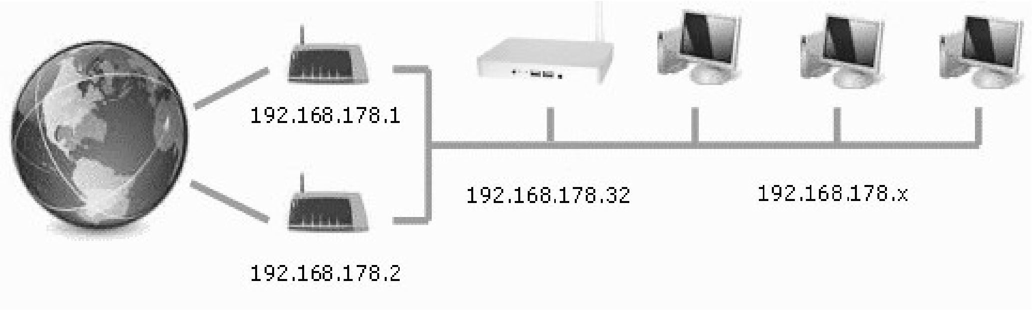
NAT32 Supplementary Router **25. July, 2016**

1. Introduction

A supplementary router is an IP router that resides in a home or office network for the purpose of providing participating machines with additional features and services that the main router cannot (or will not) provide. The supplementary router is simply added to the home network via an Ethernet or WiFi connection, and machines that wish to use it must either request a DHCP lease from that router or manually configure their TCP/IP stack to use that router. No configuration changes are required on the main router, although it is advisable to disable the router's DHCP Server. The supplementary router software can be run on any PC running Windows 7 or higher. The many low-cost mini-PCs running Windows 8.1 or Windows 10 currently on the market are ideally suited for this purpose, because their performance characteristics are more than adequate and because they use very little power (typically 5-10 Watts).



The above diagram illustrates how the NAT32 Supplementary Router (192.168.178.32), running on a PiPO X7 mini-PC, is added to an existing local area network that connects to the Internet via (in this case) two DSL Routers.

2. Features and Benefits

The main components and features of the NAT32 supplementary router are:

2.1 A DHCP server has been implemented that can configure user machines in a flexible manner. Parameters such as DNS Server address and Gateway address are configurable on a per-machine basis. One can therefore specify that some machines use a specific DNS server and gateway, whilst other machines continue to use the main router's DNS Server and Gateway.

2.2 A DNS server has been implemented that can analyse DNS names and resolve black-listed names to the address of the supplementary router itself. DNS analysis can also be used to specify names that are to be reached via a different gateway such as the client end of a VPN connection. To this end, the router installs a host-specific route that causes all traffic to the resolved address to be routed via the VPN connection.

2.3 HTTP and HTTPS honeypot servers have been implemented that provide safe "dummy" content to machines requesting data from known malware distribution and tracking sites as specified in a HOSTS list. Black-listed

DNS names also resolve to the address of the honeypot and subsequent HTTP requests are fulfilled by the honeypot without delay. This protects machines from malware attacks and information leakage, and it also significantly reduces web page download times.

2.4 A special built-in Web Browser allows web pages to be previewed in a safe mode that queries each source prior to access. This allows the user to determine the names of sites serving undesirable content and to add those names to the black list. The black list can be edited at any time by users with administrator rights.

2.5 Sharing of one or more VPN connections amongst participating machines and to route traffic to certain sites via a particular VPN connection is also possible. Communicating via a VPN adds an additional level of encryption that the user's Internet Service Provider has no control over. The ISP can record that a VPN connection has been established, but it is not possible to record details of the traffic passing over that connection.

2.6 OpenVPN connections are fully supported. The desired connection can be started or stopped via a small web app that can be run on a mobile device.

2.7 Multiple Internet connections are supported so that certain traffic can be routed via an additional DSL connection or an additional Mobile Internet connection that is only used during periods of heavy traffic.

2.8 A traffic management (user admin) feature allows Internet access to be controlled on a machine-specific and user-specific basis.

2.9 A traffic monitoring feature allows all traffic (including VPN traffic) to be monitored in real time via a proprietary monitor implemented within the supplementary router or via an external traffic monitor such as Wireshark. In addition, traffic to and from the Internet side of the author's main router (an AVM FritzBox 7390) can be monitored in real time via Wireshark.

3. Installation and Configuration

The NAT32 Supplementary Router software requires no installation and can be run directly from a USB Drive or an SD Card. However, if all supported features are to be made available, the WinPkFilter Device Driver from ntkernel.com must first be downloaded and installed. That driver is freely available for personal use.

Initial configuration consists of selecting network interfaces from a list and then specifying to which kind of network (Internet or Private) the interface connects. Subsequent configuration tasks include specifying black lists, specifying static or dynamic DHCP configurations, and configuring the desired VPN connections.

4. Performance

The NAT32 Supplementary Router was tested on a PiPO X7 mini-PC fitted with a 1.6GHz quad-core INTEL Z3736F CPU, 2 GB DDR3 RAM and a 100 Mbps Ethernet adapter. The WiFi adapter was configured to support a separate private address space, and it was only used for allowing guest devices to access the Internet. The machine came with a preinstalled copy of Windows

8.1 with Bing and was modified to prevent the system from entering the Connected Standby mode. This was necessary to ensure that the machine operated continuously, and the modification consisted of changing just one value in the Registry. A few additional modifications were needed to allow Remote Desktop access and headless operation.

As expected, the machine was able to effortlessly handle the traffic on a typical home network of approximately 4 desktop computers, 4 mobile devices, two smart TVs and a NAS. CPU usage was evenly spread over the four cores and never exceeded 6% per core. The machine remained cool to the touch at all times, and power usage was typically under 7 Watts, with occasional brief spurts of up to 10 Watts.

5. Summary

The NAT32 Supplementary Router dramatically improves the web browsing experience because of its ability to block the download and execution of large amounts of unwanted Javascript code and third-party advertising content that many sites inflict upon their visitors. Much of the blocked Javascript code serves no useful purpose, and is simply there to detect ad blockers and to pass private information on to dubious tracking sites.

Protection against ISP-logging practices can be achieved though the sharing of a VPN connection, albeit with the penalty of reduced throughput. However, the throughput penalty depends to a large degree on which VPN service is used, the geographical location of the VPN server and the location of the website being accessed.

It is also important to note that NAT32 never performs network address translation on traffic from a local machine if its next-hop address is that of the main router, and so the dreaded double-NAT issues that plague some networking applications never arise. In fact, NAT32 only performs address translation on traffic from devices connected to the WLAN, and then only if that WLAN is configured to use a private network address that differs from that of the main router.

Local DNS resolution times are always well below a few milliseconds, even when a large host table lookup needs to be performed. Through careful selection of names in the black list, even IP address detection attempts via the various WebRT mechanisms can be rendered futile.

Many beta testers of the software were pleasantly surprised by the improved speed and appearance of web pages when accessed via the NAT32 Supplementary Router.