Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Bachelorarbeit

Mona Lüdemann

Sicherheitsbetrachtung:
Application Layer Firewall und
Application Layer Proxy

Fakultät Technik und Informatik
Department Informatik

Faculty of Engineering and Computer Science
Department of Computer Science

Mona Lüdemann

Sicherheitsbetrachtung: Application Layer Firewall und Application Layer Proxy

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung

im Studiengang Bachelor of Science Technische Informatik
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer : Prof. Dr. Klaus-Peter Kossakowski
Zweitgutachter : Prof. Dr. Philipp Jenke

Abgegeben am 16.03.2018

Mona Lüdemann

Thema der Arbeit
Sicherheitsbetrachtung: Application Layer Firewall und Application Layer Proxy

Stichworte
Proxy, Firewall, Netzwerksicherheit

Kurzzusammenfassung
In dieser Arbeit werden sowohl Application Layer Firewalls als auch Application Layer Proxys definiert. Um einen Vergleich zu ermöglichen, werden Unterscheidungsmerkmale und Funktionalitäten beider Sicherheitsmaßnahmen herausgearbeitet. Vor- und Nachteile beider Techniken werden abgewogen. In den Vergleich fließen ferner Aspekte ein, wie die Betrachtung des Verkehrsflusses bei Einsatz einer Application Layer Firewall bzw. bei Einsatz eines Application Layer Proxys. Damit ein Vergleich möglich ist, werden zwei konkrete Dienste „Web“ und „Mail“ betrachtet. Außerdem erfolgt ein grober Herstellervergleich der Marktführer. Um das Zusammenspiel von Application Layer Firewall und Proxy nachzustellen und zu testen, wird ein Laboraufbau entwickelt und entsprechend samt Ergebnisse skizziert.

Mona Lüdemann

Title of the paper
Security considerations: application layer firewall and application layer proxy

Keywords
proxy, firewall, network security

Abstract
In this work application layer firewalls and application layer proxies are defined. In order to make a comparison possible, distinguishing characteristics and functionalities of both security measures are worked out. The advantages and disadvantages of both techniques are weighted. The comparison also includes aspects such as the consideration of traffic flow when using an application layer firewall or when using an application layer proxy. To make a comparison possible, two concrete services "web" and "mail" are considered. In addition, a rough manufacturer comparison of the market leaders is drawn. In order to simulate and test the interaction between the application layer firewall and the proxy, a laboratory setup is developed and accordingly outlined with the results.

Inhaltsverzeichnis

1 Einleitung

In Firmen einer gewissen Größe gilt der Einsatz von Proxys als unverzichtbar. Ein Proxy stellt eine zentrale Vermittlungsstelle dar, indem er Anfragen entgegennimmt und über eine neue Session eine Verbindung zur anderen Seite über seine eigene Adresse herstellt. Häufig kommen mehrere Proxys zum Einsatz, die jeweils auf ein bestimmtes Kommunikationsprotokoll spezialisiert sind und die Daten vor der Weiterleitung analysieren und gegebenenfalls anpassen bzw. verwerfen.
Seit einigen Jahren sind jedoch die sogenannten Next Generation Firewalls in aller Munde. Der Begriff Next Generation Firewall (NGFW) ist die Bezeichnung der Hersteller, im Prinzip meint eine Next Generation Firewall hinsichtlich ihrer Funktionalitäten eine Application Layer Firewall. Der Begriff wurde schon einmal Anfang 2000 von Herstellern für Marketingzwecke verwendet.
Eine NGFW stellt nicht mehr eine reine Stateful Inspection Firewall dar, sondern ist auch in der Lage, Inhalte des Datenverkehrs auf Layer fünf bis sieben (Sitzungsschicht, Darstellungsschicht & Anwendungsschicht) des ISO/OSI-Referenzmodells zu analysieren. In den letzten Jahren wurden Funktionalitäten von Application Layer Firewalls immer weiter ergänzt und intensiviert, dieser Vorgang scheint nach wie vor nicht abgeschlossen. Die Hersteller werben damit, in ihren Next Generation Firewalls zahlreiche Funktionalitäten zu koppeln und somit ein „All-In-One“-Device bereitzustellen. Im Zeitverlauf sind auch ähnliche Produkte wie UTM (Unified Threat Management) auf dem Markt erschienen. UTMs lassen sich kaum von Next Generation Firewalls unterscheiden. Lediglich die Durchsatzraten unterscheiden sich. So sind UTMs in der Regel eher für kleine bis mittelständische Unternehmen ausgelegt, wohingegen NGFWs mit hohen Durchsatzraten ausgestattet sind und für große Unternehmen in Frage kommen (vgl. Casey 2014).
Sowohl Proxys als auch Application Layer Firewalls sind als Übergang bzw. Bestandteil des Übergangs von Zonen unterschiedlicher Sicherheitsniveaus zu sehen und finden daher in vielen Bereichen Anwendung wie beispielsweise bei der Abschottung von externen Anbindung wie das Internet oder auch als Sicherung einer internen Datacenter-Struktur. Dabei stellt sich die Frage, inwieweit Proxys durch Application Layer Firewalls ersetzt werden

können oder welche Einsatzweise beider Techniken in Hinblick auf den momentanen Technikstand empfehlenswert ist.

1.1 Ziel der Arbeit

In dieser Arbeit sollen Unterscheidungsmerkmale und Funktionalitäten von Application Layer Firewall und Application Layer Proxy herausgearbeitet werden. Dabei gilt es zu klären, welche Funktionalitäten bei beiden Komponenten übereinstimmen bzw. welche Unterschiede sich ergeben. Erarbeitet werden soll, inwieweit es sinnvoll ist, die beiden Sicherheitsmaßnahmen für konkrete Dienste einzusetzen oder zu kombinieren, um deren Funktionen möglichst effizient umzusetzen, ohne dass sich einzelne Funktionalitäten behindern oder die Transparenz einzelner Funktionen beeinträchtigt wird. Um einen Vergleich zu ermöglichen, werden zwei konkrete Dienste „Web“ und „Mail“ betrachtet.

1.2 Zielgruppe der Arbeit

Diese Arbeit richtet sich an alle Interessierten der Netzwerksicherheit. Vor allem aber an Netzwerksicherheitsexperten und Netzwerkdesigner, die eine Entscheidung für den Einsatz von Application Layer Firewalls und Application Layer Proxys empfehlen oder sogar treffen müssen. Außerdem richtet sich diese Arbeit an Netzwerkadministratoren, die tagtäglich Firewalls und Proxys administrieren und die Hintergründe in der Platzierung dieser Netzwerkkomponenten nachvollziehen möchten.

1.3 Struktur der Arbeit

In Kapitel 2 wird die Firewall als Netzwerkkomponente definiert. Es werden drei unterschiedliche Firewall Technologien beleuchtet und Funktionen von Application Layer Firewalls dargestellt und erklärt. Außerdem erfolgt eine Abgrenzung der Begrifflichkeiten „Application Layer Firewall“ und „Web Application Firewall“.
In Kapitel 3 wird der Proxy definiert. Verschiedene Unterscheidungen hinsichtlich technischer Aspekte, sowie hinsichtlich der Anwendung werden dargestellt. Es werden Beispiele bezüglich ihrer Funktionen erläutert.
In Kapitel 4 wird ein Laboraufbau skizziert, Konfigurationen werden dargelegt und Tests werden abgebildet. Daraus folgende Ergebnisse werden erläutert. Der Laboraufbau soll insbesondere das Zusammenspiel von Application Layer Firewall und Proxy nachstellen und testen.
In Kapitel 5 erfolgt eine Gegenüberstellung der beiden Sicherheitsmaßnahmen Application Layer Proxy und Application Layer Firewall. Der Verkehrsfluss, der sich bei Einsatz beider Komponenten ergibt, wird dargestellt. Außerdem erfolgt ein Herstellervergleich der Marktführer. Bei der Gegenüberstellung der beiden Sicherheitsmaßnahmen werden konkrete Unterscheidungsmerkmale veranschaulicht und die Funktionsblöcke beider Techniken werden gegenübergestellt. Darüber hinaus werden Vor- und Nachteile

abgewogenen. Durch die unterschiedlichen Verkehrsflüsse ergeben sich auch Unterschiede hinsichtlich des Routings, die ebenfalls dargestellt werden. Außerdem wird ein Bezug zu Session-Angriffen hergestellt.
Im letzten Kapitel 6 erfolgt ein Fazit, bei dem geklärt wird, was in dieser Arbeit erarbeitet wurde und ob das Ziel dabei erreicht wurde. Anschließend erfolgt ein Ausblick.

2 Firewall

In diesem Kapitel wird die Firewall als Netzwerkkomponente definiert, die den Übergang von Zonen mit unterschiedlichen Sicherheitsniveaus ermöglicht. Drei wesentliche Firewall Technologien werden dabei vorgestellt und Funktionen von Application Layer Firewalls ausgeführt. Des Weiteren erfolgt eine Abgrenzung der Begrifflichkeiten „Application Layer Firewall“ und „Web Application Firewall“.

2.1 Definition

Eine Firewall kontrolliert Datenverkehr anhand fest definierter Regeln. Ziel ist es dabei, unerwünschte Netzwerkzugriffe zu unterbinden. Es wird unterschieden zwischen einer Personal Firewall (auch Desktop Firewall), welche auf dem schützenswerten Endgerät selber agiert, und einer externen Firewall (auch Netzwerk- oder Hardware-Firewall), die auf einem separaten Gerät (Netzkoppelelement) wirkt.

2.2 Firewall Technologien

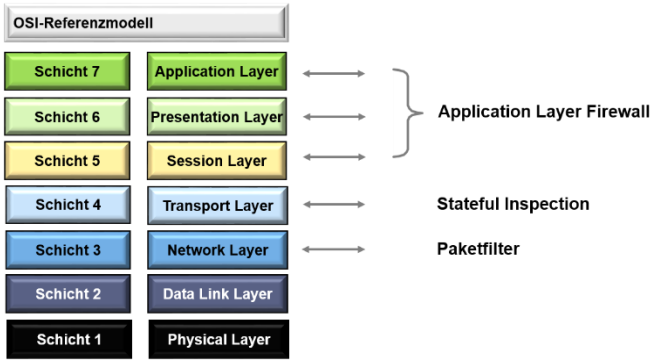


Abbildung 1: Firewall Technologien im Überblick

Wie in der Abbildung 1 zu erkennen, unterscheidet man bei Firewalls zwischen Paketfiltern, Stateful Inspection und Application Layer Firewalls. Die Technologien bauen aufeinander auf und jeder dieser lässt sich ein bestimmter Layer im ISO/OSI-Referenzmodells zuordnen.

2.2.1 Paketfilter

Paketfilter Firewalls stellen die primitivste Variante einer Firewall dar und sind daher auch auf Layer drei (Vermittlungsschicht) des ISO/OSI-Referenzmodells angesiedelt. Hier wird der IP-Header überprüft und das Paket wird je nach Regel durchgelassen (allow), verworfen (deny) oder zurückgewiesen (reject) (vgl. Bloebel und Koeppe: 256). Beim Zurückweisen erfolgt eine Meldung an den Absender. Diese Meldung ist abhängig vom Firewall-Produkt sowie von der Konfiguration. Verschiedene ICMP-Meldungen sind möglich oder bei TCP ein TCP-Reset (Segment mit gesetztem RST-Flag).

<table>
<tr><td>Version</td><td>IHL</td><td>TOS (Diensttyp)</td><td colspan="3">Gesamtlänge</td></tr>
<tr><td colspan="3">Kennung</td><td>Flags</td><td colspan="2">Fragment-Offset</td></tr>
<tr><td colspan="2">Zeitangabe</td><td>Protokoll</td><td colspan="3">Kopf-Prüfsumme</td></tr>
<tr><td colspan="6">Absender-IP-Adresse</td></tr>
<tr><td colspan="6">Empfänger-IP-Adresse</td></tr>
<tr><td colspan="5">Optionen</td><td>Füllzeichen</td></tr>
</table>

Abbildung 2: IP Paket Header

Überprüft werden können alle Inhalte des IP-Headers (dargestellt in der Abbildung 2). Typischerweise werden Quell- und Zieladresse sowie Protokollnummern kontrolliert. Paketfilter Firewalls stellen im Allgemeinen die Funktionsweise von Routern oder Multilayer Switchen mit Access Control Lists (ACLs) dar.

2.2.2 Stateful Inspection

Unter Stateful Inspection versteht man eine dynamische Paketfilterung, die aus dem (statischen) Paketfilter hervorgegangen ist. Jedes Datenpaket wird hier zustandsorientiert (stateful) überprüft und einer bestimmten Session zugeordnet, sodass der Verbindungsstatus einer Session in die Entscheidung mit einbezogen wird (vgl. ITWissen.info 2016). Im ISO/OSI-Referenzmodells ist diese Technologie auf Layer vier (Transportschicht) einzuordnen. Es können prinzipiell alle Inhalte des Headers vom Transportprotokoll (dargestellt in der Abbildung 3) zusätzlich geprüft werden.

