ExtraHop

WHY REMOTE DOESN'T HAVE TO MEAN LONELY

Addressing the challenges of remote site management for a cloud-focused future

In today's world of instant gratification and the app-for-everything mindset, consumers have high expectations for a streamlined, fully integrated digital experience as well as countless alternatives if your organization can't deliver. While every industry must evolve and innovate in order to provide the experience consumers demand, remote site environments face even more pressure to adopt cloud and SaaS or risk losing business to more agile, service-focused competitors. That transition requires rethinking traditional wide-area network (WAN) designs in order to address growing visibility gaps, attack surfaces, and bandwidth requirements.

Branch Office Workflows Are Changing

More and more organizations are deploying cloud-based services: the rate of public cloud adoption, according to Forrester Research, will reach 50% in 2018[1] and spending on public cloud services and infrastructure, according to International Data Corporation (IDC), is expected to increase 23.2%.[2]

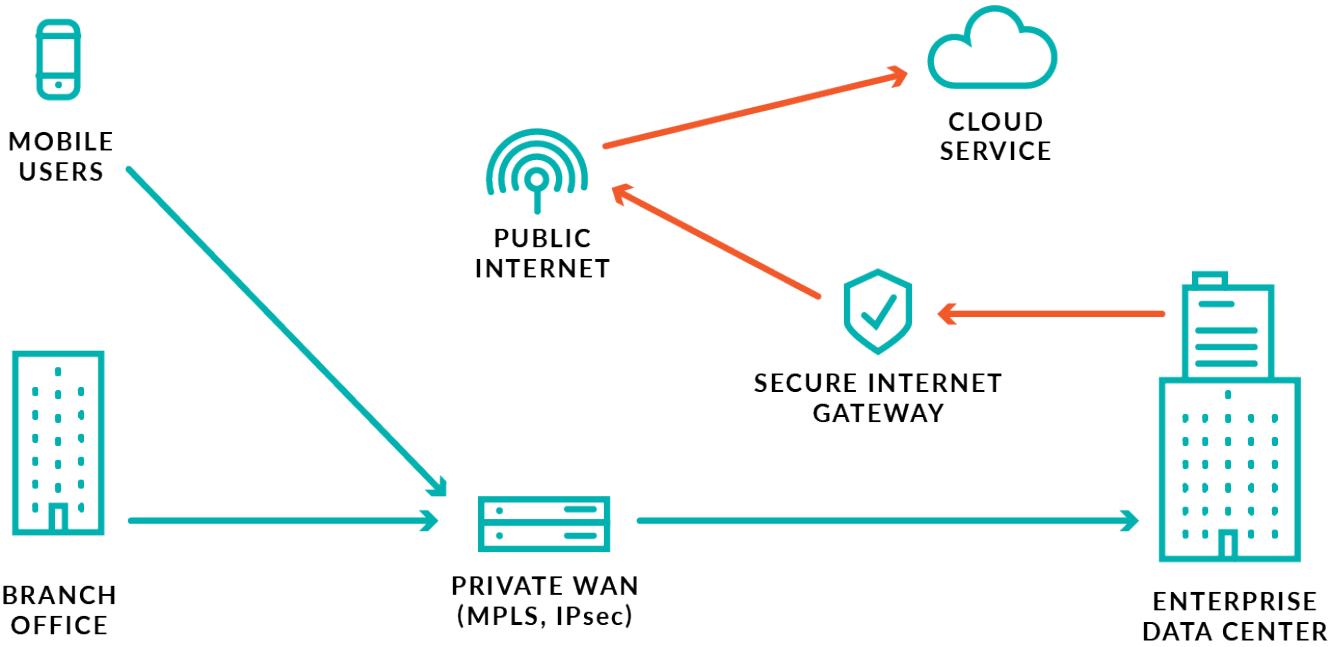
But the transition to more cloud services has a pretty significant impact on traditional wide-area network (WAN) designs, especially in industries like retail, banking, and healthcare. A department store chain might have hundreds or even thousands of store or branch office locations that serve customers directly, and healthcare organizations often consist of a large network of hospitals, clinics, and physician offices that need to keep in touch in order to give their patients the most consistent care.

