Campus Security Measures

by Christopher Iwen

and Jane Whelan

Devry University

04/03/2016

One of the most important things we will be doing is setting up access control lists on every Layer 3 device blocking any connection originating from outside the network. Assuming the gateway ip address is 192.168.1.1 an example of this would be #access-list 101 permit tcp any 192.168.1.1 255.255.255.255 established #access-list 101 deny tcp any any. We will also be using ACL’s to turn off all unused ports to prevent intruders from exploiting a service that we aren’t even using.

We will be setting up separate OSPF areas for the DMZ, the backbone, and each building. The DMZ will contain the Email server, citrix server, cloud storage, and HTTP server all on separate VLAN’s. The cloud storage will be running a Linux OS and scanning all incoming files for virus using the Clam Anti-virus tool. Linux is the best OS to do the job because most viruses are made for Windows and won’t have any effect at all on the Linux server. The webserver will force all connections to use HTTPS for more security. This means if someone is capturing packets on our network they will still need to decrypt the data to to make any use of it. Just inside the DMZ we will have our network DHCP server, private DNS server, and Database server containing usernames and passwords for students and faculty. The passwords are required to be at least 10 characters in length and include at least one uppercase, one lowercase, one number, and one special character. All users will be required to change their passwords every 60 days, and the password cannot be reused. The command #access-list 1 deny 192.168.1.1 255.255.255.255 will be used to create an ACL that will protect these device from any connections originating from the gateway. This means that only connections originating from inside the network will be able to have access to our DHCP, DNS, and Login Database. The DHCP server will also try to set the DNS addresses to our DNS server. Having our own DNS server assures that no one inside our network will be sent to a malicious website via a DNS redirect hack. It also means that we can simply remove listings for urls that we don’t want people going to, and unless they have another DNS setup the webpage will be unreachable.

We will setup the Gateway to deny pings (config)#access-list 102 deny icmp any any (config)#access-list 102 permit ip any any (config-if)#ip access-group 102 in. The DMZ itself will have two firewalls protecting the network, one on the outside and one on the inside of the DMZ.

We will be using Network Address Translation overload ( more commonly known as Port Address Translation) on our edge router to hide the actual IP addresses on our network, using the command #ip nat inside source list 1 interface serial 0/0/0 overload. Each 3750 switch will be setup to act as a router on a stick and will also be preforming PAT. This means that anyone snooping on the inside of our network will still have a difficult time figuring out what IP addresses are connected and mapping the entire network. By doing this we make it a little harder for the attacker to target and take over computers on campus.

All unused ports will be shutdown to prevent anyone from hooking a device to them, and being granted network access. We will have a total of 70 VLANS. Each 2960 switch will have its own VLAN setup to prevent devices connected to other switches from being able to directly communicate with computers that it shouldn’t. Two 3750 will also be setup to have VLANs, one for the Pixar offices and one for the Security/ IT office. We will also have one VLAN in each building for the Wi-Fi access points to connect to. By segregating the network this much we limit the number of devices that hackers can gain contact with. All 2960 switches, except Nassau Residence, will have sticky mac addresses set up on every port that is not connected to another switch using the command #switchport port-security mac-address sticky. These ports will also have BPDU guard setup to prevent someone from connecting a switch to them. The ports connected to other switches will all be configured as trunk ports to handle traffic from each VLAN in case of a network device failure and for load balancing. Because Nassau is a residence we assume that new devices will get plugged into the network all the time so we won’t be limiting the number of Mac addresses available on each port.

Each buildings switches will be cross connected for redundancy. This means that if one networking device goes down then only the end devices connected to it will lose connectivity. All other devices will still have a connection through other switches and will be able to route around the problem. We will be using Spanning Tree Protocol on every switch to prevent switching loops form happening.

Our campus wide Wi-Fi will have two SSID’s. The first one will be hidden from the public and exist only for students and faculty. The information for the hidden SSID will be available from our IT/ Security department and will allow full access to the intranet. Connection to this network will require a valid username and password that is unique to each individual and are only given to students and faculty. The public SSID will be broadcast and open for use by anyone on the campus. The public SSID will only allow access to the internet, not to local network services. We will be heavily logging all activity on the network to help us block or prosecute anyone using it for devious purposes. Once connected to the network the user will be redirected to a webpage requiring them to accept our terms of use. This should prevent intruders from having an easy way onto our private network, and give us some idea of who did what and how to prevent it in the future.

For Physical security we will have cameras on each floor monitoring entrances, exits, hallways, and stairwells. All students and faculty will be required to carry photo id badges with rfid chips to gain access to buildings. The lobby of each building will have a security guard to monitor camera footage, and keep shady people out, as well as prevent tampering with devices.

Our security room will have one way windows lining the offices so that they can see who is coming without being seen in case of camera failure. The cameras in the hallway will monitor everyone who comes and goes, including who enters the security office. The Main Distribution Frame (MDF) equipment is kept in a locked room inside the security room. The security room requires an rfid card and finger print reader to gain access. Once inside the security room the door to the MDF room will have an electronic lock with keypad and inside it will have cages with pad locks protecting the switches and routers from physical tampering. This means in order to gain access to the MDF room you have to pass multiple checks against who you are, what you know, and what you have. There will be several cameras inside the MDF room monitoring everything that goes on. One of these cameras will be inside the cage making it harder for an intruder to physically tamper with all the cameras, even once he is inside the MDF room. All security computers in every building will also require a chipped card to be inserted to a card reader, if the card is removed the computer locks down. These chips will be part of the security team’s normal badge but will not be part of the faculty and student’s badges. Chip readers will also be connected to any terminal that can SSH into the servers. ACL’s will be used to restrict all other IP’s from creating remote connections to the server room. Telnet will not be allowed anywhere on our network.

That does it for our current security plan. We believe this is a good way to secure the network. But this doesn’t mean that we will stop there. We will continually monitor the network and run our own pen testing to make sure everything is up to date and secured now and in the future.