

MEHR SICHERHEIT UND PRODUKTIVITÄT
APPLIKATIONSKONTROLLE

WHITE PAPER



Inhaltsverzeichnis

Management Summary	3
Die Applikationen-Evolution	3
Protokolle der Applikationen	4
Entwicklung von Applikationen	4
Nutzung von Applikationen	5
Tabelle Applikationen	6
Einschränkung der Anwenderrechte	7
Mehr als nur Security: Applikationskontrolle	7
Applikationskontrolle + AntiVirus	8
Applikationskontrolle + Web Filter	8
Die Fortinet-Lösung: Integrierte Sicherheit ohne Kompromisse	9
Die wesentlichen Komponenten	9
Fazit	11

Management Summary

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.

Applikationskontrolle stellt ein Werkzeug zur Verfügung, welches 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 Anwendungsverhaltens und beeinflusst so im positiven Sinne die Bandbreite, Performance, Stabilität und Zuverlässigkeit sowie die Compliance der IT-Infrastruktur.

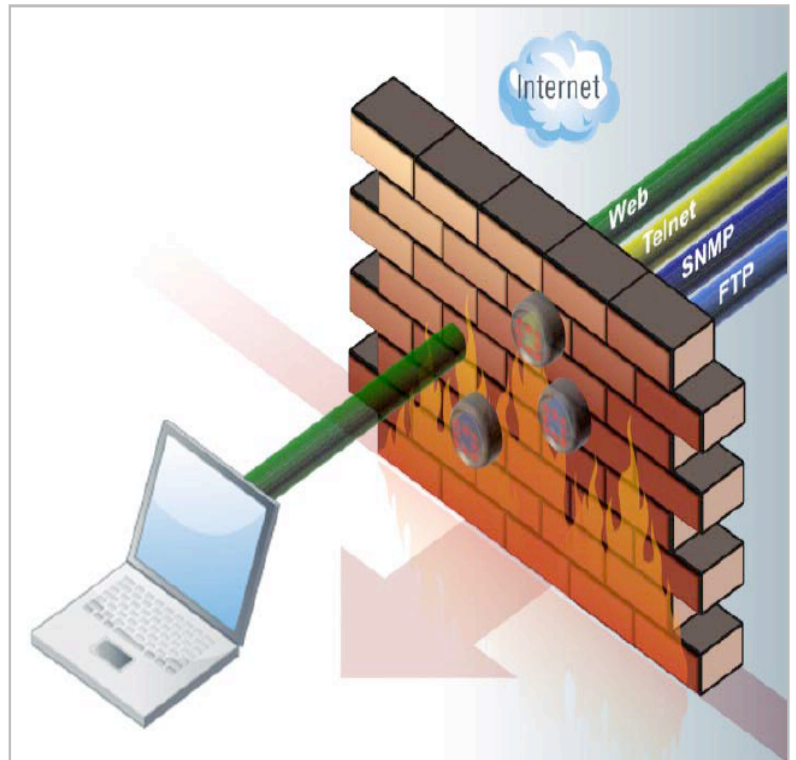
Die Applikations-Evolution

Netzwerk-Sicherheit erfordert in dem Maße zusätzliche Aufmerksamkeit, wie IP basierende Verbindungen die Kommunikation verändern. Unternehmensnetze geraten in Abhängigkeit von einer ständig wachsenden Zahl von Protokollen, inkl. HTTP und P2P, die von Business- und z.T. auch Non-Business Anwendungen verwendet werden. Anwender haben vermehrt Zugriff auf Applikationen bzw. können diese aus dem Internet laden, die sie für persönliche Zwecke nutzen, wie z.B. Web Email, Instant Messaging, kostenlose VoIP Telefonie, Browser Toolbars und diverse Social Media Anwendungen wie etwa Twitter oder Facebook. Mitarbeiter sind es gewohnt, mit diesen Applikationen zu arbeiten und nicht selten nutzen und installieren sie sie auch auf ihren dienstlich genutzten PCs bzw. Laptops. Die Popularität vieler dieser Anwendungen hat Unternehmen dazu gebracht, diese für Marketing- und

