Configure the correct IP ranges to enable a VPN Firewall to work in conjunction with an existing Router.

This document describes the steps to undertake in configuring an existing router to work in conjunction with a VPN Firewall (for example FVX538v1/v2, FVS318, FVS336G, FVG318, FVS338).

The document is to be considered as a guideline and the User will need to adapt the information provided to his/her specific requirements.

Table of Contents

Existing connection to the Internet

It is assumed that the User already has a setup that allows a connection to the Internet as per below diagram:

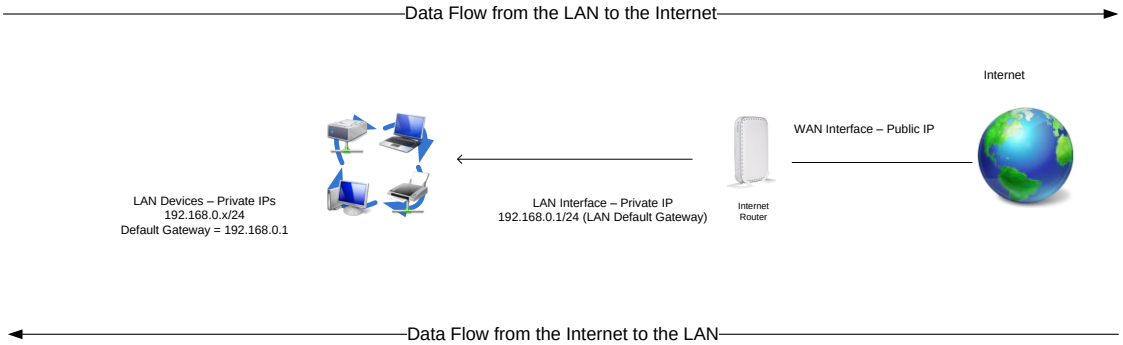


Diagram 1

In the Diagram 1 scenario we have an Internet router configured to access the Internet, with the LAN devices working on the range 192.168.0.x (where x can have a value from 2 to 254).

This is a scenario where single-NAT (Network address translation) takes place.

Considerations when introducing a VPN Firewall in the existing setup

When introducing a VPN Firewall (router) some considerations will need to be made with Regards to the configuration of different IP ranges.

The User will be presented with the following generic scenario:

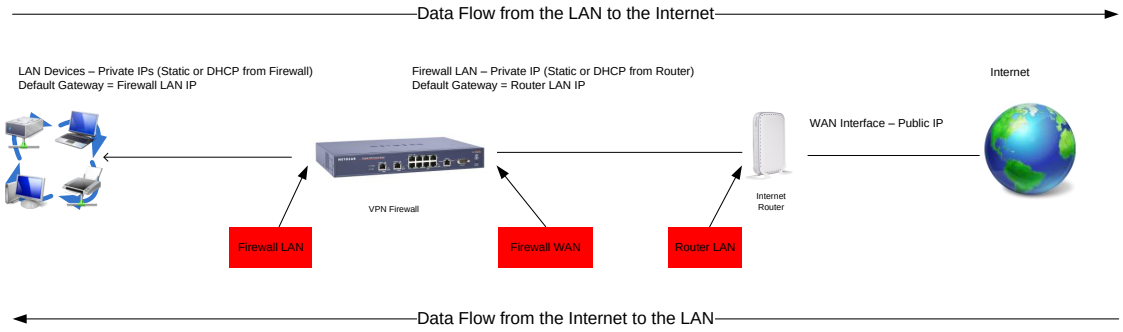
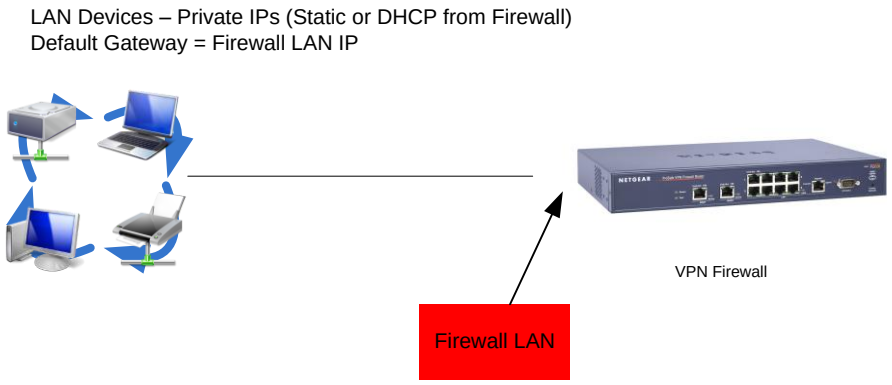


