

# QTRUST SERVER

## Multilevel Security-Appliance

„Sicherheit ist kein kaufbares Feature sondern eine Reihe von aufeinander abgestimmten Prozessen und Lösungen“

„Sicherheit versus Funktion – Ein Balance-Akt“

„Reduzierung von Komplexität erhöht die Sicherheit“

### WEB-APPLIKATIONSSICHERHEIT

In der Welt heterogener Betriebssysteme gewinnen Web Applikationen, die über eine statische Repräsentation von Unternehmen hinausgehen, eine immer größere Bedeutung. Sie sind unabhängig von lokalen Systemen und können auf nahezu beliebigen Plattformen ausgeführt werden. Oft werden sie vorschnell und unüberlegt für die ganze Welt geöffnet, damit die Mitarbeiter und Partner unabhängig von deren Aufenthaltsort auf die Plattformen zugreifen können.

In diesem Dokument soll gezeigt werden, wie durch den QTrust Server die von offenen Web Applikationen ausgehenden Gefahren auf ein Minimum reduziert werden können.

# INHALTSVERZEICHNIS

**EINLEITUNG** ..... 1

**QTRUST REVERSE PROXY SERVER MODUL**..... 2

Technische Grundlagen..... 2

Arbeitsweise und Funktionen ..... 2

    Kommunikation..... 2

    Trusted Operating System und Security Domains ..... 2

    Intrusion Prevention System..... 2

    Skalierbarkeit..... 2

    Verschleierung ..... 2

    Unternehmenswachstum und Denial of Service..... 3

    Ausfälle und Wartungsarbeiten ..... 3

    SSL und TLS..... 3

    Mobile Dienste ..... 3

    Logdateien und Auswertung..... 3

    DNS Poisoning und Virtual Primary DNS ..... 4

Beispielszenarien..... 4

A. Microsoft Outlook Web Access ..... 4

B. Absicherung eines Kreditkartendienstleisters ..... 5

C. MS Direct Push / Blackberry Enterprise Server ..... 6

## ABBILDUNGSVERZEICHNIS

Abbildung 1: Beispiel einer einfachen Absicherung..... 5

Abbildung 2: Beispiel eines Redundanz Konzepts ..... 6

Abbildung 3: Beispiel Microsoft OMA..... 7

## EINLEITUNG

Die Ubiquität der Computer nimmt immer weiter zu und damit verbunden wächst ständig die Bedeutung der standortunabhängig nutzbaren Web Applikationen und Portale.

Aus Bewusstheits-, Zeit- und Ressourcenmangel werden Web Server oft vorschnell und unüberlegt für die ganze Welt geöffnet und sind somit direkt angreifbar.

Nicht selten erlauben auch die auf Flexibilität getrimmten Geschäftsmodelle keine ausreichenden Investitionen in Sicherheits- und Qualitätsmanagement der genannten Applikationen – alles muss sofort, flexibel und zeitnah zur Verfügung stehen.

Diese Mängel können mithilfe des QTrust Servers minimiert und teilweise sogar beseitigt werden, so dass ein optimaler Kompromiss zwischen Funktionalität, Konfigurierbarkeit und Sicherheit erreicht wird.

Der QTrust Server, die Schaltstelle zwischen den externen und internen Netzen, verhindert den direkten Datenaustausch zwischen den angeschlossenen Netzwerken und prüft den Datenverkehr auf IP- und Applikationsebene.

Das Reverse Proxy Modul des QTrust Servers arbeitet nicht nur als einfacher Spiegel für die dahinterliegenden Web Applikationen, sondern bietet darüber hinaus noch eine ganze Reihe Zusatzfunktionen, mit denen die Sicherheit der Web Applikationen weiter gesteigert werden.

Dieses Dokument soll die verschiedenen Funktionen aufzählen und anhand praktischer Anwendungsfälle aufzeigen, welche Vorteile durch den QTrust Server geboten werden.

# QTRUST REVERSE PROXY SERVER MODUL

## • TECHNISCHE GRUNDLAGEN

Das QTrust Webprotector Modul basiert auf einem modifizierten Apachen 2 Kern, der durch eigene Module ergänzt und abgerundet wird. So bietet er zusätzliche Sicherheits-, Verschleierungs- wie auch Filterfunktionen und arbeitet nahtlos mit dem QTrust IPS System zusammen.

