

Application Gateways und Stateful Inspection: Vergleich und Gegenüberstellung

Avolio und Blask
Trusted Information System, Inc.

22.01.1998

Inhaltsverzeichnis

1	Einleitung	2
2	Anbieter	2
3	Übersicht und Vergleich	2
3.1	Packet Filtering - Erste Generation	2
3.2	Packet Filter – Zweite Generation	3
3.3	Application Gateways - Erste Generation	5
3.4	Transparente Application Gateways - die zweite Generation	7
4	Spezifische Behauptungen und Gegenargumente	7
4.1	Benutzung von Application Gateway und Stateful Packet Filter	8
5	Abschliessende Gedanken	9

1 Einleitung

Die Internet-Security-Industrie ist in den letzten Jahren sehr stark gewachsen: die Nachfrage für entsprechende Produkte hat dieses Wachstum sogar noch übertroffen. Für den Beschaffer ist es schwer geworden, die Qualität der konkurrierenden Produkte zu beurteilen. Dieses Papier ist entstanden, um eine der zur Zeit im Security-Markt diskutierten Streitfragen klarer zu machen: Packet Filter versus Application Gateway Technik als Basis für sichere Verbindung zum Internet.

Dank an die Mitglieder der Internet Firewall Mailing List für ihre Beiträge.

2 Anbieter

Anbieter in den beiden hier betrachteten Kategorien sind zum einen Trusted Information Systems mit einem transparenten Application Gateway und Check Point, die ein Stateful Packet Filter Gateway anbieten.

Trusted Information Systems (TIS) wurde 1983 in Rockville, Maryland gegründet und entwickelt Internet Security Software seit den frühen Tagen von TCP/IP und ARPAnet. TIS ist der Entwickler des TIS Internet Firewall Toolkit (FWTK), das frei über das Internet verfügbar ist und von mehr als 50.000 Internet Sites verwendet wird.

Check Point wurde 1993 in Tel Aviv gegründet und ist der Entwickler einer verbesserten Packet Filter Technik mit dem Handelsnamen "Stateful Multilevel Inspection".

Dieser Beitrag soll kein direkter Vergleich der beiden Firmen oder ihrer Produkte sein. Die hier vermittelten Informationen sind genereller Natur und beziehen sich auf alle bekannten Implementationen der beiden Kategorien.

3 Übersicht und Vergleich

In den letzten zehn Jahren wurden Firewalls in "Generationen" weiterentwickelt. Auch die Verfahren, die wir in dieser Schrift betrachten, haben verschiedene Generationen durchlaufen und werden im Folgenden entsprechend ihrer Entwicklung beschrieben.

3.1 Packet Filtering - Erste Generation

Packet Filtering ist ein Verfahren, das anhand der Informationen im Header eines IP-Paketes entscheidet, ob die Information weiter geleitet wird oder nicht. Die im Header verfügbaren Informationen wie Herkunft, Ziel oder Port (Service) sowie einige andere Informationen werden verwendet, um Regeln zu erstellen für die Weiterleitung oder Abweisung des Paketes. Bevor kommerzielle Firewalls verfügbar waren, erstellten Netzwerkverantwortliche Regeln für die Abweisung von gewissem unerwünschten Datentransfer und die Routerhersteller entwickelten Werkzeuge dafür. Man spricht hier von "statischen" Packet Filtern, weil die Verbindung zwischen internem und externem Netzwerk immer offen sein muss.

Die Vorteile dieses Verfahrens sind:

- Hoher Durchsatz
- billig oder sogar kostenlos
- Gut geeignet für Traffic-Management

Der Overhead dieses Verfahrens ist äusserst gering, deshalb liegt die Übertragungsgeschwindigkeit nahe an der Geschwindigkeit der Hardware. Fast jede Internet Connectivity Hardware (typischerweise Router) bietet die Möglichkeit, Packet Filter zu installieren. Deshalb ist dieses Verfahren gut geeignet, den Datenfluss innerhalb von Netzwerken zu steuern.

