

User module **Advanced Security**

APPLICATION NOTE



ENABLING CONNECTED INTELLIGENCE

Used symbols



Danger – important notice, which may have an influence on the user's safety or the function of the device.



Attention – notice on possible problems, which can arise in specific cases.



Information, notice – information, which contains useful advice or special interest.



Conel s.r.o., Sokolska 71, 562 04 Usti nad Orlici, Czech Republic
Manual issued in CZ, May 22, 2015

Contents

| | | |
|----------|--|-----------|
| 1 | Description of user module | 1 |
| 2 | Configuration | 2 |
| 2.1 | Network security options | 2 |
| 2.2 | SSH access administration | 6 |
| 2.2.1 | Add host to access list | 6 |
| 2.2.2 | Remove host from access list | 7 |
| 2.2.3 | Clear list | 8 |
| 3 | Module activity monitoring | 9 |
| 3.1 | System log | 9 |
| 3.2 | Setup log | 10 |
| 4 | Recommended literature | 11 |


List of Figures

| | | |
|---|--|----|
| 1 | Access to the router with <i>Advanced Security</i> via SSH | 1 |
| 2 | Network security options | 5 |
| 3 | Add host to access list | 6 |
| 4 | Remove host from access list | 7 |
| 5 | Clear access list | 8 |
| 6 | System log | 9 |
| 7 | Setup log | 10 |

List of Tables

| | | |
|---|---|---|
| 1 | Description of security rules | 3 |
| 2 | Enabled / blocked ICMP messages | 4 |

1. Description of user module

 User module *Advanced Security* is not contained in the standard router firmware. Uploading of this user module is described in the Configuration manual (see [1, 2]).



The user module is v2 and v3 router platforms compatible.

Advanced Security module extends configuration of Conel router of ability to set the number of additional security features. These include for example disabling (or enabling) sending error messages within the ICMP protocol, disabling (or enabling) the ICMP protocol as a whole, disabling (or enabling) access to the router via Telnet or SSH etc. Detailed descriptions of all options can be found in chapter 2 *Configuration* on page 2.

This module also allows user to regulate access to the router via SSH (network protocol for secure data communication). There is an access list, where it can be specified IP addresses from which it is possible to access to the router via SSH. Access from other addresses is automatically disabled (packets are dropped).

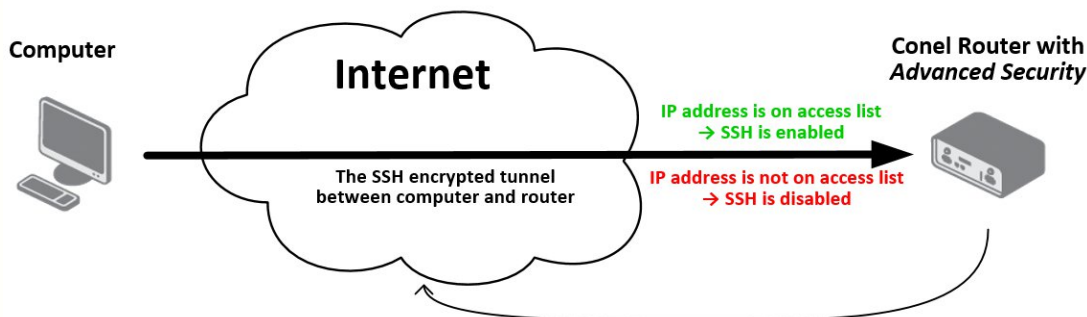


Figure 1: Access to the router with *Advanced Security* via SSH

For configuration *Advanced Security* user module is available web interface, which is invoked by pressing the module name on the *User modules* page of the router web interface. The left part of the web interface contains the menu with pages for monitoring (*Status*), configuration of security rules (*Network security options*), *SSH access administration* and *Customization* of the module. *Customization* block contains only the *Return* item, which switches this web interface to the interface of the router.

