



# QuipaLoop Whitepaper

SIMPLE. SECURE. AGILE.

---

**AUSTRALIA**

p. +61 (0) 2 9290 1820  
sales@quipa.com.au

**UNITED KINGDOM**

p. +44 (0) 207 290 3958  
sales@quipa.co.uk

**NEW ZEALAND**

p. +64 (0) 9 914 3100  
sales@quipa.co.nz

**IF YOU REQUIRE SUPPORT**

with QuipaLoop contact your nearest region or  
visit [www.quipa.net](http://www.quipa.net) for more information.

# > Quipa Quipaloop

SIMPLE. SECURE. AGILE.

## TABLE OF CONTENTS

Introduction	3
System Overview	4
Session Establishment	5
Security Features	7
Supported Protocols	8
Firewall Settings	9
Key Technology Features	10
Appendix 1: Glossary	11

## Introduction

### PURPOSE

This QuipaLoop Whitepaper document is a technical overview for the QuipaLoop product. The intended audience is Architects and other Technical Experts who wish to know more about QuipaLoop as part of an evaluation or training process.

This document is not intended as an Administration Manual, Installation Guide or a User Guide. These documents are also available through your Quipa Managed Service Provider or Quipa Sales Representative.

You may also wish to review the QuipaLoop Use Cases and FAQ at [www.quipa.net](http://www.quipa.net).

## Content Map

The QuipaLoop Whitepaper document is structured as shown in the table below:

System Overview	A description of the QuipaLoop system including the components and their roles.
Session Establishment	This section describes how the QuipaLoop session is established. This provides the foundation for understanding the QuipaLoop technology.
Security Features	QuipaLoop has been architected to be secure 'from the ground up'. This section describes some of the security features of QuipaLoop, in addition to encryption.
Supported Protocols	The list of the QuipaLoop lab-certified protocols. This list is constantly expanding and updates will be provided at <a href="http://www.quipa.net">www.quipa.net</a>
Firewall Settings	Information about the firewall rules required for QuipaLoop.
Key Technology Features & VPN Comparison	Some of the key features of QuipaLoop are listed along with the main points that differentiate QuipaLoop from some types of VPNs.
Glossary	Definitions for terms/words in this document that are unique to QuipaLoop.

# System Overview

## OVERVIEW

A user with Administration permissions and the QuipaLoop software installed creates a Quipa Secure Loop (loop ) for sharing services and other resources. When another user wishes to join the loop, they connect to the publicly accessible Secure Connection Broker (SCB) and request a connection to the loop by entering joining information. The loop receives the request and accepts the connection and invitation key. The joining device and the loop establish a connection and the new device is joined into the loop.

See Figure 1

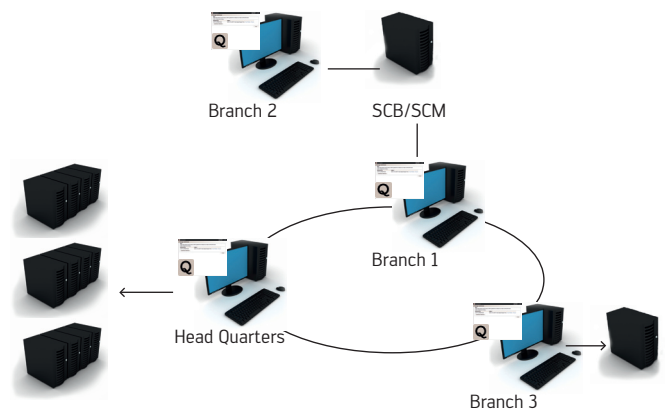


Figure 1

Any services or resources that are TCP/IP addressable by a device in a loop can be shared as services with other members of the loop. The QuipaLoop device can also act as a relay to make the services available on the local network. Services that have been shared into a loop can be accessed via a standard bookmark process or by launching directly from within QuipaLoop.