Die Nachteile sind:

- es gibt direkte Verbindungen zwischen dem internen Host und dem externen Client
- damit sind ständig Löcher offen im Netzwerk
- in komplexen Umgebungen wird das Packet Filtering schnell unverwaltbar
- die Firewall ist verletzlich gegenüber Angriffen wie z.B. dem "Spoofing" (das Vortäuschen einer vertrauenswürdigen Ansenderadresse)
- es gibt keine Benutzer-Authentifizierung

Statische Packet Filter werden in einigen Organisationen noch genutzt. In vielen Fällen liegt dies an Unerfahrenheit mit dem Internet und seinen Sicherheitsproblemen, an Altinstallationen oder Packet Filter werden als minimale Sicherheitsmassnahme genutzt.

3.2 Packet Filter – Zweite Generation

Der offensichtliche Nachteil der statischen Packet Filter liegt in den "Türen", die immer offen gehalten werden müssen, um Datentransfer zu ermöglichen. Diese Schwäche macht Netzwerke mit statischen Packet Filtern zur Beute von einer großen Anzahl an Angriffsverfahren, die die Sicherheit der Systeme im internen Netz korrumpieren wollen. Da Sicherheit häufig als Thema von geringer Priorität angesehen wird, waren und sind diese Angriffe sehr häufig auch erfolgreich.

Mit dem dynamischen Packet Filter versucht man, diese Gefahren zu reduzieren. Ein dynamischer Packet Filter öffnet und schließt "Türen" in der Firewall ebenfalls basierend auf den Headerinformationen. Sobald eine Anzahl von Paketen die Tür passiert hat, schließt sie die Firewall wieder. Das Stateful Packet Filtering ist eine Erweiterung des dynamischen Packet Filters. Hier versucht man, die Eigenschaften von Protokollen zu nutzen und Filterregeln an protokollspezifische Anforderungen anzupassen (z.B. simulierte Verbindungen für verbindungslose Protokolle wie NFS oder RPC). Der Stateful Packet Filter verfolgt Status und Verbindungsinformationen einer Sitzung. Dieses Verfahren kann auch für das UDP Protokoll verwendet werden, indem man eine virtuelle Sitzung aufbaut und so eine Illusion von

Sicherheit erzeugt, wo in Wirklichkeit keine Sicherheit vorhanden ist. In der Checkpoint Implementation sitzt dieses Modul zwischen der Datalink Schicht und der Netzwerkschicht. Das Hinzufügen der Statusverfolgung zu einem Packet Filter verbessert sicher die Sicherheit des Packet Filters. Die Inhalte oder Auswirkungen der Datenübertragung werden aber nicht berücksichtigt.

Die Vorteile des dynamischen Packet Filters sind:

- es stehen nur zeitweise Löcher in das Netzwerk offen
- hoher Durchsatz bei geringem Overhead
- fast jeder Dienst wird unterstützt (so müssen beispielsweise Back-Channel Dienste wie FTP lediglich als Spezialfall behandelt werden).

Da die Zeit, in der ein Loch in das Netzwerk offen steht, erheblich reduziert ist, werden viele Arten von Angriffen schwieriger oder gar unmöglich. Ausserdem wird hier neben der Informationsweiterleitung nur sehr wenig Aufwand erzeugt. Deshalb haben von der Hardware her vergleichbare Systeme mit dynamischen Packet Filtern oft einen höheren Durchsatz als bei der Verwendung von Application Gateways.

Da sich der Packetfilter nicht um die Anwendung kümmert, kann er für jede Art von IP-Traffic verwendet werden.

Die Nachteile sind:

- direkte Verbindungen von externen Clients zu internen Hosts sind möglich
- es gibt keine Benutzer-Authentifizierung (wenn, dann wird sie durch ein zusätzliches Application Gateway durchgeführt)
- es kann jeder IP-Service unterstützt werden.

Obwohl dynamisches Packet Filtering erheblich die Offenheit reduziert, können externe Systeme unter Kontrolle der Firewall immer noch eine direkte IP-Verbindung mit einer internen Maschine herstellen. Der Hauptnachteil liegt darin, dass, sobald einmal der Zugriff auf ein System im internen Netz erlaubt wurde, ein Angreifer die Möglichkeit hat, jede Schwachstelle von Software oder Konfiguration dieses Systems auszunutzen. Die Möglichkeit von diesem System auf andere Systeme im Netzwerk zuzugreifen, wird lediglich durch allfällig vorhandene Sicherheitsmassnahmen auf diesen Systemen eingeschränkt.

