BLAZE NETWORKS

CASE STUDY

Routes Healthcare

routes

SD-WAN, an End-End Security Fabric, and the Blaze Private Core Network deliver a secure, reliable and agile network for branches and central services.

We build the network.
You build the business.

blazenetworks.co.uk

SECURE
MANAGED
AGILE

CHALLENGE

Routes Healthcare offers complex care packages for people with long-term health conditions and end of life care in the north of England. The organisation provides a fully integrated offering of health and social care to people in their own homes and communities, 365 days a year through a team of over 1,000 care workers and 120 operational and management staff leveraging 18 service centres and a large recruitment and training hub.

Because of the nature of the services which Routes' carers provide, considerable importance is placed on both the confidentiality of customer information and on the ability to recruit, train and coordinate staff to deliver dependable, high quality customer service (leveraging a new central services and training hub in Rochdale).

Already a Blaze customer, the company needed to update its IT infrastructure to better enable change and growth in the organisation, and to support the increased use of SaaS platforms and cloud services.

Routes' existing MPLS wide area network was designed to connect on-premise services out to the branches and was being outpaced by modern requirements. Also, older remote access connectivity methods using IPsec lacked the broader security controls to match modern threats. A more solid foundation was needed to support the digital evolution of the business, particularly related to digital enablement of cloud services and full use of Microsoft 365 capabilities to deliver best practice, improved data and operational efficiencies.

Key outcomes needed were improved collaboration abilities across the organisation, more comprehensive cybersecurity, the ability to support increased use of cloud-based services, and reliable, resilient and secure connectivity for all sites..

SOLUTION

Blaze proposed a fully-managed private network based on Fortinet's SD-WAN technology and Security Fabric platform. A fully integrated technology stack has been provided, covering firewalls, switches, and wireless infrastructure across all Routes Healthcare sites. Professional project management by Blaze ensured a smooth deployment across all locations.

All Routes offices are directly connected back to Blaze Networks' secure Private Core Network, with limited traffic going over the public internet. The SD-WAN design supports better branch firewall protection and integrated switch and wireless infrastructure, to create a faster, intent-based network where changes can be made quickly and easily.

Use of SD-WAN's intent-based capabilities allows all traffic on the network to be monitored and automatically assigned to the most appropriate network segments, as defined by rules programmed into the network.

Each site has a FortiGate firewall, sized appropriately to the location and available connectivity, while a direct connection and the use of SD-WAN enables the centralisation of Unified Threat Management (UTM), Blaze Security Analyzer, and Endpoint Management Services (EMS), all orchestrated through Network Access Control (using FortiNAC). Running these services on the Blaze Private Core Network both saves expense and provides enhanced security by reducing Routes' cyber-attack surface on the public internet.

Secure connection of remote branches is supported into the Blaze Private Core Network infrastructure through use of Fortinet's ZTNA (Zero Trust Network Access) solution that is incorporated in the Fortinet endpoint management services technology (FortiClient EMS).

The Fortinet EMS security management solution enables scalable and centralized management of multiple endpoints. FortiClient EMS is designed to maximize operational efficiency whilst providing better visibility of what business assets are connecting into the network remotely.

We build the network.
You build the business.

As well as providing remote user connectivity, EMS was also configured to provide remote web filtering so devices are protected when outside of the secure network and computer telemetry that further strengthens the Fortinet security fabric capability by sharing device information with the rest of the integrated security infrastructure.

Two factor authentication (as required from most security related frameworks like ISO 27001, Cyber Essential Plus and the PCI-DSS framework) is provided, as well as additional capabilities as detailed above.

NHS security requirements as detailed in the NHS data security and protection toolkit DSTP are also supported. This NHS toolkit also helps organisations like Routes Healthcare achieve the NHS standards around cyber security. All elements of these NHS compliancy requirements at a network level were met as part of Blaze Networks implementation with heavy use of the Fortinet Security Fabric and network access control NAC solution being utilised. NHS requirements for the network infrastructure itself were also met.

Enhanced security technologies protect the Routes infrastructure and branch locations, including:

- UTP (unified threat protection)
- Antivirus
- BOT Net detection
- IPS (Intrusion Prevention Services)
- Application Control
- Network Automation

Content Filtering integrated with Active Directory provides user level identification and co-management access is provided through Blaze Networks' TACAS platform and change control systems.