<table>
<tr><td colspan="11">Absender-Port</td><td colspan="5">Empfänger-Port</td></tr>
<tr><td colspan="16">Sequenznummer</td></tr>
<tr><td colspan="16">Bestätigungsnummer</td></tr>
<tr><td>Daten-Offset</td><td colspan="3">Reserviert</td><td>NS</td><td>DWR</td><td>ECE</td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td colspan="4">Fenster</td></tr>
<tr><td colspan="11">Prüfsumme</td><td colspan="5">Dringlichkeitsanzeiger</td></tr>
</table>

Abbildung 3: TCP Segment Header

Beim verbindungsorientierten Transport-Protokoll TCP bedeutet das konkret, dass die Firewall erkennt, wenn ein Dreiwege-Handschake, anhand der Analyse der gesetzten Flags (SYN, SYN-ACK, ACK), erfolgt ist. Welcher der Kommunikationspartner zur Initiierung berechtigt ist, wird über das Regelwerk bestimmt. In dem Fall ist ein zulässiger Verbindungsaufbau zustande gekommen und die Firewall kann alle Pakete dieser Session in beide Richtungen unter der Voraussetzung von konsistenten Sequenz- und Bestätigungsnummern erlauben. Mit zulässigem Verbindungsabbau, ebenfalls gekennzeichnet über Flags (FIN, FIN-ACK, ACK), wird der entsprechende Eintrag der betreffenden Session wieder auf der Firewall gelöscht und eine Kommunikation der beiden Teilnehmer kann erst dann wieder von der Firewall gewährleistet werden, wenn ein neuer Verbindungsaufbau realisiert wurde. Es gibt auch Abwandlungen vom Verbindungsabbau durch unsaubere Programmierung, die Stateful Inspection Firewalls ebenfalls erkennen müssen.

Absender-Port	Empfänger-Port
Länge	UDP-Prüfsumme

Abbildung 4: UDP Datagram Header

Die Abbildung 4 zeigt einen UDP Datagram Header. Da das verbindungslose Transport-Protokoll UDP im Gegensatz zu TCP zustandsfrei arbeitet, ist eine äquivalente Überprüfung nicht möglich. Daher wird oft ein Zeitlimit von wenigen Sekunden festgelegt, in der ein Antwortpaket von der Firewall durchgelassen wird. Etablierte TCP-Sessions haben auch ein Zeitlimit, das jedoch häufig im Bereich von Stunden liegt.

2.2.3 Application Layer Firewall

Eine Application Layer Firewall (ALF) ist eine Sammelbezeichnung für Firewalls, die auf Layer fünf bis sieben (Sitzungsschicht, Darstellungsschicht & Anwendungsschicht) des ISO/OSI-Referenzmodells arbeiten. In Ergänzung zu den Funktionen von Paketfiltern und Stateful Inspection analysieren diese Firewalls auch die Header von höheren Protokollen wie beispielswiese HTTP/HTTPS.

Im Gegensatz zu klassischen Paketfiltern oder Stateful Inspection Firewalls werden bei einer Application Layer Firewall jedoch nicht nur die Header sondern auch der Payload des Datenpaketes auf bestimmte Merkmale überprüft. Diese Kontrolle nennt man Deep Packet Inspection (DPI). Sie ermöglicht es, Datenpakete, die bestimmte Daten oder Code-Segmente enthalten, zu erkennen, zu klassifizieren, weiterzuleiten oder zu blockieren (vgl. Dubrawsky 2003).

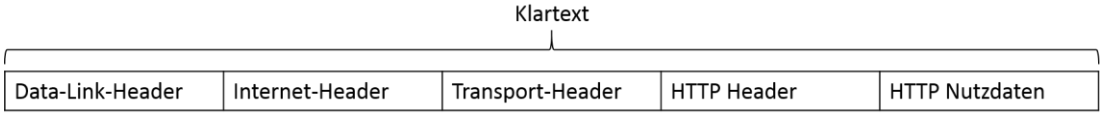


Abbildung 5: HTTP Daten

Die Abbildung 5 zeigt den Aufbau von HTTP Daten. HTTP nutzt TCP als Transport-Protokoll. Da es genau zwei Nachrichtentypen „Request“ und „Response“ gibt, unterscheiden sich je nach Nachrichtentyp auch die Felder des Headers. Es gibt eine Reihe von allgemeinen Feldern, Request- als auch Response-Felder sowie Entitäts-Felder, die entsprechend von der Firewall geprüft werden können.

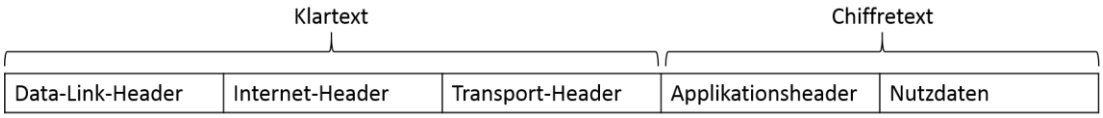


Abbildung 6: HTTPS Daten

Die Abbildung 6 zeigt den Aufbau von HTTPS Daten. HTTPS ermöglicht durch die Nutzung von SSL/TLS (Secure Sockets Layer/Transport Layer Security) auf OSI Layer fünf eine Verschlüsselung und Authentifizierung der per HTTP übertragenen Daten. Eine Analyse durch die Firewall entfällt dadurch auf den ersten Blick. Sie kann nur dann erfolgen, wenn die Firewall die Verschlüsselung aufbricht und die Daten danach wieder mit dem eigenen Zertifikat verschlüsselt.

Auch andere Protokolle wie FTP, LDAP, SMTP nutzen SSL/TLS für den sicheren Transport.

2.3 Funktionen von Application Layer Firewalls

Eine Application Firewall hat eine Reihe von Funktionalitäten, die in Form von Funktionsblöcken definiert werden können. Je nach Hersteller wird eine Auswahl dieser Funktionen realisiert. Weitere Funktionen sind jederzeit denkbar. Folgende Tabelle (Tabelle 1) stellt die unterschiedlichen Funktionsblöcke in Abhängigkeit zum OSI Layer dar.

	Funktionsblock	**OSI Layer**
Funktionen traditioneller Firewalls	Network Address Translation (NAT)	Layer 3
	Anti-Spoofing	Layer 3
	Stateful Inspection	Layer 4
Weitere Funktionen	SSL/TLS Inspection	Layer 5
	Deep Packet Inspection (DPI)	Layer 5-7
	Applikationsidentifizierung und -filter	
	Content Filterung	
	URL Filterung	
	File Policies	
	DNS Policies	
	User-basiertes Firewalling (Identity Firewall)	
	Malwareschutz (Anti-Virus, Anti-Spyware/Adware)	
	Anti-Bot	
	Anti-Spam & Anti-Phishing	
	Intrusion Detection & Prevention (IDS/IPS)	Layer 2-7
	Data Loss/Leakage Prevention (DLP)	Layer 5-7

Tabelle 1: Funktionsblöcke einer Application Layer Firewall

(Statisches) NAT (Network Address Translation) ermöglicht es, dass die Ziel- oder Quell-IP-Adressen eines Datenpakets durch eine andere Adresse ersetzt werden können. Aufgrund der Knappheit an öffentlichen IPv4-Adressen wird NAT häufig verwendet, um eine Kommunikation zwischen öffentlichen IP-Adressen und privaten IP-Adressen zu ermöglichen (vgl. tutanch 2017).
Ein dynamisches NAT (auch „PAT“ (Port and Address Translation), „Hiding NAT“) bildet mehrere Adressen auf eine einzige ab. Dabei werden auch die Portnummern ausgetauscht. Auf diese Weise können alle privaten Adressen eines Netzwerkes auf eine einzelne öffentliche IP-Adresse abgebildet werden (maximal 65535 Source-Ports stehen zur Verfügung).

Anti-Spoofing ist ein Verfahren, um Pakete mit einer falschen Quelladresse zu identifizieren und zu verwerfen. Bei einem Spoofing-Angriff wird die Quelladresse modifiziert, um eine vertrauenswürdige Quelle vorzutäuschen (vgl. Rouse 2014).

Der Funktionsblock „Applikationsidentifizierung und -filter“ ist dafür zuständig, Applikationen zu identifizieren, zu monitoren und gemäß Regelwerk zu erlauben oder zu blocken. Meist werden Applikationsfilter umgesetzt, indem nach Kategorien oder Tags gefiltert wird.

Content Filter ermöglichen eine Filterung auf Basis von Zeichenketten. Diese Zeichenketten können vorgegeben werden. Eine Realisierung mittels Kategorien ist auch hier möglich. Gängige Kategorien sind zum Beispiel „Sex“ oder „Rechtsextremismus“.

Über die URL Filterung können konkrete URLs oder URL-Kategorien erlaubt/geblockt werden. Eine Realisierung über Black- und Whitelists ist ebenfalls üblich. Typische Kategorien sind beispielsweise „Erwachsene und Pornographie“, „Botnetze“, „Bestätigte Spam-Quellen“, „Glücksspiel“ und weitere.

Mithilfe von File Policies können bestimmte File-Extensions für konkrete Protokolle wie z.B. HTTP, SMTP, IMAP, POP & FTP erlaubt oder blockiert werden. Übliche File-Kategorien sind „Ausführbare Dateien“, „Systemdateien“ oder auch „Archive“. Bei Archiven wird meist eine bestimmte Maximaltiefe für die Analyse über den Hersteller definiert.

Über DNS Policies können Black- und Whitelists erstellt werden, welche vorgeben, welche DNS Server genutzt werden dürfen und welche nicht. So können bösartige Hosts (beispielweise von Angreifern oder auch Bots) rausgefiltert werden.

User-basiertes Firewalling ermöglicht eine differenziertere Zugriffssteuerung basierend auf den Identitäten der Benutzer. Auf diese Art können Zugriffe und Regeln auf der Grundlage von Benutzer und Benutzergruppen alternativ zu IP-Adressen konfiguriert werden. Damit diese Funktion nutzbar ist, ist eine Kopplung der Firewall beispielweise mit einer Benutzerdatenbank wie dem AD (Active Directory) nötig.

Malwareschutz stellt einen weiteren Funktionsblock der Application Layer Firewall dar. Dieser Schutz beinhaltet unter anderem Anti-Virus oder auch Anti-Spyware/Adware. Bei Anti-Virus wird zwischen klassischen auf Signaturen basierenden Anti-Viren-Systemen und Datei-Signaturen basierenden Anti-Viren-Systeme (Beispiel: Cisco AMP) unterschieden. Bei Datei-Signaturen basierenden Systemen wird jede Datei bzw. jedes Objekt über einen eindeutigen Hash-Wert identifiziert. Ist etwas unbekannt, dann sind häufig dynamische Analysen (Sandboxing) inbegriffen, bei der Dateien in die Cloud geladen werden können oder auch in ein lokales System, um dort analysiert zu werden. Anti-Spyware/Adware ist Software,

die spezialisiert ist, Spyware (z.B. Keylogger) und (aggressive) Werbung zu erkennen und zu filtern.

Das Anti-Bot-Funktionsmodul prüft, an welche Adresse und Port (meistens HTTP/HTTPS) etwas geschickt wird und vergleicht das mit einer Datenbank mit bekannten, bösartigen Adressen/Ports (Bot-Netze). Auf diese Weise kann die Kommunikation mit Bot-Netzen verhindert werden.

Das Funktionsmodul Anti-Spam verhindert hauptsächlich die Zustellung von unerwünschten Emails, häufig auch mit werbenden Inhalten. Anti-Phishing soll die Zustellung von betrügerischen Emails unterbinden. Beim Phishing wird häufig eine Reihe von Social-Engineering-Techniken eingesetzt, um die Email möglichst echt wirken zu lassen, um den Leser dazu zu bewegen, persönliche und oft auch finanzielle Daten preiszugeben.

Bei der Intrusion Detection und Prevention geht es im Allgemeinen darum, Angriffe zu erkennen, zu monitoren oder auch aktiv zu verhindern bzw. abzuwehren. Intrusion Detection Systeme (IDS) dienen der Erkennung. Intrusion Prevention Systeme (IPS) hingegen wehren Angriffe darüber hinaus auch aktiv ab. IDS/IPS wird ermöglicht auf Grundlage einer Datenbank. Wie auch alle anderen Datenbanksätze der anderen Funktionsmodule sollte auch dieser Satz an Daten in regelmäßigen Abständen auf der Application Layer Firewall aktualisiert werden. Denn diese Datenbank ermöglicht es dem IDS, Angriffe anhand von Auffälligkeiten oder bekannter Angriffsmuster im Netz zu erkennen und sollte dementsprechend möglichst aktuell sein, um auch neuste Angriffe abwehren zu können. Der Inhalt der Datenbank richtet sich nach einer einstellbaren Sicherheitsstufe und kann häufig auch manuell angepasst werden. Auch Anomalien (signifikante Abweichungen vom Normalbetrieb) sollte ein IDS erkennen können. Das Besondere bei einem IDS ist, dass Angriffe auch nach Durchqueren der Firewall erkannt werden können. Beim IPS/IDS wird zwischen unterschiedlichen Arten unterschieden. Die Realisierung eines IDS/IPS auf einer Application Layer Firewall stellt ein Netzwerkbasiertes IDS/IPS dar. Es gibt auch hostbasierte IDS/IPS, die direkt auf dem zu überwachenden bzw. zu schützenden System installiert sind. Außerdem gibt es noch sogenannte hybride Systeme, die beide Arten kombinieren.

Data Loss/Leakage Prevention/Protection (DLP) ist eine Sicherheitstechnik um Datenverlust bzw. Datendiebstahl zu unterbinden. Datenverlust bzw. Datendiebstahl kann auf diverse Arten herbeigeführt werden, beispielsweise beim Übertragen von Nachrichten oder Dateien (über Emails, File Transfer, Uploads, etc.). Daten können aber auch über Medien wie USB-Sticks, CDs, DVDs oder andere Speichermedien abfließen. DLPs sollten dazu in der Lage sein, sensible Daten im Unternehmen zu identifizieren und nach der Identifizierung deren Nutzung bzw. deren Verbreitung zu kontrollieren. Konzept von DLPs ist es, auch im Fall von Versagen anderer Funktionsmodule der Application Layer Firewall wie Anti-Virus, den Verlust und Diebstahl sensibler Daten dennoch zu verhindern.

