

Parameter	Static Route Configuration
Destination	The destination address of a packet
Netmask	The subnet mask which forms, in combination with the destination, the network to be addressed. A single host can be specified by a netmask of 255.255.255.255, a default route corresponds to 0.0.0.0.
Gateway	The next hop which operates as gateway for this network (can be omitted on peer-to-peer links)
Interface	The network interface on which a packet will be transmitted in order to reach the gateway or network behind it
Metric	The routing metric of the interface (default 0), higher metrics have the effect of making a route less favorable
Flags	(A)ctive, (P)ersistent, (H)ost Route, (N)etwork Route, (D)efault Route

The flags obtain the following meanings:

Flag	Description
A	The route is considered active, it might be inactive if the interface for this route is not yet up.
P	The route is persistent, which means it is a configured route, otherwise it corresponds to an interface route.
H	The route is a host route, typically the netmask is set to 255.255.255.255.
N	The route is a network route, consisting of an address and netmask which forms the subnet to be addressed.
D	The route is a default route, address and netmask are set to 0.0.0.0, thus matching any packet.

Table 5.53.: Static Route Flags

5.4.2. Extended Routing

Extended routes can be used to perform policy-based routing, they generally precede static routes.

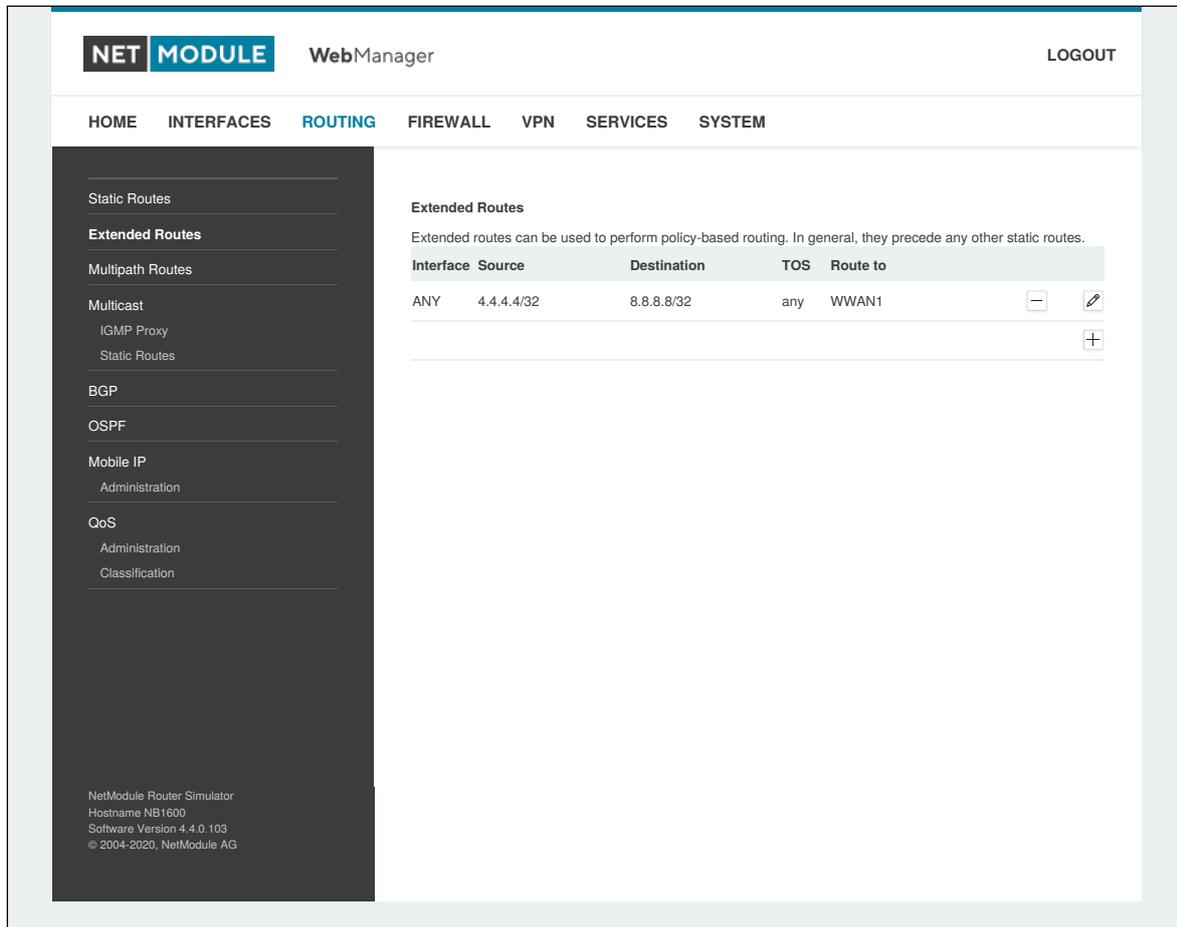


Figure 5.25.: Extended Routing

In contrast to static routes, extended routes can be made up, not only of a destination address/netmask, but also a source address/netmask, incoming interface and the type of service (TOS) of packets.

Parameter	Extended Route Configuration
Source address	The source address of a packet
Source netmask	The source address of a packet
Destination address	The destination address of a packet
Destination netmask	The destination address of a packet
Incoming interface	The interface on which the packet enters the system
Type of service	The TOS value within the header of the packet
Route to	Specifies the target interface or gateway to where the packet should get routed to
discard if down	Discard packets if the specified interface is down

5.4.3. Multipath Routes

Multipath routes will perform weighted IP-session distribution for particular subnets across multiple interfaces.

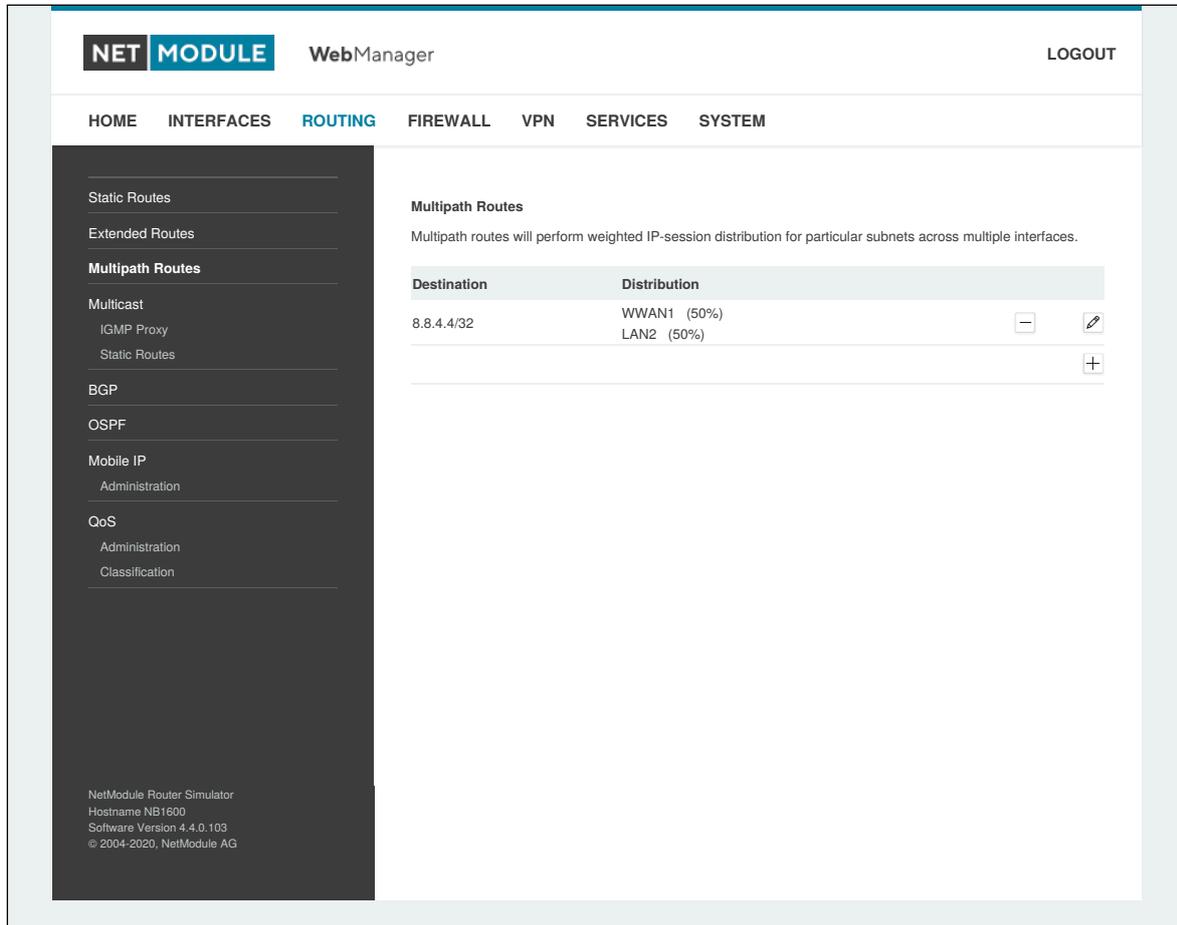


Figure 5.26.: Multipath Routes

At least two interfaces have to be defined to establish multipath routing. Additional interfaces can be added by pressing the plus sign.

Parameter	Add Multipath Routes
Target network/netmask	Defines the target network for which multipath routing shall be applied
Interface	Selects the interface for one path
Weight	Weight of the interface in relation to the others
NextHop	Overrides the default gateway of this interface



Parameter	Static Multicast Route
Group	IP address of MCR group
Source	Source-IP of the packets
Incoming interface	Interface to the packet source
Outgoing interface	Interface to forward the packets to



Parameter	BGP Networks
Prefix length	Length of the prefix to be distributed

5.4.7. Mobile IP

Mobile IP (MIP) can be used to enable seamless switching between different kinds of WAN links (e.g. WWAN/WLAN). The `mobile node` hereby remains reachable via the same IP address (`home address`) at any time, independently of the WAN link being used. Effectively, any WAN link switch causes very small outages during switchover while keeping all IP connections alive.

Moreover, NetModule routers also support NAT-Traversal for mobile nodes running behind a firewall (performing NAT), which makes mobile nodes even there accessible from a central office via their home address, and thus, bypassing any complicated VPN setups.

The `home agent` accomplishes this by establishing a tunnel (similar to a VPN tunnel) between itself and the `mobile node`. WAN link switching works by telling the `home agent` that the WAN IP address (called the `care-of address` in MIP terms) of the `mobile node` has changed. The `home agent` will then encapsulate packets destined to a `mobile node's` home address into a tunnel packet containing the current `care-of address` of the `mobile node` as its destination address.

To prevent problems with firewalls and private IP addressing, the MIP implementation always employs reverse tunneling, which means that all traffic sent by a `mobile node` is relayed via the tunnel to the `home agent` instead of directly being conveyed to the final destination. This fact also empowers MIP to be used as a lightweight VPN replacement (without payload secrecy).

The MIP implementation supports RFCs 3344, 5177, 3024 and 3519. For applications requiring vast numbers of mobile nodes, interoperability with the Cisco 2900 Series `home agent` implementation has been verified. However, since NetModule routers implement a `mobile node` as well as a `home agent`, a MIP network with up to 10 mobile nodes can be implemented without requiring expensive third party routers.

If MIP is run as a `mobile node`, the following settings can be configured:

Parameter	Mobile IP Configuration
Primary home agent address	The address of the primary <code>home agent</code>
Secondary home agent address	The address of the secondary <code>home agent</code> . The <code>mobile node</code> will try to register with this <code>home agent</code> , if the primary <code>home agent</code> is not reachable.
Home address	The permanent home address of the <code>mobile node</code> which can be used to reach the mobile router at any time.
SPI	The Security Parameter Index (SPI) identifying the security context for the mobile IP tunnel between the <code>mobile node</code> and the <code>home agent</code> . This is used to distinguish mobile nodes from each other. Therefore each mobile node needs to be assigned a unique SPI. This is a 32-bit hexadecimal value.
Authentication type	The used authentication algorithm. This can be <code>prefix-suffix-md5</code> (default for MIP) or <code>hmac-md5</code> .



Parameter	Mobile IP Configuration
Shared secret	The shared secret used for authentication of the <code>mobile node</code> at the <code>home agent</code> . This can be either a 128-bit hexadecimal value or a random length ASCII string.
Life time	The lifetime of security associations in seconds.
UDP encapsulation	Specifies whether UDP encapsulation shall be used or not. To allow NAT traversal, UDP encapsulation must be enabled.
Mobile network address	Optionally specifies a subnet which should be routed to the <code>mobile node</code> . This information is forwarded via Network Mobility (NEMO) extensions to the <code>home agent</code> . The <code>home agent</code> can then automatically add IP routes to the subnet via the <code>mobile node</code> . Note that this feature is not supported by all third party <code>home agent</code> implementations.
Mobile network mask	The network mask for the optional routed network.

If MIP is run as a home agent, you will have to set up a home address and network mask for the home agent first. Then you will need to add the configuration for all mobile nodes which is made up of the following settings:

NET MODULE WebManager LOGOUT

HOME INTERFACES **ROUTING** FIREWALL VPN SERVICES SYSTEM

Static Routes
Extended Routes
Multipath Routes
Multicast
IGMP Proxy
Static Routes
BGP
OSPF
Mobile IP
Administration
CoS
Administration
Classification

Mobile IP
Mobile IP can be used to move from one network to another while maintaining a permanent IP address and thus avoiding that running IP sessions (including VPN tunnels) must be reconnected.

Administrative status: mobile node
 home agent
 disabled

Primary home agent address:

Secondary home agent address: (optional)

Home address:

SPI:

Authentication type:

Shared secret:

Life time:

MTU:

UDP encapsulation: enabled disabled

Mobile network address: (optional)

Mobile network mask: (optional)

NetModule Router Simulator
Hostname NBT600
Software Version 4.4.0.103
© 2004-2020, NetModule AG

Figure 5.27.: Mobile IP

Parameter	Mobile IP Node Configuration
SPI	The Security Parameter Index (SPI) identifying the security context for the tunnel between the mobile node and the home agent. This is used to distinguish mobile nodes from each other. Therefore each mobile node needs to be assigned a unique SPI. This is a 32-bit hexadecimal value.
Authentication type	The used authentication algorithm. This can be prefix-suffix-md5 (default for mobile IP) or hmac-md5.



Parameter	Mobile IP Node Configuration
Shared secret	The shared secret used for authentication of the <code>mobile node</code> at the <code>home agent</code> . This can be either a 128-bit hexadecimal value or a random length ASCII string.

5.4.8. Quality Of Service

NetModule routers are able to prioritize and shape certain kinds of IP traffic. This is currently limited on egress, which means that only outgoing traffic can be stipulated.

The current QoS solution is using Stochastic Fairness Queueing (SFQ) classes in combination with Hierarchy Token Bucket (HTB) qdiscs. Its principle of operation can be summarized as ceiling the max. throughput per link and shaping traffic by reflecting the specified queue priorities. In general, the lowest priority number of a queue gets most out of the available bandwidth.

In case of demands for other class or qdisc algorithms please contact our support team in order to evaluate the best approach for your application.

QoS Administration

The administration page can be used to enable and disable QoS.

QoS Classification

The classification section can be used to define the WAN interfaces on which QoS should be active.

Parameter	QoS Interface Parameters
Interface	The WAN interface on which QoS should be active
Bandwidth congestion	The bandwidth congestion method. In case of <code>auto</code> the system will try to apply limits in a best-effort way. However, it is suggested to set fixed bandwidth limits as they also offer a way of tuning the QoS behaviour.
Downstream bandwidth	The available bandwidth for incoming traffic
Upstream bandwidth	The available bandwidth for outgoing traffic
IP to ping (primary)	An IP, which answers ICMP echo requests to determine the bandwidth of the link
IP to ping (secondary)	An IP, which answers ICMP echo requests to determine the bandwidth of the link

When defining limits, you should consider bandwidth limits which are at least possible as most shaping and queues algorithms will not work correctly if the specified limits cannot be achieved. In particular, any WWAN interfaces operating in a mobile environment are suffering variable bandwidths, thus rather lower values should be used.

5.5. FIREWALL

5.5.1. Administration

NetModule routers use Linux's netfilter/iptables firewall framework (see <http://www.netfilter.org> for more information) which supports stateful inspection, that is, granting the same permissions for inherited connections within an IP session (e.g. FTP which builds up a control and data connection).

The administration page can be used to enable and disable firewalling. When turning it on, a shortcut can be used to generate a predefined set of rules which allow administration (over HTTP, HTTPS, SSH or TELNET) by default but block any other packets coming from the WAN interface.

5.5.2. Address/Port Groups

This menu can be used to form address or port groups which can be later used for firewall rules in order to reduce the number of rules. If address or port groups have been referenced, packets will match if one of the configured entities apply to the packet.

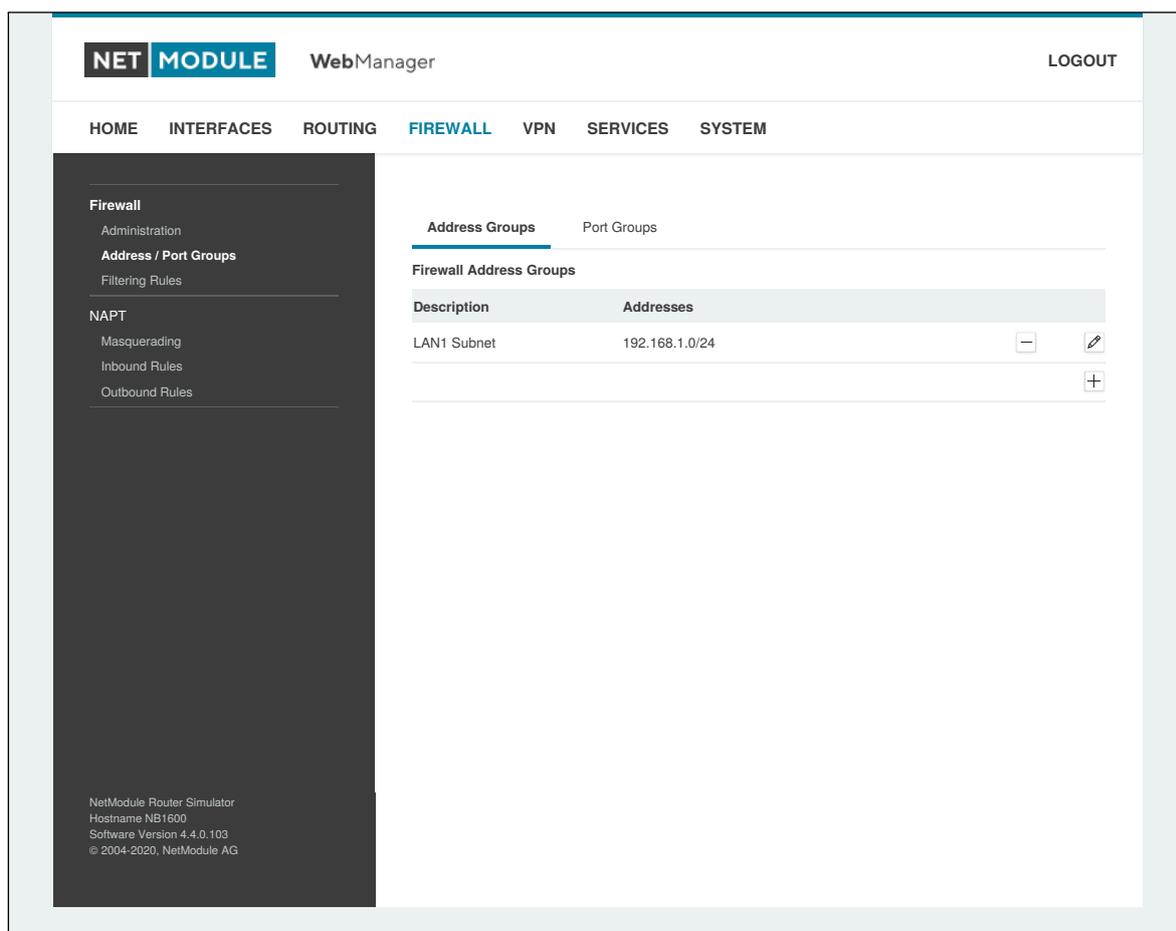


Figure 5.28.: Firewall Groups



Parameter	Firewall Rule Configuration
Protocol	The used IP protocol of matching packets (UDP, TCP or ICMP)
Destination port(s)	The destination port of matching packets, which can be specified by a single port or a range of ports (only UDP/TCP).

