This unit builds on the GNS3 setup from U18.

21.1 At your (Web-)Service

After setting up the internals of the company network, you decide to get started with the web server. To save a little bit of money you decided to set up an old machine as the web server inside the office network.

- Adjust your address plan and gateway-configuration for an additional subnet you will be using for the web server.
- Place a *www*-node into the subnet and configure its network parameters using a static IP address. (You can access the interfaces file from the node configuration dialog)
- Configure your DNS server to resolve the name `www.startup.local.` to the web server's IP address
- Verify your setup by trying to access the web server from each of the department networks.

21.2 Securing the Network

Now that you setup the web server it is time to think more about security. Before we open up our network to the outside world, we have to configure some firewall rules.

Design a firewall to be installed on `gateway` realizing the following policy. Use a **whitelisting** approach.

- Services running on `gateway` should not be accessible from the Internet
- Everyone should be able to browse the web site.
- Each department network should be able to to access the other.
- The department networks should be able to access the internet without restrictions.
- The server network should not be able to access the department networks (but still the departments should be able to access the web server).
- The servers should only be able to establish connections to the Internet using *HTTP* and *HTTPS* (ports 80/tcp and 443/tcp)
- ICMP messages required for proper IP operation should not be blocked by the firewall. All other ICMP message types should be blocked.

21.3 Opening Up

The last step in building our network is enabling Internet access for the employees and making the web server available to the outside world.

Unfortunately our ISP does not supply us with a complete subnet (or even a static ip address), but just one publicly routable IP address which is chosen randomly every 24h.

In order to make the web server accessible to the outside world we have to configure our gateway to forward requests to the HTTP port to our web server.

- Enable Internet access for all departments as well as the server network (in accordance with the security policy).

- Setup iptables rules to forward and allow access to the web server from the Internet.

- Verify your configuration (e.g. by attaching a *webterm*-node to the hub/switch between the gateway and the Internet).

21.4 Tunneling Through

Business is booming. A big company has approached you and your colleagues. They are asking you to help them with a big networking project. In order to be closer to the customer it is agreed that a few of the engineers will work in a new branch offce close to the new customer.

The new branch office will have to be connected to your main network. Since dedicated network connections are too expensive, you opt for using the available Internet connection by setting up some tunnels.

- Modify your address plan to accommodate the branch office (IPv4 and IPv6).

- Setup a remote site with an independent gateway (hostname `branch`, connected to the Internet) and at least one workstation.

- Setup Internet connection for the workstation(s) at the remote site (DNS resolution, NAT, ...).

For the sake of simplicity we will set up an *unencrypted* tunnel, which is obviously *not secure*, but sufficient for this tutorial.

- Setup an ipip tunnel between `gateway` and `branch`.

- Setup a 6in4 tunnel between `gateway` and `branch`.

- Update your firewall configuration on `gateway` to allow tunnel traffic through the firewall if necessary.

- **Challenge Task:** Make sure you can ping workstations at the branch office from `gateway`, workstations at the main office from `branch`, as well as the internal addresses of the respective remote gateway.

Hints:

- Don't worry about persisting the tunnel configuration for now. Since the outside connections of the office gateways use dynamic IP addresses, just set up a temporary tunnel on the shell.
- Tunnel interfaces do not necessarily require ip addresses.
- Pay special attention to the routing table.
  - Show the routing table: `ip route show`
  - You can get detailed information about the kernel's routing decision for a specific destination using the command `ip route get <dest. ip>`