MLL Telecom Ltd
Secure SD-Branch
Service Definition

Date: January 2026

MLL Ref: G Cloud 15 - RM1557.15

Secure SD-Branch - Service Definition

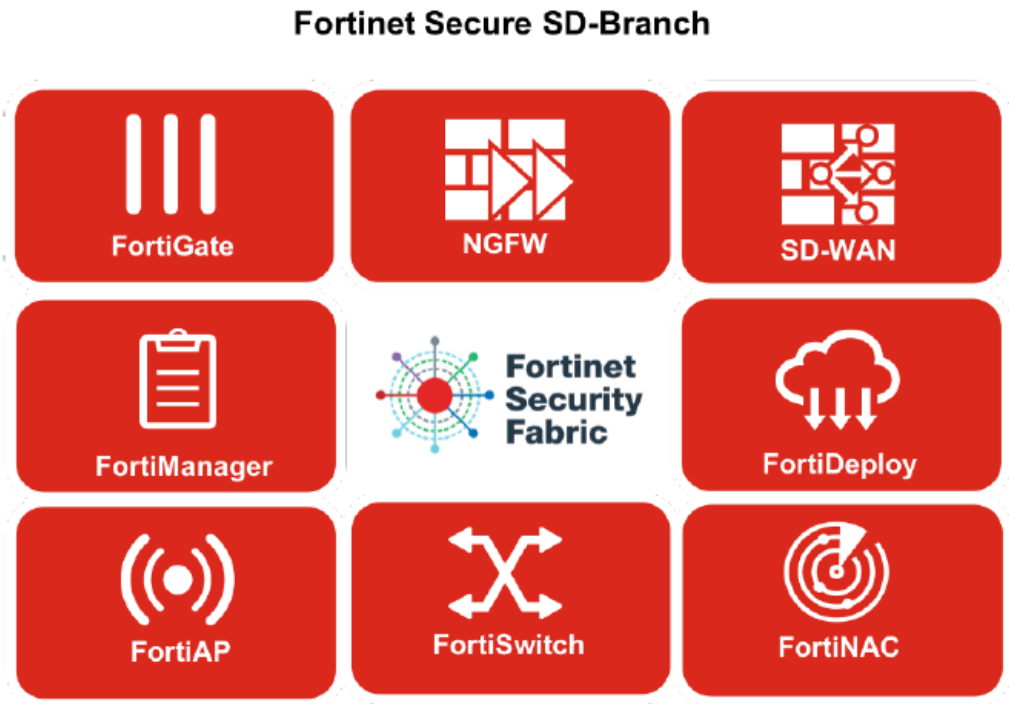
About MLL

MLL Telecom is a leading provider of managed Wide Area Networks and telecommunication services including LAN, Unified Communications (UC), Wi-Fi, and Security to the UK public sector. Our services are provided through our MLL's UK based support teams and engineering service and selected partners. Formed in 1991, MLL has established a reputation for customer-focused service delivery and agility.

Service Overview

MLL's Secure SD-Branch (Software-Defined Branch) service is designed to provide integrated security, networking, and management capabilities for distributed branch offices.

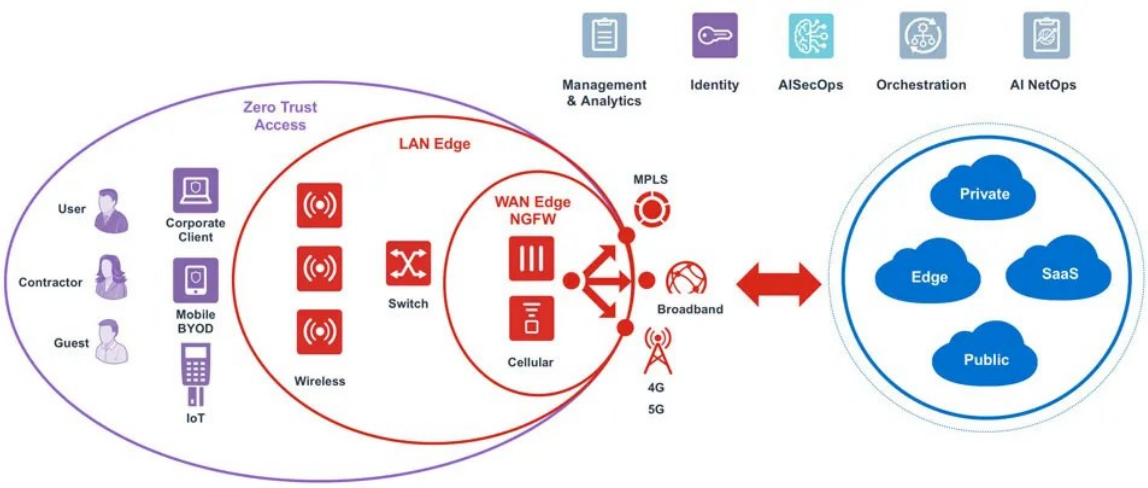
Secure SD-Branch enables customers to converge their security, WAN, and LAN, extending the benefits of the Fortinet Security Fabric to their distributed branches. Secure SD-Branch comprises FortiGate Secure SD-WAN, FortiSwitch, FortiAP, and FortiExtender to deliver consolidation of branch services. FortiGate uses "FortiLink" technology to communicate with switch and wireless platforms and requires no additional licenses. SD-Branch capabilities are included as part of the FortiOS running on every FortiGate.



