**Week 5 Comprehensive Review**  
Nate Bachmeier  
June 2nd, 2014  
NTC362: Networking Fundamentals  
University of Phoenix  
Facilitator: John Buono

# Week 5 Comprehensive Review

## Include a timeline for the project.

The project could be implemented in phases over the next 3-6 months. The first phase would be to install any IPSec and additional authentication services. Once those have been tested next the wireless access points can be installed and associated with the authentication solution. The third phase would be to order any services from the ISP for site to site connectivity.

## Explain the design approach and rationale.

The design approach is a highly open system where it is easy for anyone to authorized person to join the network. Once they are connected authentication and authorization policy limits where their traffic is permitted to flow. This allows for central administration and the ability to dynamically grant or deny end users.

## Analyze the detailed design.

The detailed design follows the same design as the normal design. When remote employees want to connect into the network, they will connect across a VPN connection. The connection will then be associated with the IPSec policy and have the same effect as if the traffic originated within the LAN.

## Prove that the design meets the data rate requirements.

Using standard Wireless-N will give connectivity of up to 300mbps. This will more than exceed the requirements of most users. If the traffic is degrading below an optimal point then it is possible to scale out with more hardware. For the VPN users standard cable Internet, gives 20-50mbps which will be sufficient for transmitting and receiving the requests. Once the requests are submitted they will primarily flow between machines on the LAN which is backed by high speed cabling.

## Analyze the existing security situation in the organization.

The existing security solution meets the immediate needs of the organization, but will be completely superseded by the new implementation.

## Identify the predominant electronic and physical threats to communications networks.

The largest threat would be someone connecting to a physical port or getting an authentication password to join the network. In both cases this threat is mitigated by requiring the Kerberos login to being the secure channel.

There is also a risk with any boundary boxes as they do not require the secure channel to being the communication. If one of those was compromised the attacker would be able to initiate a secure channel to another device.

## Explain the importance of explicit enterprise security policies and procedures.

If the organization does not have a clear direction and a well-defined set of actions and reactions; then it will be difficult to efficiently run the organization. For instance if the business is always consistent then auditing will be easier to complete.

## Describe potential threat detection and protection techniques.

Threats can be identified through Network Intrusion Detection Systems. These solutions can perform deep packet and look for signs of an attack. A sign might be a stream of binary NOP or known shell exploit code. Similar to antivirus signatures for attacks can be created and used to detect many attacks.

## Describe how firewalls mitigate some network attack scenarios.

A firewall is a device that looks at inbound or outbound traffic and then makes a decision based on business policy. For instance if a local service needs to listen on port 1234, a firewall can be used to say only the local machine can communicate with this port. It is also possible to define network ACLs for the firewall, such as machines in 1.2.3.0/24 are allowed to communicate with local port 1234.

## Describe common security concerns inherent to wired, wireless, and mobile networking.

Wired has the inherent risk that anyone can plug in and begin communication with other devices. This can be mitigated through policy and configuration but it is not the default behavior. Wireless poses a risk that it is a broadcast technology, where multiple receivers can listen to the traffic. To mitigate this encryption such as WPA2 can be deployed to keep communication secure between sender and receiver. Mobile networking runs the risk that all traffic by default is flowing across a potentially hostile collection of public networks. Anything that is not encrypted can be read or tampered with along the hops.