Das "Spoofing" - das Vortäuschen einer vertrauenswürdigen Absenderadresse, um das Netzwerk hinter dem Filter angreifen zu können - ist seit langem eine wohl bekannte Verletzbarkeit von Sites. Moderne dynamische Packet Filter enthalten heute Fixes für die meisten bekannten Spoofing-Methoden. Das Problem bleibt aber dadurch bestehen, dass die IP-Adresse eines externen Systems für vertrauenswürdige gehalten wird. Selbst wenn der eingehende Datenstrom von einem erlaubten Host kommt, ist nicht sichergestellt, dass dieser Host von autorisierten Benutzern betrieben wird. Mit anderen Worten: wenn ein Hacker dieses System kompromittiert hat, kann er es als Gateway zum Netzwerk benutzen. Desweiteren

unterstützen Packet Filter Firewalls nicht das Konzept der starken User Authentifizierung. Es ist ein ernsthafter Bruch der Netzwerksicherheit, wenn von unbekanntem Netzwerken ohne Authentifizierung auf ein Netzwerk zugegriffen werden kann. Einige Anbieter von Packet Filter Systemen haben angefangen, dieses Problem rudimentär einzuschränken durch den Einsatz von Application Gateways.

Einer der Vorteile eines Packet Filters gegenüber einem Application Gateway liegt darin, dass jede Art von Traffic erlaubt ist. Hier liegen aber auch gleichzeitig die größten Gefahren. Wenn man nicht prüft, was eine Anwendung in einem internen Netz anrichten kann, hat man keine Möglichkeit, diese Gefahr einzuschätzen. Deshalb gelangen oft gefährliche Anwendungen durch Packet Filter Firewalls in typische Benutzerinstallationen.

3.3 Application Gateways - Erste Generation

Ein Application Gateway ist ein Firewallsystem, in dem Prozesse die gesamte TCP-Verbindung steuern. Application Gateway Firewalls prüfen adressieren oft den Datenstrom um, so dass es bei ausgehendem Datenstrom aussieht, als käme er von der Firewall und nicht aus dem internen Netz.

Experten halten Application Gateways für den sichersten Firewall-Typ. Alle Verbindungen zum internen Netz gehen durch die Firewall. Bei der Application Level Firewall wird mit Security Proxies unterschieden zwischen den einzelnen Diensten wie z.B. FTP, Telnet usw. Damit wird direkter Zugriff auf Dienste im internen Netz verhindert.

Die Vorteile von Application Gateways sind:

- sie erlauben keine direkte Verbindung zwischen internen und externen Systemen
- sie unterstützen Authentifizierung auf Benutzerebene
- sie analysieren Anwendungsbefehle im Datenpaket (was Packet Filter nicht tun)
- sie führen umfassende Logs über Datenfluss und Aktivitäten

Der hauptsächliche Vorteil liegt darin, dass unter keinen Umständen eine direkte Verbindung durch die Firewall zustande kommt. Application Gateway Software wird oft als Proxy-Software bezeichnet, weil sie wie Server-Software für den Client aussieht und wie Client-Software für den Server.

Man stelle sich das Telefongespräch eines Mandanten mit seinem Rechtsanwalt vor, der wiederum in Verbindung steht mit einer anderen Person, an die er Informationen seines Mandanten weitergibt. Da der Inhalt der Unterhaltung wichtig ist, haben Mandant und Anwalt miteinander vereinbart, dass die dritte Person nicht erfährt, wer der Mandant ist, wo er ist und ob er überhaupt existiert. Jeder Versuch, den Mandanten über diese Verbindung anzugreifen, wird bei dem Anwalt landen, der für diesen Zweck speziell ausgebildet ist und geschützt wird durch bekannte Strukturen (im Beispiel: Gesetze). Der Packet Filter als Anwalt in diesem Beispiel würde den Mandanten und die dritte Person zusammenbringen und dann den Raum verlassen.

Ein Application Gateway hat eine ähnliche Funktion wie der Anwalt in obigem Beispiel. Der Anwalt würde jedes Dokument erst prüfen, bevor er es weitergibt. Der Anwalt muss fundierte Kenntnisse haben bezüglich der Bedeutung des Inhalts eines Dokuments und die Auswirkungen, die der Inhalt auf seinen Mandanten haben kann. Er muss seinen Mandanten vor Schaden schützen, der ihm aus dem Inhalt des Dokuments entstehen könnte. Dies erfordert, dass der Anwalt ein Experte in dem einschlägigen Umfeld ist.

