Network automation:

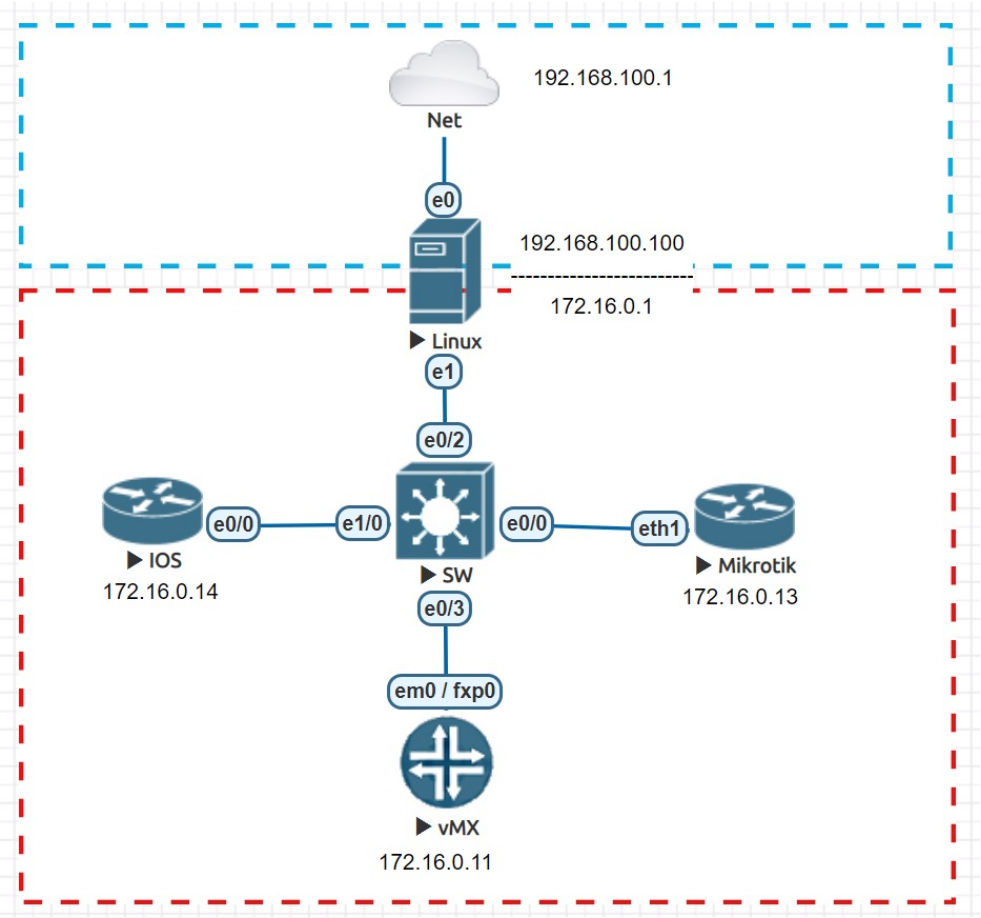
Idempotency in the configuration of an AS

Motivation

- Provide autonomy for network operator who don´t have experience with automation tools.
- Provide a playbook in Ansible with simple implementation in order to provide the automation of antispoofing configurations according to the good practices proposed by MANRS.

- Cisco: BOGON, block port 25, RA IPv6, CDP and enable RP Filter
- Juniper: BOGON, block port 25 and enable RP Filter
- Mikrotik: BOGON, block port 25, MNDP and enable RP Filter

Laboratory



- Ubuntu: Ansible 2.9 + python 2.7 (ncclient)

