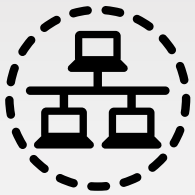
WHITE PAPER

How To Achieve Secured Wired and Wireless Networks

Top Challenges and How To Solve Them

Executive Summary

The access layer offers the broadest attack surface in an enterprise's network. It supports all network connectivity (via both wired Ethernet switches and wireless access points) for employees, contractors, and guests—as well as Internet-of-Things (IoT) devices. With ever-increasing numbers of devices connecting to networks each day, ensuring access layer security becomes a critical need. And with remote working becoming a new standard during the COVID-19 pandemic (and even beyond), proper security to mitigate access layer attacks has never been more important.[1]



Upgrading the campus LAN not only refreshes a neglected part of the network—it can also set the stage toward full, end-to-end management and visibility.[3]

Problems with Existing Access Infrastructure

The LAN edge presents a broad and potentially vulnerable target for cyber criminals—especially at a time when businesses in every sector are depending on network connectivity to survive. And attacks are increasing. For example, in the first quarter of 2020, distributed denial-of-service (DDoS) attacks seeking to overwhelm network connections were 542% higher than the previous quarter (Q4 2019).[2]

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)

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

Complexity Creates Challenges for Local-area Networks (LANs)

Traditional LAN networks gain complexity as they physically expand due to business growth and the addition of users and devices. As a result, IT administrators need to spend more time keeping track of all the different comings and goings. With the deployment of branch or satellite offices and increasing numbers of employees working from home, the LAN situation gets steadily more complicated and costly at an operations level.

Managing Configuration

- In large campus instances, one small change can disrupt major pieces of the network. Organizations must ensure that any adds, changes, and updates can all be tracked and managed so that all parts of the network remain in sync and operational.
- Network deployment at remote sites also presents potential configuration problems. Installing and overseeing a common standard across many 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 coming and going at all times. Typical LAN edge visibility can provide details about the device connection, but it can be missing upper-layer device context such as the user authentication level and any associated resource access limits.
- 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 overall security of the network at risk. In locations without on-site IT staff, this can be even more difficult—as the only information on a particular device is what's provided in the access layer interface.

High Total Cost of Ownership (TCO)

- Modern LAN networks have tried to solve their complexity issues by adding additional licenses and/or subscriptions to address the various needs of the IT group. In the process of adding all these features, 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 edge, IT groups become stretched thin learning and managing all of these different, disconnected solution interfaces.

Mint ut porem eatur aut aut a et quiderciae re niet et re molorem essenis dolorest, cor ataturi aut ipid mi, aut maximperis qui sum sequunt acitio.

Security

- As LAN networks get increasingly complex, security across all network ingress points for every variety of authorized network user can also become overly complicated. Many organizations add on 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.

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**. When looking at how to deploy a secure LAN, one key aspect is the nature of the sites where the network will be deployed. Is this a collection of large campuses or several small branches? Will there be remote workers requiring connectivity? Very often, the solution will 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 so that it can add value and offer functionality that is appropriate in each scenario.
- ✓ **Connected devices**. What types of devices will be connecting to the network? And who are the different users? The LAN must be kept secure if guests and contractors with outside devices will also need access. 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 growing bandwidth demands of end devices.[6]
- ✓ **Low TCO**. While a solution may be able to 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 deployment and maintenance of operations can also vary quite a bit. Decision-makers should be prepared to ask how complicated is the solution to manage? Does it work together out of the box or are there multiple “glue” products needed for it to function properly?
- ✓ **Integrated security**. Many LAN solutions lack built-in security. This requires a “bolt-on” approach to securing the network after the fact, which adds both cost and complexity. Or sometimes security options are available, but they are not integrated with the LAN edge. 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, as well as minimal impact to 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 VPs of IT should carefully review all of their options to find a solution that offers deployment flexibility at the access layer with integrated security to ensure continuous operations.

[1] "In addition to traditional DDoS attacks, researchers see various abnormal traffic patterns," Help Net Security, July 21, 2020.

[2] Ibid.

[3] Andrew Froehlich, "A Network's Weakest Link May be Different Than you Think," Network Computing, November 26, 2019.

[4] Ibid.

[5] Ibid.

www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

April 20, 2021 4:35 PM

wp-FA-challenges-to-achieving-secure-wired-and-wireless-solution

762006-A-0-EN