugriffsmöglichkeiten in modernen Netzwerken entwickelt. Dank der hohen Benutzerfreundlichkeit ist eine Skalierung nach Ihren Anforderungen jederzeit möglich.

FORTISWITCH-348B

Der Secure Access Wire-Closet Switch FortiSwitch-348B bietet ein exzellentes Preis-Leistungs-Verhältnis und hervorragende Skalierbarkeit für Organisationen mit unterschiedlichen operativen Anforderungen. Der Switch verfügt über 96 Gbps sowie 48 Secure Access Ports und 2 gemeinsam genutzte SFP- bzw. RJ45 Uplink-Ports. Mit seiner Größe von 1RU Rack Mount verbindet dieser Switch Netzwerkgeräte mit der Ethernet-Infrastruktur.

FORTISWITCH-448B

Der FortiSwitch 448B ist ein 1RU großer Ethernet Switch, der speziell für den Schlatschrank-Einbau mit hoher Dichte in mittleren Unternehmen und Klassenzimmern entwickelt wurde. Mit seinen 48 GbE-Access Ports sowie 10 GbE Uplinks erfüllt der FortiSwitch-448B optimal die Anforderungen an Bandbreite und Portdichte in modernen Netzwerken.

FORTISWITCH-548B

Der FortiSwitch-548B ist ein High-End 10G-Ethernet Switch für Top-Rack Anwendungen. Mit seinen 960 Gbps Durchsatz und 48x 10GbE-Ports eignet er sich für Umgebungen mit extrem hohen Anforderungen an hohe Performance und kurze Latenzzeiten, wie z.B. In großen Server-Farmen, E-Trading, Finance, Simulationen oder Multi-Media-Streaming.

FORTISWITCH-80-POE

Der FortiSwitch-80-POE ist ein Power over Ethernet Switch, der auf vier der acht Gigabit Ethernet Ports 15.4W zur Verfügung stellt und sowohl für den Einsatz im Enterprise, als auch für Small Office Umgebungen geeignet ist. Typische Einsatzszenarien sind der Anschluss von IP Telefonen (wie die FortiFone Produktfamilie), Thin Access Points (wie die FortiAP Produktfamilie) oder IP Kameras, ohne eine zusätzliche PoE Quelle installieren zu müssen.

FORTISWITCH-124B-POE

Dieser gemanagte Switch ermöglicht die VLAN-Segmentierung für Sprach- und Videodaten sowie Wireless Traffic. Die eingebaute PoE-Stromversorgung leistet bis zu 100 Watt auf den ersten 12 Ports. Im typischen Büro-Einsatz lassen sich so drahtlose APs, VoIP-Telefone und PCs anbinden. Jeder PoE-Port liefert dabei bis zu 15,4 Watt Leistung.

FORTISWITCH 224B-POE ETHERNET SWITCH

Dieser gemanagte Switch ermöglicht die VLAN-Segmentierung für Sprach- und Videodaten sowie Wireless Traffic. Der Switch ist in einem 1RU-Gehäuse untergebracht und bietet dedizierte 180 Watt PoE-Leistung. Der Switch ist ganz einfach über eine standardmäßige serielle Konsole und ein web-basiertes GUI konfigurierbar.

FORTISWITCH-324B-POE

Der FortiSwitch-324B-PoE ist ein leistungsfähiger Switch mit einer hohen Portdichte speziell für Umgebungen, in denen viele PoE-fähige Endgeräte (WLAN-Access Points und/oder VoIP-Telefone, IP-Kameras oder andere IP-basierende Gebäudetechnik) zum Einsatz kommen.

