Westpac Institutional Bank

A division of Westpac Banking Corporation ABN 33 007 457 141

QuickStream

Security Features Guide

Document History

Date	Version	Description	Author
03-Feb-2003	7.1	Original Version	Qvalent
15-Sep-2003	7.1	Updated	Qvalent
7-Jul-2004	8.0	Updated for v8.0 software	Qvalent
14-Jul-2004	8.01	Updated	Qvalent
24-Jun-2005	8.1	Updated	Qvalent
8-May-2006	8.2	Updated	Qvalent
16-Aug-2006	8.3	Updated	Qvalent
27-Nov-2006	8.4	Updated	Qvalent
31-Dec-2007	9.0	Updated for v9.0	Qvalent
3-Jun-2008	10.0	Updated with LTM information	Qvalent
16-Jul-2008	10.1	Updated	Qvalent
4-Nov-2008	11.0	Updated	Qvalent
5-Nov-2008	11.1	Updated	Qvalent
22-Feb-2010	11.2	Updated	Qvalent
22-Feb-2010	11.3	Updated with FAQ	Qvalent
12-Mar-2010	11.4	Updated	Qvalent
3-May-2010	11.5	Updated	Qvalent
17-Mar-2011	11.6	Updated	Qvalent
7-Oct-2011	11.7	Updated	Qvalent
12-Oct-2011	11.8	Updated	Qvalent

Table of Contents

1 Introduction 5

2 Security Features 6

2.1 Passwords / Authentication 6

2.2 Accountability and Auditing 7

2.3 Single Sign On 7

2.4 Role Based Security 7

2.5 Intrusion Detection Controls 7

2.6 Inactivity Controls 8

2.7 Encryption 8

3 Web Based Application Development 9

3.1 Secure Coding Practices 9

3.2 Web Session Management 10

4 Messaging Controls 11

5 Credit Card Processing 13

5.1 Overview 13

5.2 How Does Qvalent Process Cards? 13

5.3 Credit Card Integration Security 14

5.4 PCI-DSS Compliance 15

6 Banking File Transfer 22

7 Data Centre Facilities 24

7.1 WAN 25

7.2 Internet 26
7.3 Network Firewalls 26
7.4 BigIP Local Traffic Manager (LTM) 28
7.5 BigIP Application Security Manger (ASM) 30
7.6 Servers 31
7.7 Monitoring and reporting 31
8 Disaster Recovery 33
8.1 What are Qvalent's disaster recovery plans? 34
9 Backups, Data Storage and Destruction 34
10 General FAQ's 35
11 Glossary 38

1 Introduction

Qvalent is a 100% owned subsidiary of the Westpac Banking Corporation and operations the QuickStream platform for Westpac.

Qvalent treats security as a prime concern. As Qvalent is a 100% wholly owned subsidiary of the Westpac Banking Corporation, it must conform to all Westpac security policies. This is to ensure that the Customer's and Westpac's data is secure, no insecure network applications are used and all communications between Qvalent applications themselves or external applications are carried out over secure links. In addition all financial data transmitted between Qvalent (Westpac) must be encrypted and digitally signed for both the customer and Westpac's protection. Some of the key security measures used by Qvalent consist of:

- PCI-DSS Compliant (Level 1).
- AS2805 Compliant.
- Application firewalls to prevent data leakage.
- Single sign on for all users;
- All applications share same security code base;
- Every page validates a user's security;
- Users are only allowed to view data for companies that they are associated with;
- Message encryption using SSL between both internal and external systems;
- Basic authentication for all messages sent between Qvalent and external systems;
- Reverse IP lookup's to check to origin of received messages;
- Full digital certificate (both client & server) support;
- All critical user and financial information is stored encrypted using private keys in the database;
- Access to the database is only allowed through security data access objects;
- Multiple firewall cells; and
- All ports and IP addresses blocked by default, only specific addresses and ports are open.
- Qvalent's wide area network is managed by Optus and its data centre / internal network by Hewlett Packard. Both of these companies use best of breed practices.

2 Security Features

2.1 Passwords / Authentication

The application authenticates users through X.509 certificates or by a user name/password combination. The database cannot be read to reveal user passwords as they are held in encrypted form. To this end when a user wishes to change their password, the system will only transmit the keystrokes encrypted, thus the line cannot be 'sniffed' effectively. Once authenticated, the user has a session variable created and kept as a server-side cookie, which is passed to every page accessed throughout the user's session.

When a user is authenticated, they are assigned user rights within a company. These security rights can be limited to an individual, group or company level. Access to information is based on a user's security rights and the company administrator controls this.

Some of Qvalent's password management capabilities include:

- Minimum of eight characters;
- Must contain letters and numbers;
- Can only be changed once in a 24 hour period;
- Must be changed every 42 days;
- Cannot reuse the last 5 password;
- Ability to enforce password expiration;
- Passwords stored as a hash;
- Ability to require automatic password expirations when initially assigned or reset;
- Ability to require re-authentication after 15 minutes of inactivity.
- Ability to automatically disable accounts after a period of inactivity (120 days);
- Ability to manually lock out a user account;
- Ability to lock out an account automatically after a defined number of incorrect logins (5 attempts);
- Password suppression (masked) during entry at sign on dialogue;
- Passwords are masked from all outputs (e.g. reports, logs, etc);
- Passwords cannot be retrieved or viewed from password database;
- Ability to permit user-initiated resetting of passwords;
- Forced password re-entry verified (old pw, new pw, and new pw again);
- Ability to deactivate or change passwords of vendor supplied Ids;
- Ability to force password changes; and
- Support for One Time Passwords (OTP).

2.2 Accountability and Auditing

Qvalent products provide the following accountability and auditing functionality;

- Audit logs can be secured from unauthorized access;
- Ability to log activities performed by specific ID or time of day;
- Ability of audit log to time and date stamp all actions for each ID;
- Ability to filter the level of logging based on log masks;
- Ability to identify and log all subsequent access points - accountability is maintained throughout session;
- Ability to log successful and unsuccessful single sign-on attempts;
- Failed access attempts to specific domains, files, directories, URLs can be logged;
- Administrative functions can be logged and are auditable;
- Ability to maintain the user's identity for the duration of the session; and
- Ability to prevent the display of passwords on audit logs.

2.3 Single Sign On

Qvalent applications allow external validation systems to be used to replace its standard login processor. A custom "Authenticator" java class that implements a defined interface can be created to meet specific customer requirements. Typical uses for this "Authenticator" revolve around a company having a single sign-on system (SSO) that all users must log on too. Through the use of an "Authenticator", Qvalent Procurement can be integrated with such a system. The creation and deletion of Procurement user accounts can also be managed through Qvalent's iConnect technology. This allows users to be added, updated or deleted automatically via iConnect integration packages. Once again these packages can be integrated with SSO systems.

2.4 Role Based Security

All users require individual sign ons to the applications, no generic accounts are allowed. All user id's are role based with particular rights assigned to those roles. Quick Stream provides a flexible framework that allows organisations to be 'self managing'. This means that within an organisation rights and roles can be assigned by personnel within that organisation (Community Administrators).

2.5 Intrusion Detection Controls

The Qvalent suite offers a number of Intrusion Detection Controls. These include:

- Ability to set an unsuccessful access attempt limit;

- Ability to suspend ID after reaching the unsuccessful access threshold;
- Ability to display time/date of last successful logon;
- Ability to display number of unsuccessful logon attempts since last successful log-in;
- Ability to send alerts to administrators for unauthorized access attempts;
- Ability to detect incoming messages from unauthorised sources; and
- In addition to software control Hewlett Packard provides comprehensive network event detection and notification management.

2.6 Inactivity Controls

Qvalent products provide the following inactivity controls:

- Automatic logoff of ID after a 15 minute period of session inactivity; and
- After lock-out, re-access require password authentication

2.7 Encryption

Externally, all inbound and outbound sensitive data is encrypted and digitally signed. For file based transfers this is PGP with a 1024bit key. For stream based exchanges this is over SSL with 128bit certificates.

Internally, Qvalent uses the triple DES algorithm in cipher-feedback mode and AES for all two-way data encryption. The encrypted information can optionally be returned in a base 64 encoded string.

3 Web Based Application Development

3.1 Secure Coding Practices

Qvalent web software and applications development philosophy is based on secure coding guidelines such as the Open Web Application Security Project guidelines. Review custom application code to identify coding vulnerabilities. See www.owasp.org - "The Ten Most Critical Web Application Security Vulnerabilities." Cover prevention of common coding vulnerabilities in software development processes, to include:

- Unvalidated input - All data is validated by a common framework in the application, where required fields are checked, along with input length and data format (for non-free text fields).

