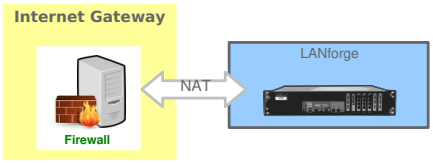
sales@candelatech.com
support@candelatech.com
+1 (360) 380-1618 [PST, GMT -8]

Configure a Remote LANforge

Goal: Configure LANforge to be securely accessed via an Internet accessible gateway.

Follow these guidelines to configure a LANforge server so that it is less abusable if accessible via the Internet. Ideally the only method of access is via SSH. Remember that LANforge systems are designed for isolated environments and convenient usability. Never connect a LANforge system directly to the Internet. It is not secure. Requires version 5.4.6



1. Prepare the Gateway

The internet gateway would want the LANforge system management address plugged into it. The following steps assume the gateway is configured to provide DHCP on the LAN and the LANforge management port (eth0) is using DHCP. Use the LANforge Configuration tool or `lfconfig` as necessary.

A. We do not suggest placing the LANforge in a full DMZ network where all public requests are forwarded to the LANforge. That is not secure.

B. Just forward the SSH port (`22/tcp`) to the LANforge

C. Disable Universal Plug-n-Play (UPnP)

D. Disable WAN administration ports (those are never secure)

2. Prepare the LANforge

We will configure the LANforge server to change the management port and to not manage the default ethernet interface. The server should not accept LANforge protocol commands on every interface, making it much more secure. For this discussion, we will use the `lfconfig` script because that is always easy to access from an SSH connection. Also, we will assume that the LANforge GUI will **NOT run on this machine.**

A. Stop the GUI and disable the autostart GUI feature

A.
```
$ killall lfclient.bash
```

B.
```
$ killall java
```

C.
```
$ rm -f /home/lanforge/.config/autostart/LANforge-auto.desktop
```

B. ## Configure LANforge server to use loopback as management port

A.
```
$ sudo -s
```

B.
```
# cd /home/lanforge
```

C.
```
# ./serverctl.bash stop
```

D.
```
# ./lfconfig
```

E. Typical screen:

```
Interfaces: eth0
Resource interface assignment:
  Resource 1:
Specified Resource Addresses:
  127.0.0.1:4004
Key               Acceptable Values          Value
*************************************************
log_level         [0-65535]                  7
log_dir           [directory path]           /home/lanforge
add_resource_addr [host:port]                SEE LIST ABOVE
rem_resource_addr [host:port]                SEE LIST ABOVE
realm             [1-255]                    255
resource          [1-511]                    1
mgt_dev           [ethernet device]          eth0
mode              [resource, manager, both]  both
log_file_len      [0-2G]                     0
bind_mgt          [0-1]                      0
shelf             [1-8]                      1
dev_ignore        [eth0 eth1 ... ethN]
first_cli_port    [1025-4199]                4001
connect_mgr       [host:port]
gps_dev           [device file]              NONE
max_tx            [1-500]                    5
max_send_mmsg_mem [1000-500000]              32000
max_send_mmsg_pkts [1-1000]                  500
keepalive         [1000-500000]              30000
wl_probe_timer    [50-2000]                  50
Other Commands:   help, show_all
*************************************************
If these values are correct, enter "config", otherwise change
the values by entering the key followed by the new value, for example:
mode manager
Your command:
```

F. Your command: `mgt_dev lo`

G. Your command: `bind_mgt 1`

H. Your command: `dev_ignore eth0`

I. Your command: `show_all`

J.
```
Key               Acceptable Values          Value
*************************************************
log_level         [0-65535]                  7
log_dir           [directory path]           /home/lanforge
add_resource_addr [host:port]                SEE LIST ABOVE
rem_resource_addr [host:port]                SEE LIST ABOVE
realm             [1-255]                    255
resource          [1-511]                    1
mgt_dev           [ethernet device]          lo
mode              [resource, manager, both]  both
log_file_len      [0-2G]                     0
bind_mgt          [0-1]                      1
shelf             [1-8]                      1
dev_ignore        [eth0 eth1 ... ethN]       eth0
first_cli_port    [1025-4199]                4001
connect_mgr       [host:port]
gps_dev           [device file]              NONE
max_tx            [1-500]                    5
max_send_mmsg_mem [1000-500000]              32000
max_send_mmsg_pkts [1-1000]                  500
keepalive         [1000-500000]              30000
wl_probe_timer    [50-2000]                  50
Other Commands:   help, show_all
*************************************************
```

