technologywithin®

Chevron Business Park,
Limekiln Lane,
Holbury,
Southampton,
SO45 2QL

twiindata

IT Security, Disaster Recovery and Storage of Data

Introduction

twiindata by technologywithin is an advanced network infrastructure controller including firewall, IP router, switch management and bandwidth control tool designed and supported in-house to give controllable levels of internet access to multiple clients in a building whilst securely segregating their data from one other.

Advanced features of the tool include allocation of public addresses and port forwarding, bandwidth control, monitoring and reporting of both historical and live traffic.

twiindata can also optionally be used to control wireless services at varying service levels and VOIP telephony.

The main features of **twiin**data can be configured from a simple user interface making the product ideally suited for a business centre environment where multiple tenants can share an internet connection whilst retaining security of their data. The advanced features of the system are valued by the more technological tenants, and the user interface enables the onsite centre management staff to easily set up the system for occupier needs.

Occupiers are free to bring their own equipment to make their own individual networks, which can include provision of their own firewalls to take the place of the standard **twiin**data firewall, and the customer can then obtain appropriate security certification for their own equipment.

Technical description and security principles

A **twiin**data managed network installation consists of one or more physical **twiin**data firewall/router devices, a number of managed network switches, a license for the **twiin**data central cloud server platform and optionally wireless access points.

Chevron Business Park,
Limekiln Lane,
Holbury,
Southampton,
SO45 2QL

The firewall/router device will be a Mikrotik Routerboard device, the specific model will vary depending on the speed of the line and other factors but is likely to be one of the following:

CCR1072, CCR1036, CCR0016, CCR1009, RB2011
Further information: https://mikrotik.com/products/group/ethernet-routers

The device runs the RouterOS operating system L5 or L6. Firmware updates are applied automatically to ensure the manufacturer's latest stable firmware release is present on the device. Our engineers also regularly review the release notes and are pro-actively notified of any vulnerabilities published by Mikrotik.

Managed switches vary across sites. If supplied by technologywithin, these will typically be from the Cisco portfolio but **twiin**data is compatible with many other manufacturer ranges including Netgear Allied Telesis, HP, Aruba, TP-Link, Ubiquity and Extreme. We can integrate further equipment providing it satisfies some basic requirements.

All **twiin**data compatible switches are capable of isolating client networks using VLANs which are used by the **twiin**data to segregate clients.

The **twiin**data cloud server is a central installation managed and supplied by technologywithin. It provides the single website for customers to manage all their site deployments, view usage and update the settings deployed on across all sites.

twiindata managed wireless installations typically use Ubiquiti Unifi branded equipment (but could also be another manufacturer, for example Cisco, Aruba or Ruckus). The more basic non-managed wireless delivery could employ any brand of off-the-shelf access point. Where the WiFi controllers/APs support VLAN isolation on client setting, this is used to support client network isolation features.

Firewalling and client segregation

The **twiin**data enterprise grade firewall by default blocks all traffic originating from the internet unless a rule has been specifically created as an exception, which can be done for any public IP

Chevron Business Park,
Limekiln Lane,
Holbury,
Southampton,
SO45 2QL

address allocated to a client to allow clients to access their office networks externally. Firewall rules can be locked to source IP addresses for increased security.

The **twiin**data firewall can be disabled on a per-VLAN basis, allowing individual clients to maintain their own public facing IP connection and configure their own firewall/routing equipment. In this "passthru" configuration, the **twiin**data only adjusts the traffic for bandwidth control purposes and the responsibility of inbound and outbound firewalling lies with the end users. Because this setting is applied on a per-VLAN basis, the impact is on the individual clients only.

twiindata uses managed switches use VLAN technology to secure data internally, i.e., between clients. Each client is connected to their own group of ports on the managed switch stack. The switches are configured by default to deny any exchange of data between VLANs (other than the external gateway) which prevents any transfer of traffic between clients. This is the industry standard for network isolation and provides a highly secure method of segregating individual clients and protecting internal data from other tenants.

meshdata central portal

The configuration interface for **twiin**data is available via a secure web page and access is secured with a username and password. Login as standard is restricted to source IP address, however for users seeking to relax this restriction and log on from remote locations, 2 factor authentication is forced. The **twiin**data interface has a number of access levels, intended for differing levels of end user access, which are secured by separate usernames and passwords.

