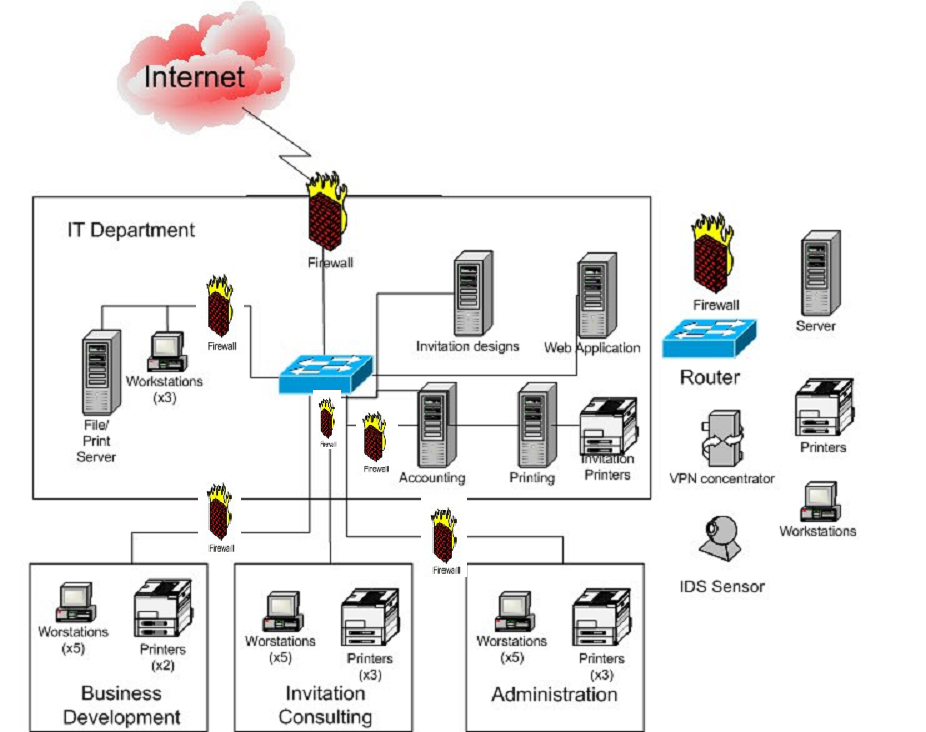
# Week 2 – Course Project

## 11/11/18

## **Group 6:** Noah Bentzler, Sheena Bibee, Terance Cooley, Roman Kovtun, Dean Reiner Jr

**Problem 1:** Review the network diagram and make recommendations on where you would place additional firewalls to filter network traffic, provide a 1 paragraph explanation

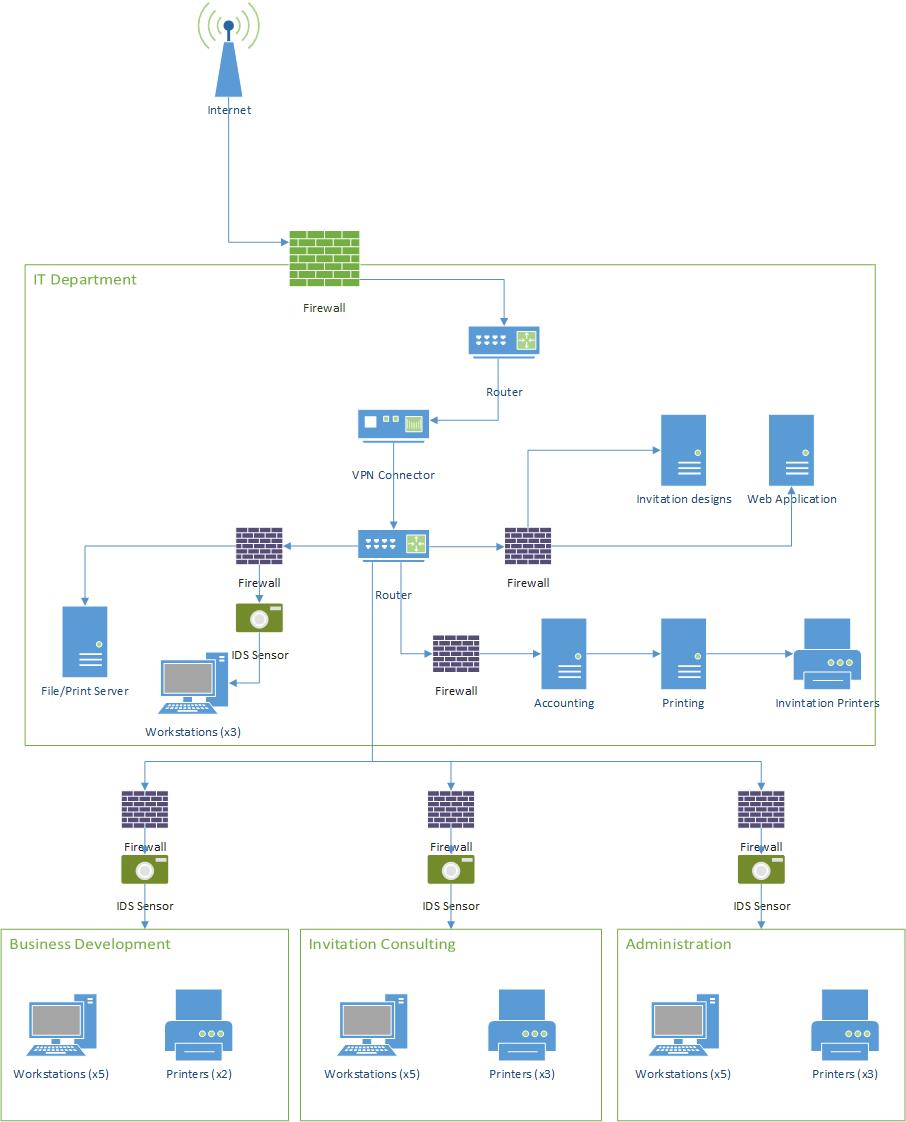
**Proposed Solution:** In order to maximize security, I would recommend including a Stateful Packet Firewall as the outer protection and implementing standard Packet Firewalls as a secondary line of defense for all connections coming out of the Router except for the web application itself. To defend areas most likely to contain sensitive or internal dates, this would include a second defense for: the connection to the 3 IT Workstations and File/Print Server; shared connection to the 5 Invitation Consulting Workstations and printers along with the Invitation Designs server; the connection to the Accounting server and printers; and the 5 Administration Workstations and printers. A first line Stateful Packet Firewall greatly reduces the risk of a DOS attack by either flooding with packets or authentication requests, since Stateful Packet Firewalls filter out suspicious traffic based on previous packets within the same IP conversation but do not require user authentication. A second line of defense through standard Packet Firewalls on separate portions of the network may discourage a potential attack from continuing and isolate the attack to one area if it continues.



