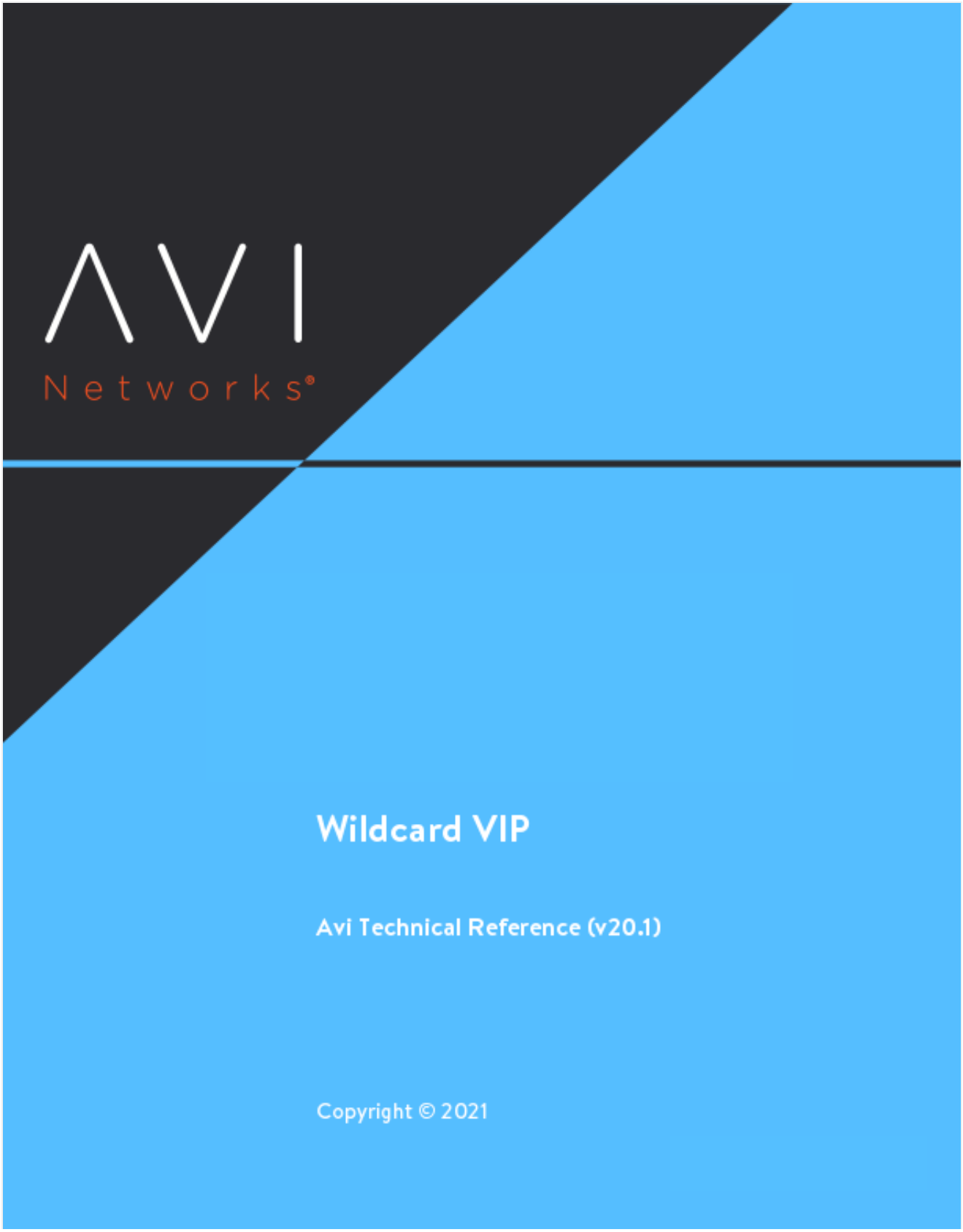


Wildcard VIP

Avi Technical Reference (v20.1)

Wildcard VIP

view online

Overview

In Avi Vantage, a virtual service is configured with an IP address as VIP and ports as Services to load balance the client traffic from the external world. Avi Vantage processes the client connection or request against a list of settings, policies and profiles, then load balances valid client traffic to a back-end application server that is listed as a pool member of the virtual service.

In addition to load-balancing the client traffic to the application servers, Avi Vantage also gives many benefits like supportability, manageability and scalability to the application servers. Application servers can be upgraded with zero downtime, when deployed with Avi Vantage. For more information, refer to The Avi Vantage Platform Overview page.