Werbe-Zwecke intensiv zu nutzen – und somit auch den eigenen Mitarbeitern den Zugang zu gestatten. Weiterhin werden wichtige Unternehmensdaten über entsprechende Web-Applikationen, vermehrt auch von außen, zugänglich gemacht – und es ist kaum noch managebar, wer auf welche Anwendungen und Daten von wo aus Zugang haben darf. Es sind oft nicht mehr nur die Mitarbeiter, sondern auch Kunden, Partner, Lieferanten, Franchiser, Freelancer usw. die bestimmte Zugriffsrechte benötigen.

Üblichweise versuchen Unternehmen über herkömmliche Firewall-Systeme eine erste Abwehrkette zu errichten – am Netzwerk-Perimeter, also am Übergang zwischen internem und externem Netz. Auf diese Weise wird zu regeln versucht, welche Art von Datenverkehr passieren darf und welche Ports – und somit Applikationen bzw. Protokolle – blockiert werden sollen. Beispielsweise können FTP-basierende Anwendungen durch das Sperren der Ports 20 und 21 für ausgehenden Verkehr unterbunden werden.

Durch die steigende Vielfalt von Applikationen und deren Kommunikation unter- und Integration ineinander entstehen in hohem Tempo neue Bedrohungen, die über die Anwendung den Weg vorbei an der Firewall finden. Einige Gründe für solche Verwundbarkeiten seien hier genannt:



Protokolle der Applikationen

Viele Anwendungen in großen Unternehmen sind extrem weit entwickelt und in der Lage, dynamische Services und dynamische Inhalte zur Verfügung zu stellen. Sie kommunizieren untereinander über eine Vielzahl von Protokollen wie z.B. HTTP, häufig genutzte oder auch proprietäre – und verhindern so, dass statische Regelwerke die Nutzung solcher Anwendungen sinnvoll steuern können.

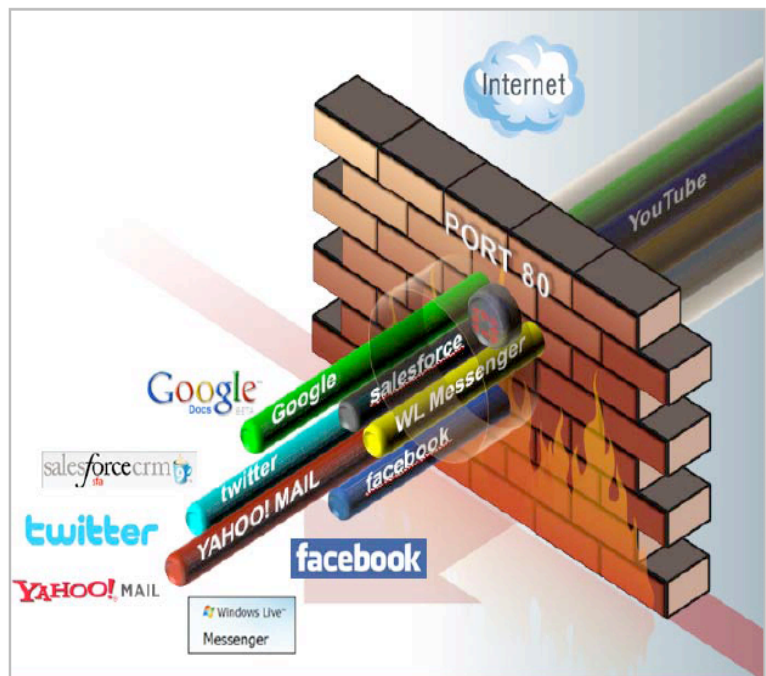
Entwicklung von Applikationen

Die rapide Entwicklung und Adaption von Web 2.0 Features auch in Enterprise Applikationen hat dazu geführt, dass die Nutzung von Web-Browsern als Plattform breite Akzeptanz in solchen Anwendungen gefunden hat. Noch vor wenigen Jahren machte die Entwicklung von Applikationen unternehmens-spezifische Anwendungen und damit auch entsprechende proprietäre Protokolle notwendig – die mit statischen Regelwerken kontrollierbar waren.