FortiSwitch Highlights

- *Hohe Performance**
- *10GbE-Uplinks**
- *10GbE High-Densitiy Switch**
- *Niedrige Latenzzeiten**
- *SFP-Support für unterschiedliche Kabeltypen (Kupfer/Glasfaser)**
- *PoE-Support**
- *Redundantes PowerSupply**
- *Integration in FortiManager**
- *Bestes Preis-/Leistungsverhältnis**

**modellabhängig*

FortiCam
Netzwerkbasierte Videoüberwachung

Mit FortiCamera lösen Sie ihre Probleme bei der Videoüberwachung und verbessern das Nutzererlebnis. Sichern Sie Ihre Eingänge und kritischen Bereiche, wie Verkaufsterminals, Lagerhäuser, öffentliche Bereiche und Laderampen mit Kameras ab. Die Bilder werden vom Netzwerk-Videorecorder aufgezeichnet. Die Videoüberwachung wird somit zu einer Erweiterung Ihres Netzwerks.

APPLIANCE ODER VM OHNE LIZENZGEBÜHREN

FortiCameras erfordern keinerlei Softwareinstallation, Patches oder nutzerbasierte Lizenzgebühren. FortiCamera ist einfach. Verbinden Sie die Kamera, schalten Sie die Appliance an, öffnen Sie einen Webbrowser, und alles ist einsatzbereit. Der FortiRecorder ist ebenfalls als virtuelle Maschine erhältlich.

Features & Vorteile

- *Hohe Performance*
- *Kontinuierliche oder bewegungsgesteuerte Aufzeichnung (oder beides)*
- *Alarmmeldungen und Benachrichtigungen über Momentaufnahmen halten Sie auf dem Laufenden*
- *Mit der Ereigniszeitleiste lassen sich Bewegungen schnell und einfach suchen*
- *Kameras nutzen Power over Ethernet (PoE) zur einfachen Installation*
- *Webbasierte Oberfläche erfordert keinen dedizierten Client*

FortiBridge
Datenbank Security

FailOver-Schutz für FortiGate Appliances, die Inline genutzt werden. Überbrückt die Verbindung ohne Unterbrechung bei System- oder Stromausfall.

PoE-Power Injector
Spannungsversorgung für PoE-Geräte

Der PoE-Power Injector ermöglicht die Spannungsversorgung von PoE-fähigen Endgeräten wie den FortiAP WLAN Access Points oder FortiFon VoIP-Telefonen auch an FortiGate Appliances oder Switches ohne PoE-Support.

Rackmount IT

Fortinet bietet hochleistungsfähige Geräte für kleine und mittlere Unternehmen – allerdings handelt es sich dabei um Desktop-Modelle. Derzeit steigen immer mehr Unternehmen auf 19-Zoll-Racks um. Die neuen FortiRack-Kits eignen sich dabei hervorragend für den Einbau von Fortinet-Geräten in 19-Zoll-Schaltschränke.
Das FortiRack-Kit ist die ideale Ergänzung, für den Einbau der hochleistungsfähigen FortiGate-Einheit in einem 19-Zoll-Rack. Darüber hinaus werden so die wichtigsten Konsolen- und Netzwerkverbindungen an die Vorderseite verlagert. Der Zusammenbau ist in nur 5 Minuten erledigt. Hierzu wird einfach die FortiGate-Einheit in den Kit eingesetzt, die Halter angebracht und die mitgelieferten Kabel werden mit den Keystones verbunden.
FortiRacks gibt es für alle Geräte der Baureihen FortiGate, FortiAnalyzer, FortiManager & FortiMail, die nicht in ein Rack passen.

FortiGate
Integrated Network Security Platform - Industry's #1 Network Security Solution