Starting with Avi Vantage release 20.1.1, Wildcard VIP extends the capability of a Virtual service to provide advanced load balancing services to network elements like firewalls and FW devices.

This article explains the concept of wildcard VIP and its configuration, common deployment and use case scenarios.

Features Supported

In Avi Vantage release 20.1.1, the wildcard virtual service is supported with the following profiles: * Network Profile: TCP fast path and UDP fast path. * Application Profile: System L4 application profile

Supported Environments

The wildcard VIP functionality is supported in the following environments:

- Active/ Standby SE group, in DPDK based environments
- VMware Read/Write modes and Bare-metal clouds

Wildcard VIP

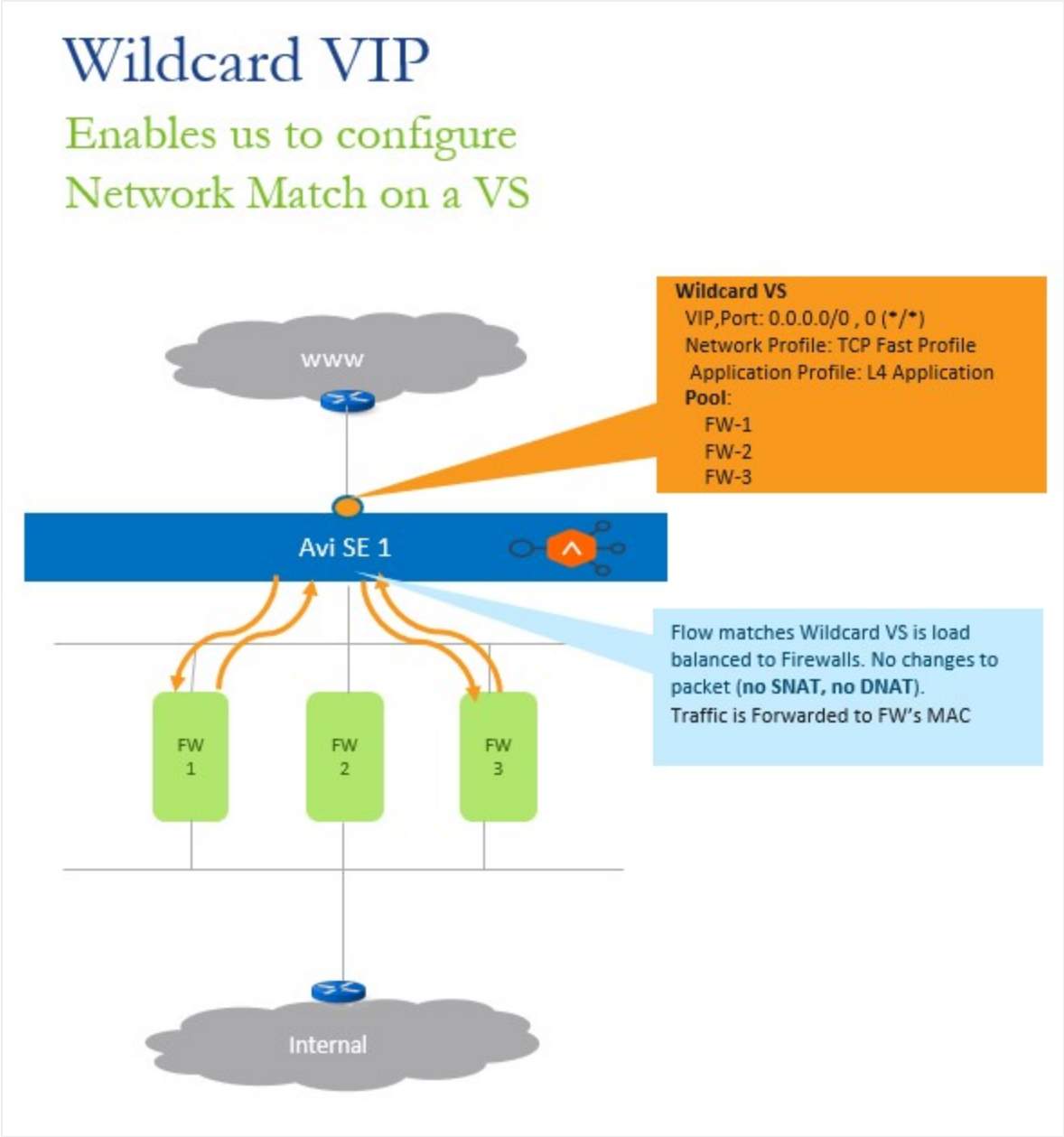
The wildcard VIP allows the network match configuration in a virtual service (VS). The application VS accepts the connections destined to a VIP, whereas the wildcard VIP accepts the connections destined to a subnet and is configurable as CIDR notation.