- Broken Access control – Qvalent applications automatically lock out accounts after a set number of invalid login attempts to prevent 'brute force' attacks. Broken authentication and session management (use of account credentials and session cookies) - Session IDs are generated using a 128-bit cryptographic pseudo-random number generator, making guessing the next ID implausible. The session ID is 128-bits long. The session ID is temporary in nature, and is not stored on the user's disk. It is also only contained in the memory of the application server, and never written to disk. Sessions are also automatically timed out after a period of inactivity.

- Cross Site Scripting (XSS) attacks - Qvalent's architecture uses XSL to generate the HTML displayed to users. The servlets on the application server generate XML which is then transformed into what the user sees. The underlying technology prevents this kind of attack, since any dangerous characters in the output (such as "<script>") are automatically escaped by the framework. The consequence of this is that if a user enters "<script>" into an input field, that data will later be sent back to the browser as "<script>", which will be displayed as "<script>" by the browser.

- Buffer Overflow Attacks - The underlying platform is Java, which is not vulnerable to using exceptionally long string s to overflow buffers. The application server prevents requests which would be large enough to fill the entire server memory.

- SQL Injection Flaws – Qvalent uses prepared statements for all its SQL. This prevents SQL statements that are entered into data fields from being executed.

- Improper Error Handling - System error messages contain only a reference number which can be reported to the helpdesk. No stack traces of any kind are included in the page.

- Insecure Storage – All sensitive data is stored encrypted in Qvalent databases. These databases reside behind multiple firewalls.
- Denial Of Service - Qvalent uses Hewlett Packard to host its servers. HP have intrusion detection systems in place to detect and respond to these kinds of attacks such as ping of death, tear drop, Syn flood etc. Qvalent web servers also limit the number off sessions from a particular IP address.

- Insecure Configuration Management – All Qvalent servers are built to strict security standard using a specific build process. All non essential services and accounts are removed at build time.

- Cross Site Request Forgery - Qvalent applications do not allow login on any page - login is only allowed from the login page. High profile actions (such as making a payment or changing user details) can only be performed via POST. These pages also include a random token to prevent automated CRSF attacks.

- Failure to restrict URL Access - Qvalent applications use a common authorisation framework to ensure that users only access pages permitted by their defined user roles. Internal application server URLs are blocked by the web server - they are not externally accessible. All Qvalent servers are built to strict security standard using a specific build process. All non essential services and accounts are removed at build time.

3.2 Web Session Management

Key features of web session management that are built into Qvalent products:

- All sessions timeout after 15 minutes of inactivity. If the user attempts to access another page after this timeout, they are informed that they must login again.

- All session state is stored on the server – no session data is stored in the browser. The browser only has a non-persistent cookie containing the session ID.

- Session id's are 256 bits in length and are generated using a secure cryptographic random number generator.

- Application firewalls monitor session IDs for evidence of tampering

- Cross site request forgery (CSRF) is prevented through the server requiring HTTP POST and a random token for pages that perform an action (such as making a payment or updating data).

- User sessions are under SSL all the way through the untrusted and trusted zones to the app servers. There is no unencrypted session transmissions on the internal production network.

4 Messaging Controls

System interfaces involve sharing of data between the various modules of the Qvalent product suite and systems external to the Qvalent suite. Interfaces between Qvalent modules involve the following elements:

- Extensible Mark-up Language (XML); Hypertext Transport Protocol (HTTP); Secure HTTP (HTTPS); and XML Remote Procedure Calls (XMLRPC);
- Using QXML, cXML or OBI messages transported by HTTP or HTTPS provides asynchronous communication between modules and Supplier systems. XMLRPC is used to manage synchronous communication between these systems;
- iConnect facilities (iConnect Exchange Manager and iConnect Integration Manager) provide guaranteed delivery and routing of messages between modules and with customer business systems;
- Interfaces with customer business systems can use a combination of the following elements - HTTP or HTTPS; XCOM with encryption and signatures using X.509 or Pretty Good Privacy (PGP); XML, OBI; and flat files (fixed width fields or delimited) or custom solutions based on Customer requirements;
- All external systems sending messages to Qvalent must be pre-registered otherwise the message will not be accepted (reverse IP lookup is used for all incoming messages);
- All financial data transmitted between the customer and Qvalent must be encrypted and digitally signed to ensure security and non-repudiation of the source;
- All Qvalent messaging is compatible with firewalls and proxy servers.
- 128-bit SSL is the only available level of encryption. SSL version 2 is not allowed, and neither is step-down encryption to 56-bit keys. RC4/MD5 is the allowed combination for 128-bit encryption.

- Automated scanning is performed on a 3 monthly basis by an independent security firm as part of PCI security requirements.

5 Credit Card Processing

5.1 Overview

Qvalent operates a high performance IP to X.25 card interchange known as P&P Cards. This is part of the Quick Stream Platform. P&P Cards allows customers to connect to Westpac via a variety of different technologies over an IP based network and process card transactions.

5.2 How Does Qvalent Process Cards?

Qvalent accepts an IP based card request and once security is verified the IP request is converted into a standard AS2805 message. Once this conversion is complete it is transmitted directly into Westpac's Tandem's for processing. In addition to credit card, Qvalent also has high performance IP based links into Westpac's extranet to allow daily files such as the credit card transaction log to be transmitted to Westpac for end of day settlement.

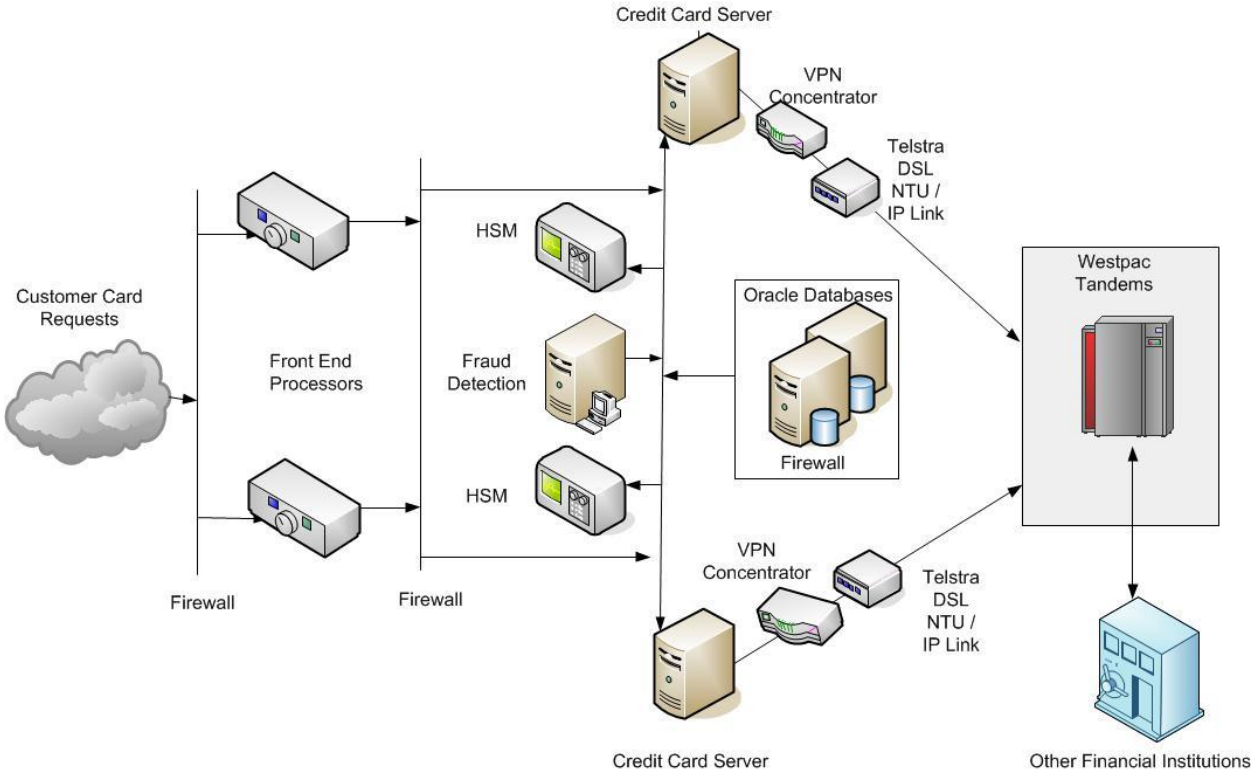


Figure 1, Qvalent / Westpac Tandem Links

5.3 Credit Card Integration Security

For a solution of this nature, security is critical. Qvalent must be absolutely confident that they are receiving a credit card processing request from an authorised source. To ensure the source of the request is valid, the following measures will be adopted:

- The Customer must be registered before credit card processing will begin. Part of this registration will be to issue the customer with a username and password. This username/password combination must be passed in with every request.