	FG/FWF-30D	FG/FWF-60C	FG/FWF-60D	FG/FWF-90D	FG-100D	FG-200D	FG-240D	FG-280D-POE	FG-300C	FG-600C
Firewall Throughput (1518/512/64 byte UDP)	800 / 800 / 800 Mbps	1 / 1 / 1 Gbps	1.5 / 1.5 / 1.5 Gbps	3.5 / 3.5 /3.5 Gbps	2500 / 1000 / 200 Mbps	3 / 3 / 3 Gbps	4 / 4 / 4 Gbps	4 / 4 / 4 Gbps	8 / 8 / 8 Gbps	16 / 16 /16 Gbps
Firewall Latency	8 µs	4 µs	4 µs	4 µs	37 µs	2 µs	6 µs	2 µs	2 µs	7 µs
Concurrent Sessions	200,000	400,000	500,000	1.5 Mil	3 Mil	1.4 Mil	3.2 Mil	3.2 Mil	2 Mil	3 Mil
New Sessions/Sec	3,500	3,000	4,000	4,000	22,000	77,000	77,000	77,000	50,000	70,000
Firewall Policies	5,000	5,000	5,000	5,000	10,000	10,000	10,000	10,000	10,000	10,000
IPSec VPN Throughput	350 Mbps	70 Mbps	1 Gbps	1 Gbps	450 Mbps	1.3 Gbps	1.3 Gbps	1.3 Gbps	4.5 Gbps	8 Gbps
Max G/W to G/W IPSEC Tunnels	20	50	200	200	2,000	2,000	2,000	2,000	2,000	2,000
Max Client to G/W IPSEC Tunnels	250	500	500	1,000	5,000	5,000	5,000	5,000	10,000	50,000
SSL VPN Throughput	25 Mbps	19 Mbps	30 Mbps	35 Mbps	300 Mbps	400 Mbps	400 Mbps	400 Mbps	200 Mbps	1 Gbps
Recommended SSL VPN Users	80	100	100	200	300	300	300	300	500	5,000
IPS Throughput	150 Mbps	135 Mbps	200 Mbps	275 Mbps	950 Mbps	1.7 Gbps	2.1 Gbps	2.1 Gbps	1.4 Gbps	4 Gbps
Antivirus Throughput (Proxy-Based/ Flow-Based)	30 / 40 Mbps	20 / 40 Mbps	35 / 50 Mbps	35 / 65 Mbps	300 / 700 Mbps	600 / 1,100 Mbps	600 / 1,100 Mbps	600 / 1,100 Mbps	200 / 550 Mbps	1.3 / 2.8 Gbps
Max FortiAPs (Total / Tunnel)	2 / 2	10 / 5	10 / 5	32 / 16	64 / 32	64 / 32	64 / 32	64 / 32	512 / 256	1024 / 512
Max FortiTokens	20	100	100	100	1,000	1,000	1,000	1,000	1,000	1,000
Max Registered FortClient	10	200	200	200	2,000	2,000	2,000	2,000	2,000	2,000
Virtual Domains (Default/Max)	-	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10
Interfaces (FE, GE ports)	5x GE RJ45	8x GE RJ45	10x GE RJ45	16x GE RJ45	20x GE RJ45, 2x Shared Port Pairs (100D only)	18x GE RJ45, 2x GE SFP	42x GE RJ45, 2x GE SFP	54x GE RJ45, 32x PoE GE RJ45, 4x GE SFP	10x GE RJ45	18x GE RJ45, 4x Shared Port Pairs, 2x Bypass Pairs
Interfaces (Others)	FWF - a/b/g/n	FWF - a/b/g/n	FWF - a/b/g/n	FWF - a/b/g/n	-	-	-	-	-	-
Local Storage	-	-	-	32 GB	32 GB	16 GB	32 GB	64 GB	32 GB	64 GB
Power Supplies	Single AC Power Supply	Single AC Power Supply	Single AC Power Supply	Single AC Power Supply	Single AC Power Supply	Single AC Power Supply, opt. Ext RPS	Single AC Power Supply, opt. Ext RPS	Single AC Power Supply, opt. Ext RPS	Single AC Power Supply, opt. Ext RPS	Single AC Power Supply, opt. Dual PS or Ext RPS
Form Factor	Desktop	Desktop	Desktop	Desktop	Rack Mount, 1 RU	Rack Mount, 1 RU	Rack Mount, 1 RU	Rack Mount, 2 RU	Rack Mount, 1 RU	Rack Mount, 1 RU
Variants	WiFi, POE	WiFi, Anal.Modem, Wifi+Ana. Modem, LENC, SFP, POE, ADSL	WiFi, POE, LENC	WiFi, POE, LENC	LENC, High port density, High port density + POE	LENC	-	-	DC, LENC	DC, LENC

