WHITE PAPER

Ensure Secure Wired and Wireless Networks

Solving the Top Challenges Facing Enterprises Today

Executive Summary

The access layer is the broadest attack surface in an enterprise's network. It supports all network connectivity (via wired Ethernet switches and wireless access points) for employees, contractors, guests, and Internet-of-Things (IoT) devices. With more than 29 billion IoT devices expected to be connecting to networks every day by 2030,[1] proper security to mitigate access layer attacks has never been more crucial.

As enterprises rethink the workplace, the LAN must be reimagined to provide agility, flexibility, reduced risk, and enhanced user experience.[2]

Problems with Existing Access Infrastructure

The local area network (LAN) presents a broad and potentially vulnerable target for cybercriminals, especially at a time when businesses in every sector depend on network connectivity to survive.

Some of the specific challenges that IT organizations face when managing their access layers include:

- Keeping different configurations in sync
- Gaining visibility across the network
- Managing differing levels of access
- High total cost of ownership (TCO)

Enterprises are looking at integrated platform approaches to better manage and secure the network. A solution that combines wired, wireless, and security management is becoming more common as IT groups streamline operational overhead. However, not all networking solutions offer the required simplicity, features, and performance.

Complexity Creates Challenges for LANs

Traditional LAN networks gain complexity as they physically expand due to business growth and adding users and devices. As a result, IT administrators need to keep track of all the different comings and goings. With the deployment of branch and satellite offices, the LAN situation gets steadily more complicated and costly at the operational level.

Managing configuration

- In large campus instances, one small change can disrupt major pieces of the network. Institutions must ensure that any adds, changes, or updates can be tracked and managed to keep all network parts in sync and operational.
- Network deployment at remote sites also presents potential configuration problems. Installing and overseeing a common standard across remote locations and disparate branch topologies can rapidly drain IT resources.

Network visibility

- Campus networks are in constant flux, with devices from employees, contractors, and guests always coming and going. Typical LAN visibility can provide details about the device connection. Still, upper-layer device contexts, such as user authentication and associated resource access limits, can be missing.
- IoT devices pose a particular challenge in terms of visibility. As these devices appear on the network, IT is under pressure to enable the applications they represent without putting the network's overall security at risk. This can be even more difficult in locations without on-site IT staff as the only information on a particular device is what's provided in the access-layer interface.

High TCO

- Modern LAN network manufacturers have tried to solve their complexity issues by adding additional licenses or subscriptions to address the various needs of the IT group. In adding all these features, however, the overall cost of the solution increases by twofold or even threefold over the cost of the networking gear alone.
- In addition, as more systems and overlay tools are brought online to manage and secure the LAN, IT groups become stretched thin, learning and managing all of these different, disconnected solution interfaces.

Security

- As LAN networks get increasingly complex, security across all network ingress points for every variety of authorized network users can also become overly complicated. Many organizations add individual point security products to close gaps one at a time. This complex, disaggregated approach to security can put the entire organization at risk. A single misconfiguration of a LAN security solution can lead to the broader network being breached.

An outdated LAN risks data loss, security breaches, and expensive downtime.[3]

Things to Consider When Evaluating a Solution

When updating a wired and wireless LAN network, there are several considerations that any organization should factor into the decision-making process:

- **Topology structure:** One key aspect of deploying a secure LAN is the nature of the sites where the network will be deployed. Is this a collection of large campuses or several small branches? The solution will often be a hybrid of two or more operational requirements. As each topology comes with its own challenges and limitations, the solution chosen should be extensible and scalable to add value and offer appropriate functionality in each scenario.
- **Connected devices:** What types of devices will be connecting to the network? And who are the different users? The LAN may need to securely give access to guests and contractors with external devices. A good LAN-edge solution should offer capabilities to deal with all types of devices and users as they connect without needing constant involvement from IT staff. Technologies for link aggregation make it relatively easy for network architects to keep up with the growing bandwidth demands of end devices.
- **Low TCO:** While a solution may offer all the above features, the cumulative costs for licensing, enabling, and subscribing to a la carte capabilities can add up. Network decision-makers must keep careful track of how many systems and solutions need to be purchased for the overall desired functionality to work across the entire organization, how many licenses may be required, and if any key features require recurring subscriptions.

  Also, cost of ownership goes beyond capital investment and subscriptions. The amount of staff time that a given solution demands for operations deployment and maintenance can also vary quite a bit. Decision-makers should be prepared to ask how complicated the solution is to manage. Does it work out of the box? Or are multiple "glue" products needed to function correctly?
- **Integrated security:** Many LAN solutions lack built-in security. This requires a bolt-on approach to securing the network after the fact, which adds cost and complexity. Or sometimes, security options are available, but they are not tied into the larger security footprint. This can create "seams" in the network, opportunities for configurations to drift, and for bad actors to take advantage, slipping through the cracks. Networks should be built and maintained within a security context to ensure the best possible protection and minimal impact on managing the LAN infrastructure as a whole.

Secure Access Requires a Seamless Solution

Wired and wireless LAN networks may form the backbone of every enterprise, but they also represent a significant monetary and time investment for any IT group. Picking the right solution helps IT and security teams fully enable and drive company initiatives.

There are many network equipment vendors in the market today, and to ensure continuous operations, IT decision-makers should carefully review all of their options to find a solution that offers deployment flexibility at the access layer with integrated security.

[1] Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2023, with forecasts from 2022 to 2030, Statista, 2023.

[2] Rich Smith, Reinventing the LAN for the future, Orange Business, October, 2023.

[3] Ibid.

March 13, 2024 4:46 PM

762006-C-0-EN