See Figure 2

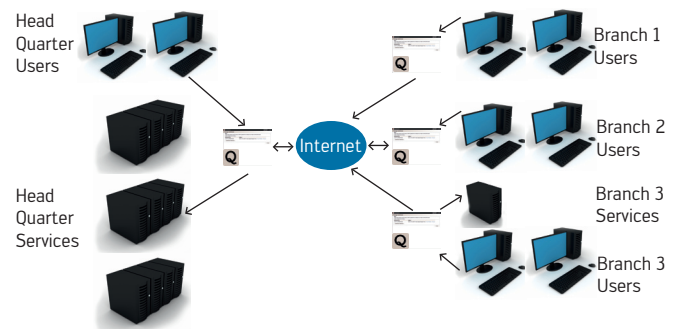


Figure 2

## COMPONENTS

Joining Device	A Joining Device is a device that has had the QuipaLoop application software installed on it and is utilising the functionality provided by the SCB to become a member of a Quipa Secure Loop.
Secure Connection Broker	The SCB is the only required publically addressable service in the QuipaLoop system. It supplies several functions. The first is a licence management point that controls the creation of users, end-point devices and QuipaLoops. The second role is an authentication point to authenticate a user on an end-point device. The third role is as a connection assistant to help facilitate connections between end-point devices. The SCB does not store an IP address registry, rather it utilises Quipa’s proprietary dynamic “waiting room” process.
QuipaLoop Device	The QuipaLoop device is a device that has had the QuipaLoop application software installed on it. The QuipaLoop software allows this device to utilise the functionality provided by the SCB to become a member of a Quipa Secure Loop. Depending on the configuration of the end-point device it can act as a client, a server, a peer or any combination thereof.
Quipa Secure Loop	The Quipa Secure Loop is a virtual construction that is created by establishing trust between a defined group of end-point devices. The Quipa Secure Loop is created via a Quipa proprietary invitation process initiated from the founding end-point device. It is used to define a perimeter into which services can be shared. It is possible to have multiple Quipa Secure Loops overlaid across a single device. Each Quipa Secure Loop maintains its own security and integrity.

## Session Establishment

The QuipaLoop session is established in four stages which result in a secure connection between an end-user and the shared service. The session is established with no requirement for download and installation of ActiveX controls or modifications to WinSock. There is no modification of proxy settings and no requirement for elevated (Administration) privileges to run QuipaLoop, although some services such as SMB may require these privileges.

The four stages of the QuipaLoop session establishment are:

Stage 1: Secure End-point to Secure Connection Broker Session.

Stage 2: End-point to End-point Session.

Stage 3: Virtual Layer Session.

Stage 4: Service Layer Session.

### STAGE 1: SECURE END-POINT TO SECURE CONNECTION BROKER SESSION

The first stage in the establishment of the QuipaLoop session involves establishing a secure session between the user on an end-point device and the Secure Connection Broker (SCB). The SCB is used to register and authenticate all devices in the client's QuipaLoop system, the devices being registered as a user/device combination.

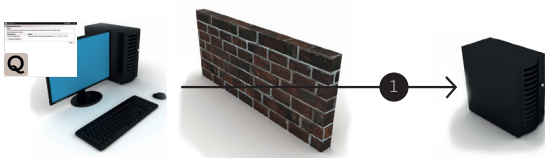


Figure 1: Secure connection establishment between end-point and SCB

1) End-point device securely connects to the SCB which authenticates the device/user combination.

A Public/Private key is used to establish the connection to the SCB and to exchange random session keys. Knowledge of the previous end-point active session is confirmed by the SCB. SCB transactions are also protected from replay attacks. Only registered user/end-point combinations are able to utilise the services provided by the SCB.

### STAGE 2: END-POINT TO END-POINT SESSION

The second stage of the QuipaLoop session involves establishing mutually authenticated connections between the end-point devices. The SCB is employed as a "waiting room" to help broker these connections. An end-point device wishing to connect to another end-point device enters the waiting room and when the target end-point device checks in, it is able to accept or reject the waiting end-point device. Both end-point devices independently verify each other.