2. Configuration

Configuration of *Advanced Security* user module is divided into two separate parts – *Network security options* and *SSH access administration*.

2.1 Network security options

Configuration form on *Network security options* page allows user to set a few security rules which ensure higher security of Conel routers. Their meaning is described in the table below.

| Item | Description |
|------------------------|--|
| SSHD banner | Disables (or enables) displaying of a banner informing unauthorised users that their use is in fact unauthorised (they are not in the access list). |
| Restrict SSHD access | Regulates access to the router via SSH. Only authorized users are accepted (specified in the access list). |
| Restrict Telnet access | Regulates access to the router via Telnet. Only authorized users are accepted. |
| Source based routing | Controls the ability to use source basic routing mechanism in kernel. Attackers can use source routing to generate traffic pretending to originate from inside your network, but that is actually routed back along the path from which it came, so attackers can compromise your network. Source routing is rarely used for legitimate purposes, so it is safe to disable it. By using this control option, its possible to turn off such routing rule by disabling source routing ability in kernel completely. |
| Directed broadcast | Enables or disables permit to send directed broadcast. Directed broadcast is a packet whose destination address is a valid broadcast address for some IP subnet, but which can originates from a node that is not itself part of that destination subnet. Drops ICMP reply and requests to broadcast address and network base (ICMP 0, ICMP 8). |
| IP classless routing | <i>Disabled</i> – router drops packet which are classless <i>Enabled</i> – it performs default Linux behaviour and route packet to supernet. |

Continued on next page

Continued from previous page

| Item | Description |
|-----------------------|--|
| ICMP messages | Filters out or disables non mandatory ICMP messages. Only ICMP messages needed for proper network function will be kept and processed. Table of enabled/blocked ICMP messages is placed below this table. |
| DNS broadcast | By default, name queries are sent to the broadcast address 255.255.255.255. This item disables DNS name resolution if it is not needed. |
| ICMP protocol | Disables (or enables) ICMP protocol in kernel. This also means that disabling this option overset <i>ICMP messages</i> option. This should be used only in case of specific situations, because it also disables ICMP unreachable messages, which can lead to unexpected behaviour... |
| Fragmentation | Disables (or enables) packet fragmentation. If a packet is fragmented, only the first fragment contains the complete header. Other fragments contain only IP addresses (for example, there is no specified protocol). |
| TCP establish timeout | The time of waiting for establishing of TCP connection. |

Table 1: Description of security rules

The table below shows enabled/blocked ICMP messages in case that *ICMP messages* option is set to *Disabled*.

| Type | Code | Description | Query | Error | Status |
|------|------|---|-------|-------|---------|
| 0 | 0 | Echo Reply | x | | enabled |
| 3 | 0 | Network Unreachable | | x | blocked |
| 3 | 1 | Host Unreachable | | x | enabled |
| 3 | 2 | Protocol Unreachable | | x | blocked |
| 3 | 3 | Port Unreachable | | x | enabled |
| 3 | 4 | Fragmentation needed but no frag. bit set | | x | enabled |
| 3 | 5 | Source routing failed | | x | blocked |
| 3 | 6 | Destination network unknown | | x | blocked |
| 3 | 7 | Destination host unknown | | x | blocked |
| 3 | 8 | Source host isolated (obsolete) | | x | enabled |
| 3 | 9 | Destination network administratively prohibited | | x | blocked |
| 3 | 10 | Destination host administratively prohibited | | x | blocked |