Der Packet Filter ist in diesem Beispiel ein Anwalt, der lediglich prüft, ob ein Brief an seinen Mandanten einen Absender hat und dann diesen Brief und alle weiteren Dokumente von der selben Adresse an seinen Mandanten weiterleitet. Er hat keine Ahnung davon, um was es in dem Brief geht und prüft nicht mal, ob der Umschlag nicht vielleicht eine Briefbombe enthält.

Die Nachteile einiger Application Gateways:

- sie sind langsamer als Packet Filter
- der interne Client benötigt Informationen über die Firewall
- sie unterstützen nicht jede Art von Service.

Der erstgenannte Nachteil wird bei Application Gateways immer auftreten, weil die Firewall mehr Sicherheitsprüfungen durchführen muss. Um bei dem Beispiel mit dem Anwalt zu bleiben: wenn der Inhalt jedes Briefes geprüft werden muss, wird das immer länger dauern als wenn man die Post nur sortiert. Glücklicherweise kann man diesen Prüfaufwand durch entsprechende Hardware-Plattformen ausgleichen. Üblicherweise wird der Durchsatz eines Application Gateways viel höher sein als der Durchsatz der Verbindung zum externen Netzwerk. Der zweite Nachteil ist der unbequemste. Um mit dem "Anwalt" in der Firewall sprechen zu können, muss auf den Client-Workstations entsprechende Software installiert sein. Mit "Transparenz", dem Merkmal der nächsten Generation, verschwindet dieser Nachteil.

Der Auswirkung des letzten Nachteils hängt ab von dem Sicherheitsgrad, den der Firewall-Betreiber fordert. Auch hier ein Beispiel: angenommen, es taucht im externen Netzwerk (in der Regel wohl dem Internet) eine neue Anwendung auf - nennen wir sie "Cool Format". Diese neue Anwendung ist der Renner; die internen Nutzer haben von ihr gehört und wollen sie unbedingt über das Internet nutzen. Das Application Gateway wird dieses nicht erlauben, weil die Applikation nicht bekannt ist. Der Administrator wird sie erst freischalten, wenn er weiss, was die Anwendung tut und welchen und ob sie Schaden im internen Netz anrichten kann. (Im Beispiel erlaubt "Cool Format", Festplatten auf anderen Systemen remote zu formatieren). Um beim Anwaltsbeispiel zu bleiben: das Verbot der Nutzung von "Cool Format" durch das Application Gateway ist vergleichbar mit einer Anweisung an den Anwalt, alle Briefe in blauen Umschlägen nicht zu lesen und nicht weiter zu leiten.

Im wirklichen Leben liefern Anbieter von Application Gateways für solche Fälle Werkzeuge zur Erstellung von "generischen" Proxies oder sie erlauben eine Art Packet Filtering (unter Ausschluss von Garantie in solchen Fällen). Natürlich ist es durchaus das Qualitätsmerkmal eines Anbieters, wie schnell er neue Proxies für neue und gewünschte Anwendungen liefern kann.

3.4 Transparente Application Gateways - die zweite Generation

Transparenz ist die wesentliche Weiterentwicklung der Application Gateways der zweiten Generation. Einer der lästigsten Probleme mit Application Gateways der ersten Generation war, dass jede Workstation hinter der Firewall speziell konfiguriert werden musste, um mit der Firewall in Kontakt treten zu können und dass auf der Workstation spezielle Software installiert werden musste, damit sie mit der Proxy-Software kommunizieren konnte. Transparenz bedeutet: die Client-Workstation müssen nicht mehr wissen, dass es die Firewall gibt und brauchen keine spezielle Software mehr.

Im letzten Abschnitt wurde gesagt, dass der Grund für den Geschwindigkeitsunterschied zwischen Packet Filtern und Application Gateways abhängt vom Grad der Sicherheit, die die Firewall liefert. Glücklicherweise muss mit den heute verfügbaren Hardware-Plattformen der Einsatz von Packet Filtern nur erwogen werden, wenn ein Durchsatz von mehr als 75-100 Mbps erforderlich ist. Da T3 (45 Mbps) Internet Verbindungen schon sehr schnell sind (die meisten Anwender nutzen T1 oder 1,5 Mbps), muss nur bei Intranet-Anwendungen auf Hochgeschwindigkeitsnetzwerken wie ATM oder Gigabit Ethernet ernsthaft an den Einsatz von Packet Filtern gedacht werden.

