VERTICAL® LINK NEXT GENERATION FIREWALL

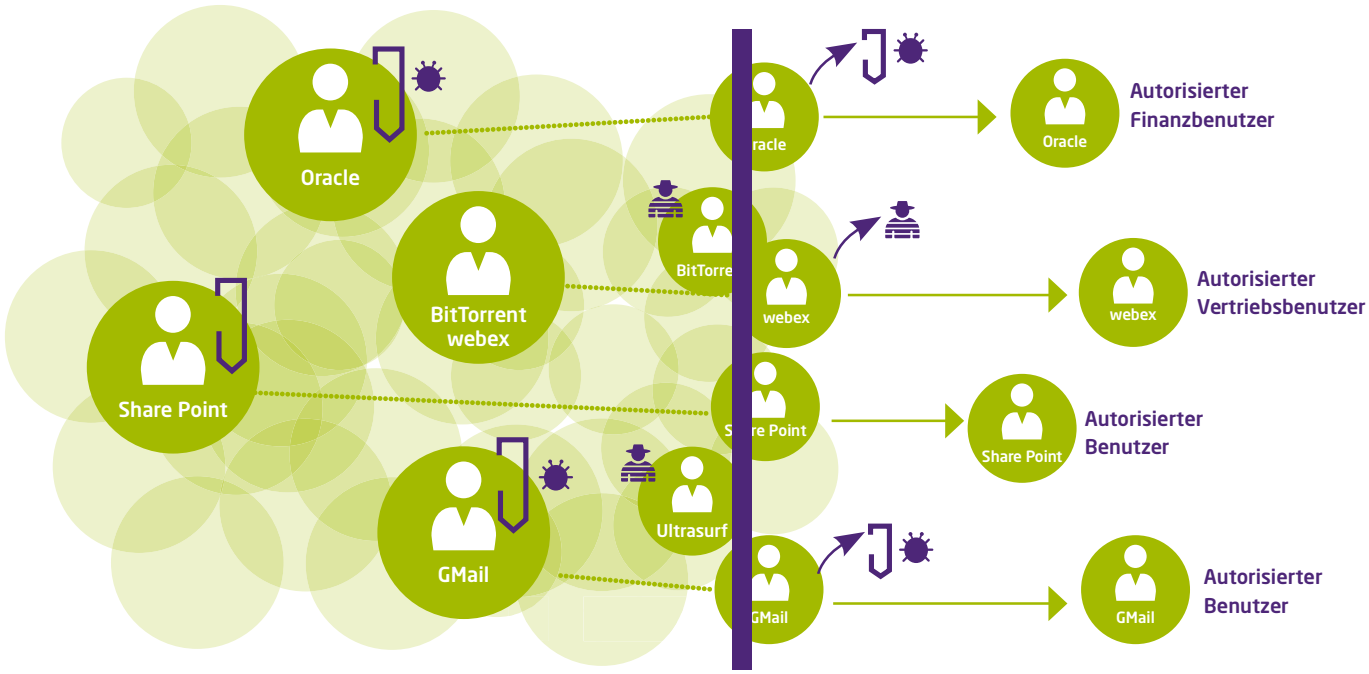
Stand: Juni 2017

vertical® Next Generation Firewall

Sicherheit in einer digitalen Welt

Die Informationstechnologie ist ein Biotop, das ständiger Evolution unterliegt. Anwendungen, das Benutzerverhalten und Netzwerkinfrastrukturen ändern sich, Sicherheitsmaßnahmen und Bedrohungen befinden sich – wie in der freien Natur – im ständigen Wettlauf. Was gestern noch eine erfolgreiche Strategie war, ist heute überholt. Jüngst hat es die traditionelle Port-basierte Firewall erwischt: Zunehmend können Benutzer von überall her und über unterschiedlichste Endgeräte auf alle Arten von Anwendungen zugreifen. Oft müssen sie das sogar, weil ihre Arbeit das notwendig macht. Zudem erfordert die Digitale Transformation die sichere Integration von Partnern und Kunden über Apps und Webportale. Virtualisierung, Mobilität und Cloud-basierte Plattformen sind im Vormarsch. Es wird Zeit darüber nachzudenken, wie man die Chancen der Digitalisierung mit dem Schutz von Unternehmensdaten und geistigem Eigentum vereinbaren kann.

