DHCP, Firewall and VLAN Requirements for Mount Olive Servers in Church/School Network

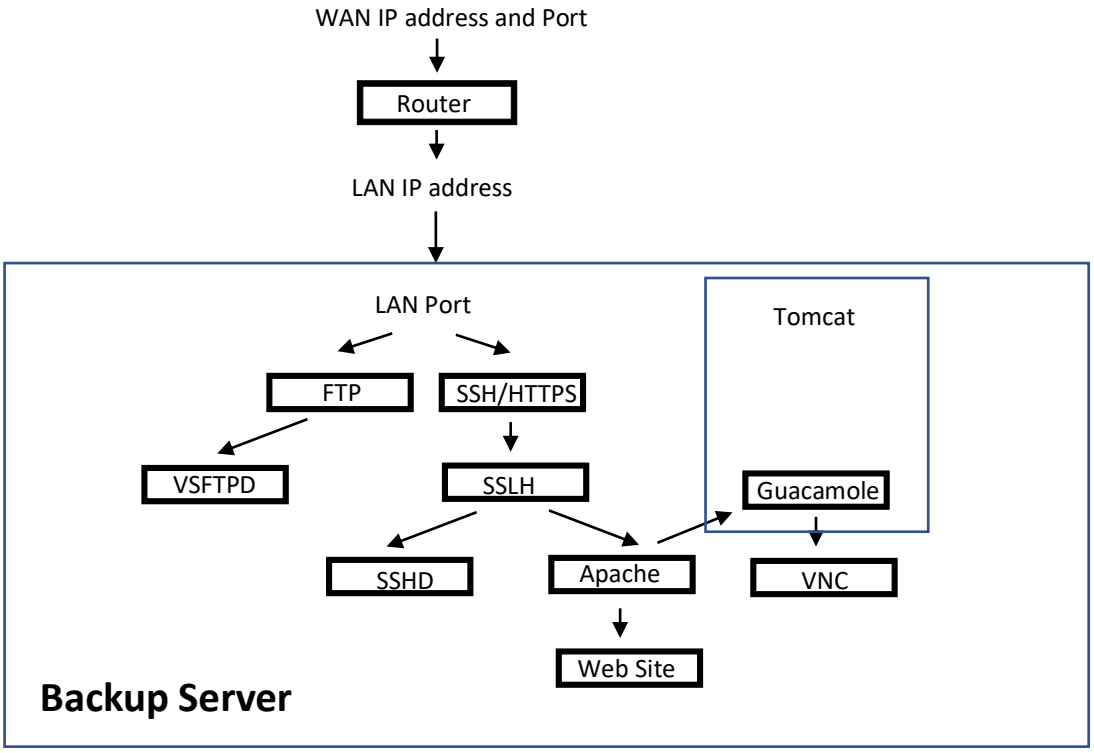
Dan Nessett
6/12/23

This document specifies the DHCP, firewall and VLAN parameters in order to integrate two servers into the church/school network. These servers are: 1) A Backup Server that backs up web server data on the church/school web sites hosted by IONOS and the data on the School Laptop server, and 2) a School Laptop server that manages the school student laptops, providing parental controls, anti-virus and malicious software detection/elimination and laptop configuration management.

Both servers are in the upstairs crawlspace next to Alicia McCall's classroom. This is the location of the 24-port switch.

The Backup Server

The Backup Server architecture is shown in the following figure:



The Backup Server provides the following services:

- An FTP server that accepts weekly backup data sourced by the church/school web servers hosted by IONOS. It also provides backup storage for the School Laptop server. Access to the FTP server uses the traditional FTP protocol, rather than SFTP. This is a requirement of the Wordpress plugins available for backing up the web site. SFTP support is not free and would require payment of $80/year for the upgrade, which is not authorized by the Parish Council.
- A web server (apache2) that supports Home School courses provided by the Mount Olive Homeschool COOP and also Remote Desktop access using the VNC protocol.