The statistics page can be used to figure out if rules have matched any packets and provides a convenient way to debug your firewall setup.

5.5.4. NAPT

This page can be used to configure Network Address and Port Translation (NAPT) for packets traversing the system. NAPT hereby modifies IP addresses or/and TCP/UDP ports in matching IP packets. By tracking those connections, it will also automatically adjust the returning packets of an IP session.

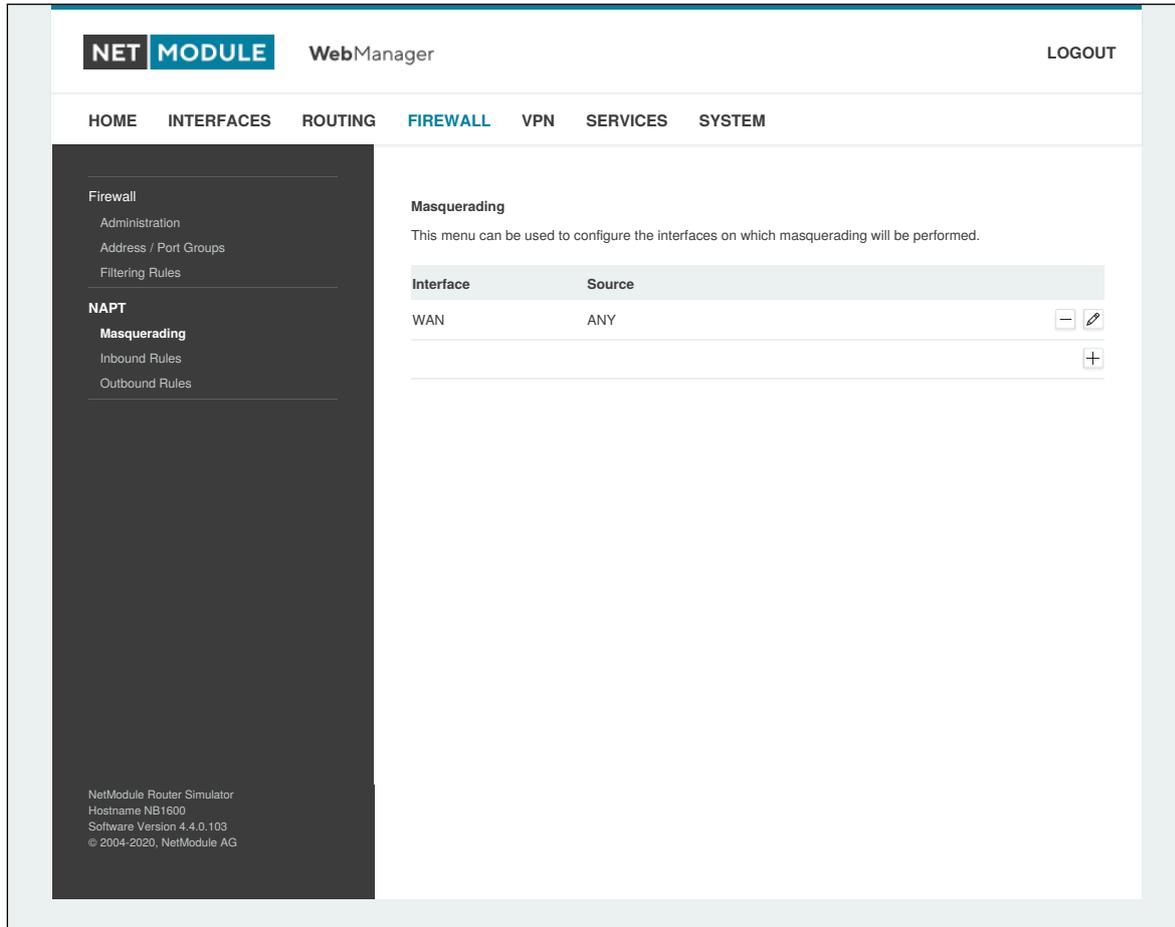


Figure 5.30.: Masquerading

The administration page lets you specify the interfaces on which masquerading will be performed. NAT will hereby use the address of the selected interface and choose a random source port for outgoing connections and thus enables communication between hosts from a private local area network towards hosts on the public network.

Parameter	Masquerading Rules
Interface	The outgoing interface on which connections will be masqueraded
Source address	The source address or network from which matching packets are masqueraded
Source netmask	The source netmask of the network from which matching packets are masqueraded

NAPT Inbound Rules

Inbound rules can be used to modify the target section of IP packets and, for instance, forward a service or port to an internal host. By doing so, you can expose that service and make it available from the Internet. You may also establish 1:1 NAT mapping for a single host using additional outbound rules.

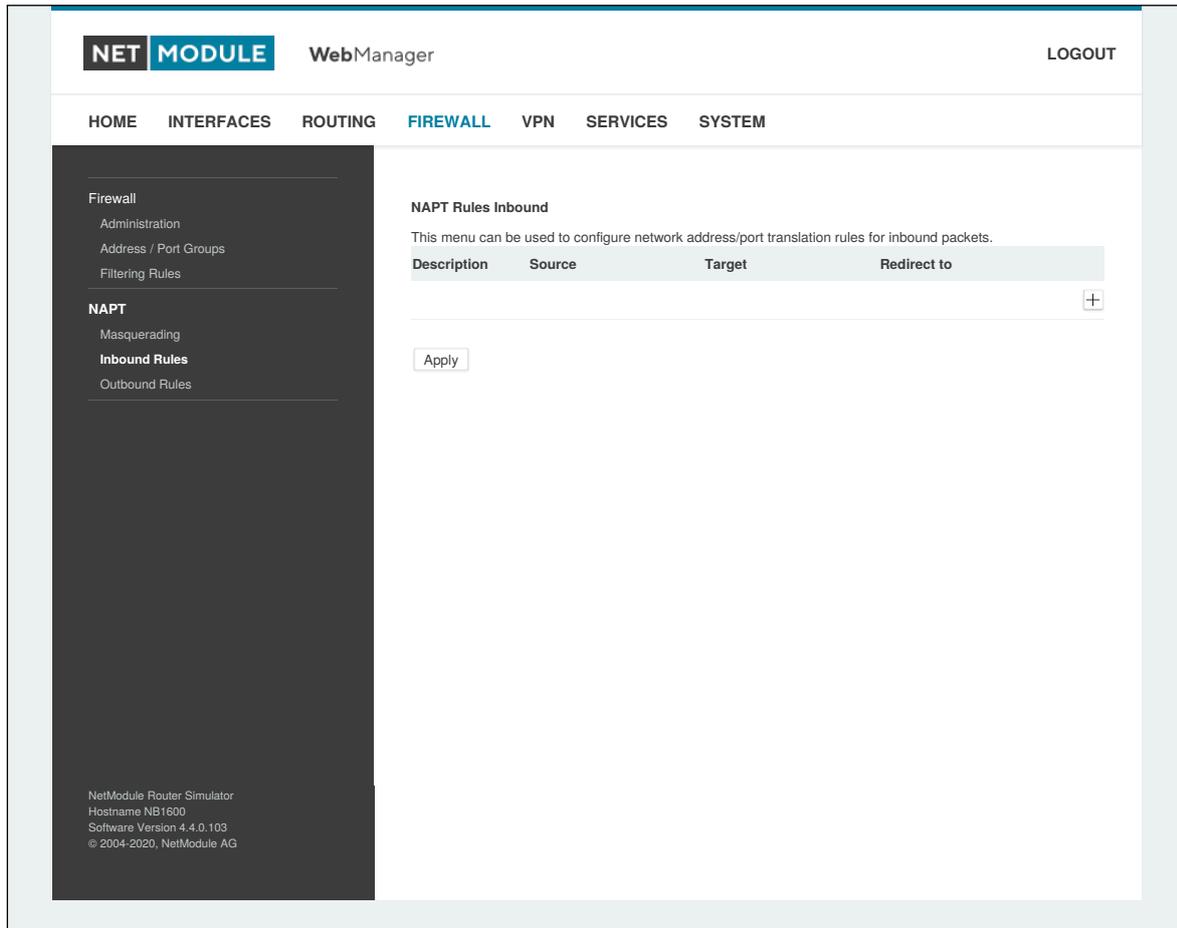


Figure 5.31.: Inbound NAPT

Please note that the specified rules are processed by order, that means, traversing the list from top to bottom until a matching rule is found. If there is no matching rule found, the packet will pass as is.

Parameter	Inbound NAPT Rules
Description	A meaningful description of this rule
Map	Context for this rule: Host, Network or Port-Range - see table below
Incoming interface	The interface from which matching packets are received
Source	The source address or network from which matching packets are received
Target address	The destination address of matching packets (optional)
Protocol	The used protocol of matching packets



Parameter	Inbound NAT Rules
Ports	The used UDP/TCP port of matching packets
Redirect to	The address to which matching packets shall be redirected
Redirect port	The port to which matching packets will be redirected

Select mapping context according to your needs:

Parameter	Mapping contexts
host	Rewrite destination address and port for one given host (i.e. 10.0.0.1:8080 → 192.168.1.100:80)
network	Rewrite destination address for a full network (i.e. 10.0.0.0/24 → 192.168.1.0/24)
port range	Rewrite destination address and port based on the incoming port (i.e. 10.0.0.1:22000-22255 → 192.168.1.0/24:22). There is no corresponding rule for port range translation in outbound rules. Use network based mapping there.

NAPT Outbound Rules

Outbound rules will modify the source section of IP packets and can be used to establish 1:1 NAT mappings but also to redirect packets to a specific service.

Parameter	Outbound NAT Rules
Description	A meaningful description of this rule
Outgoing interface	The outgoing interface on which matching packets are leaving the router
Target	The target address or network to which matching packets are destined
Source address	The source address of matching packets (optional)
Protocol	The used protocol of matching packets
Ports	The used UDP/TCP port of matching packets
Rewrite source address	The address to which the source address of matching packets shall be rewritten
Rewrite source port	The port to which the source port of matching packets shall be rewritten

5.6. VPN

5.6.1. OpenVPN

OpenVPN Administration

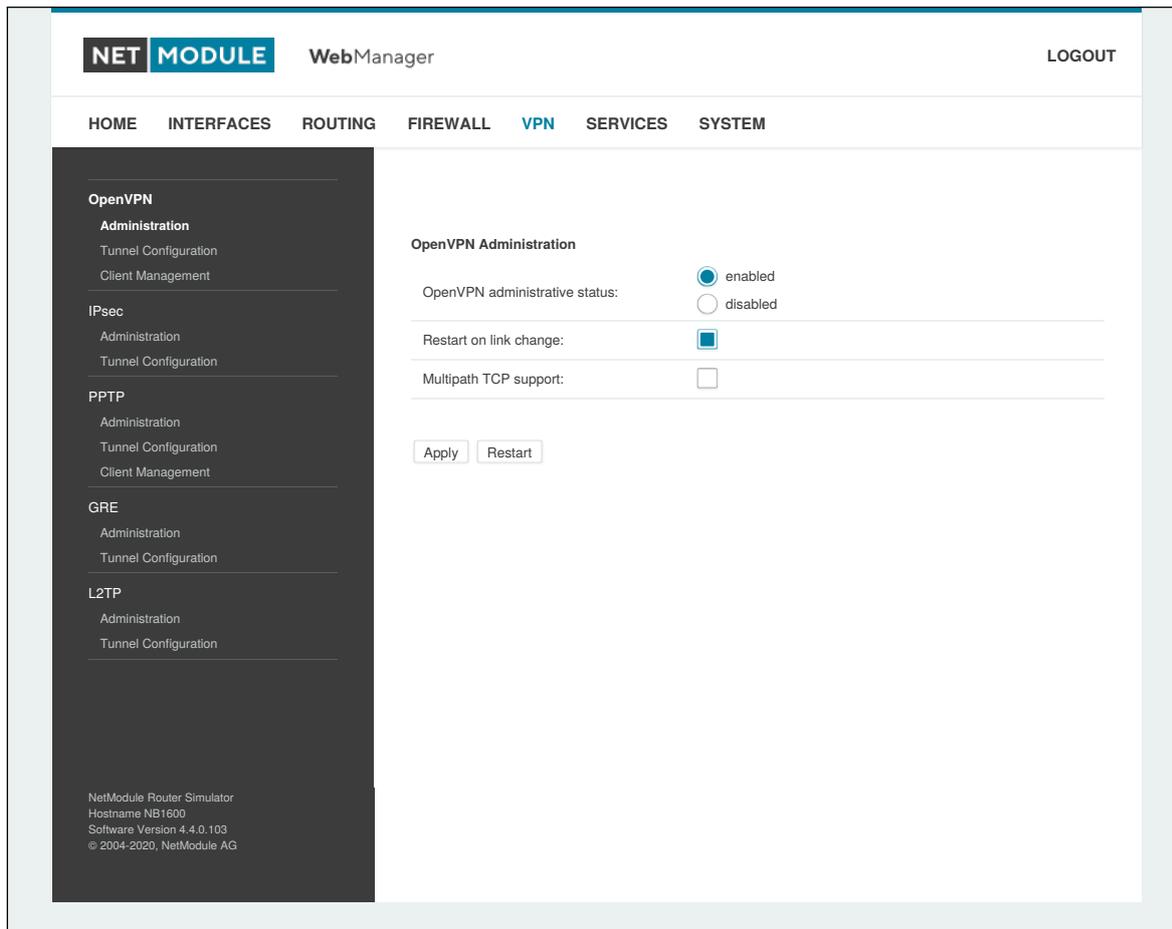


Figure 5.32.: OpenVPN Administration

Parameter	OpenVPN Administration
Administrative status	Specifies whether OpenVPN is active
Restart on link change	restarts the OpenVPN daemon in case of a wanlink change if enabled
Multipath TCP support	enables multipath TCP support

Tunnel Configuration

NetModule routers support one single server tunnel and up to four client tunnels. You can specify tunnel parameters either in standard configuration or upload an expert mode file which has been created in advance. Refer to chapter 5.6.1 to learn more about how to manage clients and generate the files.

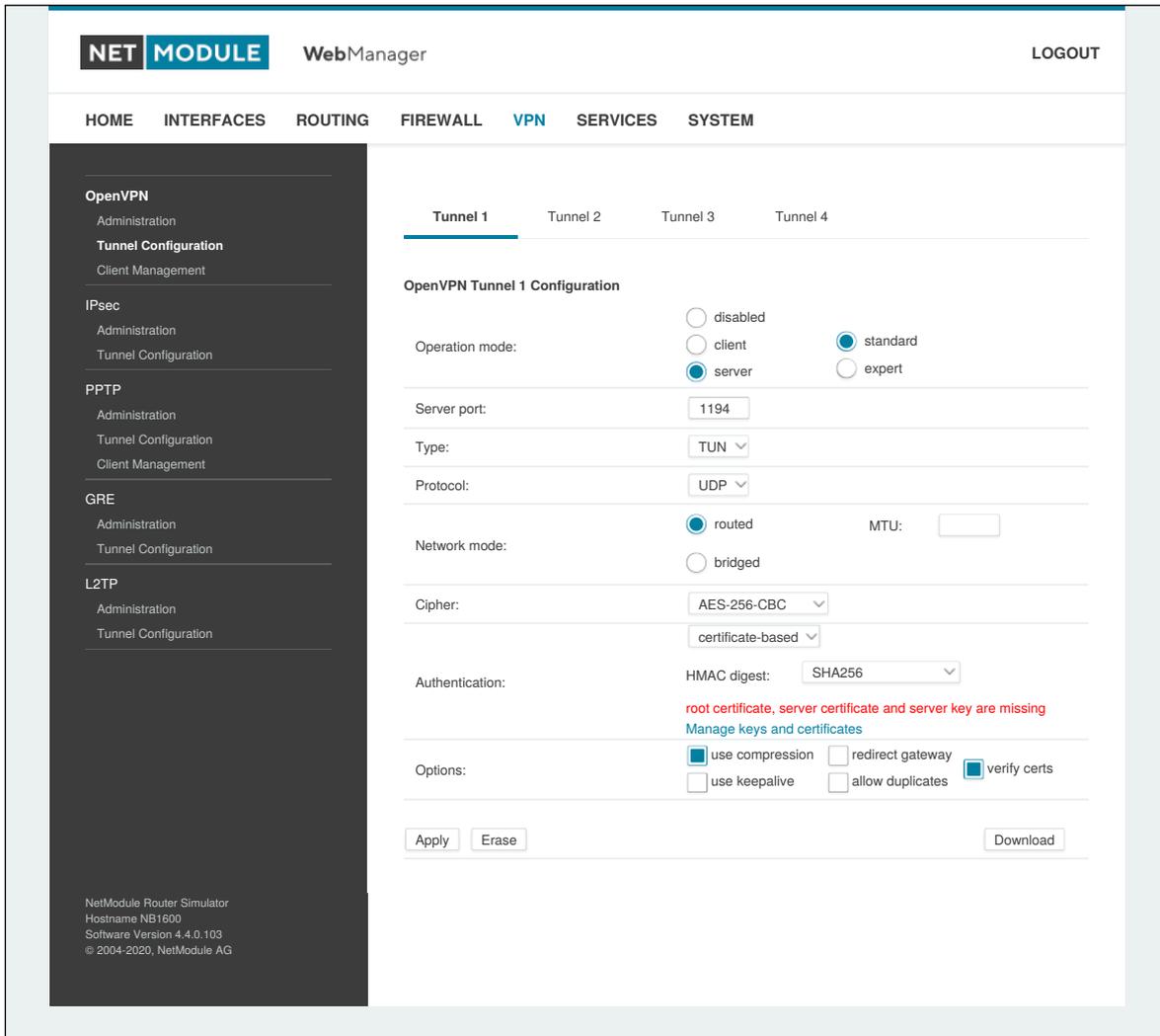


Figure 5.33.: OpenVPN Configuration

Parameter	OpenVPN Configuration
Operation mode	Specifies whether client or server mode should be used for this tunnel, it further specifies if tunnel shall be configured in a standard way or if an expert mode file shall be used.
Multipath TCP	Enables OpenVPN multipath TCP support

The following further options can be applied:

Parameter	OpenVPN Options
use compression	Enable or disable LZO packet compression
use keepalive	Can be used to send a periodic keepalive packet in order to keep the tunnel up despite of inactivity
redirect gateway	By redirecting the gateway, all packets will be directed to the VPN tunnel. Please ensure that essential services (such as DNS or NTP servers) can be reached at the network behind the tunnel. In doubt, create an extra static route pointing to the correct interface.
allow duplicates	Allow multiple clients with the same common name to concurrently connect. (server mode only)
verify certs	Check peer certificate against local CRL. (server mode only)
negotiate DNS	If enabled, the system will use the nameservers which have been negotiated over the tunnel.