Application Gateways unterstützen die üblichen im Internet benutzten Dienste. TIS zum Beispiel hat einen eigenen Stab von Entwicklern, die die Bedeutung von neuen Applikationen und Protokollen prüfen. Wenn die Nachfrage für die neuen Dienste wächst, werden Proxies entsprechend entwickelt.

4 Spezifische Behauptungen und Gegenargumente

In Check Point's technischer Beschreibung des Stateful Packet Filtering (der Titel lautet: "Stateful Inspection Firewall Technology") stellen die Autoren einige einleitende Behauptungen auf:

"Stateful Packet Filtering ist eine neue Firewall-Generation" Wie vorne schon bemerkt, ist dies eine willkürliche Feststellung. Es gibt nicht einfach Firewall-Generationen. Der dynamische Packet Filter ist höchstens die Verbesserung für den statischen Packet Filter.

"Stateful Packet Filtering wird zum Industriestandard" Die meisten Firewalls, die im Internet genutzt werden, sind Application Gateways (und davon sind wiederum viele von TIS). Der de facto Internet-Stand ist die Application Gateway Technik.

Check Point behauptet, dass seine SPF-Technik fähig ist, Informationen aller sieben Schichten des IP-Paketes zu erlangen, zu analysieren und zu nutzen. SPF mag "fähig" sein dieses zu tun, aber die Implementation tut es nicht in den meisten von Check Point unterstützten Netzwerkdiensten (wenn es sie überhaupt tut).

Check Point sagt, dass Application Gateways die übertragenen Daten und die dazugehörigen Zustände nur teilweise prüfen. Diese Behauptung ist unverständlich, da Application Gateways grundsätzlich in der Lage sind, beides zu tun.

Natürlich sind Application Gateways auch "Stateful" Firewalls. Die Gartner Group stellt hierzu fest (Mai 1997): "Die Stateful Firewall kann ein Proxy Gateway oder eine Stateful Inspection Firewall sein. Typische Beispiele sind... Trusted Information Systems Gauntlet oder Check Points Firewall-1".

Check Point sagt, dass sein dynamisches Packet Filter Produkt die Sicherheit eines Application Gateways bringt mit der Geschwindigkeit eines Packet Filters. Einerseits sagen sie, dass es sehr einfach ist, einen neuen Dienst mit einem dynamischen Packet Filter hinzuzufügen; andererseits behaupten sie, dass der Filter auch Application-Level-Technik nutzt. Diese beiden Behauptungen schliessen sich gegenseitig aus. Auf Check Points Website wird beispielsweise gezeigt, wie man ein neues Protokoll implementiert:

"Anleitung für die Implementierung von Sybase SQL Server Support auf der Firewall-1: Sybase SQL nutzt TCP Ports oberhalb von 1024. Der benutzte Port ist in der Konfiguration des Sybase Servers definiert. Um die Firewall-1 für Sybase SQL zu konfigurieren: 1. Füge TCP Service "Sybase SQL" hinzu auf der GUI 2. Bestätige diesen neuen Service in der Regeldatenbank."

Hier gibt es keinen Hinweis dafür, dass die Firewall in dieser Konfiguration irgendwas über die Internas des Sybase SQL Datenflusses erfährt.

Ein anderes Beispiel:

"Anleitung für die Implementierung von Microsoft Netmeeting Support auf der Firewall-1: Füge in der GUI TCP Port 1503 hinzu"

Wieder scheint es keine Informationen darüber zu geben, was diese neue Applikation tut. Im Gegensatz dazu hat die NetMeeting Proxy der Gauntlet Firewall verschiedene der Zugriffskontrolle wie z.B. host-basierten Zugriff oder ACLs für äquivalente Benutzernamen. "Quick and easy" Einfügungen in Stateful Packet Filtern können nicht das gleiche leisten.

4.1 Benutzung von Application Gateway und Stateful Packet Filter

Wir sind überzeugt davon, dass für Anwender, die das Thema Sicherheit ernst nehmen, Application Gateways die einzige Lösung für externe Firewall-Technik sind. Trotzdem können Stateful Packet Filter durchaus eine Lösung sein für Intranets, für Organisationen, bei denen Sicherheit nicht so wichtig sein muss oder als Grobfilter für ein Application Gateway. Internet Service Provider und Firmen, die Stateful Packet Filter nutzen, um einen im Internet stehenden Server zu schützen (z.B. einen Webserver), sind ebenfalls potentielle Kandidaten für Packet Filter Firewalls.

