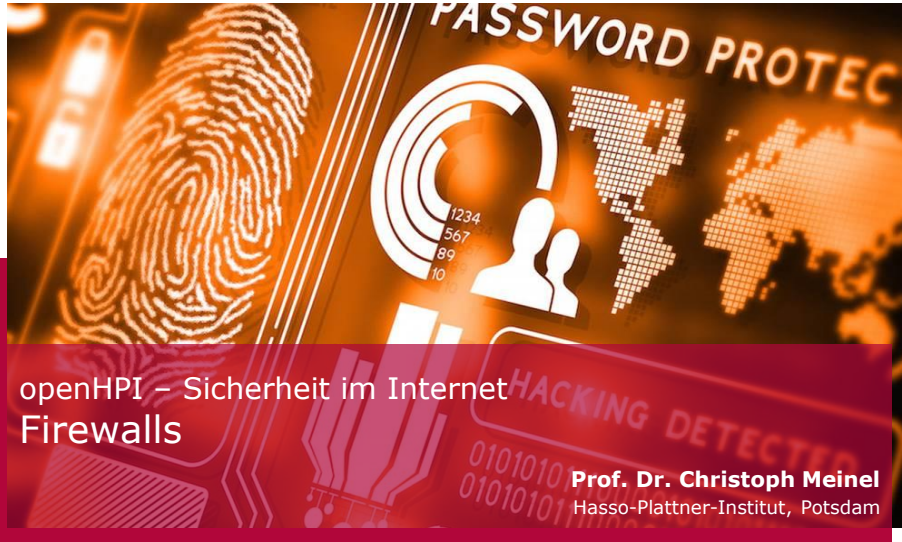




Firewalls

Firewalls sind Sicherungssysteme, die einen einzelnen Computer oder ein Rechnernetz vor **unerwünschten Netzwerkzugriffen** schützen

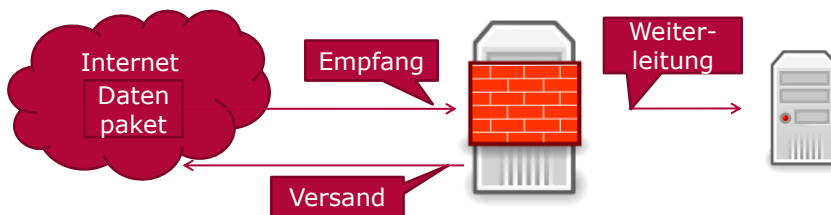
- Überwachen ein- und ausgehende Verbindungen und den darüber laufenden Netzwerkverkehr
- Können unautorisierte Verbindungsversuche unterbinden
- Bieten zusätzlichen Schutz gegen Angriffe, wie z.B.
 - Angriffe durch Backdoors und Botnets
 - Jeder dieser Angriffe erfordert eine Verbindung zum/vom Angreifer, die vorher unautorisiert hergestellt werden muss
 - Derartige Angriffe können verhindert werden oder ein Alarm kann ausgelöst werden

Firewall-Regeln definieren, unter welchen Umständen welche Verbindungen bzw. welcher Netzwerkverkehr zulässig bzw. nicht zulässig ist

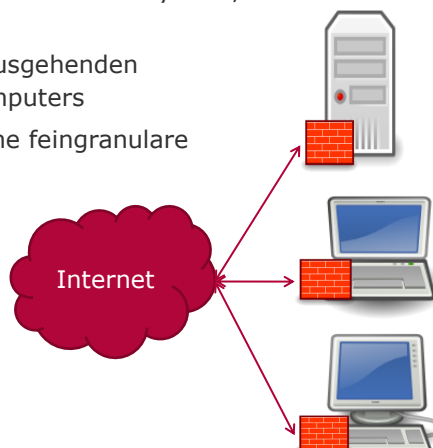
- Regeln können spezifisch für einzelne Protokolle, Ports, Ziel- und Quelladressen oder Programme formuliert werden
- Für jedes ein- und ausgehende Netzwerkpaket wird überprüft, ob eine Regel passt und angewendet werden muss
- Trifft eine Regel auf ein Netzwerkpaket zu, können verschiedene Aktionen ausgeführt werden
 - Paket kann erlaubt, weitergeleitet, modifiziert, verworfen oder geblockt werden, Warnung kann angezeigt werden, ...
- Zur Definition der Regeln sind Fachkenntnisse über die Verbindungen des Computers notwendig
- Fehlerhafte Definitionen können valide Verbindungen blocken

- Bei fehlenden Definitionen oder keiner passenden Regel kommt die **allgemeine Sicherheitsrichtlinie (Policy)** des Systems zur Anwendung
 - Sicherheitsrichtlinien schreiben vor, ob sonstige Verbindungen geblockt bzw. erlaubt werden oder ob eine Bestätigung des Nutzers erforderlich ist
- Firewalls können alle explizit erlaubten Verbindungen speichern und setzen für diese automatisch die Regeln um
- **Lokale Firewall** setzt die definierten Firewall-Regeln nur auf dem Computer um, auf dem sie installiert ist
- **Netzwerkfirewall** prüft den gesamten Netzwerkverkehr und ist typischerweise auf dem Verbindungsknoten zwischen einem lokalen Netzwerk und dem Internet installiert

- Regeln können in verschiedenen Stadien bzw. an verschiedenen Stellen der Paketverarbeitung angewendet werden
- Bei der Definition der Regeln ist das jeweilige Stadium anzugeben, in dem die Regel anzuwenden ist, z.B.
 - beim Empfang, Versand, Weiterleitung, vor dem Routen, ...
- Definierte Aktionen werden im jeweiligen Stadium ausgeführt



- **Lokale Firewall** agiert nur auf dem System, auf dem sie installiert ist
- Überprüft alle ein- und ausgehenden Verbindungen dieses Computers
- Erlaubt System-spezifische feingranulare Einstellungen
 - Warnungen und Paketblockierung gelten nur für das jeweilige System



- **Netzwerkfirewall** prüft sämtlichen ein- und ausgehenden Netzwerkverkehr und ist typischerweise auf dem Verbindungsknoten zwischen einem lokalen Netzwerk und dem Internet installiert
- Verbindungen innerhalb des Netzwerkes werden nicht überprüft, es sei denn, die Firewall fungiert als zentraler Verbindungsknoten
- Einstellungen betreffen alle Clients im Netzwerk
- Administration der Firewall-Regeln für das lokale Netzwerk wird dadurch vereinfacht