Nutzung von Applikationen

Das Hosting der Applikationen bietet heutzutage vielfältige Möglichkeiten. Unternehmen können das Hosting selbst betreiben, sie können einen Application Service Provider (ASP) nutzen, virtuelle Umgebungen schaffen – oder eine beliebige Kombination dieser Möglichkeiten zur Anwendung bringen. In jedem Fall wird es zunehmend schwieriger, Applikationen zu kontrollieren und gutartige oder schädliche Inhalte zu unterscheiden.

Das HTTP Protokoll stellt die größte Herausforderung im Bereich Regel-Durchsetzung und Applikations-Kontrolle dar. Es repräsentiert heute beides – den „Highway“ für unternehmenskritische Anwendungen ebenso wie das beliebteste Transportmedium für viel Arten von Angriffen und Malware. Die ständig wachsende Zahl verbundener Standorte (Niederlassungen ebenso wie mobile Geräte) und der Anwender (inkl. Partner, Kunden, Lieferanten, Freelancer usw.) sind abhängig von HTTP-basierenden Applikationen. Diese Abhängigkeit von HTTP-Traffic ermöglicht applikations-basierenden Angriffen klassische Firewall-Mechanismen zu unterlaufen, da diese nicht in der Lage sind, zwischen legitimen und schädlichen Inhalten zu unterscheiden. Die Grafik zeigt, dass das Sperren des Ports 80 (für HTTP) nicht möglich ist, da viele Anwendungen genau auf diesem Weg erst nutzbar sind.



Die Auswirkungen fehlender Applikationskontrolle erstrecken sich jedoch nicht allein auf die Möglichkeit, Unternehmensnetze anzugreifen bzw. zu infizieren. Neben der Tatsache, dass hier Löcher in die klassischen Schutzmaßnahmen gerissen werden, können sie sich nachteilig auf die operativen Ausgaben und damit auf den Kapitalbedarf auswirken.

- ❑ Anwender werden von ihrer produktiven Tätigkeit abgehalten (Chatrooms wie Google.Talk, MSN, ISQ, etc.)
- ❑ Zusätzliche Bandbreite wird verbraucht (BitTorrent, eDonkey, YouTube usw., TV-Streaming)
- ❑ Das Unternehmen wird weiteren Sicherheits-, Zuverlässigkeits- und Compliance-Risiken ausgesetzt (Remote Desktop, PCAnywhere, VNC)

Die folgende Tabelle illustriert, in welcher Weise Applikationen, die in 18 Kategorien aufgeteilt wurden, das Unternehmensnetzwerk beeinflussen.

