

Ensure a Secure LAN Edge for All Devices

Table of Contents

Executive Overview	3
Challenges of Ensuring a Secure LAN Edge	4
Effectively Gating Network Access	6
Simple and Secure Network Access From Fortinet	8
Covering the Basics With FortiLink NAC	8
What is FortiLink NAC?	8
How does FortiLink NAC work?	9
Going Beyond the Basics With FortiNAC	9
Conclusion	11



Executive Overview

The rapid growth of personal and Internet-of-Things (IoT) devices connecting to enterprise networks has increased the need to have fine-grained control over what is allowed into the network and with what permissions. Network access control (NAC) solutions can ensure only devices that should attach to the network do, and can restrict what they have access to. But many of these solutions are just as complex as the problem they are trying to solve. Ideally network access control would be streamlined and included with the local-area network (LAN) edge solution for simplicity and consistent security policy.

Fortinet has an innovative solution that enables secure onboarding of myriad devices without the complexity. This eBook will cover why this is needed and how FortiLink provides this functionality.



Challenges of Ensuring a Secure LAN Edge

Onboarding devices and securing the network are often at odds. What's needed is a quick and easy method for those entering the network, but that isn't always achievable following security best practices. Network complexity is on the rise, but there is not a single source to easily address. Complexity increases for a variety of reasons, such as:

- Work-from-anywhere initiatives that result in more bring-your-own-device (BYOD) items entering the network
- On-site guests
- IoT devices

IT teams must handle large volumes of different types of devices connecting to the network, which comes with a lot more exposure than they'd like. Getting all these devices safely onto the network is more challenging since they are not all the same.

Company-owned employee devices can be trusted once they go through rigorous checks, and the endpoint state plus RADIUS or AD authentication would give that device full entry.

BYOD devices, however, require different security and access. There's still user login available, but less direct control of the devices.

IoT is even more challenging, with headless devices that have limited to no security functionality. They're not going to be able to log in with a username and password, and they're notoriously easy to hack and compromise. It's extremely risky to give them access to the entire network.

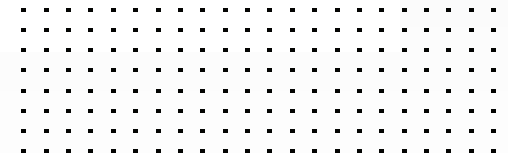
The network needs a way to set the security posture of each device to the correct level at the time of connection, and to do this without making the network needlessly complicated for IT or end-users. There is no need for additional wireless networks or dedicated air-gapped wired networks just to handle these devices. Nor should users need to find the right SSID, go through complex captive portal arrangements, or other complicated steps.

Historically, this is where network access control (NAC) has come into play.





“Shadow IoT devices are creating security holes within organizations that cyber criminals are looking to exploit.”¹



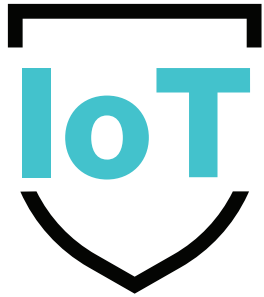
Effectively Gating Network Access

To ensure the network is well-protected, a solution must be able to scale with and handle all the new challenges being thrown at the network operator. This requires functionality that can understand what to do with a wide variety of disparate devices. This is where NAC software solutions traditionally added value. They could monitor each device entering the network and ensure that it was given the correct levels of access and permissions.

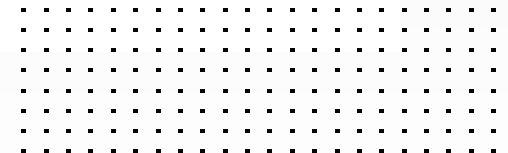
NAC solutions can encompass a large array of features and functionality, and in many cases, they offer a wider solution set than necessary to solve the access problems of most network administrators. It's understandable how this happened, as NAC providers see a need to cover each and every situation that has arisen over time. Unfortunately, this leads to complex solutions that can be costly both in terms of money and the amount of time needed to set up and manage them. Often this leads to vendor lock-in as just the thought of abandoning all the work put into finally making a solution functional, to then start over, is very unpleasant.

