Onboarding and Firewall Enablement

This chapter describes how to setup Layer 4-Layer 7 service accceleration on the Cisco N9300 Series Smart switch.

For troubleshooting infromation, see Cisco N9300 Series Smart Switches Troubleshooting.

Setup Layer 4-Layer 7 service accceleration

Licensing requirements

The service acceleration feature requires you to be on the Premier licensing tier. You require a separate Cisco Hypershield license for Layer-4 stateful segmentation capabilities and security use cases.

Workflow for Layer 4 - Layer 7 service acceleration

Perform these steps to enable the Layer 4 - Layer 7 service acceleration features provided by the DPU.

1. Bring up the switch by installing the software on the switch.
2. Configure VRF contexts and Layer 3 interfaces with VRF members.
3. Configure loopback interface for Hypershield source-interface.
4. Enable service acceleration feature
5. Request the token from Hypershield Security Cloud Control.
6. Add the configuration to connect to the Hypershield.
7. Configure traffic inspection for traffic in required VRFs.
8. Enable the firewall service functionality.

Guidelines and limitations

Recommendation on VRF usage and IP address configuration

The recommendations provide guidance on VRF usage and reserved IP-address ranges.

- Use VRF-lite to keep traffic separate and for redirection to assign the traffic of each VRF to a specific DPU.

  Allocate one or more VRFs (in addition to the default VRF) for traffic that requires filtering with the DPU.

- The IP-address range 169.254.x.x should *not* be used. It is used for communications to the DPU within the switch.

- In addition to the normal IP addresses requirements (like the mgmt0 IP), you need assign a loopback IP address for the Hypershield Agent running on the Cisco N9300 Series Smart switch.

Restrictions and considerations for firewall service configuration

These restrictions and considerations address limitations and best practices for operating the firewall service, covering traffic inspection behavior, protocol interactions, and service acceleration VRF functionality.

- The Hypershield management traffic uses the default VRF. You *cannot* configure default VRF and management VRF for traffic inspection under service firewall.

- The connectivity to the Hypershield requires the use of a front panel interface, and it cannot use the mgmt0 interface.

- Once a loopback interface is used as the source interface for the service instance, the loopback IP address *cannot* be used for any other purpose other than communication between the agent and the Hypershield.

  This loopback IP address *cannot* be reused for any control protocols running on the switch. Any attempt to test reachability to other destinations using ICMP echo from the NXOS CLI fails, when the loopback IP address is specified as the source.

  Use the troubleshooting commands instead to verify the connectivity between the Hypershield Agent and the Hypershield Controller. For more information, see Cisco N9300 Series Smart Switches Troubleshooting.

- If a VRF is configured under the service firewall configuration (that means the VRF is subject to traffic filtering), and if the service firewall is *not* “in-service”, the IPv4 and IPv6 traffic routed by this VRF is dropped until the service firewall is “in-service” (and until a security rule to allow that traffic is in place).

Note The control protocol traffic in the VRFs configured for service-acceleration, that is destined to the supervisor of the Cisco N9300 Smart switch is *not* inspected. Hence it is *not* dropped regardless of whether service firewall is “in-service” or not, and regardless of security rules are configured.

- The firewall service *does not* inspect multicast traffic, traffic destined for the local switch, traffic originating from the supervisor, BFD echo packets, the default and management VRFs, and any VRFs that *are not* added under service firewall.

- When the service firewall is *not* in "in-service" state, and the DPU is *not* ready to inspect traffic, the Layer 3 routing protocols ensure graceful insertion and removal (GIR) behavior.

  To achieve this, the service-acceleration VRFs isolate the switch from the network by altering the route advertisement behavior. Protocols supporting this functionality include Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF).

  The protocols resume regular route advertisement behavior once the service firewall is ready for use and is in "in-service" state.

These features are *not* available in Cisco Nexus NX-OS Release 10.5(3s)F.