Einen guten Ansatz bieten Firewalls der jüngsten Generation. Diese sogenannten Next Generation Firewalls ermöglichen es Unternehmen, ihren Usern unabhängig vom Standort sicheren Zugriff auf Anwendungen einzuräumen und ihre Geschäfts- und Sicherheitsrisiken zu minimieren.



Was ist anders?

Herkömmliche, auch „Stateful Inspection Firewall“ genannte Firewall-Technologie legt als einziges Filterkriterium Ports und Protokolle zugrunde. Infolgedessen kontrolliert sie lediglich, welche Geräte mit dem eigenen Netzwerk kommunizieren dürfen, nicht aber die Art der Kommunikation, d. h. was das Gerät will, tut und welche Daten ausgetauscht werden. So kommuniziert eine Applikation wie Skype beispielsweise über Port 80 nach außen, wobei dieser eigentlich für das Abrufen von Websites über http freigegeben wurde und nicht für die Video-Telefonie und Filesharing. Die Next Generation Firewall analysiert im Gegensatz zur klassischen Port-basierten Variante das Applikationsverhalten. Sie ermöglicht es nicht nur, den individuellen Benutzer anhand einer User-ID zu identifizieren, sondern untersucht auch die verwendeten Applikationen und kontrolliert die ausgetauschten Inhalte. Das macht es möglich, viel spezifischere Sicherheitsrichtlinien zu definieren und umzusetzen.

Ihr Schutz als monatlicher Service

vertical bietet Ihnen den Schutz von Next Generation Firewalls auf Basis der Marktführertechnologie von Palo Alto Networks als Full-Service an. Im Gegensatz zum klassischen Kaufmodell, müssen Sie nicht in Hard- und Software investieren und diese dann selbst administrieren, sondern bekommen den „Next Generation Firewall“-Service zur monatlichen Pauschale schlüsselfertig von vertical geliefert. Das alles funktioniert Plug’n’Play, wird aus dem vertical Operations Center zentral betrieben, Tag und Nacht überwacht und proaktiv gewartet, so dass Ihr Unternehmen immer bestmöglich geschützt ist.

Die Kehrseite der Digitalisierung

Über all die Segnungen, die das Phänomen der Digitalisierung in seiner Gesamtheit mit sich bringt, darf man die immanenten Bedrohungen nicht übersehen. Wir haben uns die potenziellen Auswirkungen und Risiken von Anwendungen auf das Unternehmen und dessen Prozesse einmal genauer angeschaut und sind auf die folgenden gefährdeten Bereiche gestoßen:

Compliance

Die meisten Unternehmen müssen zahlreiche behördliche und geschäftliche Regulatorien beachten. In den USA sind dies z. B. GLBA, HIPAA, FD, SOX, FISMA und PCI. Auch in Europa gibt es eine lange Liste: Basel II, Datenschutzrichtlinien (Arbeitnehmer-datenschutz, Auftragsdatenschutz), stringente Richtlinien zur Meldepflicht beim Datenverlust in Deutschland (Novelle II des Bundesdatenschutz-gesetzes BDSG, §42a) sowie Regelungen zum Arbeitnehmerschutz (Jugendarbeitsschutzgesetz, Beschäftigtenschutzgesetz), dem Telemediengesetz, sowie dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG).

Die meisten dieser Regelungen dienen der Absicherung der betrieblichen und finanziellen Risiken eines Unter-nehmens sowie dem persönlichen Datenschutz von Kunden und Mitarbeitern. Viele Anwendungen für die private Nutzung bergen das Risiko von Datenlecks und stellen so nicht unerhebliche und potenziell teure Compliance-Risiken dar.

Produktivität

Wenn Mitarbeiter Systeme und Ressourcen missbräuchlich nutzen, kann das ihre Produktivität und damit die des gesamten Unternehmens einschränken. Zwei unerwünschte Auswirkungen liegen auf der Hand: Private Anwendungen wie WhatsApp, Facebook, persönliche E-Mails und privates Surfen während der Arbeitszeit können Mitarbeiter verlocken, ihre beruflichen Aufgaben zu vernachlässigen.