## • ARBEITSWEISE UND FUNKTIONEN

### **Kommunikation**

Der QTrust Server, die Schaltstelle zwischen den externen und internen Netzen, verhindert den direkten Datenaustausch zwischen den angeschlossenen Netzwerken. Das bedeutet, die Firewall erlaubt keinen Datenaustausch mit dem eigentlichen Applikations Server und verschleiert die Existenz desselbigen.

### **Trusted Operating System und Security Domains**

Für einen Angreifer ist der QTrust Server der vermeintliche Webserver und einzig erreichbares System. Doch selbst bei einer erfolgreichen Übernahme des Prozesses bleiben alle anderen Systeme des QTrust Servers sowie auch der eigentliche Webserver funktionsfähig. Dies wird durch das Trusted Operating System „PitBull LX“ der Argus Systems Group gewährleistet. Dieses schließt jeden Prozess in einer eigenen Security Domain ein, die nur minimal für den Betrieb notwendige Zugriffsrechte auf System- und Netzwerkressourcen gewährt.

### **Intrusion Prevention System**

Des Weiteren verhindert das integrierte Intrusion Prevention System, dass durch einen erfolgreichen Angriff weiterer Schaden entsteht; der Netzwerkverkehr zu und von dem korrumpierten Dienst wird unterbunden bis der Administrator die notwendigen Schritte des Ausnahmeprozesses durchführt.

### **Skalierbarkeit**

Der Anzahl der durch den QTrust Server abgesicherten Web Applikationen sind nur physikalische Grenzen gesetzt. Für jeden Webserver kann eine eigene Instanz in einer eigenen Security Domain gestartet oder es können mehrere Server in einem Prozess virtualisiert werden. Auch die zugrundeliegende Hardware kann entsprechend den individuellen Anforderungen ausgewählt werden.

### **Verschleierung**

Der QTrust Server bietet die Möglichkeit, HTTP Anfragen auf unerwünschte Ketten zu untersuchen. Dadurch können sowohl kritische Verzeichnisse versteckt als auch SQL Injections unterbunden werden. Hierzu gibt es für Standard Cases bereits eine vordefinierte Auswahl an Filterregeln.

Darüberhinaus bietet der QTrust Server die Möglichkeit, Informationen über den eigentlichen Web Server zu verstecken, um dem Angreifer auf eine falsche Fährte zu locken (Honeypot).

### **Unternehmenswachstum und Denial of Service**

Mit einem wachsenden Unternehmen sind mittlerweile wachsende Zugriffszahlen der Internetportale unmittelbar verbunden. Nicht selten müssen leistungsstärkere Server angeschafft oder gar die Plattform grundlegend gewechselt werden, um der Überlast Herr zu werden.

Durch das integrierte Loadbalancing Modul ist es möglich, die Last auf mehrere Web Server zu verteilen, ohne dass komplizierte Clustering Mechanismen notwendig werden.

### **Ausfälle und Wartungsarbeiten**

Auch ermöglicht der QTrust Server das Anzeigen einer aussagekräftigen Fehlermeldung für den Endanwender, wenn aufgrund eines Ausfalls oder auch regulärer Wartungsarbeiten das Endsystem nicht erreichbar ist.

Dies erspart nicht nur ständige Anrufe beim Systemadministrator, sondern verhindert auch, dass der Endanwender im Glauben, der Fehler liege an seiner Verbindung, unnötige Zeit in Analysen verliert.

### SSL und TLS

Der QTrust Server kann selbstverständlich auch die Kommunikation mit dem Endsystem via HTTPs absichern. Darüberhinaus bietet er die Möglichkeit, durch Senden entsprechender Befehle an das Backend System die intern ungesicherte Kommunikation nach außen über HTTPs darzustellen. Dies führt zu einem Performancegewinn am Backend System, da die CPU-intensive Verschlüsselung an dieser Stelle entfällt.

### Mobile Dienste

Es werden sowohl W3C-Standard konforme Formate als auch die insbesondere von Microsoft abgewandelten Protokolle unterstützt. Somit zählen das Absichern von Standardapplikationen wie Outlook Web Access, Outlook Mobile Access und auch das seit Windows Mobile 5 sich immer größerer Beliebtheit erfreuende Direct Push zur Selbstverständlichkeit.