Eine Abgrenzung zwischen den Funktionsmodulen ist nicht immer eindeutig möglich. Es ist erkennbar, dass Maßnahmen an unterschiedlichen Stellen realisiert werden können. Beispielweise können Maßnahmen gegen Botnetze über URL-Filterung, DNS-Policies und auch über das Funktionsmodul „Anti-Bot“ ermöglicht werden. Weitere Realisierungen sind möglich. Auch Anti-Spam kann an unterschiedlichen Stellen umgesetzt werden (beispielweise über das Funktionsmodul Anti-Spam, aber auch über Applikationsfilter, Content-Filter und URL-Filter). Auch hier sind andere oder ergänzende Maßnahmen denkbar. Im Allgemeinen besteht eine Abhängigkeit innerhalb der Module und Prävention wird so mehrfach in unterschiedlicher Ausprägung umgesetzt.

2.4 Abgrenzung Application Layer Firewall und Web Application Firewall

Web Application Firewalls (WAFs) stellen eine besondere Form von Application Layer Firewalls dar. Sie finden ihren Einsatz insbesondere in Firmen, dessen Existenz von ihren Webressourcen abhängt. WAFs sind darauf spezialisiert, alle HTTP/HTTPS/SOAP/XML-RPC/Web-Service-Anfragen und -Antworten zu untersuchen und Angriffssignaturen, sowie ungewöhnliche Verhaltensmuster zu identifizieren (vgl. Rouse 2015). Sie kontrollieren den Datentransfer von Web-Clients zu Web-Servern. Die Kommunikationsrichtung verläuft also in der Regel vom öffentlichen Bereich, dem Internet, zum teilöffentlichen Bereich, in dem Serverfarmen angesiedelt sind. Die Abbildung 7 zeigt die beschriebene Funktionsweise einer Web Application Firewall (WAF). In der folgenden Arbeit wird auf diese Art von Firewalls nicht weiter eingegangen.

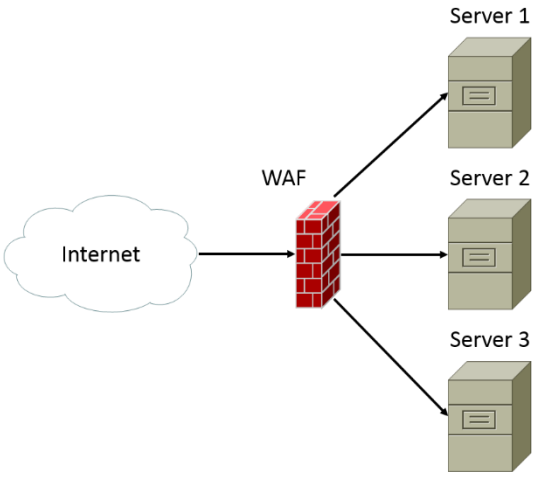


Abbildung 7: Funktionsweise einer Web Application Firewall (WAF)

3 Proxy

In diesem Kapitel wird der Proxy als ein Bestandteil des Übergangs zweier Zonen mit unterschiedlichem Sicherheitsniveau definiert. Verschiedene Unterscheidungen hinsichtlich technischer Aspekte, sowie hinsichtlich der Anwendung werden dargestellt. Dabei werden Beispiele bezüglich ihrer Funktionen erläutert.

3.1 Definition

Ein Proxy stellt eine zentrale Vermittlungsstelle dar, indem er Anfragen entgegennimmt und über eine neue Session eine Verbindung zur anderen Seite über einer seiner Adressen herstellt.

3.2 Technische Unterscheidung

Beim Proxy trifft man eine wesentliche technische Unterscheidung zwischen Application Level Proxys und Circuit Level Proxys.

3.2.1 Circuit Level Proxy (Generic Proxy)

Ein Circuit Level Proxy oder auch Generic Proxy ist nicht auf ein bestimmtes Anwendungsprotokoll spezialisiert. Er arbeitet auf Transportebene (ISO/OSI-Referenzmodell Layer vier). Konkret bedeutet das, dass diese Art von Proxy die Header bis Layer vier modifiziert, die nachfolgenden Daten (Layer fünf bis sieben) jedoch unangetastet kopiert.

3.2.2 Application Level Proxy (Dedicated Proxy)

Ein Application Level Proxy oder auch Dedicated Proxy analysiert Daten bis zur Anwendungsebene (ISO/OSI-Referenzmodells bis Layer sieben). Daraufhin werden diese entweder verworfen oder verändert bzw. unverändert weitergeleitet. Meist steht dabei ein bestimmter Dienst im Fokus: Web (HTTP, HTTPS), File-Transfer (FTP, SFTP, …), Email (SMTP,

IMAP, POP) und andere Dienste. Ein Application Level Proxy ist auf das zugehörige Anwendungsprotokoll angepasst und versteht und interpretiert die Kommandos dieses Anwendungsprotokolls.

3.3 Anwendung

Im Folgenden werden zwei Anwendungen von Proxys unterschieden, indem es darum geht, die Kommunikationsrichtung zu betrachten.

3.3.1 Forward Proxy

Ein Forward Proxy betrachtet die Kommunikationsrichtung vom internen Bereich in den öffentlichen Bereich. Ein wesentlicher Nutzen eines Forward Proxy ist der Schutz der Identität einzelner Clients. Forward Proxys leiten Anfragen eines Clients an einen Server weiter. Die Abbildung 8 bildet die beschriebene Funktionsweise eines Forward Proxy ab.

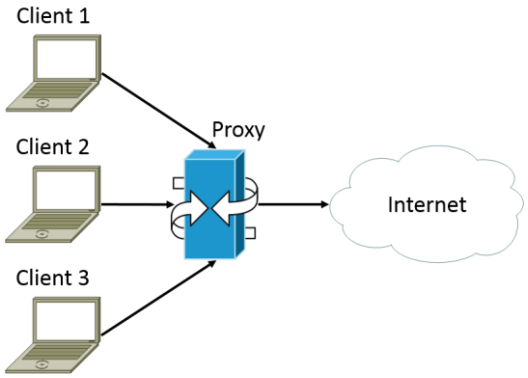


Abbildung 8: Funktionsweise eines Forward Proxy

3.3.2 Reverse Proxy

Ein Reverse Proxy betrachtet die Kommunikationsrichtung vom öffentlichen Bereich in den internen Bereich. Ein wesentlicher Nutzen eines Reverse Proxy ist der Schutz der Identität von Servern. Der Datenverkehr wird über den Proxy an den betreffenden Server weitergeleitet. Dabei werden viele Server wie ein einzelner dargestellt, was einen Angriff erschwert. Ein weiterer Nutzen ist die Möglichkeit des Load Balancing[1], es erfolgt eine Weiterleitung der Anfrage an den Server mit den meisten Kapazitäten. Die folgende Abbildung (Abbildung 9) demonstriert die beschriebene Funktionsweise eines Forward Proxy.

[1] Load Balancing als Funktionsbestandteil eines Reverse Proxys ermöglicht:
- Lastverteilung
- Sicherung der Verfügbarkeit

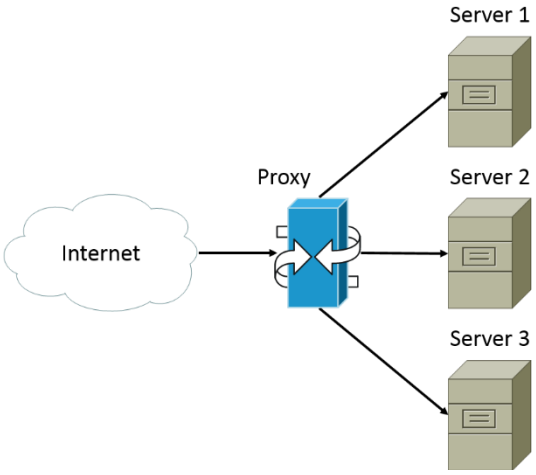


Abbildung 9: Funktionsweise eines Reverse Proxy

3.4 Beispiele und deren Funktionen

Nachfolgend werden zwei populäre Proxy Beispiele erläutert und Funktionen dieser konkret betrachtet.

3.4.1 Web-Proxy

Ein Web-Proxy (auch HTTP-Proxy) kann je nach Hersteller unter anderem folgende Funktionsblöcke realisieren:

Abbildung 10: Mögliche Funktionsblöcke eines Web-Proxys

- Proxy Mode (Transparent & Explicit Forwarding)
- Authentifizierung (Benutzerdatenbank)
- Identities, Policies & Filter (Access Policy, URL-Kategorien, Applikationsfilter, Objekt Filter, MIME-Typ Filter, Anti-Virus Scanning)
- HTTP/HTTPS (HTTPS aufbrechen, blocken oder erlauben, Zertifikate)
- Upload Scanning, DLP (Data Loss/Leakage Prevention)

Neben dem Dienst Web (HTTP, HTTPS) wird auch oft File-Transfer (Protokolle wie FTP, SFTP, SCP, TFTP, …) durch Web-Proxys mit unterstützt.

Häufig stellen Proxy-Hersteller unterschiedliche Proxy Modi bereit. Typische Modi sind beispielsweise „Explicit Forwarding“ und „Transparent Forwarding“. Beim expliziten Forwarding wird beim Client ein fester Proxy (beispielsweise im Web-Browser oder über PAC-Files) eingestellt. Die Abkürzung PAC steht für Proxy Auto-Configuration. Der Client richtet seine Anfragen an den Proxy. Beim transparenten Forwarding richtet der Client seine Anfragen nicht an den Proxy, sondern an das eigentliche Ziel. Der Proxy muss im Datenpfad liegen und es ist oft eine angepasste Netzwerkinfrastruktur von Nöten, damit der Web-Verkehr zum Proxy geleitet wird. Es ist beispielsweise üblich PBR (Policy Based Routing) oder auch das WCCP (Web Cache Communication Protocol) dafür zu nutzen.

Ein weiterer Funktionsblock von Web-Proxys ist die Authentifizierung. Eine Authentifizierung kann mittels einer Benutzerdatenbank wie AD (Active Directory) oder auch mittels LDAP (Lightweight Directory Access Protocol) realisiert werden. Protokolle wie HTTP und FTP sehen Authentifizierung vor.

Identities, Policies und Filter bilden einen weiteren Funktionsblock von Web-Proxys. So können Einschränkungen für konkrete Anwender bzw. Anwendergruppen getroffen werden. Es können beispielsweise URL-Kategorien, Applikationsfilter, Objekt Filter oder auch MIME-Typ Filter gesetzt werden. Zeitabhängige Filter oder auch das Filtern von Objektgrößen sind möglich. Außerdem kann in diesem Block Anti-Virus Scanning mittels eines Scanners (Sophos, Webroot, McAfee, AMP, …) ermöglicht werden. Die Kombination von mehreren unterschiedlichen Herstellern ist üblich. Anti-Virus wird bei Proxys auch oft als externe Funktion umgesetzt, d.h. auf einer separaten Komponente, die mit dem Proxy verknüpft ist.

Über den Funktionsblock „HTTP/HTTPS“ können Regeln definiert werden, die festlegen, ob HTTP aufgebrochen, geblockt oder erlaubt werden soll, zum Beispiel in Hinblick auf URL-Kategorien. Eine Entschlüsselung bzw. Verschlüsselung wird über dieses Modul realisiert.

Des Weiteren bildet Upload Scanning einen weiteren Funktionsblock. Es ist möglich, auch für Uploads einen AV-Scan durchzuführen und Policies für Uploads festzulegen. Außerdem kann an dieser Stelle DLP (Data Loss/Leakage Prevention) (Erklärung von DLP siehe Abschnitt 2.3) bereitgestellt werden. Häufig wird dies über einen externen DLP Server (ein extra Produkt) umgesetzt.

3.4.2 Email-Proxy

Ein Email-Proxy, dessen Fokus auf dem Dienst Email (Email-Protokolle wie SMTP, IMAP, POP) liegt, kann je nach Hersteller unter anderem folgende Funktionsblöcke realisieren:

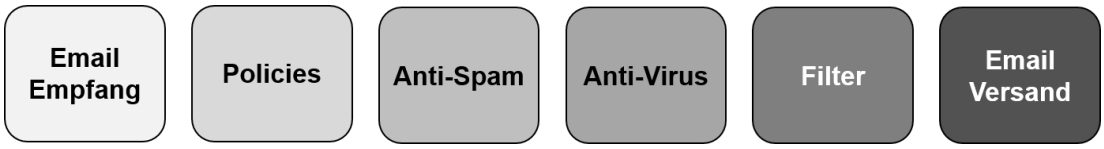


Abbildung 11: Mögliche Funktionsblöcke eines Email-Proxys

- Email Empfang (Entschlüsselung, Authentifizierung)
- Policies (Mail Routing, Aliasing, Masquerading)
- Anti-Spam (Spam-Quarantäne, Bounces (Profile))
- Anti-Virus (Systeme, Policy für AV)
- Filter (Attachments, Content, Web-Link-Filter (Anti-Phishing), DLP)
- Email Versand (Verschlüsslung, Authentifizierung, Signatur)

Der erste Funktionsblock realisiert den Email Empfang. An dieser Stelle kann, wenn nötig, eine Entschlüsselung erfolgen. Gängige Verschlüsselungstechniken sind TLS (Transport Layer Security), S/MIME (Secure/Multipurpose Internet Mail Extensions) oder auch PGP (Pretty Good Privacy). Mail Authentifizierung beispielsweise in Form von DKIM (DomainKey Indentified Mail) Verifikation oder auch SPF (Sender Policy Framework) Verifikation ist möglich.