Continued on next page

Continued from previous page

| Type | Code | Description | Query | Error | Status |
|------|------|--|-------|-------|----------|
| 3 | 11 | Network unreachable for TOS | | x | blocked |
| 3 | 12 | Host unreachable for TOS | | x | blocked |
| 3 | 13 | Communication administratively prohibited by filtering | | x | blocked |
| 3 | 14 | Host precedence violation | | x | blocked |
| 3 | 15 | Precedence cutoff in effect | | x | blocked |
| 4 | 0 | Source quench | | | enabled |
| 5 | 0 | Redirect for network | | | blocked |
| 5 | 1 | Redirect for host | | | blocked |
| 5 | 2 | Redirect for TOS and network | | | blocked |
| 5 | 3 | Redirect for TOS and host | | | blocked |
| 8 | 0 | Echo request | x | | see note |
| 9 | 0 | Router advertisement | | | blocked |
| 10 | 0 | Route solicitation | | | blocked |
| 11 | 0 | TTL equals 0 during transit | | x | blocked |
| 11 | 1 | TTL equals 0 during reassembly | | x | enabled |
| 12 | 0 | IP header bad (catchall error) | | x | enabled |
| 12 | 1 | Required options missing | | x | enabled |
| 13 | 0 | Timestamp request (obsolete) | x | | blocked |
| 14 | | Timestamp reply (obsolete) | x | | blocked |
| 15 | 0 | Information request (obsolete) | x | | blocked |
| 16 | 0 | Information reply (obsolete) | x | | blocked |
| 17 | 0 | Address mask request | x | | blocked |
| 18 | 0 | Address mask reply | x | | blocked |

Table 2: Enabled / blocked ICMP messages

Note for *Echo request*: sending is blocked, receiving is limited to 2 per second.

| Advanced network security configuration | |
|---|------------|
| SSHD banner | Disabled ▼ |
| Restrict SSHD access | Disabled ▼ |
| Restrict Telnet access | Disabled ▼ |
| Source based routing | Disabled ▼ |
| Directed broadcast | Enabled ▼ |
| IP classless routing | Enabled ▼ |
| ICMP messages | Enabled ▼ |
| DNS broadcast | Enabled ▼ |
| ICMP protocol | Enabled ▼ |
| Fragmentation | Enabled ▼ |
| TCP establish timeout | 63 ▼ |