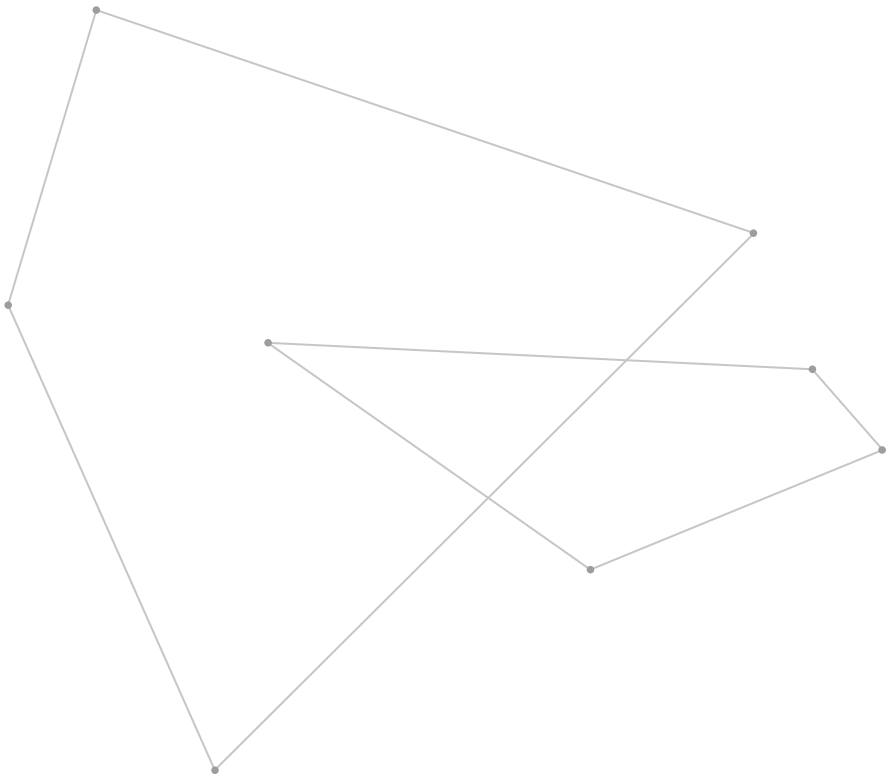
Sind solche private Anwendungen wie YouTube oder Audio-Streaming auch noch mit hohem Datenverkehr verbunden, können sie so viel Bandbreite belegen, dass legitime oder sogar Business-kritische Anwendungen nur noch eingeschränkt verfügbar sind.

Datenverlust

Das Risiko von Datenverlust betrifft den herkömmlichen Bereich der Informationssicherheit in Bezug auf Diebstahl, Preisgabe oder Zerstörung von Daten. Betroffen sind öffentliche und private Daten ebenso wie das geistige Eigentum des Unternehmens oder seiner Geschäftspartner. Hierbei kommen verschiedene Bedrohungen zum Tragen, darunter immanente Sicherheitsrisiken privater Anwendungen wie Facebook oder Webmail. Zugleich können Würmer, Trojaner und Spyware Unternehmensdaten an unbefugte Dritte preisgeben oder im Fall von Ransomware unwiderruflich verschlüsseln.

Web 2.0 Plattformen

Moderne Web 2.0 Internetplattformen bringen interaktive Möglichkeiten mit sich. Für den Anwender leicht zu bedienen sind diese Portale verlockend und werden teils ungefragt verwendet. So sind in solchen Webseiten Datenaustausch-, WebConferencing- und Informationsveröffentlichungs-funktionalitäten integriert. Für klassische Sicherheits-lösungen kaum ersichtlich, verlassen Informationen unkontrolliert das Unternehmen und der Anwender ist sich keiner Schuld bewusst, handelte nicht mit schlechter Absicht, dennoch ist der Schaden entstanden. Deshalb ist es unerlässlich mit so genannten Data Loss Prevention (DLP) Maßnahmen zu verhindern, dass unternehmensinterne Daten versehentlich an Externe versendet werden oder unbemerkt das Unternehmen verlassen.



