

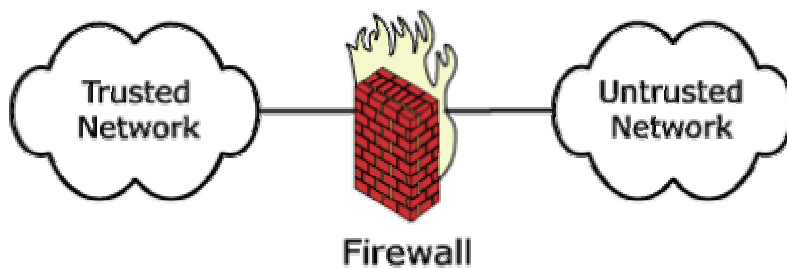
# Firewalls



von Sebastian Kleinschmager, Christian Borchardt, Timmy Metzler

## 1. Definition einer Firewall :

Eine Netzwerkfirewall ist ein System oder eine Gruppe von Systemen die den Zugang zwischen zwei Netzen kontrollieren - einem vertrauenswürdigen und einem nicht vertrauenswürdigen Netzwerk. Dafür werden vorkonfigurierte Regeln und Filter benutzt.



### 1.1 Positive Effekte :

Aussenstehende erhalten keinen Zugang zum Intranet.

Die User erhalten nur Zugang zu erlaubten Seiten bzw. keinen Zugang zu gesperrten.

Die Aktivitäten der User werden geloggt. Diese Informationen können dazu verwendet werden, um die Policies zu setzen. Die Firewall kann das Intranet vor anderen Netzen verstecken (z.B. Internet). Man muß nur an einer Stelle die Firewall konfigurieren – geringe Kosten, wenig Änderungen am bestehenden Netz. Firewalls können transparent implementiert werden, so dass die User im internen Netz nichts davon bemerken, es sei denn ein Service auf den sie zugreifen wollen ist blockiert.

### 1.2 Negative Effekte :

Eine Firewall kann ein „single point of failure“ sein, da der komplette Traffic, der zwischen den beiden Netzen läuft, zwangsmässig durch die Firewall muss. Fällt diese aus oder ist falsch konfiguriert, findet keine Kommunikation statt.

Eine Firewall mit für das gegebene Netz zu schwacher Hardware, die die Daten nicht schnell genug verarbeiten kann, verlangsamt die Datenübertragung, ist ein sogenannter Flaschenhals (bottleneck). Je nach Ausmass des Netzes und Typ der Firewall kann die Implementation und Wartung ein grosser administrativer Aufwand sein.

### 1.3 Wie arbeiten Firewalls ?

Die meisten Firewalls arbeiten nach dem Prinzip : Was nicht erlaubt ist, ist verboten.

Das ist eine vorbeugende Maßnahme gegen ungewollten /nicht autorisierten Zugang zum Intranet. Es muss vom Administrator jede Regel, die den Zugang erlaubt, manuell konfiguriert werden. Somit wird eine höhere Standardsicherheit gewährleistet. Diese Einstellung ist jedoch sehr einschränkend. Es dauert, ehe alle Berechtigungen richtig gesetzt wurden.

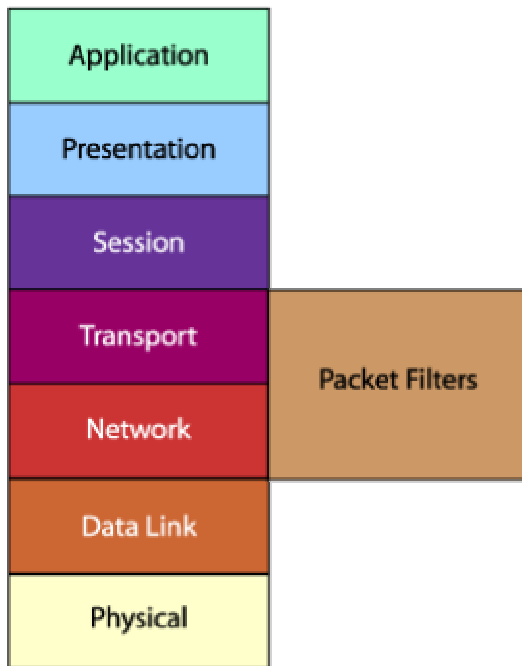
Die andere Lösung ist eine unsicherere Lösung. Ungewollter Zugang muss erst verhindert werden. Der Vorteil ist das der legitime Verkehr nicht leidet, da alles zugelassen ist.

