VERIFLOW

Network Segmentation

Network segmentation and micro-segmentation can by design protect prized IT assets. By implementing networks with protected zones of access and reachability, network architects can turn their network into their greatest defender against malicious actors, limiting the effects of a security breach. This tried-and-proven strategy to prevent lateral movement often is underutilized because it is difficult to deploy and maintain in complex, often changing environments. With Continuous Network Verification, Veriflow is creating an easy button for network segmentation.

5 THINGS TO KNOW ABOUT NETWORK SEGMENTATION

1 KNOW WHAT IS WHERE

Being able to identify and map all network devices effectively is critical to implementing any network segmentation strategy. You must be able to acknowledge a device, its location and any risks associated with it. Veriflow dynamically models and maps all network infrastructure devices regardless of vendor in any environment.

2 IDENTIFY THE BUSINESS DRIVERS

Improperly deployed and verified segmentation can raise reachability issues and slow down the business. Knowing the intent of the business and being able to continuously verify that no update or change will adversely impact the intent are key to deploying an active network segmentation strategy.

3 THERE ARE A LOT OF PATHS

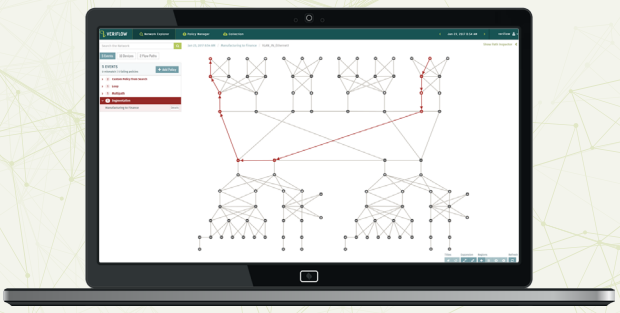
Today's approaches to testing and validation using manual scripts, ping, and traceroute fail to provide any assurance or confidence that network behavior will match business needs and intent. Veriflow mathematically verifies across the entirety of the network that no backdoors allow access to your prized IT assets.

4 CHANGE IS THE ENEMY

Any small change to the network can introduce a new vulnerability and weaken your security posture. Network architects and operation teams need to have the ability to continuously verify that the reality of the network meets the business intent — before, during, and after every change.

5 SEGMENTATION IS NOT SIMPLY 'SET IT AND FORGET IT'

Rules and policies need to be continuously verified to ensure that proper enforcement of the business intent is met. This can be extremely difficult amongst hundreds of devices with hundreds or thousands of rules per device across millions of possible paths. Veriflow enables continuous verification through the use of advanced algorithms that mathematically verify the entire network stays protected, predicting network vulnerabilities before they can be exploited.



Can't Wait?

Book a demo and see how Continuous Network Verification enables Network Segmentation in any networking environment, and learn how you can step into intent-based networking without any network disruption in less than a day.

REQUEST A DEMO

Contact Us (408) 809-1790 info@veriflow.net www.veriflow.net