OpenVPN Expert Configuration (Client)

The expert configuration mode offers a straightforward way to configure a tunnel by simply uploading a zip package containing the required configuration and optionally key/certificate files. A client tunnel usually consists of the following files:

Parameter	Client Expert Files
client.conf	OpenVPN configuration file (see http://www.openvpn.net for available options)
ca.crt	Root certificate authority file
client.crt	Certificate file
client.key	Private key file
client.p12	PKCS#12 file
ta.key	TLS authentication key file

Please note that you may specify arbitrary file names, however, the configuration file suffix must be `.conf` and all files referred in the configuration file must correspond to relative path names.



OpenVPN Expert Configuration (Server)

A server tunnel typically requires the following files:

Parameter	Server Expert Files
server.conf	OpenVPN configuration file
ca.crt	Root certificate authority file
server.crt	Certificate file
server.key	Private key file
dh1024.pem	Diffie-Hellman parameters file
ccd	A directory containing client-specific configuration files

Keep in mind that a certificate becomes valid once its validity time has been reached, thus an accurate system time has to be set prior to creating certificates and establishing a tunnel connection. Please ensure that all NTP servers are reachable. Using host names also requires a working DNS server.

5.6.2. IPsec

IPsec is a protocol suite for securing IP communications by authenticating and encrypting each packet of a communication session and thus establishing a secure virtual private network.

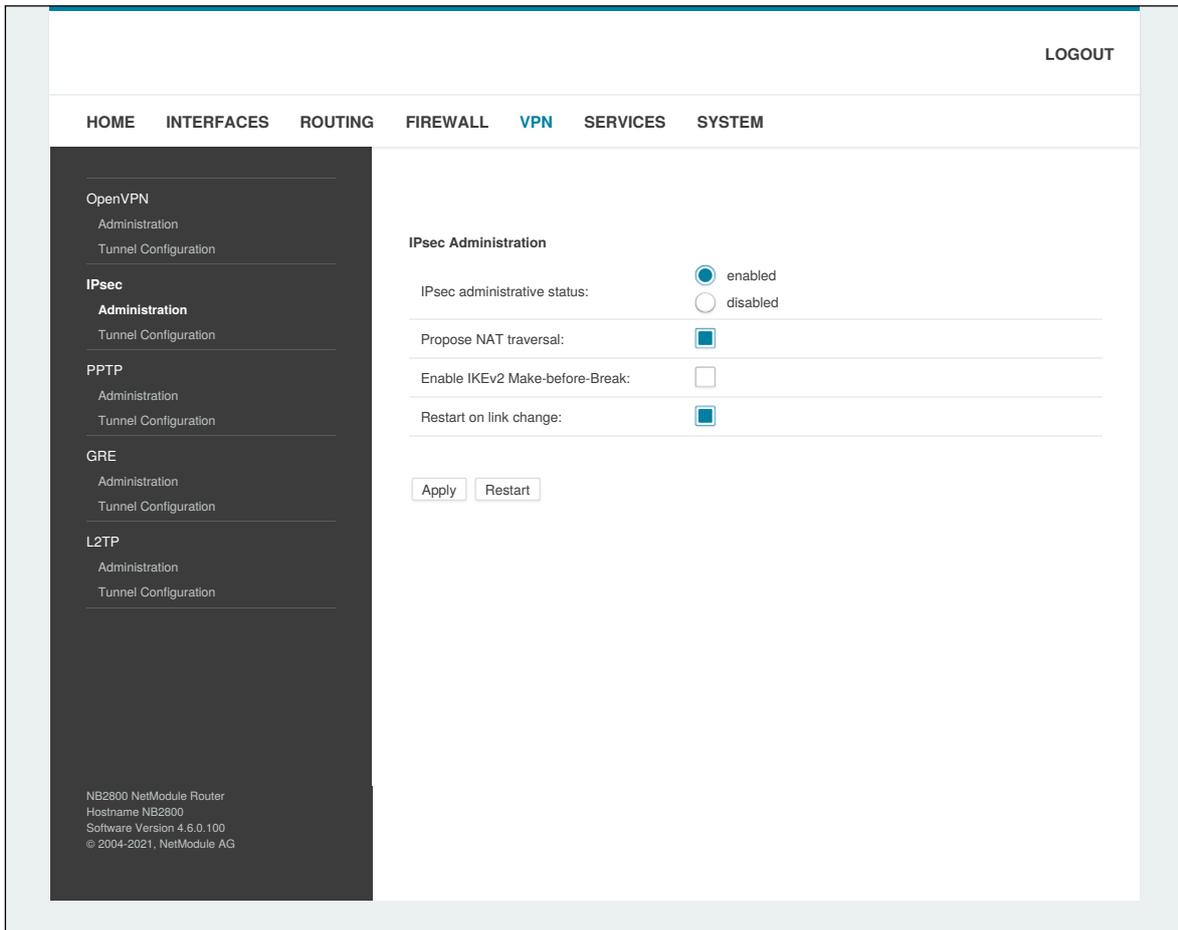
IPsec includes various cryptographic protocols and ciphers for key exchange and data encryption and can be seen as one of the strongest VPN technologies in terms of security. It uses the following mechanisms:

Mechanism	Description
AH	Authentication Headers (AH) provide connectionless integrity and data origin authentication for IP datagrams and ensure protection against replay attacks.
ESP	Encapsulating Security Payloads (ESP) provide confidentiality, data-origin authentication, connectionless integrity, an anti-replay service and limited traffic-flow confidentiality.
SA	Security Associations (SA) provide a secure channel and a bundle of algorithms that provide the parameters necessary to operate the AH and/or ESP operations. The Internet Security Association Key Management Protocol (ISAKMP) provides a framework for authenticated key exchange.

Negotiating keys for encryption and authentication is generally done by the Internet Key Exchange protocol (IKE) which consists of two phases:

Phase	Description
IKE phase 1	IKE authenticates the peer during this phase for setting up an ISAKMP secure association. This can be carried out by either using <code>main</code> or <code>aggressive</code> mode. The <code>main</code> mode approach utilizes the Diffie-Hellman key exchange and authentication is always encrypted with the negotiated key. The <code>aggressive</code> mode just uses hashes of the pre-shared key and therefore represents a less-secure mechanism which should generally be avoided as it is prone to dictionary attacks.
IKE phase 2	IKE finally negotiates IPsec SA parameters and keys and sets up matching IPsec SAs in the peers which is required for AH/ESP later on.

Administration



The screenshot displays the 'IPsec Administration' configuration page. The left sidebar is dark grey with white text, listing navigation options under 'OpenVPN', 'IPsec', 'PPTP', 'GRE', and 'L2TP'. The main content area is white and features the following settings:

- IPsec Administrative Status:** A radio button labeled 'enabled' is selected, with 'disabled' unselected.
- Propose NAT traversal:** A checked checkbox.
- Enable IKEv2 Make-before-Break:** An unchecked checkbox.
- Restart on link change:** A checked checkbox.

Below these settings are two buttons: 'Apply' and 'Restart'. The top navigation bar includes 'HOME', 'INTERFACES', 'ROUTING', 'FIREWALL', 'VPN', 'SERVICES', and 'SYSTEM'. The 'VPN' menu is currently selected. In the top right corner, there is a 'LOGOUT' link. At the bottom of the interface, the following text is visible: NB2800 NetModule Router, Hostname NB2800, Software Version 4.8.0.100, © 2004-2021, NetModule AG.

Figure 5.35.: IPsec Administration

This page can be used to enable/disable IPsec, you may also specify whether NAT-Traversal and IKEv2 Make-before-break should be used.

NAT-Traversal is mainly used for connections which traverse a path where a router modifies the IP address/port of packets. It encapsulates packets in UDP and therefore requires a slight overhead which has to be taken into account when running over small-sized MTU interfaces.

Please note that running NAT-Traversal makes IKE using UDP port 4500 rather than 500 which has to be taken into account when setting up firewall rules.

Make-before-break is an IKEv2 option used to optimize the necessary regular reauthentication by creating an overlapping SA (=make) before deleting the currently used SA (=break). This way, the interruption of the data stream is minimized. Both peers have to be able to handle overlapping SAs to use this option.

Parameter	IPsec General Settings
Failure threshold	The number of unanswered DPD requests until the IPsec peer is considered dead (the router will then try to re-establish a dead connection automatically)
Action	The action to perform if a peer disconnects. Available choices from the drop-down menu are to clear, hold or to Restart the peer.

IKE Authentication

NetModule routers support IKE authentication through pre-shared keys (PSK) or certificates within a public key infrastructure. Extended Authentication (XAUTH) leverages RADIUS-like authentication and can be used to apply user level access control over IPsec.

Using PSK requires the following settings:

Parameter	IPsec IKE Authentication Settings
PSK	The pre-shared key used to authenticate at the peer
Local ID Type	The type of identification for the local ID which can be a FQDN, username@FQDN or IP address
Local ID	The local ID value
Remote ID Type	The type of identification for the remote ID
Remote ID	The remote ID value

When using certificates you would need to specify the operation mode. When run as PKI client (initiator) you can create a Certificate Signing Request (CSR) in the certificates section which needs to be submitted at your Certificate Authority and imported to the router afterwards. In PKI server mode (concentrator), the router represents the Certificate Authority and issues the certificates for remote peers. They are revokable.

Using XAUTH the following settings can be made:

Parameter	IPsec XAUTH Settings
User name	The name of the XAUTH user
User password	The password of the XAUTH user
Group name	The group ID
Group password	The group secret



Parameter	IPsec Network Settings
Peer network	The address of the remote network behind the peer
Peer netmask	The netmask of the remote network behind the peer
NAT address	Optionally, you can apply NAT (masquerading) for packets coming from a different local network. The NAT address must reside in the network previously specified as local network. If NAT address is enabled but the value is empty the router will try to guess a valid NAT address (not recommended).

Client Management

Once you have successfully set up an IPsec tunnel, you can manage and enable clients connecting to your service. It is possible to generate and download expert mode files for enabled clients which can be used to easily populate each client.

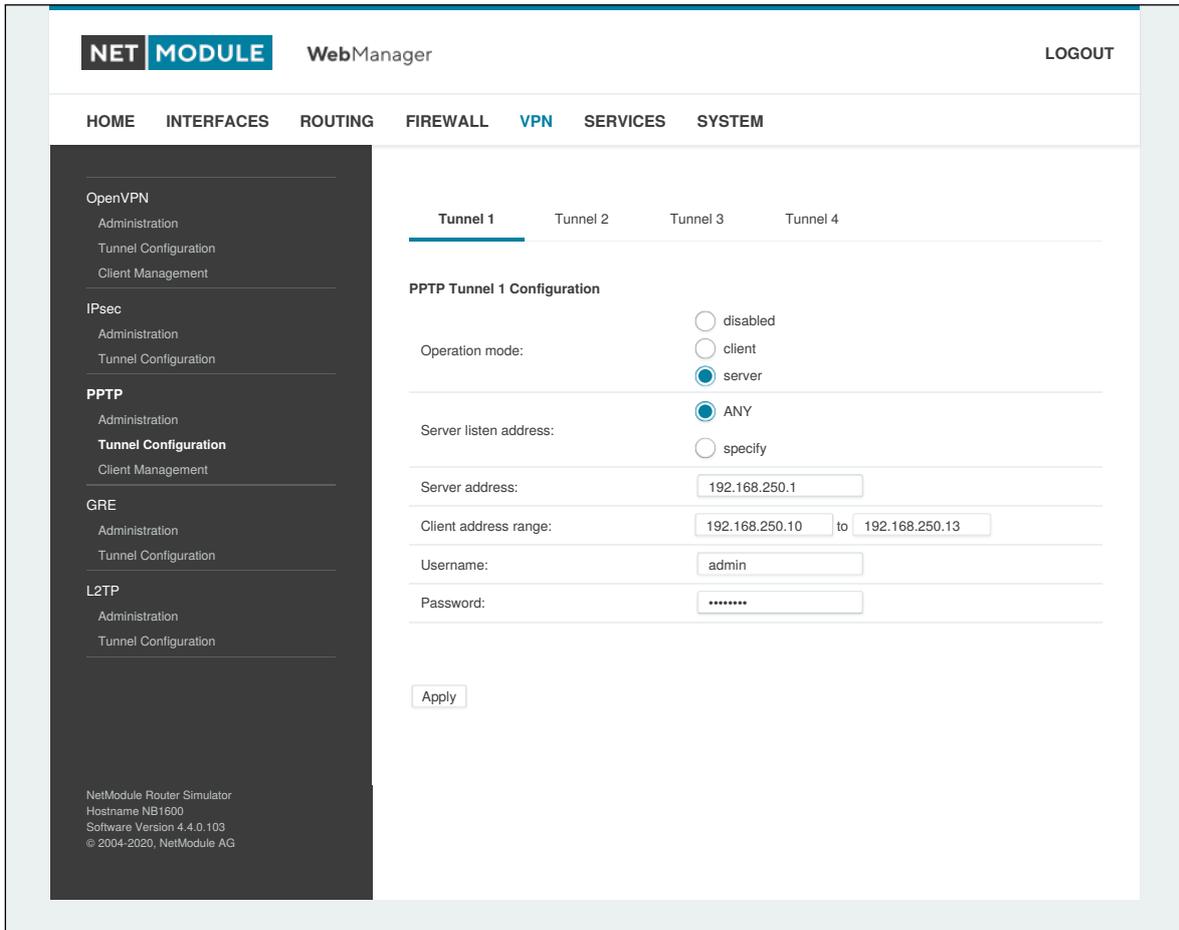


Figure 5.38.: PPTP Tunnel Configuration

Setting up a server requires the following settings:

Parameter	PPTP Server Settings
Listen address	Specifies on which IP address should be listened for incoming client connections
Server address	The server address within the tunnel
Client address range	Specifies a range of IP addresses assigned to each client

PPTP Client Management

PPTP clients for a server tunnel need to be configured here. They are made up of user-name and password. A fixed IP address can be assigned to them which can be used to point any routes to a dedicated tunnel.

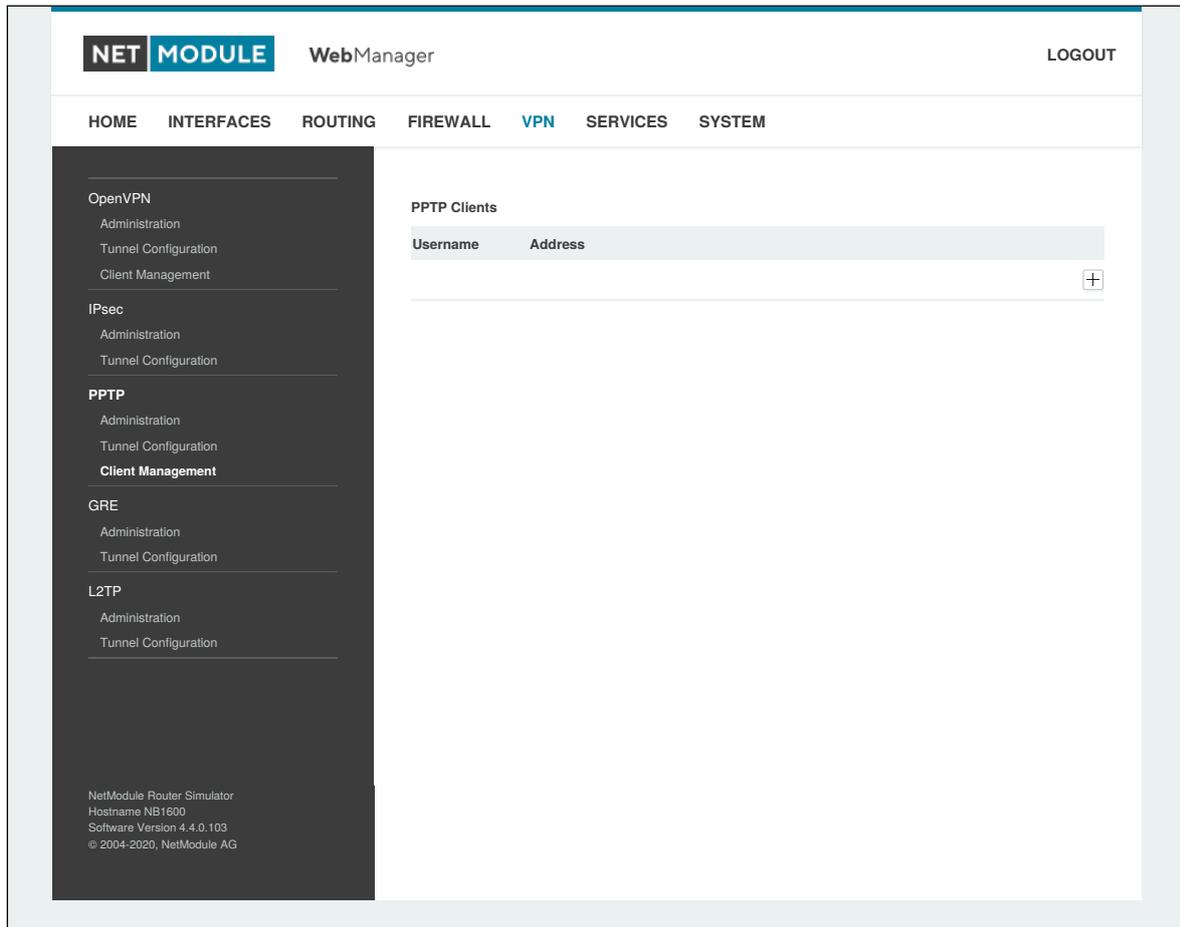


Figure 5.39.: PPTP Client Management

5.6.5. L2TP

The Layer 2 Tunneling Protocol is a tunneling protocol which does not support any encryption or confidentiality. It relies on an encryption protocol that it passes within the tunnel to provide privacy. The following parameters are required for setting up a tunnel:

Parameter	L2TP Configuration
Transport protocol	The transport portocol which shall be used
Local IP	The local IP address of the tunnel
Remote IP	The remote IP address of the tunnel
Local port	The local port address of the tunnel
Remote port	The remote port address of the tunnel
Local tunnel ID	The local tunnel ID identifies the tunnel into which the session will be created
Remote tunnel ID	The remote tunnel ID identifies the tunnel assigned by the peer
Local Session ID	The local session ID identifies the session being created
Remote Session ID	The remote session ID identifies the session assigned by the peer
Local Cookie	The local cookie sets an optional cookie value to be assigned to the session
Remote Cookie	The remote cookie set an optional pper cookie value to be assigned to the session
MTU	The Maximum Transmission Unit of the tunnel interface
Bridge Interface	The interface to which the guest interace shall be bridged

5.6.6. Dial-In

On this page you can configure the Dial-In server in order to establish a data connection over GSM calls. Thus, one would generally apply a required service type of 2G-only, so that the modem registers to GSM only. Naturally, a concurrent use of outgoing WWAN interfaces and Dial-In connection is not possible.