Backup and disaster recovery

Local site

A number of resiliency options are available to ensure services can remain functioning, including provision of redundant hardware for either attended or unattended continuity of service. Further redundancy can be built into the network design. All customers are provided with an SLA to support their architecture.

Registered Office: CP House, Otterspool Way, Watford, WD25 8JJ, U.K
Registered in England No: 5964349 | VAT Number: GB 902 5369 37

technologywithin®

Chevron Business Park,
Limekiln Lane,
Holbury,
Southampton,
SO45 2QL

Central database

The **twiin**data configuration database is mirrored across multiple cloud servers using resilient hosting providers but is also backed up over encrypted channels daily. The **twiin**data central cloud is highly robust, however should there be a system failure at cloud level, the operational ability of the individual sites is not affected, only the administration of the system (i.e., it would not be possible to make changes), so a cloud outage does not represent a critical outage of end user connectivity.

Monitoring of external lines

The **twiin**data central monitoring system will automatically monitor the status of all external connections every second. Alerts can be generated to appropriate nominated contacts in the event of line outages and the **twiin**data can be configured to use alternative external connectivity in the event of failure of primary lines. Public IP addresses may not be preserved depending on the configuration.

Bandwidth control and traffic routing

twiindata includes advanced algorithms to shape bandwidth according to pre-defined groups containing multiple customers. Bandwidth rules can allocate dedicated or shared slices of the external interfaces and it is possible to oversubscribe the external bandwidth to achieve maximum efficiency.

It is also possible to create custom rules to divert specific packets, for example hosted VOIP traffic can be syphoned to a dedicated and prioritised bandwidth group to achieve appropriate quality on the voice calls.

Traffic usage logging

twiindata stores traffic usage by VLAN by recording data over 5-minute average intervals. Appropriate extrapolation is performed on this data to provide up to three years of historical bandwidth usage data.

Real-time traffic statistical data is generated every second and presented as graphical display. The equivalent metadata may be logged depending on the site's deployment.

technologywithin®

Chevron Business Park,
Limekiln Lane,
Holbury,
Southampton,
SO45 2QL

Physical security

Physical Security of the **twiin**data hardware varies according to each individual site. The expectation is that all comms cabinets will be locked or preferably situated within a dedicated comms room facility with access controlled and monitored by the site management.

Capture of data

twiindata includes the ability to capture meta-data logs of internet access which may include the time, date, IP destination, port and associated internal VLAN ID, MAC address and IP address of the connecting device. This information may be kept securely in accordance with any legal requirement to do so for an appropriate length of time to comply with legislation.

If this service is enabled, **twiin**data automatically logs all blocked connection attempts to the system, and all initial packets for any incoming connection via a public IP address and every outgoing connection to a remote site. These logs are securely stored offline on the **twiin**data central infrastructure. **twiin**data includes the facility to enable advanced logging on request of more specific activities should this be thought necessary.

Storage of personal data

twiindata does not include any ability to capture financial data (credit card numbers, etc). The **twiin**data managed WiFi platform holds e-mail addresses and names of users together device MAC addresses and other circumstantial information, for example time and data of login. Removal of this data can be requested via the centre management staff but this may result in suspension of the wireless service and users would need to sign-up once again to regain access, at which point equivalent data associated with the sign-up will again be held. The username and password for user access logins is also be considered personal data.

Third party security testing

technologywithin engage with a third party to perform security penetration testing on a regular basis and the results of this are carefully reviewed by our in-house engineers. If any vulnerabilities are found, the in-house team will close off these issues and then the application will be re-tested by the third party.

technologywithin®

Chevron Business Park,
Limekiln Lane,
Holbury,
Southampton,
SO45 2QL

Third party equipment

As explained in this document, a network managed by **twiin**data is dependent on third party equipment and this enables customers to exercise choice over their equipment and network design. Because of this, the security of the whole system is also dependant on the inherent security of the third-party equipment (which applied to the Mikrotik router), and correct configuration by the users.