Apply

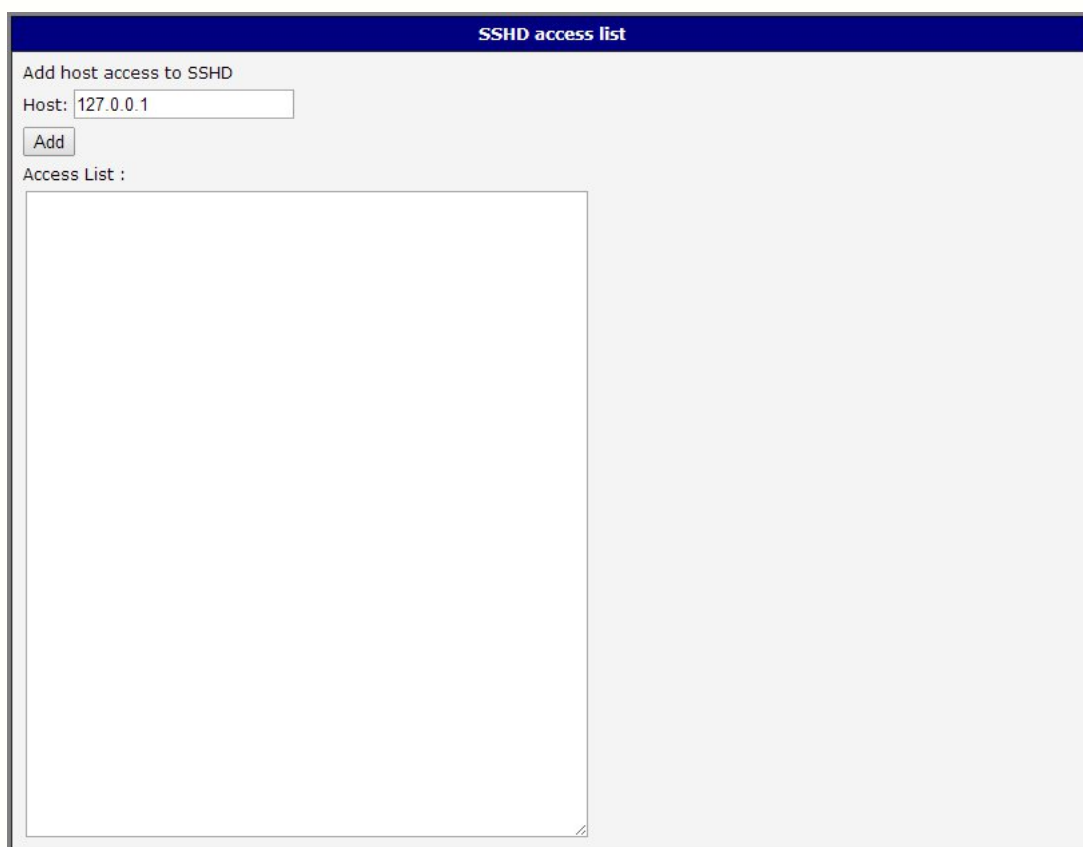
Figure 2: Network security options

2.2 SSH access administration

For the administration of access to the router via SSH serve three items in the *SSH access administration* part of the main menu.

2.2.1 Add host to access list

The first item intended for the administration of access to the router via SSH – *Add host to access list* – allows user to add IP address to Access List. IP address is entered to the *Host* box and added to the Access List using *Add* button. Access from IP addresses which are not listed in the Access List is automatically rejected.



The screenshot shows a web-based configuration interface titled "SSHD access list". It contains a section "Add host access to SSHD" with a "Host:" label and a text input field containing "127.0.0.1". Below the input field is an "Add" button. Underneath this section is a label "Access List :" followed by a large, empty rectangular box intended for displaying the list of IP addresses.

Figure 3: Add host to access list

2.2.2 Remove host from access list

Remove host from access list item allows user to remove particular IP address from access list (before removing this address from access list, it is possible to access to the router via SSH). IP address is entered to the *Host* box and removed from the Access List using *Delete* button under the *Host* box.