- Installation:

apt install software-properties-common

apt-add-repository ppa:ansible/ansible

apt update

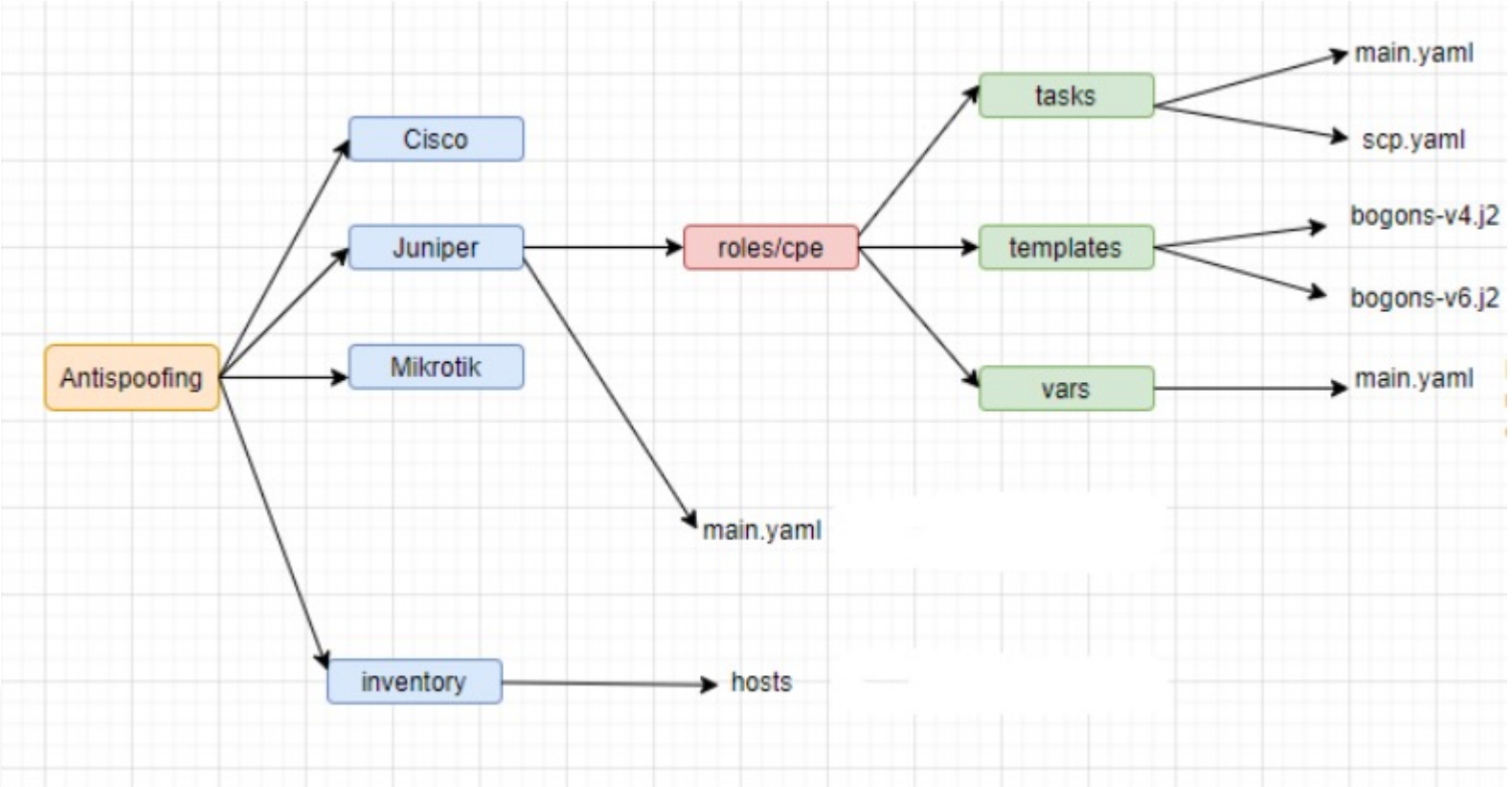
apt install ansible

Linux virtual - Ubuntu 18.04 - Ansible

- Generate SSH key:

```
cd ~ / .ssh
ssh-keygen -t rsa -b 2048 -f Ansible_SSH_key
chmod 400 Ansible_SSH_key.pub # 640
```