Whatever your industry, and whether you're breaking apart a legacy application and moving it to the cloud or replacing an application with a software-as-a-service (SaaS) solution, cloud adoption means you'll have to adapt to changing performance management workflows at branch locations as well. Not only will you need to wrangle new traffic patterns, a larger attack surface, and unanticipated black boxes, but—depending on your vendor—cloud-based application performance is often entirely out of your internal team's control.

All of these changes put a lot of pressure on branch office communications and WAN designs: the right WAN structure can make or break your success in modern digital business.

Classic Branch Office: Traditional Network Design

Branch office networks, especially ones that have been in place for years, often utilize a classic hub-and-spoke architecture. In a hub-and-spoke design, most computing services are centralized into a primary or regional data center. Routers are placed at remote locations, and users and devices at those locations communicate with the central data center via a private WAN using Multiprotocol Label Switching (MPLS) or IPsec:



Prior to the Internet this design was all the rage, and for good reason. Critical applications and data all resided at the central data center, so it was easy to centralize data management and security functions. This architecture enabled branch office users to access the applications they needed with minimal network latency and operational overhead.

Even when some applications became distributed and moved to the branch office LAN, the hub-and-spoke model made sense because you were still required to communicate with the central data center in order to get anything done. But now, as more and more cloud-based applications are deployed, organizations must face the impact of this kind of network design on cloud workflows.

In a traditional hub-and-spoke system, Internet access is centralized in order to enforce security: Internet-bound traffic at branch office sites is routed through the central data center via a private WAN and then sent out through secure Internet gateways. According to Gartner, more than 60% of enterprises use this kind of centralized Internet security model.[3]

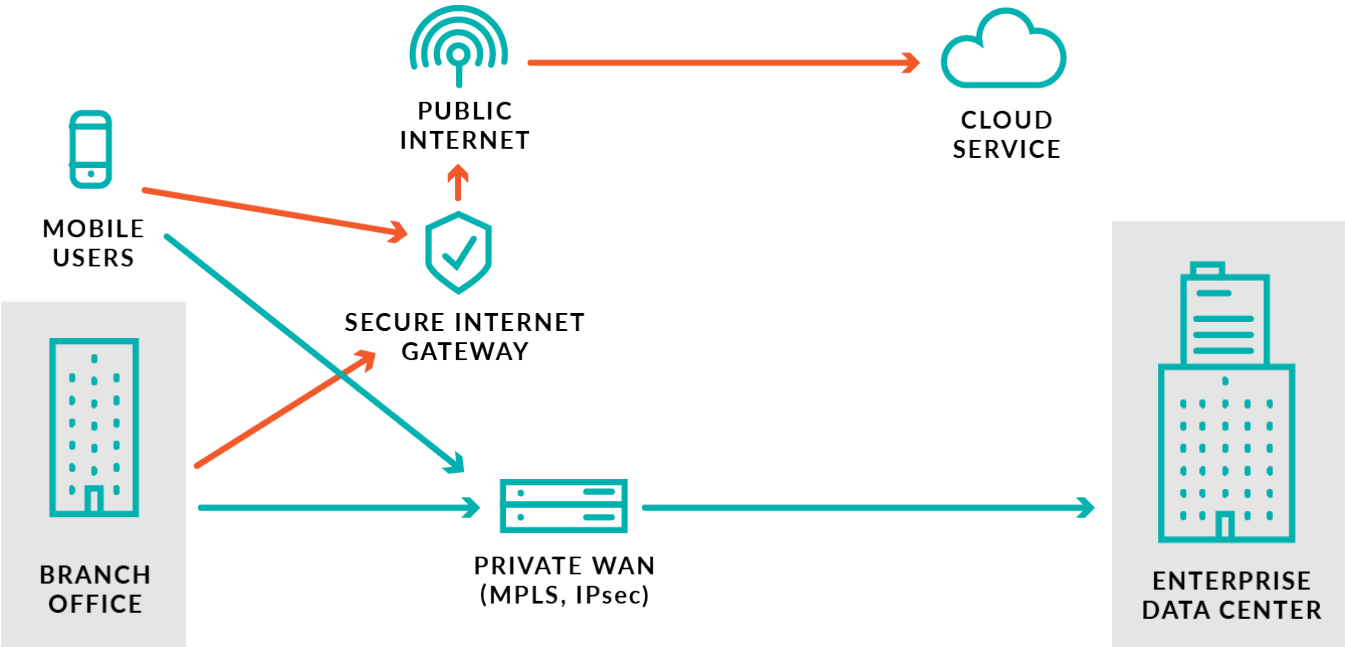
While forcing traffic through a private Internet gateway does help address security concerns with remote sites, it also increases network latency—and the farther the cloud service is from the Internet gateway, the more latency you get.