Im nächsten Modul können diverse Policies für Mail-Empfang und –Versand definiert werden. Falls Mail Routing, Aliasing und/oder Masquerading erforderlich wird, ist beispielsweise eine Realisierung über LDAP denkbar.

Der Funktionsblock „Anti-Spam“ definiert, für welche Sender und Empfänger Spam-Filterung erfolgen soll. Spam Quarantäne ist möglich. Dabei sind häufig Einstellungen möglich, die den Zugriff auf die Quarantäne oder auch Benachrichtigungen an Mail-Anwender regeln.

Ein weiteres Modul behandelt „Anti-Virus“ mittels eines oder mehreren Anti-Viren-Scannern (Sophos, McAfee, AMP, Outbreak-Filter, …). Genau wie beim Web-Proxy wird Anti-Virus oder hier auch Anti-Spam manchmal als externe Funktion umgesetzt, d.h. auf einer separaten Komponente, die mit dem Proxy verknüpft ist. Außerdem können diverse unterschiedliche Policies für Anti-Virus festgelegt werden, die beispielweise bestimmen, ob erkannte Sicherheitsrisiken direkt gedropped werden oder in Quarantäne kommen oder ob das Scanning für ein- oder ausgehenden Verkehr erfolgen soll. Es kann auch eingestellt werden, welche Benutzer oder –gruppen bzw. File-Typen keinen Scann erfordern. Des Weiteren können Policies für unscannbare und verschlüsselte Daten festgelegt werden.

Filter können unterschiedliche Ausprägungen haben. Es können beispielsweise Attachment Typen gefiltert werden, es kann nach (nicht-)verschlüsselten Anhängen oder nach Stichwörtern im Body und/oder im Attachment gesucht werden. Außerdem können auch Filter für die Größe der Mail festgelegt werden, Web-Link-Filter (Anti-Phishing) sind ebenfalls denkbar. Darüber hinaus kann an dieser Stelle auch DLP Software genutzt werden (Erklärung von DLP siehe Abschnitt 2.3).

Email Versand beinhaltet eine mögliche Verschlüsselung sowie die Signatur.

4 Anwendung – Kombination von Application Layer Firewall und Proxy

Um die Funktionsweise einer Application Layer Firewall besser nachvollziehen zu können und um das Zusammenspiel von Application Layer Firewall und Proxy nachzustellen und zu testen, wird ein Laboraufbau entwickelt. Dieser wird skizziert, Konfigurationen werden dargelegt und Tests werden abgebildet. Daraus folgende Ergebnisse werden dargestellt.

4.1 Laboraufbau

Folgende Abbildung (Abbildung 12) zeigt den Laboraufbau:

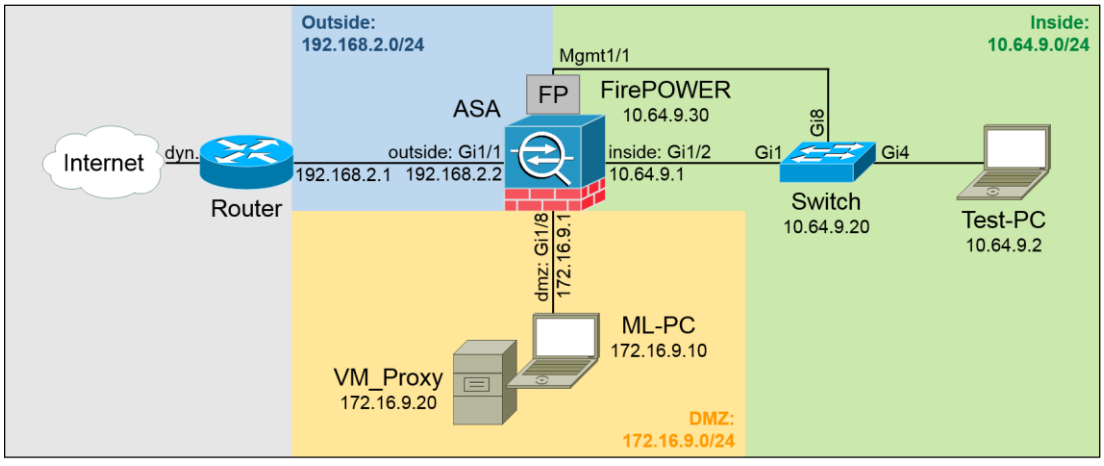


Abbildung 12: Topologie des Laboraufbaus

Dabei dominieren drei Netzwerkkomponenten den Aufbau:

1. Die Application Layer Firewall: Cisco ASA5506-X mit FirePOWER Services mit einer Control License
2. Ein PC, auf dem mittels einer Virtuellen Maschine mit dem Betriebssystem Ubuntu (17.10) der Web-Proxy Squid (Version 3.5.23) realisiert wird
3. Ein weiterer PC, der als Test-PC dienen soll

Außerdem ist das dargestellte Netzwerk in drei unterschiedliche Sicherheitszonen unterteilt:

1. Outside (öffentlich)
2. DMZ (Demilitarized Zone, teilöffentlich)
3. Inside (intern)

Die Application Layer Firewall dient als Zonenübergang zum einen von der Zone „Inside“ zur Zone „DMZ“ und zum anderen als Übergang von der Zone „DMZ“ zur Zone „Outside“. Der PC, über den der Proxy realisiert wird, ist in der Zone „DMZ“ positioniert. Der Test-PC ist in der Zone „Inside“ positioniert.

4.2 Konfiguration Stateful Inspection Firewall

In diesem Abschnitt wird die Konfiguration der Cisco ASA (Stateful Inspection Firewall) dargestellt. Es wurden insgesamt drei Interfaces konfiguriert, die die Abtrennung der Zonen ermöglichen (siehe Listing 1). Dabei wurden die Security-Level so gewählt, dass die Inside-Zone mit der höchsten Sicherheitsstufe assoziiert wird, die DMZ-Zone mit einer mittleren Sicherheitsstufe und die Outside-Zone mit der niedrigsten Sicherheitsstufe. Daraus folg, dass Verkehr initiiert von „Inside“ nach „DMZ“ und „Outside“ erlaubt ist. Verkehr initiiert von „DMZ“ ist Richtung „Outside“ erlaubt, Richtung „Inside“ nicht. Verkehr initiiert von „Outside“ ist weder in Richtung „DMZ“ noch in Richtung „Inside“ erlaubt.

```
1  !
2  interface GigabitEthernet1/1
3   nameif outside
4   security-level 0
5   ip address 192.168.2.2 255.255.255.0
6  !
7  interface GigabitEthernet1/2
8   nameif inside
9   security-level 100
10  ip address 10.64.9.1 255.255.255.0
11 !
12 interface GigabitEthernet1/8
13  nameif dmz
14  security-level 50
```

```
 ip address 172.16.9.1 255.255.255.0
!
```

Listing 1: Interface-Konfiguration der ASA

Darüber hinaus wurde ein dynamisches NAT konfiguriert, eine Zuweisung zwischen Access-Liste und Interface hergestellt sowie die Default Route definiert (siehe Listing 2). Verwendete Netzwerkobjekte zeigt Listing 3.

```
!
nat (inside,outside) after-auto source dynamic sn_ML-INSIDE
 interface
nat (dmz,outside) after-auto source dynamic sn_ML-DMZ interface
access-group outside_access_in in interface outside
access-group inside_access_in in interface inside
access-group dmz_access_in in interface dmz
route outside 0.0.0.0 0.0.0.0 192.168.2.1 1
!
```

Listing 2: NAT-Konfiguration, Zuweisung zwischen Access-Liste und Interface & Default Route

```
!
object network sn_ML-DMZ
 subnet 172.16.9.0 255.255.255.0
!
object network sn_ML-INSIDE
 subnet 10.64.9.0 255.255.255.0
!
```

Listing 3: Verwendete Netzwerkobjekte

Um den Verkehr nach dem Prinzip „Deny-All“ gezielt einzuschränken, wurde pro Interface eine Access-Liste definiert. Für das Interface „inside“ wird nach außen DNS und HTTP bzw. HTTPS erlaubt. Diese Freischaltung dient lediglich für den ersten Test, bei dem zunächst ohne Proxy-Konfiguration Applikationsfilterung geprüft wird. Außerdem ist der Port 3128 mit der Proxy-IP als Ziel freigeschaltet. Der restliche Verkehr wird geblockt. Diese Freischaltung dient für den zweiten Test, bei dem die Applikationsfilterung unter Voraussetzung, dass der Internetverkehr über den Proxy geleitet wird, getestet wird. Die Konfiguration der Access-Liste für das inside-Interface ist in Listing 4 dargestellt.

```
!
access-list inside_access_in remark INET_Name-Service
access-list inside_access_in extended permit udp object
 ip4_Test-PC object ip4_DNS-Root-Server eq domain
!
access-list inside_access_in remark INET_Web-Service
```

```
7  access-list inside_access_in extended permit tcp object
8   ip4_Test-PC any eq www
9  access-list inside_access_in remark INET_Web-Service
10 access-list inside_access_in extended permit tcp object
11  ip4_Test-PC any eq https
12 !
13 access-list inside_access_in remark Proxy rule
14 access-list inside_access_in extended permit tcp object
15  ip4_Test-PC object ip4_VM_Proxy eq 3128
16 !
17 access-list inside_access_in remark Implicit rule
18 access-list inside_access_in extended deny ip any
19 !
```

Listing 4: Access-Liste für das inside-Interface

Für das Interface „dmz“ wird nach außen nur DNS und HTTP bzw. HTTPS erlaubt. Die Konfiguration der Access-Liste für das dmz-Interface zeigt Listing 5.

```
1  !
2  access-list dmz_access_in remark INET_Name-Services
3  access-list dmz_access_in extended permit udp object
4   ip4_VM_Proxy object ip4_DNS-Root-Server eq domain
5  !
6  access-list dmz_access_in remark INET_Web-Services
7  access-list dmz_access_in extended permit tcp object
8   ip4_VM_proxy any eq www
9  access-list dmz_access_in remark INET_Web-Services
10 access-list dmz_access_in extended permit tcp object
11  ip4_VM_Proxy any eq https
12 !
13 access-list dmz_access_in remark Implicit rule
14 access-list dmz_access_in extended deny ip any
15 !
```

Listing 5: Access-Liste für das dmz-Interface

Für das Interface „outside“ wird der gesamte Verkehr geblockt. Die Konfiguration der Access-Liste für das outside-Interface wird in Listing 6 abgebildet.

```
1 !
2 access-list outside_access_in remark Implicit rule
3 access-list outside_access_in extended deny ip any
4 !
```

Listing 6: Access-Liste für das outside-Interface

Verwendete Netzwerkobjekte innerhalb der Access-Listen zeigt Listing 7.

```
!
object network ip4_DNS-Root-Server
 host 141.1.1.1
!
object network ip4_Test-PC
 host 10.64.9.2
!
object network ip4_VM_Proxy
 host 172.16.9.20
!
```

Listing 7: Verwendete Netzwerkobjekte

Außerdem wird eine Service-Policy zur FirePOWER-Einbindung definiert. Diese wird in Listing 8 dargestellt.

```
!
class-map inside-class
 match any
class-map dmz-class
 match any
!
policy-map dmz-policy
 class dmz-class
  sfr fail-open
policy-map inside-policy
 class inside-class
  sfr fail-open
!
service-policy inside-policy interface inside fail-close
service-policy dmz-policy interface dmz fail-close
!
```

Listing 8: Service-Policy zur FirePOWER-Einbindung

4.3 Konfiguration & Tests Application Layer Firewall

In diesem Abschnitt wird die Konfiguration des FirePOWER-Moduls der Cisco ASA (Application Layer Firewall) dargestellt. Es werden zwei Tests durchgeführt:

1. Test: Blockierung der Applikation „Facebook“ ohne Proxy-Konfiguration
2. Test: Blockierung der Applikation „Facebook“ mit Proxy-Konfiguration

Bei dem ersten Test wird über das FirePOWER-Regelwerk die Applikation „Facebook“ für die Test-PC IP-Adresse als Quelle geblockt. Der Webzugriff des Test-PCs erfolgt in diesem Fall direkt ohne Umleitung über den Proxy. Die Folgende Tabelle (Tabelle 2) zeigt das FirePOWER-Regelwerk für den 1. Test.

#	Name	Source	Destination	Applications	Source Ports	Dest. Ports	URLs	Action
1	Test-block-Application-1	Test-PC	any	Tags: Facebook	any	any	any	Block with reset

Tabelle 2: FirePOWER Regelwerk (Test1)

Im Logging (siehe Abbildung 13) mit Filterung auf die IP des Test-PCs (10.64.9.2) sowie mit Filterung auf die Web Applikation „Facebook“ ist erkennbar, dass die Anfrage geblockt wird.