- Qvalent will only accept requests from certain pre-agreed IP addresses.

- For high volume customers Qvalent will recommend that a virtual private network (VPN) be installed between the customer's site and Qvalent's data centre.

- For added security a card verification number (CVN) can be supplied with the credit card API call. The CVN is not stored by Qvalent.
- All transaction data will be communicated via HTTPS with 128-bit encryption.

- In order of preference, the recommended communications infrastructure would be as follows:
  1. Leased line between the customer's site and Westpac's credit card server. In this scenario, no data would be transmitted over the Internet. Username / password are still mandatory.

  2. Client certificate exchange with username / password over HTTPS. With client certificates Westpac can be assured of the source of the request. The Customer must obtain a 128-bit SSL Certificate from a registered Certificate Authority (eg Verisign). This may be purchased or an existing, valid certificate may be used for this purpose. **Note: this SSL certificate must have the property "Proves your identity to a remote computer". Without this property set on the certificate, Qvalent will not accept credit card API connection requests.**

5.4 PCI-DSS Compliance

Qvalent is a tier 1 Interchange and PCI-DSS compliant (Level 1). The below table is Qvalent's answers to the PCI-DSS questionnaire.

Install and maintain a firewall configuration to protect data		Yes	No	N/A
1.1	Are all router, switches, wireless access points, and firewall configurations secured and do they conform to documented security standards?	√		
1.2	If wireless technology is used, is the access to the network limited to authorized devices?			√
1.3	Do changes to the firewall need authorization and are the changes logged?	√		
1.4	Is a firewall used to protect the network and limit traffic to that which is required to conduct business?	√		
1.5	Are egress and ingress filters installed on all border routers to prevent impersonation with spoofed IP addresses?	√		
1.6	Is payment card account information stored in a database located on the internal network (not the DMZ) and protected by a firewall?	√		
1.7	If wireless technology is used, do perimeter firewalls exist between wireless networks and the payment card environment?			√
1.8	Does each mobile computer with direct connectivity to the Internet have a personal firewall and anti-virus software installed?	√		
1.9	Are Web servers located on a publicly reachable network segment separated from the internal network by a firewall (DMZ)?	√		
1.10	Is the firewall configured to translate (hide) internal IP addresses, using network address translation (NAT)?	√		

Do not use vendor-supplied defaults for system passwords and other security parameters		Yes	No	N/A
2.1	Are vendor default security settings changed on production systems before taking the system into production secured and do they conform to documented security standards?	√		
2.2	Are vendor default accounts and passwords disabled or changed on production systems before putting a system into production?	√		
2.3	If wireless technology is used, are vendor default settings changed (i.e. WEP keys, SSID, passwords, SNMP community strings, disabling SSID broadcasts)?			√
2.4	If wireless technology is used, is Wi-Fi Protected Access (WPA) technology implemented for encryption and authentication when WPA-capable?			√
2.5	Are all production systems (servers and network components) hardened by removing all unnecessary services and protocols installed by the default configuration?	√		
2.6	Are secure, encrypted communications used for remote administration of production systems and applications?	√		

Protect stored data		Yes	No	N/A
3.1	Is sensitive cardholder data securely disposed of when no longer needed?	√		
3.2	Is it prohibited to store the full contents of any track from the magnetic stripe (on the back of the card, in a chip, etc.) in the database, log files, or point-of-sale products?	√		
3.3	Is it prohibited to store the card-validation code (three-digit value printed on the signature panel of a card) in the database, log files, or point-of-sale products?	√		
3.4	Are all but the last four digits of the account number masked when displaying cardholder data?	√		
3.5	Are account numbers (in databases, logs, files, backup media, etc.) stored securely for example, by means of encryption or truncation?	√		

Protect stored data		Yes	No	N/A
3.6	Are account numbers sanitized (removed, truncated or encrypted) before being logged in the audit log?	√		

Encrypt transmission of cardholder data and sensitive information across public networks		Yes	No	N/A
4.1	Are transmissions of sensitive cardholder data encrypted over public networks through the use of SSL or other industry acceptable methods?	√		
4.2	If SSL is used for transmission of sensitive cardholder data, is it using version 3.0 with 128-bit encryption?	√		
4.3	If wireless technology is used, is the communication encrypted using Wi-Fi Protected Access (WPA), VPN, SSL at 128-bit, or WEP?	√		
4.4	If wireless technology is used, are WEP at 128-bit and additional encryption technologies in use, and are shared WEP keys rotated quarterly?			√
4.5	Is encryption used in the transmission of account numbers via e-mail?	√		

Use and regularly update anti-virus software		Yes	No	N/A
5.1	Is there a virus scanner installed on all servers and on all workstations, and is the virus scanner regularly updated?	√		

Develop and maintain secure systems and applications		Yes	No	N/A
6.1	Are development, testing, and production systems updated with the latest security-related patches released by the vendors?	√		
6.2	Is the software and application development process based on an industry best practice and is information security included throughout the software development life cycle (SDLC) process?	√		
6.3	If production data is used for testing and development purposes, is sensitive			√

Develop and maintain secure systems and applications		Yes	No	N/A
	cardholder data sanitized before usage?			
6.4	Are all changes to the production environment and applications formally authorized, planned, and logged before being implemented?	√		
6.5	Were the guidelines commonly accepted by the security community (such as Open Web Application Security Project group (www.owasp.org)) taken into account in the development of Web applications?	√		
6.6	When authenticating over the Internet, is the application designed to prevent malicious users from trying to determine existing user accounts?	√		
6.7	Is sensitive cardholder data stored in cookies secured or encrypted?			√
6.8	Are controls implemented on the server side to prevent SQL injection and other bypassing of client side-input controls?	√		

Restrict access to data by business need-to-know		Yes	No	N/A
7.1	Is access to payment card account numbers restricted for users on a need-to-know basis?	√		

Assign a unique ID to each person with computer access		Yes	No	N/A
8.1	Are all users required to authenticate using, at a minimum, a unique username and password?	√		
8.2	If employees, administrators, or third parties access the network remotely, is remote access software (such as PCAnywhere, dial-in, or VPN) configured with a unique username and password and with encryption and other security features turned on?	√		
8.3	Are all passwords on network devices and systems encrypted?	√		
8.4	When an employee leaves the company, are that employees user accounts and passwords immediately revoked?	√		

Assign a unique ID to each person with computer access		Yes	No	N/A
8.5	Are all user accounts reviewed on a regular basis to ensure that malicious, out-of-date, or unknown accounts do not exist?	√		
8.6	Are non-consumer accounts that are not used for a lengthy amount of time (inactive accounts) automatically disabled in the system after a pre-defined period?	√		
8.7	Are accounts used by vendors for remote maintenance enabled only during the time needed?			√
8.8	Are group, shared, or generic accounts and passwords prohibited for non-consumer users?	√		
8.9	Are non-consumer users required to change their passwords on a pre-defined regular basis?	√		
8.10	Is there a password policy for non-consumer users that enforces the use of strong passwords and prevents the resubmission of previously used passwords?	√		
8.11	Is there an account-lockout mechanism that blocks a malicious user from obtaining access to an account by multiple password retries or brute force?	√		

Restrict physical access to cardholder data		Yes	No	N/A
9.1	Are there multiple physical security controls (such as badges, escorts, or mantraps) in place that would prevent unauthorized individuals from gaining access to the facility?	√		
9.2	If wireless technology is used, do you restrict access to wireless access points, wireless gateways, and wireless handheld devices?			√
9.3	Are equipment (such as servers, workstations, laptops, and hard drives) and media containing cardholder data physically protected against unauthorized access?	√		
9.4	Is all cardholder data printed on paper or received by fax protected against unauthorized access?	√		

Restrict physical access to cardholder data		Yes	No	N/A
9.5	Are procedures in place to handle secure distribution and disposal of backup media and other media containing sensitive cardholder data?	√		
9.6	Are all media devices that store cardholder data properly inventoried and securely stored?	√		
9.7	Is cardholder data deleted or destroyed before it is physically disposed (for example, by shredding papers or degaussing backup media)?	√		

Track and monitor all access to network resources and cardholder data		Yes	No	N/A
10.1	Is all access to cardholder data, including root/administration access, logged?	√		
10.2	Do access control logs contain successful and unsuccessful login attempts and access to audit logs?	√		
10.3	Are all critical system clocks and times synchronized, and do logs include date and time stamp?	√		
10.4	Are the firewall, router, wireless access points, and authentication server logs regularly reviewed for unauthorized traffic?	√		
10.5	Are audit logs regularly backed up, secured, and retained for at least three months online and one-year offline for all critical systems?	√		