Applikations-Kategorie	Beispiel-Anwendungen	Auswirkungen		
		Produktivitäts-verlust	Bandbreiten-Verbrauch	Sicherheits-/ Zuverlässigkeits-/ Compliance-Risiko
Instant Messaging	AIM, Google.Talk, MSN, QQ, Yahoo	Ja	Ja (Voice/Video)	Ja
Peer-to-Peer (P2P)	BitTorrent, Edonkey, Gnutella, Kazaa, Skype	Ja	Ja	Ja
Voice over Internet Protocol (VoIP)	H.245, MGCP, Net2phone, Netmeeting, SIP.TCP	Ja	Ja	Ja
File Transfer	FTP, HTTP.Audio, HTTP.EXE, RapidShare, YouSendIt		Ja	Ja
Video/Audio Streaming	Itunes, Peercast, PPStream, Quicktime, RealPlayer	Ja	Ja	Ja
Internet Proxy	Ghostsurf, Hamachi, HTTP.Tunnel, Tor.Web.Proxy, Ultrasurf	Ja	Ja	Ja
Remote Access Connection	Gotomypc, MS.RDP.Request, PCAnywhere, Teamviewer, VNC.Request			Ja
Spiele	AIM.Game, KnightOnline, MSN.Game, PartyPoker, Second.Life, WorldofWarcraft	Ja	Ja	Ja
Web Browser Toolbar	Alexa.Toolbar, AOL.Toolbar, McAfee.SiteAdvisor, MSN.Toolbar, Yahoo.Toolbar	Ja		Ja
Datenbanken	DB2, MSSQL, MySQL, Oracle, Postgres, Sybase			Ja
Web-Email	AIM.Webmail, Gmail, Hotmail, MySpace.Webmail, Yahoo.Webmail	Ja		Ja
Web	Amazon, Ebay, Facebook, Google.-Safe.Search.Off, Myspace, Wikipedia	Ja	Ja	Ja
Protokoll-Befehle	FTP.Command, HTTP.Method, IMAP.Command, POP3.Command, SMTP.Command			Ja
Internet Protokoll	ICMP, IGMP, IPv6, L2TP, RDP, RSVP			Ja
Netzwerk Dienste	LDAP, MSRPC, RADIUS, SSH, SSL, Telnet			Ja
Enterprise Anwendungen	Centric.CRM, IBM.Lotus.Notes, Salesforce, SugarCRM, Webex.Weboffice			Ja
System Updates	Adobe.Update, Apple.MacOS.Update, McAfee.Update, Microsoft.Update, TrendMicro.Update			Ja
Netzwerk Backup	Big.Brother, CA.MQ.Backup, Ibackup, IBM.Tivoli.-Storage.Manager, Rsync		Ja	Ja

Anmerkung: Weitere Informationen, inklusive einer Datenbank mit Applikations-Suchfunktion finden sich unter www.fortiguard.com

Einschränkung der Anwenderrechte

Unternehmen, die die Bedrohungen und Auswirkungen der o.g. Phänomene erkannt haben, führen mehr oder weniger strenge Richtlinien zur Nutzung von Endgeräten und/oder Anwendungen ein, um das Risiko für das Unternehmen zu reduzieren. Unglücklicherweise gibt es jedoch eine Reihe von technischen und politischen Aspekten, die die Einhaltung solcher Regelwerke erschweren.

Technisch betrachtet sind viele Firewall und IPS Systeme nicht in der Lage, zuverlässig zwischen den Anwendungen zu unterscheiden, die über das HTTP-Protokoll getunnelt werden. Viele dieser Applikationen wurden inzwischen derart weiterentwickelt, dass sie automatisch bestehende Schutzmaßnahmen (z.B. Port-Sperren) umgehen können – BitTorrent verwendet z.B. Port-Hopping, andere Applikationen tunneln anstelle von HTTP via SSL oder P2P. Web Filter können zwar den Zugriff auf bestimmte Webseiten verhindern, nicht jedoch das Starten von Web-Applikationen von diesen Seiten. Außerdem haben Anwender inzwischen Wege gefunden, WebFilter durch Einsatz von Proxies, wie etwa GhostSurf oder Hamachi, zu umgehen.

Diese Proxies erlauben nicht nur anonymes Surfen, sie gestatten auch den Zugriff auf gesperrte Webseiten, über die zumeist nicht gesperrten Proxy-Seiten. Unternehmen mit hochsensiblen Daten und Prozessen, die auf hohe Verfügbarkeit und Zuverlässigkeit setzen müssen, verwenden viel Zeit und Geld darauf, die ausgeklügelten Tricks und Strategien, die interne IT-Sicherheit zu umgehen, zu verhindern. . Derartige Gegenmaßnahmen verschlingen so Budget, das eigentlich für die Weiterentwicklung der IT-Infrastruktur geplant war – und wirken sich oft auch negativ auf die Produktivität der User aus.

