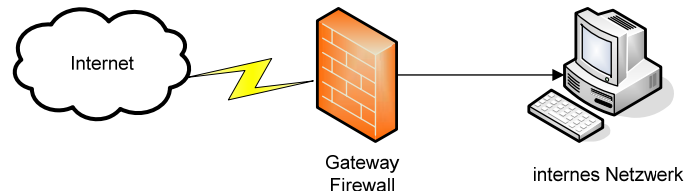


Infoblatt - Netzwerk – Security: Firewall / Virenschutz

Einer der Sicherheitstechnisch relevantesten Knotenpunkte in einem Netzwerk ist die Verbindung zum Internet (Gateway).

Deshalb bieten wir Lösungen an die genau an diesem Punkt eingesetzt werden (Firewall) und eine maximale Möglichkeit von Schutzarten/Schutzvarianten bieten.



Schutzarten/Schutzvarianten:

- IP Firewall** Klassische Firewall Lösung mit auf Policy (Regeln) basierten Routen (Wegen), die auf IP (Adresse) und Port (Bereich) Ebene reglementieren.
- IPS** Intrusion Detection/Prevention = Erkennung und Verhinderung unerlaubter Zugriffe.
- Virenschutz** Die Überprüfung auf Viren findet direkt am Gateway statt.
D.h. – die Identifizierung und Entfernung eines Virus findet statt bevor es ins Netzwerk zum Client gelangt (E-Mails, Dateien...).
- Spamschutz** Überprüfung sämtlicher E-Mails die durch das Gateway ankommen hinsichtlich der Herkunft und der Beschaffenheit auf „Spam“ (unerwünschte Mail) Verdacht.
- Web Filter** Durch eine Kategorisierung der Webinhalte kann der Zugriff auf bestimmte Bereiche des Internets gesteuert bzw. reglementiert werden (z.B.: gefährliche Inhalte, illegale Inhalte...)

Da aber teilweise der kontrollierte Zugriff von außen über das Internet notwendig ist (Filialvernetzung, Teleworker, mobiler Außendienst,,), bieten unsere Firewalls natürlich auch entsprechende gesicherte Lösungen an.

Zugriffs-/Verbindungsvarianten:

- VPN Site** Verschlüsselte fixe Verbindung von z.B. 2 Filialen über eine gesicherte VPN (Virtual Private Network) Verbindung (2 Standorte – 2 Internetanbindungen – 2 Firewalls).
- VPN Client** Fixe Anbindung von Teleworkern oder mobilen Außenstellen (PC oder Notebook mit VPN Client Software greift via Internet verschlüsselt auf Zentrale zu).
- WEB/HTTPS** Zugriff auf bestimmte interne Netzwerkdienste über einen beliebigen Internetzugang (Internetcafe, Hotel...). Die Absicherung erfolgt durch eine Sichere Übertragung (HTTPS) und einer Authentifizierung an der Firewall (Anmeldung, Benutzername, Kennwort, Einmalpasswörter, Token, Radius...).

Virenschutz am Client:

Ein Virenschutzlösung am Gateway kann natürlich nur Gefahren erkennen die über das Internet versuchen in das Netzwerk zu gelangen.

Für eine Absicherung gegen Angriffe von innen (CD, DVD, USB Stick...) bzw. als zweite Sicherheitsebene bieten wir zentrale Antivirenlösungen für die internen Clients an (Management Software am Server, Virenschutz Software am Client, Server aktualisiert die Antivirendatenbanken via Internet und verteilt sie an die Clients).