This stage may involve an optional component, the Secure Connection Matrix (SCM). The SCM is used to help form connections in difficult conditions (firewalled devices) and is slaved by the SCB. The SCM is a transparent relay point that has no understanding or access to client data.

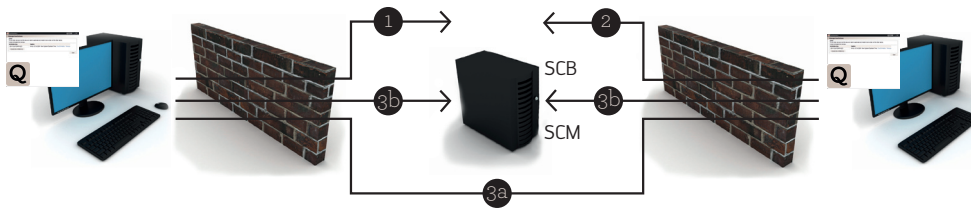


Figure 2: Mutually authenticated connections between end-points

- 1) End-point device enters the waiting room on the SCB.
- 2) Target device checks and accepts the end-point device in the waiting room.
- 3a) The two devices establish a direct connection and mutually authenticate each other. NAT Traversal technology is built into the QuipaLoop software.
- 3b) If required, the two devices establish outbound connections to the SCM and mutually authenticate each other.

### STAGE 3: VIRTUAL LAYER SESSION

The third Stage of the QuipaLoop session involves establishing a service sharing layer – this is called a Quipa Secure Loop. This service sharing layer is overlaid above the physical connections formed by the second Stage. Each sharing layer has its own cryptographic material and multiple of these sharing layers can be overlapped on the same physical devices, but remain completely isolated. These layers are created over two or more devices.

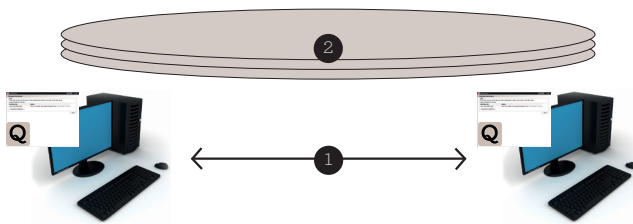


Figure 3: Quipa Secure Loop establishment

- 1) Secure mutually authenticated connection has been established.
- 2) Secure virtual layers (Quipa Secure Loop) are created over the physical connection.

### STAGE 4: SERVICE LAYER SESSION

The fourth Stage involves establishing the connection to the shared service and utilises the Quipa Secure Loop established by the third Stage. The QuipaLoop client application connects to a TCP/IP port listening on the remote device and the QuipaLoop system securely establishes a connection from the sharing device to the shared service. Application data is then securely transmitted over the relayed connection.

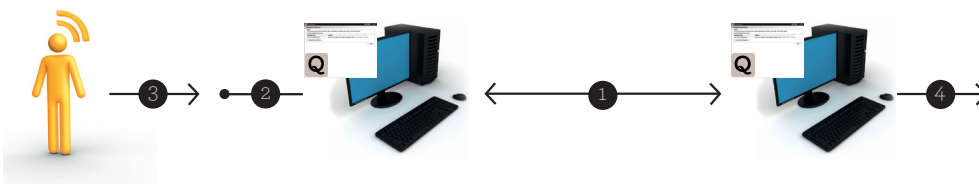


Figure 4: Connection to the shared service

- 1) Quipa Secure Loop is established.
- 2) Local Socket Listener added to end point device to accept connection. The Local Socket Listener is filtered to local connections only.
- 3) User connects to Local Socket Listener with client application (e.g. Windows IE).
- 4) Connection is relayed through the Quipa Secure Loop to the shared service.

## Security Features

Understanding that security vulnerabilities occur at several different levels (physical, software and social) Quipa designs its products to be secure from the ground up. QuipaLoop products have the security mechanisms described below.