In vielen Unternehmen ist es nicht ohne erheblichen Aufwand möglich, bestehende Arbeitsverträge hinsichtlich der (privaten) Nutzung des Internets während der Arbeitszeit zu verändern. Darüberhinaus belegen Studien, dass die Produktivität von Mitarbeitern, denen Internetzugang auch für nicht-dienstliche Zwecke zur Verfügung steht, produktiver sind, wenn sie eine – wenn auch zeitlich begrenzte – Möglichkeit haben, im Internet zu surfen. In USA spricht man vom sogenannten Workplace Internet Leisure Browsing (WILB) .

In jedem Fall stehen IT-Administratoren vor dem Problem, Bandbreite nach Business und Non-Business Applikationen vergeben zu müssen – was zu unterscheiden ohne adäquate Mittel jedoch oft nicht möglich ist.

Mehr als nur Security: Applikationskontrolle

Applikationskontrolle überwindet all diese Beschränkungen und Probleme, in dem sie Mittel bereitstellt, die Applikationen erkennen und deren Nutzung im Detail kontrollieren können – auch dann, wenn diese non-standard Ports verwenden oder über gängige oder auch weniger gängige Protokolle getunnelt werden. Dies geschieht durch die Analyse des applikations-spezifischen Paket-Verhaltens sowie eines umfangreichen Protokoll-Decodings. Eine herkömmliche Firewall kontrolliert den Datenstrom basierend auf Port- bzw. Service-Kontrollmechanismen.

Applikationskontrolle setzt auf dynamische Untersuchung der Daten und ermöglicht überdies die Anwendung weiterer Kontrollen, wie etwa Bandbreitenvergabe pro Applikation oder Zeitfenster bzw. –konten für deren Nutzung. Überdies kann sogar innerhalb von Applikationen ein Teil deren Funktionalität eingeschränkt werden, z.B. die Nutzung von Facebook, aber das Unterbinden von Facebook Chat oder das Nutzen von Google.Docs, aber das Unterbinden von Google.Talk.

Applikationskontrolle ergänzt somit die Funktionalität von Firewall- und IPS-Mechanismen um eine granulare Steuerung von Anwendungen und Protokollen. Somit wird die maximale Nutzbarkeit von Applikationen bei minimalem Risiko erzielt. Derartige Regeln zur Nutzung können bis auf Anwenderebene und selbstverständlich auch Geräte- oder Abteilungs-bezogen erstellt werden.

Es ist wichtig, Applikationskontrolle 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 sogenannten 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. Sie beeinflussen oft auch negativ die Gesamt-Performance des Netzwerks, da durch diese Vorgehensweise Pakete mehrfach analysiert werden – oder im schlimmsten Fall sogar Paketinformationen für eine sinnvolle Analyse gar nicht mehr zur Verfügung stehen.

Unternehmen müssen also darauf achten, eine voll und nahtlos integrierte Applikationskontrolle zu etablieren, um nicht nur deren umfängliche Wirksamkeit sicherzustellen, sondern auch um laufende und künftige Kosten für Betrieb, Troubleshooting und Updates so gering wie möglich zu halten. Diese Strategie wird von einer Gartner-Studie gestützt, nach der 2010 nur noch ca. 10% aller Security-Bedrohungen Nischen-Lösungen erfordern – verglichen mit früheren Studien, die in 2005 noch ca. 80% solcher Point-Solutions als erforderlich betrachteten.

Als Beispiel für die Bedeutung einer Integration von Applikationskontrolle in ein Multi-Layer-Security System seien folgende zwei Szenarien beschrieben:

Applikationskontrolle und AntiVirus

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

Applikationskontrolle und Web Filter

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

Die Fortinet Lösung: Integrierte Sicherheit ohne Kompromisse

Fortinet bietet eine Alternative zu den übrigen isolierten Lösungsansätzen: Durch den Einsatz von FortiGate-Appliances erhalten Unternehmen integrierte, umfassende und hoch-performante Security, die die Kontrolle des gesamten Datenstroms mittels AntiVirus, Web Filter, IPS, Firewall, VPN, DLP und SSL Inspection ebenso übernimmt, wie den Schutz vor ungewollten und die Kontrolle von zulässigen Applikationen – und das, ohne die Netzwerk-Performance zu beeinträchtigen. Durch den Einsatz von ASIC-Technologien, also speziellen Chipsets, die rechenintensive Aufgaben der Security-Module übernehmen und somit deutlich beschleunigen, heben sich FortiGate-Appliances von anderen Lösungen ab, die auf modifizierten Standard-Betriebssystem oder Standard-Prozessoren basieren.