Next Generation Firewalls von Palo Alto Networks

2005 gründete der Security-Visionär Nir Zuk Palo Alto Networks mit der Mission, die Firewall neu zu definieren und wieder zu dem zu machen, was sie einmal war: Zum wichtigsten strategischen Sicherheits-Baustein im Netzwerk. Seither hat sich Palo Alto zu einem der Marktführer im Firewall-Bereich entwickelt. Dies bestätigen erschienene Gartner Studien, in denen Palo Alto Networks ein Top-Ranking im Bereich der Next Generation Firewalls erhalten hat. Dabei wurde das Konzept der Firewall mit zahlreichen marktführenden Innovationen bereichert, zum Beispiel mit einer beispiellosen Transparenz und Kontrolle über Anwendungen und deren Inhalte – und zwar basierend auf Usern und nicht nur IP-Adressen.

Kontrolle über Anwendungen, Benutzer und Inhalte

Die akkurate Identifizierung des Netzwerkverkehrs ist Grundvoraussetzung für das Funktionieren jeder Firewall und deshalb die Basis jeder Sicherheits-Policy. Die Next Generation Firewalls von Palo Alto Networks bieten nicht nur die vollständige Kontrolle über Ports, IP-Adressen und Pakete, sondern machen auch Anwendungen, Benutzer und Inhalte transparent wie nie zuvor. Dazu verwenden sie drei einzigartige Identifizierungstechniken: App-ID, User-ID und Content-ID. Anders als viele andere Sicherheits-Infrastrukturen verfolgen diese nicht den „Alles-oder-Nichts“-Ansatz herkömmlicher Port-Blocking-Firewalls, sondern erlauben stattdessen die sichere Nutzung von Anwendungen auf der Basis eines intelligenten, geschäftsrelevanten Konzepts.