Network Address Match

Network traffic match is configured to handle a huge range of incoming traffic. As in the case of a corporate network it could be a subnet/prefix configuration.

For example, it could be a prefix of 10.0.0.0/8 (to accept between 10.0.0.0 - 10.255.255.255) or 0.0.0.0/0 (to accept every incoming packet).

A demonstration of wildcard VIP in deployment is as shown below:



In the deployment mode shown above, the wildcard virtual service is in the front-end, facing the client traffic. Three firewalls FW1, FW2, and FW3 are configured as pool members. The wildcard virtual service load balances the traffic across the firewalls FW1, FW2, and FW3.

Firewalls are rarely the destination for the client traffic, and the traffic is expected to be transparently forwarded to the firewall. Hence, the traffic from the client should be sent as is to the pool member without any source or destination address translation (SNAT or DNAT)

In such a deployment, the network address match is configured in the traffic selection criteria of the VIP. The wildcard VIP of the virtual service will only load balance the traffic to these firewalls without changing the client traffic.

Traffic Selection Criteria

With the introduction of network address match as part of the virtual service, the following combinations can be configured as the traffic selectors for the VIP:

```
<th>Destination</th>
<th>Service Port</th>
<th>Virtual Service Configuration</th>
```

```
<td>IP Address</td>
 <td>Port</td>
 <td></td>
```

```
<td>IP Address</td>
  <td>Any</td>
  <td>Service Port is 1 - 65535</td>
</tr>
```

```
<td>Network Address</td>
  <td>Port</td>
  <td>Prefix in ip_address (VIP)</td>
```

```
<td>Network Address</td>
  <td>Any</td>
  <td>Prefix in ip_address, Service Port: 0</td>
```

```
<td>Any</td>
   <td>Port</td>
   <td>Prefix 0 in ip_address</td>
</tr>
```

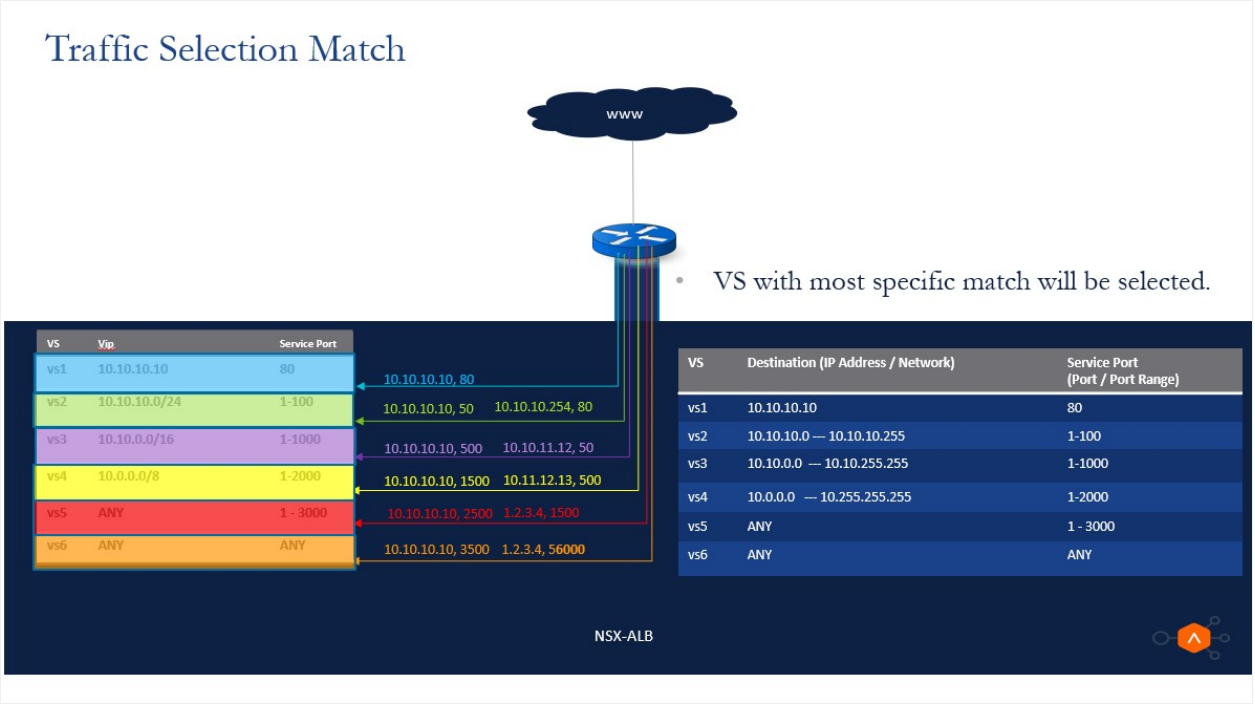
```
<td>Any</td>
  <td>Any</td>
  <td>Prefix 0 in ip_address<br>Service Port 0</td>
  </tr>
```