Die gesamte integrierte Hardware- und Software-Architektur von FortiGate-Systemen wurde speziell für hoch-performante Content-Analysen oder für Application-Level-Security entwickelt, die Multi-Gigabit-Performance bereitstellen, wie sie am Perimeter, in Unternehmens-zentralen oder Rechenzentren erforderlich sind.

Die beiden wesentlichen Komponenten dieser Serie sind:

1. FortiOS

FortiOS ist das modulare Security-Betriebssystem aller FortiGate-Lösungen. Es stellt neben den einzelnen Security-Engines Schnittstellen für das System-Management sowie zu den vorhandenen Prozessoren (ASICs) bereit. Unternehmen haben die freie Wahl, einzelne Security-Module zu aktivieren oder aber das gesamte Feature-Set einer umfangreichen UTM-Suite zu nutzen. Über die FortiGuard-Services werden die FortiGate-Systeme in Echtzeit auf den jeweils aktuellen Stand gebracht und schützen somit zuverlässig auch gegen neueste Bedrohungsszenarien. FortiOS 4.2 stellt folgende Security-Engines zur Verfügung:

-  Firewall
-  VPN (IPsec und SSL)
-  Dynamisches Routing
-  AntiVirus/AntiMalware
-  URL-Filter
-  AntiSpam
-  Applikationskontrolle
-  Intrusion Prevention (IPS)
-  Data Loss Prevention (DLP)
-  Endpoint Security (NAC)
-  SSL Inspection
-  Wireless Controller (für FortiAP WLAN Access Points)

2. FortiASIC

FortiASIC ist die Grundlage der hochperformanten Fortinet-Security-Technologie. FortiASICs repräsentieren eine Familie von anwendungsspezifischen Prozessoren, die als Netzwerk- oder Content-Prozessor in Kooperation mit einem Standard-Prozessor rechenintensive Security-Services, wie etwa AntiVirus oder IPS, außerordentlich beschleunigen. Durch diese Hardware-Unterstützung stellen FortiGate-Lösungen maximale Übertragungsraten bis in den Multi-Gigabit-Bereich zur Verfügung, die in den grossen Unternehmen benötigt werden, um höchstmögliche Security zu etablieren und Performance-Einbrüche zu vermeiden. Durch Einsatz der FortiASICs, die mit der patentierten Fortinet Content Pattern Recognition Language (CPRL) arbeiten, stehen unabhängig vom Einsatz nur eines oder aller Security-Services, jederzeit ausreichende Leistungsreserven zur Verfügung.

FortiOS 4.0. Applikationskontrolle: Security PLUS

Fortinet FortiOS 4.0. ist die Grundlage aller Funktionen der FortiGate-Familie, angefangen von Kernel-Funktionen bis hin zu umfangreichen Security-Processing-Features wie Applikationskontrolle. Wie nahezu alle übrigen Security-Funktionen nutzt auch Applikationskontrolle die schon lange vorhandenen FortiOS Features wie etwa die IPS-Scan-Engine und IPS-Signaturen oder den Proxy-Support. Applikationskontrolle ergänzt das FortiOS um eine dynamische Application Identification Engine, die Anwendungen anhand ihres Verhaltens erkennt. Somit ist die Möglichkeit des Schutzes gegen Applikations-Schwachstellen und plattform-unabhängige Angriffen ebenso gewährleistet, wie die Abwehr von plattform-spezifischen Bedrohungen, gegen die typischerweise IPS-Mechanismen greifen.