Structure of roles and playbooks



Idempotency

- Idempotency was addressed in the code. A register was created for each status check task. For each execution task, the previous return is compared:

main.yaml

```yaml
- name: Check if the prefix-list v4 already exists
  junos_command:
    commands: show configuration policy-options
    wait_for: result[0] contains FILTRO-BOGONS-v4
    retries: 2
  ignore_errors: yes
  register: checkFiltroBogonsv4
```

```yaml
- name: Include task scp
  include_tasks: scp.yaml
```

scp.yaml

```yaml
- name: Send template v4
  junos_scp:
    provider: "{{ connection_info }}"
    src: roles/cpe/templates/bogons-v4.j2
    dest: /tmp/
  connection: local
  when: checkFiltroBogonsv4 is failed
  register: uploadBogonv4
```

main.yaml

```yaml
- name: Create prefix-list BOGONS v4
  junos_config:
    src: bogons-v4.j2
    src_format: set
  when: uploadBogonv4.changed
  register: setBogonV4
```

Use case: Juniper

ansible-galaxy install Juniper.junos

pip install junos-eznc

pip install ncclient

pip install jxmlease

```
vanessa@gatewaydefault:~/testes-ansible$ ansible-galaxy install Juniper.junos
- downloading role 'junos', owned by Juniper
- downloading role from https://github.com/Juniper/ansible-junos-stdlib/archive/2.4.3.tar.gz
- extracting Juniper.junos to /home/vanessa/.ansible/roles/Juniper.junos
- Juniper.junos (2.4.3) was installed successfully
```

- Configure SSH-key

Use case: Juniper

- Enable netconf e ssh.

```
root> configure
Entering configuration mode
[edit]
root# set system services netconf ssh
```

- Configure interfaces, default route, user and hostname

Use case: Juniper

- Juniper operates with exclusive mode in the Juniper module and already commits:

```
root@vmx1> configure
Entering configuration mode
Users currently editing the configuration:
  ansible (pid 14271) on since 2020-12-30 18:41:47 UTC, idle 00:01:53
      exclusive
```

- If an error occurs in the playbook and needs to be interrupted, the editing mode may become stuck, requiring manual intervention:

```
[edit]
root@vmx1# exit
Exiting configuration mode

root@vmx1> request system logout pid 14271
```

Use case: Juniper

- Ansible connection:

Value of ansible_connection	Protocol	Requires
network_cli	CLI over SSH	network_os setting
netconf	XML over SSH	network_os setting
local	depends on provider	provider setting

- netconf: better interaction with modules (except junos_scp):

```
TASK [cpe : Enviar template v4] ************************************************************************************
[WARNING]: provider is unnecessary when using ansible.netcommon.netconf and will be ignored
fatal: [vmx1]: FAILED! => {"changed": false, "msg": "You must provide either 'host' or 'sock_fd' value"}

PLAY RECAP *********************************************************************************************************
vmx1                       : ok=3    changed=0    unreachable=0    failed=1    skipped=0    rescued=0    ignored=3
```

Use case: Juniper

- Junos_scp issue:

provider dictionary		**Deprecated** Starting with Ansible 2.5 we recommend using `connection: network_cli` or `connection: netconf`. For more information please see the Junos OS Platform Options guide. A dict object containing connection details.
host string / required		Specifies the DNS host name or address for connecting to the remote device over the specified transport. The value of host is used as the destination address for the transport.

Use case: Juniper

- Task tests with net_put and connection network_cli were discarded as it was not possible to use arguments like wait_for.

```
TASK [cpe : Enviar template v4] ****************************************************************************************
fatal: [vmx1]: FAILED! => {"changed": false, "msg": "connection type ansible.netcommon.netconf is not valid for net_put module, please use fully qualifie
d name of network_cli connection type"}
```

```
TASK [cpe : Checa se a prefix-list v4 já existe] ******************************************
[WARNING]: arguments wait_for, match, rpcs are not supported when using transport=cli
ok: [vmx1]

TASK [cpe : Checa se a prefix-list v6 accept já existe] ***********************************
ok: [vmx1]
```

```yaml
- name: Enviar template v4
  ansible.netcommon.net_put:
    src: roles/cpe/templates/bogons-v4.j2
    dest: /tmp/
  connection: network_cli
  when: checkFiltroBogonsv4 is failed
  register: uploadBogonv4
```

