Patton Fuller Community Hospital: Section III (Week 4)  
Nate Bachmeier  
May 26, 2014  
NTC/362: Networking Fundamentals  
Facilitator: John Buono

# Patton-Fuller Community Hospital: Section III

Patton-Fuller is redesigning their network to include remote access via VPN to various staff members and WLAN support within the building. Now that the system has been designed and implemented, the next phase is to choose hardware and security solutions.

# Identify Hardware and Software to Protect the Network

The Hospital’s network will contain lots of Personally Identifiable Information (PII), which is a high value target for hackers and other attackers. To keep it safe and secure hardware and software solutions need to be added to the environment.

## Network Access Protection (NAP)

According to the Security Intelligence Report, it is becoming the norm for attackers to begin launching exploits within ten to thirty days of the patch being released (Microsoft, 2013, p. 5). Given the significant risk presented here, the first step would be to ensure a good patch management story is in place.

On solution is called Network Access Protection (NAP), which has a server component and a client side State Health Validator (SHV). After installation the clients will contact the DHCP server to get routing information. The DHCP server will reply with a challenge that various patches need to be installed or other business policy is being followed. The SHV will compute a response and give it back to the DHCP server (Microsoft, 2014).

If the response is valid, the device is given full access to the network. Otherwise the device is quarantined such that it can only communicate with the software updating and deployment infrastructure. After applying all the patches, the SHV will send another request for routing information and finally be allowed to join the rest of the network.

## Web Application Firewalls

Having a good patch management story prevents vulnerabilities that are publicly known and fixed. The next set of risk comes from known unknown vulnerabilities in the supporting systems of the Network Operating System (NOS). For instance there might be a SQL injection vulnerability in the website that no one has discovered yet.

To mitigate this risk Web Application Firewalls (WAF) can be installed at critical junction points throughout the network. As traffic flows through the WAF deep packet inspection is performed to find signs of malicious intent. If the traffic is classified as malicious it can be audited and dropped, before reaching the protected system (ex: web server) (Wikipedia, 2014).

## Virtual Local Area Networks

Another protection that can be applied is the deployment of Virtual Local Area Network (VLAN), which “providing a layer-2 network that is partitioned to create multiple distinct broadcast domains (Wikipedia, 2014).” This allows multiple networks to exist within the same physical network.

Once the network is partitioned it would be possible to define trust zones such as the web server can talk to the database server, but a person in radiology could not directly talk to the database server. Preventing unexpected traffic from being routable can significantly reduce attack space and increase the complexity of exploit.

# Distinguish Between Area Networks

There are a lot of achromous for area networks such as LAN, PAN, MAN, WAN, WLAN, etc. They each act more or less the same with the differences being seen in the scope of the network and the protocols used by them.

If the network is very small, such as around a single person; then it is a Personal Area Network. As the network gets larger it will encompass a handful of devices and become a Local Area Network. Growing out over an entire city is a Metropolitan Network. As the network spans multiple cities or long distances then it becomes a Wide Area Network.

# Building Blocks of a Network

## Hub

A hub is a simple device that accepts multiple connections and funnels them into a single upstream connection. The responses back from the upstream are then broadcasted to all ports. This enables scenarios such as easy auditing of network traffic or two computers sharing a single cable modem.

## Switch

Similar to hub is a switch which takes traffic from many locations and aggregate it for an upstream connection. This helps make traffic patterns more efficient and removes the need to have thousands of ports on our edge routers. Unlike a hub the responses are only sent to a specific port instead of a broadcast.

## Router

A router is a hardware device that takes data from one network and moves it to another network. For instance your edge router moves the traffic to the upstream ISP’s network. Another key feature of routers is they often implement firewalls and Network Address Translation (NAT) services. Both are useful to defense in depth strategies.

# Conclusion

Security is a real concern that needs to be handled across the network. This can be addressed by deploying hardware and software solutions such as Network Access Protection (NAP), Web Application Firewalls (WAF), and Virtual Local Area Network (VLAN) technologies.

In addition to selecting the proper security equipment it is also important to select the correctly network building blocks, such as routers and switches. Having the right tool for the job will make the network more efficient and easier to manage.

# References

Microsoft. (2013). *SIR Volume 16*. Retrieved from http://download.microsoft.com/download/7/2/B/72B5DE91-04F4-42F4-A587-9D08C55E0734/Microsoft\_Security\_Intelligence\_Report\_Volume\_16\_English.pdf

Microsoft. (2014). *Network Access Protection*. Retrieved from MSDN: http://msdn.microsoft.com/en-us/library/windows/desktop/aa369712(v=vs.85).aspx

Wikipedia. (2014). *Application Firewall*. Retrieved from Wikipedia: http://en.wikipedia.org/wiki/Application\_firewall

Wikipedia. (2014). *VLAN*. Retrieved from Wikipedia: http://en.wikipedia.org/wiki/VLAN