- Inter-VRF flows are *not* supported: the traffic being filtered must be entering and existing the smart switch from the same VRF.
- Cisco Nexus NX-OS Release 10.5(3s)F only supports Layer 3 physical interfaces and port-channels, as well as physical and port-channel subinterfaces. Only incoming traffic is supported on the Layer 3 physical interfaces.
- High availability features such as redundancy, stateful failover is *not* supported. If you use ECMP for traffic distribution, you need to make sure that traffic is sent symmetrically to the switch.
- Layer 2 features such as access or trunk ports, VLAN extension across networks, and MAC address table management are *not* supported.
- VRF sharing feature that enables route exchange between different VRFs using import or export policies configured with route maps is *not* supported.
- Virtual Port Channels (vPCs) that allow links across two devices to appear as a single port channel, are *not* supported.
- Switch virtual interfaces (SVI) are *not* supported; You can use Layer 3 interfaces for routing traffic.
- Hot Standby Router Protocol (HSRP) and Virtual Router Redundancy Protocol (VRRP) protocols that provide seamless failover are *not* supported.
- VXLAN and EVPN features are *not* supported.
- The **feature service-acceleration** command is a hardware-intensive feature. When enabled, NXOS powers up the DPUs, which takes some time. As a result, NXOS prevents the execution of **no feature service-acceleration** command until the DPUs are fully powered up and reach a terminal state. These statements hold true:
  - The **feature service-acceleration** command *cannot* be disabled until all DPUs in the system have been powered on.
  - The **feature service-acceleration** command can only be re-enabled, once it has been disabled, after a switch reboot.

  If you use the **configure replace** feature (see Performing Configuration Replace), the success of **configure replace** may depend on the timing of the configuration relative to when service-acceleration was enabled or disabled.
- Management traffic from Hypershield Agent to Hypershield system is *not* supported over IPv6.

Configure and assign the VRF to an interface

Perform this task to configure a VRF on an interface.

Procedure

Step 1 Create a new VRF using the **vrf context** *vrf-name* command.

Example:

```
switch# configure terminal
switch(config)#vrf context red
switch(config)#vrf context blue
switch(config)#vrf context green
switch(config-vrf)# exit
```

Step 2 Configure a Layer 3 interface using the **interface** *interface-typeslot/port* command

Example:

```
switch# configure terminal
switch(config)# interface ethernet 1/1
```

Step 3 Assign the VRF to the interface using the **vrf member** *vrf-name* command.

Example:

```
switch(config-if)# vrf member red
```

This removes any existing IPv4/IPv6 address already configured on the interface.

Step 4 Configure an IP address for the interface using the **ip address** *ip-address/length* command. You must do this step after you assign this interface to a VRF.

Example:

```
switch(config-if)# ip address 192.0.2.1/16
```

Example

Verify the VRF contexts and Layer 3 interface configuration.

```
switch# show run
..
vrf context red
vrf context green
vrf context blue
!
!
switch# show run interface 1/1
interface Ethernet1/1
  vrf member red
  ip address 192.0.2.1/16
  no shutdown
<…etc…>
...!
```

Create a loopback interface

Perform this task to create a loopback interface, and associate this loopback interface with the Hypershield agent in the service system Hypershield configuration.

Procedure

Step 1 Create a loopback interface for the Hypershield source-interface using the **interface loopback** *instance* command.

Example:

```
switch(config)# interface loopback 100
switch(config-if)#
```

Step 2 Configure an IP address for the interface using the **ip address** *ip-address/length* command.

Example:

```
switch(config-if)# ip address 192.0.2.1/32
```

For more information about IP addresses, see the Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide.

ip-address/length: Sets a IP address for the loopback

Note
You have to configure /32 as length of the IP address for Hypershield Agent.

Note
Management traffic from Hypershield Agent to Hypershield system is *not* supported over IPv6.

Example

Verify the loopback interface configuration.

```
switch# show run
!
interface loopback100
  ip address 192.0.2.1/32
```

Enable service acceleration

Perform this task to enable power up the DPU in the switch.

Procedure

Enable the **feature service-acceleration** command to power up the DPUs.

Example:

```
Switch(config)# feature service-acceleration
```

If the **feature service-acceleration** command is *not* configured, the DPUs are powered off. The switch functions as a NXOS switch.

