



QTRUST SERVER

Multilevel Security-Appliance

“Security is not a feature you can buy,
but a multiplicity of fine tuned processes and solutions”

“Security versus function – a balance act”

“Reducing complexity allows for more security”

STRATEGY

In a comprehensive security strategy security appliances play a central role as they protect company networks against attacks from the Internet. In the following document we are going to give you a short introduction of the QTrust Server since it offers you the perfect base for network security in your company.

The QTrust Server is aiming at a simple security strategy:

REDUCING AND PREVENTING POSSIBLE ATTACKS AND MINIMIZING THE NEGATIVE EFFECTS IN CASE OF SUCCESSFUL ATTACKS

Modern applications are complex and this complexity may imply vulnerabilities or even compromised systems. Useful communication may also lead to misuse and therefore to successful attacks.

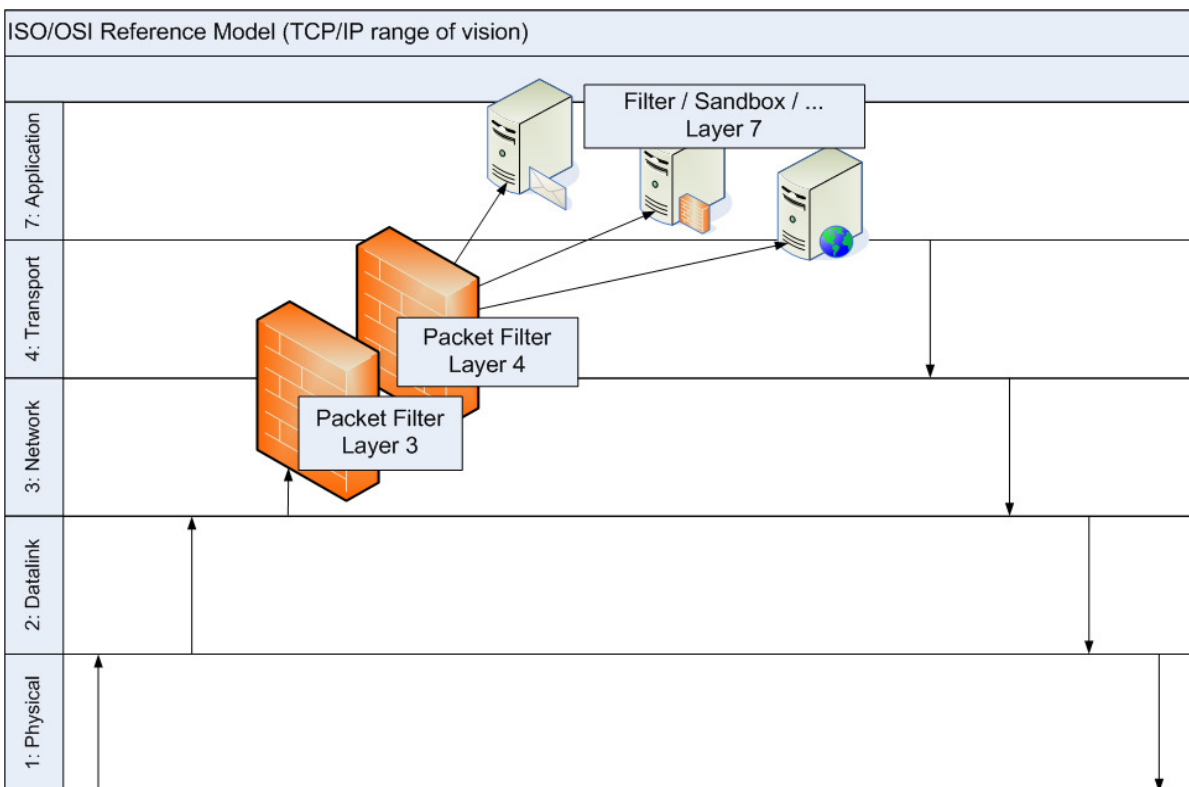
We should not forget one of the principles of security:

MORE IT IS EASY, MORE IT IS SECURE.

We have been aiming at creating a product which responds to highest security demands being at the same time easy to use and to maintain.

THE QTRUST SERVER

This completely integrated solution in form of a Multilevel Security Appliance consolidates the most important network security functions in one easy to maintain and high secure system. It consists of several layers of the ISO/OSI model, further security functions being added on each layer.



The QTrust Server acts as a proxy of the final application where it takes over communication and protects the systems lying behind according to the sandbox principle. The sandbox principle can be compared to a sandbag, which stops a bullet. The attack is neutralized via absorption. This means that a hacker who has succeeded in gaining access to one application on the QTrust Server, will have no direct access to the real servers and the data saved there. The QTrust Server therefore performs the task of a complete DMZ (Demilitarized Zone) compressed in one single system offering the same or even higher security standard by using a technology which separates a physical system in several application unities.