To extend protection to the device edge, built-in Zero Trust features in the FortiOS operating system allow for secure onboarding of devices. Additional real-time auditing of device behaviour can be obtained by adding FortiNAC network access control capabilities.

FortiManager is also used to centrally manage SD-branch architectures. It allows efficient deployment at scale with zero-touch provisioning. FortiGate devices can initiate the connection to FortiManager,

which pushes the relevant configuration, including the switching configuration for all managed switches and other extension devices (FortiAP wireless access points and FortiExtender WAN) in the branch, making deployment simple, and accomplished within minutes. This architecture can be replicated to multiple sites giving an efficient and consistent deployment at scale.



The service is fully supported by MLL's UK-based 24x7x365 NOC and field engineering services.

Service Description

Functional Elements

Fortinet's **Secure SD-Branch** is designed to consolidate and secure branch networks by extending the features of SD-WAN across the entire branch network. The mandatory components of Fortinet Secure SD-Branch are:

1. **FortiGate Secure SD-WAN**: This component provides next-generation firewall capabilities and integrates with WAN, LAN, and WLAN elements. It ensures secure connectivity and management for remote branches.
2. **FortiManager**: This provides centralised management and configuration of Fortinet devices deployed, simplified administration, centralised security policy management and enforcement, and software updates across multiple branch locations.
3. **FortiSwitch**: FortiSwitch is an Ethernet switch that allows you to control LAN interfaces with the same level of enforcement as firewall interfaces. It's essential for managing local network traffic within the branch.
4. **FortiAP (Access Points)**: FortiAP provides wireless LAN (WLAN) connectivity for branch offices. It allows secure wireless access and extends the network coverage within the branch.
5. **FortiExtender**: FortiExtender enables LTE/5G backhaul connectivity for remote branches. It ensures reliable and secure communication even in areas with limited wired infrastructure.

Additionally, Fortinet's Secure SD-Branch incorporates Zero Trust features within its FortiOS operating system. These features allow for secure onboarding of devices and real-time auditing of device behaviour.

Optional Elements

The following are optional components or services that will enhance the branch with additional functionality and features, such as user/device authentication, remote access, posture assessment and analytics.

1. FortiAnalyzer Logging and Reporting
    - FortiAnalyzer collects and analyses logs generated by Fortinet devices, offering insights into network traffic, security events, and compliance violations.
    - It provides customisable reports, dashboards, and alerts to facilitate monitoring and troubleshooting.
2. FortiAuthenticator
    - FortiAuthenticator can identify users, through a varied range of methods and integrate with third party LDAP or Active Directory systems, to apply group or role data to the user and communicate with FortiGate for use in Identity-based policies. The platform is completely flexible and can utilise these methods in combination.
    - FortiAuthenticator extends multi-factor authentication capability to multiple FortiGate appliances and to third party solutions that support RADIUS or LDAP authentication.
3. FortiClient Endpoint Security
    - FortiClient is an endpoint security solution that extends security policies and enforcement to remote devices, such as laptops, smartphones, and tablets.
    - It integrates with FortiGate for endpoint protection, VPN connectivity, and compliance enforcement.
4. FortiNAC Network Access Control
    - FortiNAC provides network access control capabilities, allowing organisations to enforce security policies based on user identity, device type, and security posture.
    - It integrates with Fortinet SD-Branch components to ensure secure access and compliance across wired and wireless networks.

