Presentation

Authors

- Antoine de Barbarin
- Nicolas Moyon
- Sabrina Eloundou

In this project, we will describe and explain an IT solution for a small business setting up a private local network connected to internet, in which there are 5 devices:

> - a firewall,
> - a web server,
> - a backup server,
> - a linux client,
> - a Windows client.

The **web server** hosts a web documentation of the business's network solution, and it should be reachable from inside or outside the private local network.

The **backup server** needs to periodically save the web server's files so that it can be rolled back anytime to a previous pristine/stable/working version.

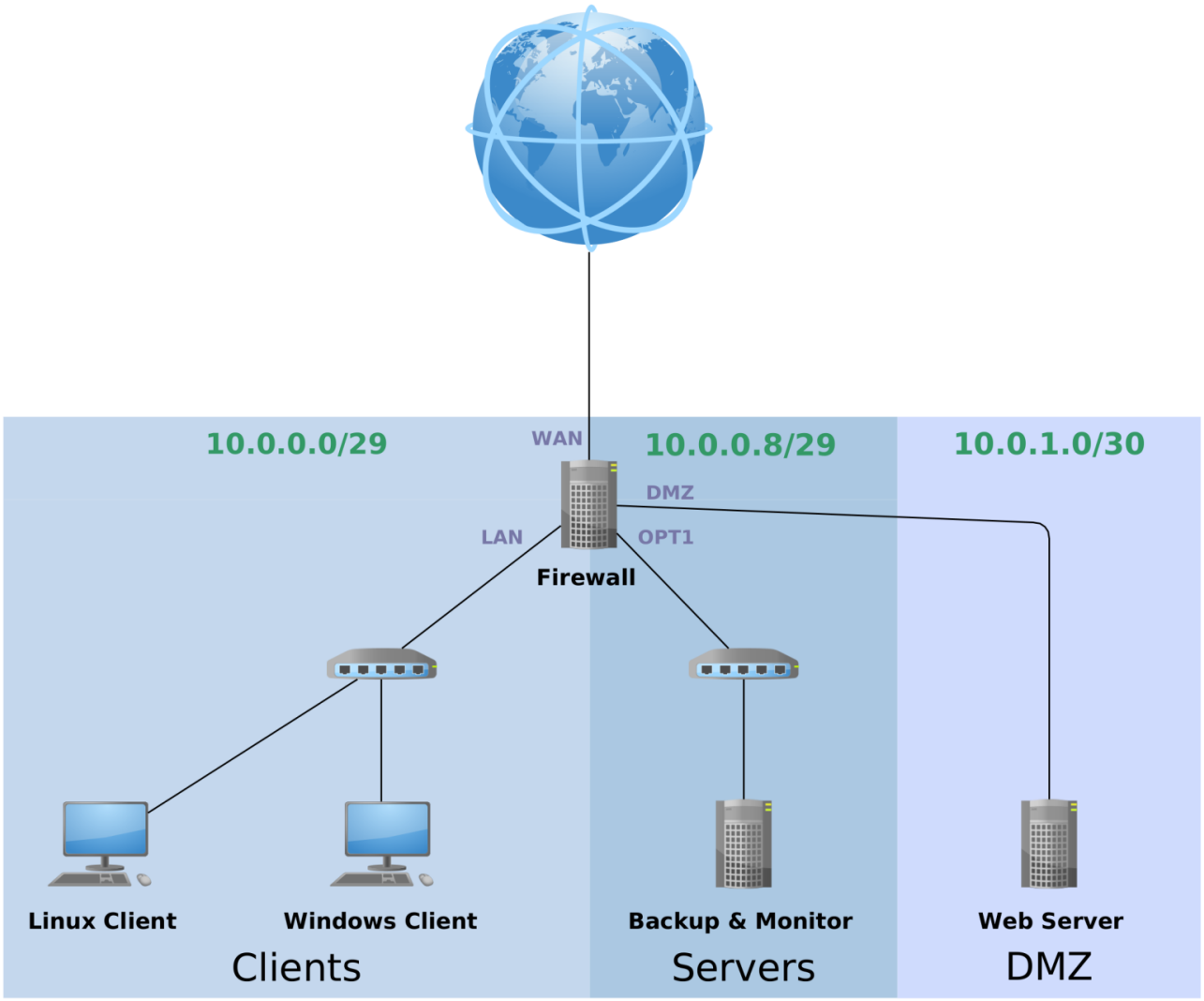
The **clients** are standard desktop workstations intended for general employee use within the corporate office environment. Both fulfill the same function but utilize distinct operating systems: Windows and Ubuntu.

IP addresses

devices \ networks	10.0.0.0 /29	10.0.0.8 /29	10.0.1.0 /30	Other
Firewall	**LAN** 10.0.0.1	**OPT1** 10.0.0.9	**DMZ** 10.0.1.1	**WAN** DHCP (from ISP)
Web Server	---	---	10.0.1.2	---

devices \ networks	10.0.0.0 /29	10.0.0.8 /29	10.0.1.0 /30	Other
Backup Server	---	10.0.0.10	---	---
Linux Workstation	DHCP (10.0.0.2)	---	---	---
Windows Workstation	DHCP (10.0.0.3)	---	---	---
{style="both"}				

Overview



There are few things in the graphic just shown:

- the firewall is the only device directly connected to the exterior, to internet
- the servers and client are on three different subnets inside the business's LAN
  - firewall's LAN interface for clients

    - firewall's OPT1 interface for backup server (and any other internal server that may be needed in the future)
    - firewall's DMZ interface for web server (extendable only when changing the subnet mask from /30 to a lower one)
- the three different sub-LANs are differentiated through the firewall's DHCP and the three physical LAN interfaces (LAN, OPT1 and DMZ on pfSense)
- each sub-LAN (except the DMZ) has a switch of its own, and it can be extended if necessary (up to 6 devices per subnet with the current subnet mask for LAN and OPT1 interfaces)
- the web server is a sensitive point in the current architecture, because of the access from outside the business's private network, that's why it is put in a DMZ, to isolate it from the rest of the network. Also, it will have no access to the other subnets and scheduled access to internet (for updating purposes). Others, however, may access it through SSH, in very defined rules present in the firewall: from the Linux workstation and the backup server, the former for administration purposes, and the latter for backup purposes, as its name suggest it.

Revision #6
Created 9 August 2024 08:33:24 by Admin
Updated 9 August 2024 09:45:57 by Admin