Note
Enabling feature service-acceleration powers up the DPUs; however, to finalize the configuration, you must define which VRFs traffic should be redirected to the DPU. See Configure VRFs for traffic redirection to the firewall service, on page 9.

Verify service acceleration

Perfrom this task to verify service acceleration enablement.

Procedure

Step 1 Verify the service acceleration status using the **show run service-acceleration | grep feature** command.

Example:

```
switch# show run service-acceleration | grep feature

feature service-acceleration
```

Step 2 Use the **show interfaces brief** command to view the status of the interfaces.

Example:

```
Switch# show interface brief
..!
--------------------------------------------------------------------------------
Service         VLAN    Type Mode   Status  Reason                 Speed     Port
Ethernet                                                                     Ch #
--------------------------------------------------------------------------------
SEth1/1         --      eth  routed up      none                   200G(D) --
SEth1/2         --      eth  routed up      none                   200G(D) --
SEth1/3         --      eth  routed up      none                   200G(D) --
SEth1/4         --      eth  routed up      none                   200G(D) --
```

All DPUs power up when the feature service-acceleration is enabled.

Example

You can verify the DPUs are powered up and online using the **show module** command.

```
switch# show module
Mod Ports                 Module-Type                          Model           Status
--- ----- ------------------------------------------------ ---------------------- ---------
1    24   24x40/100G QSFP28 Ethernet Module                N9324C-SE1U           ok
27   0    Virtual Supervisor Module                        N9324C-SE1U           active *

<…snip…>

* this terminal session
Mod DPU   Module-Type           Model           Status
--- ---  ------------- ---------------------- --------
```

```
1    1     DPU              N9324C-SE1U-DPU       ok
1    2     DPU              N9324C-SE1U-DPU       ok
1    3     DPU              N9324C-SE1U-DPU       ok
1    4     DPU              N9324C-SE1U-DPU       ok

Mod DPU     Sw             Hw      Serial-Num   Online Diag Status
--- ---  ------------- ---------- ------------ ------------------
1    1    1.5.3.s        1.0       FDO285215F3      Pass
1    2    1.5.3.s        1.0       FDO285215F4      Pass
1    3    1.5.3.s        1.0       FDO285215F5      Pass
1    4    1.5.3.s        1.0       FDO285215F6      Pass
```

Disable service-acceleration feature

Procedure

Disable service-acceleration feature and Layer 4-7 services on the switch, for it to function in DPU powered-off state, using the using the **no feature service-acceleration** command.

Example:

```
Switch(config)# no feature service-acceleration
```

Note
If you want to re-enable the feature (after it is disabled), you need to reload the Cisco N9300 Smart switch.

Register the Cisco N9300 Smart switch with Hypershield

You should obtain a one time password (OTP) token from Hypershield. The token includes the information on how to reach Hypershield.

This token must be entered on the switch to establish communication between the switch and Hypershield.

Procedure

Establish communication between the switch and Hypershield with the obtained token using the **service system hypershield register** *otp* command.

Example:

```
Switch# service system hypershield register 34C58A…
```

Execute this comamnd at the EXEC level.

otp: Indicates the token string (maximum size 4094). Type the token without any quotes.

Verify Hypershield connection status

Procedure

Verify the status of the connectivity using the **show service-acceleration status details** command.

Example:

```
switch# show service-acceleration status details

 Service System: hypershield
  Source Interface: loopback100 (192.0.2.1/32)
  Agent Status: firewall-ready,redirect-installed
  Agent Health Status: failed (Error: dial unix /run/agw.sock: connect: connection refused)
  Controller Connection Status: success

[...]
```

Configure Hypershield connectivity

Perform this task to connect to to establish connectivity between the Hypershield Agent in the Cisco N9300 Smart switch and the Hypershield system.

Procedure

Step 1 Enable the **service system hypershield** command to set up the Hypershield instance.

Example:

```
Switch(config)# service system hypershield
```

Step 2 Configure the **source-interface** command to assign the loopback interface with the IP address to the Hypershield Agent.

Example:

```
Switch(config-svc-sys)# source-interface loopback 100
```

The loopback IP address must be configured in the default VRF. See Create a loopback interface, on page 5.