Note: Wildcard VIP is supported only for TCP/UDP fast network profiles.

In addition to the network, port supported, with the network address match feature, all the aforesaid variants of the wildcard virtual service can be configured.

In case you configure multiple virtual services with varying combinations as specified in the table, the virtual service with the most specific match will be selected in the same order of preference as listed in the table.

Refer to the following image for further details:



Configuring Wildcard VIP

As of Avi Vantage release 20.1.1, configuring wild card VIP is supported via the CLI only. Log in to the Avi Controller CLI shell and implement the following steps:

The wildcard VIP is configured in the virtual service.

A new field called `prefix_length` is introduced to take the net mask into consideration. If a VIP has the `prefix_length` field configured, it is a wildcard VIP.

Enabling Wild Card VIP in Virtual Service Configuration

To enable wildcard VIP, the placement subnet is mandatory for the virtual service that is referring the inline virtual service VIP.

```
configure vsvip <vsvip_name>
    vip index 0
    ip_address 10.0.0.0
    prefix_length 8
    save
    vrf_context_ref <vrf>
    tenant_ref <tenant>
    cloud_ref <cloud>
save
```

The placement subnet is configured as shown below:

```
[admin:abc-ctrl-wildcard]: > show vsvip vsvip-wc-Default-Cloud
+----------------------------+-------------------------------------------------------------+
| Field                      | Value                                                       |
+----------------------------+-------------------------------------------------------------+
| uuid                       | vsvip-7524a40f-33d0-4e4e-8d20-2193f31b8b39                  |
| name                       | vsvip-wc-Default-Cloud                                      |
| vip[1]                     |                                                             |
|   vip_id                   | 0                                                           |
|   ip_address               | 10.0.0.0                                                    |
|   enabled                  | True                                                        |
|   auto_allocate_ip         | False                                                       |
|   auto_allocate_floating_ip | False                                                      |
|   avi_allocated_vip        | False                                                       |
|   avi_allocated_fip        | False                                                       |
|   auto_allocate_ip_type    | V4_ONLY                                                     |
|   placement_networks[1]    |                                                             |
|     network_ref            | vxw-dvs-26-virtualwire-9-sid-2210008-wdc-02-vc21-avi-dev001 |
|     subnet                 | 100.64.1.0/24                                               |
|   prefix_length            | 8                                                           |
| vrf_context_ref            | global                                                      |
| east_west_placement        | False                                                       |
| tenant_ref                 | admin                                                       |
| cloud_ref                  | Default-Cloud                                               |
+----------------------------+-------------------------------------------------------------+
[admin:abc-ctrl-wildcard]: >
```

Note: The fields `placement_subnet` and `prefix_length` are configured.

Configuring the Port Range

Port ranges can be configured as part of the service object of the virtual service.
Starting with Avi Vantage release 20.1.1, you can configure port 0 that accepts the complete port-range of *1-65535* as shown below:

```
configure virtualservice <vs-name>
     services
        port 0
     save
save
```

Configuring the Application Profile

In the application profile, a new field,`preserve_dest_ip_port` has been introduced to enable the *no-DNAT* functionality.

As firewalls expect the client traffic unchanged for validation, the application profile of the wildcard virtual service has to be configured with `preserve_client_ip`, `preserve_client_port`, and `preserve_destination_ip_port`.