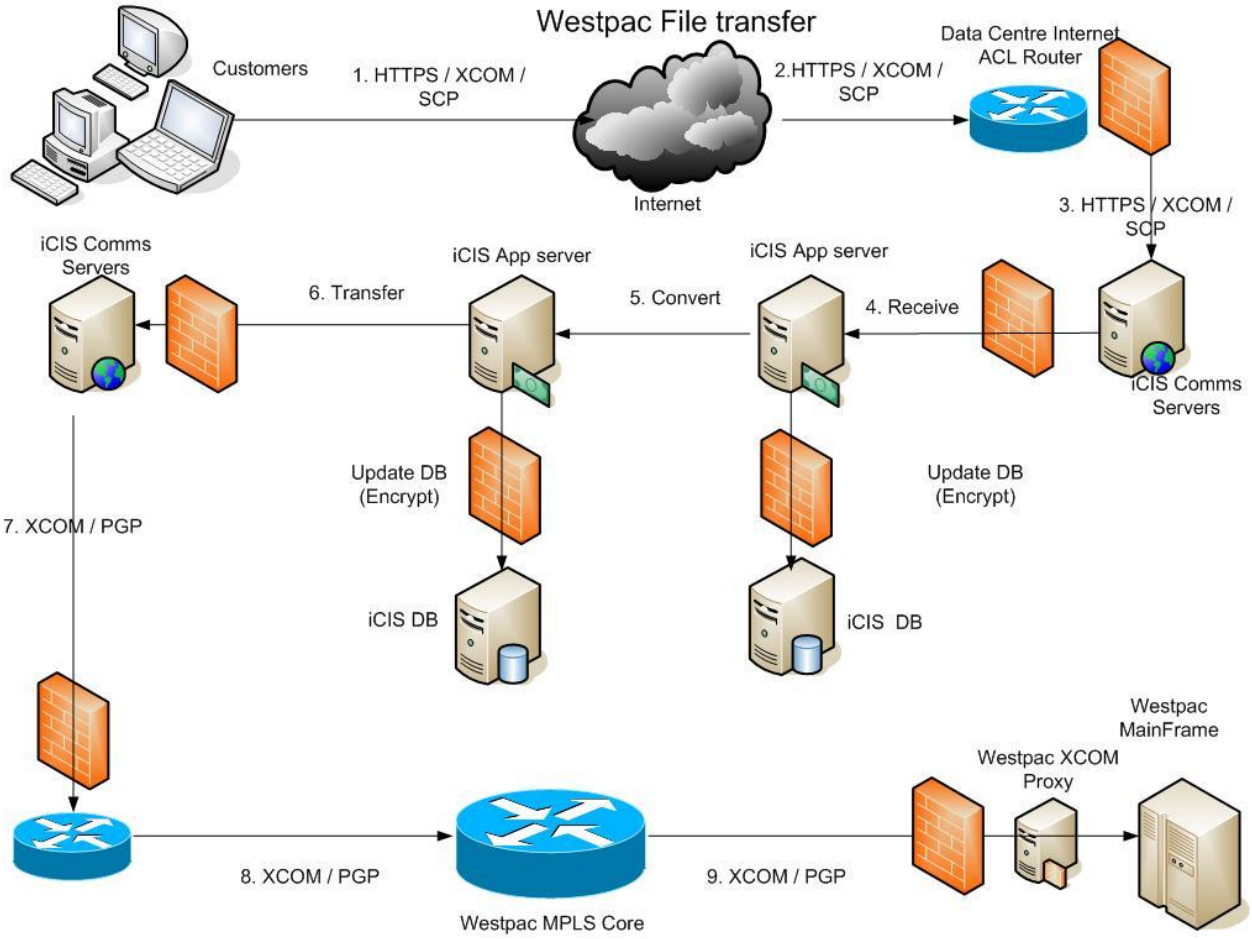
Regularly test security systems and processes		Yes	No	N/A
11.1	If wireless technology is used, is a wireless analyzer periodically run to identify all wireless devices?			√
11.2	Is a vulnerability scan or penetration test performed on all Internet-facing applications and systems before they go into production?	√		
11.3	Is an intrusion detection or intrusion prevention system used on the network?	√		
11.4	Are security alerts from the intrusion detection or intrusion prevention system (IDS/IPS) continuously monitored, and are the latest IDS/IPS signatures	√		

Regularly test security systems and processes		Yes	No	N/A
	installed?			

Maintain a policy that addresses information security		Yes	No	N/A
12.1	Are information security policies, including policies for access control, application and system development, operational, network and physical security, formally documented?	√		
12.2	Are information security policies and other relevant security information disseminated to all system users (including vendors, contractors, and business partners)?	√		
12.3	Are information security policies reviewed at least once a year and updated as needed	√		
12.4	Have the roles and responsibilities for information security been clearly defined within the company?	√		
12.5	Is there an up-to-date information security awareness and training program in place for all system users?	√		
12.6	Are employees required to sign an agreement verifying they have read and understood the security policies and procedures?	√		
12.7	Is a background investigation (such as a credit- and criminal-record check, within the limits of local law) performed on all employees with access to account numbers?	√		
12.8	Are all third parties with access to sensitive cardholder data contractually obligated to comply with card association security standards?	√		
12.9	Is a security incident response plan formally documented and disseminated to the appropriate responsible parties?	√		
12.10	Are security incidents reported to the person responsible for security investigation?	√		
12.11	Is there an incident response team ready to be deployed in case of a cardholder data compromise?	√		

6 Banking File Transfer

Qvalent operates dual redundant Ethernet links into Westpac's MPLS network. These links are with different providers and have automatic failover. Similar Ethernet links are also installed at Qvalent's DR site. Customers transfer files to Qvalent via various means such as HTTPS, XCOM or SCP either via the internet or leased lines. All received data must be encrypted. Qvalent in turn encrypts and digitally signs (PGP) all data before sending it onto Westpac. All transfers are via XCOM over Qvalent's secure Ethernet links.



The following steps take place when Customers need to transfer data to Qvalent for processing. Qvalent then inturn forwards it onto Westpac. This can be a user to system transfer (via iLinc) or a system to system transfer process:

1-3 Customers attempt to connect to Qvalent via one of various means such as HTTPS, XCOM, SCP/SFTP or other mechanism. The data centre internet facing routers screen the incoming IP addresses against their ACL lists. All connections require security credentials and the data is checked to ensure that it came from a trusted source.

4. Protocol and port redirection take place through the firewall to the iCIS messaging hub. This is the central switch for all messaging communications with Qvalent. This data is then stored encrypted in Qvalent's databases.

5-6. The iCIS App server converts the file into the required Westpac format then PGP encrypts and digitally signs the file. The file is then passed to the iCIS comms server for transmission.

7-9. The iCIS comms server transmitted the encrypted file via XCOM to the Westpac proxy server. The Westpac proxy server decrypts the file then passes it to the Westpac mainframe for processing.

The reverse applies when Westpac sends files back to Qvalent.

7 Data Centre Facilities

Qvalent is a 100% owned subsidiary of Westpac and operates an A2 class data centre and associated disaster recovery (DR) facilities for Westpac's QuickStream product suite. This facilities and infrastructure has been designed to ensure the minimum failover time to the disaster recovery facility in the event that the primary facility becomes incapacitated.

Qvalent operates an A2 class data centre facility that is managed by Hewlett Packard (HP) on Qvalent's behalf. HP is a world leader in data centre management and brings world's best practices to the daily running of this centre. This data centre has all the features you would expect in a state of the art facility including 24x7 security, battery back up, diesel generators and fire suppression systems. Once again, like Qvalent's WAN all paths are redundant with automatic failover.

