

# Konzepte von Betriebssystem-Komponenten:

## Denial of Service-Attacken, Firewalltechniken

Frank Enser  
[frank.enser@web.de](mailto:frank.enser@web.de)

08.07.2002

### 1. (D)DoS Attacken

#### 1.1.DoS Attacken

DoS steht für ‚Denial of Service‘ und bedeutet, dass z.B. ein Web-Server, nachdem er mit automatisierten Anfragen bombardiert wurde, die Vielzahl der Anfragen (Requests) nicht mehr abarbeiten kann und offline gehen muss. Die Angreifer sind nur sehr schwer auszumachen, weil sich der Weg der Daten effektiv verschleiern lässt.

Die Programme hierzu werden immer ausgefeilter und der Vormarsch der Breitband Internetzugänge (xDSL) trägt dazu bei, dass bereits solche Attacken im großen Stil möglich sind. Blitzkrieg, Fornax und Stacheldraht [1] sind nur drei der vielen DoS-Tools, welche bereits weitläufig im Internet kursieren.

#### 1.2.DDoS Attacken

Im Gegensatz zu den DoS-Attacken der ersten Generation, die einen Server von einem Computer aus angreifen, greifen die ‚Distributed Denial of Service‘ Attacken von vielen an das Internet angeschlossenen Computern ein einziges Ziel an.

In der Praxis bedeutet dies, dass ein Hacker zuvor mehrere (vielleicht sogar Hunderte) Computer kompromittiert (mittels Trojanischen Pferden) und dann von diesen Computern eine riesige Datenflut auf den Zielrechner lenkt. In den Logfiles des angegriffenen Webservers tauchen dann nur die IP-Adressen der vermeintlichen Angreifer-Computer und nicht die des tatsächlichen Angreifers auf.

#### 1.3.die verschiedene Arten von (D)DoS Angriffen [2]

##### 1.3.1. ‚Flood Attacken‘

Der Zielcomputer wird durch eine andauernde Flut von Anfragen überlastet. Entweder durch das Verbrauchen von CPU Zeit und/oder der Netzwerk Bandbreite.

##### 1.3.1.1. SYN Flood

Bei einem SYN Flood Angriff schickt der Angreifer IP Pakete mit falscher Absenderadresse (Spoofed IPs) und gesetztem SYN Flag. Dadurch wird dem Zielrechner ein Verbindungsaufbau vorgetäuscht und der Zielrechner schreibt einen Eintrag in seine Connection Table. Falls nun die Connection Table voll ist, werden keine neuen Verbindungen mehr angenommen und echte Verbindungen zurückgewiesen bis wieder Platz in der Connection Table ist (der Connection Timeout ist normalerweise 3min.).

##### 1.3.1.2. Smurf Attack

Bei einem Smurf Angriff sendet der Angreifer andauernd ICMP Echo Request (Ping) Pakete an die Broadcast Adresse eines Netzwerkes, wodurch alle Rechner dieses Netzwerkes ein ICMP Echo Reply Paket an die Source Adresse senden. Der Angreifer muss somit nur die IP des Zielrechners als die Source Adresse in die Pakete schreiben um dessen Netzwerkverbindung zu überlasten.

### 1.3.1.3. Fraggle oder UDP Flood Attack

Dieser Angriff basiert weitgehend auf dem Smurf Angriff nur werden bei diesem Angriff UDP Pakete verwendet.

### 1.3.1.4. ICMP Flood Attack

Dieser Angriff ist der einfachste. Der Angreifer sendet einfach ICMP Pakete und überlastet die Netzwerkverbindung des Ziels (dazu muss der Angreifer natürlich mehr Bandbreite als das Ziel haben).

## 1.3.2. 'Logic' oder 'Software' Angriffe

Dieser Typ von Angriffen nutzt Fehler in der Software des Zielrechners aus um ihn auszuschalten.

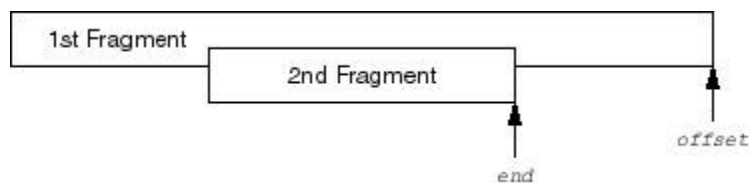
### 1.3.2.1. Ping of Death [3]

Bei diesem Angriff sendet der Angreifer ein überlanges ICMP Echo Request Paket (größer als 65536 Bytes), welches früher in vielen Betriebssystemen den Buffer für IP Pakete überlaufen ließ (da die maximale IP Paket Größe auf 65536 Bytes beschränkt ist - RFC-791) und die Rechner zum Absturz oder Reboot geführt hat.

