INTERNAL REPORT

Simulating connection between distributed intranet LAN devices across the WAN

Author: A.Fara

Report N. 68, released: 15/07/2017

Reviewer: A.Orlati

OAC
Osservatorio
Astronomico
di Cagliari

Author Reviewer	**A.Fara** **A.Orlati**	Date	15/07/2017
Title	***Simulating connection between distributed intranet LAN devices across the WAN***	Pag.	1/12

Simulating connection between distributed intranet LAN devices across the WAN

INDEX

1 INTRODUCTION

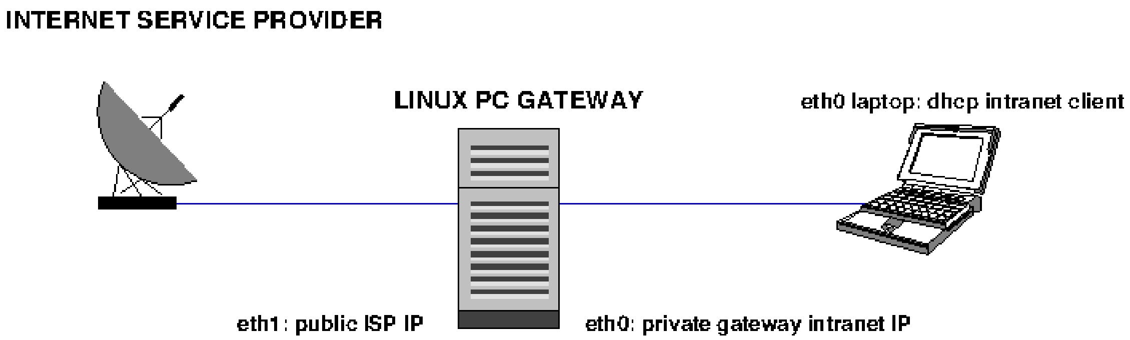
SRT INAF site is going to host "non INAF" devices and instruments. Some of them will be monitored from a remote site, and they will be configured as device of a fixed private intranet. So the local backbone router must redirect the incoming and the outgoing traffic from the local devices to the monitoring stations, into the private intranet, across our public IP provider.

2 THE PROBLEM

The redirection of all services between devices geographycally distributed on a specific intranet requires a complex VPN infrastructure, with a router supporting it and gateway nodes.
None of this elements are available for the first test, which is required only to check the bandwidth and performances of the SRT satellite link. So we simulated a basic equivalent setup connecting:

- the ISP satellite link modem;
- a linux gateway PC;
- a laptop and/or a virtmachine.

We assume that the bottleneck is due to the bandwidth and the latency of the satelite link, not to the internal links between the gateway and the intranet device.


INTERNET SERVICE PROVIDER
LINUX PC GATEWAY
eth0 laptop: dhcp intranet client
eth1 : public ISP IP
eth0: private gateway intranet IP

3 PROJECT TEST SETUP

3.1 Basic informations

We don't have any information about the device behavior under production environment, but only:

- the ip address of the private C class intranet, the default gateway and the fixed address of the device (mandatory)
- the request to make a direct ssh connection from a specific IP public address to the private intranet device address

At the start of the experiment we don't have information about all services listening from the device that need to be monitored, so we check and setup only the ssh forward.

3.2 The satellite connection across a Linux PC

We have to connect a Linux PC el6 family, with two physical NIC eth0 and eth1. The eth1 is configured as dhcp client and connected directly to the ISP satellite modem. A public IP address and all the default provider network parameters are assigned to the eth1 NIC, so that each PC user can reach its account from internet by standard ssh and vnc-ssh tunnel. A specific username=asiesoc account is created.
In this step the PC is connected to internet and isolated from our SRT private network.

3.2.1 Actions: dhcp and user environment

- Configure eth1 as dhcp client [/etc/sysconfig/network-scripts/ifcfg-eth1];
- add the user requiring remote ssh login;
- install and setup vnc server starting at boot;
- configure the vnc environment for the new user [/etc/sysconfig/vncservers].