Example e-mail:

An integrated filter recognizes SPAM long before the undesired e-mail reaches the real mail server offloading hence security tasks from the mail server and user. A virus scan detects virus already at the Internet interface before they reach the internal network. Thus the whole network and not only individual machines are protected.

Contrary to the average firewall systems the QTrust Server avoids any data exchange between the outside and inside networks – for almost all configurations without exception. Every internal data service, that has to communicate with the outside world, is audited and decoupled via the QTrust Server. Communication is only possible between the QTrust Server and the external world. All actual data services and sources as for instance the mail server are safely hidden behind the Qtrust Server.

WHAT EXACTLY IS THE QTRUST SERVER?

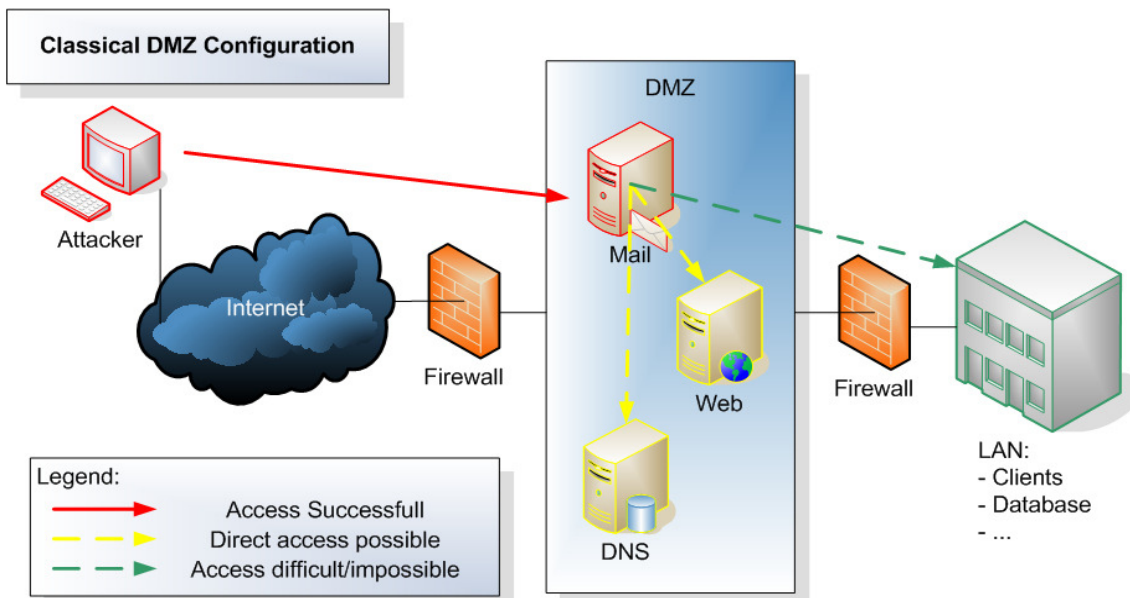
The QTrust Server integrates a variety of security mechanisms in one single system offering at the same time several mechanisms for mobile or location-spread connections.

In addition to classical firewall functionality (IP-Filter, VPN-Gateway) data is also controlled on the application level.