Es gibt viele Gründe dafür, dass die meisten Firewall-Experten Packet Filter als ungeeignet betrachten für Umgebungen, die sicher sein müssen.

- Bei Packetfiltern besteht die Gefahr, dass Firewall-Administratoren die Sicherheitsregeln anpassen für jeden neuen Service, ohne den Dienst selber zu analysieren, und damit Löcher öffnen.
- Ein Packetfilter kümmert sich nicht um Probleme auf der Datenstromebene wie sie z.B. aufkamen bei Angriffen gegen Windows NT 1997. Man verlässt sich auf die Sicherheit der Software auf den internen Systemen, obwohl die das schwächste Glied in der Kette ist. Beispielsweise wird jede Art von Packet Filter eine SMTP-Verbindung an den internen Mailserver durchreichen. Keiner ist in der Lage, bekannte Probleme zu prüfen vor der Weitergabe an den internen Mail-Verteiler. Ein Application Gateway wie die Gauntlet kann das und tut es auch.
- Ein Stateful Packet Filter behält Zustandsinformationen über Verbindungen. Es reicht das eingehende Paket weiter, wenn es den Regeln entspricht. Der Packet Filter prüft nicht die Daten, wie es ein Proxy tut. Wenn man ein Application Gateway benutzt, muss man nicht das TCP/UDP/ICMP Handling nachahmen, weil das tatsächliche Handling von der Firewall erleidigt wird.
- Die derzeitigen Packet Filter schreiben Pakete nicht um. Damit ist das interne

Netzwerk offen für paketbasierte Angriffe. Die Pakete werden weitergereicht auf Grund von Sicherheitsregeln. Application Gateways geben keine Pakete weiter. Sie bauen eine neue Verbindung auf. - Packet Filter protokollieren viel weniger Informationen wie ein Application Gateway. Der Packet Filter protokolliert Quelle und Ziel eines Paketes, die Annahme des Paketes oder die Ablehnung. Z.B. werden bei HTTP-Verbindungen nur die einzelnen Pakete protokolliert, aber nicht Dateinamen, URLs, Paketanzahl usw.

Packet Filter schauen nicht so tief in den Datenstrom und bieten deshalb nicht soviel Sicherheit wie ein Application Gateway. Deshalb sind sie nutzlos in all den Fällen, in denen Sicherheit absolut notwendig ist. Was man mit Packetfiltern nicht machen kann ist z.B.:

- Ausfiltern auf URL-Level bei HTTP-Datenströmen
- Abblocken von Java oder ActiveX oder anderen Dingen, die über HTTP kommen
- Prüfen von FTP-Befehlen, um z.B. PUT zu erlauben, aber nicht GET
- Prüfen von E-Mail auf Sendmail-Attacken.

Check Point hat einige Features für diese Probleme in seine ursprünglich reine Stateful Packet Filter Firewall eingebaut mit Proxy-Software. Damit wird die Firewall-1 zu einer Art Zwitter-Firewall.

5 Abschliessende Gedanken

Es wird immer wieder festgestellt, dass Stateful Packet Filter schneller sind als Application Gateways. Natürlich sind sie schneller - sie machen weniger Sicherheitsprüfungen. Stateful Packet Filter schauen nicht so tief in den Datenstrom wie Application Gateways; sie prüfen kein Protokoll.

Der Sicherheitsexperte Bill Stout schrieb in der Firewall-Mailingliste: "Der Zweck einer Sicherheitseinrichtung ist es, ein Netzwerk zu schützen und nicht, schnell zu sein. Schnelligkeit ist etwas, das Flugpassagiere schätzen, wenn sie durch den Sicherheitscheck im Flughafen müssen; Sicherheit ist das, was sie sich wünschen, wenn sie nach der Sprengung ihres Flugzeuges durch die Luft stürzen."

Stateful Packet Filter mögen sinnvoll sein in Intranets, in denen man von geringen Sicherheitsrisiken ausgeht, oder in Fällen, in denen reiner Durchsatz wichtiger ist als Sicherheit. Application Gateways sollten immer dann eingesetzt werden, wenn Sicherheit für Netzwerke wirklich wichtig ist.