Ungewollter Traffic muss manuell ausgesperrt werden, dabei kann leichter etwas übersehen werden.

## 2. Die verschiedenen Firewalltypen

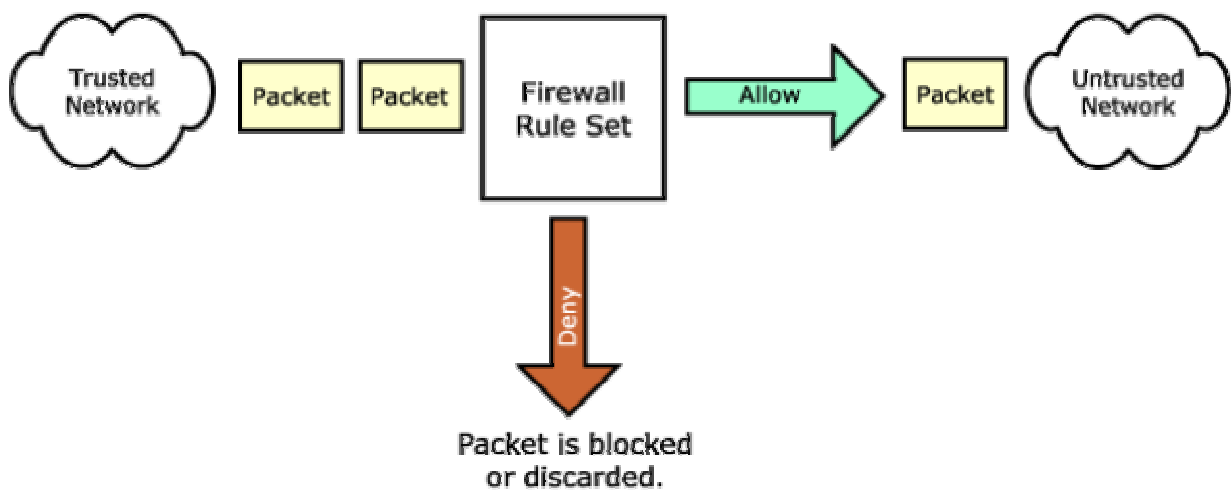
Es gibt 3 verschiedene Typen von Firewalls. *Paketfilter Firewalls*, *Stateful Firewalls* und *Application Gateways/Proxies*.

### 2.1 Packet filter Firewalls :



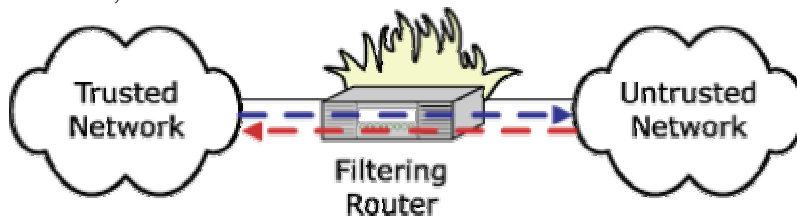
#### **2.1.1 Funktionsweise :**

Dieser Typ Firewall checkt die Headerinformationen jedes durchlaufenden Paketes mit den auf ihr konfigurierten Regeln und leitet entsprechend die Pakete weiter oder verwirft sie. Dabei werden folgende Informationen beachtet : Source und Destination IP-Adresse, Source and Destination Port und Layer 4 Protokoll (TCP oder UDP).