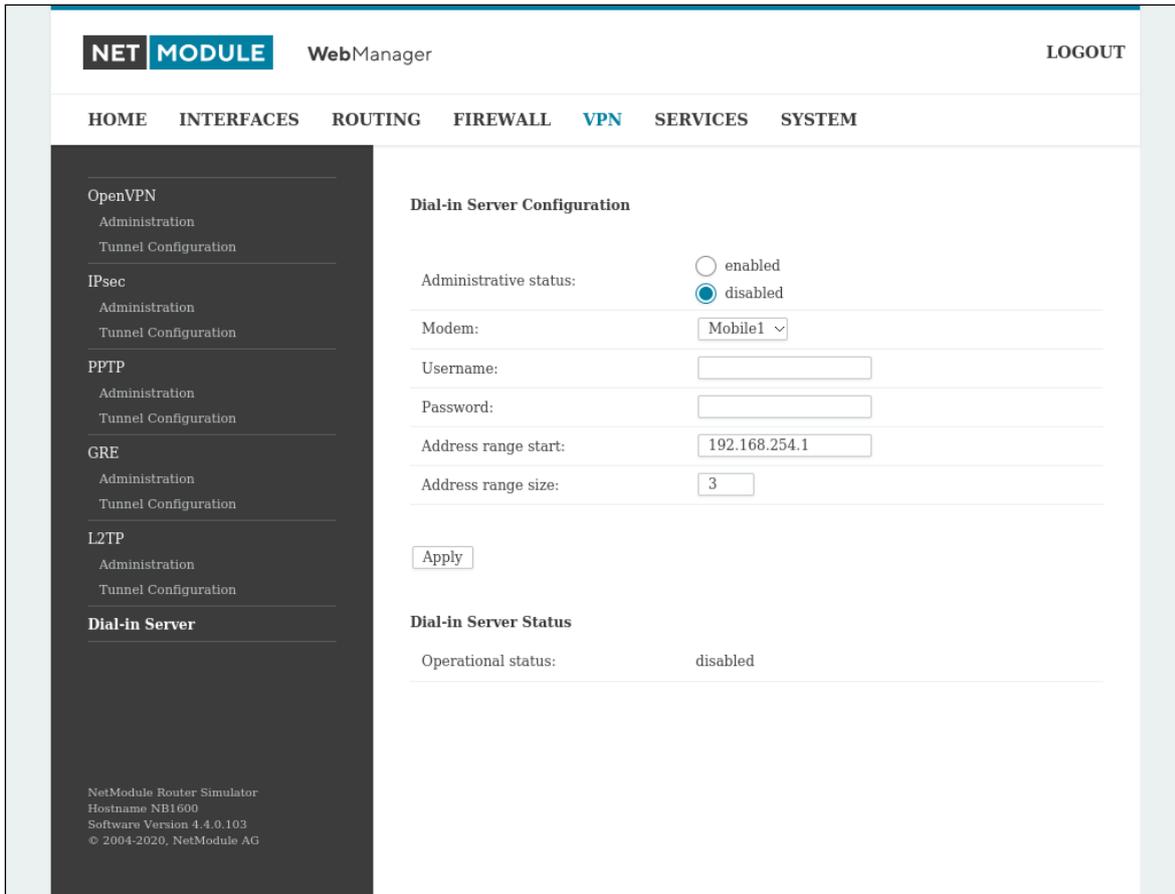


Figure 5.40.: Dial-in Server Settings

The following settings can be set:

Parameter	Dial-in Server Configuration
Administrative status	Specifies whether incoming calls shall be answered or not
Modem	Specifies the modem on which calls can come in
User	Specifies the username for the incoming PPP connection
Password	Specifies the password for the incoming PPP connection
Address range start	Start of the IP address range assigned to incoming clients
Address range size	Number of addresses for client IP address range



Please note that Dial-In connections are generally discouraged. As they are implemented as GSM voice calls, they suffer from unreliability and poor bandwidth.

5.7. SERVICES

5.7.1. SDK

NetModule routers are shipping with a Software Development Kit (SDK) which offers a simple and fast way to implement customer-specific functions and applications. It consists of:

1. An SDK host which defines the runtime environment (a so-called sandbox), that is, controlling access to system resources (such as memory, storage and CPU) and, by doing so, catering for the right scalability
2. An interpreter language called arena, a light-weight scripting language optimized for embedded systems, which uses a syntax similar to ANSI-C but adds support for exceptions, automatic memory management and runtime polymorphism on top of that
3. A NetModule-specific Application Programming Interface (API), which ships with a comprehensive set of functions for accessing hardware interfaces (e.g. digital IO ports, GPS, external storage media, serial ports) but also for retrieving system status parameters, sending E-Mail or SMS messages or simply just to configure the router

Anyone, reasonably experienced in the C language, will find an environment that is easy to dig in. However, feel free to contact us via support@netmodule.com and we will happily support you in finding a programming solution to your specific problem.

The Language

The arena scripting language offers a broad range of POSIX functions (like printf or open) and provides, together with tailor-made API functions, a simple platform for implementing any sort of applications to interconnect your favourite device or service with the router.

Here comes a short example:

```
/* We are going to eavesdrop on the first serial port
 * and turn on lights via a digital I/O output port,
 * otherwise we'd have to send a short message.
 */

for (attempts = 0; attempts < 3; attempts++) {
    if (nb_serial_read("serial0") == "Knock Knock!") {
        nb_serial_write("serial0", "Who's there?");

        if (nb_serial_read("serial0") == "Santa") {
            printf("Hurray!\n");
            nb_dio_set("out1", 1);
        }
    }
}
nb_sms_send("+123456789", "No presents this year :)")
```

A set of example scripts can be downloaded directly from the router, you can find a list of them in the appendix. The manual which can be obtained from the [NetModule support web page](#) gives a detailed introduction of the language, including a description of all available functions.

SDK API Functions

The current range of API functions can be used to implement the following features:

1. Send/Retrieve SMS
2. Send E-mail
3. Read/Write from/to serial device
4. Control digital input/output ports
5. Run TCP/UDP servers
6. Run IP/TCP/UDP clients
7. Access files of mounted media (e.g. an USB stick)
8. Retrieve status information from the system
9. Get or set configuration parameters
10. Write to syslog
11. Transfer files over HTTP/FTP
12. Perform config/software updates
13. Control the LEDs
14. Get system events, restart services or reboot system
15. Scan for networks in range
16. Create your own web pages
17. Voice control functions
18. SNMP functions
19. CAN socket functions
20. Various network-related functions
21. Other system-related functions

The SDK API manual (which can be downloaded from the router) provides an overview but also explains all functions in detail.

Please note that some functions require the corresponding services (e.g. E-Mail, SMS) or configured interfaces (e.g. CAN) to be properly configured prior to utilizing them in the SDK.

Here is an example how one might adopt those functions:

```
/* check current city and enable the second WAN link */  
  
location = nb_status("location");  
if (location) {  
    city = struct_get(location, "LOCATION_CITY");  
  
    if (city == "Wonderland") {  
        for (led = 0; led < 5; led++) {  
            nb_led_set(led, LED_BLINK_FAST|LED_COLOR_RED);  
        }  
    } else {  
        printf("You'll never walk alone in %s ...\n", city);  
        nb_config_set("wanlink.1.mode=1");  
    }  
}
```

Running SDK

In the SDK, we are speaking of scripts and triggers which form jobs.

Any arena script can be uploaded to the router or imported by using dedicated user configuration packages. You may also edit the script directly at the Web Manager or select one of our examples. You will further have a testing section on the router which can be used to check your syntax or doing test runs.

Once uploaded, you will have to specify a trigger, that is, telling the router when the script is to be executed. This can be either time-based (e.g. each Monday) or triggered by one of the pre-defined system events (e.g. wan-up) as described in Events chapter 5.7.7. With both, a script and a trigger, you can finally set up an SDK job now. The `test` event usually serves as a good facility to check whether your job is doing well. The admin section also offers facilities to troubleshoot any issues and control running jobs.

The SDK host (`sdkhost`) corresponds to the daemon managing the scripts and their operations and thus avoiding any harm to the system. In terms of resources, it will limit CPU and memory for running scripts and also provide a pre-defined portion of the available space of the storage device. You may, however, extend it by external USB storage or (depending on your model) extended flash storage.

Files written to `/tmp` will be hold in memory and will be cleared upon a restart of the script. As your scripts operate in the sandbox, you will have no access to tools on the system (such as `ifconfig`).

Administration

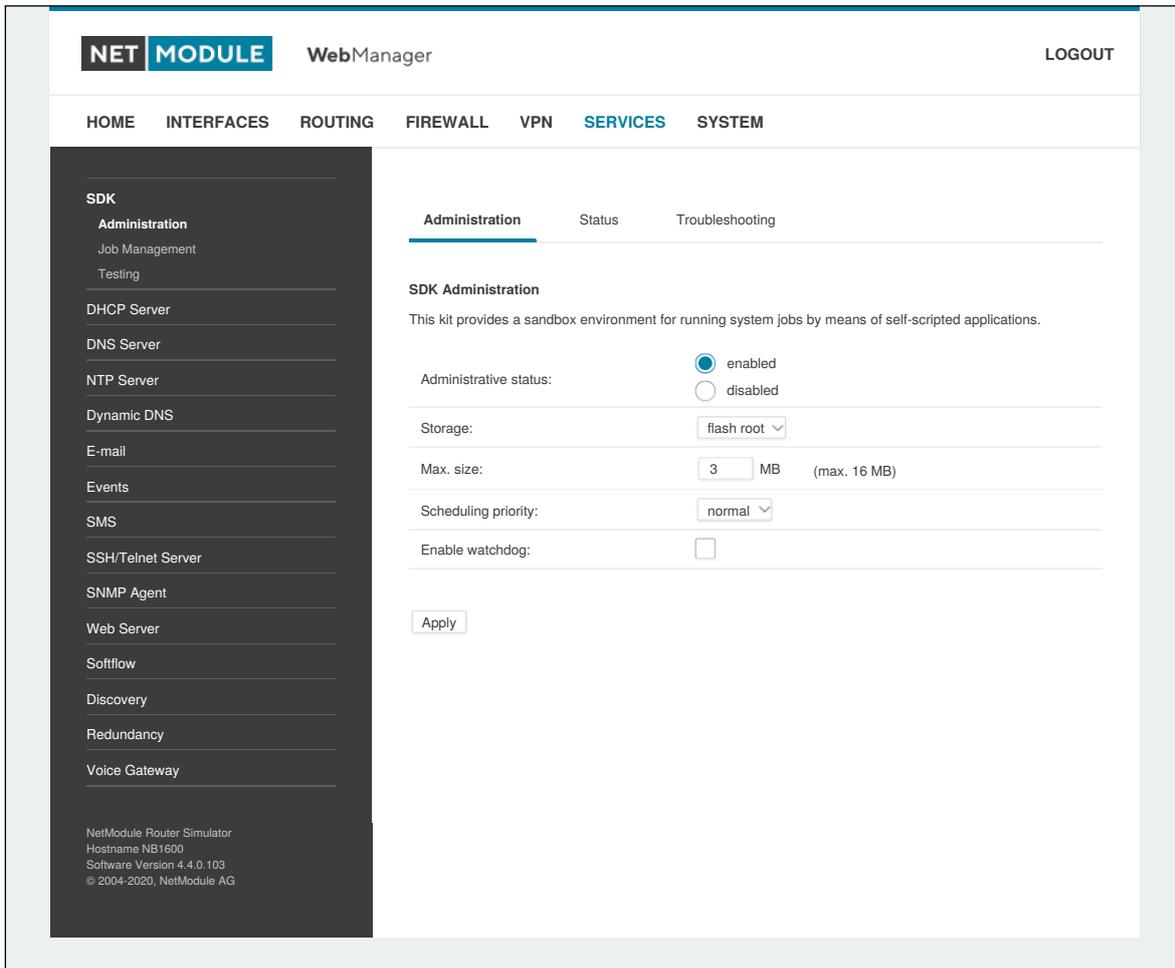


Figure 5.41.: SDK Administration

This page can be used to control the SDK host and apply the following settings:

Parameter	SDK Administration Settings
Administrative status	Specifies whether SDK scripts should run or not
Storage	The storage device on which the sandbox shall be stored (see chapter 5.8.1)
Max. size	The maximum amount of MBytes your scripts can consume on the storage device
Scheduling priority	Specifies the process priority of the sdkhost, higher priorities will speed up scheduling your scripts, lower ones will have less impact to the host system
Enable watchdog	This option will enable watchdog supervision for each script which leads to a reboot of the system if the script does not respond or stopped with an exit code not equal zero.

The status page informs you about the current status of the SDK. It provides an overview about any finished jobs, you can also stop a running job there and view the script output in the troubleshooting section where you will also find links for downloading the manuals and examples.

Job Management

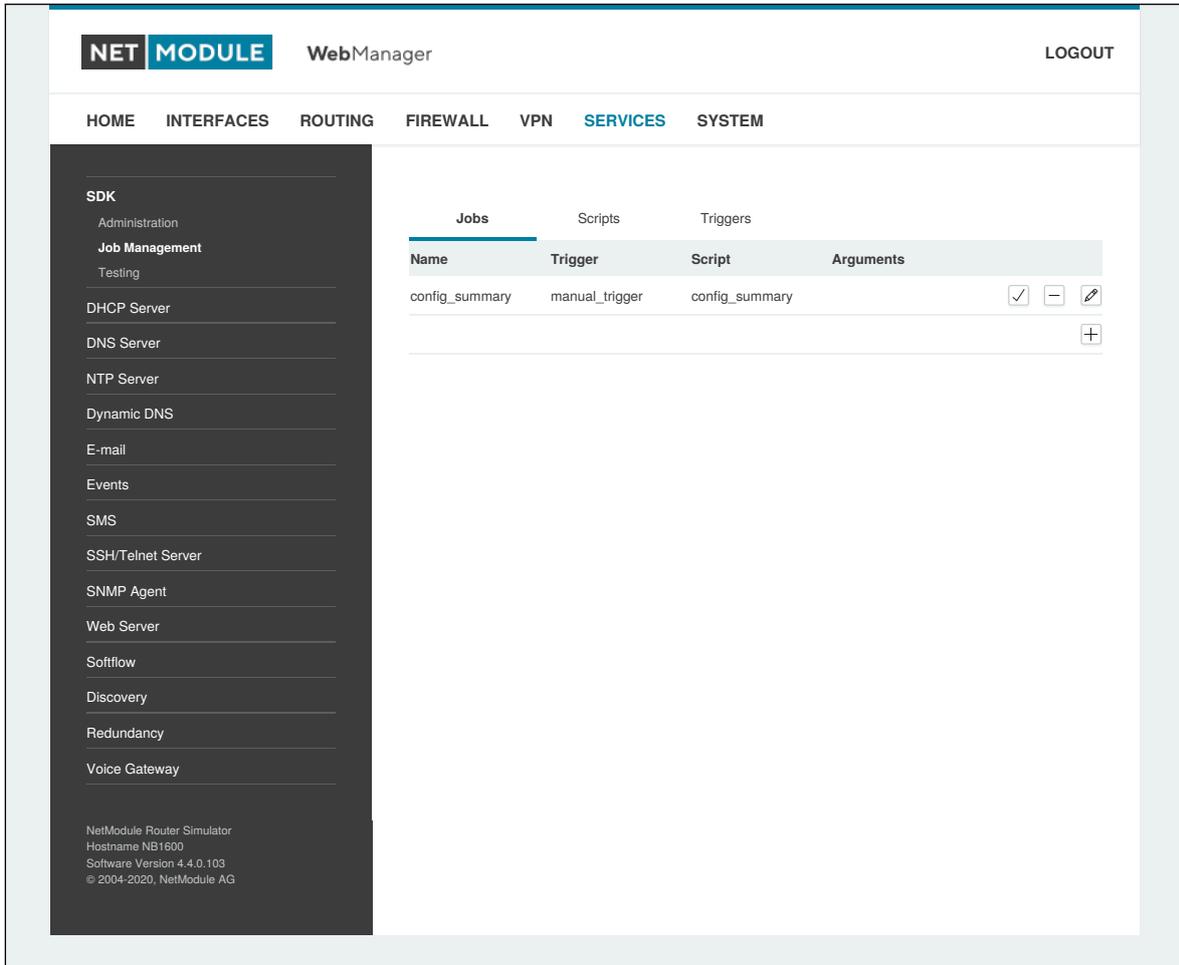


Figure 5.42.: SDK Jobs

This page can be used to set up scripts, triggers and jobs. It is usually a good idea to create a trigger first which is made up by the following parameters:

Parameter	SDK Trigger Parameters
Name	A meaningful name to identify the trigger
Type	The type of the trigger, either time-based or event-based
Condition	Specifies the time condition for time-based triggers (e.g. hourly)
Timespec	The time specification which, together with the condition, specifies the time(s) when the trigger should be pulled
Event	The system event upon which the trigger should be pulled

You can now add your personal script to the system by applying the following parameters:



Parameter	SDK Script Parameters
Name	A meaningful name to identify the script
Description	An optional description of the script
Arguments	An optional set of arguments passed to the script (supports quoting)
Action	You may either edit a script, upload it to the system or select one of the example scripts or an already uploaded script

You are ready to set up a job afterwards, it can be created by using the following parameters:

Parameter	SDK Job Parameters
Name	A meaningful name to identify the job
Trigger	Specifies the trigger that should launch the job
Script	Specifies the script to be executed
Arguments	Defines arguments which can be passed to the script (supports quoting), they will precede the arguments you formerly may have assigned to the script itself

You can trigger each configured job directly which can be helpful for testing purposes.

Pages

Any programmed SDK pages will show up here.

Testing

The testing page offers an editor and an input field for optional arguments which can be used to perform test runs of your script or test dedicated portions of it or upload an entire file. Please note that you might need to quote arguments as they will otherwise be separated by white-spaces.

```
/* arguments: 'schnick schnack "s c h n u c k"'
for (i = 0; i < argc; i++) {
    printf("argv%d: %s\n", i, argv[i]);
}

/* generates:
*     argv0: scriptname
*     argv1: schnick
*     argv2: schnack
*     argv3: s c h n u c k
*/
```

In case of syntax errors, arena will usually print error messages as follows (indicating the line and position where the parsing error occurred):

```
/scripts/testrun:2:10:FATAL: parse error, unexpected $, expecting ';''
```

SDK Sample Application

As an introduction, you can step through a sample application, namely the SMS control script, which implements remote control over short messages and can be used to send a status of the system back to the sender. The source code is listed in the appendix.

Once enabled, you can send a message to the phone number associated with a SIM / modem. It generally requires a password to be given on the first line and a command on the second, such as:

```
admin01
status
```

We strongly recommend to use authentication in order to avoid any unintended access, however you may pass `noauth` as argument to disable it. You can then skip the first line containing the password. Having a closer look to the script, you will see that you will also be able to restrict the list of permitted senders. Please inspect the system log for troubleshooting any issues.



