FW CNaaS and SUNET-MGMT-VRF

IP VPN is used to establish connectivity to the CNAAS Firewall from SUNET management servers. For information about SUNET management VPN's see Management VPN

On-net FW installations

CNAAS on-net firewalls are managed outbound (a dedicated connection). A hub-spoke IP-VPN VRF (infra-cpe-mgmt) is used for this purpose on the SUNET PE router. The same VPN/ VRF is used for different customer FW / CPE attachments to the same PE. On the CNAAS firewall the interface connected to the SUNET PE is separated from other interfaces using a local VRF "SUNET-infra-cpe-mgmt". The CNAAS firewall should use security policys allowing traffic **only** for the required announce(from PE) SUNET management servers. See Management VPN section "VRF Infra-cpe-mgmt (SPOKE)".

The IP VPN connection to the PE is established using VLAN-ID 9 and eBGP is used between the PE and the CNAAS distribution switch. A policy is used on the CNAAS Firewall to restrict BGP announcements to only include the loopback attached to the "SUNET-infra-cpe-mgmt" VRF.

The loopback address for the Link and loopback addresses are assigned from the following ranges:

links PE - CNAAS / CNAAS FW)
86.105.113.128/26 (https://ipam.sunet.se/prefix/list#/query_string=86.105.113.128/26&search_opt_parent=undefined&search_opt_child=undefined&explicit=true)

loopbacks (CNAAS FW)
86.105.113.192/26 (https://ipam.sunet.se/prefix/list#/query_string=86.105.113.192/26&search_opt_parent=undefined&search_opt_child=undefined&explicit=true)

Example configuration SUNET PE:

```
Example configuration SUNET PE. In case the VRF is present new connections are added to the same VRF.

routing-instances {
    infra-cpe-mgmt {
        routing-options {
            auto-export;
        }
        protocols {
            bgp {
                group <cnaas_fw_node_name> {
                    import primary-in;
                    peer-as <cnaas_switch_peer_asn>;
                    as-override;
                    neighbor <cnaas_switch_peer_ip> {
                        family inet {
                            unicast {
                                prefix-limit {
                                    maximum 10;
                                    teardown {
                                        80;
                                        idle-timeout 5;
                                    }
                                }
                            }
                        }
                    }
                }
            }
        }
        instance-type vrf;
        interface <name>.9;
        route-distinguisher 1653:883;
        vrf-target {
            import target:1653:898;
            export target:1653:899;
        }
    }
}

interfaces {
    <name> {
        description "<description>";
        flexible-vlan-tagging;
        mtu 9192;
        encapsulation flexible-ethernet-services;
        unit 9 {
            description "infra-cpe-mgmt for <fw-node-name>";
            vlan-id 9;
            family inet {
                mtu 1500;
                address <link_address>;
            }
        }
    }
}
```

Example configuration CNAAS FW routing-instance "SUNET-infra-cpe-mgmt"

```
CNAAS FW:
routing-instances {
    SUNET-infra-cpe-mgmt {
        protocols {
            bgp {
                group sunet-mgmt {
                    type external;
                    export SUNET-infra-cpe-mgmt;
                    peer-as <cnaas_switch_peer_asn>;
                    local-as <SUNET-infra-cpe-mgmt_local_asn>;
                    multipath;
                    bfd-liveness-detection {
                        minimum-interval 1000;
                    }
                    neighbor <cnaas_switch_peer_ip> {
                        description <cnaas_switch_name>;
                    }
                    neighbor <cnaas_switch_peer_ip> {
                        description <cnaas_switch_name>;
                    }
                }
                log-updown;
            }
        }
        interface lo0.9;
        interface reth0.251;
        description SUNET-infra-cpe-mgmt;
        instance-type virtual-router;
    }
}

policy-statement SUNET-infra-cpe-mgmt {
    term 1 {
        from {
            protocol direct;
            route-filter <lo0.9_address>/32 exact;
        }
        then accept;
    }
    term default {
        then reject;
    }
}
```

Off-net FW installations (e.g. using Tele2 Network)

Off-net CNAAS FW is managed inbound in the customer IP-VPN (in the same way an off-net CPE's are managed). On the SUNET IP-VPN NNI connection (NNI to the off-net network) connection routes used for management of the CNAAS Firewall (the link address to the CNAAS Firewall) is exported to the SUNET-MGMT-VRF. The customer VRF on the NNI imports routes used by SUNET management servers. The link address between the off-net CPE and the CNAAS Firewall is used for management connectivity (hostname of the CNAAS Firewall is set to the link address).

The address range 86.105.113.64/26 is used to assign /30 link networks for the off-net Firewall.

https://ipam.sunet.se/prefix/list#/query_string=86.105.113.64/26&search_opt_parent=undefined&search_opt_child=undefined&explicit=true

For information how to configure IP-VPN and IP-VPN inbound management see; Juniper PE kund IP-VPN and Juniper PE - Tele2 VPN-NNI IP-VPN

For general information about off-net IP-VPN see Tele2 VPN-NNI & off-net provided IP-VPN