### 2.1.2 Vorteile :

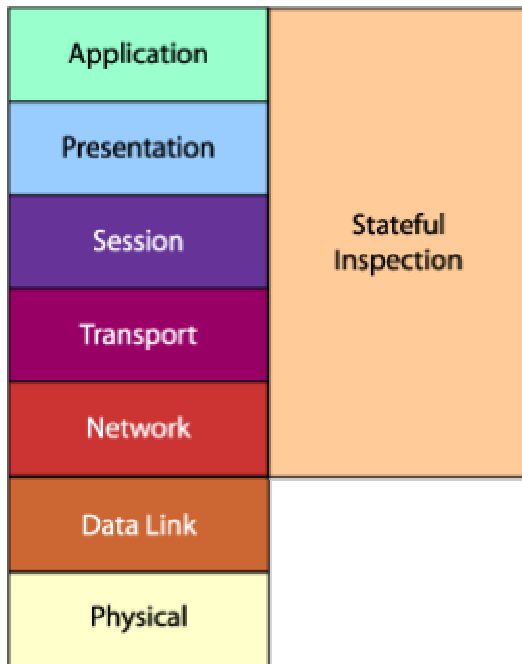
Schnell, da die Kontrolle nur auf den Schichten 3 und 4 des OSI-Modells stattfindet.  
Die Firewall behindert die Netzwerkperformance kaum, wird transparent implementiert.  
Die Firewall ist kostensparend. Die meisten Hardwarekomponenten enthalten diesen Typ Firewall, z.B. Router.



### 2.1.3 Nachteile :

Direkte Verbindung zwischen zwei Endpunkten ist erlaubt.  
Die Verbindung zwischen Client/Server wird nicht unterbrochen. Die Firewall ist schnell, basiert aber nur auf dem Prinzip "Alles oder Nichts". Ein offener Port lässt jeden Traffic durch, was die gesamte Sicherheit gefährdet.  
Die Definition der Filter und Regeln ist sehr komplex, da jeder Zugang einzeln konfiguriert werden muss.  
Das Testen dieser Firewall ist ein schwieriges Unterfangen, da die Ergebnisse irreführend sein können.  
Diese Firewall ist leichter zu umgehen, da nur der Paketheader geprüft wird. Auf Anwendungsebene ist die Firewall nutzlos. Anfällig für IP-Spoofing, Buffer Overruns, ICMP tunneling, Man-in-the-middle Attacken.

## **2.2 Stateful Inspection Firewalls :**



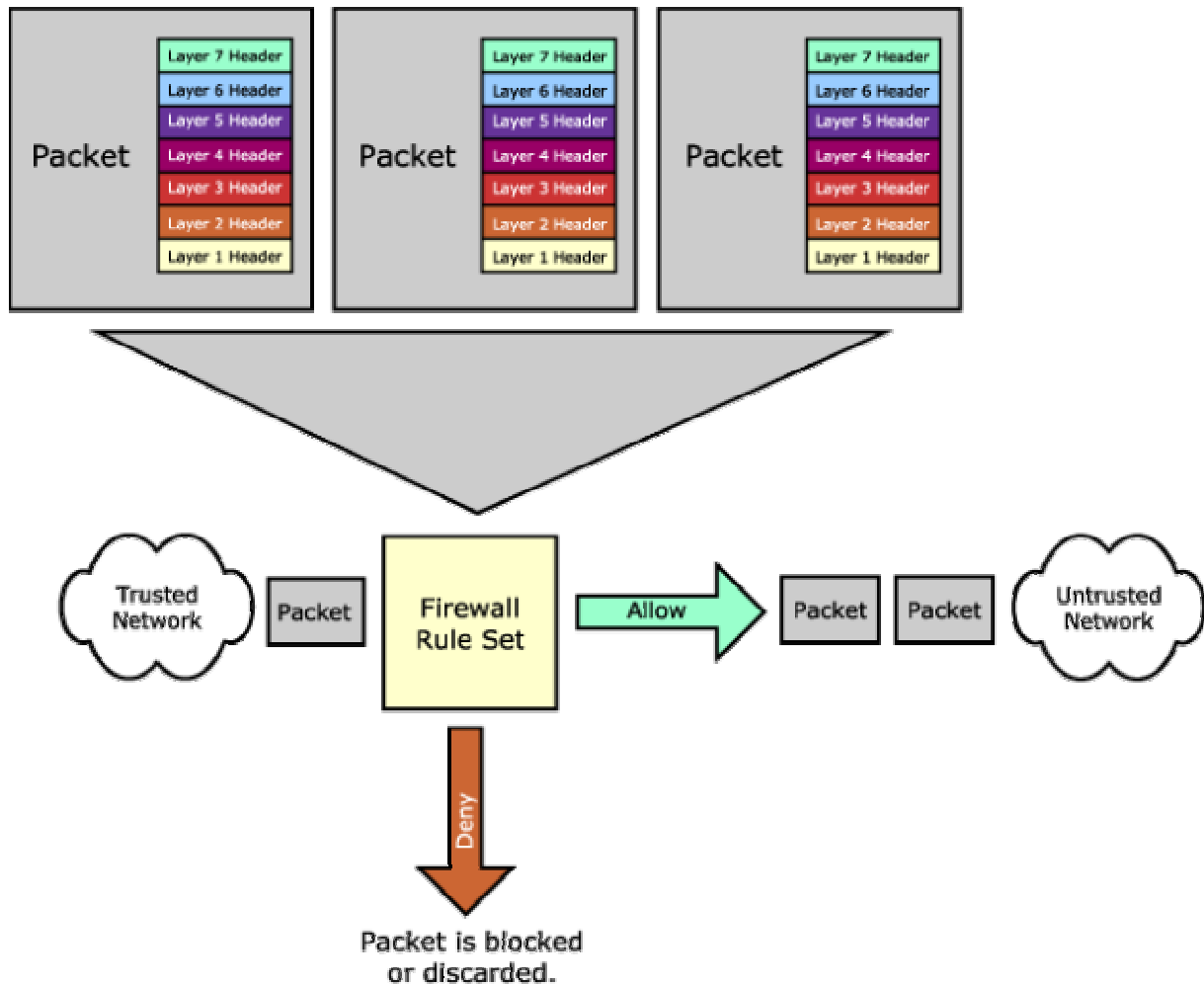
### **2.2.1 Funktionsweise :**

Basiert auf den Funktionen der Packet Filter Firewall.

Bei Paketen, die durch die Firewall gelangen, wird der Header gelesen und die Informationen in einer dynamischen Tabelle gespeichert. Die Pakete werden auch hier mit vorkonfigurierten Regeln verglichen und Entscheidungen werden aufgrund dieses Ergebniss getroffen.

Die Firewall überprüft im Gegensatz zur Packet Filter Firewall auch den Verbindungsstatus (connection state), um zu verifizieren, dass die Pakete zu einer gültigen Verbindung gehören.

Erweiterte Versionen von Stateful Firewalls überprüfen Pakete sogar bis auf Applikationsebene (content control). Sie setzen eingehende Pakete zusammen und prüfen die enthaltenen Daten.



### 2.2.2 Vorteile :

Wie Paketfilter, jedoch:

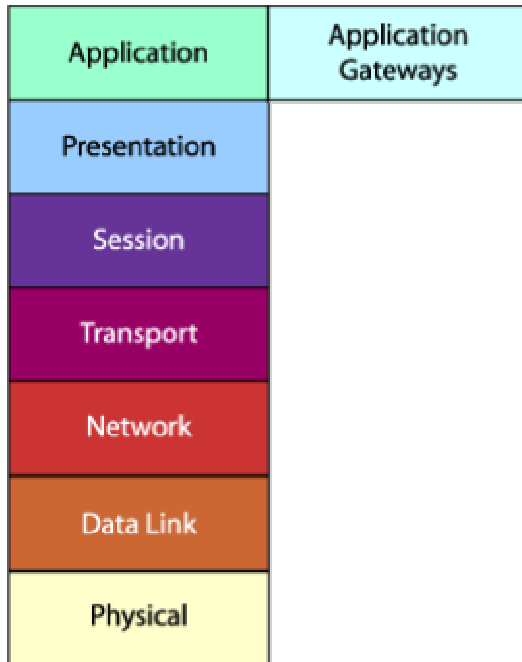
Sicherer, da die Headerinformationen gründlicher untersucht werden.