The following commands are supported:

Command	Action
status	Will reply a message to the sender including a short system overview
connect	Will enable the first WAN link configured on the system
disconnect	Will disable the first WAN link configured on the system
reboot	Initiates a reboot of the system
output 1 on	Turns on the first digital output port
output 1 off	Turns off the first digital output port
output 2 on	Turns on the second digital output port
output 2 off	Turns off the second digital output port

Table 5.101.: SMS Control Commands

A response to the status command typically looks like:

```
System: NB2700 hostname (00:11:22:AA:BB:CC)
WAN1: WWAN1 is up (10.0.0.1, Mobile1, UMTS, -83 dBm, LAI 12345)
GPS: lat 47.377894, lon 8.540055, alt 282.200
OVPN: client on tun0 is up (10.0.8.4)
DIO: IN1=off, IN2=off, OUT1=on, OUT2=off
```


Parameter	DHCP Server Settings
Last lease address	The last address out of this range
Lease duration	Number of seconds how long a given lease shall be valid until it has to be requested again
Persistent leases	By turning on this option the router will remember issued leases even after a reboot. This can be used to ensure that the same IP address will be assigned to a particular host.
DHCP options	By default the DHCP will hand out the interface address as default gateway and the current DNS server addresses if not configured otherwise. You can specify fixed addresses here.
Only allow static hosts	Any requests coming from none-static hosts will be ignored.

Parameter	DHCP Options
Gateway address	The default gateway address
Primary DNS	The primary nameserver
Secondary DNS	The secondary nameserver
Primary WINS	The primary WINS server
Secondary WINS	The secondary WINS server
Agent ID	The relay agent ID (DHCP option 82)

Parameter	DHCP Relay Settings
Primary relay server	The primary DHCP relay server
Secondary relay server	The secondary DHCP relay server

It is also possible to configure specific lease addresses for particular clients.

Parameter	DHCP Static Hosts Settings
IP address	The IP address of the lease
Identified by	Specifies by which criteria the client shall be identified
MAC address	The MAC address of the client
hostname	The client identifier (DHCP option 61)
port	The Ethernet port on which the DHCP request is received

Additional DHCP options can be specified via the custom DHCP options.

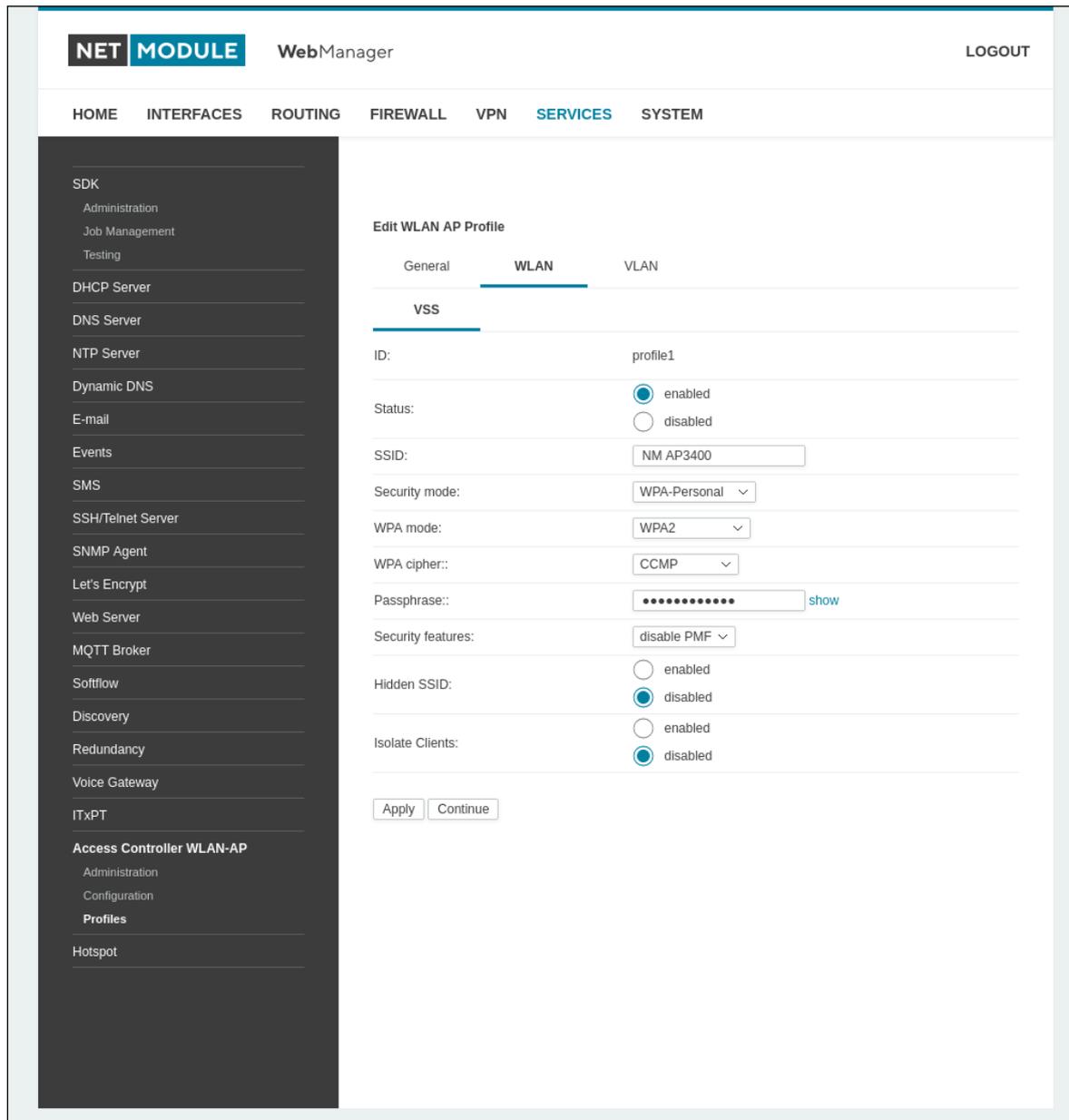


Figure 5.61.: AC WLAN-AP Profiles

Parameter	AC profile general parameters
ID	The unique name for the profile
Description	The description of the profile

Parameter	AC profile WLAN parameters
Status	Enables or disables this profile



Parameter	AC profile WLAN parameters
SSID	The network name (called SSID)
Description	The description of the profile
Security mode	The desired security mode
WPA mode	The desired encryption method. WPA3 should be preferred over WPA2 and WPA1
WPA cipher	The WPA cipher to be used, the default is to run both (TKIP and CCMP)
Passphrase	The passphrase used for authentication with WPA-Personal, otherwise the key passphrase for WPA-EAP-TLS. In case of WPA-Personal: The passphrase must be at least 8 to 63 characters long.
Security features	Enables Protected Management Frames
Hidden SSID	Hides the SSID
Isolate clients	Disables client-to-client communication
RADIUS server	The RADIUS server address
RADIUS secret	The secret used to authenticate against the RADIUS server
Authentication port	The port used for authentication
Accounting port	The port used for accounting messages

Parameter	AC profile VLAN parameters
VLAN ID	The VLAN ID for the profile. If no VLAN ID shall be used with this profile the parameter has to be empty

5.8. SYSTEM

5.8.1. System

System Settings

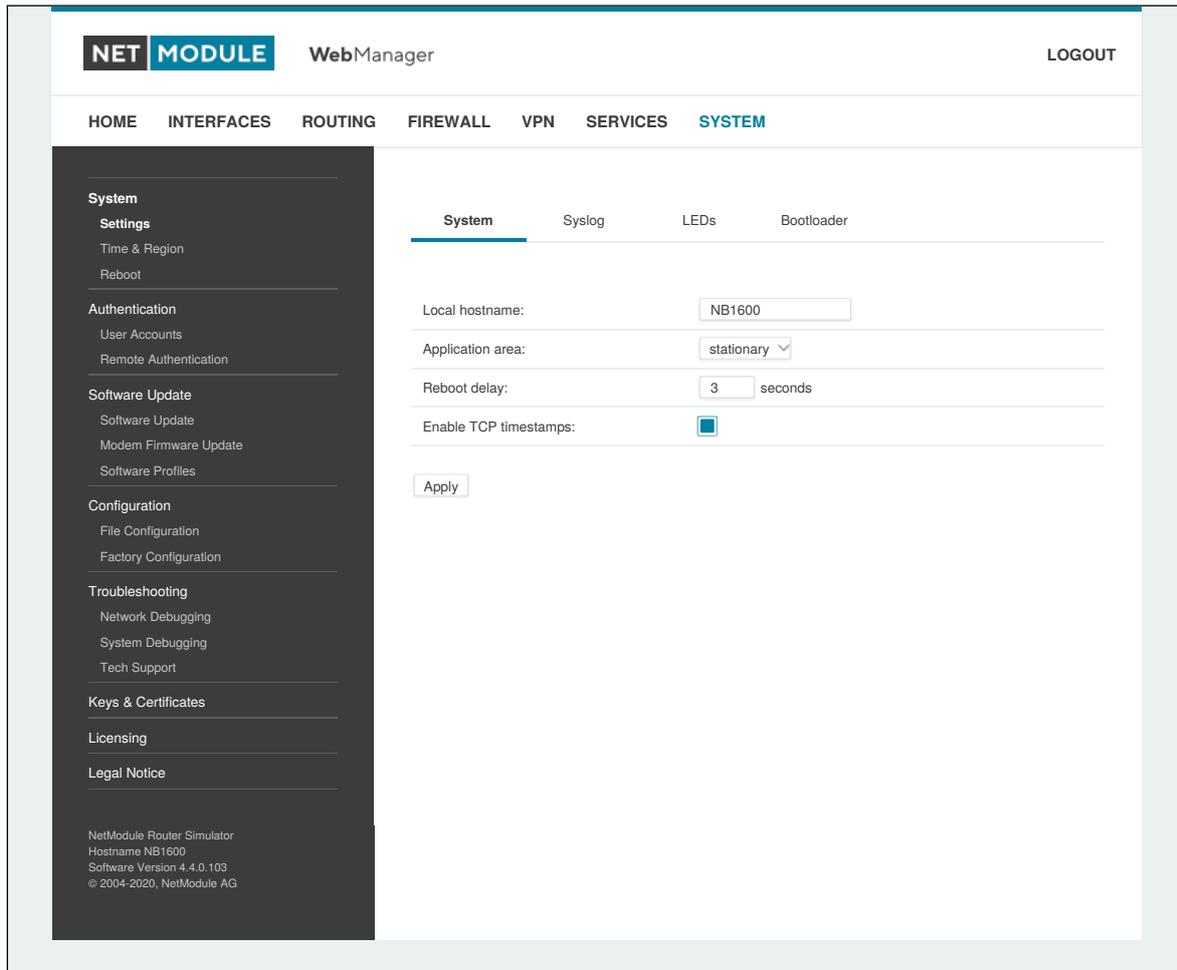


Figure 5.62.: System

System

The following system parameters can be set:

Parameter	System Settings
Local hostname	The hostname of the system
Application area	The desired application area which influences the system behaviour such as registration timeouts or other adaptations when operating in mobile environments.
Reboot delay	The number of seconds which will be waited before regular system reboots (might be needed for <code>system-rebooting</code> events)

Parameter	System Settings
Enable TCP timestamps	Enable TCP timestamps for system wide TCP communication. This is needed for Protection Against Wrapped Sequence numbers (PAWS), but with these timestamps enabled a remote attacker can guess the uptime of the system. The uptime is a lower bound for the age of the main system components like the kernel. If the system has an uptime of 3 years it's unlikely that recent security patches were applied.
Show messages and infos on log-in screen	Show error messages and notifications on login screen. If this option is enabled these messages are also shown before logging in with user credentials.

Syslog

The following syslog parameters can be set:

Parameter	Syslog Settings
Storage	The storage device on which log files shall be stored.
Max. filesize	The maximum size of the log files (in kB) until they will get rotated.
Redirect address	Specifies an IP address to which log messages should be redirected to. A tiny system log server for Windows is included in TFTP32 which can be downloaded from our website.

In general, the box comes with an internal flash device which can be used to store data. Depending on your model this can be extended by additional flash or USB disks. The following storage devices exist:

Parameter	Storage Devices
flash root	The root partition of the internal flash
flash data	The data partition of the internal flash
extended disk	An extended storage disk
USB disk	A storage disk connected to the external USB port

LEDs

The following LED parameters can be set:

Parameter	LED Settings
LED	You can customize the behavior of all status LEDs on the front panel of your device. They are usually divided into two banks (top/bottom). You may configure toggle mode, so that the LEDs periodically cycle between two separated configured LED schemes.

Bootloader

The following bootloader parameters can be set:

Parameter	Bootloader Settings
Password	The password used to unlock the bootloader. If empty, the admin password will be used.

Autorun

This feature can be used to automatically launch a shell script or perform a software/config update as soon as an external storage device has been plugged in. For authentication, a file called `autorun.key` must exist in the root directory of a FAT16/32 formatted device. It can be downloaded from that page and holds the SHA256 hash key of the autorun password. The file can hold multiple hashes which will be processed line-by-line during authentication which can be used for setting up more systems with different admin passwords.

For new devices with an empty password the hash key

```
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
```

can be used.

The hash keys can be generated by running the command `echo -n "<password>" | sha256sum` on a Linux system or an Internet hash key generator (search for "sha-256 hash calculator").

Once authentication has succeeded, the system scans for other files in the root directory which can perform the following actions:

1. For running a script: `autorun.sh`
2. For a configuration update: `cfg-<SERIALNO>.zip` (e.g. `cfg-00112B000815.zip`), or if not available `cfg.zip`
3. For a software update: `sw-update.img`

Time & Region

This page can be used for setting the system time and configuring the time zone. You may further enable daylight saving changes for your specific time zone. NetModule routers can synchronize their system time by using one or more servers by the help of the Network Time Protocol (NTP) or via GNSS. If enabled, the time synchronization is usually triggered after a WAN link has come up but before starting any VPN connections. Further time synchronization cycles are scheduled in background.

Most routers don't have a battery backed clock (RTC). In this case the system time is set during boot to the last valide time, e.g. before power off.

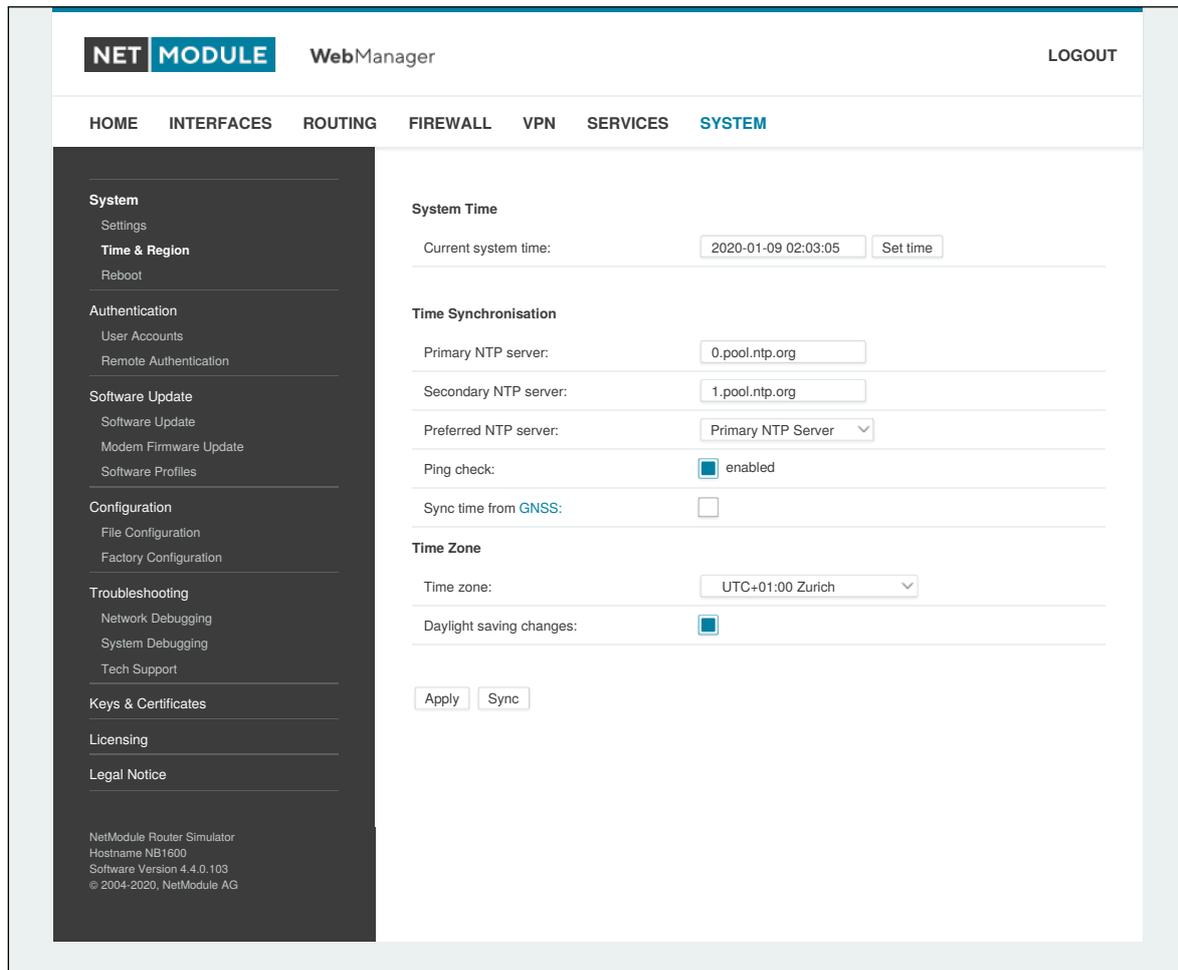


Figure 5.63.: Regional settings

Parameter	Time Synchronisation
NTP server	Address of the primary NTP server
NTP server 2	Optionally, the address of a second NTP server
Ping check	Uses an ICMP ping to check whether NTP servers are available when running initial time update
Sync time from GNSS	Derive time from first GNSS device (if enabled)

Parameter	Time Zone
Time Zone	Set the local time zone.
Daylight saving changes	Enable/disable daylight saving changes.

Virtualization

Virtualization techniques can be used to run multiple isolated guests on top of the host system. The netmodule routers use OS-level virtualization: A system is virtualized at the operating system level,

enabling multiple isolated user-space instances called containers. The same operating system kernel is used to implement the guest environments, applications running in a guest environment view it as a stand-alone system.

General settings:

Parameter	Virtualization Settings
Administrative status	Defines whether virtualization is enabled or not

The following parameters can be used to configure a virtual guest:

Parameter	Guest Settings
Type	Defines which virtualization technique is being used
Description	The description of the guest
Storage	Specifies the storage device on which the root file system of the guest will be located

To Install a root-file-system you can set up a URL to load a the image from and trigger the installation:

Parameter	Install
URL	The URL to load the image from. The Image needs to be provided as XZ compressed TAR archive containing the files of a root FS compatible with our CPU architecture (). Different protocols may be used for the transaction like 'http://' or 'https://', 'ftp://' or 'tftp://'. If you uploaded the the image to the router in advance you can also use 'file://' followed by the local path of the file. We can provide various tailored Linux distribution images (such as Debian) on demand.
Install	If this trigger is set the image download will start on apply. Any existing root file system will be overwritten. This parameter will not be stored in the configuration. After the installation was proceeded the value will be reset and needs to be set again if a new image shall be installed.

