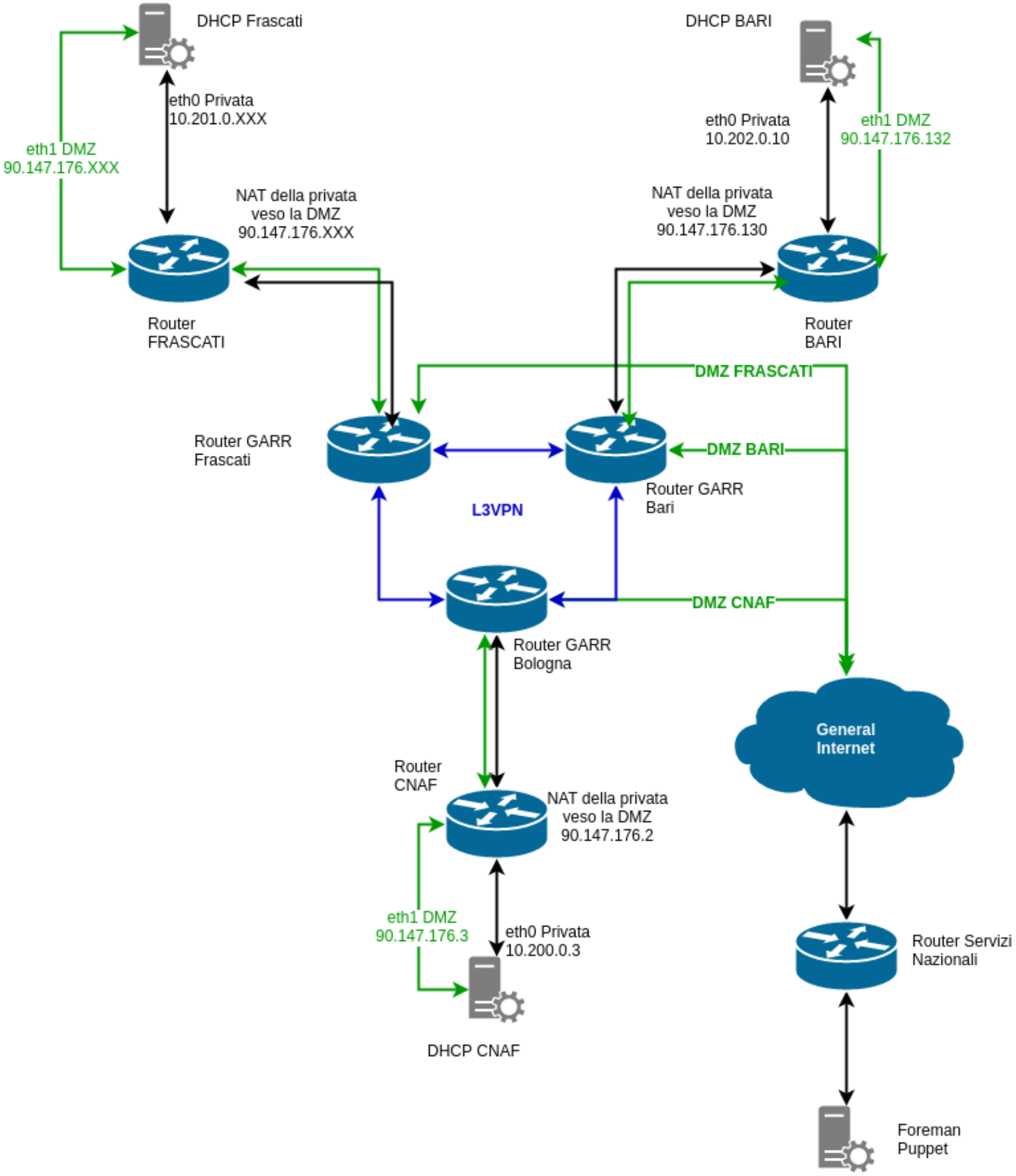
Instradamenti



Instradamento puppet agent, puppet server

Le comunicazione di tutte le macchine configurate via puppet verranno instradate sulla rete privata, quindi attraverseranno il NAT della rete privata di riferimento uscendo con un IP della rete DMZ, da qui la comunicazione passa attraverso General Internet e arriva sul router dei Servizi Nazionali attraverso la DMZ dei servizi Nazionali si raggiunge la macchine con il server puppet.
Con questa tipologia di comunicazione, il puppet server è raggiunto sfruttando il default gateway della macchina che sta sulla rete privata, permettendo di avere anche tutte le comunicazioni tra le macchine (es DHCP) e tra servizi (es. Cluster Percona, Ceph, RabbitMQ) sulla rete privata sfruttando i link a 10Gb/s dedicati alla L3VPN.

Instradamento Foreman, Foreman-proxy DHCP

Al momento della creazione di un'associazione MAC - IP sul servizio Foreman quest'ultimo interroga il Foreman-Proxy di riferimento per la rete dell'IP selezionato attraversando general internet e arrivando ad interrogare il servizio foreman-proxy sulla porta 8443 dell'IP del servizio DHCP attestato sulla DMZ.
Per permettere alla macchina di rispondere correttamente alle richieste foreman è necessario abilitare il policy based routing sull'interfaccia pubblica dela macchina creando un'apposita routing table per la rete DMZ.
Questo tipo di configurazione è necessaria non solo per il servizio DHCP ma anche per tutte quelle macchine che hanno servizi OpenStack pubblici. Per esempio il controller node che controlla l'infrastruttura OpenStack comunicando con i cluster RabbitMQ e Percona sulla l'interfaccia e allo stesso tempo esponendo la dashboard sull'interfaccia DMZ.