Die Protokolle werden hier auf Fehlverhalten überprüft.

### 2.2.3 Nachteile:

Die Regeln und Filter werden komplexer, schwieriger einzustellen, anfällig für Fehler und schwer zu testen.

## 2.3 Application Gateways/Proxies

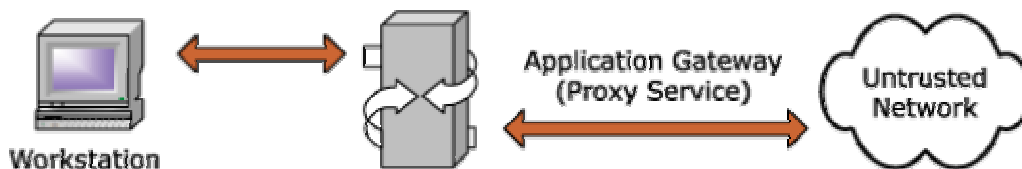


### 2.3.1 Funktionsweise :

Anders als die Packet Filter und Stateful Inspection Firewalls wird beim Application Gateway das Client/Server Modell gebrochen. Ein Application Gateway/Proxy besitzt 2 Netzwerkkarten und baut mit jedem Teilnehmer der Verbindung eine eigene End-zu-End Verbindung auf. Aufgrund dessen wird der Application Gateway/Proxy auch als Dual-Home Gateway bezeichnet. Die Application Gateway Firewall arbeitet auf OSI-Schicht 7.

Wenn ein Client aus dem eigenen Netz auf das externe Netz zugreifen will, greift er direkt auf das Application Gateway zu, wo zuerst geprüft wird ob die gewünschte Verbindung aufgebaut werden darf. Darf die Verbindung aufgebaut werden, wird eine Anfrage vom Proxy zur eigentlichen Destination gesendet. So entsteht niemals eine direkte Verbindung vom Client ins externe Netz.

Diese Art von Firewall kann sogar den Inhalt auf sehr genaue Informationen prüfen, z.B. ob eine E-Mail eine nicht erlaubte Datei enthält oder eine Webpage Java benutzt.



### 2.3.2 Vorteile :

Das interne Netz ist nach aussen hin nicht sichtbar.

Application Gateways haben die besten content filtering Methoden und bieten robuste Möglichkeiten der User-Authentifizierung. Dem Administrator stehen ausführliche Logging Informationen zur Verfügung.

### 2.3.3 Nachteile :

Application Gateways/Proxies bringen grössere Kosten mit sich und haben grössere Auswirkungen auf die Performance als andere Firewalls.

Jedes Protokoll benötigt eine eigene Applikation auf dem Proxy.

Die Clients im Netz müssen so konfiguriert werden dass sie den Proxy nutzen, ansonsten haben sie keinen Zugriff ins Netz.

Application Gateways/Proxies sind darauf angewiesen, auf ein sicheres Betriebssystem aufgesetzt zu werden.

Sie sind ausserdem anfälliger gegen DoS (Denial of Service) Attacken.

## 3. Firewall Technologien und Techniken

### 3.1 NAT :

Als NAT (Network Address Translation) bezeichnet man die Layer-3 Technik, mit der eine lokale IP-Adresse auf eine öffentliche IP-Adresse gemappt wird. Dies hat den Vorteil, dass der lokale Host nach aussen hin nicht direkt zugänglich ist, sondern nur über die öffentliche IP-Adresse der Firewall/des Routers.