These components work together to provide a unified, secure, and scalable solution for branch office connectivity, ensuring optimal performance, resilience, and protection against evolving cyber threats.

Features

Fortinet SD-Branch is a solution designed to provide secure and efficient branch office networking. Here are some of its key features:

1. Unified Security Fabric: Integration with Fortinet's Security Fabric enables consistent security policies and enforcement across the entire distributed network infrastructure, including branch offices, data centres, and cloud environments.

2. Next-Generation Firewall (NGFW): Fortinet's NGFW capabilities provide advanced threat protection, intrusion prevention, application control, and web filtering to safeguard branch office networks from a wide range of cyber threats.

3. Secure SD-WAN: Fortinet's SD-WAN functionality allows organisations to optimise WAN connectivity by dynamically routing traffic across multiple links based on performance metrics such as latency, jitter, and packet loss. This improves application performance, reliability, and availability while reducing costs.

4. Zero Trust Network Access (ZTNA): Secure SD-Branch implements a Zero Trust security model, ensuring that all users, devices, and applications are authenticated and authorised before accessing branch office resources. This helps prevent unauthorised access and lateral movement of threats within the network.

5. Integrated Wireless LAN (WLAN): Secure offers integrated wireless LAN solutions that provide secure and reliable Wi-Fi connectivity for branch office users and devices. These solutions support advanced features such as Wi-Fi 6 (802.11ax), secure onboarding, and guest access management.

6. Network Access Control (NAC): Fortinet's NAC capabilities enable organisations to enforce security policies and control access to branch office networks based on user identity, device type, and security posture. This helps ensure compliance with regulatory requirements and protect against insider threats.

7. Endpoint Security Integration: Integration with Fortinet's endpoint security solutions, such as FortiClient, extends security policies and enforcement to remote devices connecting to branch office networks. This helps prevent malware infections, data breaches, and other security incidents.

8. Centralised Management and Orchestration: Secure SD-Branch provides centralised management and orchestration capabilities, allowing administrators to configure, monitor, and troubleshoot branch office networks from a single pane of glass. This streamlines network operations, reduces complexity, and improves efficiency.

9. Cloud Integration: Fortinet's SD-Branch solutions seamlessly integrate with cloud environments, enabling organisations to extend consistent security policies and enforcement to branch office workloads hosted in public, private, or hybrid clouds.

10. Comprehensive visibility and reporting: Secure SD-Branch offers comprehensive visibility into network traffic, security events, and user activities, along with customisable reporting and analytics capabilities. This enables organisations to monitor network performance, identify security threats, and demonstrate compliance with regulatory requirements.

By combining security, SD-WAN, and LAN edge access in a single appliance, Secure SD-Branch aims to simplify and secure branch office networking while providing high performance and reliable connectivity.

Benefits

The main benefits of Secure SD-Branch include:

1. Integrated Security: Secure SD-Branch integrates advanced security functionalities, including next-generation firewall (NGFW), secure SD-WAN, Zero Trust Network Access (ZTNA),

network access control (NAC), and endpoint security, into a single solution. This provides comprehensive protection against a wide range of cyber threats, simplifies security management, and reduces the attack surface.

2. Enhanced Connectivity: Secure SD-Branch optimises WAN connectivity through secure SD-WAN capabilities, enabling organisations to leverage multiple links (MPLS, broadband, LTE) for improved application performance, reliability, and cost-efficiency. Dynamic traffic routing based on real-time performance metrics ensures optimal connectivity and user experience.

3. Simplified Management: With centralised management and orchestration capabilities, Secure SD-Branch streamlines network operations by providing a single pane of glass for configuring, monitoring, and troubleshooting branch office networks. This reduces complexity, minimises manual tasks, and improves efficiency for IT administrators.

4. Scalability and Flexibility: Secure SD-Branch is designed to scale with organisational growth and evolving network requirements. It supports a wide range of deployment scenarios, from small branch offices to large enterprise networks, and can adapt to changing business needs through flexible deployment options and licensing models.

5. Improved User Experience: By integrating wireless LAN (WLAN) solutions with advanced features such as Wi-Fi 6 (802.11ax), secure onboarding, and guest access management, Secure SD-Branch delivers a seamless and secure wireless experience for branch office users and devices, enhancing productivity and satisfaction.