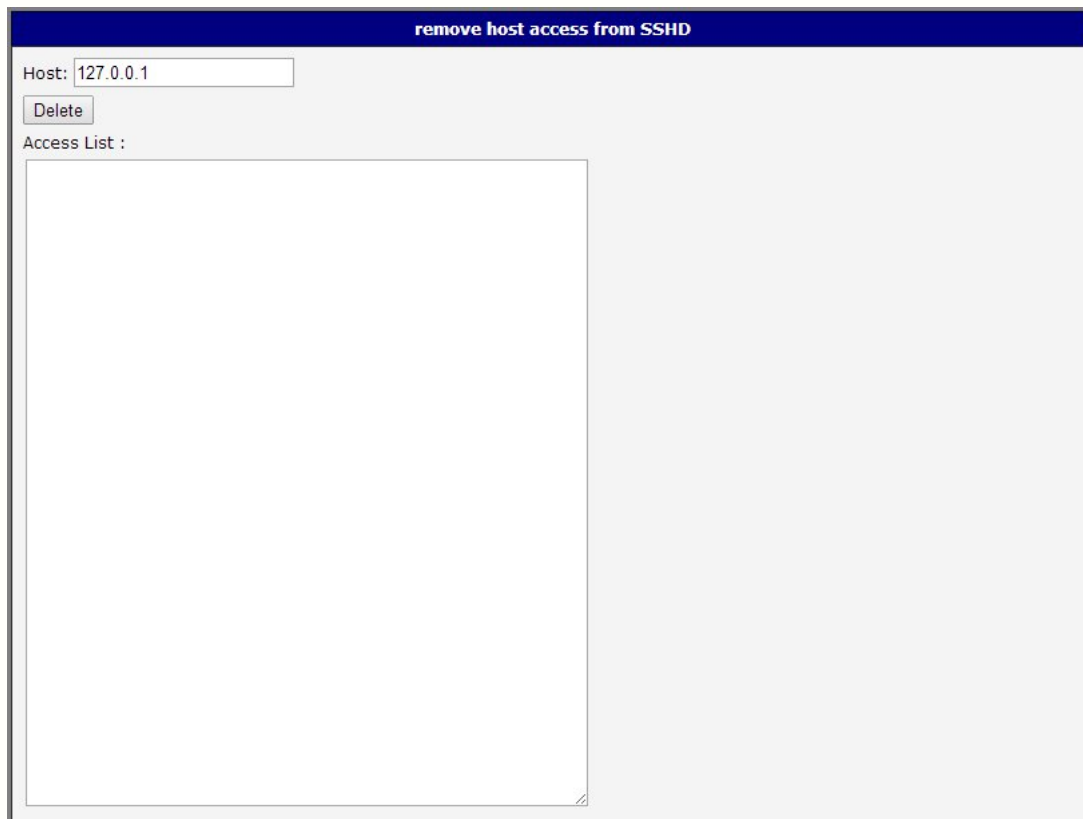


Figure 4: Remove host from access list

2.2.3 Clear list

The last item intended for the administration of access to the router via SSH – *Clear list* – allows user to delete all IP addresses from the Access List. Clearing is done by pressing *Clear* button on the top of the window.

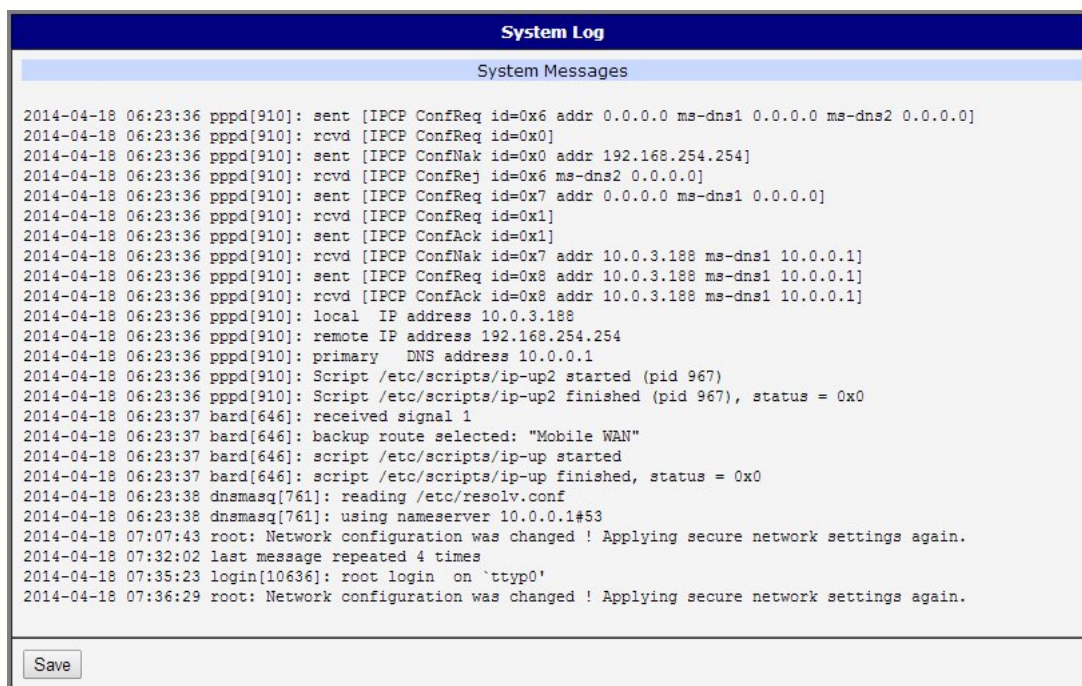


Figure 5: Clear access list

3. Module activity monitoring

3.1 System log

In case of any problems it is possible to view the system log by pressing the *System Log* menu item. In the window are displayed detailed reports from individual applications running in the router including possible reports relating to the *Advanced Security* module.