### WAITING ROOM

When a user logs into QuipaLoop they only get access to a 'waiting room'. They do not get access to any Quipa Secure Loop services until they are invited into the Quipa Secure Loop and authenticated by a device that is already in the Quipa Secure Loop.

### DEVICE-BASED SECURITY

For many VPN solutions all that is required to access the network is a username, password and a copy of the client software. With QuipaLoop, even if a hacker gained access to the username and password and had a copy of the software, they would not gain access to the network services; instead they would go into the 'waiting room'. A new device must be invited into the Quipa Secure Loop before it will gain access to the services.

This also has advantages at an administration level. The administrator is able to see exactly which devices are part of a Quipa Secure Loop and which devices are online and offline. The administrator has the ability to manage not only users but also devices. They can suspend or remove devices and if a device is lost or stolen they can mark the device as stolen which will clear the QuipaLoop configuration data on the stolen device.

Further, each user has device limits. This means that even if a hacker obtained a valid invite to a Quipa Secure Loop, the hacker's device would not be able to log in if the device limit would be exceeded. A Quipa Secure Loop that has no outstanding invitations and all devices online will not accept any new connections from the SCB and is effectively its own distributed security bubble.

### COMPARTMENTALISED SECURITY MODEL

QuipaLoop security is compartmentalised, which means that if there is a breach in one part of the QuipaLoop system this does not flow over to the other parts of the system. A breach in one QuipaLoop component will not automatically give access to other components.

### REPLAY PROTECTION

All transmitted QuipaLoop system data is protected from replay attacks. This includes device-to-device transactions and also transactions with the SCB.

### SHORT SESSION ENCRYPTION KEY DURATION

Session encryption keys used for device-to-device transactions are changed at regular and random time intervals.

### MUTUAL DEVICE AUTHENTICATION

All devices mutually authenticate each other. They confirm the identity of the other device, but also confirm that the remote device has awareness of itself. Devices entering a loop are independently mutually authenticated by up to two devices already in the loop.

### TAMPER DETECTION

This includes detecting invalid activity such as copying QuipaLoop executables and information. The device will be suspended immediately and the QuipaLoop data will be cleared from the device.

### FIREWALL COMPLIANCE

QuipaLoop device connections can always be outbound which means no port forwarding or inbound ports need to be allowed on a firewall that is protecting the end services. QuipaLoop has been designed to work with corporate network policies so that its usage can be controlled by the corporate administrators. QuipaLoop will not do anything to subvert the policies that were put in place by the corporate administrators, so QuipaLoop will not fail over to different ports such as port 80.

### ENCRYPTION IN TRANSIT

Data always remains encrypted in transit between the QuipaLoop devices; it is never decrypted by a gateway device.

## KEY LOGGER PROTECTION

As described under the 'device-based security' point, even if a hacker has the username and password they will only get access to the 'waiting room'. Furthermore, QuipaLoop integrates well with existing Key Logger-protection software such as virtual keyboards and identity management tools.

## DENIAL OF SERVICE PROTECTION

Quipa Secure Loops once established are capable of running independently of the SCB. This means any down-time

of the SCB will not bring the whole system down and most clients will be unaware of this event.

## ENCRYPTION

QuipaLoop uses the Crypto++ Encryption Library as the underlying encryption library for QuipaLoop. The Crypto++ library has FIPS 140-2 certified DLLs that can be employed by the QuipaLoop system. Other libraries can be used to replace crypto++ if needed. QuipaLoop uses SHA512, RSA 1024 and AES256 encryption algorithms in the QuipaLoop standard product.

# Supported Protocols

QuipaLoop has an extensible service sharing architecture. At this point TCP/IP protocol handlers such as Web and FTP are implemented and our Roadmap includes extending this to the UDP protocol.