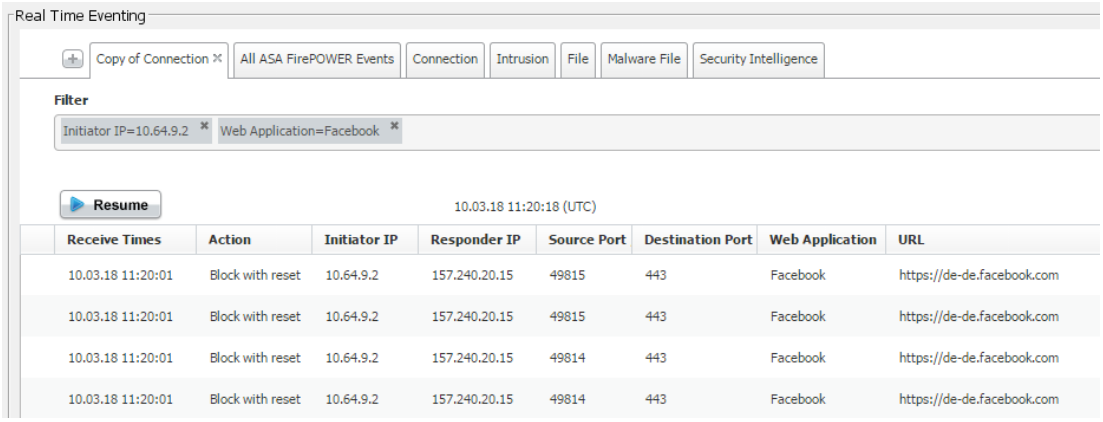


Abbildung 13: FirePOWER Logging (Test1)

Im Web-Browser des Tests-PCs ergibt sich folgende Fehlermeldung beim Aufruf von https://de-de.facebook.com (siehe Abbildung 14):

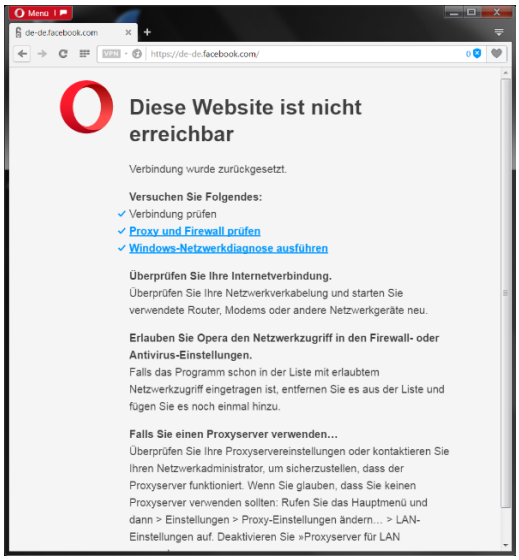


Abbildung 14: Aufruf von https://de-de.facebook.com im Web-Browser des Test-PCs

Außerdem ist klar erkennbar, dass Inhalte wie der Facebook Button aus externen Seiten herausgefiltert werden. Folgende Abbildungen zeigen die Darstellung im Web-Browser des Test-PCs vor (siehe Abbildung 15) und nach (siehe Abbildung 16) der Aktivierung der „Test-block-Application-1“-Regel.

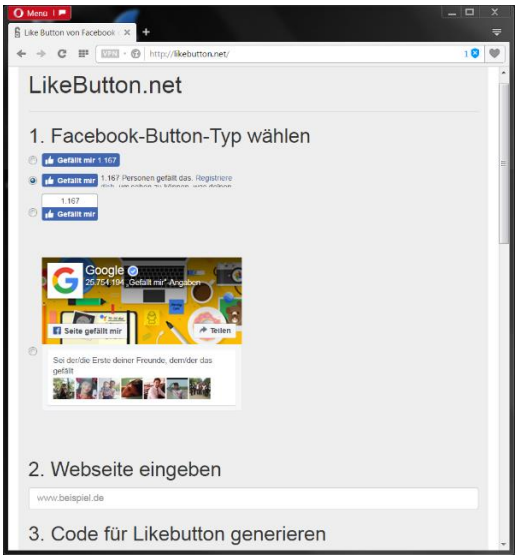


Abbildung 15: Darstellung vor Aktivierung der „Test-block-Application-1“-Regel

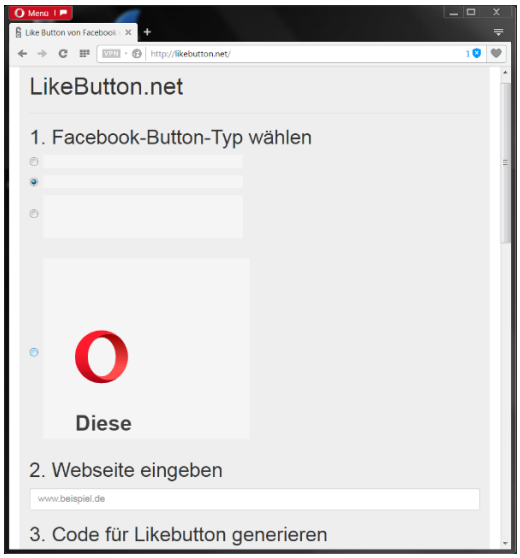


Abbildung 16: Darstellung nach Aktivierung der „Test-block-Application-1“-Regel

Bei dem zweiten Test wird über das FirePOWER-Regelwerk die Applikation „Facebook“ für die Proxy IP-Adresse als Quelle geblockt. Die Folgende Tabelle (Tabelle 3) zeigt das FirePOWER-Regelwerk für den 2. Test.

#	Name	Source	Destination	Applications	Source Ports	Dest. Ports	URLs	Action
1	Test-block-Application-2	Proxy	any	Tags: Facebook	any	any	any	Block with reset

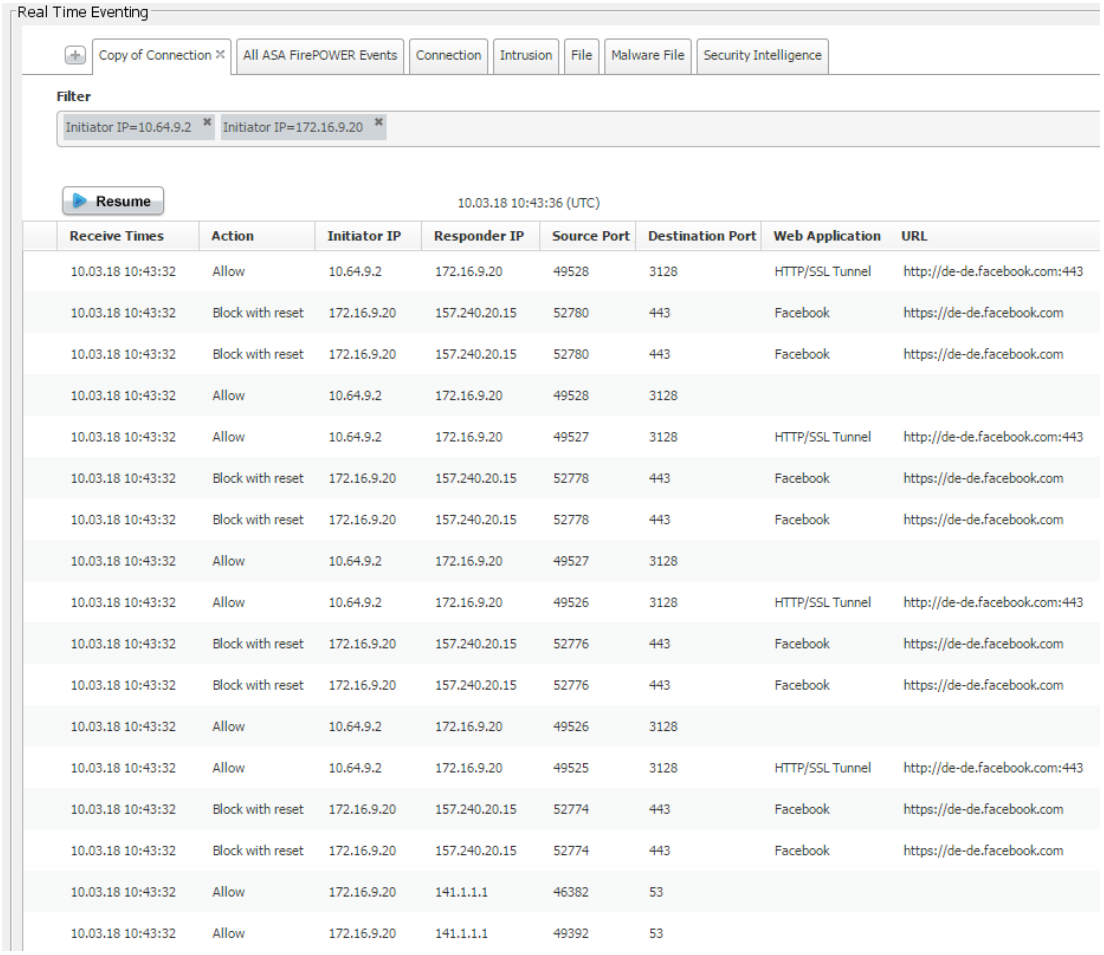
Tabelle 3: FirePOWER Regelwerk (Test2)

Der Webzugriff des Test-PCs erfolgt in diesem Fall mit Umleitung über den Proxy. Dafür muss die default Squid Konfiguration (siehe Listing 9) in der VM auf dem PC „ML-PC“ angepasst werden und der Service muss neu gestartet werden. Außerdem muss im Web-Browser des Clients der Proxy eingetragen werden.

```
1 acl localnet src 10.64.9.0/24
2 http_access allow localnet
```

Listing 9: Squid Konfiguration

Im Logging (siehe Abbildung 17) mit Filterung auf die IP des Test-PCs (10.64.9.2) sowie mit Filterung auf die IP des Proxys (172.16.9.20) ist erkennbar, dass der HTTP/HTTTPS-Verkehr über den Proxy läuft. DNS-Anfragen laufen ebenfalls über den Proxy. Außerdem ist erkennbar, dass die Web Applikation „Facebook“ nur noch der Kommunikation zwischen Proxy und Facebook-Server zugeordnet wird. Für die Kommunikation zwischen Client und Proxy wird die Applikation „HTTP/SSL Tunnel“ erkannt. Woraus sich ergibt, dass keine Zuordnung zwischen der Applikation „Facebook“ und dem Client gezogen wird. Lediglich über die angefragte URL des Clients (https://de-de.facebook.com:443) lässt sich ein Zusammenhang herstellen.



Real Time Eventing

Copy of Connection | All ASA FirePOWER Events | Connection | Intrusion | File | Malware File | Security Intelligence

Filter

Initiator IP=10.64.9.2 | Initiator IP=172.16.9.20

Resume 10.03.18 10:43:36 (UTC)

Receive Times	Action	Initiator IP	Responder IP	Source Port	Destination Port	Web Application	URL
10.03.18 10:43:32	Allow	10.64.9.2	172.16.9.20	49528	3128	HTTP/SSL Tunnel	http://de-de.facebook.com:443
10.03.18 10:43:32	Block with reset	172.16.9.20	157.240.20.15	52780	443	Facebook	https://de-de.facebook.com
10.03.18 10:43:32	Block with reset	172.16.9.20	157.240.20.15	52780	443	Facebook	https://de-de.facebook.com
10.03.18 10:43:32	Allow	10.64.9.2	172.16.9.20	49528	3128		
10.03.18 10:43:32	Allow	10.64.9.2	172.16.9.20	49527	3128	HTTP/SSL Tunnel	http://de-de.facebook.com:443
10.03.18 10:43:32	Block with reset	172.16.9.20	157.240.20.15	52778	443	Facebook	https://de-de.facebook.com
10.03.18 10:43:32	Block with reset	172.16.9.20	157.240.20.15	52778	443	Facebook	https://de-de.facebook.com
10.03.18 10:43:32	Allow	10.64.9.2	172.16.9.20	49527	3128		
10.03.18 10:43:32	Allow	10.64.9.2	172.16.9.20	49526	3128	HTTP/SSL Tunnel	http://de-de.facebook.com:443
10.03.18 10:43:32	Block with reset	172.16.9.20	157.240.20.15	52776	443	Facebook	https://de-de.facebook.com
10.03.18 10:43:32	Block with reset	172.16.9.20	157.240.20.15	52776	443	Facebook	https://de-de.facebook.com
10.03.18 10:43:32	Allow	10.64.9.2	172.16.9.20	49526	3128		
10.03.18 10:43:32	Allow	10.64.9.2	172.16.9.20	49525	3128	HTTP/SSL Tunnel	http://de-de.facebook.com:443
10.03.18 10:43:32	Block with reset	172.16.9.20	157.240.20.15	52774	443	Facebook	https://de-de.facebook.com
10.03.18 10:43:32	Block with reset	172.16.9.20	157.240.20.15	52774	443	Facebook	https://de-de.facebook.com
10.03.18 10:43:32	Allow	172.16.9.20	141.1.1.1	46382	53		
10.03.18 10:43:32	Allow	172.16.9.20	141.1.1.1	49392	53		

Abbildung 17: FirePOWER Logging (Test2)

4.4 Ergebnisse

Durch das Zusammenschalten von Application Layer Firewall und Proxy in dem skizierten Laboraufbau zeigt sich, dass bei Einsatz beider Netzwerkkomponenten die erkannte Applikation auf einer Application Layer Firewall nicht mehr dem Client zugeordnet werden kann, welcher diese aufgerufen hat. Dadurch, dass der Proxy die Web-Session des Clients terminiert und eine neue Session zum Zielserver aufbaut, wird diese Zuordnung behindert. Beim Einsatz eines Proxys muss das Regelwerk einer Application Layer Firewall darüber hinaus so gestaltet werden, dass die Applikationseinschränkung pauschal für die Proxy IP-Adresse getroffen wird. Eine Unterscheidung nach Client ist somit nicht ohne weiteres möglich. Diese fehlende Zuordnung schränkt das Monitoring und somit auch das Troubleshooting ein, weshalb im Fall einer Kombination beider Techniken Tags oder User-Authentication eingeführt werden sollten, um die Transparenz weiterhin aufrechtzuerhalten.