The screenshot shows a window titled "System Log" with a sub-header "System Messages". It displays a list of system messages with timestamps and details. At the bottom, there is a "Save" button.

```

2014-04-18 06:23:36 pppd[910]: sent [IPCP ConfReq id=0x6 addr 0.0.0.0 ms-dns1 0.0.0.0 ms-dns2 0.0.0.0]
2014-04-18 06:23:36 pppd[910]: rcvd [IPCP ConfReq id=0x0]
2014-04-18 06:23:36 pppd[910]: sent [IPCP ConfNak id=0x0 addr 192.168.254.254]
2014-04-18 06:23:36 pppd[910]: rcvd [IPCP ConfReq id=0x6 ms-dns2 0.0.0.0]
2014-04-18 06:23:36 pppd[910]: sent [IPCP ConfReq id=0x7 addr 0.0.0.0 ms-dns1 0.0.0.0]
2014-04-18 06:23:36 pppd[910]: rcvd [IPCP ConfReq id=0x1]
2014-04-18 06:23:36 pppd[910]: sent [IPCP ConfAck id=0x1]
2014-04-18 06:23:36 pppd[910]: rcvd [IPCP ConfNak id=0x7 addr 10.0.3.188 ms-dns1 10.0.0.1]
2014-04-18 06:23:36 pppd[910]: sent [IPCP ConfReq id=0x8 addr 10.0.3.188 ms-dns1 10.0.0.1]
2014-04-18 06:23:36 pppd[910]: rcvd [IPCP ConfAck id=0x8 addr 10.0.3.188 ms-dns1 10.0.0.1]
2014-04-18 06:23:36 pppd[910]: local IP address 10.0.3.188
2014-04-18 06:23:36 pppd[910]: remote IP address 192.168.254.254
2014-04-18 06:23:36 pppd[910]: primary DNS address 10.0.0.1
2014-04-18 06:23:36 pppd[910]: Script /etc/scripts/ip-up2 started (pid 967)
2014-04-18 06:23:36 pppd[910]: Script /etc/scripts/ip-up2 finished (pid 967), status = 0x0
2014-04-18 06:23:37 bard[646]: received signal 1
2014-04-18 06:23:37 bard[646]: backup route selected: "Mobile WAN"
2014-04-18 06:23:37 bard[646]: script /etc/scripts/ip-up started
2014-04-18 06:23:37 bard[646]: script /etc/scripts/ip-up finished, status = 0x0
2014-04-18 06:23:38 dnsmasq[761]: reading /etc/resolv.conf
2014-04-18 06:23:38 dnsmasq[761]: using nameserver 10.0.0.1#53
2014-04-18 07:07:43 root: Network configuration was changed ! Applying secure network settings again.
2014-04-18 07:32:02 last message repeated 4 times
2014-04-18 07:35:23 login[10636]: root login on 'tty0'
2014-04-18 07:36:29 root: Network configuration was changed ! Applying secure network settings again.
  
```

Figure 6: System log

3.2 Setup log

The *Advanced security setup log* window displays detailed information about the current settings of this module. The data reflect the settings made in the *Network security* configuration form.



```
Advanced security setup log

Fri Apr 18 07:07:43 GMT-1 2014
Disabling SSHD banner.
SSHD banner not enabled, skipping.
Disabling source routing.
Enabling directed broadcast.
Enabling IP_CLASSLESS_ROUTING.
enable_ip_classless_routing , not implemented
Enabling DNS broadcasting.
Enabling ICMP protocol.
Enabling ICMP messages.
Enabling fragmentation.
TCP SYN timeout set to 63 seconds
Restricting SSHD access
Block access to ssh for all unlisted hosts.
Fri Apr 18 07:07:48 GMT-1 2014
```

Figure 7: Setup log

4. Recommended literature

- [1] Conel: **Configuration manual for v2 routers**
- [2] Conel: **Configuration manual for v3 routers**