The ideal way to solve this overwhelming problem is to have basic NAC services baked into the LAN that are simple enough to not add complexity, and robust enough to cover the required set of use cases.





In cybersecurity terms, IoT devices greatly expand the “attack surface” or the amount of potential areas for cyber criminals to penetrate a secure network.²



Simple and Secure Network Access From Fortinet

Securing edges throughout the network is key to a secure enterprise. The Fortinet Security Fabric enables IT professionals to accelerate digital rollouts without hitting security roadblocks. Creating a secure LAN edge is an important component of increasing IT's agility in support of these initiatives. And effective and efficient network access control is key to achieving a secure LAN edge.

Covering the Basics With FortiLink NAC

Fortinet Security-Driven Networking converges security and networking, in this case to best solve the issues of network administrators needing to securely onboard devices throughout their deployment. Fortinet includes base NAC features on the FortiGate Next-Generation Firewall (NGFW) that can be used with Fortinet LAN equipment (switching and wireless). The feature is called FortiLink NAC, as the technology that converges and controls our LAN equipment with the FortiGate is called FortiLink. All Fortinet LAN Edge equipment, FortiSwitch Ethernet switches, and FortiAP Wi-Fi Access Points (APs) utilize FortiLink to extend firewall policies throughout the LAN.

What is FortiLink NAC?

FortiLink NAC is a rules-based NAC system that allows for automated onboarding of devices onto the LAN. It ensures that they are placed in the proper security context. By leveraging the consolidated security and networking controls in the FortiGate NGFW appliance, it performs NAC services for LAN devices as they attach.



How does FortiLink NAC work?

FortiLink NAC uses a set of prioritized user-configurable rules to determine what to do with a device when it attaches to the network (whether by wire or wirelessly). It places all incoming devices into an onboarding virtual LAN (VLAN) while it processes the correct posture for the device. This ensures that no traffic is passed to the wider network until the correct posture has been set.

NAC rule options

Within the FortiLink NAC system, rules can be set based on device properties (device manufacturer, operating system, etc.), user groups, or EMS tags, and then the device is assigned to specific VLANs. VLAN sub-interfaces are based on interfaces that are used for the VLAN assignment.

Special considerations for IoT

As noted, IoT devices offer a special challenge for network administrators, and it's no different for a NAC system. New devices are introduced regularly. Fortinet offers an IoT service for the FortiGate that keeps a regularly updated list of devices. This service is leveraged with FortiLink NAC to offer the best functionality for NAC rules.

Going Beyond the Basics With FortiNAC

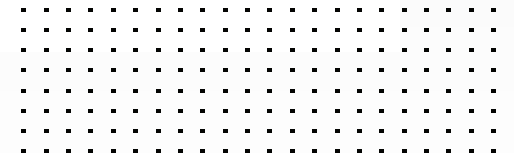
While FortiLink NAC covers the needs of an average deployment, it is not intended for complex or multivendor environments. This is where our FortiNAC offering shines. It offers support for over 2,000 different switch and access point models across a variety of vendors, as well as anomaly detection/MAC spoofing, endpoint compliance scans, and a self-remediation portal.





70%

**of workers are still
using personal
devices for work.³**



Conclusion

As we continue to work from anywhere, time spent on professional and personal devices becomes more fluid, and IT teams need to support more access from more BYODs. At the same time, IoT in the workplace is increasing.

The good news is that organizations can count on FortiLink NAC to deliver network access control, with no expensive investment or complicated deployment and management.

¹ Danny Palmer, "[Rogue IoT devices are putting your network at risk from hackers](#)," ZDNet, February 3, 2020.

² Kate Began, "[5 challenges still facing the Internet of Things](#)," IoT Now, June 3, 2020.

³ "[Security threats increasing with 70% using personal devices for work](#)," Help Net Security, March 16, 2021.



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.