### 1.3.2.2. Teardrop [4]

Dieser Angriff nutzt einen Fehler in älteren Windows Versionen (Win95, NT4) beim Zusammenfügen von IP Paket Fragmenten. Beim Eintreffen von Fragmenten werden bei allen Fragmenten (außer dem ersten) die IP Header entfernt und die Nutzdaten zusammengefügt. Bei der Teardrop Attacke werden falsche Fragment Offset Werte benutzt um das folgende Pakete vollständig in das vorhergehende Paket zu ,integrieren'. Dadurch wird der Kopierfunktion ein negativer Wert übergeben (zu kopieren = end – offset). Da die Kopierfunktion aber ein ,unsigned integer' erwartet, wird dadurch möglicherweise – je nach IP Implementation der Stack überschrieben, was wiederum zum Absturz des IP Moduls oder des ganzen Systems führt.

„Falsches Paket“ :



### 1.3.2.3. Land

Der Angreifer schickt ein Paket mit der gleicher Ziel- und Sourceadresse sowie gleichen Source- und Targetports. Einige ältere Systeme kommen damit nicht zurecht und stürzen ab oder rebooten.

### 1.3.2.4. Echo/Chargen [5]

Im Grunde genommen ist dieser Angriff eine Form des UDP Flood Angriffs. Der Angreifer sendet ein gefälschtes UDP Echo Request Paket (mit Source IP des Ziels) an den Port 19 (chargen) eines anderen Rechners. Dieser wiederum sendet ein Paket mit zufälligen Zeichenketten an den Echo Service Port des Zielrechners, der wiederum antwortet. Dadurch wird schnell die Bandbreite der Rechner ausgelastet.

## 2. Firewalltechniken

### 2.1. Was ist eine Firewall?

Eine Firewall ist, streng nach Definition, lediglich ein Filter welchen Netzwerkpakete beim Eintreffen oder Verlassen passieren müssen.

In der Praxis können Firewalls lediglich aus einem einzigen Rechner (sogenannte Single-Box-Architekturen) oder aus komplexen Geflechten aus überwachten Teilnetzen, Routern und Bastion-Hosts bestehen. Die Komplexität hat wiederum erheblichen Einfluss auf Konfigurierbarkeit und Sicherheit.

### 2.2. Firewall Konzepte [6] [7]

#### 2.2.1. Packet Filtering

Packet Filtering ist die einfachste Form eines Firewallsystems. Sie beschränken sich ausschließlich auf Schicht 3 des OSI/ISO Referenzmodells (Transportschicht) und können somit nur nach den Daten des IP Headers filtern (also nach Protokolltyp, Send- und Empfangsadresse, Port, Flags, ...).

Packet Filter Firewalls sind aufwendig zu installieren und zu warten. Jeder einzelne Verbindungstyp muss entweder explizit verboten werden (extrem unsicher) oder explizit erlaubt werden, was zur Folge hat, dass für jedes Protokoll mindestens 2 Filterregeln (je 1 Regel für die Eingehende und Ausgehende Verbindung) erstellt werden müssen (diese Ports sind damit aber immer geöffnet). Genaue Kenntnis des jeweiligen Protokolls ist daher unverzichtbar.

#### 2.2.2. Stateful Filtering (Circuit-level gateway)

Stateful Packet Filter (SPF) sind eine Weiterentwicklung der einfachen Packet Filter. SPFs besitzen zusätzlich intern eine Tabelle über alle offenen Verbindungen und ihrem Zustand.

Dadurch sind auch – im Gegensatz zu den einfachen Packet Filter - wirklich nur Ports ‚offen‘ welche auch gebraucht werden. Davon abgesehen ist die Konfiguration und Warten einfacher, da nur eine Filterregel pro Protokoll erstellt werden muss.