Note
You *cannot* configure the default VRF as service acceleration VRF as the system automatically blocks the configuration.

Example

The example shows service acceleration feature configuration.

```
switch# show run service-acceleration
!
feature service-acceleration
service system hypershield register 34C58A…
```

```
!
service system hypershield


  source-interface loopback 100
  ...!
```

Configure VRFs for traffic redirection to the firewall service

Peform this task to specify the VRFs whose traffic must be firewalled.

Procedure

Step 1 Enable the **service firewall** command.

Example:

```
Switch(config-svc-sys)# service firewall
```

Step 2 Configure the VRF under the service firewall to redirect the traffic in the VRF for inspection by the firewall service using the **vrf** *vrf-name* command.

Example:

```
Switch(config-svc-sys-fw)# vrf red module-affinity dynamic
```

The switch decides which DPU must inspect the traffic in the VRF, when **module-affinity dynamic** is used. The VRF context and other required networking configuration is entered as usual on the switch.

Step 3 (Optional) Configure a specific DPU number to indicate that traffic in the VRF must be inspected by the firewall service in that DPU using the **module-affinity** command.

Example:

```
Switch(config-svc-sys-fw)# blue module-affinity 1
```

Traffic in the VRF blue is inspected by DPU1.

This is a sample configuration example of a VRF for traffic redirection to the DPU.

```
Switch(config-svc-sys)# service firewall
Switch(config-svc-sys-fw)# vrf red module-affinity dynamic
Switch(config-svc-sys-fw)# vrf blue module-affinity 1
```

Example

The example shows service acceleration with firewalling enabled.

```
switch# show run service-acceleration
!
feature service-acceleration
service system hypershield register 34C58A…
!
service system hypershield
```

```
source-interface loopback 100
service firewall
  vrf blue module-affinity 1
  vrf red module-affinity dynamic
```

Enable traffic inspection with in-service for service firewalls

The **in-service** command enables the service firewall functionality, and allows traffic inspection by the DPUs.

You can also use the **no service firewall no in-service** commands to trigger maintenance mode for the firewall functionality and, to modify the service firewall DPUs and VRF pinning.

Procedure

Enable the **in-service** command to enable the service firewall to redirect specific traffic.

Example:

```
Switch(config-svc-sys-fw)# in-service
```

Verify traffic redirection to the DPU

Procedure

Use the **show service-acceleration status details** command to view the status of the VRFs.

Example:

The example shows the firewall service in "out-of-service" state.

```
switch# show service-acceleration status details
  Service System: hypershield
  Source Interface: Lo100 (192.0.2.1/9)
  Agent Status: firewall-disable
  Controller Connection Status: init
  Services:
  Firewall: out-of-service
      VRF             Operational State      Affinity
      ================================================
      blue            isolated                 n/a
      red             isolated                 n/a
```

Verify in-service functionality for service firewalls

Procedure

Step 1 Use the **show service-acceleration status details** command to view the status of the VRFs with module-affinity.

Example:

The example shows the firewall service in "in-service " state and the VRF enabled for firewalling.

```
switch# show service-acceleration status details
  Service System: hypershield
    Source Interface: Lo100 (192.0.2.1/8)
    Agent Status: firewall-ready,redirect-installed
    Controller Connection Status: success
    Services:
      Firewall: in-service

      VRF               Operational State       Affinity
      ================================================================
      blue              forwarding ready        1
      red               forwarding ready        3
```

Step 2 Use the command **show service-acceleration redirect-policy brief** to identify the service-ethernet subinterfaces for redirecting traffic from the VRF to the DPU.

Example:

```
switch# show system internal service-acceleration redirect-policy brief

VRF                              AF Type Interface[Status]  Affinity Redirect Status
================================================================================================
blue                             IPv4    SEth1/3.11[UP]     1        Enabled
red                              IPv4    SEth1/1.10[UP]     3        Enabled
blue                             IPv6    SEth1/3.11[UP]     1        Enabled
red                              IPv6    SEth1/1.10[UP]     3        Enabled
```