### Logdateien und Auswertung

Der QTrust Server bietet bereits eine integrierte Auswertung der Logdateien, die für die meisten Fälle ausreichend ist. Selbstverständlich können auch alle Dateien heruntergeladen werden, um archiviert oder in einem externen Auswertungsprogramm analysiert zu werden.

Darüberhinaus ermöglicht der QTrust Server das periodische Kopieren der Logdatei des letzten Tages auf ein Netzlaufwerk, so dass es dort automatisiert in einem externen Auswertungsprogramm analysiert werden kann. Somit stehen jeden Morgen die aktuellen Berichte zur Verfügung.

### DNS Poisoning und Virtual Primary DNS

Ein häufiges Problem mit der Verfügbarkeit von Web Applikationen waren neben der Sicherheit derselbigen allein auch die Sicherheit der dafür verantwortlichen DNS Server. Weil kaum ein Endanwender über die IP Adressen auf die Portale eines Unternehmens zugreift, führen diese Angriffe zu einem sogar schlimmeren Ergebnis. Es wird nicht nur der Zugriff auf die Web Applikation unterbunden, sondern darüber hinaus das Portal mit anderen Inhalten gefüllt. Dies kann zum Ausspähen unternehmenskritischer Daten oder gar Börsencrashes führen.

Der QTrust Server, der über die reine Absicherung von Web Applikationen hinausgeht, verfügt über ein Virtual Primary DNS Modul. Dieses ermöglicht es, den internen DNS Server in der gleichen Art und Weise abzusichern wie die Web Applikation selbst. In einer eigenen Security Domain ausgeführt, werden die Anfragen nach außen so beantwortet, als wäre der QTrust Server der primäre DNS Server. Es findet keine direkte Kommunikation zwischen dem Internet und dem internen DNS Server mehr statt.

## • BEISPIELSZENARIEN

### A. Microsoft Outlook Web Access

Dieses Beispiel stellt den wohl häufigsten Fall einer Absicherung dar. Eine einfache Webapplikation wird durch einen internen Server bereitgestellt und soll nach außen freigeschaltet werden.

Der QTrust Server arbeitet im Unternehmen sowohl als Firewall für drei Netze, das Internet, die DMZ und die Clients. Darüber hinaus ist das Reverse Proxy Modul für den Microsoft Exchange Server konfiguriert und sichert den Dienst mit den bereits beschriebenen Sicherheitsmechanismen ab.

Durch die Erweiterung der Konfiguration des QTrust Servers mit dem Virtual Primary DNS und dem Mail Relay Modul wird das System abgerundet, so dass alle Kommunikation von außen am QTrust Server terminiert und die Existenz des Exchange Servers verschleiert wird. Hierbei greifen auch noch Viren und SPAM Filtermechanismen. Optional können auch die Clients durch das transparente Proxy Modul abgesichert werden, indem deren Existenz verschleiert, Zugriffe protokolliert und Daten nach Viren untersucht werden.

\* Beispiel für die Folgen einer falschen Information: <http://times.hankooki.com/lpage/200304/kt2003040418034312070.htm>

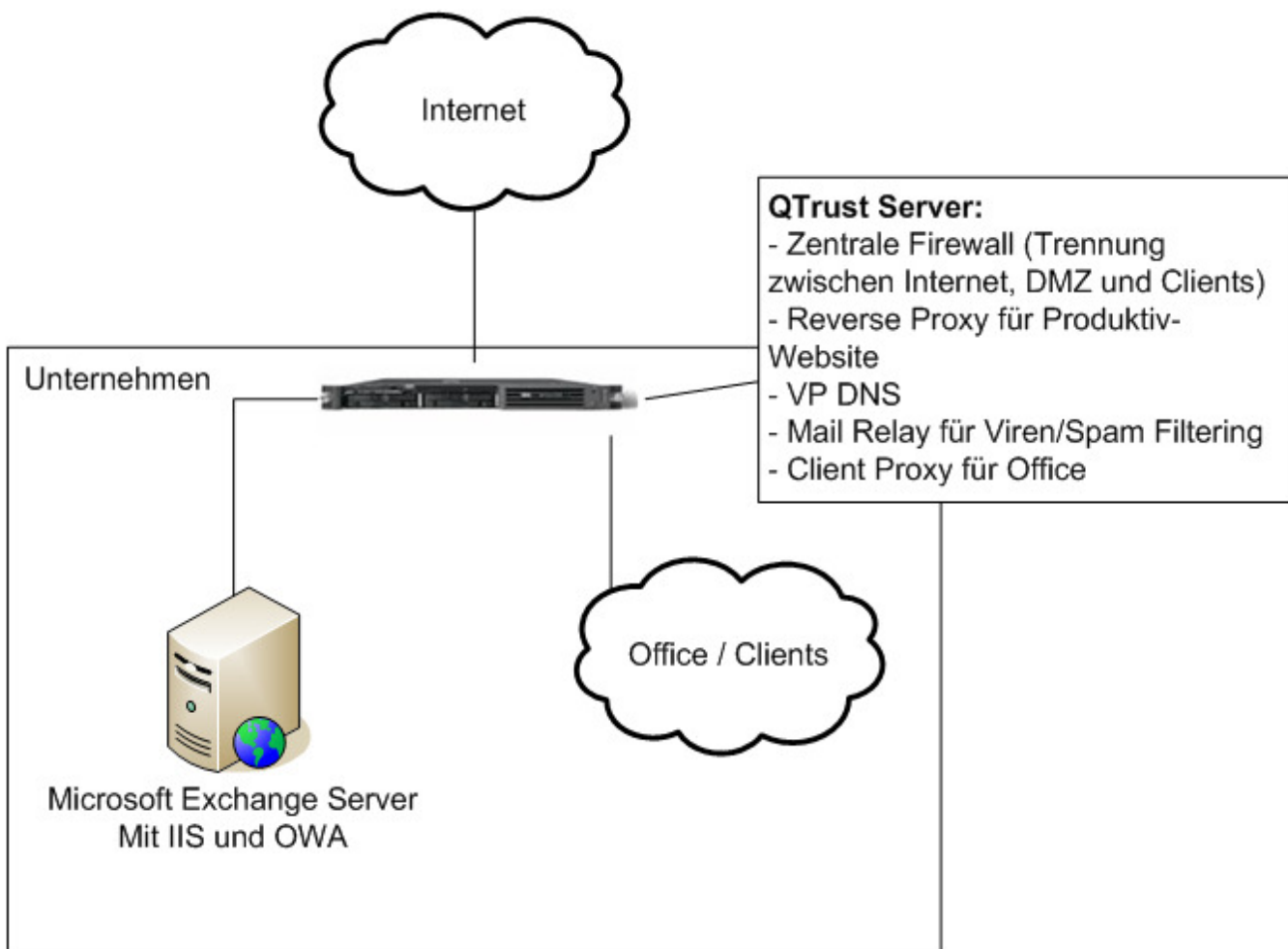


Abbildung 1: Beispiel einer einfachen Absicherung

**B. Absicherung eines Kreditkartendienstleisters**

In diesem Business Case geht es um einen Web Auftritt, in dem alle in der Brieftasche enthaltenen Karten verwaltet und im Verlustfall über eine einzige Meldung an den Dienstleister von diesem gesperrt werden können. Es handelt sich hierbei um eine hochverfügbare Applikation, da Verlustmeldungen der Kunden in jedem Fall zeitnah eingehen müssen. Verspätete Kartensperrungen bedeuten kritische Folgen für den Kunden und das Unternehmen selbst.

Aus diesem Grund wird ein Konzept mit zwei synchronisierten Standorten gewählt. Jeder dieser Standorte ist mit einem QTrust Server abgesichert. Das Büro des Unternehmens befindet sich an Standort 1 während Standort 2 lediglich ein synchronisiertes Abbild erhält.

In einem zentralen, redundant angebotenen Rechenzentrum wird ein QTrust Server als Load Balancer zwischen beiden Standorten konfiguriert. Dieser verteilt zum einen die Last zwischen beiden Standorten und zeigt darüber hinaus eine Wartungswebsite an, wenn keiner der beiden Abbilder mehr erreichbar ist. Diese enthält u.a. eine Telefonnummer, über die im Verlustfall die Meldungen abgegeben werden können.

Alle Standorte verfügen durch den QTrust Server über eine Firewall und sind durch einen verschlüsselten VPN Tunnel miteinander verbunden, so dass die datenschutzrechtlich kritischen Kreditkartendaten mit der entsprechenden Sicherheit synchronisiert werden können.

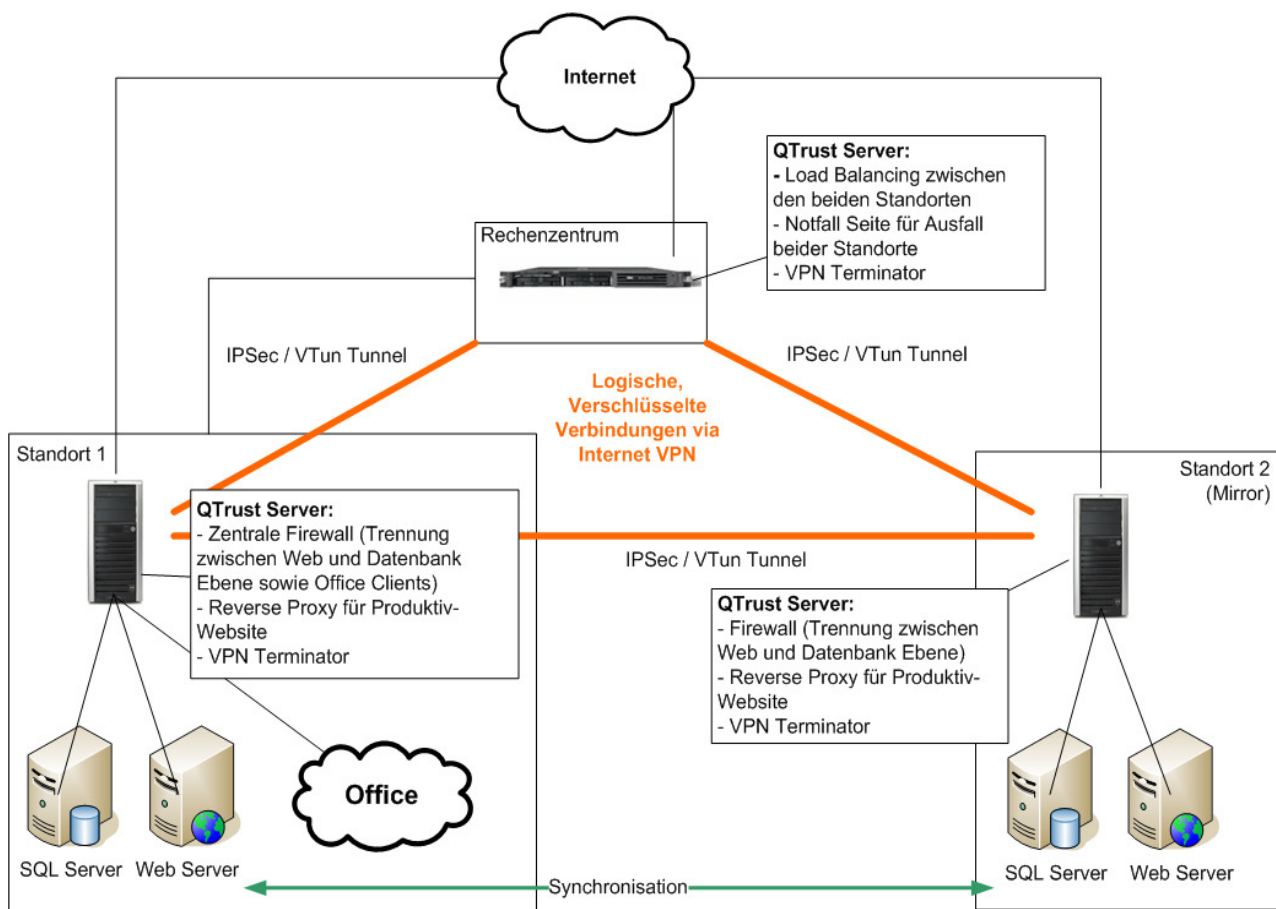


Abbildung 2: Beispiel eines Redundanz Konzepts

### C. MS Direct Push / Blackberry Enterprise Server

PDA's in den verschiedensten Formen erfreuen sich immer größerer Beliebtheit. Doch die Möglichkeiten werden oftmals nur in beschränktem Umfang ausgeschöpft; sei es aufgrund fehlender Kenntnis derselbigen, begrenzten Ressourcen oder der Angst, neue Schwachstellen zu offenbaren.

Im folgenden Beispiel arbeitet der QTrust Server als HTTP's Terminator für Outlook Mobile Sync, stellt das Zertifikat für die Verschlüsselung bereit und ist alleiniger von außen erreichbarer Server.