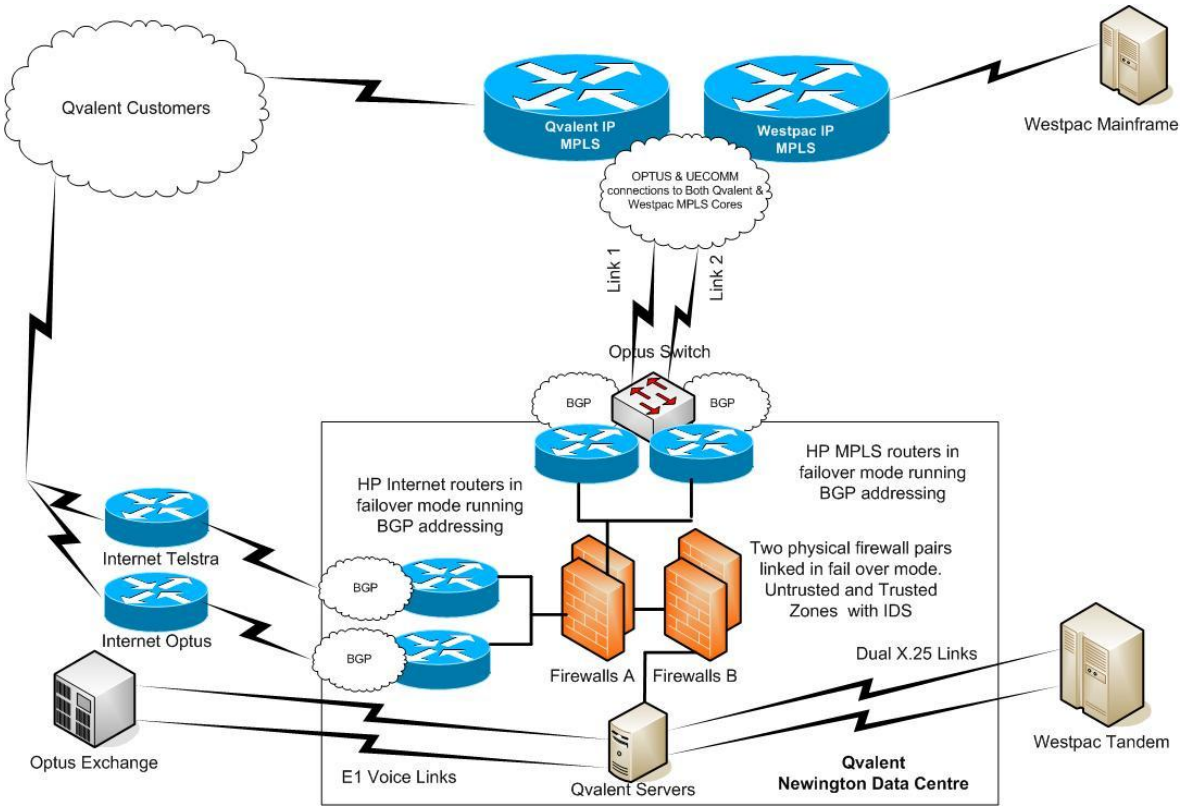


Figure 2, Qvalent Primary Data Centre

7.1 WAN

To achieve a successful transition to Qvalent's DR facility Qvalent utilises a 'hub and spoke' network design that allows network traffic to be redirected to the Qvalent DR site without any hardware changes. In addition to this the network is designed with redundancy in mind. This ensures that no single point of failure will prevent the network from functioning. Qvalent utilises Optus's MPLS IP based network technology and dual paths with different internet service providers (Optus and Telstra) to ensure that all network path are redundant with automatic failover.

The Qvalent infrastructure has been reviewed by Westpac and external auditors against the AS2805 standard and the Visa / MasterCard PCI standard. As part of these standards Qvalent submits to yearly security audits and tri-monthly network vulnerability scans.

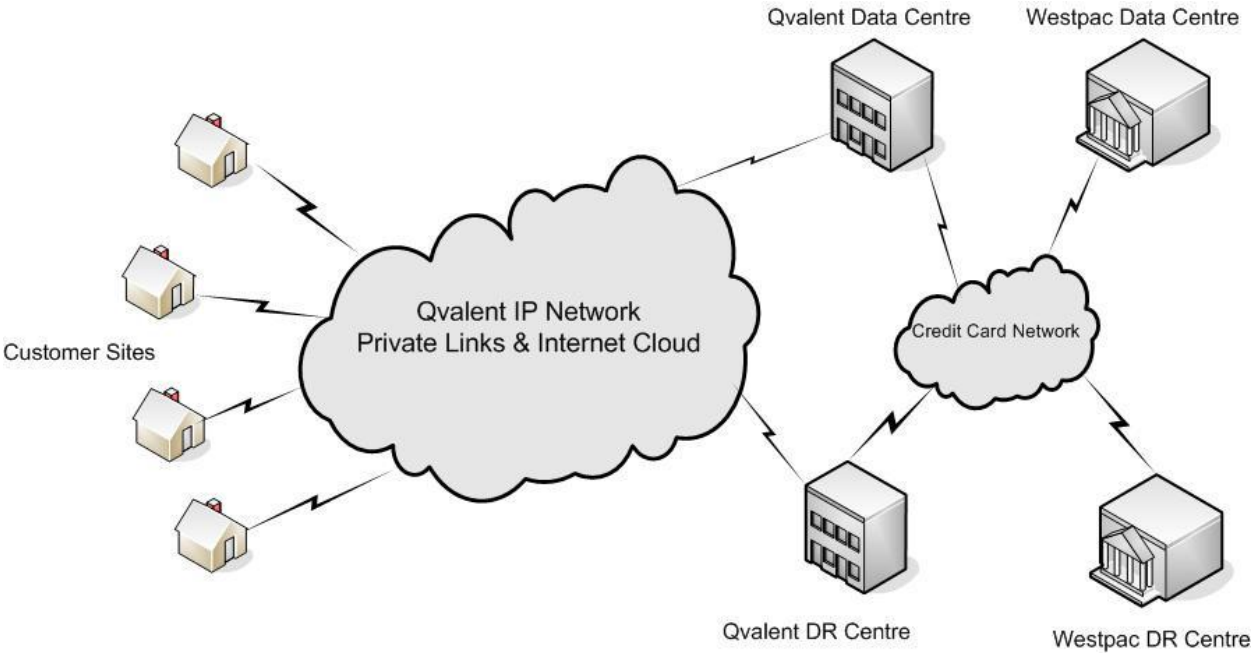


Figure 3, WAN Network

7.2 Internet

Qvalent's data centre has dual redundant internet links with both Telstra and Optus. HP's internet facing routers run access control lists to limit any Internet addresses (for example due to a DOS attack) before they hit the firewalls or servers. Internet connections through the firewalls can only be approved by Qvalent's Chief Technology Officer. Refer to Figure 2, Qvalent Primary Data Centre.

7.3 Network Firewalls

All firewalls within Qvalent's data centre are managed by Hewlett Packard. All servers are partitioned into a three layer firewall model with the web, application and database cells all being separated by firewalls. No data is kept on the web or application servers. In addition to this port redirection is used. For example, the web firewall will only let in port 443 on specified IP addresses, the application cells will only let in tomcat port numbers on specific addresses and the DB cell will only let in DB port numbers on specific addresses.

By default, all IP addresses and ports are blocked on all firewalls. Firewall changes can only be approved by Qvalent's Chief Technology Officer (CTO). Dual firewalls are used between trusted and non-trusted zones. All data received from customers arrives in the untrusted zone where it is checked, then moved into the trusted zone for processing. Decryption only takes place in the trusted zone. All firewalls operate in pairs with automatic failover. An overview of the zones and firewalls are shown in Figure 4, Firewalls.