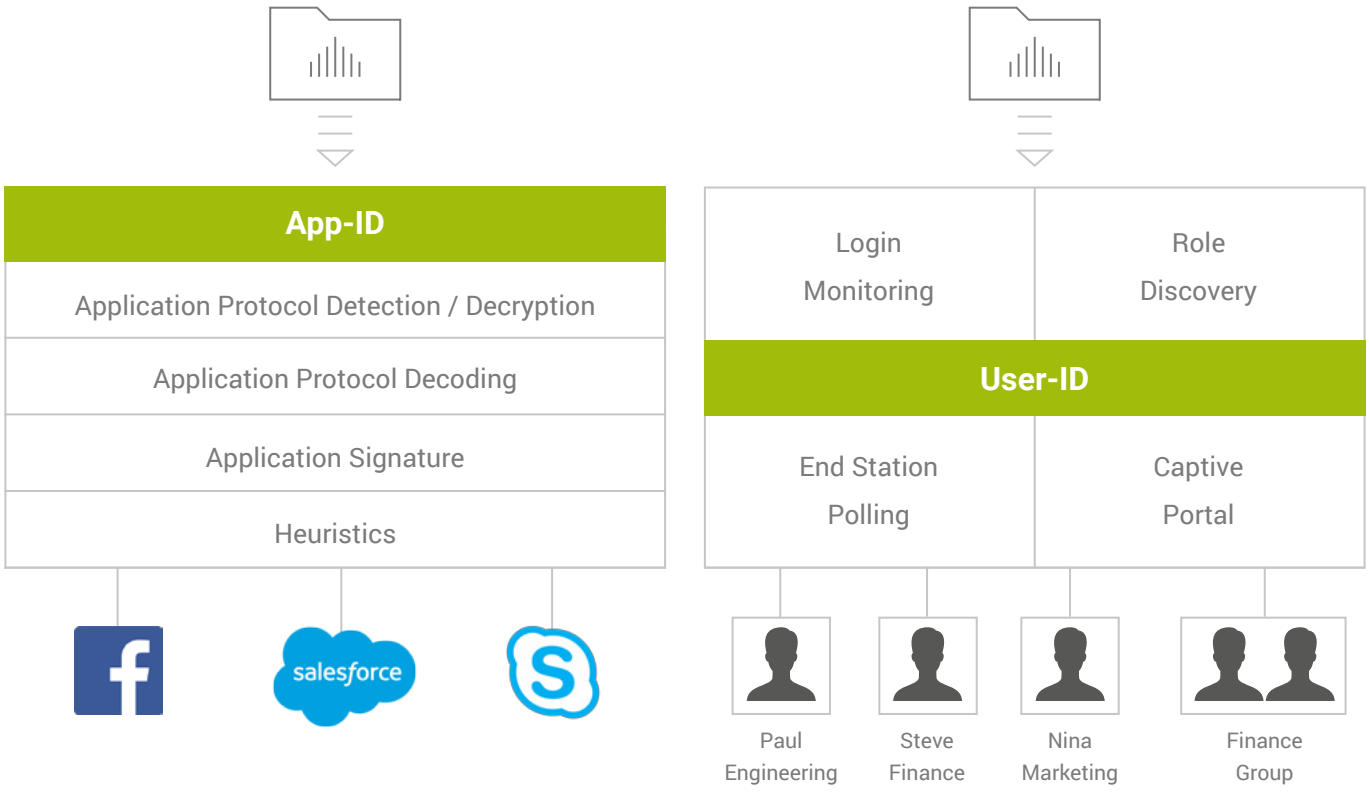
Die Grundsätze der Lösung

Technologie und Module

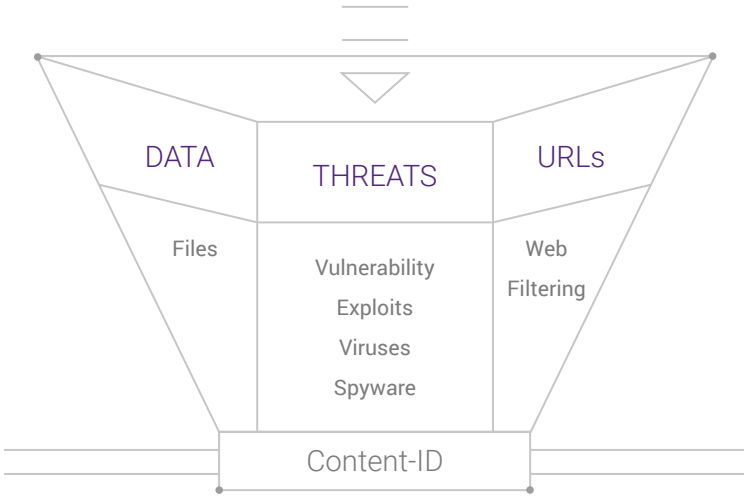
Next Generation Firewalls von Palo Alto Networks ermöglichen die sichere Aktivierung von Anwendungen, Benutzern und Inhalten im gesamten Unternehmen. Dazu wird eine Kombination von Technologien und Diensten in einer zweckorientierten Hardwareplattform eingesetzt.

App-ID: Mithilfe mehrerer Verkehrsklassifizierungs-mechanismen kann App-ID eine Anwendung genau definieren, sobald sie die Firewall passiert. Dabei spielt es keine Rolle, welchen Port die Anwendung verwendet oder welche Umgehungsmethode eingesetzt wurde. Die Identität der Anwendung wird zur Grundlage für alle Entscheidungen hinsichtlich der Sicherheitsrichtlinien. Unbekannte Anwendungen werden für die Analyse und systematische Verwaltung kategorisiert.

User-ID: Ermöglicht dem Unternehmen, personen- und gruppenbezogene Richtlinien für den Anwendungs- und Dienstzugriff zu erstellen. User-ID lässt sich nahtlos in eine Vielzahl von Verzeichnisdiensten wie Microsoft Active Directory, eDirectory und Open LDAP sowie Ter-minal Services (Citrix und Microsoft Terminal Services) integrieren. Durch die Integration in Microsoft Exchange und weitere Verzeichnisdienste, können Unternehmen ihre Richtlinie auf Apple Mac OS X-, Apple iOS- und UNIX-Benutzer ausdehnen, die sich in der Regel außerhalb der Domäne befinden.



Content-ID: Verhindert Schwachstellen, Malware und den damit verbundenen Befehls- und Steuerungsverkehr mithilfe eines einheitlichen Signaturformats und einer Single-Pass-Scanning-Engine, bei zugleich minimaler Latenz. Somit wird der Schutzbereich traditioneller AntiVirus-, AntiSpyware-, IDS- und IPS-Systeme abgedeckt. Der Bedrohungsschutz wird im vollständigen Anwendungs- und Protokollkontext verwendet, um sicherzustellen, dass Bedrohungen unabhängig von der eingesetzten Umgehungstechnik erkannt und blockiert werden. Die URL Filterung ermöglicht eine Richtlinienkontrolle der Web-Aktivitäten, während durch die Datei- und Datenfilterung nicht autorisierte Datentransfers kontrolliert werden. Die Funktionalität wird durch eine verhaltensbasierte Botnetz-Analyse abgerundet.