Im Falle eines Smartphones mit Windows Mobile 5 sendet der Exchange Server bei einem erfolgten Dateneingang ein Signal an das Gerät. Dieses verbindet sich daraufhin mit dem QTrust Server, um die Synchronisation durchzuführen. Auch hier bleibt der QTrust Server alleiniger von außen erreichbarer Server.

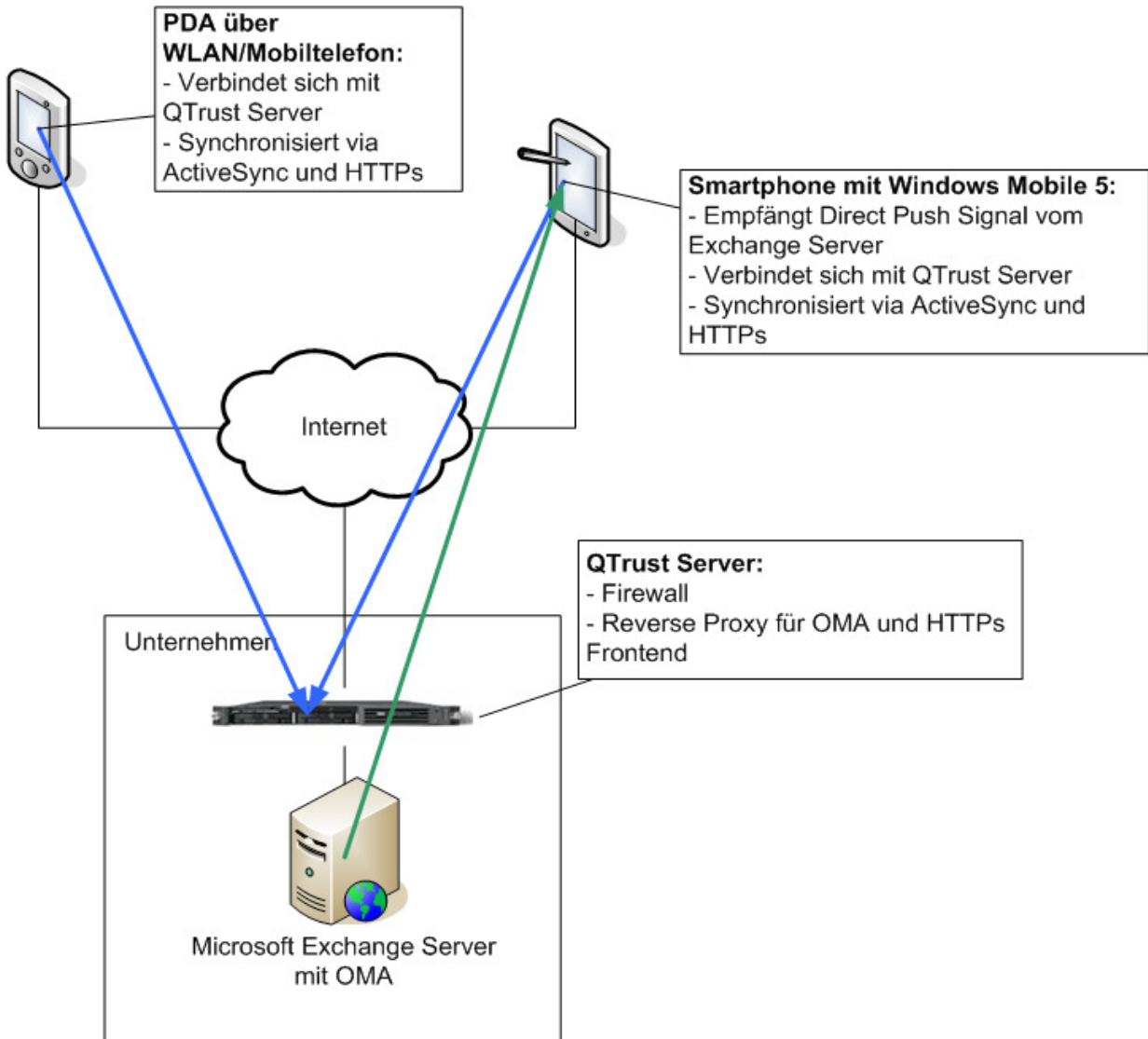


Abbildung 3: Beispiel Microsoft OMA