



Facts & FAQs: Port-based Access Control

FACTS:

Probably one of the most important challenges that DISA (Defense Information Systems Agency) faces today is ensuring that only authorized and qualified users gain access to protected DoD (Department of Defense) assets.

To solve this problem, in December 2008, DISA released a Security Technical Implementation Guide (STIG), which (essentially) requires all DoD networks be controlled at the switch port. By controlling traffic at switch ports rather than at the perimeter of the network, both internal and external threats can be mitigated.

FAQs:

Does DISA stipulate the need to implement a network access control solution?

The DISA STIG states that, "Network ports should be both physically and logically secured to prevent unauthorized access to the DoD enclave." It goes on to say that, "Both unclassified and classified networks require the implementation of a logical network port security solution." The DISA STIG does not specify what type of technology must be used to secure network ports, it just says that it must be done.

Don't all NAC solutions provide port-based access control?

Some do, and some don't. And some do only in certain situations. Take 802.1X for example. Many NAC solutions require the deployment of 802.1X to provide port base access control. This is unfortunate for those organizations that have yet to deploy it or are not in a position to deploy it. Some solutions meet the DISA STIG requirement in a multitude of environments including those with and without 802.1X deployed.

So no matter what you call it, the key to fulfilling the DISA STIG requirements is to control access at the switch port?

Yes, but it goes beyond just that. The key is to implement port-based access control in a scalable way without blowing your operations budget. Agencies can meet this requirement through "port-based security" whereby an individual asset is associated with a specific switch port. This type of security is extremely resource-intensive to maintain because the network administrator needs to manually modify switch configurations anytime a device is added or moved. Also, the drawbacks of this approach are highlighted in the DISA STIG: It is very easy for someone to spoof individual machine (MAC) address and connect to the network -- bypassing this type of solution.

Are there products – or educational resources – that can help IT staff meet the DISA STIG requirements for port-based access control today?

Absolutely. In fact, the Army has an approved product list which lists the network access control products that have been tested, proven and certified to work "as advertised". It's called the United States Army Information Assurance Approved Products List (AIAAPL). Products on the AIAAPL must complete a rigorous series of tests to meet the Army's high standards, such as successful testing at the Army Technology Integration Center (TIC), FIPS-140-2 Level 2 compliance, receipt of Common Criteria certification (Evaluation Assurance Level 2, with EAL4 pending), and more.

ForeScout CounterACT is among the products listed on the AIAAPL – and the only NAC solution listed. CounterACT does many of the things described above (and other things, as well). It works with other products on the AIAAPL – such as vulnerability scanners, active asset management tools, switches, identity servers, endpoint protection software, etc. – to help build and maintain asset inventories and make sure only authorized users and devices gain network access.

To learn more:

Look to the AIAAPL "recommended list of products" and the vendors listed there: IT staff are asked to trust and use only those solutions that have been certified and added to the list, so this will save you some time.

Also, visit:
iase.disa.mil/stigs/stig/index.html
forescout.com/DoD