Access to the Backup Server from the WAN side of the church/school network for management purposes requires passing SSH traffic through the church/school router and firewall. HTTPS and SSH traffic are multiplexed over the same IP port using the SSLH application. Support of HTTPS and SSH on the Backup Server necessitates NAT/Firewall rules that allow the passage of this traffic. HTTPS supports both the web server and VNC remote desktop access to the Backup server.

The Backup server requires opening ports in the router/firewall to allow both WAN and LAN FTP and HTPPS/SSH traffic from clients to reach the server. The Backup server resides in its own private Subnet space. The subnet assigned to the Backup server is 192.168.50.X, X in [1,2] and the Backup server's assigned address is 192.168.50.2 (192.168.50.1 is reserved for the router on the 192.168.50.X subnet). Since the Laptop server uses the Backup server to store home directory backups (see next section), it is necessary to specify here the subnet assigned to the laptops and the address of the Laptop server. The laptops reside in subnet 192.168.1.X (X taking a value in the interval [2,199]). The Laptop server is assigned the address 192.168.1.200.

Given these subnet values, the following DHCP and Firewall rules support Backup Server operations.

- The Backup server must accept connections from the WAN side of the router for both FTP and SSH/HTTPS traffic.

- The use of FTP, rather than SFTP means the Backup server is potentially vulnerable to hacker attacks. Therefore, the Backup server resides in its own private subnet space and is prevented from originating traffic. That is, it is only allowed to respond to requests from clients. This configuration implements a DMZ.

- To mitigate successful port scans by hackers attempting to penetrate the Backup server, the NAT rules for the Backup server use non-standard ports for FTP and HTTPS/SSH traffic.

- The web server on the Backup server machine will support Home School course material that needs to be accessible both from the School laptops and from the WAN side of the router (so students can access course material for homework assignments). The former allows the management of the Backup server from any school laptop.

- In addition, in order to back up the School Laptop server, the router allows LAN traffic from the local subnet address of the laptops to the Backup server subnet.

The Firewall and NAT forwarding rules that implement this configuration are:

- All response traffic from the Backup server to WAN or LAN initiating traffic is allowed. No originating traffic from the Backup server is permitted.

- The NAT forwarding rules map an arbitrary WAN source address and WAN destination port 20554 to LAN address 192.168.50.2 and destination port 443 for HTTPS/SSH management traffic from the WAN side.

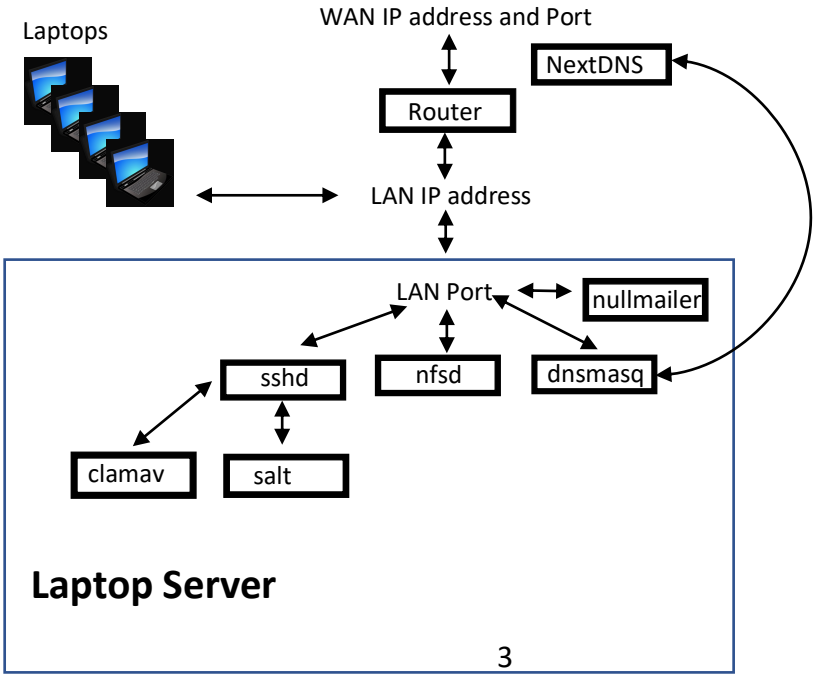
- The NAT forwarding rules map a LAN source address 192.168.1.X, where X is in the interval [2,255], and destination port 443 to LAN address 192.168.50.2 and destination port 443 for HTTPS/SSH management traffic from the LAN side.