Folgende Applikationskontroll-Funktionen sind ab FortiOS 4.0 in allen FortiGates integriert:

- ❑ Port-Unabhängige Erkennung: Die Erkennung von Anwendungen, die sich nicht der Standard-Ports bedienen (z.B. HTTP Port 80 oder SSL Port 443) oder SSL MS SGQ Datenbanken, die nicht Port 1443 nutzen.
- ❑ Erkennung von Tunneling: Erkennung von Applikationen, die andere Anwendungen als Tunnel benutzen, z.B. BitTorrent oder Skype via HTTP.
- ❑ FortiGate Applikations-Datenbank: Eine in derzeit 18 Kategorien gegliederte Datenbank von z.Zt. 1100 Applikationen, die dynamisch über FortiGuard-Services aktualisiert wird.
- ❑ Granulare Kontrolle: Erstellung von Regelwerken für die Nutzung von Applikationen bis auf User-ID, Abteilung oder Geräte-Typ.
- ❑ Kundenspezifische Anpassung: Je nach Regelwerk, kann für bestimmte User/Gruppen das Applikations-Verhaltens angepasst werden und die Nutzung und die Eigenschaften von Anwendungen definiert werden. Dazu zählen: Blockieren, Erlauben, Bandbreiten-Management, Sperren einzelner Befehle, wiez.B PUT bei FTP,. Für bestimmte Services können Einschränkungen fest gelegt werden; File Transfer in Instant Messaging, oder z.B. Facebook ohne Chat.

- ❑ Einfachstes Management: Durch Integration in das FortiOS Management Interface besteht die Möglichkeit der Kombination von Policies über Engines (FW, VPN, IPS, AV usw.) hinweg.
- ❑ Flexibles und umfangreiches Reporting: Mit Hilfe des FortiAnalyzers Auswertung der Nutzung (Art, Dauer, User) von Applikationen; Standard-Reports, die auch für Audits nutzbar sind und kontinuierliche und automatisierte Analyse des Applikations-Verhaltens

Fazit

Das breite Spektrum von Applikationen, wie es heutzutage in Unternehmen anzutreffen ist, stellt eine wesentliche Herausforderung für die Durchsetzung von Security-Regelwerken dar. Klassische Security-Mechanismen wie Firewall oder Web Filter allein genügen nicht, um die dynamischen und multi-protokollbasierenden Applikationen sicher zu kontrollieren und zwischen erlaubten und schädlichen Inhalten, die diese austauschen und übertragen, zu unterscheiden. Ungewollte oder schadhafte Applikationen führen überdies zu einer Minderung der Produktivität und übermäßigem Bandbreitenverbrauch sowie zu instabilen Systemen, Prozessen und Endgeräten – und oft auch zu Compliance-Problemen.

Unternehmen benötigen Multi-Layer Security-Funktionen wie AntiVirus/AntiMalware, IPS, Web Filter und Applikations-Kontrolle, um komplementäre und sich gegenseitig „überlappende“ Schutzebenen wirksam gegen die von Applikationen ausgehenden Bedrohungen einzusetzen. Die nahtlose und effektive Integration dieser Sicherheits-Module ist nur innerhalb einer einzigen Plattform sinnvoll möglich, die überdies noch die Kosten für den Betrieb senkt und Fehl-Bedienungen oder unsinnige Regelwerke über viele Plattformen hinweg vermeiden hilft.

Fortinets Familie von FortiGate-Appliances trägt diesen Anforderungen in höchstem Maße Rechnung, in dem sie basierend auf einem dedizierten Security-Betriebssystem (FortiOS) und unterstützt von anwendungsspezifischen Prozessoren (FortiASICs) höchste und granular konfigurierbare Sicherheit bei höchster Performance bereitstellt.

Security ohne Kompromisse!

Copyright© 2010 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions. Network variables, different network environments and other conditions may affect performance results, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding contract with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.