3.3 The second NIC

The eth0 NIC plays the role of gateway for any kind of internal device. So we need to configure the eth0 with thegateway IP address parameters. The intranet seems to be “closed”, so the connected devices can reach each other member, but not “browse” the Internet wan (?)

3.3.1 Actions: verify intranet parameters and configure the gateway

- Complete and verify the information about private network parametrs (class, broacast, netmask etc) [sipcalc or ipcalc-webtool];
- configure a the eth0 NIC with private intranet gateway IP parameters [/etc/sysconfig/network-scripts/ifcfg-eth0];
- optionally configure name resolving [/etc/hosts].

3.4 Addressing the client device(s)

For the experiment we don't have any physical instrument device to connect, so in the first step we simulate it with a laptop. The operation is transparent to the user due to the dhcp server listening on the eth0 NIC of the gateway PC. The dhcp server gives to the laptop client connected to eth0 the required private network parameters and the IP address of the simulated device.

3.4.1 Actions: dhcp server setup

- Install and configure the dhcp server listening on eth0 [/etc/sysconfig/dhcp] and giving ASI network parametrers [/etc/dhcp/dhcpd.conf]

3.5 Nat filtering

The laptop or any device connected to the eth0 NIC can't reach the internet, so a standard iptables nat filter masquerading the internal IP must be implemented. The nat chain forwards the traffic between the two gateway PC NIC. The classical forward filter chain allows all ougoing connections and only ingoing existing and related ones. This must be modified in the sense of allowing all the connections ingoing.

3.5.1 Actions: natfilter

- Write the iptables natfilter configuration file [/usr/local/bin/natfilter];
- configure it to start it at boot [/etc/rc.local].

4 ADVANCED CONFIGURATION

The described setup can be sufficient to address and reach from any device physically connected to eth0 NIC of PC, by a double ssh connection:

- from the internet to PC gateway;
- from the gateway to the testing laptop.

Another step must be done to reach the device directly from outside, in order:

- to avoid a double ssh-login session (from the external IP to the gateway and from the gateway to the final device);
- to bypass the addition of any user in the gateway PC.

4.1 Port forwarding

Port forwarding and traffic redirection is an usual practice in routers. To reach the same result with a Linux PC some rules must be added to the nat filter, so that each ssh connection from a specific external IP will be redirect to a specific internal subnet IP.

4.1.1 Action: natfilter redirect ssh

- Add nat ipchain rule, to redirect incoming ssh traffic from an IP address to laptop or device IP.

4.2 Non standard ssh-server

If the IP address of the remote PC is also natted by a gateway device, or redirected, is difficult to make the chain working, because the real IP of the incoming ssh traffic can be unknown or variable. If natfilter chain redirects all ssh incoming on the external NIC to the internal destination IP, we lost the remote access to the PC gateway. Otherwise if weredirect and disconnect the test laptop, all the incoming ssh request will stay “pending”. If ssh incoming request is made in “verbose mode” (for debug), the gateway PC log will register a SYN FLOOD message. A good solution is doubling ssh server to linsten to two different ports, so that:

- the standard ssh port listen to all the incoming connections to the PC gateway, without any redirection;
- all the incoming request to the second non-standard ssh port are redirected to the internal IP laptop simulating the intranet device;
- the second ssh server must be started only for the connection experiment and must be shutdown after disconnecting the laptop.This is important to avoid PC DOS attack made by robot portscan requests.

4.2.1 Actions: duplicate ssh-server

- link executable with a “double name” [/usr/sbin/sshd -> /usr/bin/sshd-double];
- duplicate all the configuration files and scripts replacing “sshd” string with the “sshd-double” string in filenames and internal text [/etc/ssh/sshd_config_double, /etc/init.d/sshd-double];

- give to the second server a different from 22 standard port and a different Pid filename identifier in server configuration file [/etc/ssh/sshd_config_double];
- write the option of /usr/sbin/sshd-double executable to point to its specific configuration file sshd_config_double, in a new file /etc/sysconfig/sshd-double;
- setup the sshd-double server runlevel script in init.d services environment, also if the service will not be started at boot [chkconfig service off], using the same standard sshd default.