5 Analyse und Ergebnisse

In diesem Kapitel erfolgt eine Gegenüberstellung von den beiden Sicherheitsmaßnahmen Application Layer Proxy und Application Layer Firewall. Der Verkehrsfluss, der sich bei Einsatz beider Komponenten ergibt, wird dargestellt. Außerdem erfolgt ein Herstellervergleich der Marktführer.

5.1 Vergleich von Application Layer Firewall und Application Layer Proxy

Bei der Gegenüberstellung der beiden Sicherheitsmaßnahmen werden konkrete Unterscheidungsmerkmale veranschaulicht und die Funktionsblöcke beider Techniken werden gegenübergestellt. Darüber hinaus werden Vor- und Nachteile abgewogen.

5.1.1 Unterscheidungsmerkmale

	Application Layer Firewall	Application Layer Proxy
Terminierung von Sessions	✗ (nur bei SSL/TLS)	✓
Deep Packet Inspection	✓	✓
Keine Festlegung auf einen Dienst bzw. einer Dienstgruppe	✓	✗
Gewährleistung der Anonymität von Client/Server	✓ (via NAT)	✓ (via Terminierung)

Tabelle 4: Unterscheidungsmerkmale Application Layer Firewall & Application Layer Proxy

Tabelle 4 veranschaulicht Unterscheidungsmerkmale von Application Layer Firewall und Application Layer Proxy.
Merkmal einer Application Layer Firewall ist, dass sie eine bestehende Session nicht terminiert. Lediglich bei SSL/TLS-Inspection erfolgt zwangsweise eine Terminierung der Session auf Layer fünf des ISO/OSI-Referenzmodells. Application Layer Firewalls ermöglichen im Gegensatz zu klassischen Firewalls (Paketfilter und Stateful Inspection) auch Deep Packet Inspection. Des Weiteren ist eine Firewall nicht auf einen Dienst bzw. eine Dienstgruppe festgelegt.
Merkmal eines Proxys hingegen ist, dass entgegengenommene Sessions stets terminiert werden und über eine neue Session eine Verbindung zur anderen Seite herstellt wird. Dadurch ist Deep Packet Inspection möglich, bei der nicht nur die Header sondern auch der Payload des Datenpaketes auf bestimmte Merkmale überprüft wird. Außerdem ist ein Proxy meist auf ein Dienst bzw. eine Dienstgruppe spezialisiert.

Ein wesentlicher Nutzen eines Proxys ist der Schutz der Identität einzelner Clients (Forward Proxy) bzw. von Servern (Reverse Proxy), der mittels der Terminierung erreicht wird. Wie in Abbildung 18 erkennbar werden beim Proxy bei der Terminierung alle Layer abgebaut und neu aufgebaut.

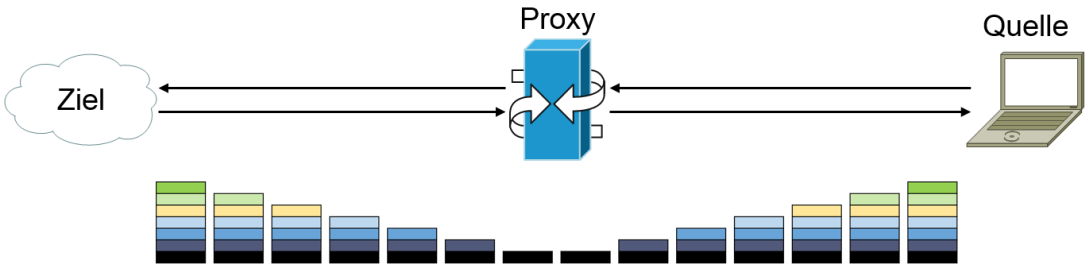


Abbildung 18: Anonymität mittels Terminierung von Sessions

Diese Anonymität kann bei der Firewall mittels NAT (Network Address Translation) oder mittels dynamischem NAT realisiert werden. Dies ist in der Abbildung 19 veranschaulicht. Der IP Packet Header sowie der Frame Header und Trailer werden lediglich von der Firewall modifiziert.

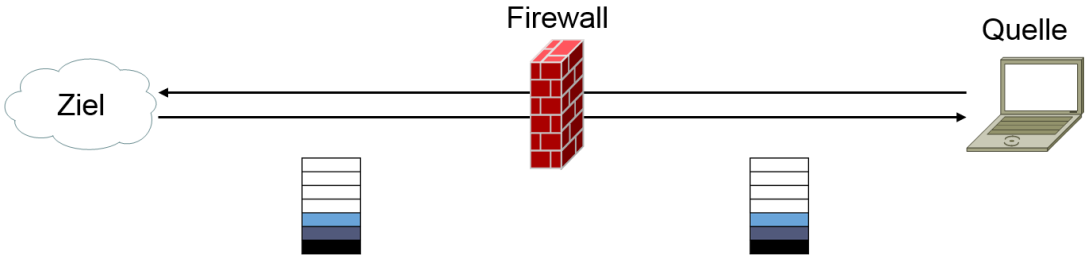


Abbildung 19: Anonymität mittels NAT

5.1.2 Gegenüberstellung der Funktionsblöcke

	Application Layer Proxy	Application Layer Firewall
Web-Proxy	(indirekt über die Session-Terminierung)	Network Address Translation (NAT)
	×	Anti-Spoofing
	(indirekt über die Zuordnung der Sessions beider Kommunikationspartner)	Stateful Inspection
	HTTP/HTTPS	SSL/TLS Inspection
	Identities, Policies & Filter (Access Policy, URL-Kategorien, Applikationsfilter, Objekt Filter, MIME-Typ Filter, …)	Deep Packet Inspection
		Applikationsidentifizierung und -filter
		Content Filterung
		URL Filterung
		File-Policy
		DNS-Policy
	Authentifizierung	User-basiertes Firewalling
	Identities, Policies & Filter (Anti-Virus Scanning)	Malwareschutz (Anti-Virus, Anti-Spyware/Adware), Anti-Bot
	×	Intrusion Detection & Prevention
	Upload Scanning, DLP (Data Loss/Leakage Prevention)	Data Loss/Leakage Prevention (DLP)
Email-Proxy	Email Empfang (Entschlüsselung, Authentifizierung)	×
	Policies (Mail Routing, Aliasing, Masquerading)	×
	Anti-Spam	Anti-Spam
	Anti-Virus	Malwareschutz (Anti-Virus, Anti-Spyware/Adware), Anti-Bot
	Filter (Attachments, Content, Web-Link-Filter (Anti-Phishing), DLP)	File-Policy, Content Filter etc.
		Anti-Phishing
		Data Loss/Leakage Prevention (DLP)
	Email Versand (Verschlüsslung, Authentifizierung, Signatur)	×

Tabelle 5: Gegenüberstellung der Funktionsblöcke von Application Layer Firewall & Application Layer Proxy

Anhand der Tabelle 5 lässt sich erkennen, dass sich Web-Proxy und Application Layer Firewall hinsichtlich ihrer Funktionsblöcke stark ähneln. Alle Funktionsblöcke eines Web-Proxys

lassen sich mit einer Application Layer Firewall abdecken. Die Application Layer Firewall bietet darüber hinaus noch einen weiteren Funktionsblock „Intrusion Detection & Prevention“.
Außerdem bietet eine Application Layer Firewall auch die optionalen traditionellen Funktionen einer Firewall wie NAT und Anti-Spoofing. NAT wird beim Proxy indirekt über die Terminierung der Sessions umgesetzt. Anti-Spoofing-Funktionen stellen Proxys in der Regel nicht bereit.
Stateful Inspection wird bei einem Proxy indirekt umgesetzt, indem der Proxy eine Zuordnung zwischen den Sessions auf beiden Seiten treffen muss und einen zulässigen Verbindungsaufbau bzw. einen zulässigen Verbindungsabbau erkennt.

Der Email-Proxy hingegen weist deutlich mehr Funktionsblöcke auf als die, mit der die Application Layer Firewall dienen kann. Die Funktionalitäten „Anti-Spam“ und „Anti-Virus“ können auch auf einer Application Layer Firewall realisiert werden. Auch „Filter“ sind in einer Application Layer Firewall in Bezug auf Email-Verkehr möglich. Es können zum Beispiel File-Policies oder auch Content-Filter für Protokolle wie SMTP, IMAP und POP definiert werden. Es gibt jedoch einige Funktionsblöcke des Email-Proxys, die eine Application Layer Firewall nicht vorweisen kann, dazu gehören Email Empfang (Entschlüsselung, Authentifizierung), Policies (Mail Routing, Aliasing, Masquerading) und Email Versand (Verschlüsslung, Authentifizierung, Signatur).

Gemäß der dedizierten Betrachtung der Dienste „Web“ und „Mail“ zeigt sich, dass eine Application Layer Firewall zwar die Funktionalitäten eines Web-Proxys übernehmen kann und sogar mit weiteren ergänzt, jedoch nicht alle Funktionalitäten eines Email-Proxys bereitstellt. Daraus ergibt sich im Allgemeinen, dass es Funktionen gibt, die Application Layer Firewalls abdecken und Proxys nicht. Anders herum gibt es aber auch Funktionen, die Proxys abdecken und Application Layer Firewalls nicht.

5.1.3 Vor- und Nachteile beider Komponenten

Eine Application Layer Firewall verfolgt die „All-In-One“-Strategie. Wohingegen beim Application Layer Proxy der Fokus auf jeweils nur einen Dienst bzw. einer Dienstgruppe liegt. Diese unterschiedliche Betrachtungsweise führt zu diversen Vor- und Nachteilen.

Der Vorteil der „All-In-One“-Strategie liegt darin, dass alle Funktionen in einer Komponente gebündelt sind. Dadurch ist es möglich, dass alle Funktionsmodule zusammenarbeiten und sich austauschen, wodurch ein übergeordnetes Zusammenwirken entsteht, welches es ermöglicht, noch gezielter und effizienter Angriffe abzuwehren bzw. Schwachstellen zu kompensieren. Die Zusammenarbeit der Funktionsmodule äußert sich ebenfalls positiv im Bereich des Monitoring, wodurch sehr komplexe, ausführliche und übergreifende Reports erstellt werden können. Außerdem ergeben sich Vorteile für die Administration. Da ein Gerät mehrere Geräte ersetzt, ist nicht das Fachwissen für mehrere Geräte notwendig, sondern

lediglich das Fachwissen für dieses eine Gerät. Es ist ebenfalls zu erwarten, dass der Zeitaufwand sowohl einmalig für die Inbetriebnahme der Application Layer Firewall als auch für die stetige Administration geringer ausfällt als für die Inbetriebnahme und Administration mehrerer Geräte mit einzelnen Funktionalitäten.
Allerdings gibt es auch Nachteile der „All-In-One“-Strategie. Es ergeben sich Abhängigkeiten zwischen den Modulen und durch die Komprimierung vieler Funktionsblöcke in Form einer Hardwarekomponente, fällt Troubleshooting deutlich schwerer, da zunächst das betroffene Modul identifiziert werden muss und darüber hinaus ein Zusammenwirken der einzelnen Module schnell unübersichtlich und unnachvollziehbar wirken kann. Beim Application Layer Proxy entfällt dieser Nachteil, eine Eingrenzung muss nicht getroffen werden und außerdem ist die Funktionsweise aufgrund der Eingrenzung auf einen bestimmten Dienst ohne die Ergänzung von weitere Funktionalitäten wie IDS/IPS besser nachzuvollziehen.
Des Weiteren ist bekannt, dass die Aktivierung von Modulen wie „Anti-Virus“ die Performance einer Application Layer Firewall enorm herabsenkt. So ist es üblich, dass bei Aktivierung aller Funktionen eine deutlich größer dimensionierte Application Layer Firewall benötigt wird. Selbst wenn eine sehr groß dimensionierte Application Layer Firewall ausgewählt wird, ist es häufig so, dass bei der „All-In-One“-Strategie einzelne Funktionsmodule dennoch nicht in derselben Intensität/Qualität bereitgestellt werden, wie es bei einem funktionsspezifischen Gerät möglich ist.

5.2 Betrachtung des Verkehrsflusses

An dieser Stelle wird der Verkehrsfluss betrachtet, der sich bei Einsatz von einer Application Layer Firewall bzw. eines Application Layer Proxy ergibt. Durch die unterschiedlichen Verkehrsflüsse resultieren auch Unterschiede hinsichtlich des Routings, die ebenfalls dargestellt werden. Außerdem wird ein Bezug zu Session-Angriffen hergestellt.

5.2.1 Application Layer Firewall

Folgende Abbildung (Abbildung 20) zeigt den Verkehrsfluss vom internen Bereich in den öffentlichen Bereich beim Einsatz einer Application Layer Firewall. Es existiert eine durchgehende Session vom internen Bereich in den öffentlichen Bereich.

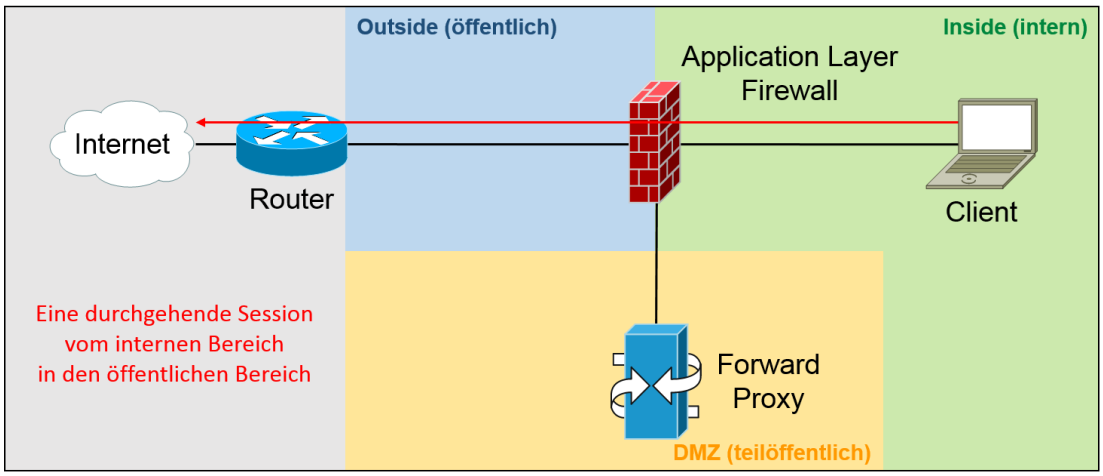


Abbildung 20: Verkehrsfluss beim Einsatz einer Application Layer Firewall

5.2.2 Application Layer Proxy

Folgende Abbildung (Abbildung 21) zeigt den Verkehrsfluss vom internen Bereich in den öffentlichen Bereich beim Einsatz eines Application Layer Proxys. Es existiert keine durchgehende Session vom internen Bereich in den öffentlichen Bereich.

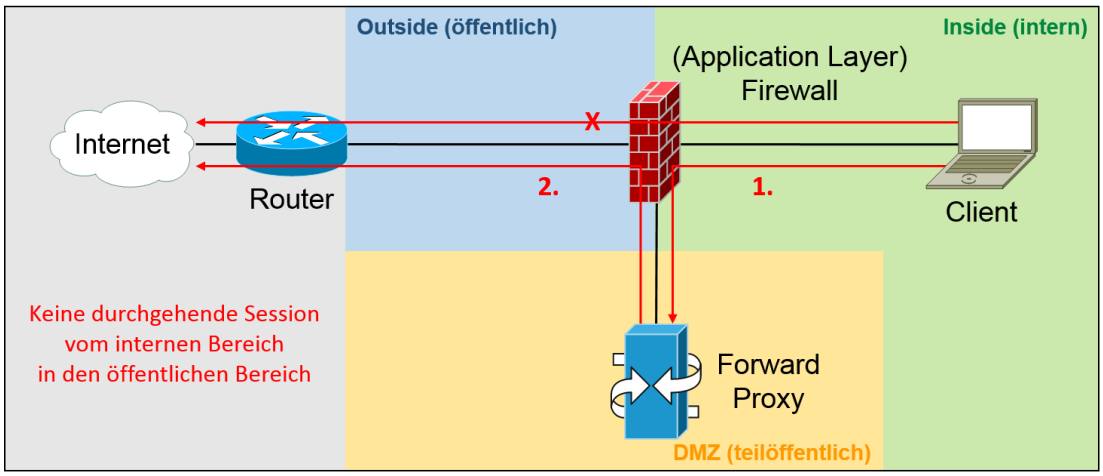


Abbildung 21: Verkehrsfluss beim Einsatz eines Application Layer Proxys

5.2.3 Routing

Durch die Betrachtung des Verkehrsflusses ergeben sich Unterschiede für das Routing. Die Default-Route ist eine Standardroute, die greift, wenn keiner der anderen konkreten Routen für eine angegebene Zieladresse ermittelt werden kann. Bei einer Default-Route wird das Ziel mit 0.0.0.0/0 angeben. Als Gateway wird häufig ein Router angegeben, der eine Verbindung

zum Internet verfügt. Alle Pakete mit einem Ziel außerhalb des lokalen Netzwerkes werden über die Default-Route ins Internet geroutet.

Beim Einsatz einer Application Layer Firewall ist es nötig, dass eine Default-Route im internen Netz definiert ist.
Beim Einsatz eines Application Layer Proxys hingegen ist es lediglich nötig, eine Default-Route auf der Firewall, die eine Verbindung zum öffentlichen Bereich darstellt, zu definieren. Da der Client nie direkt eine öffentliche Adresse aus dem Internet anspricht, sondern seine Anfragen immer an den Proxy richtet, benötigt der Client hingegen ausschließlich eine Route zum Proxy. Dadurch, dass im internen Netz keine Default-Route definiert ist (zumindest beim Einsatz eines transparenten Proxys) und aus Sicherheitsgründen auch nicht definiert sein sollte, ist dieser dementsprechend auch gar nicht ohne Einsatz des Proxys in der Lage, öffentliche Adressen aus dem Internet zu erreichen. Der Internetzugriff kann beim Einsatz eines Application Layer Proxys also zentral über den Proxy gesteuert werden. Diese Eigenschaft ist sehr bedeutend und sollte nicht unterschätzt werden.

5.2.4 Bezug zu Session-Angriffen

Hinsichtlich der Betrachtung des Verkehrsflusses stellt sich die Frage, ob sich beim Einsatz eines Proxys als Session Terminator Vorteile bei Session-Angriffen wie Session-Fixation oder Session-Hijacking ergeben.

Session-Fixation ist ein Angriff auf den Sessionschlüssel, der zur Identifizierung bei der Webanwendung genutzt wird. In diesem Angriffsszenario versucht der Angreifer den Sessionschlüssel nicht zu erraten, sondern er versucht ihn vorzugeben. Benutzt ein Nutzer diesen gefälschten Sessionschlüssel, kann auch der Angreifer sich Zugang verschaffen (vgl. Kachel 2009).

Beim Session-Hijacking (aktiver Angriff) wird der Sitzungsschlüssel mit- bzw. ausgelesen. Auf diese Art kann der Angreifer die Identität eines Nutzers übernehmen. Mittels Mitlesen des Netzwerkverkehrs, durch Auslesen des Sitzungsschlüssels aus der Webseite und durch Auslesen des Sitzungsschlüssels aus der Sessionverwaltung kann der Sitzungsschlüssel ausgespäht werden (→ Sniffing, passiver Angriff) (vgl. Kachel 2009).

In dem Fall, dass es einem Angreifer gelingt, einen Proxy mittels eines Session-Angriffs zu kapern, so ist dies deutlich unkritischer, als wenn es dem Angreifer gelingen würde, einen Client zu kapern. Im Unterschied zum Client ist der Proxy in der DMZ (im teilöffentlichen Bereich) positioniert und der Angreifer müsste weitere Sicherheitsmaßnahmen überwinden, um sich Zugriff zum internen Netz zu verschaffen. Der Client jedoch steht im internen Netz und der Angreifer könnte so direkt weiteren Zugriff im internen Netz erlangen.
Darüber hinaus sind Proxys durch ihre Positionierung nahe des öffentlichen Bereichs darauf ausgelegt, generell Angriffe und auch Session-Angriffe aus dem öffentlichen Bereich zu

unterbinden und sollten durch Administratoren auch fortlaufend durch Einspielen von Patches und Nachjustieren der Konfiguration geschützt werden. Üblicherweise wird sich bei dieser Art von Angriffen zunächst Zugang zur Web-Benutzeroberfläche eines Proxys verschafft. Eine Separierung des Management-Zugangs ist eine Maßnahme, die man treffen sollte. Das Auslesen des Sitzungsschlüssels aus dem Netzwerkverkehr wird verhindert bzw. erschwert durch die Verwendung einer sicheren HTTP-Verbindung (HTTPS) bzw. einer sicheren SSH-Verbindung zwischen Administrator und Proxy. Zudem sollte es nicht möglich sein, eine Vertrauensstellung lediglich basierend auf einem gemeinsamen Geheimnis (Shared Secret) zu erlangen. Sicherer sind beispielsweise Challenge-Response-Authentifizierung oder Multifaktor-Authentifizierung.
Beim Client hingegen ist es wahrscheinlicher, dass einer der Clients nicht ausreichend stark gegen einen Session-Angriff geschützt ist, da es dort viele Angriffspunkte abzusichern gilt und diese bei jedem Client ohne Ausnahme umgesetzt werden müssen.

Generell sollten Sicherheitsmaßnahmen im Netz eingeführt werden, um Session-Angriffe zu vermeiden. Anomalien, die Hijacking-Techniken im Netzwerkverkehr erzeugen, sollten mittels IDS erkannt werden. IP-Spoofing wird beispielsweise auch als zentrales Element für Angriffe wie Session-Hijacking genutzt, weshalb Anti-Spoofing ebenfalls die Grundlage einer Session-Attacke einschränkt.

5.3 Herstellervergleich der Marktführer

In diesem Kapitel werden die momentanen Markführer von Application Layer Firewalls und Application Layer Proxys (Web-Proxy & SMTP-Proxy) genannt und in groben Ansätzen verglichen.

5.3.1 Übersicht Application Layer Firewalls

Gemäß des „Magic Quadrant for Enterprise Network Firewalls“ von Gartner (siehe folgende Abbildungen 22 und 23) gelten momentan Check Point Software Technologies, Palo Alto Networks und Fortinet als klare Marktführer. Cisco und Huawei zählen zu den Herausforderern. Fast ein Dutzend weiterer Hersteller werden als Nischenanbieter bzw. Visionäre betrachtet.

Abbildung 22: Magic Quadrant for Enterprise Network Firewalls (Mai 2016) (Quelle: [26])

Abbildung 23: Magic Quadrant for Enterprise Network Firewalls (Juli 2017) (Quelle: [27])

Je nach Hersteller werden unterschiedliche Funktionalitäten in variierender Intensität umgesetzt. Check Point als Hersteller kann die höchste IPS-Block-Rate aufweisen sowie die größte Applikationsdatenbank mit über 5.000 Applikationen. Palo Altos Aushängeschild ist die sehr gute User- und Applikations-Identifizierung. Laut Herstelleranagaben bietet das Produkt FortiGate von Fortinet eine fünfmal bessere Performance als andere, preislich vergleichbare Produkte. Die Cisco Produkte bieten mehr Firewall-Funktionen für Intrusion Detection und Protection Threat Services als andere Hersteller (vgl. Villegas 2016). Die Application Layer Firewall von Huawei findet hauptsächlich Anwendung in der Region Asien/Pazifik und EMEA.

5.3.2 Übersicht Application Layer Proxys

Web-Proxy

Gemäß des „Magic Quadrant for Secure Web Gateways“ von Gartner (siehe folgende Abbildungen 24 und 25) gelten momentan Symantec (ehemals Blue Coat) und Zscaler als führend, wobei Zscaler lediglich Cloud-Service Proxys und keine Hardware-Proxys vertreibt. Forcepoint, Cisco und McAfee gelten als Herausfoderer. Weitere sechs Hersteller werden als Nischenanbieter bzw. Visionäre eingestuft.

Abbildung 24: Magic Quadrant for Secure Web Gateways (Mai 2016) (Quelle: [28])

Abbildung 25: Magic Quadrant for Secure Web Gateways (Juni 2017) (Quelle: [29])

Email-Proxy

Zu den bedeutesten Herstellern und Produkten im Email-Sicherheitsmarkt zählen:

- Cisco Email Security Appliance
- Clearswift SECURE Email Gateway
- Fortinet FortiMail
- Proofpoint Email Protection
- Sophos Email Appliance
- Symantec Messaging Gateway

Die letzte Betrachtung „Magic Quadrant for Secure Email Gateways“ von Gartner (siehe folgende Abbildung 26) vom Juni 2015 stuft Proofpoint, Cisco und Microsoft als Markführer ein. Symantec wird als Herauforderer gekennzeichnet.

Abbildung 26: Magic Quadrant for Secure Email Gateways (Juni 2015) (Quelle: [30])

Alle aufgeführten Hersteller stellen die Basisfunktionen wie Anti-Virus, Anti-Malware, Anti-Phishing und Anti-Spam bereit. Unterschiede ergeben sich beispielsweise in der Bereitstellung von Sandboxing, um eine Datei in einer isolierten Umgebung zu testen. Diese Funktionalität ermöglichen Cisco Email Security Appliance, Fortinet FortiMail sowie Sophos Email Appliance. Darüber hinaus gibt es Abweichungen im Bereich von Threat Intelligence. Lediglich Clearswift SECURE Email Gateway wirbt nicht damit, Threat Intelligence anzubieten. Auch bei erweiterten Funktionen wie DLP (Data Loss/Leakage Prevention) und Email-Verschlüsselung sind Differenzen zu verzeichnen. Beides bietet Proofpoint Email Protection als einziges Produkt von den oben aufgeführten nicht.
Im Bereich von Spam ist 99 Prozent Spam-Erkennung ein zu erfüllendes Kriterium. Die Produkte Cisco Email Security Appliance, Proofpoint Email Protection und Symantec Messaging Gateway erfüllen diese Erkennungsrate. Clearswift SECURE Email Gateway bietet sogar 99,9 Prozent Spam Erkennung. Viren-Erkennung für bekannte Viren sollte beim ausgewählten Produkt 100 Prozent betragen.
Über False-Positive-Raten (erwünschte Mail als Spam aussortiert) können ebenfalls Abweichungen festgestellt werden. So kann das Produkt Clearswift SECURE Email Gateway eine False-Positive-Rate von einer Mail in 300.000 Mails vorweisen. Die Produkte Cisco Email Security Appliance und Symantec Messaging Gateway weisen sogar eine Rate von weniger als einer Mail in einer Million Mails vor (vgl. Scarfone 2017).

6 Fazit

Ob im eigenen Unternehmen der Einsatz einer Application Layer Firewall oder der Einsatz eines Application Layer Proxys sinnvoller ist, richtet sich danach, welche Funktionen in welcher Intensität/Qualität benötigt werden. Außerdem ist entscheidend, welcher Dienst oder welche Dienstgruppe abgedeckt werden soll.
Bevor man sich also für ein konkretes Produkt entscheidet, sollte zunächst eine Evaluation durchgeführt werden, welche Funktionalitäten bereits durch entsprechende Komponenten im Netz bereitgestellt werden, ob diese ergänzt oder durch die Inbetriebnahme eines neuen Devices abgelöst werden sollen. Nach der Entscheidung für eine der beiden Techniken sollte der passende Hersteller gefunden werden, um letztendlich ein Produkt mit der benötigten Dimension zu wählen.

6.1 Was wurde erarbeitet? / Wurde das Ziel erreicht?

Wie in der Einleitung beschrieben, konnten Unterscheidungsmerkmale und Funktionalitäten von Application Layer Firewall und Application Layer Proxy herausgearbeitet werden. Hinsichtlich der Funktionalitäten konnten Übereinstimmung sowie Unterschiede festgestellt werden. Dabei ergab sich, dass eine Application Layer Firewall zwar die Funktionalitäten eines Web-Proxys übernehmen kann und sogar mit weiteren ergänzt, jedoch nicht alle Funktionalitäten eines Email-Proxys abdeckt. Im Allgemeinen bedeutet das, dass es Funktionen gibt, die Application Layer Firewalls bereitstellen und Proxys nicht. Anders herum gibt es aber auch Funktionen, die Proxys bereitstellen und Application Layer Firewalls nicht.
Wenn es darum geht, ein Funktionsmodul in besonders starker Intensität/Qualität einzusetzen, sollte beachtet werden, dass die Intensität/Qualität in „All-In-One“-Devices generell häufig nicht der eines professionellen Gerätes entspricht, welches nur diese eine Funktion bereitstellt.
Darüber hinaus konnten Vor- und Nachteile beider Techniken festgestellt werden, bei denen jedes Unternehmen entscheiden sollte, welche Variante besser zum Unternehmen passt bzw. sich besser integrieren lässt. Außerdem konnten Unterschiede hinsichtlich der

Betrachtung des Verkehrsflusses festgestellt werden. Application Layer Proxys bieten durch ihre Positionierung in der DMZ und durch ihre Eigenschaft, Sessions aller Art stets zu terminieren, einen Sicherheitsvorteil gegenüber Application Layer Firewalls in Bezug auf Session-Angriffe.
Darüber hinaus wurde eine Kombination von Application Layer Firewall und Proxy nachgestellt. Diese Kombination ist prinzipiell möglich und bietet doppelten Schutz. Allerdings gilt hier zu beachten, dass eine erkannte Applikation auf einer Application Layer Firewall nicht mehr ohne Weiteres (wie Tags oder User-Authentication) dem Client zugeordnet werden kann, welcher diese aufgerufen hat, wenn zusätzlich ein Proxy eingesetzt wird. Diese fehlende Zuordnung schränkt das Monitoring und somit auch das Troubleshooting ein, weshalb im Fall einer Kombination beider Techniken Tags oder User-Authentication eingeführt werden sollten, um die Transparenz weiterhin aufrechtzuerhalten. Alles in allem konnten die in der Einleitung genannten Ziele demnach erreicht werden.

6.2 Ausblick

Da die Anzahl von ortsunabhängigen Services (Cloud Services) steigt und auch in absehbarer Zeit zu steigen scheint, verringert sich die Bedeutung der Filtermöglichkeiten für Source und Destination IPs, wohingegen sich die Bedeutung von Filtermöglichkeiten hinsichtlich der Applikation vergrößert. Daraus ergeben sich die Berechtigung von Application Layer Firewall und Application Layer Proxy.
Der Trend zeigt, dass der Dienst Mail auch bei großen Unternehmen immer mehr und mehr in die Cloud ausgelagert wird. Bei vollständiger Auslagerung verliert der Email-Proxy im Unternehmen selber seine Daseinsberechtigung.
Es ist erkennbar, dass immer mehr Unternehmen ihre herkömmlichen Stateful Inspection Firewall insbesondere im Internet-Zugang durch Application Layer Firewalls austauschen. Bei der Aktivierung aller Funktionsmodule sollte jedoch Vorsicht geboten sein. Eine Aktivierung aller Module kann zu Folge haben, dass die Performance der Firewall nicht mehr ausreicht. Außerdem sollte beispielsweise der Einsatz von SSL-Inspection gut vorbereitet sein, da eine Umsetzung nicht trivial ist (→ Zertifikatsmanagement).
Um auch in der Zukunft effizient Schwachstellen zu kompensieren und Angriffe zu verhindern, sollte die Qualität der einzelnen Module von Application Layer Firewalls weiter gestärkt werden. Auch die Funktionalitäten von Application Layer Proxys sollten mit der Zeit ausgebaut werden. Es gilt vor allem die Intensität/Qualität von Applikationsidentifizierung und –filter zu intensivieren, um dem Wandel der Zeit gerecht zu werden und eine Filterung für ortsunabhängige Services bereitzustellen.
Proxys werden häufig von Anwendungsspezialisten mit entsprechender Fachkenntnis zu unterschiedlichen Anwendungen betreut. Firewalls wurden bisher von Netzwerk-Administratoren administriert. Da bei der Betreuung von Application Layer Firewalls auch anwendungsspezifisches Wissen nötig ist, gilt es abzuwarten, inwieweit sich die Rollenverteilung verändert und ob Application Layer Firewalls künftig in den Zuständigkeitsbereich von Anwendungsspezialisten fallen.

Abbildungsverzeichnis

Tabellenverzeichnis

Listings

Literaturverzeichnis

[1] B. Casey, „Vergleich: Unified Threat Management (UTM) vs. Next-Generation Firewalls (NGFW),“ TechTarget, April 2014. [Online]. Available: http://www.searchnetworking.de/antwort/Vergleich-Unified-Threat-Management-UTM-vs-Next-Generation-Firewalls-NGFW. [Zugriff am 10 März 2018].

[2] K. Washburn und J. Evans, TCP/IP Aufbau und Betrieb eines TCP/IP Netzes 2. Auflage, Addison Wesley Longman Verlag GmbH, 1997.

[3] IKT-Consulting LG GmbH, „Was ist eigentlich eine Firewall?,“ 9 Januar 2018. [Online]. Available: http://www.netzwerker.news/content/Was-ist-eigentlich-eine-Firewall.html. [Zugriff am 10 März 2018].

[4] Wikipedia, „Firewall,“ 21 Februar 2018. [Online]. Available: https://de.wikipedia.org/wiki/Firewall. [Zugriff am 10 März 2018].

[5] B. Blobel und D. Koeppe, Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen, DATAKONTEXT GmbH, 2016.

[6] ITWissen.info, „SPI (stateful packet inspection),“ DATACOM Buchverlag GmbH, 16 Mai 2016. [Online]. Available: https://www.itwissen.info/SPI-stateful-packet-inspection.html. [Zugriff am 10 März 2018].

[7] I. Dubrawsky, „Firewall Evolution - Deep Packet Inspection,“ Symantec Corporation, 28 Juli 2003. [Online]. Available: https://www.symantec.com/connect/articles/firewall-evolution-deep-packet-inspection. [Zugriff am 10 März 2018].

[8] tutanch, „Was ist NAT (Network Address Translation)?,“ Vogel Business Media, 1 August 2017. [Online]. Available: https://www.ip-insider.de/was-ist-nat-network-address-translation-a-663954/. [Zugriff am 10 März 2018].

[9] „Network Address Translation (NAT/ PAT/ IP Masquerading),“ 6 April 2009. [Online]. Available: http://www.tcp-ip-info.de/tcp_ip_und_internet/ip_masquerading.htm. [Zugriff am 10 März 2018].

[10] M. Rouse, „What is antispoofing?," TechTarget, Juli 2014. [Online]. Available: http://searchsecurity.techtarget.com/definition/antispoofing. [Zugriff am 10 März 2018].

[11] P. Schmitz, „Data Loss Prevention - Maßnahmen gegen Datendiebstahl," Vogel Business Media, 12 August 2009. [Online]. Available: https://www.security-insider.de/data-loss-prevention-massnahmen-gegen-datendiebstahl-a-224846/. [Zugriff am 10 März 2018].

[12] M. Rouse, „Was ist Web Application Firewall (WAF)?," TechTarget, Juni 2015. [Online]. Available: http://www.searchsecurity.de/definition/Web-Application-Firewall-WAF. [Zugriff am 10 März 2018].

[13] „Proxy Server – Arten, Einsatz und Nutzungsempfehlung," 2 März 2016. [Online]. Available: http://office-server-vergleich.de/proxy-server/. [Zugriff am 10 März 2018].

[14] N. Hosking, „Transparent vs Explicit proxy - which method should I use?," Loadbalancer.org, 14 Juni 2017. [Online]. Available: http://www.loadbalancer.org/blog/transparent-vs-explicit-proxy-which-method-should-i-use/. [Zugriff am 10 März 2018].

[15] Cisco, „Cisco Email Security Data Sheet," 2017. [Online]. [Zugriff am 10 März 2018].

[16] Cisco, „Cisco Web Security Aplliance Data Sheet," 2013. [Online]. [Zugriff am 10 März 2018].

[17] E. Kachel, „Session-Angriffe – eine Analyse an PHP," 10 August 2009. [Online]. Available: https://www.erich-kachel.de/session-angriffe-eine-analyse-an-php/. [Zugriff am 10 März 2018].

[18] B. Blevins, „Next-Generation Firewall (NGFW) im Vergleich: Kein Produkt ist perfekt," TechTarget, Juni 2014. [Online]. Available: http://www.searchnetworking.de/tipp/Next-Generation-Firewall-NGFW-im-Vergleich-Kein-Produkt-ist-perfekt. [Zugriff am 10 März 2018].

[19] H. Scherff, „NGFW: Das Schweizer Taschenmesser für die IT-Sicherheit," TechTarget, November 2017. [Online]. Available: http://www.searchnetworking.de/meinung/NGFW-Das-Schweizer-Taschenmesser-fuer-die-IT-Sicherheit. [Zugriff am 10 März 2018].

[20] M. O. Villegas, „Im Vergleich: Die besten verfügbaren Next-Generation Firewalls," TechTarget, Januar 2016. [Online]. Available: http://www.searchnetworking.de/lernprogramm/Im-Vergleich-Die-besten-verfuegbaren-Next-Generation-Firewalls. [Zugriff am 10 März 2018].

[21] M. O. Villegas, „Check Point Next Generation Firewall: Product overview," TechTarget, Juli 2016. [Online]. Available: http://searchsecurity.techtarget.com/feature/Check-Point-Next-Generation-Firewall-Product-overview. [Zugriff am 10 März 2018].

[22] D. Shackleford, „NGFW PA-5060: Rezension zur Next-Generation Firewall von Palo Alto Networks," TechTarget, Juli 2014. [Online]. Available:

http://www.searchnetworking.de/tipp/NGFW-PA-5060-Rezension-zur-Next-Generation-Firewall-von-Palo-Alto-Networks. [Zugriff am 10 März 2018].

[23] M. O. Villegas, „Cisco ASA with FirePOWER: NGFW product overview," TechTarget, Juli 2016. [Online]. Available: http://searchsecurity.techtarget.com/feature/Cisco-ASA-with-FirePOWER-NGFW-product-overview. [Zugriff am 10 März 2018].

[24] K. Scarfone, „Comparing the best email security gateways," TechTarget, Juni 2017. [Online]. Available: http://searchsecurity.techtarget.com/feature/Comparing-the-best-email-security-gateways. [Zugriff am 10 März 2018].

[25] MUK, „Check Point NGFW," 4 Dezember 2013. [Online]. Available: https://www.slideshare.net/CheckPoint_MUK/check-point-next-generation-firewall. [Zugriff am 10 März 2018].

[26] Blue Apache, „Palo Alto Networks named a Magic Quadrant Leader," 7 Juni 2016. [Online]. Available: https://www.blueapache.com/palo-alto-networks-named-gartner-magic-quadrant-leader-enterprise-network-firewalls/. [Zugriff am 10 März 2018].

[27] „Magic Quadrant for Enterprise Network Firewalls 2017," 12 Juli 2017. [Online]. Available: https://www.cocheno.com/2017/07/magic-quadrant-for-enterprise-network-firewalls-2017/. [Zugriff am 10 März 2018].

[28] Y. Irfan, „Network technologies and trends," TechTarget, 7 Oktober 2016. [Online]. Available: http://itknowledgeexchange.techtarget.com/network-technologies/blue-coat-proxy-sg-leader-secure-web-gateways/. [Zugriff am 10 März 2018].

[29] iboss, „Gartner Magic Quadrant - Secure Web Gateways | iboss," [Online]. Available: https://www.iboss.com/gartner-2017-magic-quadrant. [Zugriff am 10 März 2018].

[30] proofpoint, „Thank You (Gartner Magic Quadrant for Secure Email Gateways)," [Online]. Available: https://www.proofpoint.com/de/thank-you-gartner-magic-quadrant-secure-email-gateways. [Zugriff am 10 März 2018].

Versicherung über Selbstständigkeit

Hiermit versichere ich, dass ich die vorliegende Arbeit ohne fremde Hilfe selbstständig verfasst und nur die angegebenen Hilfsmittel benutzt habe.

Hamburg, den _____ _____

Mona Lüdemann