Diagram 2

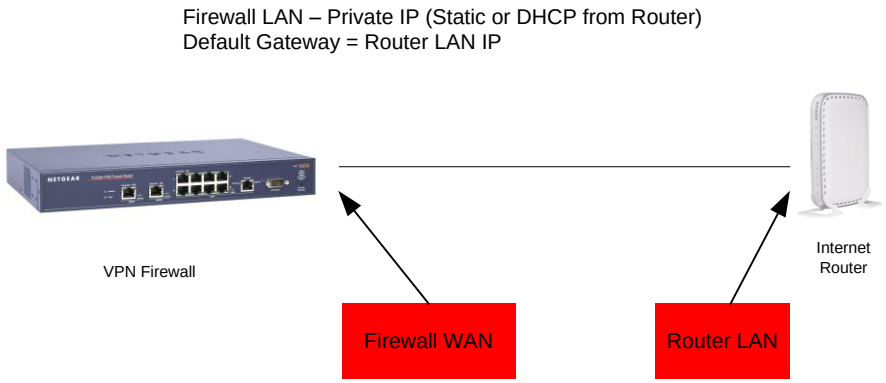
Effectively having two different networks to configure:

- A network including the Firewall LAN and all the LAN devices behind the VPN Firewall

NOTE to Diagram 1: the notation /24 is related to the subnet mask (in this case a 24 bits subnet mask = 255.255.255.0)



- A network including the Firewall WAN and the Router LAN interfaces



Due to the nature of routing – the IP ranges used in each of the two networks has to be unique and dependant on the subnet mask used.

The User has therefore two options:

Reconfiguration - Option 1

Maintain the exiting setup on the **Router LAN** interface (in this example with IP 192.168.0.1 and subnet mask 255.255.255.0) and configure:

- The **Firewall WAN** Interface with an IP address in the same range (for example 192.168.0.2 and subnet mask 255.255.255.0, and default gateway 192.168.0.1 (matching the **Router LAN** address)

  The DNS servers (primary and secondary) will be configured depending on the User's requirement either to be the **Router LAN** address or the Public DNS IPs obtained by the ISP

- The **Firewall LAN** Interface with a private IP address in any range except the range already used (in this case 192.168.1.1 will be used with subnet mask 255.255.255.0)

- The **LAN devices** will be configured either statically with an IP address in the range 192.168.1.x with subnet mask 255.255.255.0 and default gateway 192.168.1.1 (matching the **Firewall LAN** address) or dynamically to receive DHCP settings from the Firewall

The obtained network will show as:

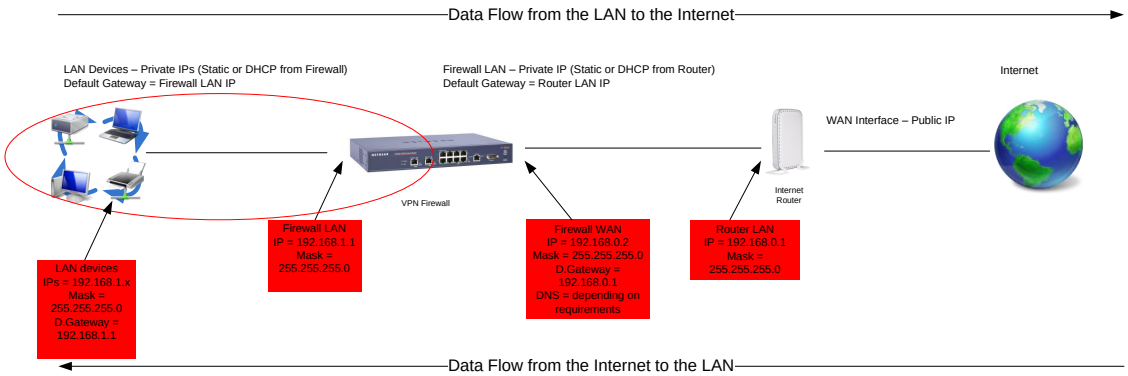


Diagram 3

Reconfiguration - Option 2

The user might require to maintain the current range of address used on the **LAN devices** (see Diagram 1) on the new LAN – the **Firewall LAN**.

In this case the following configuration will need to take place:

- The **Router LAN** Interface will be configured with an IP address in a different range than the previously used one (192.168.1.1/24 as per **Diagram 1**).
  For example the Interface will be configured with an IP address as 192.168.1.1 with subnet mask 255.255.255.0.

- The **Firewall WAN** Interface will be configured with an IP address enabling it to communicate with the new **Router LAN** interface IP.
  For example 192.168.1.2 and subnet mask 255.255.255.0, and default gateway 192.168.1.1 (matching the **Router LAN** address)

  The DNS servers (primary and secondary) will be configured depending on the User's requirement either to be the **Router LAN** address or the Public DNS IPs obtained by the ISP

- The **Firewall LAN** Interface with a private IP address in any range except the range already used between the **Firewall WAN** and **Router LAN** (in this case 192.168.0.1 will be used with subnet mask 255.255.255.0)

- The **LAN devices** will be configured either statically with an IP address in the range 192.168.0.x with subnet mask 255.255.255.0 and default gateway 192.168.0.1 (matching the **Firewall LAN** address) or dynamically to receive DHCP settings from the Firewall

In this scenario therefore the IP range 192.168.0.x which was used in the network between the **Firewall WAN** and **Router LAN** has now been shifted to the network between the **Firewall LAN** interface and the **LAN devices**.

The obtained network will appear as:

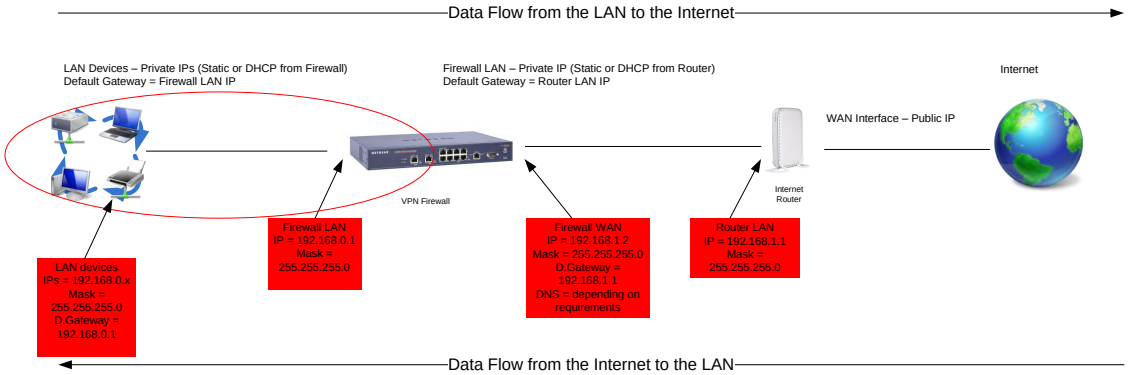


Diagram 4