Hardening your perimeter

Network Access Control

Network Access Control (NAC) is an approach to computer security that attempts to unify endpoint security technology (such as antivirus, host intrusion prevention, and vulnerability assessment), user or system authentication and network security enforcement.

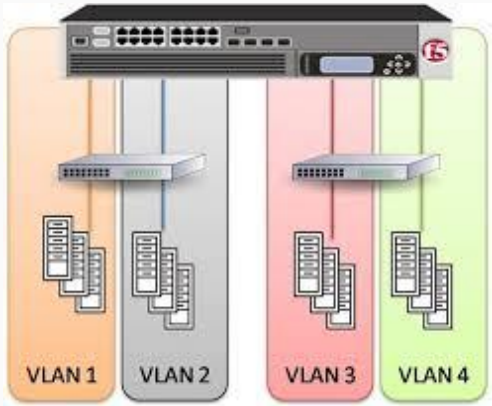
Network Access Control aims to do exactly what the name implies control access to a network with policies, including pre-admission endpoint security policy checks and post-admission controls over where users and devices can go on a network and what they can do.

Internet Protocol Security(IPSEC)

IPsec encapsulates communications in a layer of encryption that is difficult to break, but it also allows you to restrict communications to and from certain machines based on whether their machine certificates are signed and valid.

By doing this, the machines restricted by IPsec would simply ignore it, even if an exploit was introduced into your network. Using IPsec in this way also forms the basis for using network access control.

Virtual Lans(VLAN)



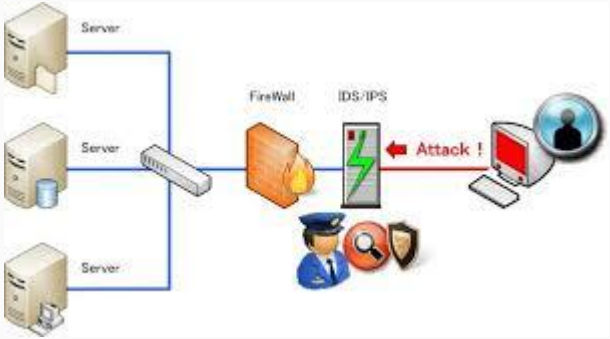
VLANs are essentially multiple logical boundaries created within one physical network.

VLANs are an easy way to divide critical areas of your network from others.

You could have one VLAN for servers and another for client machines, or you could segregate machines based on department, or any other scheme you choose.

Creating a VLAN in and of itself doesn't necessarily create a layer of protection, but it forms the basis for any number of other hardening techniques, and it provides a way to limit the scope of security procedures to only the most critical areas of a network.

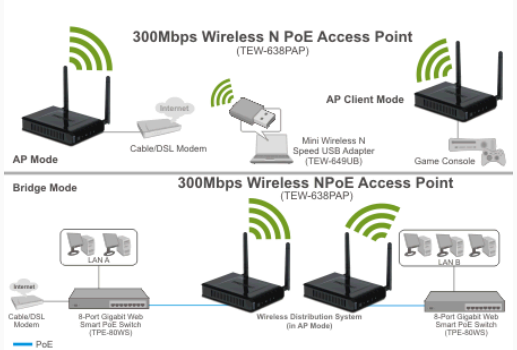
Intrusion Detection/Prevention System(IDS/IPS)



Intrusion detection/prevention systems often use heuristics that can detect malicious activity on your network before an actual definition is created by anti-virus and anti-malware vendors.

IDS/IPS systems also provide a solid foundation for forensic analysis in case you care to examine how an exploit entered your network or penetrated your network defenses.

Wireless Access Point Encryption



Simply using media access control (MAC) filtering and not broadcasting your service set identifier (SSID) are methods that just do not cut it anymore in a corporate setting.

WEP has been cracked numerous times and even the ankle biters will have no trouble gaining access to your wireless network protected only by WEP/WPA2.

★ Authenticate with RADIUS or LDAP.

Stateful Firewall & Perimeter Defense

Perimeter defense is the first, best and most effective way to protect against zero-day exploits in a variety of forms.

To help prevent your network from being a vector of delivery for a nasty vulnerability, deploy a firewall immediately. Better yet, deploy a security appliance and perform regular audits.