Communication to and from the guest can be achieved by defining network interfaces which can be either routed towards the guest or bridged with a LAN interface:

Parameter	Guest Networking
Guest interface	The name of the interface inside the guest
Mode	The network mode for this interface (either routed or bridged)
Address	The IP address of the interface inside the guest
Netmask	The netmask of the interface inside the guest
Gateway	The gateway used inside the guest which is also set on the host interface
Bridge interface	The interface to which the guest interace shall be bridged

The guest devices parameter shows a list of devices (e.g bluetooth, CAN) which can be provided to the guest system.

Parameter	Guest Devices
Enable devices	Enable or disable device for the guest

In order to limit the resources for a guest, the following settings can be applied:

Parameter	Guest Limits
CPU	The number of CPUs used for the guest
Memory	The amount of memory available for the guest

Reboot

This page can be used to set up a periodic automatic reboot but also to trigger a manual reboot which will be issued immediately.

5.8.2. Authentication

User Accounts

By using this page you can manage the user accounts on the system.

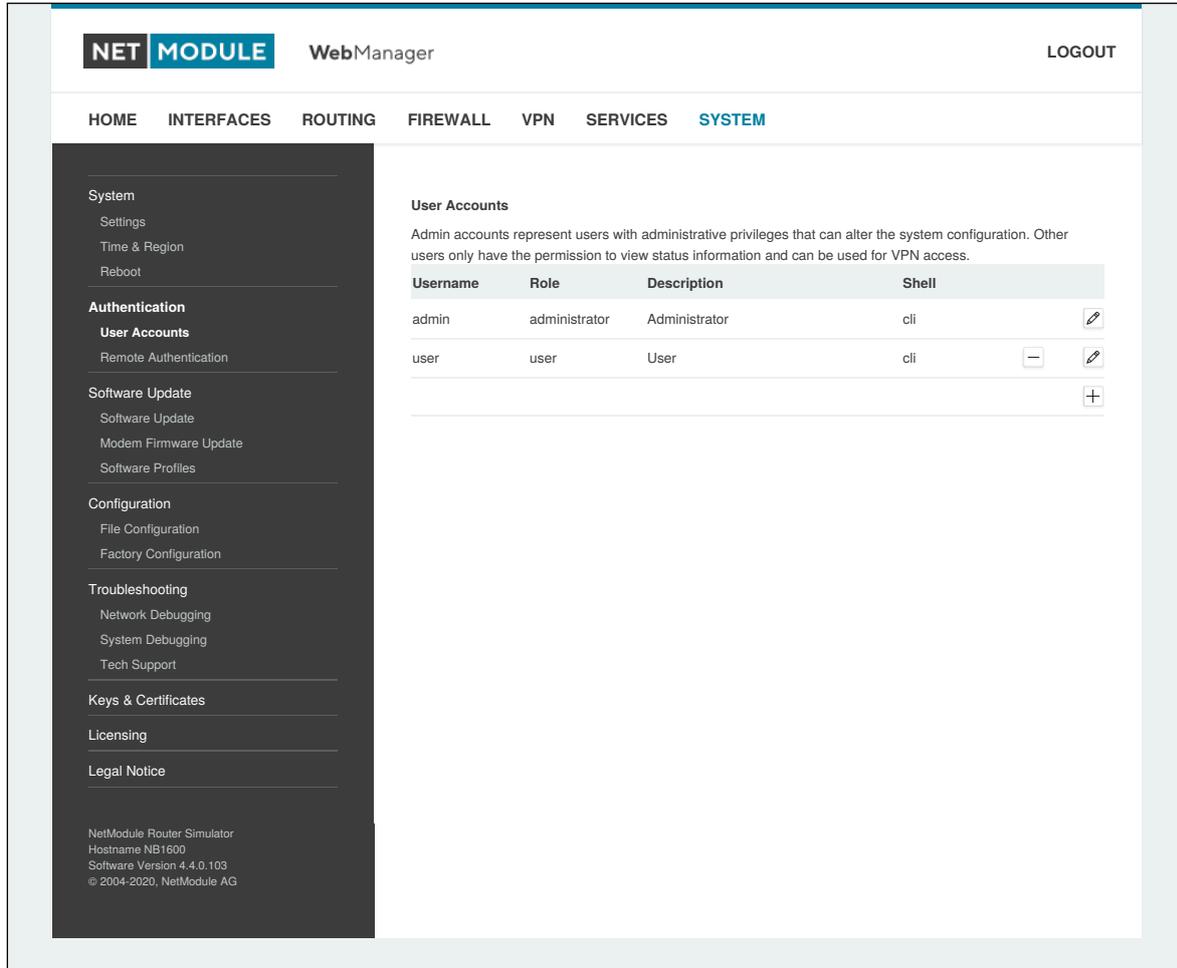


Figure 5.64.: User Accounts

The `admin` user is a built-in power user which represents the default administrator of the system. Please note that the `admin` password will be also applied to the `root` user which is able to enter a system shell. Further admin accounts with administrative privileges can be added, they can also alter the system configuration or perform administrative system tasks. Other users only have the permission to view status information. They can be also used for VPN access.

The Web Manager supports up to 5 concurrent users. Inactive users will be kicked after being idle for 30 minutes. If login was successful, any duplicate users from other remote hosts will be logged out. Remote hosts will be blocked for 5 minutes after 10 failed login attempts.

Parameter	User accounts management
Username	The name of the user
Description	A short description for the user

Parameter	User accounts management
Role	Either admin or user
Shell	Specifies if the user gets the CLI or a SHELL
Store password unencrypted	If this option is selected the user password is stored unencrypted on the device (not recommended)
Old password	The old password of the user
New password	The new password of the user
Confirm new password	The confirmed new password of the user

Please note, when adding additional admin users you are required to provide the password of the default administrator.



Storing Passwords

Normally the password for a user is only stored as a cryptographic hash, which is the recommended way to handle passwords on devices. Unfortunately the SNMP implementation makes it mandatory to store the password on the device unencrypted. Make sure to grant access rights to your users in a restrictive manner.

Remote Authentication

A RADIUS server can be used for authenticating remote users. This applies for the Web Manager, the WLAN network and other services supporting and incorporating remote authentication.

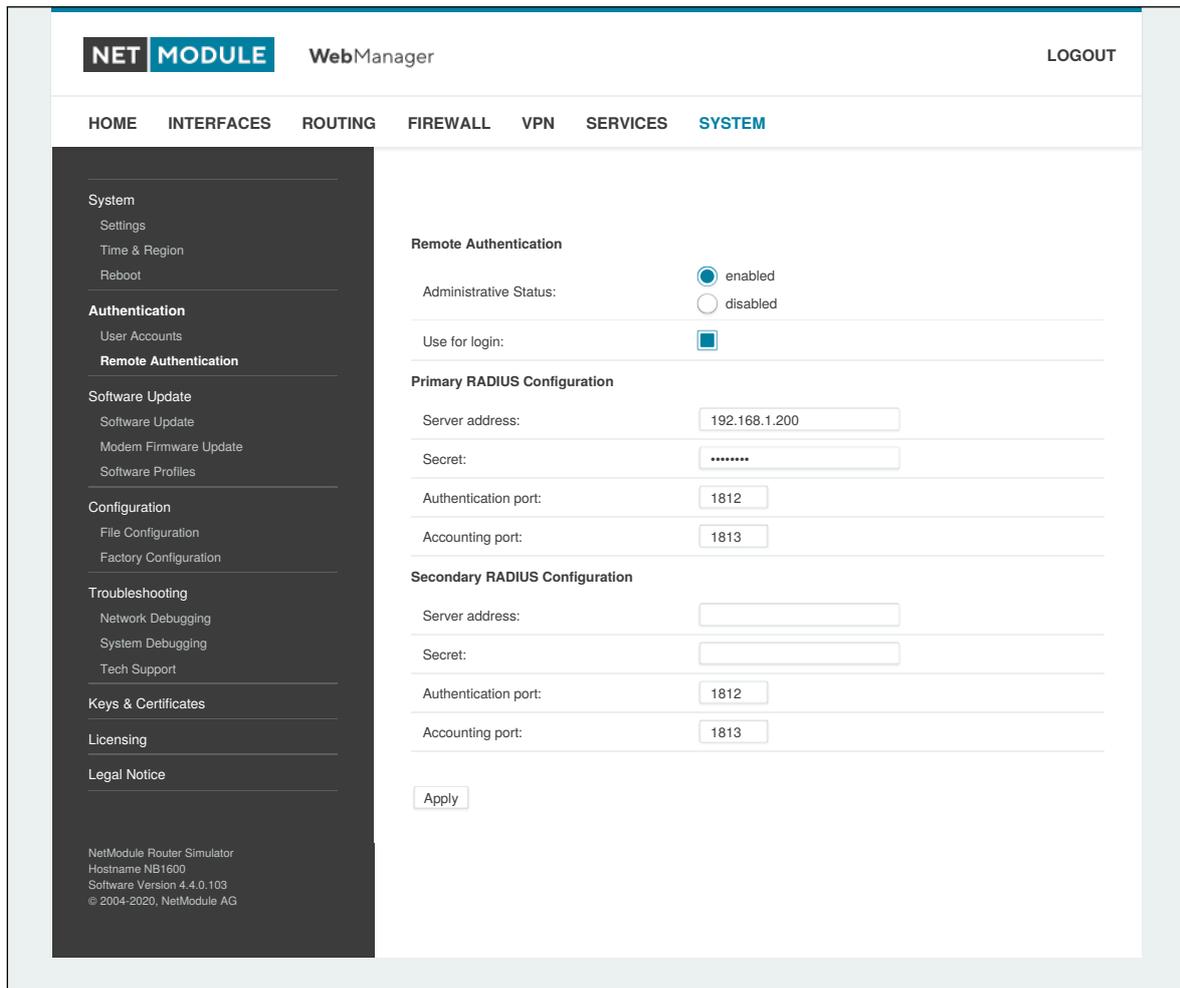


Figure 5.65.: Remote Authentication

It can be configured as follows:

Parameter	Remote authentication settings
Administrative status	Defines whether a remote server should be used for authentication
RADIUS server	The RADIUS server address
RADIUS secret	The secret used to authenticate against the RADIUS server
Authentication port	The port used for authentication
Accounting port	The port used for accounting messages
Use for login	This option enables remotely-defined users to access the Web Manager, otherwise it is only used by services which have explicitly configured it (e.g. WLAN)

5.8.3. Software Update

Manual Software Update

This menu can be used to run a manual software update of the system.

Parameter	Manual Software Update
Update operation	The update operation method being used. You can upload the image, download it from an URL or use the latest version from our server
URL	The server URL where the software update image should be downloaded from
Administrator password	Administrator password for downgrade to releases before 4.2.x



Attention

Starting with SW release 4.2 we set default to not saving passwords using password hashes instead. Storing passwords for users can be enabled, but is not recommended for new applications.

Older SW releases require the passwords to be stored encrypted on the device. As we don't have them any more in release version 4.2 and later you will have to provide the administrator password if you want to downgrade to a release 4.1.x and lower. The same passphrase will be used for bootloader login as well.

All users which have no password stored on the device will not be able to login after downgrade until new passwords have been applied.

An Uniform Resource Locator (URL) can have the following format:

```
http://<username>:<password>@<host>:<port>/<path>  
https://<username>:<password>@<host>:<port>/<path>  
ftp://<username>:<password>@<host>:<port>/<path>  
sftp://<username>:<password>@<host>:<port>/<path>  
tftp://<host>/<path>  
file:///<path>
```

When issuing a software update, the current configuration (including files like keys/certificates) will be backed up. Any other modifications to the filesystem will be erased.

The configuration is generally backward-compatible. We also apply forward compatibility when downgrading to a previous software within the same release line, which is accomplished by sorting out unknown configuration directives which actually may lead to loss of settings and features. Therefore, it's always a good idea to keep a copy of the working configuration.



Attention

In case you perform a major downgrade with a previous release line (e.g. 3.7.0 to 3.6.0), please ensure to always use the latest release of that branch (i.e. 3.6.0.X) as only those tend to be fully forward-compatible. Also keep in mind, that some hardware features may not work (e.g. if not implemented in that version). In doubt, please consult our support team.

A software image can be either uploaded via the Web Manager or retrieved from a specific URL. It will be unpacked and deployed to a spare partition which gets activated if the update completed successfully. The whole procedure is accompanied by all green LEDs flashing up, the subsequent system reboot gets denoted by a slowly blinking Status LED. The backedup configuration will be applied at bootup and the Status LED will blink faster during this operation. Depending on your configuration, this may take a while.

Automatic Software Update

This menu can be used to run a automatic software update of the system.

Parameter	Automatic software update
Status	Enable/disable automatic software update
Time of day	Every day at this time the router will do a check for updates
Operation	Download latest image from the server or specify the URL where the software update package should be downloaded from. Supported protocols are TFTP, HTTP, HTTPS, and FTP. Provide a URL like <code>protocol://server/path/file</code>

Remark: SSL certificates of HTTPS URLs will be only verified if a list of CA root certificates are provided under [5.8.8](#).

After the new software has been installed, the latest running configuration will be applied afterwards during bootup. This is indicated by a faster green blinking of the Status LED.

5.8.4. Module Firmware Update

This menu can be used to perform a firmware update of a specific module.

Parameter	Module Firmware Update
Update operation	The update operation method being used. You can either upload a firmware package or download it from a specific URL.
Module	The module which shall be updated.
Storage	The temporary storage which shall be used for the update procedure. For boxes with limited amount of flash it is possible to use an USB stick which must be properly set up in the USB section and hold a proper filesystem such as ext4.



Parameter	Module Firmware Update
URL	The server URL where the firmware package should be downloaded from (e.g. <code>protocol://server/path/file</code>). Supported protocols are TFTP, HTTP, HTTPS, and FTP. For boxes with limited amount of flash you may also use <code>usb0://<path-to-firmware-package></code> .

A firmware package (ZIP) usually consists of a flash utility, an info file and the corresponding firmware files. Please follow <https://www.netmodule.com/en/support> in order to get the latest version.

5.8.5. Software Profiles

The system consists of two root partitions which can hold different software versions and this menu can be used to switch between them. By doing so, you can test a newer software version and simply switch-back if things go wrong.

5.8.6. Configuration

Configuration via the Web Manager becomes tedious for larger volumes of devices. The router therefore offers automatic and manual file-based configuration to automate things. Once you have successfully set up the system you can back up the configuration and restore the system with it afterwards. You can either upload a single configuration file (.cfg) or a complete package (.zip) containing the configuration file and a packed version of other essential files (such as certificates) in the root directory.

Manual File Configuration

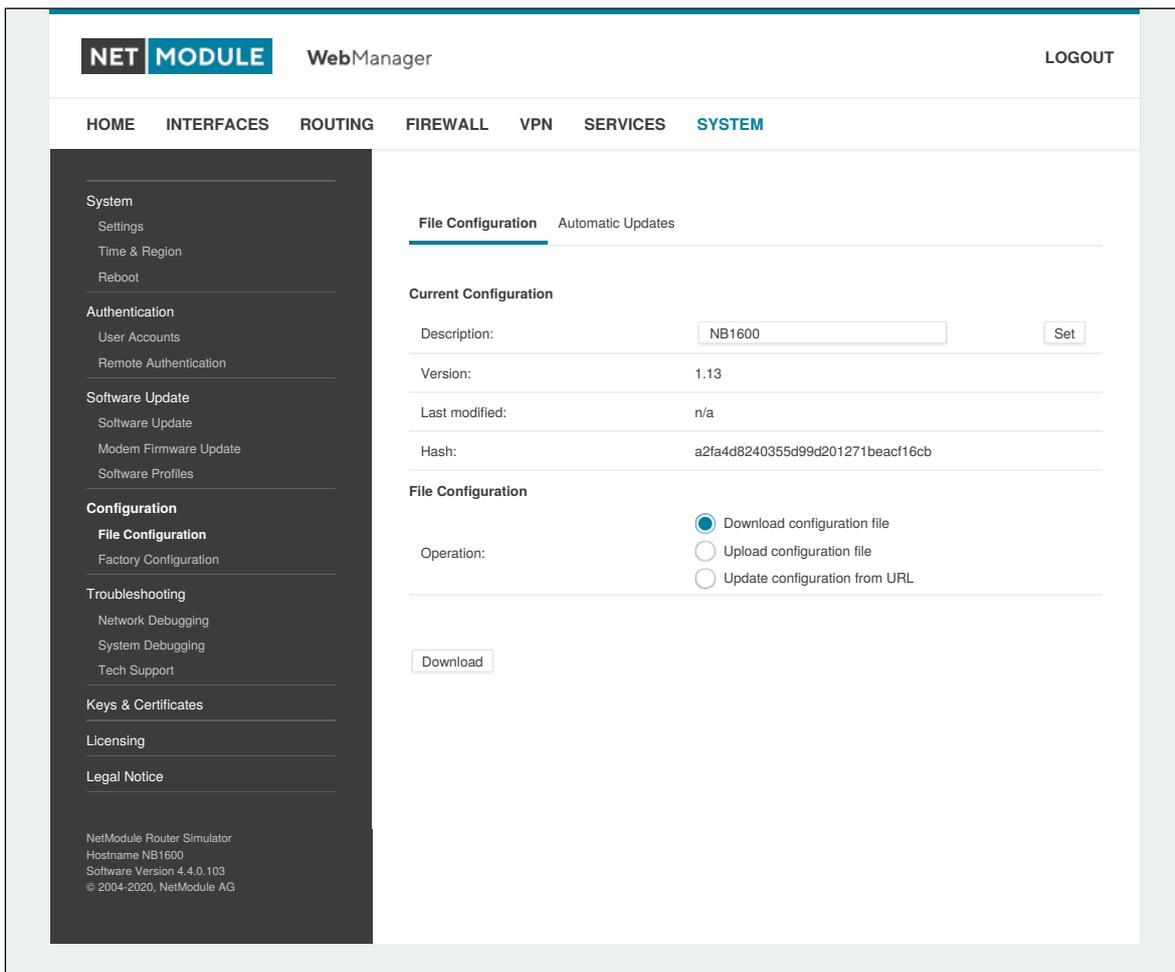


Figure 5.66.: Manual File Configuration

This section can be used to download the currently running system configuration (including essential files such as certificates). In order to restore a particular configuration you can upload a configuration previously downloaded. You can choose between missing configuration directives set to factory defaults or getting ignored, that means, potentially existing configuration directives will be kept at the system.