NB. Sulla DMZ dei servizi nazionali sono presenti ACL che permettono tutto il traffico verso il server puppet solo dagli IP dei NAT delle 3 sedi, e dal foreman server verso i foreman-proxy.

Esempio per dhcp-cnaf:

eth0: IP Privato 10.200.0.3 → il default gateway di questa rete è il 10.200.0.2 ed è settato nel file ifcfg-eth0 come si vede di seguito
eth1: IP DMZ 90.147.176.3 → il default gateway di questa rete è il 90.147.176.1 ed è stato settato nella rotta nel file **route-eth1**, inoltre per questa rete è stata creata una apposita routing table in **rt_tables** associata tramite una regola specifica per l'interfaccia eth1 in **role-eth1**

```
# cat /etc/sysconfig/network-scripts/ifcfg-eth0
TYPE="Ethernet"
BOOTPROTO="none"
DEFROUTE="yes"
IPV4_FAILURE_FATAL="no"
```

IPV6INIT="yes"
NAME="eth0"
UUID="1a9623b4-b445-4a82-b08d-e93bfc67e53c"
DEVICE="eth0"
ONBOOT="yes"
IPADDR="10.200.0.3"
PREFIX="24"
GATEWAY="10.200.0.2"
DNS1="8.8.8.8"
DNS2="8.8.4.4"
NM_CONTROLLED="no"

# cat /etc/sysconfig/network-scripts/ifcfg-eth1
TYPE=Ethernet
BOOTPROTO=static
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=no
IPADDR=90.147.176.3
PREFIX=26
NAME=eth1
UUID=a73e2800-d381-4ec9-9509-9b56b87d34ff
DEVICE=eth1
ONBOOT=yes

vim /etc/iproute2/rt_tables
#
reserved values
#
255 local
254 main
253 default
0 unspec
#
local
#
#1 inr.ruhep
200 DMZ ← AGGIUNGERE QUESTA RIGA

 # vim /etc/sysconfig/network-scripts/rule-eth1
from 90.147.176.3 table DM

 # vim /etc/sysconfig/network-scripts/route-eth1

default table DMZ via 90.147.176.1

 # systemctl restart network