	FG-800C	FG-1000C	FG-1240B	FG-1500D	FG-3240C	FG-3600C	FG-3700D	FG-3950B	FG-5001C	FG-5101C
Firewall Throughput (1518/512/64 byte UDP)	20 / 20 / 20 Gbps	20 / 20 / 20 Gbps	40-44 / 40-44 / 38-42 Gbps	80 / 80 / 55 Gbps	40 / 40 /40 Gbps	60 / 60 /60 Gbps	160 / 160 / 110 Gbps	20-120 / 20-120 / 20-120 Gbps	40 / 40 /40 Gbps	40 / 40 /10 Gbps
Firewall Latency	6 µs	6 µs	7 µs	3 µs	4 µs	4 µs	2 µs	4 µs	4 µs	7 µs
Concurrent Sessions	7 Mil	7 Mil	5 Mil	12 Mil	10 Mil	28 Mil	44 Mil	20 Mil	29.5 Mil	10 Mil
New Sessions/Sec	190,000	190,000	120,000	250,000	200,000	235,000	300,000	250K - 300K**	210,000	235,000
Firewall Policies	10,000	100,000	100,000	100,000	100,000	100,000	100,000	100,000	100,000	100,000
IPSec VPN Throughput	8 Gbps	8 Gbps	16 - 18.5 Gbps	50 Gbps	17 Gbps	25 Gbps	100 Gbps	8 - 50.5 Gbps	17 Gbps	22 Gbps
Max G/W to G/W IPSEC Tunnels	2,000	10,000	10,000	10,000	10,000	10,000	10,000	10,000	10,000	10,000
Max Client to G/W IPSEC Tunnels	50,000	50,000	50,000	50,000	64,000	64,000	64,000	64,000	64,000	64,000
SSL VPN Throughput	1.3 Gbps	1.3 Gbps	370 Mbps	4 Gbps	3.4 Gbps	5.3 Gbps	6 Gbps	1.2 Gbps	850 Mbps	970 Mbps
Recommended SSL VPN Users	10,000	10,000	1,500	10,000	30,000	30,000	30,000	25,000	30,000	25,000
IPS Throughput	6 Gbps	6 Gbps	5 - 8 Gbps	11 Gbps	8 Gbps	14 Gbps	23 Gbps	5- 20 Gbps	9.8 Gbps	9.4 Gbps
Antivirus Throughput (Proxy-Based/ Flow-Based)	1.7 / 3.1 Gbps	1.7 / 3.1 Gbps	1.2 / 1.6 Gbps	4.3 / 13 Gbps	2.6 / 9 Gbps	5.8 / 18 Gbps	7.5 / 18 Gbps	4 / 5 - 15 Gbps	3 / 4 Gbps	2 / 5 Gbps
Max FortiAPs (Tunnel, Bridge)	1024 / 512	4096 / 1024	4096 / 1024	4096 / 1024	4096 / 1024	4096 / 1024	4096 / 1024	4096 / 1024	4096 / 1024	4096 / 1024
Max FortiTokens	1,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000	5,000
Max Registered Endpoints	2,000	8,000	8,000	8,000	8,000	8,000	8,000	8,000	8,000	8,000
Virtual Domains (Default/Max)	10 / 10	10 / 250	10 / 250	10 / 250	10 / 500	10 / 500	10 / 500	10 / 500	10 / 500	10 / 500
Interfaces	2x 10GE SFP+ ,14x GE RJ45, 8x Shared Port Pairs, 2x Bypass Pairs	2x 10GE SFP+, 14x GE RJ45, 8x Shared Port Pairs, 2x Bypass Pairs	16x GE RJ45, 24x GE SFP	8 x 10GE SFP+/GE, 18x GE RJ45, 16x GE SFP	12x 10GE SFP+, 2x GE RJ45, 16x GE SFP	12x 10GE SFP+, 2x GE RJ45, 16x GE SFP	4 x 40GE QSFP+, 20 x 10GE SFP+/GE SFP, 8 x SFP+, 2 x GE RJ45	2x 10GE SFP+, 2x GE RJ45, 4x GE SFP	2x 10GE SFP+ , 2x GE RJ45	4x 10GE SFP+, 2x GE RJ45
Local Storage	64 GB	128 GB	64 GB (384 GB Max)	240 GB	64 GB	128 GB	960 GB	256 GB	128 GB	64 GB
Power Supplies	Single AC Power Supply, opt. Dual PS or Ext RPS	Dual PS	Dual PS	Dual PS	Dual PS	Dual PS	Dual PS	Dual PS	Chassis Based	Chassis Based
Form Factor	Rack Mount, 1 RU	Rack Mount, 2 RU	Rack Mount, 2 RU	Rack Mount, 2 RU	Rack Mount, 2 RU	Rack Mount, 3 RU	Rack Mount, 3 RU	Rack Mount, 3 RU	ATCA Blade	ATCA Blade
Variants	DC	DC, LENC	DC	-	DC	DC	-	DC, LENC	-	-
FG-VM01, FG-VM02, FG-VM04, FG-VM08 Virual Appliances										
VM Supported	VMware ESX/ESXi 4.0/4.1/5.0/5.1, Citrix XenServer 5.6 SP2/6.0 or later, Open Source Xen 3.4.3/4.1 or later, Microsoft Hyper-V 2008 R2/2012, KVM									

* Featured Top selling models, for complete FortiGate offernge please visit www.fortinet.com. Specifications based on FortiOS V5.0.6+
** With FM1-XH1

FortiManager
Centralized Management Platform - Tools that effectively manage Fortinet security infrastructure

	FMG-200D	FMG-300D	FMG-1000D	FMG-4000D	FMG-5001A	FMG-VM-BASE	FMG-VM-10-UG	FMG-VM-100-UG	FMG-VM-1000-UG	FMG-VM-5000-UG	FMG-VM-U-UG
Max Licensed Devices/ADoms	30	300	800	4,000	4,000	10	+10	+100	+1,000	+5,000	Unlimited
Max Web Portals/Users	-	-	800	4,000	4,000	10	+10	+100	+1,000	+5,000	Unlimited
GB Logs/Day	2	2	2	2	2	1	2	5	10	25	50
Locally Hosted Security Content	AV, IPS, VM, WF, AS	AV, IPS, VM, WF, AS	AV, IPS, VM, WF, AS	AV, IPS, VM, WF, AS	AV, IPS, VM, WF, AS	AV, IPS, VM	AV, IPS, VM	AV, IPS, VM	AV, IPS, VM, WF, AS	AV, IPS, VM, WF, AS	AV, IPS, VM, WF, AS
Total Interfaces	4x GE RJ45	4x GE RJ45	6x GE RJ45, 2x SFP	4x GE RJ45, 2x SFP	2x GE RJ45	1 / 4 (vNIC Min / Max)					
Storage Capacity	1x 1 TB	2x 2TB	4x 2 TB	8x 2 TB	1x 80 GB	80 GB / 16 TB (Min / Max)					

FortiAnalyzer
Centralized Logging & Reporting - Logging, reporting and analysis from multiple Fortinet devices

	FAZ-200D	FAZ-300D	FAZ-1000D	FAZ-2000B	FAZ-3000D	FAZ-4000B	FAZ-VM-BASE	FAZ-VM-GB1	FAZ-VM-GB5	FAZ-VM-GB25	FAZ-VM-GB100
GB Logs/Day	5	15	25	75	250	Unlimited*	1	+1	+5	+25	+100
Sessions/Day	18 Mil	55 Mil	85 Mil	260 Mil	850 Mil	Unlimited*	3.5 Mil	3.5 Mil	18 Mil	85 Mil	360 Mil
Max Log Rate (standalone Mode)	350	625	1,000	3,000	10,000	Unlimited*	-	-	-	-	-
Max. Licensed Devices/ADoms	150	200	2,000	2,000	2,000	2,000	10,000	10,000	10,000	10,000	10,000
Total Interfaces	4x GE RJ45	4x GE RJ45	6x GE RJ45, 2x SFP	6x GE RJ45	4x GE RJ45, 2x GE SFP	2x GE RJ45, 2x GE SFP	-	-	-	-	-
Storage Capacity	1x 1 TB	2x 2 TB	4x 2 TB	2x 2 TB (12 TB Max)	8x 2 TB	6x 1 TB (24 TB Max)	200 GB	+200 GB	+1 TB	+8 TB	+16 TB
RAID Support	No	Yes (Mirrored)	Yes, (RAID 0, 1, 5, 6, 10, 50, 60)	Yes, (RAID 0, 1, 5, 10, 50)	Yes, (RAID 0, 1, 5, 6, 10, 50, 60)	Yes, (RAID 0, 1, 5, 6, 10, 50, 60)	-	-	-	-	-

* Only restricted to the hardware platform performance (e.g. there are no software licensing limitations)

FortiAP
Wireless Access Point - Extending FortiGate Wireless connectivity

	FAP-11C	FAP-14C	FAP-28C	FAP-112B	FAP-221B/223B	^FAP-221C	FAP-222B	FAP-320B	^FAP-320C
Target Environment	Remote	Remote	Remote	Indoor/Outdoor	Indoor	Indoor	Indoor/Outdoor	Indoor	Indoor
Number of Radio / Antennas	1 / 1 Internal	1 / 1 Internal	1 / 2 Internal	1 / 1 Internal	221B: 2 / 4 Int. 223B: 2 / 4 Ext.	2 / 4 Internal	2 / 4 External	2 / 6 internal	2 / 6 internal
TX / RX Streams (802.11n / ^802.11ac)	1x1 MIMO - 150 Mbps	1x1 MIMO - 150 Mbps	2x2 MIMO - 300 Mbps	1x1 MIMO - 150 Mbps	2x2 MIMO dual spatial stream - 600 Mbps Total	2x2 MIMO dual spatial stream - 1167 Mbps Total	2x2 MIMO dual spatial stream - 600 Mbps Total	3x3 MIMO with 3 spatial streams - 900 Mbps Total	3x3 MIMO with 3 spatial streams - 1750 Mbps Total
Total (Client access + Monitoring) Simultaneous SSIDs	8	8	8	8	16	16	16	16	16
Max Transmission Power	17dBm (50mW)	17dBm (50mW)	17dBm (50mW)	24 dBm (250mW) *	17dBm (50mW)	17dBm (50mW)	27dBm (500mW) hardware capable	24 dBm (250mW) *	24 dBm (250mW) *
Ethernet Interface	2x GE RJ45	5x FE	10x GE RJ45	2x FE	1x GE RJ45	1x GE RJ45	1x GE RJ45	2x GE RJ45	2x GE RJ45
Power over Ethernet (PoE)	-	-	-	802.3af	802.3af	802.3af	802.3at	802.3af / 802.3at	802.3af / 802.3at