Configure `preserve_destination_ip_port` in the application profile as shown below:

```
configure applicationprofile <app_profile_name>
    preserve_dest_ip_port
save
```

The application profile is configured as shown below:

```
[admin:abc-ctrl-wildcard]: > show applicationprofile test1 | grep preserve|
| preserve_client_ip                  | True                              |
| preserve_client_port                | True                              |
| preserve_dest_ip_port               | True                              |
```

Configuring Routing Pool

To configure the routing pool,

```
configure pool <pool_name>
    routing_pool
save
```

The configured routing pools appear as shown below:

```
[admin:abc-ctrl-wildcard]: > show pool test1 | grep routing_pool
| routing_pool| True
[admin:abc-ctrl-wildcard]: >
```

Note: The field `routing_pool` is set to *True*.

Placement Network in VIP

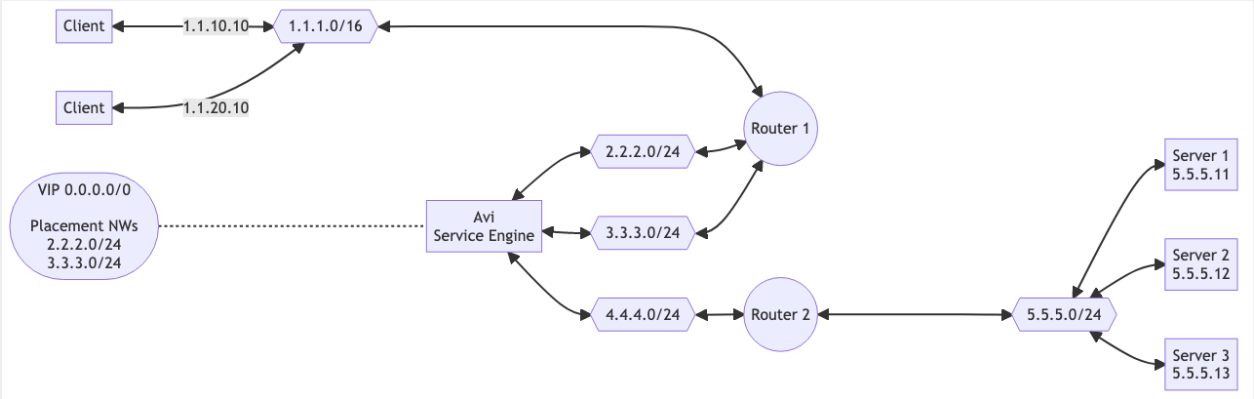
In No-Access and Linux Server Cloud scenarios, the Controller cannot configure the vNICs on demand on the SE. In this case, the SE is configured with a specific number of VNICs which have access to specific sub-nets. To load balance a VIP which is not present on any of the sub-nets accessible to the SE, the Controller cannot place the virtual service on the SE.

A placement network can be configured from the subnets accessible to the SE. Once that is configured, the Controller will forcefully place the VIP on the VNICs which have access to the placement networks. The user can then configure static routes on the SE, or on the previous hop router to ensure the traffic for the VIP is forwarded to the placement vNIC.

Consider this configuration where,

- The VIP is 0.0.0.0/0, with placement networks in 2.2.20/24 and 3.3.3.0/24
- The clients are trying to access 1.1.10.10 and 1.1.20.10
- The servers are 5.5.5.11, 5.5.5.12, 5.5.5.13
- The SE has vNICs in the subnets 2.2.2.0/24, 3.3.3.0/24 and 4.4.4.0/24

- Router 1 provides connectivity between 1.1.1.0/16, 2.2.2.0/24 and 3.3.3.0/24
- Router 2 provides connectivity between 4.4.4.0/24 and 5.5.5.0/24



In this case, all traffic intended for 1.1.10.10 and 1.1.20.10 is matched by the VIP 0.0.0.0/0 and is routed to the SE via the VNIC in 2.2.2.0/24 network subnet, and then load balanced across the Servers via the vNIC in 4.4.4.0/24 network subnet.

Prior to Avi Vantage version 20.1.5, only a single placement network was supported. Starting with Avi Vantage 20.1.5, all the matching networks on the SE are checked and place the virtual service on all the vNIC's of the matching SEs.

Multiple placement networks are supported and the virtual service can be placed on multiple vNICs.