NAT wird in folgende 3 Typen unterschieden:

1. Static NAT:

Beim statischen NAT wird einer nicht routbaren internen Host-IP-Adresse eine öffentliche routbare IP-Adresse zugeordnet (one-to-one-mapping).

2. Dynamic NAT:

Beim dynamischen NAT wird einer nicht routbaren internen Host-IP-Adresse eine öffentliche routbare IP-Adresse aus einem Adresspool zugeordnet. Besteht der Adresspool aus drei öffentlichen Adressen, so können drei Hosts im LAN gleichzeitig online sein.

3. NAT with overloading:

Beim NAT with overloading wird eine einzige öffentliche routbare IP-Adresse allen Hosts im LAN zugeordnet. Um die Pakete eindeutig zuzuordnen, wird die Portnummer verwendet. Man spricht dabei von Port Address Translation (PAT).

Die Kommunikationsverbindungen werden anhand der Portnummer unterschieden (>1024).

Beispiel:

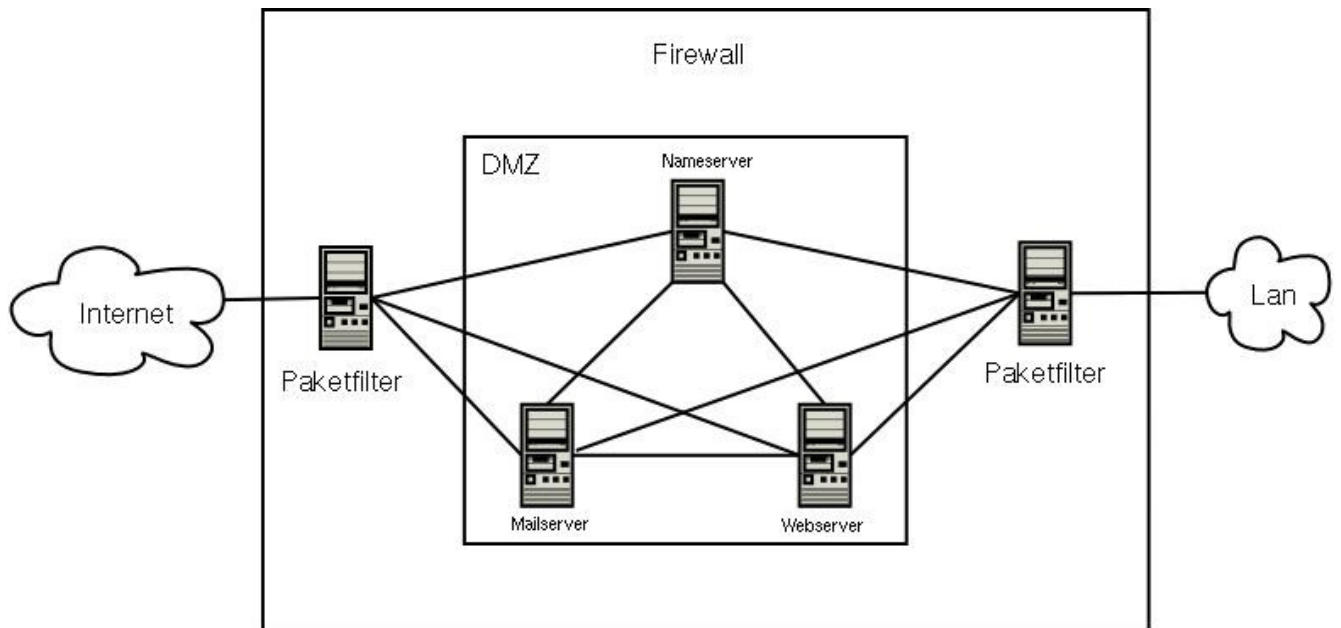
Inside Source:	Inside Destination:	Outside Source :	Outside Destination :
192.168.1.2.:2001	199.1.2.3:80	173.16.1.2:2001	199.1.2.3:80
-----PAT-----			

PAT (Port Adresstranslation) versucht immer die ursprüngliche Portnummer zu übernehmen. Ist diese bereits vergeben, wird die nächst höhere, freie Portnummer verwendet.