Automatic File Configuration

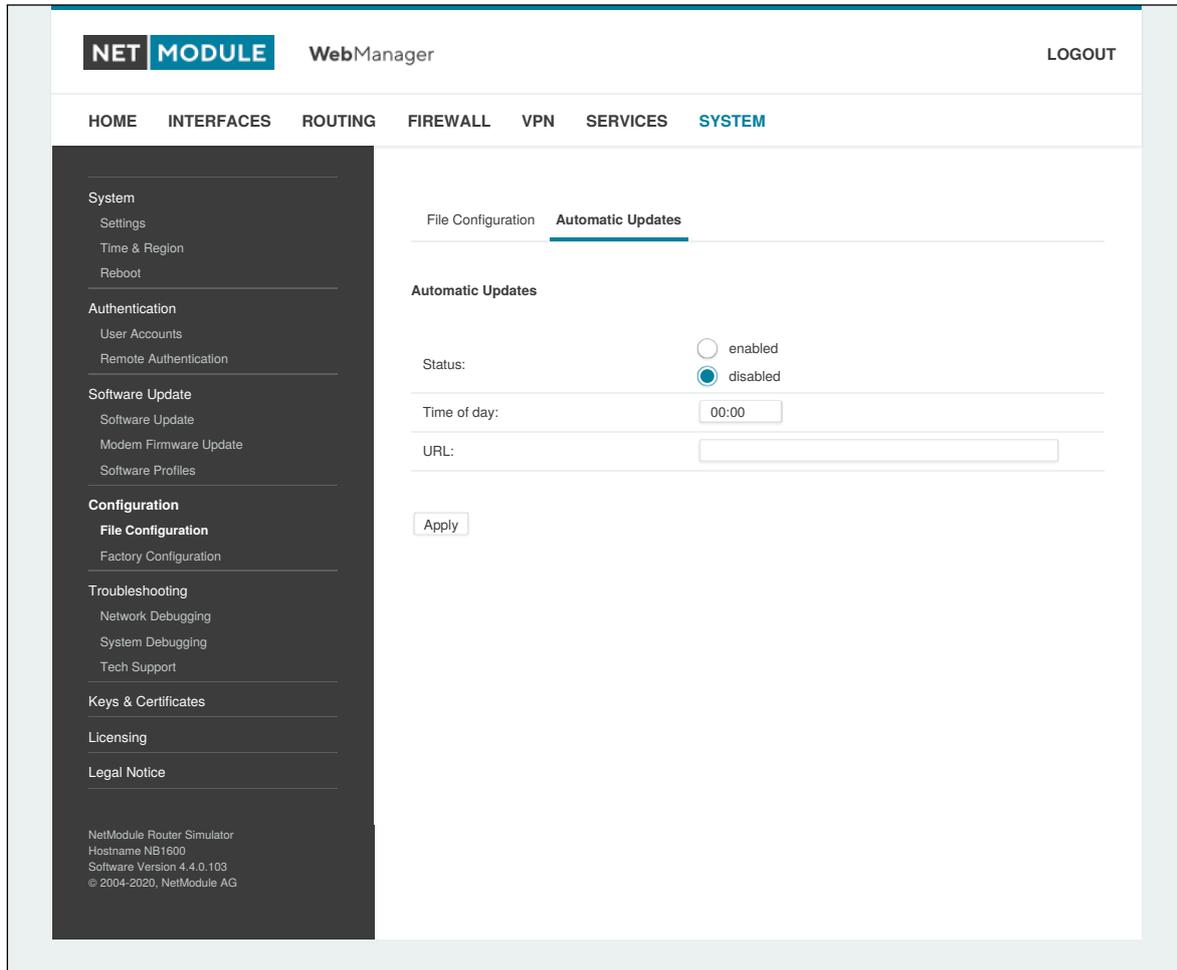


Figure 5.67.: Automatic File Configuration

This menu can be used to run an automatic configuration update of the system. It is configured as follows:

Parameter	Automatic File Configuration
Status	Enable/disable an automatic configuration update
Time of day	Time of day when the system should check for updates
URL	The URL where the configuration file should be retrieved from (supported protocols are HTTP, HTTPS, TFTP, FTP)

Factory Configuration

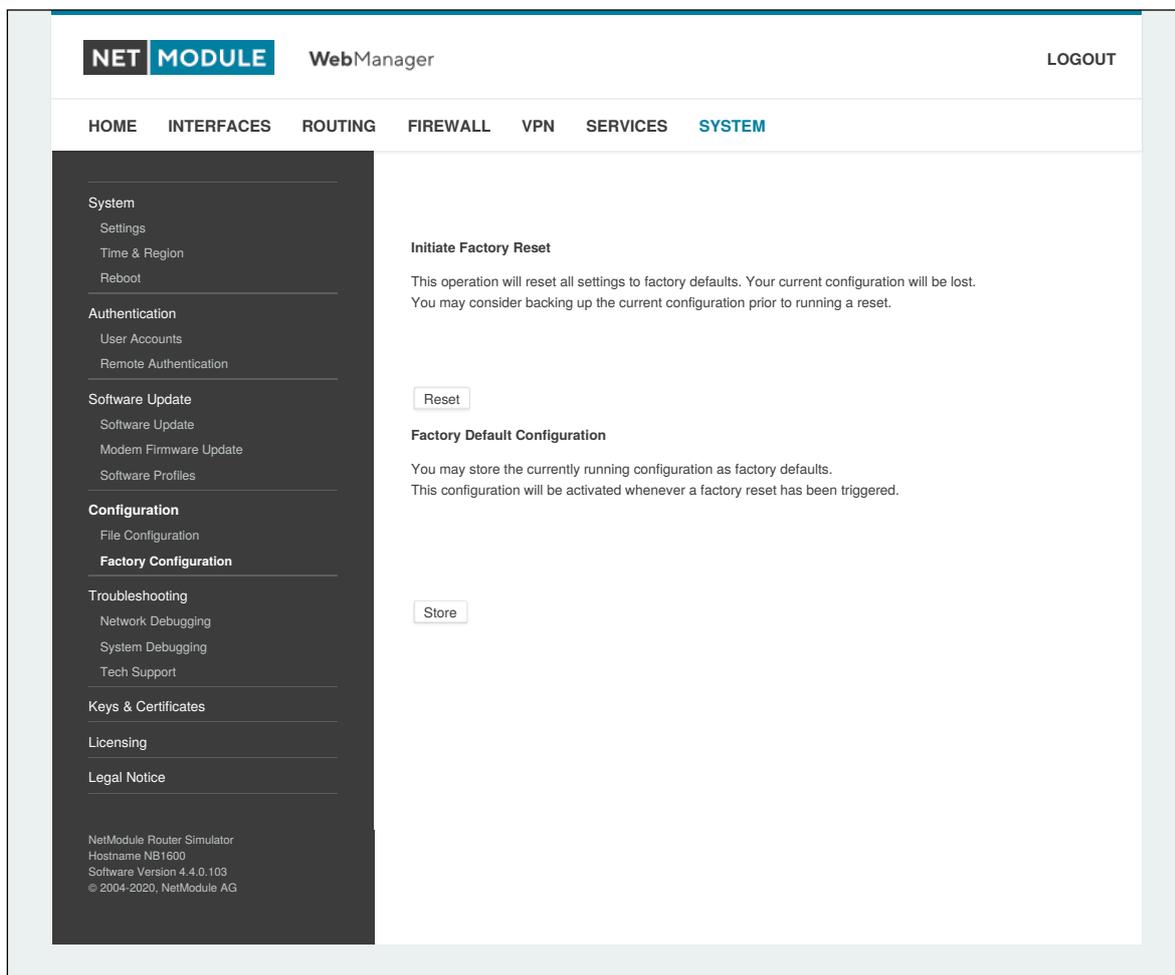


Figure 5.68.: Factory Configuration

This menu can be used to reset the device to factory defaults. Your current configuration will be lost. A successfully initiated factory reset can be noticed by all LEDs having been turned on. The factory reset will set the IP address of the first Ethernet interface back to 192.168.1.1. You will be able to communicate again with the device using the default network parameters. You may store the currently running configuration as factory defaults which will reside active even when a factory reset has been initiated (e.g. by your service staff).

Please ensure that this corresponds to a working configuration. A real factory reset to the default settings can be achieved by restoring the original factory configuration and initiating the factory reset again.

5.8.7. Troubleshooting

Network Debugging

There are several tools for network debugging like ping, traceroute, tcpdump and darkstat.

Parameter	Automatic software update
Ping	The ping utility can be used to verify whether a remote host can be reached via IP.
Traceroute	The traceroute utility can be used to print the route packets trace to a remote host.
Tcpdump	The tcpdump utility generates a network capture (PCAP) of an interface which can be later analyzed with Wireshark.

System Debugging

You can view the system log here by selection the option *Debug log* or if you are interested in the boot log select *Boot log*.

Another way to see what is going on on the box is opening a SSH or Telnet session as *root* and typing `tail-log`. Furthermore the system log can be redirected to a syslog server, see section 5.8.1.

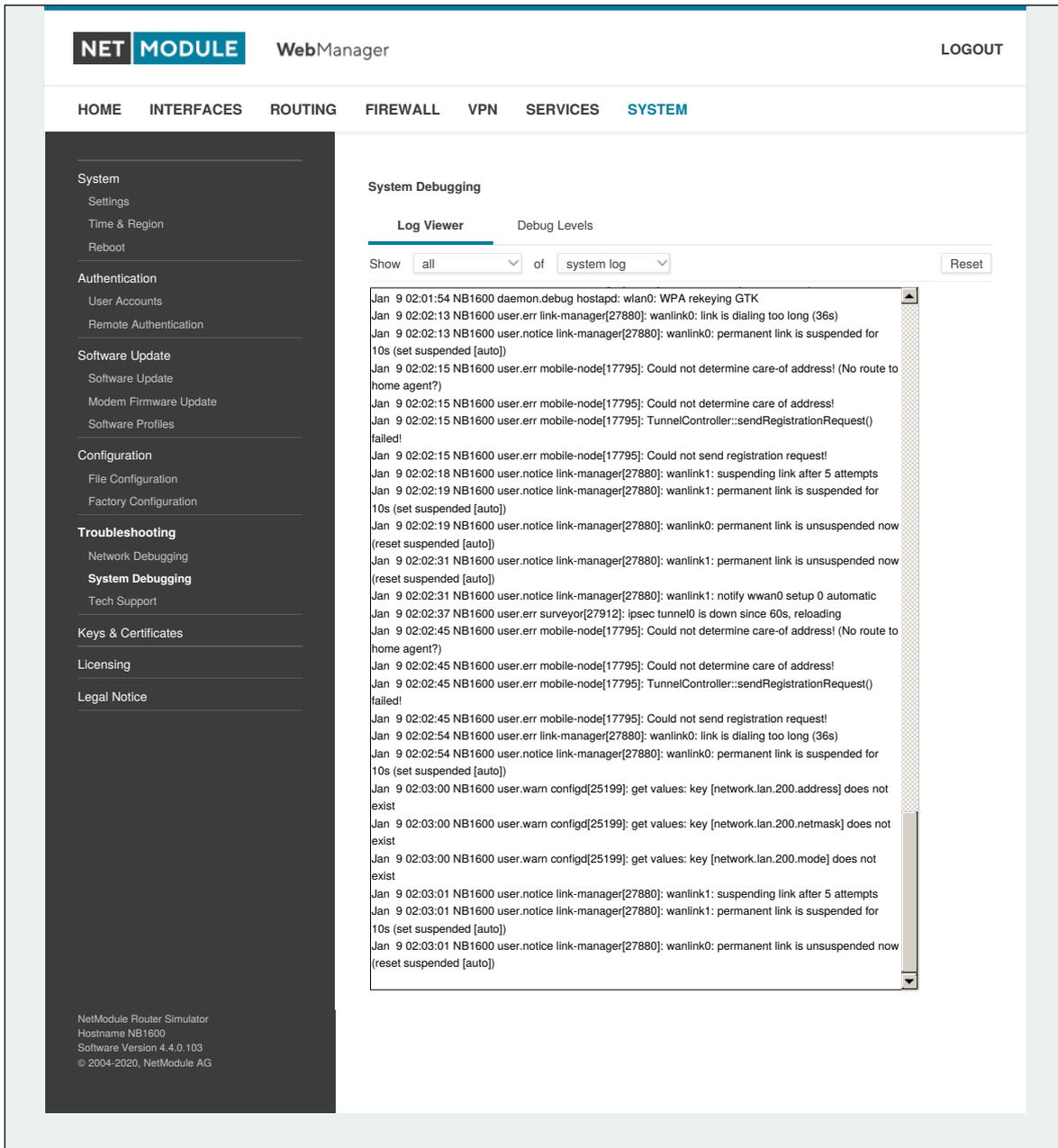


Figure 5.69.: Log Viewer

Tech Support

You can generate and download a tech support file here. We strongly recommend providing this file when getting in touch with our support team, either by e-mail or via our on-line support form, as it would significantly speed up the process of analyzing and resolving your problem. Log files can be viewed, downloaded and reset here. Please study them carefully in case of any issues. Various tools reside on this page for further analysis of potential configuration issues.

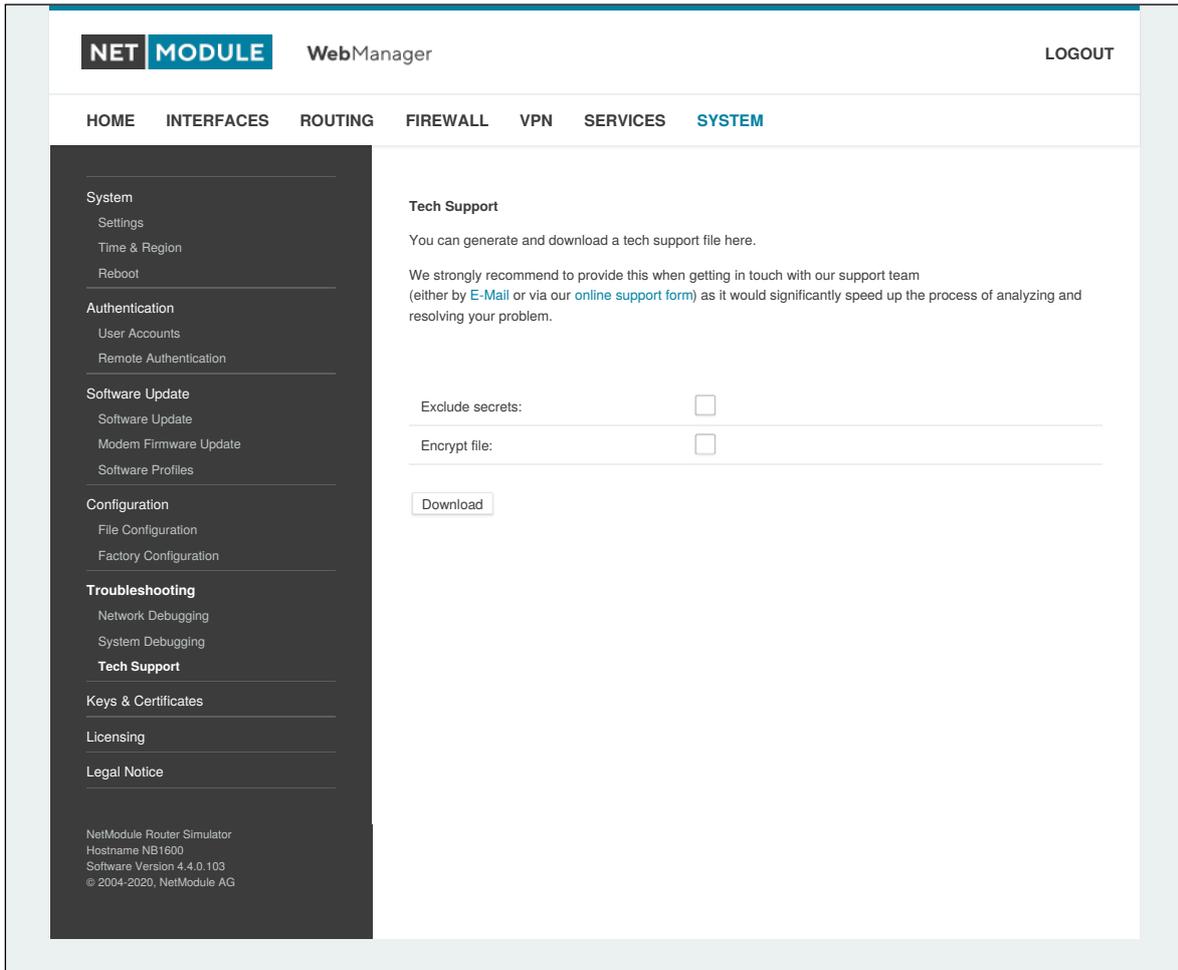


Figure 5.70.: Tech Support File

It is possible to trace any IP interface and inspect individual packet flows between hosts. This can be achieved by logging onto the box and start a network packet capture by using the tool *tcpdump*. We recommend to use the *-n* switch to bypass name resolution (e.g. *tcpdump -n -i lan0*). You may also generate a dump in PCAP format using the Web Manager, download it to your computer and perform further inspections with Wireshark (available at www.wireshark.org).

5.8.8. Keys and Certificates

The key and certificate page lets you generate required files for securing your services (such as HTTP and SSH server) but also to implement authentication and encryption for certificate-based VPN tunnels and WLAN clients.

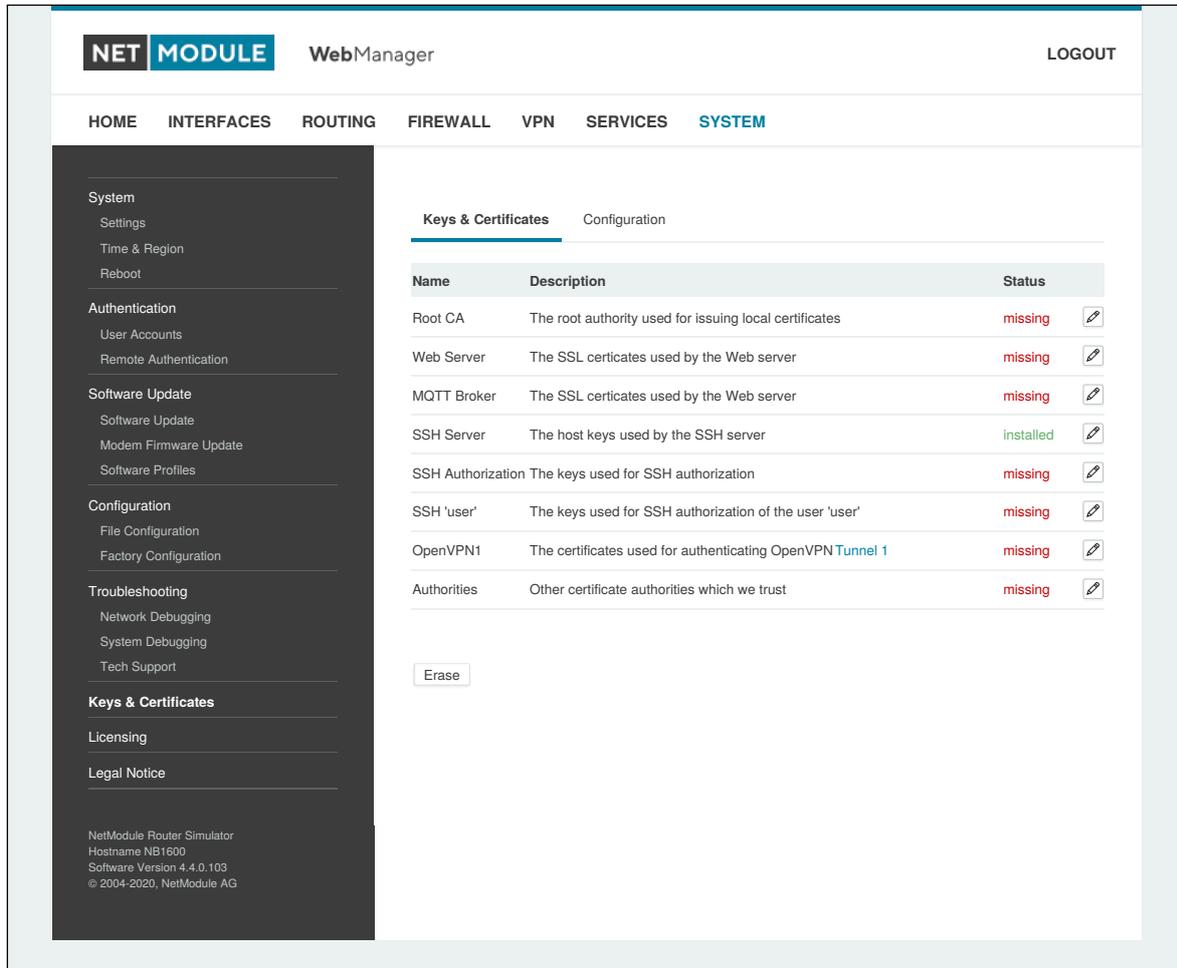


Figure 5.71.: Keys and certificates

The entry pages shows an overview about installed keys and certificates. The following sections may appear:

Type	Description
Root CA	The root Certificate Authority (CA) which issues certificates, its key can be used to certify it at trusted third party on other systems
Web Server	The certificates for the Web server required for running HTTP over SSL (HTTPS).
MQTT Broker	The certificates for the MQTT Broker required for running MQTT over TLS encrypted connection.
SSH Server	The DSS/DSA keys for the SSH server.