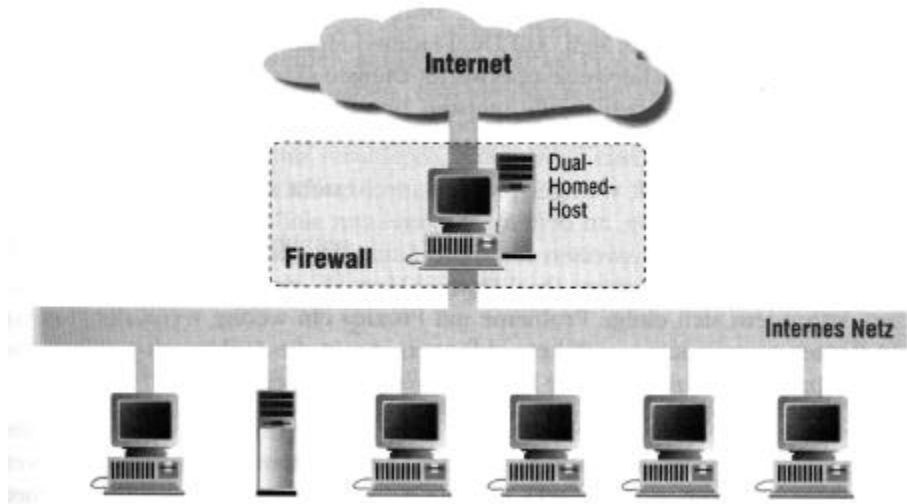
#### 2.2.3. Application Gateway (Proxy) [8]

Normalerweise besteht eine Verbindung zwischen Client und Server. Proxys verstehen sich als Vermittler und stehen zwischen Client und Server, wobei sie sich gegenüber dem Server als Client und dem Client gegenüber als Server ausgeben. Dadurch wird nie eine direkte Verbindung zwischen dem eigentlichen Client und Server aufgebaut. Dies bedeutet eine enorme Erhöhung der Sicherheit, da der Proxy auf der vierte Schicht des OSI/ISO Modells aufsetzt und somit die Daten der Pakete interpretieren und gegebenenfalls einzelne Kommandos sperren kann bevor sie den Server erreichen.

## 2.3. Typische Firewall Architekturen

### 2.3.1. Dual-Homed-Host

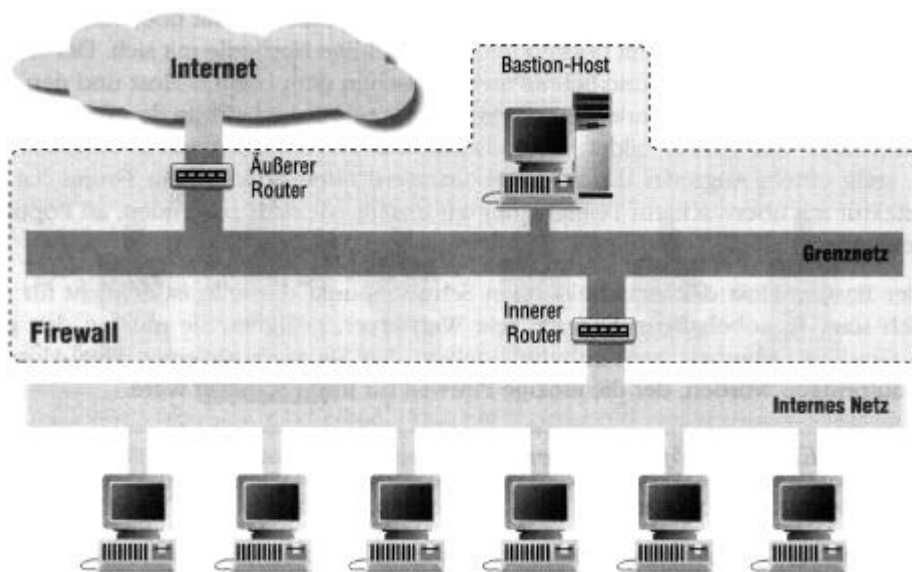
Bei dieser Architektur besteht die Firewall nur aus einem Rechner mit 2 Netzwerkschnittstellen, der das interne vom externen (z.B. Internet) trennt.



Die Installation und Wartung dieser Firewall ist vergleichsweise einfach, da hierbei nur ein Rechner korrekt konfiguriert werden muss. Andererseits ist dies auch eine Schwachstelle: falls dieser Rechner einmal ausfallen sollte (Hardware Fehler, externer Angriff) sind alle Verbindungen von und nach außen getrennt. Und sollte ein Angreifer Zugriff zum Dual-Homed-Host erlangt, besitzt er auch Zugriff auf das interne Netzwerk (und den Datenverkehr und damit auch auf sensible Daten).

