



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”

DATASHEET

The QTrust Server is the first solution that integrates application and network security functionality into one easy to administer, highly secure appliance.

Since it is the central interconnection between all external and internal networks the QTrust Server completely eliminates the direct dataflow between all connected networks. All connections are decoupled and checked by the QTrust Server on the network (IP) as well as at the application level.

All services on the attached internal servers and in the DMZ(s) are "mirrored" to the outside by the QTrust Server. The QTrust Server acts as a secure gateway for all communication and protects the attached systems, such as mail servers, web servers, etc. (based on the Sandbox Principle).

Besides application proxying and content scanning, the QTrust Server enables a large variety of logging and reporting functions, which allow detailed diagnoses. In the event of an attack, the IDS will produce an alarm.

All incoming and outgoing Email is checked for SPAM and viruses based on a defined rules/security policy. The SPAM filter is self-learning and detects new SPAM techniques automatically. Emails determined to be SPAM are marked and forwarded to the internal mail server to be processed.

All services of the QTrust Server are protected as they are completely separated and isolated by the underlying Trusted Operating System (PitBull). The PitBull TOS Technology, which in this case is integrated into a Linux Operating System optimized on security, is typically used in highly secure environments, such as transaction servers for online banking. The key advantage of this technology is that all modules or services run in their own dedicated "Security Domain", separated and isolated like they would run on their own dedicated system/hardware.

The individual modules/services are only allowed to communicate and to exchange information based on tightly defined rules. Because of this, an attack against one of the services cannot impact any of the other services running on the system. Those services will remain completely untouched.

Providing this complex variety of functionality in a highly secure way on one central system is only possible because of the integrated PitBull TOS Technology. The QTrust Server provides all required interfaces and supports all standards required for such a security appliance. Rollout and configuration is done using USB Token. This allows a seamless and easy integration into existing network and system management environments.

QUICK INFO

Product Category

- Multi-level Security Appliance

Security Appliance

- Based on Trusted Operating System Technology (Intrusion Prevention)
- Multi-level firewall and gateway
- Eliminates direct dataflow in all directions
- Omnidirectional mirroring of all services
- Highest availability as it is based on Hewlett Packard or Stratus FT Server

Gateway/Router

- Up to 20 routed networks (internal, external, DMZs [Demilitarized Zones])

Firewall

- Packet filter + stateful inspection
- IPTables, Checkpoint Firewall-1 (optional)

Application Proxies / Load Balancer

- SMTP, FTP, HTTP, HTTPS, DNS, etc.
- Forward and reverse proxying
- Load balancing

HTTP Cache for Clients

- Increase of overall Internet performance
- Traffic reduction
- High-level security for all clients

Content / Virus Scanner (omnidirectional)

- For HTTP/HTTPS, FTP, SMTP/Email

SPAM Filter (omnidirectional)

- For SMTP/Email
- Maintaining privacy

IPSec / VPN Gateway

- IPSec, PPTP, VTUN, Open VPN
- LAN to LAN between locations
- PC to LAN for employees on the road
- MobileX

Authentication Mechanisms

- Radius, PKI, LDAP, Active Directory and more

High Availability and Scalability

- Through clustering of multiple QTrust Servers
- Through high-availability systems

Logging and Reporting

- Traffic reports
- Security reports
- IDS
- Web usage

Integrated Secure SNMP Support

- Integration of system management tools

Integrated Honeypot System

- To identify attackers
- To block attacks

Ease of Use

- Role-based administration
- WEB-based administration
- Graphical configuration tools

Based on PitBull technology

- PitBull by Argus Systems Group Inc.

FEATURES (OVERVIEW)

	QTrust Server	Classical firewall	Multifunction firewall
Packet filter	✓	✓	✓
Stateful inspection	✓	•	•
Application proxy	✓	•	✓
Logging	✓	•	•
VPN functionality	✓	✓	✓
IDS support	✓	x	•
Virus protection	✓	x	•
Trusted OS	✓	x	x
USB token	✓	x	x
Sandbox principle	✓	x	x
Honeypot principle	✓	x	x
Mobile clients	✓	x	•

✓ fully available x restrictedly available • not available