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

FortiSwitch
Access Switch - Wired connectivity for secured network access

	FSW-28C	FSW-80-POE	FSW-108D-POE	FSW-124B-POE	FSW-224D-POE	FSW-324B-POE	FSW-348B	FSW-448B	FSW-548B
Total Interfaces	8 x GE RJ45 LAN, 2 x GE RJ45 WAN	8x GE RJ45 (Include 4x PoE)	8x GE POE RJ45 ports, 2x Shared Port Pairs	24x FE (include 12x PoE), 2x Shared Port Pairs	20x GE RJ45 ports (incl. 12 PoE), 4x GE Shared Port Pairs	16x GE PoE, 4x GE PoE+, 4x Shared Port Pairs	48 GE RJ45, 2x Shared Port Pairs	48 GE RJ45, 2x 10GE SFP+	48x 10G, 1x mgmt
Switch Capability	16 Gbps	2 Gbps	20 Gbps	8.8 Gbps	48 Gbps	48 Gbps	96 Gbps	136 Gbps	960 Gbps
Max VLANs	4096 (VTP v1/v2)	-	4096 (VTP v1/v2)	64	4096 (VTP v1/v2)	4096 (VTP v1/v2)	4096 (VTP v1/v2)	4096 (VTP v1/v2)	3965 (VTP v1/v2)
FortiGate Switch Controller Support	Yes (Remote Sw.)	-	Yes	-	Yes	Yes	Yes	-	-

FortiAuthenticator
Authentication Server - Identity Management, User Access Control and multi-factor identification

	FAC-200C	FAC-400C	FAC-1000D	FAC-3000D	FAC-VM Base	FAC-VM-100-UG	FAC-VM-1000-UG	FAC-VM-10000-UG	FAC-VM-100000-UG
Max Local/Remote Users/ User Group	500 / 500 / 25	2,000 / 2,000 / 50	10,000 / 10,000 / 2,000	40,000 / 40,000 / 4,000	100 / 100 / 10	+100 / +100 / +10	+1,000 / +1,000 / +100	+10,000 / +10,000 / +1,000	+100,000 / +100,000 / +10,000
Max FortiToken	500	2,000	10,000	40,000	200	+200	+2,000	+20,000	+200,000
Max NAS Devices	50	200	1,000	4,000	10	+10	+100	+1,000	+10,000
Total Interfaces	4x GE RJ45	4x GE RJ45	4x GE RJ45, 2x GE SFP	4x GE RJ45	-	-	-	-	-
Storage Capacity	1x 1 TB	1x 1 TB	2x 2 TB	2x 2 TB	60 GB / 2 TB (Min / Max)				

FortiMail
Messaging Security - Advanced antispam and antivirus filtering capabilities, with extensive quarantine and archiving capabilities

	FML-200D	FML-400C	FML-1000D	FML-3000D	FML-5002B	FML-VM01	FML-VM02	FML-VM04	FML-VM08
Email Routing (Msg/Hr)	200,000	400,000	1.5 Mil	2.3 Mil	2.3 Mil	90,000	265,000	1.32 Mil	1.76 Mil
Performance AS+AV (Msg/Hr)	175,000	320,000	1.2 Mil	2.0 Mil	2.0 Mil	77,000	185,000	1.05 Mil	1.40 Mil
Email Domains	50	500	5,000	5,000	10,000	50	500	5,000	5,000
Server Mode Mailboxes	200	1,000	3,000	3,000	3,000	200	1,000	3,000	3,000
Total Interfaces	4x GE RJ45	4x GE RJ45	6x GE RJ45, 2x GE SFP	4x GE RJ45, 2x GE SFP	3x GE RJ45	-	-	-	-
Storage Capacity	1x 1 TB	2x 1 TB	2x 2 TB	2x 2 TB (12 TB Max)	1x 146GB	50 GB - 1 TB	50 GB - 2 TB	50 GB - 4 TB	50 GB - 8 TB

FortiWeb
Web Application Security - Web application firewall to protect, balance, and accelerate web applications

	FWB-400C	FWB-1000D	FWB-3000D/Fsx	FWB-4000D	FWB-VM02	FWB-VM04	FWB-VM08
Throughput (HTTP)	100 Mbps	750 Mbps	1.5 Gbps	4 Gbps	100 Mbps	500 Mbps	1 Gbps
Total Interfaces	4x GE RJ45	2x GE RJ45, 4x GE RJ45 Bypass, 2x GE SFP	4x GE RJ45, 2x GE Bypass / 2 GE SFP	6x GE RJ45, 2x GE RJ45 Bypass, 2x GE SX Bypass	-	-	-
Storage	1 Tb	2x 2 TB	2x 2TB	2x 2TB	40 GB / 2 TB (Min / Max)		