- The NAT forwarding rules map an arbitrary WAN source address and WAN destination port 20550 to LAN address 192.168.50.2 and destination port 20550 for the FTP command channel.

- The NAT forwarding rules translate an arbitrary WAN source address and WAN destination ports 20551-20553 to LAN address 192.168.50.2 and destination ports 20551-20553 for three FTP data channels (three ports are necessary, since both the church and school web sites initiate backups at the same scheduled time and it may occur that the Laptop server makes FTP requests during this period.)

The Laptop Server

The Laptop Server architecture is illustrated by the following figure:



The Laptop server provides the following services:

- Each laptop is configured to support an account for every student in the school. Home directories for these accounts are provided by the NFS daemon (nfsd) that runs on the laptop server. The NFS server requires the laptops to be assigned an address within a CIDR block in order to authorize them to access the home directories on the NFS server. This CIDR block is 192.168.1.1/24.

- The clamav antivirus application runs nightly to scan for infections in the /home directories mounted on the Laptop server. This action is triggered by a cron job and if it finds any infections, it notifies the Laptop server administrator via email (using the nullmailer application). An ssh session (between a remote computer and the sshd daemon) configures the clamav application on the Laptop server.

- Each laptop is configured using the SALT distributed configuration application. A SALT client (known as a minion) is installed on every laptop, as well as on the Laptop server. The SALT controller application (known as the master) is installed on the Laptop server. Configuration commands are issued by the SALT master to the SALT minions via remote access over an encrypted channel.

- The Laptop server provides DNS services to each student laptop through the dnsmasq caching/forwarding DNS server. It obtains authoritative DNS information from NextDNS, which implements parental controls through a Mount Olive School account. Teacher laptops do not use the dnsmasq caching/forwarding service and therefore are not constrained by the parental controls. For example, NextDNS prevents students from accessing YouTube, whereas teacher laptops are no so constrained.

Given these service requirements, the following DHCP, Firewall, VLAN configuration is required:

- The addresses allocated by DHCP to the laptops should come from a compact address block, which for exposition purposes is assumed to be 192.168.4.X, where X is in the interval [2,199]. This requirement comes from the access control logic of the NFS server, which grants the ability to mount home directories based on the client IP address. The Laptop server is allocated the address 192.168.1.200.

- All other traffic between the WAN side and LAN side of the church/school network is initiated by processes running on the Laptop server. Services include: 1) use of nullmailer to send an email when virus infected files are discovered by clamav in home directories of students (nullmailer forwards email using port 465); and 2) a caching DNS service (the dnsmasq server accepts DNS requests from laptops on port 53 and makes upstream DNS requests to the NextDNS service on a WAN machine also on port 53).

The firewall rules to achieve these objectives are:

- All initiating traffic from the Laptop Server to the WAN is allowed.

- All response traffic from the WAN to the Laptop server is allowed.

- All initiating traffic from the WAN to the Laptop Server is blocked, except for the following exception.

- Allow arbitrary WAN source address and WAN destination port 20555 -> LAN address 192.168.1.200 and LAN destination port 22 for SSH management traffic.

- All traffic to/from 192.168.1.X from/to 192.168.1.X is allowed, where X is in the interval [2,255].