6. Compliance and Governance: Fortinet SD-Branch helps organisations maintain compliance with industry regulations and internal policies by enforcing consistent security policies and access controls across distributed branch office networks. This ensures data protection, risk mitigation, and regulatory compliance.

7. Cost Savings: Through the consolidation of networking and security functionalities into a single platform, Secure SD-Branch helps organisations reduce capital and operational expenses associated with deploying and managing separate networking and security solutions. This results in cost savings and a lower total cost of ownership (TCO) over time.

8. Business Continuity: Secure SD-Branch enhances business continuity by providing high availability and resiliency features such as redundant links, failover capabilities, and built-in redundancy mechanisms. This ensures uninterrupted access to critical applications and services, even in the event of network failures or disruptions.

Overall, Secure SD-Branch aims to provide a secure, high-performance, and cost-effective solution for branch office networking, enabling organisations to streamline operations, optimise application delivery, and maintain a strong security posture across distributed locations.

Standards based delivery

MLL will use industry standards for project and service delivery as summarised in the table below:

Delivery and Service Management	Industry Standard
Service Management	ITIL

Project Management	PRINCE2
Quality Management	ISO 9001
Security Management	ISO 27001 and Cyber Essentials Plus
Environmental Management	ISO 14001
Health and Safety Management	ISO 45001
NHS Digital	Data Security and Protection Toolkit

Delivery

MLL provides Buyers with an Implementation Coordinator for small-scale Secure SD-Branch solution deliveries, for example small branch offices, or an MLL Project Manager for large scale/ complex deliveries. The scale of the solution required, and therefore the MLL delivery team required to manage the implementation of the Buyer's requirements, including engineers, will be determined during the MLL team's assessment of the initial enquiry from the Buyer.

MLL follows an ISO 9001 audited delivery process and maintains an ISO 27001 audited configuration and change management process for customer hosting infrastructure. MLL's Project Managers are PRINCE2-qualified and, where assigned, will be MLL's stakeholder to manage the project delivery. MLL's Solutions Architects, Technical Design Authorities, and Technical Engineers, including our NOC and Field Engineers, who provide the technical aspects of our network deliveries, are also all highly skilled and well-qualified across the range of technologies used in MLL's network deliveries, including Fortinet, Juniper, Cisco and HPE Aruba.

MLL uses PRINCE2 methodologies to deliver projects, typically employing the following 4 stages of project delivery:

- Internal project set-up (including contract award, team assignment, etc)
- Project Initiation (Kick-off meeting, risk assessment, technical discovery, technical workshop, project and technical documentation)
- Project Delivery (solution delivery, risk and issue management, change management, progress reporting, escalation management, governance, progressive handover to MLL's Business as Usual (BAU) team, etc)
- Project Handover (complete handover to MLL's BAU team, project review, lessons learnt, project closure, etc)

The lead time to deliver small scale Secure SD-Branch services in this offer are expected to take between 15 and 40 working days.

The lead time to deliver a complex Secure SD-Branch solution is entirely dependent on the Buyer's overall requirements and will be assessed and advised during the scoping of the project requirements, prior to award.

MLL's team will undertake regular project reviews with the Buyer to an agreed frequency. For larger projects, governance will be provided through a project board comprising senior sponsors from MLL and the Buyer.

Support

Monitoring and Reporting

- MLL will monitor all in scope Secure SD-Branch services 24x7x365 for availability, utilisation and performance.
- Any failure which appears will be analysed and where appropriate raised as an Incident with MLL's Service Desk and the Buyer's Service Desk will be notified.
- Incidents will be managed using MLL's Incident Management Service through to resolution.
- MLL will provide access to the MyMLL service portal and through this access to the performance monitoring service.

Service Desk

MLL's Network Operations Centre is based in Marlow, Buckinghamshire, supporting customers on a 24 x7x365 basis.

The NOC and Service Desk undertakes the following functions:

- Receives Incident or Service Requests by agreed contact methods – telephone, email or via MyMLL portal.
- Records Incident or Service Requests on the Service Management System.
- Allocates a Call to Severity 1, 2, 3 or 4 and where relevant manage the Incident through to Resolution in accordance with the Service Levels.