4.3 Simulation with laptop

The remote connection will fail if the remote user does not have an account to the client laptop. This is the only action required on the client laptop, to check for ssh forward. After that the laptop must be connected to the internal NIC to the PC gateway. The laptop takes its IP and gateway address from the dhcp server, as we see giving the commands about the network connection status:

4.3.1 Actions: verify IP and routing

- /sbin/ifconfig
- /sbin/route

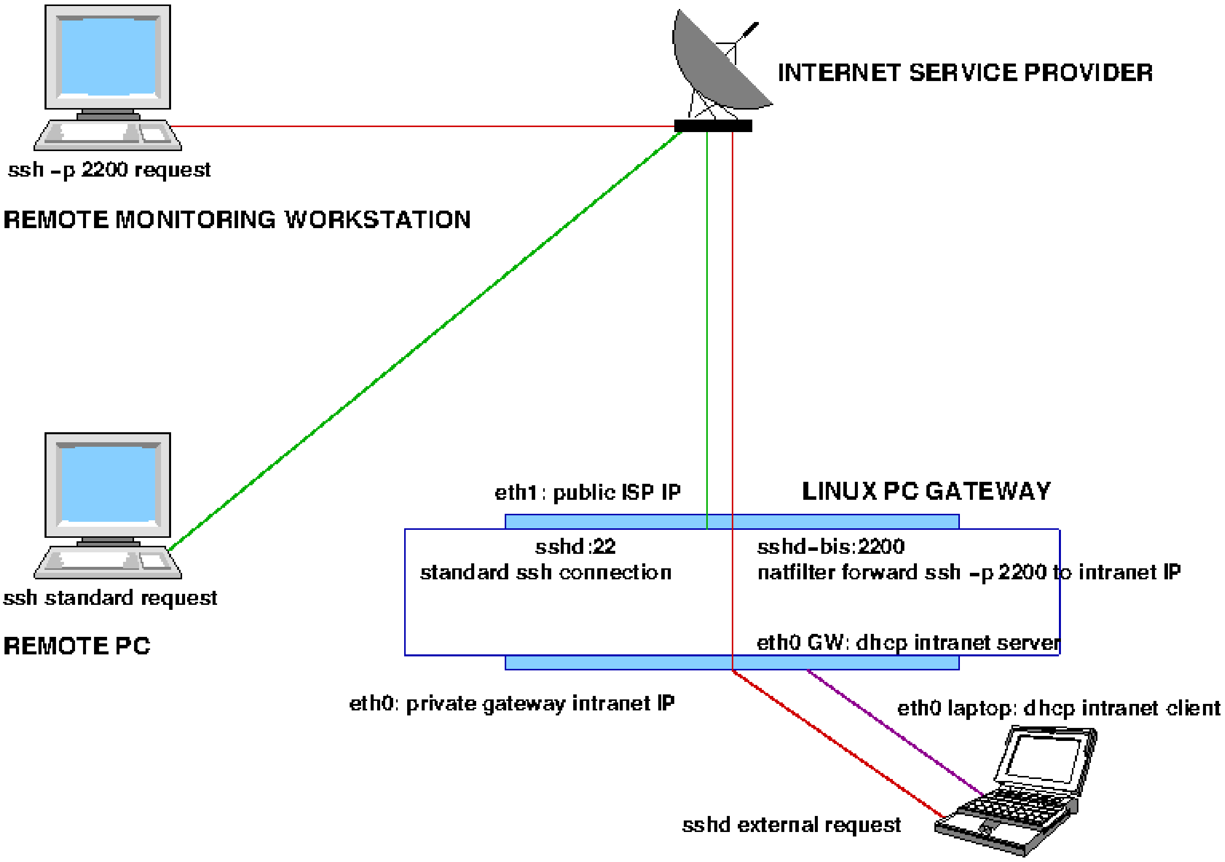
4.4 Checking remote ssh connection

The following commandline from the external IP gives a direct connection tho te testing laptop

```
ssh -XC LINKSAT-IP-ADDRESS -p EXTRA-SSH-PORT -l USERNAME
```