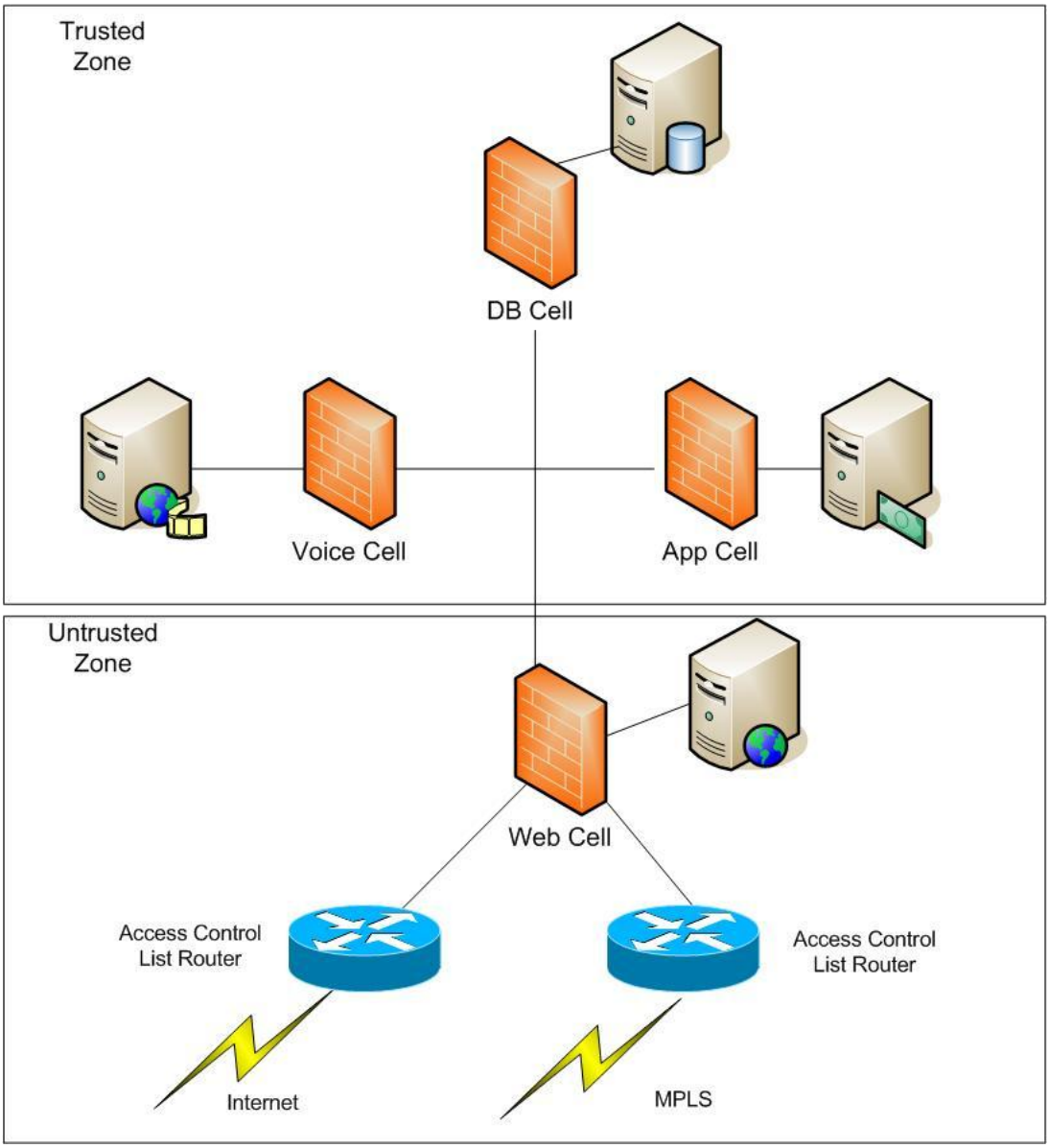


Figure 4, Firewalls

7.4 BigIP Local Traffic Manager (LTM)

The BigIP Local Traffic Manager (LTM) is a major component of our Production and Support environment BigIP Appliances produced by F5 Networks.

LTMs unlock a variety of benefits to our applications and general system security.

- Allows SSL acceleration by offloading SSL processing to the LTM appliance, rather than the application server
- Allows for web applications to be load balanced over a number of server instances to increase uptime and availability
- Reduces the need to complex network outages and redirections through the implementation of virtual IP addresses to a pool of load balanced servers for a particular application
- Allows for complex network security to be incorporated via BigIP iRules to deny certain types of traffic from entering the internal network.

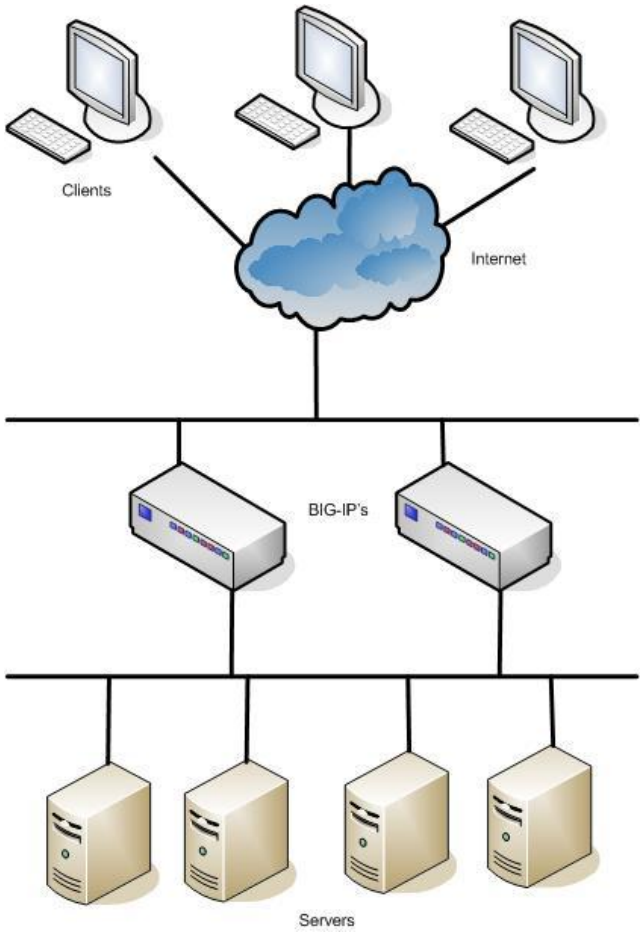


Figure 5, Big IP Local Traffic Manager (LTM) Setup

Being the point where clients are redirected to a particular web server after passing through the firewall, Qvalent vigorously logs all data coming in and out of the BigIP LTM appliances as it provides us with information regarding

- SSL session acceptance/rejection
- HTTP Requests and Responses
- Allows tracking of which web server instance a particular request was processed and served on
- Provides information on BigIP system messages such as configuration changes, system restarts, BigIP appliance users being added, deleted or modified, etc.

This information is of upmost importance to Qvalent in order to maintain our high standards of information security compliance. This log data is then sent to a variety of different systems, the most important being securely sending the log information to the RSA enVision appliance on all Production LTM appliances in order to ensure that the logs are kept tamper-proof and secure.

7.5 BigIP Application Security Manger (ASM)

The BigIP Application Security Manager (ASM) is an Application Firewall device which provides a security solution for web and IP-based applications and services. It is designed to protect against known types of external security threats at the network and application layer. ASMs main role, is the role of an Application Firewall which specifically protects the application from malicious attacks and hackers.

ASM works by:

- Scrubbing sensitive data and parameters (eg. scrubbing certain Credit Card number parameters from being returned to the user)
- Assists in the cloaking of application infrastructure design specifics from hackers
- Ensures that only expected application traffic is allowed, and suspicious or unexpected application traffic is monitored closely and blocked or denied if need be.

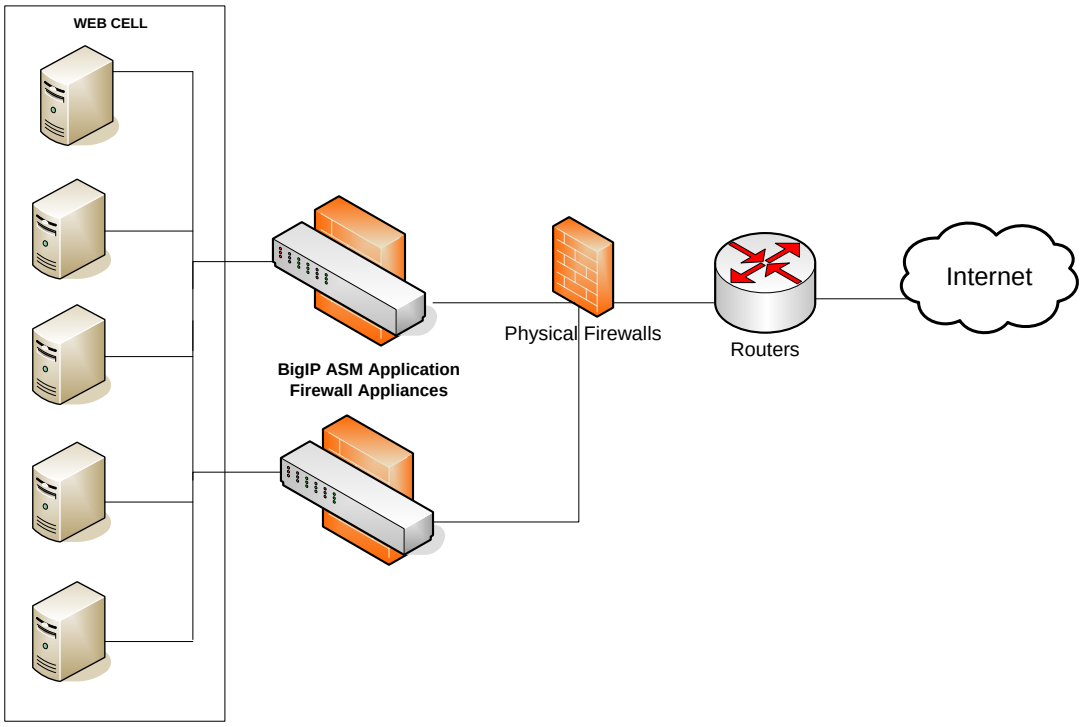


Figure 6, BigIP ASM Architecture

7.6 Servers

All servers use hardened builds and are constantly updated with the last virus definition files and security patches. All servers have real-time monitoring installed and report hourly averages of CPU, I/O and memory usage for performance monitoring and tuning. All software changes must pass through a development and staging environment before they can be installed on production servers.