FortiAnalyzer is a powerful log management, analytics, and reporting platform that provides organizations with a single console to manage, automate, orchestrate, and respond, thereby enabling simplified security operations, proactive identification and remediation of risks, and the complete visibility of the entire attack landscape.

Blaze adds further to FortiAnalyzer in the Blaze Security Analyzer solution. This enhances customer value by supplementing FortiAnalyzer with add-on services which would normally be chargeable through standard Fortinet licensing methods, but which are provided without extra charge as part of Blaze Networks' Security Analyzer solution. These add-ons include Indicators of Compromise (IOC) and Security Operations Centre (SOC) and these services are used to provide a greater level of value and protection to Routes.

All Fortinet equipment in Routes' SD-WAN sends logs back to the Security Analyzer which then provides comprehensive reporting and security operation functions. Blaze has tailored this to Route's reporting requirements and provided training to the IT team on reporting and security operational functions available within Security Analyzer.

AI (Artificial Intelligence) is used from FortiGuard to help combat virus outbreaks or ransomware using IOC (Indications of Compromise) licenses.

The network maintains a directory of all items and devices that are normally connected and other device types which can be allowed. This enables better protection of physical infrastructure involving accidental or malicious device connection to the network, including where shared or common area network cabinets are used in shared premises. Protection is provided from all newly attached devices (including non-secure Internet-of-Things / IoT devices) with network visibility, control, and with automated response.

Network automation built into Routes' SD-WAN enables the network to automatically identify known devices on connection, and to put them into the correct VLAN segment - thereby preventing any crossover or access into unauthorised business-use VLANs or Routes' wider SD-WAN. Leveraging Fortinet's FortiNAC, the system maintains a directory of all items of equipment and

devices that are normally connected to the network, as well as rules that identify other device types which can be allowed. Device types are assigned to Profiles that can be programmed within the SD-WAN to be treated differently (such as assignment to a specific VLAN segment), according to the profile definition.

Where a new, unexpected device attempts to connect, it is automatically locked out of Routes' network and put into a quarantine VLAN and an alert is sent into the Blaze Network Operations Centre.

Where the new device matches a permitted device type - for example a previously profiled corporate laptop, IP phone, building alarm system, or IoT devices like Wi-Fi enabled coffee machines – these are automatically put into their own VLAN segment according to the predefined profile rules, again preventing any crossover or access into business-use corporate VLANs or Routes' wider SD-WAN.

By detecting every device on the network, FortiNAC can see and profile everything, even headless devices. Once identified, FortiNAC can profile devices, thereby identifying what is on the network. FortiNAC configures switches, access points, and firewalls in the Routes network to restrict IoT devices to the minimal network access required to function. This protects key assets from IoT-based attacks. Furthermore, FortiNAC can take automated actions based on pre-set triggers to respond in seconds to identified risks.

RESULTS

The SD-WAN-based network design and combination of technology and Blaze services provide Routes with a secure, agile and future-proof network in a highly cost-effective manner.

Reliable and robust network connectivity is being provided, and Routes are better able to adapt rapidly to new digital requirements.

A more secure infrastructure has an enhanced level of cybersecurity and automation, able to keep pace with emerging threats and AI-driven attacks.

Provision of services to remote locations and mobile workers has been made much easier and a secure, capable, and resilient remote access infrastructure has been provided.

Cybersecurity has been enhanced by the network design and by the UTM system providing antivirus, content filtering, multi-factor authentication, and web filtering.

Overall, through an efficient and secure network design, combined with the enhanced level of service delivered by Blaze, Routes Healthcare has been able to improve the reliability and effectiveness of its wide area network whilst boosting cybersecurity and simplifying operations.

Dave Henegan, Head of IT, Routes Healthcare commented:

"Blaze has designed and implemented a successful migration from our previous MPLS network to a new SD-WAN infrastructure, improving security and enabling greater flexibility for our IT services across many remote locations and mobile workers. Blaze has proven highly responsive to our needs.

"Delivering a flexible and easy to adapt network, their entire team's responsiveness and customer-focus makes Blaze very easy to work with."

www.routeshealthcare.com

If you'd like to see how Blaze Networks could future proof your network needs, give us a call today.

0333 800 0101

BLAZE NETWORKS

www.blazenetworks.co.uk

STAY SCALEABLE
STAY SECURE

SECURE
MANAGED
AGILE

blazenetworks.co.uk
Call: 0333 800 0101 | Email: Info@blazenetworks.co.uk
@BlazeNetworksGB | Blaze-Networks-Ltd