Support Model

MLL's service support model is based on ITIL compliant processes with clearly defined roles and responsibilities, supported by industry recognised systems and tools. This model will be used to monitor the Service in order to meet the Service Level.

Incidents will be raised either proactively by MLL or reactively by the Buyer and logged in MLL's IT Service Management system.

MLL utilise the following Severity Definitions for Incident Management:

SD-Branch

Category	Definition
Severity 1	The Services are Unavailable across the entire Buyer's estate
Severity 2	The Services are Unavailable at one of the Buyer's sites

Severity 3	The Services are Unavailable to an individual user
Severity 4	All other Incidents, including any Incidents raised initially at a higher Severity Level that were subsequently deemed to be attributable to the Buyer or in any other way not attributable to the Supplier.

Wi-Fi

Category	Definition
Severity 1	The Wi-Fi Services are Unavailable across the entire Buyer's estate
Severity 2	The Wi-Fi Services are Unavailable at one of the Buyer's sites
Severity 3	The Wi-Fi services are unavailable to a single AP
Severity 4	All other Incidents, including any Incidents raised initially at a higher Severity Level that were subsequently deemed to be attributable to the Buyer or in any other way not attributable to the Supplier.
Notes	Due to single APs frequently losing power as a result of local environmental factors, they will not be proactively monitored by MLL. As such, any Incident relating to a single AP (Severity 3) must be proactively raised by the Buyer to MLL, and the SLA will only commence from the time the ticket is logged.

MLL will ensure that Incidents are resolved within the Incident Resolution Time, based on the Severity Level of the Incident.

Service Hours

Monday – Sunday (including Bank Holidays) - 00:00-23:59, (24 hours per day, 7 days per week)

Service Levels

Incident Resolution

Service Type	Severity 1	Severity 2	Severity 3	Severity 4
Wi-Fi	5 hours	8 hours	End of next Working Day (Commencing from when a ticket has been raised to MLL by the Buyer)	10 Working Days

It is also assumed that all cabling infrastructure will be managed by the Buyer. In the event of a cabling fault causing a Wi-Fi Incident, MLL would assign this to the Buyer to resolve.

Availability

The availability of the Secure SD-Branch is dictated by the branch site WAN connectivity. Availability targets associated with each connectivity type are shown below.

Connectivity Type	Availability
Fibre Ethernet	99.90%
Ethernet FTTP	99.70%
Ethernet FTTC	99.50%
FTTP	99.70%
FTTC	99.50%
ADSL	99.50%

Service Credits

Service Credits will be calculated and reported by MLL through the quarterly Service Report and reviewed with the Buyer at the Service Review Meeting. This will include a summary of any service credits accrued within the previous period.

Incident Resolution

Number of Incidents per Service Period	Coefficient (m)	Service Level Threshold (a)	Service Failure Threshold (b)	Minimum Service Credit % (c)	Maximum Service Credit % (d)
39 or fewer	Not applicable	No more than 2 Incidents are Resolved in excess of the max Incident Resolution Times	5 or more Incidents are Resolved in excess of the max Incident Resolution Times	2.5% (payable when 3 Incidents breach the Service Level Threshold in any Service Period)	5% (payable when 4+ Incidents breach the Service Level Threshold in any Service Period)
40 and more	0.25	95%	85%	2.5%	5%

Social Value

MLL is committed to providing social value as part of its contractual deliverables which will be agreed with the Buyer and detailed in the call-off contract. MLL will deliver social value against the following themes:

Fighting Climate Change - Underpinned by MLL's existing ISO 14001 environmental management system and published carbon reduction plan with a net zero target date of 2040.

Tackling Economic Inequality - We will deliver tailor-made offers to support the communities and citizens in the localities in which we serve our customers.

Equal Opportunity - This is a fundamental principle of our business and the basis of our customer relationships.

Wellbeing - MLL will provide offers that support the physical and mental wellbeing of staff and citizens through delivery of in-person and online packages.

Company Information

Company Details

MLL Telecom Limited

Marlow International, Parkway, Marlow, England, SL7 1YL

Company No: 02657917

Date of incorporation: 28th October 1991

VAT No: 203558428

Switchboard: 01628 495400

Website: www.mlltelecom.com

Contacts

Name: Ellie Coome

Position: Bid Manager

Tel: 01628 495 400

Email: gcloud@mlltelecom.com

Copyright