The *LINKSAT-IP-ADDRESS* is the fixed IP given by the Internet Service Provider **to any client device which is directly connected to the satellite modem**. In our simulation is the PC gateway, in a standard setup will be the public address of the backbone router. The *-p* option specifies the extra ssh server port configured to listen and redirect incoming requests by the iptables nat chain. The “USERNAME” is the **username account in the testing laptop** that in the real case will be the default user of the device.

4.5 Basic test setup


INTERNET SERVICE PROVIDER
ssh -p 2200 request
REMOTE MONITORING WORKSTATION
ssh standard request
REMOTE PC
eth1 : public ISP IP
LINUX PC GATEWAY
sshd :22
standard ssh connection
sshd-bis:2200
natfilter forward ssh -p 2200 to intranet IP
eth0 GW: dhcp intranet server
eth0: private gateway intranet IP
eth0 laptop: dhcp intranet client
sshd external request

5 TEST MORE SERVICES

5.1 Simulation of device

Another approach could be to replace the laptop with a VirtualBox machine running the same services of the real device. The dhcp server listening to eth0 NIC of gateway can be stopped, if the NIC of the VirtualBox is configured as bridge option with the static IP address of the real device. The VirtualBox runs a vnc-server, to check all the services from a graphical login session.

5.1.1 Actions: virtualization

- install VirtualBox package on PC gateway;
- build a virtmachine with a bridge network configuration;
- boot the virtmachine and configure the eth0 with static IP or as as dhcp client;
- add a local-user to the virtual machine;
- install vnc-server on the virtmachine;
- configure the vnc user environment on the running virtmachine;
- fix a display number in vnc-server configuration file for the user.

5.1.2 Actions: clean the gateway PC

- Remove the user account allowing remote ssh connection from the external IP to the PC gateway;
- if the virtmachine is configured with static intranet IP address stop the dhcp server in the PC gateway.

5.2 Connect to the virtualmachine (or to the real device) via vnc

The commandline to login from the external IP to the virtmachine in the graphical session will be:

```
vncviewer -via “USERNAME@LINKSAT-IP-ADDRESS -p EXTRA-SSH-PORT” localhost:DISPLAY
```

Remark:

- quotation marks are mandatory to define the extra ssh port number;
- USERNAME is the account login to the final device, not to the gateway.

6 CONCLUSIONS

The basic setup is good for testing ssh connection, not for more complex activities.

After the first basic ssh-test more checks has been requested, to verify the bandwidth and the impact of network latency:

- on passive monitoring response;
- on interactive terminal or gui operations.

The request to open and forward also the service/port RDP(3389), VNC(5900), WEB(8080), ICMP-ECHO (ping service), in addition to SSH (22 + extra-port) across the gateway has been rejected, because they make the gateway "unsafe". The port forwarding + redirect + duplicate ports of many specific services, add computational load to the gateway, and increase the complexity of natfilter rules.

A good testing solution can be reached by:

- tunnel all the services over ssh, which does not modifies the working natfilter;
- installing a tight-vncserver on the virtmachine simulating the real device;
- running vncviewer from client, under ssh tunnel;

The performance depends on the computational capability in crypting and compress data and the graphical session. Some improvement can be done, by checking different vnc servers and configuration options.

A better solution is to build Intranet with VPN technologies but we don't have informations about the possibility to implement this approach on the existing non INAF Intranet infrastructure.