### **3.2 Firewall Appliance :**

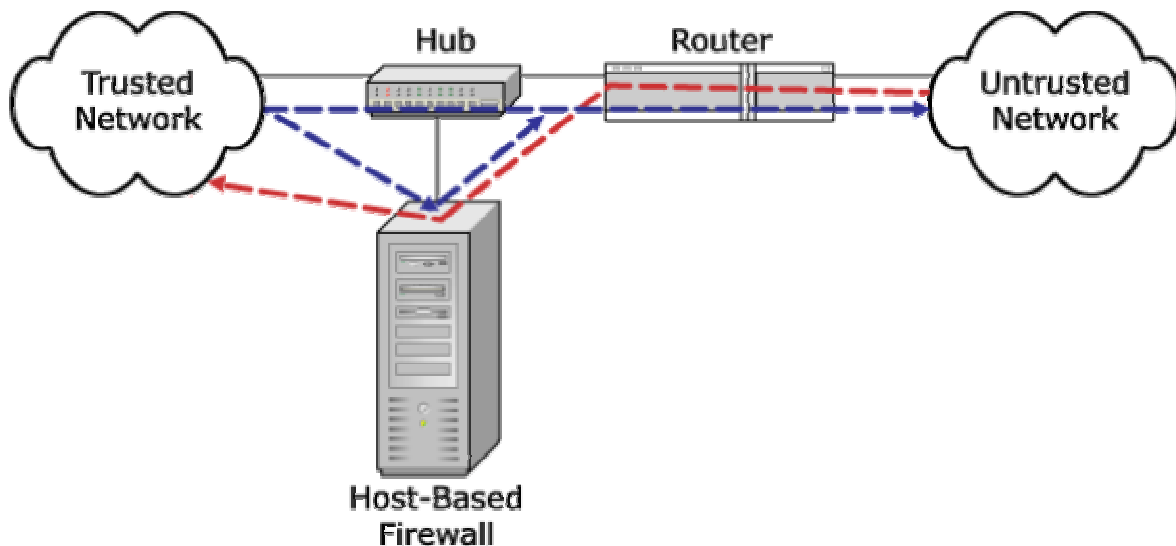
Eine Firewall ist typischerweise hinter dem Gateway (üblicherweise der Router). Diese Architektur ähnelt der Paket-Filter Router und der dual homed gateway Architektur, wobei der gesamte Traffic durch die Anwendung muss. In den meisten Fällen ist die Firewall bereits vorkonfiguriert. Meistens hat sie weitere Dienste wie Webserver und E-Mail-Server bereits implementiert. Da diese Firewall wenig aufwendige Konfiguration benötigt, wird sie oft damit geworben, dass sie viel simpler und einfacher zu benutzen ist. Einige Hersteller bieten sie als „plug-and-play“ Firewalllösung an.

### 3.3 DMZ :



Ein abgeschirmtes Subnetz oder DMZ (Demilitarized Zone) wird üblicherweise zwischen zwei Paketfilter Routern eingesetzt. Wenn diese Architektur benutzt wird, ist die Firewalllösung auf dem geschirmten Subnetz-Segment zusammen mit anderen Diensten.

### 3.4 Screened Host :



Der abgeschirmte Host wird normalerweise im vertrauten Netzwerk lokalisiert und wird geschützt vor dem nicht vertrauenswürdigen Netzwerk mit einem Paketfilter-Router. Der gesamte Verkehr, der durch den Paketfilter-Router läuft wird zum abgeschirmten Host weitergeleitet. Ausgehender Verkehr kann aber nicht zum abgeschirmten Host weitergeleitet werden. Dieser Typ von Firewall ist meistens Softwarebasierend und läuft auf einem universellen Rechner, auf dem eine sichere Version des OS läuft. Die Sicherheit wird hier auf dem Application Layer implementiert.