In a shocking twist, network lag equals poor performance for public cloud applications. For example, 25% of enterprises report poor performance from their Office 365 deployments as a side effect of the latency between the remote site and headquarters.[4] If you're, say, a hospital using Citrix to share access to electronic medical records, that kind of latency can steal up to an hour of a doctor's shift just waiting for her application to load. Which ultimately means fewer patients can be seen, resulting in less revenue for the hospital.

Fear of performance degradation like the above leads many organizations to put off implementing critical cloud-based applications until they can redesign the branch WAN—which, when you've built your entire infrastructure around a more traditional model, is an intimidating mountain to climb.

What's Hot Right Now: A Hybrid WAN Design

One way many organizations are tackling the problem of network latency (as well as high connection costs) is by deploying hybrid WANs at their branch office sites. In a hybrid WAN, multiple connection paths are used for communications. Often, those connections are a combination of MPLS, Internet Broadband, and 4G LTE; traffic is routed across these different paths based on user-defined policies:



Complex as these deployments appear compared to their predecessors, roughly 70% of organizations will leverage a hybrid WAN model by 2020[5] because hybrid WANs uniquely address a lot of those performance concerns when it comes to cloud-based applications.

With a hybrid WAN deployment, you can establish a direct connection from each branch office to the Internet while maintaining a private WAN connection to the central data center. By routing legacy application traffic to the data center via that private WAN link,

you remove the need for all traffic to pass through the central data center and therefore cut back on general latency as well as the risk of downtime due to any problems with the central hub.

In the hybrid WAN scenario, Internet-bound traffic is routed directly through a secure Internet gateway provided by your Internet service provider (ISP). While it's on your ISP to keep that data safe, this method does streamline your traffic flows by a significant margin. If cloud traffic no longer needs to traverse the private WAN, you'll deal with fewer network hops and much less communication overhead.

Of course, the performance benefits of a hybrid WAN network do have a flip side. Because each remote site needs to support multiple connections independent of the central branch office, these deployments are far more complicated to plan and implement. It's a big ask up front, both in time and capital, in exchange for greater scalability and control in the long run.

On the far end of the WAN evolution, some ambitious organizations are opting for a full mesh design where every single remote branch functions as a node connected to every other remote branch plus the central hub. These deployments automatically balance workloads in order to support massive amounts of traffic with minimal latency or risk to application delivery, but they're also expensive to build and a major commitment to maintain.

One thing is certain: Restructuring your network to better deal with dramatically increasing cloud adoption and traffic rates is the only way to keep giving customers the seamless experience they expect. Once you've modernized your network, however, you'll have to modernize your monitoring capabilities as well—there are a few key challenges already plaguing remote site management, and this is your chance to fix them.

Challenges for Remote Site Management

Organizations are pushing more applications to the cloud in part because cloud-based services allow them to improve customer and employee experience in remote site locations. As we've discussed, this move has a significant impact on branch office networks—but even once you've mapped out an effective network design, supporting more cloud applications in remote branch offices raises the stakes for remote site management in ways few organizations are equipped to address.

Visibility

Delivering service-focused digital experiences involves constant interaction with users and their devices. To effectively manage those communications, organizations need real-time visibility into what's going on at each branch location. But in a cloud services model, most of your applications run on infrastructure located in data centers managed by someone else.

With black boxes where your critical performance data should be and limited access to packets even if you ask for them, it's hard to gauge how well your applications are delivering on their promise and even harder to troubleshoot specific errors once users bring them to your attention.