Type	Description
SSH Authorization	The keys used for SSH authorization.
OpenVPN	Server or client keys and certificates for running OpenVPN tunnels.
IPsec	Server or client keys and certificates for running IPsec tunnels.
WLAN	Keys and certificates for implementing certificate-based WLAN authentication (e.g. WPA-EAP-TLS).
ETH	Keys and certificates for authentication via IEEE 802.1X on Ethernet ports.
Authorities	Other certificate authorities which we trust when establishing SSL client connections.

Table 5.184.: Certificate Sections

For each certificate section it is possible to perform the following operations:

Operation	Description
generate locally	Generate key and certificate locally on the box (see 5.8.8 for more options)
upload files	Key and certificate will be uploaded. We support files in PKCS12, PKCS7, PEM/DER format as well as RSA/DSS keys in OpenSSH or Dropbear format.
enroll via SCEP	Enroll key and certificate via SCEP (see 5.8.8 for more options)
download certificate	Download key and certificate in ZIP format (files will be encoded in PEM format)
create signing request	Generate key locally and create a signing request to retrieve a certificate signed by another authority
erase certificate	Erase all keys and certificates associated with this section

Table 5.185.: Certificate Operations

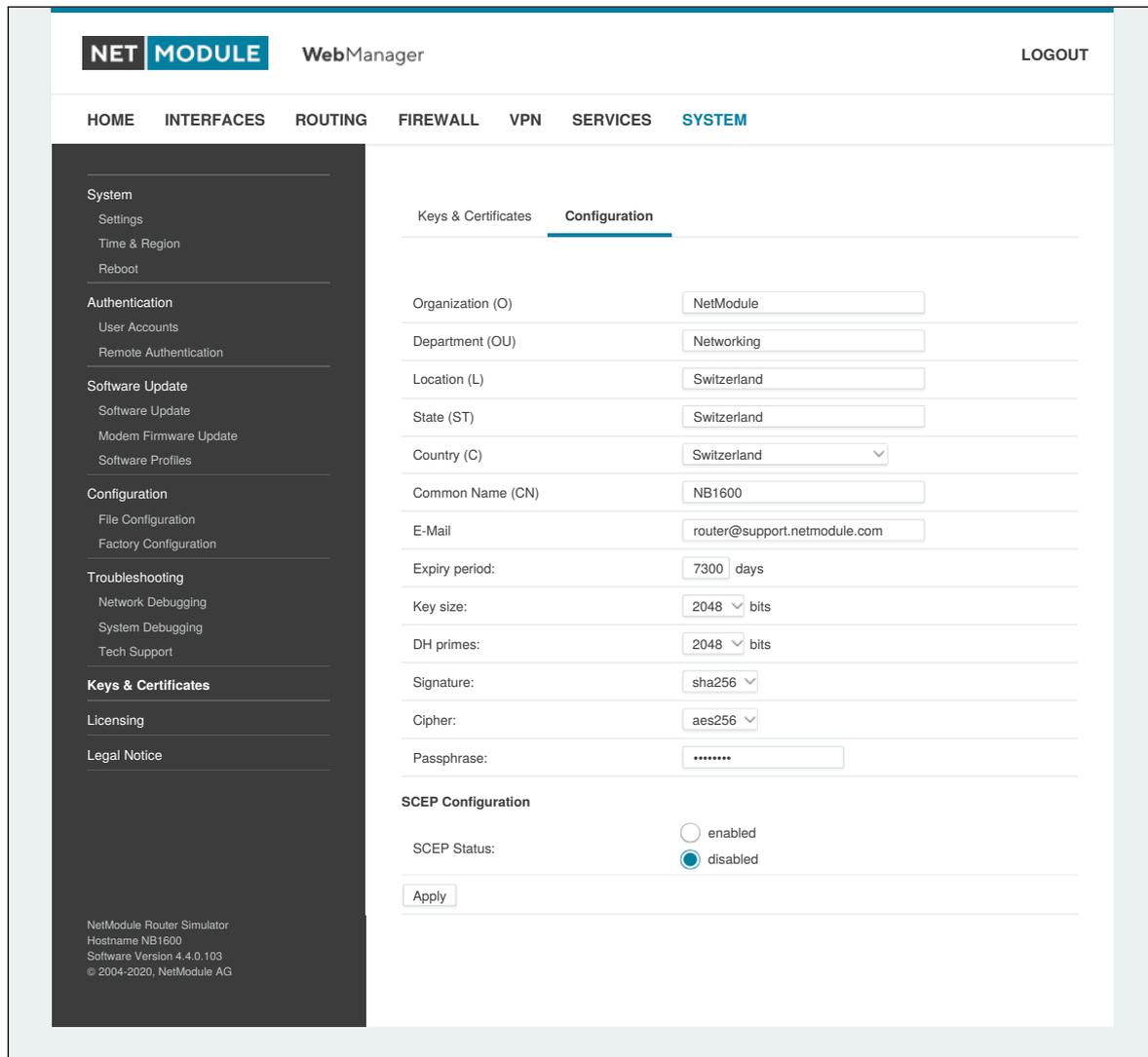
Configuration

Figure 5.72.: Certificate Configuration

This page provides some general configuration options which will be applied when operating on keys and certificates.

If keys, certificates and signing requests are generated locally, the following settings will be take into account:

Parameter	Certificate Configuration
Organisation (O)	The certificate owner's organization
Department (OU)	The name of the organizational unit to which the certificate issuer belongs
Location (L)	The certificate owner's location
State (ST)	The certificate owner's state

Parameter	Certificate Configuration
Country (C)	The certificate owner's country (usually a TLD abbreviation)
Common Name (CN)	The certificate owner's common name, mainly used to identify a host
E-Mail	The certificate owner's email address
Expiry period	The number of days a certificate will be valid from now on
Key size	The length of the private key in bits
DH primes	The number of bits for custom Diffie-Hellman primes
Signature	The signature algorithm when signing certificates
Passphrase	The passphrase for accessing/opening a private key. This passphrase is initialized to a random string the first time you log in. (see 5.1.1)

Please be aware of the fact, that the local random number generator (RNG) provides pretty good randomness for most applications. If stronger cryptography is mandatory, we suggest to create the keys at an external RNG device or manage all certificates completely on a remote certification server. Nevertheless, using a local certificate authority can issue and manage all required certificates and also run a certificate revocation list (CRL).

When importing keys, the certificate and key file can be uploaded individually encoded in PEM/DER or PKCS7 format. All files (CA certificate, certificate and private key) can also be uploaded in one stroke by using the container format PKCS12. RSA/DSS keys can be converted from OpenSSH or Dropbear formats. It is possible to specify the passphrase for opening the private key. Please note that the system will generally apply the system-wide certificate passphrase on a key when installing the certificate. Thus, changing the general passphrase will result in all local keys getting equipped with the new one.

SCEP Configuration

If certificates are getting enrolled by using the Simple Certificate Enrollment Protocol (SCEP) the following settings can be configured:

Parameter	SCEP Configuration
SCEP status	Specifies whether SCEP is enabled or not
URL	The SCEP URL, usually in the form <code>http://<host>/<path>/pkiclient.exe</code>
CA fingerprint	The fingerprint of the certificate used to identify the remote authority. If left empty, any CA will be trusted.
Fingerprint algorithm	The fingerprint algorithm for identifying the CA (MD5 or SHA1)
Poll interval	The polling interval in seconds for a certificate request
Request timeout	The max. polling time in seconds for a certificate request
ID type	Can be IP, Email or DNS
Password	The password for the scep server.

When enrolling certificates, the CA certificate will be initially fetched from the specified SCEP URL using the `getca` operation. It will be shown on the configuration page and it has to be verified that it belongs to the correct authority. Otherwise, the CA must be rejected. This part is essential when using SCEP as it builds up the chain of trust.

If a certificate enrollment request times out, it is possible to re-trigger the interrupted enrollment request and it will be resumed using the previously generated key. In case a request has been rejected, you are required to erase the certificate first and then start the enrollment process all over again.

Authorities

For SSL client connections (as used by SDK functions or when downloading configuration/software images) you might upload a list of CA certificates which are considered trusted.

To obtain the CA certificate from a particular site with Mozilla Firefox, the following steps will be required:

- Point the browser to the relevant HTTPS website
- Click the padlock in the address bar
- Click the **More Information** and the **View Certificate** button
- Select the **Details** tab press the **Export** button
- Choose a path for the file (e.g. website.pem)

Certificates from self-signed authorities can also be retrieved by running:

```
echo quit | \  
openssl s_client -showcerts -connect <host>:443 | \  
sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > other.crt
```

The PEM-encoded X.509 certificate files can be edited and concatenated using a simple editor (if required) and then uploaded to the box. Once installed, an SSL client connection will terminate if verification with any of those CA certificates fails.



5.8.10. Legal Notice

OSS Notice

We inform you that NetModule products may contain in part open-source software. We are distributing such open-source software to you under the terms of GNU General Public License (GPL), GNU Lesser General Public License (LGPL) or other open-source licenses.

These licenses allow you to run, copy, distribute, study, change and improve any software covered by GPL, Lesser GPL, or other open-source licenses without any restrictions from us or our end user license agreement on what you may do with that software. Unless required by applicable law or agreed to in writing, software distributed under open-source licenses is distributed on an "AS IS" basis, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.

To obtain the corresponding open source codes covered by these licenses, please contact our technical support at support@netmodule.com.

Acknowledgements

This product includes PHP, freely available from <http://www.php.net>.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).

This product includes cryptographic software written by Eric Young (ey@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

This product includes software written Jean-loup Gailly and Mark Adler.

This product includes software MD5 Message-Digest Algorithm by RSA Data Security, Inc.

This product includes an implementation of the AES encryption algorithm based on code released by Dr Brian Gladman.

Multiple-precision arithmetic code originally written by David Ireland
Software from The FreeBSD Project (www.freebsd.org)

Copyright (C) 2023, NetModule. All rights reserved.



5.9. LOGOUT

Please use this menu to log out from the Web Manager.



ipsec	IPsec connections
lighttpd	HTTP server
link-manager	WAN links
network	Networking
openvpn	OpenVPN connections
pptp	PPTP connections
qos	QoS daemon
smsd	SMS daemon
snmpd	SNMP daemon
surveyor	Supervision daemon
syslog	Syslog daemon
telnet	Telnet server
usbipd	USB/IP daemon
voiced	Voice daemon
vrrpd	VRRP daemon
wlan	WLAN interfaces
wwan-manager	WWAN manager

6.12. Debug System

The `debug` command can be used to obtain debug/log messages.

```
> debug -h  
Usage :  
       debug [-h] <target>
```

Available debug targets:

```
configd  
event-manager  
home-agent  
led-manager  
link-manager  
mobile-node  
qmid  
qosd  
scripts  
sdkhost  
ser2net  
smsd  
surveyor  
swupdate  
system  
voiced  
watchdog  
wwan-manager  
wwanmd
```

6.13. Resetting System

The `reset` command can be used to reset the router back to factory defaults.



send - Send USSD code

Key usage:

```
command=send&arg0=ussd&arg1=<card>&arg2=<code>
```

Notes:

The argument card specifies the card module index (e.g. 0 for wwan0). The USSD code can consist of digits, plus signs, asterisks (can be encoded with `\%2A`) and dashes (can be encoded with `\%23`).

Examples:

```
http://192.168.1.1/cli.php?version=2&output=html&usr=admin&pwd=admin01&command=send&arg0=ussd&arg1=0&arg2=%2A100%23
```



A. Appendix

A.1. Abbreviations

Abbreviation	Description
ANY	Generally includes all options offered by the current section
APN	Access Point Name
ASU	Arbitrary Strength Unit
CID	A Cell ID is a generally unique number used to identify each Base Transceiver Station (BTS).
CID	Cell-ID
CLI	Command Line Interface, a generic interface to query the router or perform system tasks
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ETH _x	Corresponds to Ethernet interfaces (either single or switched ones)
FQDN	Fully qualified domain name
GHz	GigaHertz
GNSS _x	Specifies a Global Navigation Satellite System module
GUI	Graphical User Interface
HTTP	HyperText Transfer Protocol
ICCID	Integrated Circuit Card Identifier
IMEI	International Mobile Station Equipment Identity
IMSI	International Mobile Subscriber Identity
IN _x	Specifies a digital I/O input port (DI _x)
LAC	Location Area Code
LAC	The Location Area Code corresponds to an identifier of a set of base stations that are grouped together to optimize signaling
LAI	Location Area Identification
LAI	The Location Area Identity is a globally unique number that identifies the country, network provider and location area
LAN _x	LAN interfaces which are generally based on Ethernet interfaces (including bridges)
MAC	Media Access Control
Mbps	Megabits per second
MCC	Mobile Country Code
MCS	Modulation Coding Scheme



Abbreviation	Description
MEID	Mobile Equipment Identifier
MHz	MegaHertz
MNC	Mobile Network Code
Mobilex	Identifies a WWAN modem
MOBILEIP _x	Refers to a Mobile IP tunnel interface
MSISDN	Mobile Subscriber Integrated Services Digital Network Number
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit
NAPT	Network Address and Port Translation
NAT	Network Address Translation
NTP	Network Time Protocol
OUT _x	Specifies a digital I/O output port (DO _x)
PPTP _x	Specifies a PPTP tunnel interface
PSK	Pre-Shared Key
RSRP	Referenz Signal Received Power
RSRQ	Reference Signal Received Quality
RSSI	Received Signal Strength Indication
SDK	Script Development Kit which can be used to program applications
SERIAL _x	Identifies a serial port
SIM _x	Specifies the SIM slot as seen on the front panel
SIM	Subscriber Identity Module
SMS	Short Message Service
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSID	Service Set Identifiers, can be used to define multiple WLAN networks on a module
STP	Spanning Tree Protocol
TAP _x	Specifies an OpenVPN tunnel interface (based on TAP)
TUN _x	Specifies an OpenVPN tunnel interface (based on TUN)
USSD	Unstructured Supplementary Service Data
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol

Abbreviation	Description
WAN	WAN links include all Wide Area Network interfaces which are currently activated in the system
WDS	Wireless Distribution System
WLAN _x	Refers to a Wireless LAN interface which will be represented as additional LAN interface when configured as access point
WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3
WWAN _x	Refers to a Wireless Wide Area Network (2G/3G/4G) connection

Table A.1.: Abbreviations

In general, internal interfaces are written lower-case and may have a different naming. Their index starts from zero, whereas interfaces seen by the user will be written in capital letters starting from one.

A.2. System Events

ID	Ereignis	Beschreibung
101	wan-up	WAN-Verbindung aufgebaut
102	wan-down	WAN-Verbindung unterbrochen
201	dio-in1-on	DIO IN1 eingeschaltet
202	dio-in1-off	DIO IN1 ausgeschaltet
203	dio-in2-on	DIO IN2 eingeschaltet
204	dio-in2-off	DIO IN2 ausgeschaltet
205	dio-out1-on	DIO OUT1 eingeschaltet
206	dio-out1-off	DIO OUT1 ausgeschaltet
207	dio-out2-on	DIO OUT2 eingeschaltet
208	dio-out2-off	DIO OUT2 ausgeschaltet
301	gps-up	GPS-Signal verfügbar
302	gps-down	GPS-Signal nicht verfügbar
401	openvpn-up	OpenVPN-Verbindung aufgebaut
402	openvpn-down	OpenVPN-Verbindung unterbrochen
403	ipsec-up	IPsec-Verbindung aufgebaut
404	ipsec-down	IPsec-Verbindung unterbrochen
406	pptp-up	PPTP-Verbindung aufgebaut
407	pptp-down	PPTP-Verbindung unterbrochen
408	dialin-up	Dial-In-Verbindung aufgebaut



ID	Ereignis	Beschreibung
409	dialin-down	Dial-In-Verbindung unterbrochen
410	mobileip-up	Mobile IP-Verbindung aufgebaut
411	mobileip-down	Mobile IP-Verbindung unterbrochen
412	gre-up	GRE-Verbindung aufgebaut
413	gre-down	GRE-Verbindung unterbrochen
501	system-login-failed	Anmeldung fehlgeschlagen
502	system-login-succeeded	Anmeldung erfolgreich
503	system-logout	Benutzer abgemeldet
504	system-rebooting	Systemneustart eingeleitet
505	system-startup	System gestartet
506	test	Testereignis
507	sdk-startup	SDK gestartet
508	system-time-updated	Systemzeit aktualisiert
509	system-poweroff	Systemabschaltung ausgelöst
510	system-error	System befindet sich im Fehlerzustand
511	system-no-error	System hat Fehlerzustand verlassen
601	sms-sent	SMS gesendet
602	sms-notsent	SMS nicht gesendet
603	sms-received	SMS empfangen
604	sms-report-received	SMS-Bericht empfangen
701	call-incoming	Eingehender Sprachanruf
702	call-outgoing	Abgehender Sprachanruf wird aufgebaut
801	ddns-update-succeeded	Aktualisierung des Dynamic DNS erfolgreich
802	ddns-update-failed	Aktualisierung des Dynamic DNS fehlgeschlagen
901	usb-storage-added	USB-Speichergerät hinzugefügt
902	usb-storage-removed	USB-Speichergerät entfernt
903	usb-eth-added	USB-Ethernet-Gerät hinzugefügt
904	usb-eth-removed	USB-Ethernet-Gerät entfernt
905	usb-serial-added	Seriell USB-Gerät hinzugefügt
906	usb-serial-removed	Seriell USB-Gerät entfernt
1001	redundancy-master	Router ist jetzt der Master-Router

ID	Ereignis	Beschreibung
1002	redundancy-backup	Router ist jetzt der Backup-Router

Table A.2.: Systemereignisse



A.3. Factory Configuration

The factory configuration including default values for any configuration parameter can be derived from the file `/etc/config/factory-config.cfg` on the router. You may also call `cli get -f <parameter>` for obtaining a specific default value.

