How to know when it's time for SD-WAN

This checklist is based on some of the common issues, challenges, and sentiment that can appear within organisations prior to SD-WAN implementation. Particularly those where rip-and-replace isn't a viable strategy. You'll find the themes cover four main areas: connectivity, cloud, cyber security and collaboration.

1. Scalability challenges

- [ ] Traditional MPLS is taking too long to provision and roll out
- [ ] VPNs are becoming harder to scale and manage the more sites and remote workers a company adds.
- [ ] Acquisitions have meant segmenting traffic to keep lines of business separate, and/or integrating new technology into networks.

2. Hybrid connectivity requirements

- [ ] Work across multiple types of connectivity, not only ethernet and leased lines.
- [ ] Cover remote workers' home connectivity plus 4G & 5G.
- [ ] Configure failover to keep business critical apps running while minimising performance impacts.

3. How layering should look

- [ ] Turn on new branches quickly without affecting existing infrastructure.
- [ ] Applications and access remain the same and use either the site's existing connectivity or a new link.
- [ ] Zero touch deployment, monitoring and management to deploy sites centrally without local engineering visits.

4. The need for internet breakout at every location

- [ ] Flexibility for remote locations and 4G and FTTC compatible.
- [ ] Built for leveraging SaaS applications such as Microsoft 365 that boost overall traffic yet require very low latency.
- [ ] Application visibility with analytics and reporting from within a single reporting dashboard.

5. WAN speed, bandwidth & routing

- [ ] Firewalls to provide scalable central management, local security enforcement and QoS for every branch office.
- [ ] Application-aware security ensures business-critical SaaS applications are assigned the highest priority and the best suitable uplink.
- [ ] Automatic prioritisation enables direct internet breakout for every branch office.

6. Cost savings to be realised

- [ ] Unified, simple hardware solutions and cheaper connectivity options compared to private networks and MPLS.
- [ ] Simple upgrades of features and policies instead of individual site-based policies, upgrades and maintenance.
- [ ] Reduced CapEx and evolution to an As-A-Service model, while still layering over necessary legacy systems.

7. Cyber security examples

- [ ] Ability to micro-segment traffic and data flows, to isolate attack vectors in the event of a breach.
- [ ] Creation of encrypted tunnels for data transmission between sites, for example with dynamic multipoint VPNs.
- [ ] Frequent key rotations, and/or Diffie-Hellman key exchanges, for users to safely share secret keys over insecure channels.

8. Disaster recovery features

- [ ] Multiple connectivity sources per site for load balancing.
- [ ] Primary and backup networks running simultaneously and synchronising data.
- [ ] Automatic re-diverts in cases of outages, with integration into all major cloud platforms.

Registered Office 1st Floor, The Wharf, Abbey Mill Business Park, Lower Eashing, Godalming GU7 2QN
0333 240 9880 arrowcommunications.co.uk.