K. Your command: `config`

L.
```
# ./serverctl.bash restart
```

3. # Other Security Considerations

The fewer services listening on all ports on the LANforge the safer it will be.

> i Check **`netstat -ntulp`** to find services listening on address **0.0.0.0**

You might want to disable or reconfigure services that could reduce your security posture, such as:

A. `nfs-server.service` (only useful for NFS testing)

B. `radiusd.service` (used in 802.1x roaming testing)

C. `rpc-bind.service` (only useful for NFS testing)

D. `rpc-mountd.service` (only useful for NFS testing)

E. `rpc-statd.service` (only useful for NFS testing)

F. `vncserver@:1.service` (if no local GUI needs to run, should only need ssh)

G. `xrdp.service` (because it can be logged in multiple times)

4. ## Connect via SSH

> i SSH not only does port forwarding, but it can compress the data stream between a GUI and a LANforge Server.

A. ### Using PuTTY

B. See other cookbook

C. ### Using OpenSSH

D. OpenSSH is available on Linux, MAC OS X and Windows

A. The SSH **-L** option specifies `[local-port]:[remote-host]:[remote-port]`

```
$ ssh -L 4002:127.0.0.1:4002 -CnNv lanforge@gateway-host
```

B.

C. Leave that connection running.

E. **Using public keys**

You can install a public key to your LANforge and use to avoid typing passwords. Those keys usually reside in your `$HOME/.ssh` directory.

A.
```
$ ssh-keygen -t ed25519
```

B.
```
$ ssh-copy-id lanforge@gateway-host
```

> i It is possible to specify the ssh key to avoid copying the wrong one

D.
```
$ ssh-copy-id -i $HOME/.ssh/id_ed25519 lanforge@gateway-host
```

E.
```
$ ssh -CnNv -i $HOME/.ssh/ed25519 -L 4002:127.0.0.1:4002 gateway-host
```

F. **Using Your `.ssh/config` File**

Edit the hostname and IP configuration for the host:

```
Host lanforge-a1
    Hostname gateway-host
    User lanforge
    IdentityFile ~/.ssh/id_ed25519     # needs to match the ssh key you shared with ssh-copy-id
    IdentitiesOnly yes                 # useful if you have >6 ssh keys
    Compression yes
    LocalForward 8000 127.0.0.1:80     # for browsing reports on LF system
    LocalForward 4001 127.0.0.1:4001   # for CLI telnet scripts
    LocalForward 4002 127.0.0.1:4002   # for binary GUI protocol
```

```
$ ssh -vnN lanforge-a1
```

5. ## Connect the LANforge GUI your Forwarded Connection

6. After starting your SSH connection to **gateway-host**, start your Local GUI and connect to `localhost:4002`

> i If you cannot connect, you might need to edit your **`/etc/hosts`** file.
> It might be listing **`::1 localhost`** or no localhost entry at all.

7.
```
# cat /etc/hosts
```

```
::1 localhost6.localdomain6 localhost6
192.168.1.101 lanforge.localnet lanforge.localdomain
# Loopback entries; do not change.
# For historical reasons, localhost precedes localhost.localdomain:
# See hosts(5) for proper format and other examples:
# 192.168.1.10 foo.mydomain.org foo
# 192.168.1.13 bar.mydomain.org bar
###-LF-HOSTNAME-NEXT-###
127.0.0.1 localhost localhost.localdomain vm-a490 vm-a490-local
```