



The MYTHS of NETWORK SEGMENTATION

Segmentation isn't new, just misunderstood. And with the Internet of Things looming, it's more important than ever.



MYTH #1

Role-based authentication is segmentation.

Using "typical" authentication to provide users access to certain services is not enough. There are a number of ways to break authentication.

Reality Check: Even correctly implemented authentication may not be totally reliable. If attackers gain physical access, they might still exploit software flaws to bypass authentication weaknesses (like pass-the-hash). If you really want to limit access, you need to segment resources at a physical network level too, and not rely entirely on user authentication.



MYTH #2

Switches and VLANs provide adequate network segmentation.

Switches, routers and VLANs won't provide a big enough security bump between segments. Just having something on a separate network, doesn't mean you can apply the proper security policies to traffic between those two networks.

Reality Check: It's been possible to defeat switch-based VLANs for years. It's certainly a good practice, but by no means adequate by itself. But when all you have is a hammer (the switch vendors), everything looks like a nail.



MYTH #3

I passed PCI-DSS, my segmentation must be adequate.

Recent major retail breaches have proven that once hackers get past the front door, they easily can penetrate the most private protected systems.

Reality Check: Configurations change daily and one error on how the network is configured or how the rules on either the VLANs or access control lists are configured, and you have a hole big enough to drive a truck through.



MYTH #4

Setting up many network segments is expensive, and requires multiple security devices/firewalls.

Though traditional firewalls only supported a limited three-pronged network (WAN/LAN/DMZ), and didn't offer extra security services, modern solutions now allow you to configure many secure network segments without breaking the bank and installing many appliances.

Reality Check: Today's next generation firewalls and UTM appliances offer many independent ports, which you can use to segment your network into multiple trust zones. They also provide a full suite of security services, allowing you to configure advanced security policies between each segment. You can now get truly secure segmentation at a great price.



MYTH #5

Network segmentation is just not a top business priority.

In a recent worldwide survey*, more than half of respondents said that segmentation is just not a top priority on their security list.

Reality Check: Many don't perceive network segmentation as a priority since it doesn't seem to offer direct business benefits. Yet, they forget that not properly segmenting may result in huge business costs. The Target® breach is a great example — attackers transformed access to an external partner portal into full access to Target's systems. True segmentation would have made it harder for attackers to jump from one network to another.

**WatchGuard® Firebox M440 makes it easy to
apply the right policies to the correct network
segment – without complex configurations.**

Clear up the myths. Get the facts.
Go to WatchGuard.com/FireboxM440



*WatchGuard Worldwide Survey, September 2014