CLOUDSWITCHED

FREE RESOURCE — BEST-PRACTICES GUIDE

Multi-Site Networking Guide

SD-WAN, VPN tunnels and centralised policies for connecting two or more office locations — reliable, secure, performant networking across every site you operate.

5	SD-WAN	1	2×
CONNECTIVITY OPTIONS	RECOMMENDED TECHNOLOGY	CENTRAL DASHBOARD	DIVERSE CIRCUITS PER SITE

SD-WAN · IPSEC VPN · MPLS · EXPRESSROUTE · CENTRAL POLICY

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Fillable PDF

01

Connectivity options compared

If your business operates from two or more locations that need to share data, applications or phone systems, you need a multi-site networking strategy. The right approach depends on bandwidth needs, budget, application requirements and growth plans. The five options below cover virtually every UK SME multi-site deployment we have seen.

Inter-site connectivity at a glance

TECHNOLOGY	TYPICAL SPEED	RELIABILITY	COST BAND	BEST FOR
MPLS	10 Mbps – 10 Gbps	Very high (SLA)	~~£~~~~£~~~~£~~~~£~~	Large enterprises, low-latency requirements
SD-WAN	Depends on underlay	High (redundant)	~~£~~~~£~~	Most SMEs, multi-circuit aggregation
IPsec VPN	Depends on internet	Good	~~£~~	Budget-conscious, simple site-to-site
Meraki Auto VPN	Depends on internet	High	~~£~~~~£~~	Meraki customers, easy deployment
Azure VPN / ExpressRoute	Up to 10 Gbps	Very high	~~£~~~~£~~ – ~~£~~~~£~~~~£~~~~£~~	Azure-heavy environments

WHY SD-WAN IS THE MODERN CHOICE

SD-WAN combines multiple internet circuits — fibre, broadband, 4G/5G — into a single resilient connection with intelligent traffic routing. It delivers MPLS-like reliability at a fraction of the cost, with centralised cloud management across all sites and per-application path selection that prioritises VoIP and video automatically.

01

How to choose

The table on the previous page lists the five technologies most UK SMEs will consider. The decision rules below cover the four common scenarios — pick the row that matches your situation, then read the rest of the guide with that choice in mind.

Two sites, modest budget, no real-time apps. Site-to-site IPsec VPN over business broadband is fine. Plan the upgrade path for when you outgrow it — second site, second concurrent VoIP call, or any video conferencing across the tunnel.

Three or more sites, VoIP and video are critical. SD-WAN with dual diverse circuits at every site — the right answer for the vast majority of UK SMEs. Application-aware routing keeps voice and video on the best path automatically, while bulk traffic uses the cheap underlay.

You already run Meraki. Meraki Auto VPN turns site-to-site mesh into a checkbox — lowest deployment friction if you are already on the platform. Pairs naturally with the rest of the Meraki stack (MX, MS, MR) under a single dashboard.

Heavy Azure footprint. ExpressRoute (or scaled Azure VPN gateways) gives you private, predictable connectivity into your cloud workloads — latency you can rely on, bandwidth you can scale, and bypassing the public internet for sensitive workloads.

Strict SLA-backed latency targets. MPLS still wins, at a price. Most SMEs no longer need it — SD-WAN over decent fibre gets you 95% of the way for a quarter of the cost, with the management benefits MPLS never had.

TWO QUESTIONS BEFORE YOU COMMIT

How many concurrent VoIP calls cross the WAN at peak? Multiply by 100 kbps and add 30% headroom — this sets the minimum sustained inter-site bandwidth.
What is the cost of one hour of downtime at a branch site? If the answer is hundreds of pounds or more, you need a diverse backup circuit at that site, not just a single connection.

02

SD-WAN architecture

A typical SD-WAN deployment uses dual internet circuits at each site (primary fibre plus a diverse backup — broadband from a different carrier, or 4G/5G) with an SD-WAN appliance providing automatic failover, traffic prioritisation and encrypted tunnels between sites.

Design principles

Circuit diversity. Different ISPs and different technologies for primary and backup. If primary is BT fibre, use Virgin or 4G as the backup — never another BT circuit on the same physical path.

Application-aware routing. Prioritise VoIP and video over the best-performing circuit; route bulk data (backups, file sync) over the cheapest available path.

Centralised cloud management. Pick a solution with a single cloud dashboard (Meraki, Fortinet FortiManager, Cisco vManage) for one-pane visibility, zero-touch provisioning and remote configuration of every site.

Hub-and-spoke vs full mesh. Use hub-and-spoke if most traffic flows to a central site (typical for HQ + branches). Use full mesh if sites need to talk directly (VoIP, file sync between branches).

Topology verification — tick before go-live

Primary inter-site link tested end-to-end and confirmed healthy — throughput, latency, jitter within spec.

Backup circuit diversity verified — different ISP, different physical path, different last-mile technology where possible.

SD-WAN tunnel established between every site pair required by the topology (hub-and-spoke or mesh as designed).

Automatic failover tested by pulling the primary circuit — calls survive, sessions remain stable, observed failover time under 30 seconds.

Application policies in place: VoIP, video, business apps prioritised; bulk traffic on the cheapest underlay.

Encrypted tunnels using AES-256 (or IPsec equivalent) on every site-to-site link — nothing crosses the public internet in clear.

Cloud dashboard shows green for every site — appliance, both circuits, tunnel state, latency, loss.

03

Centralised policy & security

One of the biggest advantages of modern multi-site networking is the ability to define policies centrally and push them to every site at once. This guarantees consistent security regardless of site size or the IT capability available locally — the branch with no on-site IT gets the same firewall rules as HQ, no exceptions, no drift.