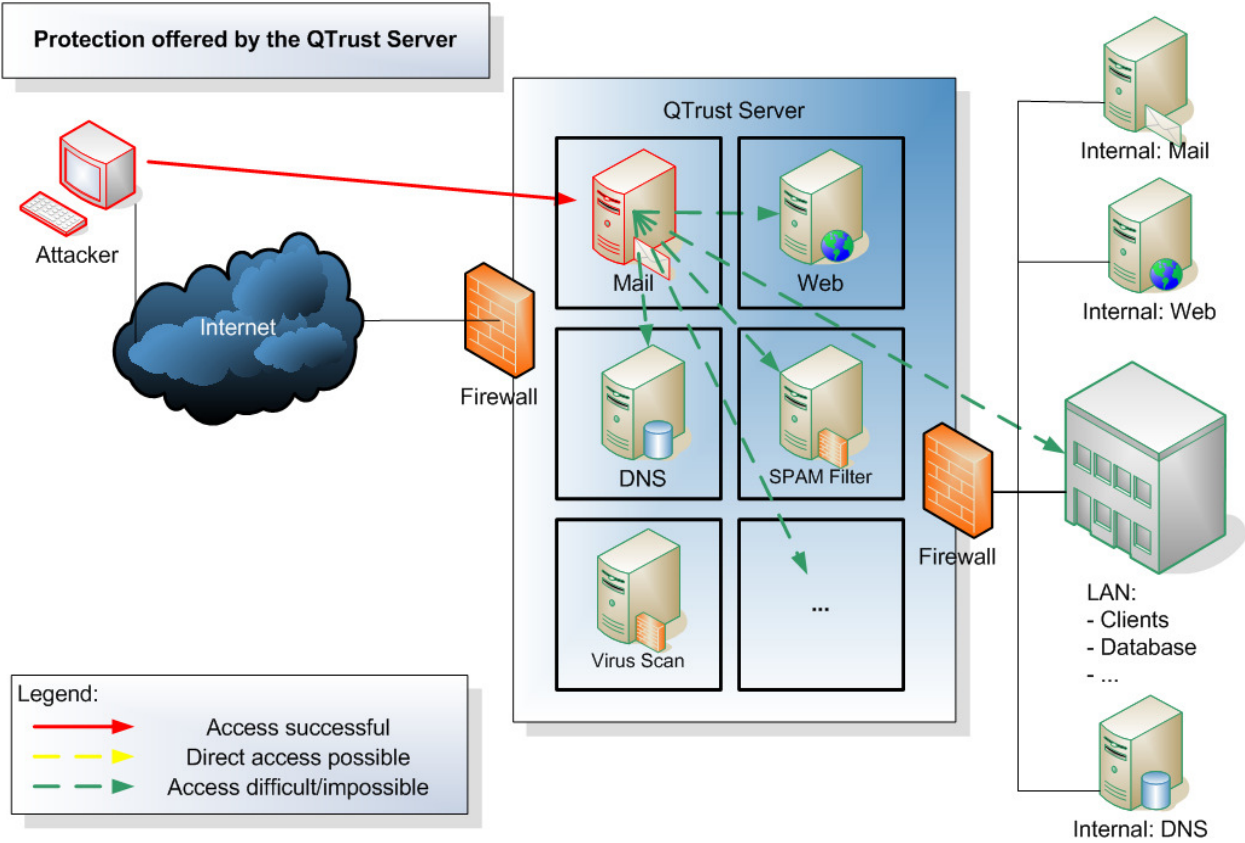
Dataflow between all internal and external networks is interrupted, audited, buffered and virus scanned. An application filter audits incoming and outgoing data packets. Attacks are recognized, logged and reported.

The QTrust Server is internally secured by the secure application environment ‚PitBull‘ of Argus Systems Group. Based on the Trusted Operating System (TOS) technology PitBull deploys firewall and gateway applications in separated compartments which can only communicate in a limited way. Within the departments access is only possible to pre-defined resources. Thus attacks against the QTrust Server and the running services can be prevented and controlled. Therefore, a hacker who manages to obtain access to the system through one specific service will find he has no influence on the other services running on the system or on the connected networks.

Up to now a comparable high-secure configuration has only been possible by distributing the services among individual independent servers. As these solutions are expensive, complex and time-consuming, they are only used by most serious security practitioners e.g. banks and insurances. (including online-banking).



The QTrust Server consolidates these individual servers on one integrated system. The Linux Distribution ,QLinx' is founded on the PitBull technology. QLinx as well as all security services can easily be maintained via a web console and without Linux knowledge. QLinx with its packet administration allows for an easy, automatic and secure administration and installation of system and security updates.



Systems of Hewlett Packard are used as hardware platform for the entire QTrust product family ensuring a high standard of availability, support and service.

In order to provide high available systems in critical environments QTrust Servers are also available on the platform of the Stratus FT Server.

The QTrust Server is an easy-to-use and scalable appliance at a reasonable price offering a high degree of security for companies of all sizes.

QTRUST SERVER FUNCTIONALITY?

The QTrust Server prevents any direct communication between external and internal networks. In case of authorized connection data packets on the QTrust Server are identified, logged, audited and transferred by proxy services. Services in internal networks or in DMZs (Demilitarised Zones) are so mirrored and portrayed via the QTrust Server to the external world.

- **DNS:**

Internal primary DNS Servers are mirrored on the QTrust Server and published to the external world. For the Internet the QTrust Server acts as Primary DNS Server (VPDNS).

- **SMTP (with SPAM filter and virus scanner):**

MX-entries for domains, at which e-mails arrive point to the QTrust Server, which verifies and audits incoming e-mails against SPAM and virus transferring them then to internal mail servers. Outgoing e-mails are treated in the same way.

- **HTTP/HTTPS:**

The QTrust Server acts as a virtual HTTP/HTTPS Server (Proxy), which transfers the data of the internal web servers to the external.

- **HTTP - HTTPS conversion:**

An internal HTTP Server can be mirrored to the outside as HTTPS Server and therefore make possible a secure connection without the internal server having to be able to know HTTPS .