Consider the following scenarios to understand this further:

Scenario	Placement Networks	Networks on SE	Placement Behavior
SE has access to the exact subnet of the VIP placement network	2.2.2.0/24	SE 1 eth1: 2.2.2.0 /24 SE 2 eth1: 2.2.2.0 /24	The virtual service will be placed on the matching vNICs of both SE - eth1 on SE 1 and eth1 on SE 2
Both the SEs have access to the same network, which is one of the two placement networks	2.2.2.0/24 3.3.3.0 /24	SE 1 SE 1 eth1: 2.2.2.0 /24 SE 2 eth1: 2.2.2.0 /24	The virtual service will be placed on the matching vNICs of both SE - eth1 on SE 1 and eth1 on SE 2

SE has access to a single network which is a superset of all the subnets of the placement network	2.2.2.0/25 2.2.2.128/25	SE 1 eth1: 2.2.2.0/24 SE 2 eth1: 2.2.2.0/24	The virtual service will be placed on the matching vNICs of both SE - eth1 on SE 1 and eth1 on SE 2
SE has access to a single network which is a superset of all the subnets of the placement network	2.2.2.0/25 2.2.2.128/25	SE 1 eth1: 2.2.2.0/24 SE 2 eth1: 2.2.2.0/24	Since the vNIC on SE covers both the placement networks, the virtual service is placed on the vNIC with 2.2.2.0/24 network - eth1 on SE 1 and eth1 on SE 2
There are two placement networks, and both SE have access to separate placement networks	2.2.2.0/24 3.3.3.0/24	SE 1 eth1: 2.2.2.0/24 SE 2 eth1: 3.3.3.0/24	The virtual service will be placed on the matching vNICs of both SE - eth1 on SE 1 and eth1 on SE 2
SE has access to all the subnets of the placement networks	2.2.2.0/24 3.3.3.0/24	SE 1 eth1: 2.2.2.0/24 eth2: 3.3.3.0/24 SE 2 eth1: 2.2.2.0/24 eth2: 3.3.3.0/24	Prior to Release 20.1.5: The virtual service will be placed on the first matching vNIC 2.2.2.0/24 of both the SEs - eth1 on SE 1 and eth1 on SE 2 Release 20.1.5 Onwards: The virtual service will be placed on all the matching vNICs of both SE - eth1, eth2 on SE 1 and eth1, eth2 on SE 2

Placement network gets modified to add a new placement network after the virtual service is placed. Network can be modified by either adding an SE network or by adding a placement network.	Before: 2.2.2.0/24 After: 2.2.2.0/24 3.3.3.0/24	Before: SE 1 eth1: 2.2.2.0 /24 eth2: 3.3.3.0 /24 After: SE 2 eth1: 2.2.2.0 /24 eth2: 3.3.3.0 /24	Prior to Release 20.1.5: Before: The virtual service will still be placed on the same vNICs of both SE - eth1 on SE 1 and eth1 on SE 2 After: The virtual service placement will not be modified to include the vNIC matching 3.3.3.0/24 placement network Release 20.1.5 Onwards: The virtual service will be placed on the matching vNICs of both SE - eth1, eth2 on SE 1 and eth1, eth2 on SE 2
SE gets access to a new network after the virtual service is placed.	2.2.2.0/24 3.3.3.0 /24	Before: SE 1 eth1: 2.2.2.0 /24 SE 2 eth1: 2.2.2.0 /24 After: SE 1 eth1: 2.2.2.0 /24 eth2: 3.3.3.0 /24 SE 2 eth1: 2.2.2.0 /24 eth2: 3.3.3.0 /24	Prior to Release 20.1.5: Before: The virtual service will still be placed on the matching vNICs of both SE - eth1 on SE 1 and eth1 on SE 2 After: The virtual service placement will not be modified to include the vNIC matching 3.3.3.0/24 placement network. Release 20.1.5 Onwards: The virtual service will be placed on the matching vNICs of both SE - eth1, eth2 on SE 1 and eth1, eth2 on SE 2

Note: Placement Networks is currently supported only for IPv4 configuration.

Caveats

The following features are currently not supported by the wildcard virtual service: * BGP based scale-out and other associated BGP features * Flow monitoring * Shared VIP * Traffic cloning

Suggested Reading

- Firewall Sandwich Topology

- Configuring Network Service
- Default Gateway (IP Routing on Avi SE)

Document Revision History

Date	Change Summary
April 15, 2020	Published the Feature Placement Network in VIP (Version 20.1.5)
July 30, 2020	Published the Feature KB for Wild Card VIP (Version 20.1.1)
June 17, 2020	Published the Feature KB for Wild Card VIP and Routing Auto Gateway Functionality(Tech Preview)