Cloud-based applications aside, you also need to take IoT devices into account. For example, more and more retail stores are leveraging IoT devices and technology to analyze shopper behavior and traffic patterns in order to learn more about inventory and purchasing decisions being made by the consumer. In the Healthcare industry, wearable IoT devices are helping to monitor patient care. As IoT device counts increase, not only must each remote site juggle its internal and customer-facing IoT assets, but customers themselves are consistently interacting with your network via their own devices; gaining visibility into this kind of traffic is difficult enough for centralized offices, let alone for remote sites already struggling to pull the data they need to notice and address issues.

Tracking

There's another angle to the visibility challenge that remote site managers have the joy of tackling: the need to track exactly which systems, applications, and devices are in use at any given site at any given time.

From a purely practical standpoint, the logistics of mapping out every asset and dependency across each remote branch can be a nightmare, especially in acquisition scenarios where the soon-to-be acquired site might use an entirely different tracking method (or

haven't been tracking their systems as diligently as they could). For example, when large hospital organizations acquire smaller regional clinics it's often difficult to gain visibility into each newly acquired clinic. The ability to quickly and accurately auto discover and classify everything in a remote site environment is a critical step in any acquisition.

Technologically speaking, IoT and cloud-based services add layers of fog to a process that's already a hassle for managers who need to understand what's actively communicating with what. Not only do remote site managers lack clear insight into performance data (as well as the ability to correlate problems across different applications and systems if they're managed by different teams and vendors), they can't always tell what they should be looking at in the first place.

Security

Cyber security is a major concern for every industry, but organizations with extended networks face even more pressure as they struggle to secure new IT managed and personal devices, application traffic routed directly to the cloud, and an attack surface that balloons with every additional branch.

As cloud-based workflows and IoT devices open up new attack vectors, often-centralized security teams are saddled with inadequate network segmentation visibility between remote locations and the risk of remote sites being used as entry points for backdoor attacks.

When traditional remote networks were first designed, a robust security discipline backed by a comprehensive, intentional architecture simply wasn't a consideration in the way it is today. Remote site managers are feeling that pain now, and it will only get worse without internal visibility that spans the entire extended environment.

CONCLUSION

There has never been a better time to expand into remote branch locations. Cloud-based services and an increasingly integrated system of IoT devices make it easier than ever to deliver the same high quality of service and user experience at remote sites as at their centralized brethren—but only if organizations are willing to put in the time, effort, and money to ensure their networks can handle the growing traffic volume without compromising on security, and only if remote site managers are equipped to thrive in such a necessarily complicated environment.

Checking off those boxes requires backing an adaptable, flexible WAN design with internal visibility throughout all branch locations. Visit www.extrahop.com/solutions/initiative/remote-site-monitoring to see how ExtraHop uses real-time analytics and machine learning to give you full visibility, automated asset discovery and mapping, and AI-driven anomaly detection so you can support whatever complexity your organization throws your way!

[1] Forrester Research: https://www.forrester.com/Forresters+2018+Technology+Predictions/-/E-PRE10165
[2] International Data Corporation (IDC): https://www.idc.com/getdoc.jsp?containerId=prUS43511618
[3] Munch, Bjarne; Orans, Lawrence. *How to Balance Performance and Security When Connecting Branch Offices to the Public Cloud*. Gartner. October 17, 2016.
[4] Ibid.
[5] Munch, Bjarne; Rickard, Neil. *Cloud Adoption Is Driving Hybrid WAN Architectures.* Gartner. April 28, 2017.

ABOUT EXTRAHOP

ExtraHop is the first place IT turns for insights that transform and secure the digital enterprise. By applying real-time analytics and machine learning to all digital interactions on the network, ExtraHop delivers instant and accurate insights that help IT improve security, performance, and the digital experience. Just ask the hundreds of global ExtraHop customers, including Sony, Lockheed Martin, Microsoft, Adobe, and Google. To experience the power of ExtraHop, explore our interactive online demo.

Connect with us on Twitter, LinkedIn, and Facebook.

ExtraHop Networks, Inc.
520 Pike Street, Suite 1700
Seattle, WA 98101 USA

www.extrahop.com
info@extrahop.com
T 877-333-9872
F 206-274-6393

Customer Support support@extrahop.com
877-333-9872 (US)
+44 (0)845 5199150 (EMEA)