## CURRENTLY SUPPORTED PROTOCOLS

- > Remote Desktop Protocol – Terminal Server, VNC, Remote Desktop, PCAnywhere
- > HTTP, HTTP/s
- > SVN
- > FTP SFTP FTPS – both Active FTP and Passive FTP
- > Telnet
- > POP3, SMTP
- > Jabber XMPP
- > NI (SAP Protocol)
- > Sharepoint
- > SMB (Driver required)
- > MPEG4, MJPEG Video Stream
- > IMAP
- > Exchange
- > SSH
- > Lotus Notes
- > Database - Oracle

## SUPPORT FOR NEW PROTOCOLS

Quipa will test and add to the supported protocols list over time.

For a full list go to [www.quipa.net](http://www.quipa.net).

## Firewall Settings

QuipaLoop connections can be outbound only and, there is no requirement for inbound connections to the devices so administrators do not need to be concerned with opening inbound ports or port forwarding. In the case that outbound ports normally used by QuipaLoop are blocked, the administrator will need to configure the firewall to allow these ports.

QuipaLoop has been designed to work with corporate network policies so that its usage can be controlled by the corporate administrators. QuipaLoop will not do anything to subvert the policies that were put in place by the corporate administrators, for example QuipaLoop will not fail over to different ports such as port 80.

There are two ways to configure the firewall for QuipaLoop; for best performance or for most restrictive settings. The difference between the two is that when the firewall is configured for best performance, the QuipaLoop devices will attempt to connect directly to each other. If the devices are able to connect directly, the performance will be improved compared to connecting to the SCM. For this reason, setting the firewall for best performance is suggested.

Before setting up the rules, please request the IP address, SCB port and SCM port from the Administrator hosting the SCB and SCM host Service.

### FIREWALL SETTINGS FOR BEST PERFORMANCE

QuipaLoop devices will try to connect directly and only if that fails, will they try to connect via the SCM. For direct connections, QuipaLoop uses a range of outbound ports from port 57001 to port 57401. Three rules will need to be added to the firewall:

Allow traffic to the SCB on the SCB port.

Allow traffic to the SCM on the SCM port.

Allow traffic to the other QuipaLoop devices on the device port range (57001 to 57401).

Example firewall rules are shown below where the IP address of the device running QuipaLoop is 192.168.0.28, the IP address of the SCB and SCM is 254.168.243.165, the SCB port is 8080 and the SCM port is 8443:

Name = SCB Rule and SCM rule

Action = Accept

Protocol = TCP and UDP (Note both TCP and UDP must be allowed for connection to SCB)

Source host = 192.168.0.28

Source ports = All ports

Destination host = 254.168.243.165

Destination ports = 8080, 8443

Name = Device Rule

Action = Accept

Protocol = TCP

Source host = 192.168.0.28

Source ports = All ports

Destination host = all

Destination ports = 57001 to 57401

### MOST RESTRICTED FIREWALL SETTINGS

For restricted outbound port settings, only allow outbound traffic from the device running QuipaLoop to the IP address of the site hosting the SCB and SCM for the SCB and SCM ports.

An example rule where the IP Address of the device running QuipaLoop is 192.168.0.28, the IP address of the SCB and SCM is 254.168.243.165, the SCB port is 8080 and the SCM port is 8443 is:

Name = SCB and SCM Rule

Action = Accept

Protocol = TCP and UDP (Note both TCP and UDP must be allowed for connection to SCB)

Source host = 192.168.0.28

Source ports = All ports

Destination host = 254.168.243.165

Destination ports = 8080, 8443

## Key Technology Features

### SIMPLICITY

- › NAT traversal technology
- › Maintains separation of subnets
- › No reliance on support of protocols such as IPSEC by the underlying network
- › No inbound firewall rules required
- › No specialist hardware or gateway device required
- › Access to services is independent of the underlying network
- › No requirement for QuipaLoop on end devices
- › Simple and easy to set up

### AGILITY

- › Multi-way sharing of services
- › No dependencies on fixed IP addresses for site networks
- › Service delivery from multiple points
- › No reliance on support protocols e.g. IPSEC by the underlying network infrastructure
- › Flexible network configuration
- › No third party access to service data
- › Easy suspension of lost or stolen devices