7.7 Monitoring and reporting

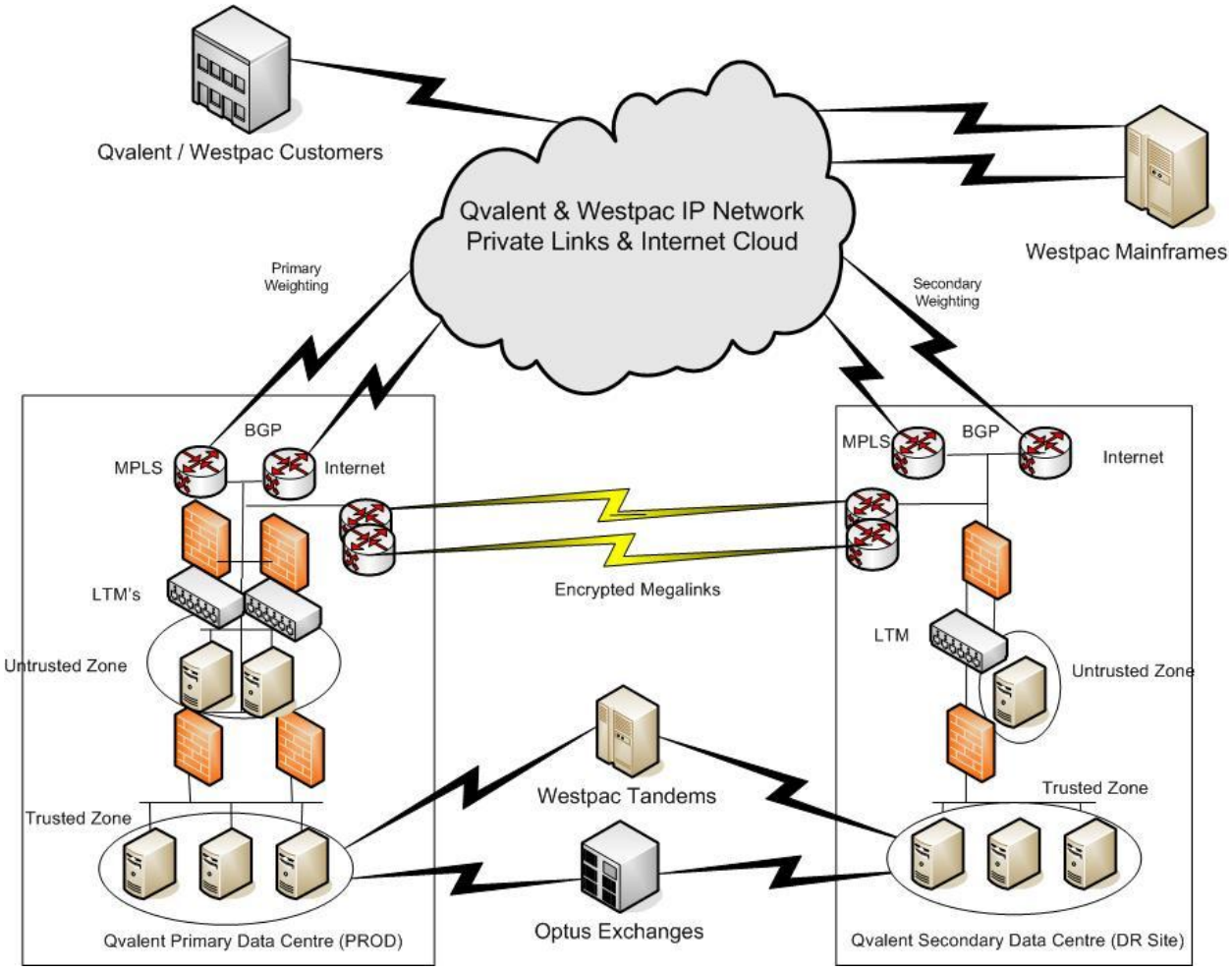
All production systems (networks, servers and applications) are monitored 24x7 via HP Openview. Any alarms generated are reported to a 24x7 help desk that will then contact the appropriate support personnel.

Monitoring also extends to security and fraud detection systems. These have the ability to take proactive messages automatically in the event that suspicious behaving is detected.

Daily Performance and capacity figures are collected on network appliances, links and servers.

8 Disaster Recovery

Qvalent operates a standby site located in a different location to its primary facility. This facility runs a replication of all applications that are currently operating in the production environment. Also, in real time, database transactions are replicated to the DR site to ensure that standby databases are always up to date. This facility contains all necessary systems and network links to operate as a production facility.



8.1 What are Qvalent's disaster recovery plans?

Qvalent has a comprehensive set of disaster recovery plans for the primary data centre site and also for the DR site itself. These plans are reviewed every six months and practised to ensure that any recovery activity takes place smoothly with minimum impact to customer services.

9 Backups, Data Storage and Destruction

The security of customer's data is of primary importance to Qvalent. All critical data stored in databases is encrypted using AES-256. All servers and databases have full backups carried out every night. These backups are then transported off site to a secure storage facility that is PCI-DSS level 1 certified every year. Transport to this facility is via vehicles with GPS transponders installed so vehicle movements can be tracked. All backup tapes are scanned in and out of the facility and stored in temperature controlled vaults. Tapes are not labelled in any way that would identify the customer or what was stored on the tape. After the seven years of storage the backup tapes are destroyed and a certificate of destruction is issued.

10 General FAQ's

Q) Provide details of your system architecture (Hardware and platforms, Operating Systems, Server hardware)

A) Qvalent's system architecture is based on industry best practice. The architecture is broken down into zones of trust with the outer zones being least trusted. The zones are physically separated and all traffic must be authenticated before it can move from one zone to another. Qvalent's systems architecture has been accredited to PCI-DSS level 1 compliant.

Qvalent operates four physically separated (in both hardware and location) environments. These consist of development, testing, production and DR.

Servers are HP Wintel X64 hardware, networking equipment is CISCO based while load balancing and application firewalls are F5 based.

Q) Provide details of your system availability, providing actual system availability figures from 2007 – 2009

A) From 2007 – 2009 Qvalent has offered an SLA of 99.5%. This has been exceeded with an uptime of 99.98% during this period.

Q) Provide details of the scalability of your systems

A) Qvalent uses F5 Big IP technology for its hardware load balancing and application firewalls. This allows additional servers to be added in the event that additional capacity is required without customer impact. Qvalent's applications are cluster aware and allow additional instances to be brought online as capacity requires it.

Reports generated on a daily basis report on current capacity across all production servers.

Q) Provide details of your redundancy processes

A) In Qvalent's production facilities all networking equipment is redundant with automatic failover. WAN routers run BGP to automatically fail over links. The routers themselves run HSRP to handle hardware failure. Firewalls and load balancers run in master / slave configuration with automatic fail over.

Multiple instances of applications run with automated failover in the event of an application becoming unavailable in the load balanced pool.

What archiving technology exists today?

Real-time:
- All data is replicated in real time to Qvalent's DR site.

Daily:
- All systems have full backups daily which are stored off site

Long term:
- Data is available up to 7 years

Q) Provide details of your software development and software release practices processes

A) The development procedure is based on Rational's Unified Process (RUP). At a high level the following procedure must be followed:

- Requirements are entered into Jira and approved by the Release / Product Manager.
- Developer codes solution and builds patch or new version. Unit tests in Dev. Marks are ready for test in Jira.
- All coding and documentation must be stored in Subversion
- Patch is installed in SOCT (test) by Operations.
- Independent tester performs UAT on the patch and performs a code review before approving in Jira.
- Peer Review control sheet is filled out.
- Management approves production release (via product release control sheet).
- Operations install into production and record installation.
- Release Manager performs post installation check

Q) Is your software written by your organization or acquired from a third party?

A) Qvalent is primarily a software development company. With the exception of its data base technology (Oracle) all payment processing software is written by Qvalent.

Q) Provide details of your system monitoring capabilities

A) Qvalent's data centre's are managed by Hewlett Packard. All production equipment is monitored 24x7 by HP OpenView via HP's manned monitoring centres. In the event of an alarm, HP's monitoring centre escalate to the necessary support personnel.

Qvalent monitoring also extends to advising customers if they have not submitted expected data during a predefined window or if there was an issue with the data submitted via their remote systems.

Q) Detail any penetration tests that your systems or applications have gone through. List the most current along with the results of these tests.