FortiBalancer & FortiADC
Application Delivery Controllers - Optimize the availability, user experience, performance and scalability

	FAD-200D	FAD-300E	FBL-400	FAD-600E	FBL-1000	FAD-1000E	FBL-2000	FBL-3000	FAD-VM01/VM02/VM04/VM08
Throughput (HTTP)	2.7 Gbps	4.8 Gbps	2 Gbps	10 Gbps	4 Gbps	13 Gbps	10 Gbps	30 Gbps	Hardware Dependent
Total Interfaces	4x GE RJ45	6x GE RJ45	4x GE RJ45	2x 10GE, 8x GE RJ45	8x GE RJ45, 2x GE SFP	2x 10GE, 8x GE RJ45	2x 10GE, 12x GE RJ45, 4x GE SFP	4x 10G, 16x GE RJ45, 4x GE SFP	

FortiSandbox
Advanced Threat Prevention - Proactive Detection and Mitigation against APTs & Unknown Threats

	FSA-3000D
File Per Day	Unlimited

FortiDDOS
Hardware Accelerated DDoS Defense - Intent Based Protection against DDOS

	FDD-100A	FDD-200A	FDD-300A
Throughput (Full Duplex)	1 Gbps	2 Gbps	3 Gbps
Simultaneous Connections	1 Mil	2 Mil	3v Mil
Session Setup/Teardown	100 K/Sec	200 K/Sec	300 K/Sec

FortiCache
Web Caching Appliance - Reduce the cost and impact of downloaded content, while increasing performance & users experience

	FCH-400C	FCH-1000D	FCH-3000C	FCH-3000D	FCH-VM01	FCH-VM02	FCH-VM04	FCH-VM08
Total Interfaces	4x GE RJ45	2x GE RJ45, 2x GE SFP, 4x GE RJ45 Bypass	4x GE RJ45, 2x GE SFP	4x GE RJ45, 2x GE SFP, 2x GE RJ45 Bypass	1 Virtual NIC min (4 Max)			
Performance (HTTP)	80 Mbps	200 Mbps	500 Mbps	800 Mbps	Hardware Dependent			
Local Storage Capacity	1x 1TB	8 TB	4x 1 TB (6 TB Max)	4x 2 TB (16 TB Max)	60 GB (2 TB Max)	60 GB (4 TB Max)	60 GB (6 TB Max)	60 GB (8 TB Max)

FortiDB
Database activity monitoring and vulnerability assessment

	FDB-400C	FDB-1000D	FDB-2000B
Max DB Instances	10	30	60
Local Storage Capacity	1 TB	4 TB (8 TB Max)	1 TB (6 TB Max)

Also Available

FortiBridge Failopen Appliance

FortiClient Host based Security Client

FortiToken 2 Factor Authentication Token

AscenLink Link Load Balancer

FortiVoice Secure VoIP Solution

FortiCamera Network-based Video Security

FortiExtender 3G/4G WAN Extender

FortiDNS Secure DNS Server

This document is provided as a convenient comparison of Fortinet products and services. The datasheet for any product or service can be found on www.fortinet.com should be consulted for the most updated specifications.

PROMTX-2014-R22-FEB

Notizen

Oberberg-Online
Informationssysteme GmbH

Oberberg-Online
Informationssysteme GmbH
Dr.-Ottmar-Kohler-Str. 1
51643 Gummersbach

Tel.: +49-2261-9 15 50-0
Fax: +49-2261-9 15 50-99

ENUM: +49-2261-70 75 93
SIP: 49180512578100 77@4voip.de
http://www.oberberg.net
vertrieb@oberberg.net

FORTINET®

Oberberg Online