Vyatta

2019-12-05

```
show interfaces

configure

# Enable SSH for remote management:
set service ssh port 22


# Configure network interfaces IPv4
set interfaces ethernet eth0 address dhcp
set interfaces ethernet eth0 description 'WAN'
set interfaces ethernet eth0 duplex full
set interfaces ethernet eth0 speed 100

set interfaces ethernet eth1 address 10.1.1.1/24
set interfaces ethernet eth1 description 'LAN'
set interfaces ethernet eth1 duplex full
set interfaces ethernet eth1 speed 100

set interfaces ethernet eth2 address 10.1.2.1/24
set interfaces ethernet eth2 description 'DMZ'
set interfaces ethernet eth2 duplex full
set interfaces ethernet eth2 speed 100

# Configure network interfaces IPv4
#set interfaces ethernet eth3 address address 10.1.3.1/30
set interfaces ethernet eth3 description 'IPS Port Mirroning'
set interfaces ethernet eth3 duplex full
set interfaces ethernet eth3 speed 100
set interfaces ethernet eth3 vif 5 description 'VLAN 5 IPS Port Mirroning'
set interfaces ethernet eth3 vif 5 address 10.1.3.1/30
set interfaces ethernet eth1 mirror eth3  # Mirror de eth1 a eth3 (IPS)
set interfaces ethernet eth2 mirror eth3  # Mirror de eth2 a eth3 (IPS)
commit

# Configure network interfaces IPv6
set interfaces ethernet eth1 address 3fb7::1/64
set interfaces ethernet eth1 ipv6 router-advert send-advert true
set interfaces ethernet eth1 ipv6 router-advert max-interval 10
set interfaces ethernet eth1 ipv6 router-advert prefix 3fb7::/64
set interfaces ethernet eth1 ipv6 router-advert other-config-flag true
set interfaces ethernet eth1 ipv6 router-advert default-preference medium
set interfaces ethernet eth1 ipv6 router-advert managed-flag true
commit

# Configure Source NAT for our "Inside" network. Ponwe un /16 no funciona
set nat source rule 100 outbound-interface eth0
set nat source rule 100 source address 10.1.1.0/24
```

```
set nat source rule 100 translation address masquerade

set nat source rule 101 outbound-interface eth0
set nat source rule 101 source address 10.1.2.0/24
set nat source rule 101 translation address masquerade

set nat source rule 102 outbound-interface eth0
set nat source rule 102 source address 10.1.3.0/30
set nat source rule 102 translation address masquerade
commit

# Configure a DHCP Server IPv4:
set service dhcp-server shared-network-name LAN authoritative
set service dhcp-server shared-network-name LAN subnet 10.1.1.0/24 default-router 10.1.1.1
set service dhcp-server shared-network-name LAN subnet 10.1.1.0/24 dns-server 1.1.1.1
set service dhcp-server shared-network-name LAN subnet 10.1.1.0/24 dns-server 9.9.9.9
set service dhcp-server shared-network-name LAN subnet 10.1.1.0/24 lease 86400
set service dhcp-server shared-network-name LAN subnet 10.1.1.0/24 range 0 start 10.1.1.100
set service dhcp-server shared-network-name LAN subnet 10.1.1.0/24 range 0 stop 10.1.1.200
set service dhcp-server shared-network-name LAN description 'DHCP LAN IPv4'
commit

# Configure a DHCP Server IPv6:
set service dhcpv6-server shared-network-name LAN subnet 3fb7::/64 address-range start 3fb7::10 stop 3fb7::10
set service dhcpv6-server shared-network-name LAN subnet 3fb7::/64 name-server 3fb7::1
commit

# And a DNS forwarder:
set service dns forwarding cache-size 0
set service dns forwarding allow-from 10.1.1.0/24
set service dns forwarding listen-address 10.1.1.1
set service dns forwarding name-server 1.1.1.1
set service dns forwarding name-server 9.9.9.9

# Apply and save
commit
save
```

Add a set of firewall policies for our “Outside” interface:

set firewall name OUTSIDE-IN default-action ‘drop’ set firewall name OUTSIDE-IN rule 10 action ‘accept’ set firewall name OUTSIDE-IN rule 10 state established ‘enable’ set firewall name OUTSIDE-IN rule 10 state related ‘enable’

set firewall name OUTSIDE-LOCAL default-action ‘drop’ set firewall name OUTSIDE-LOCAL rule 10 action ‘accept’ set firewall name OUTSIDE-LOCAL rule 10 state established ‘enable’ set firewall name OUTSIDE-LOCAL rule 10 state related ‘enable’ set firewall name OUTSIDE-LOCAL rule 20 action ‘accept’ set firewall name OUTSIDE-LOCAL rule 20 icmp type-name ‘echo-request’ set firewall name OUTSIDE-LOCAL rule 20 protocol ‘icmp’ set firewall name OUTSIDE-LOCAL rule 20 state new ‘enable’ set firewall name OUTSIDE-LOCAL rule 30 action ‘drop’ set firewall name OUTSIDE-LOCAL rule 30 destination port ‘22’ set firewall name OUTSIDE-LOCAL rule 30 protocol ‘tcp’ set firewall name OUTSIDE-LOCAL rule 30 recent count ‘4’ set firewall name OUTSIDE-LOCAL rule 30 recent time ‘60’ set firewall name OUTSIDE-LOCAL rule 30 state new ‘enable’ set firewall name OUTSIDE-LOCAL rule 31 action ‘accept’ set firewall name OUTSIDE-LOCAL rule 31 destination port ‘22’ set firewall name OUTSIDE-LOCAL rule 31 protocol ‘tcp’ set firewall name OUTSIDE-LOCAL rule 31 state new ‘enable’

Apply the firewall policies:

set interfaces ethernet eth0 firewall in name ‘OUTSIDE-IN’ set interfaces ethernet eth0 firewall local name ‘OUTSIDE-LOCAL’

Once suricata is installed and inspecting nfqueue 0 (-q 0), you can send packet to it by passing the action “inspect” to a firewall rule:

set firewall name FROM-INTERNET default-action drop set firewall name FROM-INTERNET description “From Internet” set firewall name FROM-INTERNET rule 10 description “Pass port 22 traffic to Suricata” set firewall name FROM-INTERNET rule 10 action inspect set firewall name FROM-INTERNET rule 10 protocol tcp set firewall name FROM-INTERNET rule 10 destination port ssh

and this will send packets to nfqueue 0