A) As part of Qvalent's PCI-DSS level 1 compliance requirements penetration tests are carried out against Qvalent systems every 3 months. This includes both external and internal tests. Penetration tests results are graded from 1 (informational) to 5 (critical). Qvalent systems only record a 1 (informational which is considered secure).

Q) Provide details of your capacity planning processes?

A) Capacity reports are generated on a daily basis. These reports then feed into a monthly capacity report. Each month there is a formal capacity review process that studies current utilisation, expected growth and recommends any additional capacity increase requirements.

11 Glossary

CA-XCOM
CA-XCOM is a cross-platform, value-added data transport solution, providing high-performance unattended file transfer with complete audit trails and reporting. CA-XCOM provides a single solution for sending and receiving files, as well as sending reports and jobs, to a wide range of platforms. This is Qvalent's standard file transfer mechanism.

Certificate
An electronic document that identifies an entity (e.g. a person, computer or company). Each certificate contains the entity's public key, along with details about which encryption algorithms the entity can use. Certificates are issued by Certificate Authorities (CAs) when the CA verifies the entity requesting the certificate.

Each certificate contains a subject, describing who the certificate is for, and an issuer, describing the organisation that signed the certificate.

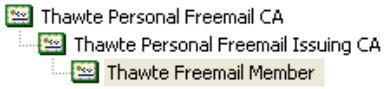
The certificate contains the entity's public key, as well as the digital signature of the CA. This signature is like a hologram on a credit card, verifying that the CA has authenticated the entity's identity.

Certificates can be marked for various purposes, including SSL client, SSL server and CA. See also *Certificate Authority*, *Digital Signature*, *SSL* and *Public Key Encryption*.

Certificate Authority
A trusted third party that signs certificates for other parties. Often in internet communications, the two parties will not trust each other, but will trust a third party. Party A can trust party B's certificate if it is signed by that third party (the certificate authority or CA).

Certain CAs (e.g. Verisign, Thawte) are automatically trusted by all certificate software. See also *Certificate* and *Certificate Hierarchy*.

Certificate Hierarchy
The chain of certificates for an entity consisting of that entity's certificate and any CAs which signed the certificate. All certificates are signed by another certificate, generating a hierarchy. This hierarchy terminates at a root certificate, which is **self-signed**. This type of certificate contains an identical issuer and subject.



A certificate is trusted by a party if the certificate chain terminates at a CA which is trusted by that party. Each party maintains a list of trusted root CAs. See also *Certificate*, *Certificate Authority and Self-signing*.

Digital Signature
A process of signing a message electronically. Normally, the sender of a message will calculate a message digest,

then encrypt that digest value with the sender's private key. This resulting value is the digital signature.

The receiver can verify the signature by calculating the message digest, and comparing it to the value obtained by decrypting the digital signature with the sender's public key. See also *Message Digest* and *Public Key Encryption*.

Encryption/Decryption
The process of scrambling a message so that it cannot be read by a third party while in transit. The sender encrypts a message before sending, and the receiver decrypts the received message before reading it.

Many algorithms are available to encrypt data. Examples include RSA, RC4 and DES. The algorithm is generally well-known, but a number (called a **key**) must be used with the algorithm to produce an encrypted result or to decrypt previously encrypted information. Decryption with the correct key is simple, whereas without the key, decryption is almost impossible.

HTTP
Hypertext Transfer Protocol: The application level protocol that is used to transfer data on the web. A client sends a request message to the server, and the server sends a response message.

Each message consists of a start line (which is either a request line or a status line as appropriate), followed by a set of message headers and finally an optional message body.

The request line contains the method (usually GET or POST) used for the request. GET is a simple request for information, whereas POST allows the client to send data to the server in the request.

A web browser generally sends a GET request to the server for information, and the server responds with a HTML document in the response for the browser to display.

The HTTP protocol uses the TCP/IP protocol to transport the information between client and server. HTTP uses TCP port 80 by default. See also *TCP/IP*.

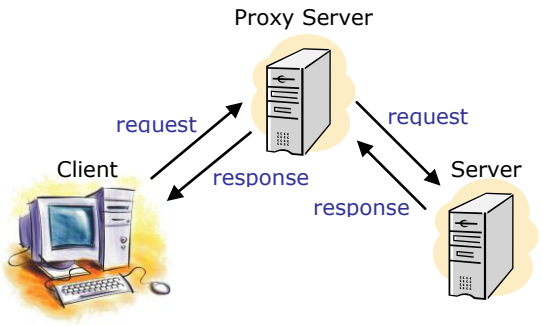
HTTPS
Hypertext Transfer Protocol, Secure: The HTTP protocol using the Secure Sockets Layer (SSL), providing encryption and non-repudiation. HTTPS uses TCP port 443 by default. See also *HTTP* and *SSL*.

Message Digest
A mathematical function which generates a number from a message (also called a one-way hash). The generated number is unique for the message, in that changing any part of the message changes the resulting number. The function is one-way in that it is, for all practical purposes, impossible to determine the message from the number. Common algorithms are MD5 and SHA-1.

Non-repudiation
Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Proxy Server
An intermediate server on the client side of a HTTP transaction which makes requests on behalf of the client. Proxy servers improve corporate security by only exposing the proxy server to the internet, rather than each individual computer in the organisation.

The client sends its request to the proxy server, which then sends the request (with any modifications) to the server. The server responds to the proxy, which then passes the response to the client.



System administrators can restrict which servers are accessible simply by configuring the proxy server. See also *HTTP*.

Public Key Encryption
An encryption method where different keys are used for encryption and decryption. Each party has two keys – a public key and a private key. Messages encrypted with the public key can only be decrypted with the private key, and messages encrypted with the private key can only be decrypted by with the public key. Each party publishes their public key and keeps their private key secret.

Encryption is accomplished by the sender encrypting the message with the receiver's public key. The message can then only be decrypted by the receiver with his private key.

Non-repudiation is accomplished by the sender encrypting the message with her private key. The message can then be decrypted by anyone with the sender's public key (which is published), but the receiver can be assured of the message's origin. See also *Symmetric Key Encryption* and *Encryption*.

Self-Signing
Self-signing occurs when the owner of a key uses his private key to sign his public key. Self-signing a key establishes some authenticity for the key, at least for the user IDs. The user ID of the signature must match the user ID of the key. (Where there are multiple user IDs, the ID of the signature must match the primary ID of the key.) Also, the key ID of the signature matches the key ID of the key. This verifies that whoever placed a user ID on a public key also possesses the private key and passphrase. Of course, this does not verify that the owner of the key is really who she says she is. That is done by the signatures of others on the public key (such as a root CA like Verisign).

SOAP
Simple Object Access Protocol: An XML-based protocol allowing remote procedure calls and asynchronous messaging. SOAP generally uses HTTP to transport the messages between computers. SOAP is becoming popular because of its use of

standard internet protocols as its basis. See *XML* and *HTTP*.

SSL
Secure Sockets Layer: A protocol designed by Netscape to encrypt data, authenticate the client and server and ensure message integrity. SSL sits between the application layer protocol (e.g. HTTP) and above the TCP/IP network protocol.

The SSL handshake establishes the SSL connection, setting up the secure channel. In this process, the server presents its certificate to the client for authentication:

- The server encrypts some data with its private key and the client then checks this signature with the public key from the server's certificate.
- The client checks that the server DNS name is the same as that in the certificate.
- The client checks that the server certificate has not expired.
- The client checks that the server's certificate is signed by a trusted CA.

The server can also optionally require the client to present its certificate to the server for authentication.

The handshake also allows the client and server to agree on an encryption algorithm (a symmetric key algorithm for speed), and securely exchange the session key. This session key is used in the encryption algorithm which encrypts the data exchanged between the client and server after the handshake is finished. The session key length can be 40-bit, 56-bit or 128-bit, with the longer keys being more difficult to break. See also *TCP/IP*.

Symmetric Key Encryption
An encryption method where the sender and receiver use the same key to encrypt and decrypt the message. This method relies on the key being kept secret between the two parties. If the key is discovered, anyone can read the messages in transit, or send false messages to the receiver.

This type of encryption is often used for bulk encryption because it is much faster than public key encryption. See also *Encryption* and *Public Key Encryption*.

TCP/IP
Transmission Control Protocol over Internet Protocol. IP allows packets of data to be sent across the internet from one computer to another. TCP provides a reliable communication stream between the two computers, using the Internet Protocol.

XML
eXtensible Markup Language: A document formatting language which describes a standard syntax, but allowing many different document types. Business partners can then agree on the specific documents they will exchange, using the standard syntax. XML documents contain a hierarchical list of tags, some of which contain values.