**Problem 2:** Review the network diagram and make recommendations about where to place a VPN concentrator, and where (and how many) Intrusion Detection Sensors (IDS) to monitor for malicious traffic, provide a 1 paragraph explanation.

**Proposed Solution:** For the following network diagram, it requires an additional VPN Connector and IDS sensor on each computer. As you can see below, each computer has IDS Sensor to detect the threat before it hit the workstation. It means that if the firewall fails and before the system lock down the virus. IDS Sensor will tell us which firewall was failing to protect. In addition to the VPN Connection it should be installed between two routes. The reason of this type of the location is because all signals that will go from the router will be secured with a specific call to specific VPN server that was called to. It means that outside systems will detect the public IP, but when it hit the router it will reroute it to different IP address that will be hidden from the public eye.

*Updated network diagram included on next page based on combination of responses to Question 1 and Question 2.*



**Problem 3:** Review the open ports returned by the provided nmap scan.  Find any critical vulnerabilities that are associated with each port.  One critical vulnerability per port is sufficient.  Provide a description of the vulnerability and how it can be remediated (i.e., fixed, usually by applying a patch).

**Proposed Solution:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Port** | **Product** | **Vulnerability** | **Fix** |
| 135 | Msrpc  System= Microsoft | DCOM  If this port is left open a hacker can use epdump (Endpoint Dump) and immediately identify every DCOM-related server/service running on the users hosting computer. | Many ISPs’ now will automatically block this port because of how vulnerable it is, many other recommend closing the port permanently as it won’t affect anything by doing so. |
| 139 | netbios-ssn  file and print sharing  system= Microsoft,SMBA | TCP netbios-ssn are made over 139. These connections are used to support connection oriented file sharing. By default File and Print sharing binds to everything , including TCP/IP, instead of just the local network. Unless it is configured properly this could make all of your shared resources all over the internet. | The main way to fix this problem is to ensure patches are installed and current and configuring the settings correctly. |
| 427 | Svrloc  System= MacOS and NetWare | Service Location Protocol  ExtremeZ-IP.exe in ExtremeZ-IP file and print server does not verify a certain number of URLs match with the packet length, this can allow hackers to use denial of service or daemon attack. | Proper configuration along with patch updates can help mitigate against attacks on port 427. |
| 445 | microsoft-ds  system = Microsoft | Microsoft Directory Services  Port 427 is a smb meaning server message block. Port 427 is used for communication over a lan connection. The port is open in order to use lan communication. | When attacked it is done via LAN and is usually malware looking for weak security settings.  Best way to protect against attacks is using current patches, using a proven anti-malware program, and implementing strong passwords. |
| 1025 | NFS-or-IIS  System = Microsoft | Dynamic allocation, when a program asks for the next available slot 1025 is given. | Keeping current patches installed will help protect this port. |
| 22 | SSH | The Secure Shell Protocol  SSH is command access line, it was used to replace Telnet. Could be used for as an encrypted tunnel for communication.  Free ssh allowed hackers to be able to cause a denial of server crash. | Patches are the best way to avoid attacks. |
| 80 | Apache | HTTP  Hyper Text Transfer Protocol which listens for a web client. Worms and backdoor functionality are the biggest threats in port 80. | Patches and proper configuration need to be done to help protect against attacks. |
| 111 | Rpcbind  System = linux | RPC program number mapper  Converts RPC program numbers into universal addresses. | Proper configuration and patches are most affective at stopping attacks. |
| 6000 | X11  System = linux | X11 provides basic framework for a GUI. Accepts connections from anywhere, remote hosts are the biggest risks. | Proper configuration and patches are the most effective at protecting against these attacks. |
| 32771 | Sometimes-rpc5  udp  System = linux | Sometimes a rpc port on Solaris box. | Patches and proper configuration are the most effective at protecting against these attacks. |

Sites used to for port analysis:

<https://www.speedguide.net/port.php?port=139>

<https://www.speedguide.net/port.php?port=1025>

<https://www.grc.com/port_445.htm>

<http://www.bnsmidwest.com/resources/Ports_exploits_trojan_virus%20List.htm>