- **FTP:**

The QTrust Server also acts as transparent proxy for FTP Servers searching for virus in data contents and filtering these.

The following protocols are supported in a transparent way, that-is-to-say without changes at the internal clients for communication from the internal networks to the outside. The QTrust Server accepts authorized data connections, tests data for virus and transfers them afterwards.

- **HTTP**

Surfing in the Internet contains a lot of perpetually changing dangers: Logging of IP addresses, Port-Scans of clients for DOS attacks, downloads of files infected by virus, spy ware or diallers. The QTrust Server being a transparent Proxy with integrated virus scan prevents these attacks without any changes at the clients' workstation being necessary. Therefore maintenance of the clients' workstation becomes easier.

- **FTP:**

Especially public FTP Servers may easily contain virus infected data. The QTrust Server scans all transferred files without any user being able to avoid this control.

Moreover the QTrust Server offers further functions which make business procedures of a company more efficient:

• **Protection against SPAM and virus:**

All incoming and outgoing e-mails are checked against SPAM and virus without exception. The SPAM filter is capable of learning and recognizes automatically new SPAM techniques. SPAM recognized e-mails are identified and can then be treated by the internal mail server in the appropriate manner.

• **Packet filter (firewall):**

Based on the IP Protocol individual connections can be filtered and/or identified.

• **IPSec / VPN Gateway:**

Due to the QTrust Server it is possible to establish tightly encoded VPNs between different company locations or partner companies. It also acts as a VPN gateway for employees who need to have authorized access to company internal data and resources when they are travelling or working from the home office. IPSec and PPTP standards are supported.

• **Intrusion Detection System (IDS):**

An IDS, which reports and notifies according to easy-to-define criteria individual connections and attacks on the QTrust Server and its services is pre-configured on the QTrust Server. This information can be used as evidence in case of prosecution.

• **DHCP Server:**

The QTrust Server can also be used as DHCP Server for internal networks.

• **Load Balancer:**

If more than one web server is used in internal networks for availability reasons or for heavy network traffic the QTrust Server acts as a load balancer. External tasks are automatically distributed among internal servers.

All systems of the QTrust product family are based on hardware of Hewlett Packard. According to their demands clients can choose between four different products including service contracts and guarantees of the manufacturer. All products can be enlarged. The smallest version is a desktop system, which can be extended to larger system servers of the ProLiant product range.

EXAMPLES OF CONFIGURATION	QTrust Server Mini	QTrust Server Basic
Hardware	HP ProLiant ML110	HP ProLiant DL320
Number of users	up to 25	uo to 250
Number of nets	up to 2	up to 4
Trusted OS	yes	yes
Server architecture	yes (restricted)	yes
Maximal number of processors	1 Intel Xeon DC	1 Intel Xeon DC
Maximal RAM	8 GB	8 GB
Rackmount compatible	No	yes
Rack units	about 3 units	1 unit



QTRUST SERVER – EASY ADMINISTRATION THROUGH USEFUL PROCESSES

Configuration parameters of the QTrust Server and of all services are saved onto an internal data base. The system is maintained via a simple web interface with different authorization layers. An installation assistant helps during the initial installation. Log files can be audited via the web interface and downloaded for evaluation. Several statistics deliver information about the current system status. For automatic treatment of protocol files a net disk drive, onto which the daily files are saved, can be installed.

Important security updates are automatically installed by the QTrust Server without any administration.

Configuration can at any time and easily be saved onto an USB stick and also be re-established – changing the hardware therefore is no problem.

Due to the security measures offered by the PitBull technology it is also sure that critical configuration data cannot be changed by unauthorized persons. In the event of system failure the system can easily be restarted.

For frequently asked questions a knowledge base can be used free of charge via the QLine Portal.

ENHANCED SERVICE

QGROUP offers for the QTrust Server an enhanced support contract with the possibility to open online problem tickets via the QLine Portal (eTicket).

By closing an extensive service contract the whole administration of the QTrust Server can be outsourced to QGROUP to begin with the initial configuration up to regular maintenance and to controlling of availability of individual services.

FEATURES (OVERVIEW)	QTRUST Server	Classical firewall	Multifunction firewall
Packet filtering	√	√	√
Stateful inspection	√	•	•
Application proxy	√	•	√
Reporting	√	•	•
VPN functionality	√	√	√
IDS support	√	x	•
Protection against virus / Integration of virus scan	√	x	•
Trusted OS	√	x	x
High-availability of hardware and world-wide service	√	x	x
Infrastructure services	√	x	x
Backup and rollout via USB token	√	x	x
Sandbox principle	√	x	x
Honeypot principle	√	x	x
Optimization of mobile clients	√	x	•

√ fully available x restrictedly available • not available