### 2.3.2. Screened Subnet (Architektur mit überwachtem Teilnetz)

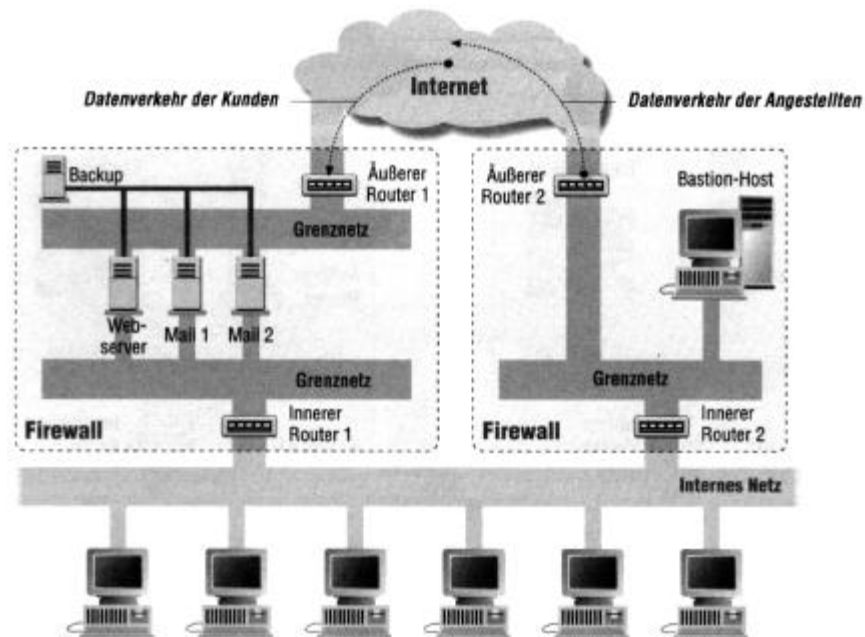
Dieser Typ bietet eine zusätzliche Schutzschicht zum internen Netzwerk, die sogenannte DMZ (DeMilitarized Zone oder Grenznetz). Sie liegt zwischen dem internen und externen Netz, jeweils mit einem Router abgesichert. In ihr stehen normalerweise Proxys und Server die Dienste nach innen und außen anbieten (Bastion Hosts).



Da der Bastion-Host (natürlich neben dem Äußeren Router) bei diesem Typ die einzig angreifbare Maschine ist, muß er besonders abgesichert und überwacht werden. Sollte einer dieser Rechner kompromittiert werden, ist es nur noch eine Frage der Zeit bis der Angreifer in das interne Netzwerk gelangt – oder er entdeckt wird. Jedoch kann der Angreifer vom DMZ aus nicht in den Netzwerkverkehr des internen Netzwerkes lauschen, was dem Administrator Zeit verschafft ihn zu entdecken ohne das der Angreifer schon Zugriff auf sensible Daten erlangt hätte.

### 2.3.3. Independent Screened Subnet (Unabhängig überwachte Teilnetze)

Diese Art von Firewall benötigt im Grunde genommen 2 Firewalls mit zwei getrennten Grenznetzen.



Bei dieser Aufteilung (nach innen gerichtet und nach außen gerichtete Dienste) ist es einfacher einen stärkeren Schutz für die einzelnen Grenznetze zu erreichen.

Unabhängig überwachte Teilnetze eignen sich auf Grund der Komplexität, Installation und Wartung nur für Netzwerke, die hohe Sicherheitsanforderungen stellen oder einen besonders hohen Grad an Redundanz benötigen.

## **Literaturverzeichnis:**

- [1] AstaNetworks, DoS Attack Tools,  
[http://www.astanetworks.com/resources/about/attack\\_tools.html](http://www.astanetworks.com/resources/about/attack_tools.html)
- [2] AstaNetworks, Types of DoS Attacks,  
<http://www.astanetworks.com/resources/types/>
- [3] Insecure.org, Ping of Death,  
<http://www.insecure.org/splotts/ping-o-death.html>
- [4] University of Maribor, Teardrop Fragmentation Attack,  
[http://www.camtp.uni-mb.si/books/Internet-Book/IP\\_TeardropAttack.html](http://www.camtp.uni-mb.si/books/Internet-Book/IP_TeardropAttack.html)
- [5] SANS (System Administration, Networking and Security Institute), Understanding DDOS Attack, Tools and Free Anti-tools with Recommendation  
[http://rr.sans.org/threats/understanding\\_ddos.htm](http://rr.sans.org/threats/understanding_ddos.htm)
- [6] Computer & Network Consulting, Firewallkonzepte für Linux,  
<http://cnc-online.net/2BLT/firewall.html#5>
- [7] Jeffrey Howard, Packet Filters, Stateful Packet Filters, and Proxies,  
<http://www.burningvoid.com/faq/firewall-type.html>
- [8] Microsoft, Multilayer Firewall,  
<http://www.microsoft.com/isaserver/evaluation/features/security/multilayerfirewall.asp>

## **Allgemeine Literatur:**

- Elizabeth D. Zwicky, Simon Cooper, D. Brent Chapman, Einrichten von Internet Firewalls, 2. Auflage, O'Reilly, 2001
- Wolfgang Barth, Das Firewall Buch, SuSE Press, 2001