### SECURITY

- › Easy suspension of lost or stolen devices
- › No open inbound ports or port forwarding on HQ LAN
- › No third party access to service data
- › Internal secured server can be completely firewalled from internal company network
- › Node locked to the physical USB device or credential locked to specific user
- › Industry standard encryption of all data

### COMPARISON TO VPN

- › QuipaLoop complies with corporate firewall rules with no circumvention of policy by utilising other protocol ports
- › It does not maintain a central list of IP addresses for Service nodes
- › QuipaLoop does away with IP conflicts, which enables greater business collaboration and reduces TCO
- › It operates independently of the underlying subnet and easily aggregates services from multiple LANs or sub-nets
- › All service aggregations are individually secured, minimising the impact of any breaches (compartmentalised security)
- › QuipaLoop operates at the applications level for all types of services and does not drop down to the network level for non-Web services
- › QuipaLoop is simple to administer, use and support. A complex network can be set-up and torn down within minutes
- › QuipaLoop provides access to specific, authorised services and never to the underlying network, therefore is it more controlled and secure
- › QuipaLoop allows two-way sharing by default, enhancing flexibility for users without sacrificing security and control
- › QuipaLoop provides access to services over the Internet without exposure to the Web, which reduces the risk of Web based exploits
- › There is no requirement to download an ActiveX plug-in and also no modification required to the WinSock layer
- › No VPN concentrator is required
- › QuipaLoop connects trusted devices only, providing greater security

## Appendix 1: QuipaLoop Glossary

In this document we have used some terminology that is specific to QuipaLoop.

### SECURE CONNECTION BROKER (SCB)

The SCB is the only required publically addressable service in the QuipaLoop system. It supplies several functions. The first is a licence management point that controls the creation of users, end-point devices and QuipaLoops. The second role is an authentication point to authenticate a user on an end-point device. The third role is as a connection assistant to help facilitate connections between end-point devices. The SCB does not store an IP address registry, rather it utilises Quipa's proprietary dynamic "waiting room" process.

### SECURE CONNECTION MATRIX (SCM)

The SCM is an optional publically addressable service. It is utilised by an SCB to help facilitate connections. The SCM is a secure transparent relay point that allows end-point devices behind strict firewalls to connect. It does this without requiring knowledge of the end-point devices. There are two modes of operation. The first uses a single static port for the end-point devices to connect to. This makes firewall configuration easier. The second mode uses dynamically allocated port pairs that are opened and then closed immediately on connection. This leaves no open ports when connections are not being formed and adds additional security.

### QUIPALOOP

QuipaLoop is the Quipa Product name.

### JOINING DEVICE

A joining Device is a device that has had the QuipaLoop application software installed on it and is utilizing the functionality provided by the SCB to become a member of a Quipa Secure Loop.

### QUIPA SECURE LOOP

The Quipa Secure Loop is a virtual construction that is creating by establishing trust between a defined group of end-point devices. The Quipa Secure Loop is created via a Quipa proprietary invitation process initiated from the founding end-point device. It is used to define a perimeter into which services can be shared. It is possible to have multiple Quipa Secure Loop overlaid across a single device. Each Quipa Secure Loop maintains its own security and integrity.

### QUIPALOOP DEVICE

The QuipaLoop device is a device that has had the QuipaLoop application software installed on it. The QuipaLoop software allows this device to utilise the functionality provided by the SCB to become a member of a Secure QuipaLoop. Depending on the configuration of the end-point device it can act as a client, a server, or a peer or any combination thereof.

#### AUSTRALIA

p. +61 (0) 2 9290 1820  
sales@quipa.com.au

#### UNITED KINGDOM

p. +44 (0) 207 290 3958  
sales@quipa.co.uk

#### NEW ZEALAND

p. +64 (0) 9 914 3100  
sales@quipa.co.nz

TO ARRANGE FOR AN IN-PERSON DEMO  
of QuipaLoop contact your nearest region  
or visit [www.quipa.net](http://www.quipa.net) for more information.