Use case: Juniper

- Resolution: Separate into two playbooks.
- tasks/scp.yaml:

```yaml
---
- name: Send template v4
  junos_scp:
    provider: "{{ connection_info }}"
    src: roles/cpe/templates/bogons-v4.j2
    dest: /tmp/
  connection: local
  when: checkFiltroBogonsv4 is failed
  register: uploadBogonv4

- name: Send template v6
  junos_scp:
    provider: "{{ connection_info }}"
    src: roles/cpe/templates/bogons-v6.j2
    dest: /tmp/
  connection: local
  when: checkFiltroBogonsv6Accept and checkFiltroBogonsv6Deny is failed
  register: uploadBogonv6
```

Use case: Juniper

- Resolution: Separate into two playbooks.
- tasks/main.yaml:

```yaml
- name: Check if prefix-list v6 deny already exists
  junos_command:
    commands: show configuration policy-options
    wait_for: result[0] contains FILTRO-BOGONS-v6-DENY
    retries: 2
  ignore_errors: yes
  register: checkFiltroBogonsv6Deny

- name: Include task scp
  include_tasks: scp.yaml

- name: Create prefix-list BOGONS v4
  junos_config:
    src: bogons-v4.j2
    src_format: set
  when: uploadBogonv4.changed
  register: setBogonV4
```

Juniper

root@eve-ng: ~

```
vanessa@gatewaydefault:~/lacnic/Antispoofing$ ansible-playbook -i inventory/hosts Juniper/main.yaml
```

root@eve-ng: ~

```
## Last commit: 2021-03-02 23:21:48 UTC by ansible
version 14.1R4.8;
system {
    host-name vmx1;
    root-authentication {
        encrypted-password "$1$W8Sljndq$vg5yfS4kq1JDWEfGnIaGL."; ## SECRET-DATA
    }
    login {
        user ansible {
            uid 2001;
            class super-user;
            authentication {
                ssh-rsa "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCq/nENkunfIiYAGWmsD8kYK2u80nRJxuLA0CR9ma3igUYEdm+
jVJcfj462xLOjrVPGCnL0f3MtYoaovveMQVTLsmtBVCn30ychC2TpQPoPO+x7tLYhTuItTFGa5HWURyMfII2TIPeSydKa1tXCLv85LB8ly/CA/BH
1grpoPpDJKwMP6OD5oHxKnL+A01tN/hgMrL2QbZjq4rW3iIlAknQmsvRdhgWymMvCphnuqnUs4uXU8KdwwGNOBEH0UPa1oDLS51ODaVpBA36UAmC
oZOUgH2wuwMXo+1f2fMGyo8KRct8finQwA6NuyEX7dWGdgQCQNP3KWL5xujHZs6lxNNPF vanessa@gatewaydefault"; ## SECRET-DATA
                }
            }
            user teste {
                uid 2002;
                class super-user;
                authentication {
                    encrypted-password "$1$LvPzYp.v$rpLGL8rFWKv2xa/1mVaMY/"; ## SECRET-DATA
                }
            }
        }
        services {
            ssh;
            netconf {
                ssh;
            }
        }
        syslog {
            user * {
                any emergency;
            }
            file messages {
                any notice;
                authorization info;
            }
            file interactive-commands {
                interactive-commands any;
            }
        }
}
interfaces {
    ge-0/0/0 {
        unit 0;
    }
    em0 {
        unit 0 {
            description mgmt;
            family inet {
                address 172.16.0.11/24;
            }
        }
    }
}
---(more)---
```

Questions?

- GIT: https://github.com/mello-vanessa/lacnic

- Social network:

https://www.linkedin.com/in/vanessa-de-oliveira-mello/

https://medium.com/vanessamelloit

https://twitter.com/vanessamelloIT