Features im Überblick

• Antivirus	• Modem Malware Protection
• Application Visibility	• Networking
• Centralized Management	• Policy Control
• Data Filtering	• Redundancy & Resiliency
• Decryption	• URL Filtering
• Device Management	• Virtual Systems
• IPS	• Virtualization Security
• IPv6	• VPN

Die Plattformen

vertical Next-Generation Firewall Small

auf Basis von Palo Alto PA-220

Die PA-220 schützt vor Cyber Attacken und ermöglicht ein sicheres Arbeiten für Zweigniederlassungen und kleine Unternehmen. Die neue PA-220 bietet vollständige PAN-OS-Fähigkeiten in einem kleinen Desktop-Footprint mit erhöhter Portdichte. Dieses Produkt verfügt über eine integrierte Ausfallsicherheit dank zweier Netzteilanschlüsse und Hochverfügbarkeitsunterstützung für Aktiv/Aktiv und Aktiv/Passiv. Sie bietet eine interaktive Darstellung und Kontrolle von Anwendung, Inhalten und Benutzern mit einer App-ID-Performance von 500 Mbit/s. Zusätzlich sorgt das lüfterfreie Design für einen geräuscharmen Betrieb. Durch den Einsatz von SSDs werden bewegliche Teile vermieden.

- 500 Mb/s Firewall-Durchsatz (aktivierte App-ID)
- 150 Mb/s Durchsatz bei Bedrohungsabwehr
- 100 Mb/s IPSec VPN Durchsatz
- 64,000 max. Anzahl an Sitzungen
- 4,200 neue Sitzungen pro Sekunde
- 250 IPSec VPN tunnels/tunnel interfaces
- 3 virtual routers
- 15 security zones
- 250 max number of policies

Hersteller-Datenblatt:
https://www.paloaltonetworks.de/content/dam/pan/de_DE/assets/pdf/datasheets/pa-200/pa-200-ds_DE.pdf

Serviceoptionen:

Bereitstellung als Full-Service zu monatlich: 133,00 €

+ URL Filtering 19,00 €

+ Hochverfügbarkeits-Option 62,00 €

Laufzeit 36 Monate

Alle Preise zzgl. MwSt. Preisänderungen vorbehalten.

vertical Next-Generation Firewall Medium

auf Basis von PaloAlto PA-850

Die Firewall der neuen Generation PA-850 schützt vor Cyber Attacken und ermöglicht ein sicheres Arbeiten in mittelständischen Firmen. Die neue Architektur liefert eine 1,9 Gbit/s App-ID-Performance und 780 Mbit/s Threat-Prevention-Performance. Die Plattform nutzt mehrere CPU-Kerne und 8 GB Speicher. Die PA-850 verfügt über eine redundante Stromversorgung für optionale Hardware-Ausfallsicherheit.

- 1.9 Gb/s Firewall-Durchsatz (aktivierte App-ID)
- 780 Mb/s Durchsatz bei Bedrohungsabwehr
- 500 Mb/s IPSec VPN Durchsatz
- 192,000 max. Anzahl an Sitzungen
- 9,500 neue Sitzungen pro Sekunde
- 1000 IPSec VPN tunnels/tunnel interfaces
- 5 virtuelle Router
- 40 Sicherheitszonen
- 1,500 max number of policies

Hersteller-Datenblatt:
https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-800-series-datasheet

Serviceoptionen:

Bereitstellung als Full-Service zu monatlich: 360,00 €

+ URL Filtering 92,00 €

+ Hochverfügbarkeits-Option 325,00 €

Laufzeit 36 Monate

Alle Preise zzgl. MwSt. Preisänderungen vorbehalten.

vertical GmbH
Otto-Volger-Straße 3 - 5 a/b
65843 Sulzbach
Hotline +49 6196 8017 0
Fax +49 6196 8017 299
www.vertical.de
info@vertical.de