Policy domains to manage centrally

Firewall rules. Define and deploy centrally; changes propagate to every site within minutes. Version-control the template — review and approve before push, the same way you would with code.

Web / content filtering. Apply consistently across every site to block malicious and inappropriate content. One policy, one allow-list, one place to update it.

IDS / IPS. Enable intrusion detection and prevention across every site firewall from the central dashboard. Tune signature sets centrally and roll them out everywhere at once.

Split tunnelling. Decide per-application whether traffic routes through the central site (more secure, single egress) or breaks out locally (better performance for SaaS). SD-WAN lets you mix per app, not all-or-nothing.

Remote-access VPN. Manage from a single point. Users connect regardless of which site they live closest to; central authentication, central logging.

AVOID CONFIGURATION DRIFT

When you manage several sites it is easy for configurations to drift apart over time — an ad-hoc change here, a one-off exception there, and six months later no two sites are the same. Use centralised management and configuration templates to prevent this, and audit site configurations quarterly to verify they still match the master template. Treat drift as a finding, not a feature.

03

Policy & VPN topology checks

Once policies are defined centrally, the next step is verifying they have landed identically at every site. Tick each item below as you confirm it — a single missed setting on a branch firewall is how a multi-site network ends up with one site quietly outside the security baseline.

- **Firewall ruleset** identical across every site — verified by a config-diff report from the central dashboard.
- **Web filtering** blocking the same category set at every site; allow-list exceptions documented and reviewed quarterly.
- **IDS/IPS signatures** on the same release everywhere; alerts feeding into a single SIEM or central log store.
- **Remote-access VPN** using SSO/MFA; per-user logging confirms which site each session originated from.
- **Site-to-site VPN tunnels** verified up and encrypted on every required pair (hub-and-spoke or full mesh as designed).
- **Split-tunnel decisions** documented per application; SaaS breaks out locally, sensitive apps hairpin via HQ.
- **Configuration template** applied via the central dashboard so every site renders the same baseline.
- **Quarterly drift audit** scheduled; deltas raised as findings against the master template, never tolerated as “local variation”.

WHAT GOOD LOOKS LIKE

A network engineer can pick any site at random, open its config, and find an exact match for the master template apart from site-specific IP addressing. If that is not true today, the next maintenance window should be a config-reconciliation exercise — not new features.

04

Implementation planning — site inventory

Capture every site you plan to deploy. Deploy the hub/HQ first and verify all policies and routing land where you expect, then bring branches up one at a time — smallest and least critical first, keeping the old connectivity live in parallel until the new SD-WAN is proven for at least one full business week.

SITE 1 — HQ / HUB

LOCATION _____ USERS ON SITE _____ SD-WAN DEVICE / MODEL _____

PRIMARY CIRCUIT (ISP / TYPE / SPEED) _____ BACKUP CIRCUIT (ISP / TYPE / SPEED) _____

BANDWIDTH REQUIRED (MBPS DOWN / UP) _____ GO-LIVE DATE _____

SITE 2 — BRANCH

LOCATION _____ USERS ON SITE _____ SD-WAN DEVICE / MODEL _____

PRIMARY CIRCUIT (ISP / TYPE / SPEED) _____ BACKUP CIRCUIT (ISP / TYPE / SPEED) _____

BANDWIDTH REQUIRED (MBPS DOWN / UP) _____ GO-LIVE DATE _____

04

Site inventory continued

Continue capturing the remaining sites. If you have more than four sites, photocopy this page or duplicate the cards in your working copy — the structure is identical for every additional branch.

SITE 3 — BRANCH

LOCATION

USERS ON SITE

SD-WAN DEVICE / MODEL

PRIMARY CIRCUIT (ISP / TYPE / SPEED)

BACKUP CIRCUIT (ISP / TYPE / SPEED)

BANDWIDTH REQUIRED (MBPS DOWN / UP)

GO-LIVE DATE

SITE 4 — BRANCH

LOCATION

USERS ON SITE

SD-WAN DEVICE / MODEL

PRIMARY CIRCUIT (ISP / TYPE / SPEED)

BACKUP CIRCUIT (ISP / TYPE / SPEED)

BANDWIDTH REQUIRED (MBPS DOWN / UP)

GO-LIVE DATE

Aggregate bandwidth summary

TOTAL USERS ACROSS ALL SITES

CONCURRENT VOIP CALLS AT PEAK

TOTAL WAN BANDWIDTH REQUIRED (MBPS)

05

Deployment sequence & sign-off

Roll out in a fixed order, with each site fully verified before you move to the next. The checks below are the gate — do not declare a site done until every box is ticked. Old connectivity stays live in parallel until the new SD-WAN underlay has carried a full business week of production traffic without incident.

DEPLOYMENT SEQUENCE

Deploy the hub/HQ first and verify all policies and routing land as designed. Then bring up branch sites one at a time, starting with the smallest or least critical. Verify each site thoroughly before moving to the next. Keep the old connectivity active in parallel until the new SD-WAN is proven over at least one full business week.

Per-site cutover checks

- **SD-WAN appliance** on-site, registered to the cloud dashboard, firmware on the standard release.
- **Both circuits** live, tested independently, latency / loss baselines captured.
- **Site-to-site tunnels** up to every required peer (hub at minimum; mesh peers if applicable).
- **Application policies** applied and verified by traffic test (VoIP call, file copy, video).
- **Failover test** performed by physically disconnecting the primary circuit — calls survive, sessions persist.
- **Old connectivity** kept warm in parallel for at least one full business week before decommissioning.
- **Monitoring** showing both underlays, tunnel state and latency; alerts wired into the on-call channel.

PREPARED BY	DATE	APPROVED BY

CLOUDSWITCHED

CLOUD NETWORKING & MULTI-SITE CONNECTIVITY

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom