


Configure Service Chains

 For supported software information, click [here](#).

This article describes how to configure service chains.

When you configure service chaining with a VNF other than a Versa Network VNF (that is, a Versa Operating System™ [VOS™] device), you cannot use forward error correction (FEC), packet replication, or per-packet load balancing.

Configure a Service Chain

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Devices > Devices in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a Controller in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Networking  > Service Chains > Service Chains in the left menu bar.
4. Click the  Add icon to configure a service chain. Enter information for the following fields.

Add Service Chain

Name*

Service_chain

Type

Internal

Description

Tags

Next Peer

Interface

Previous Peer

ID

Service Node Group


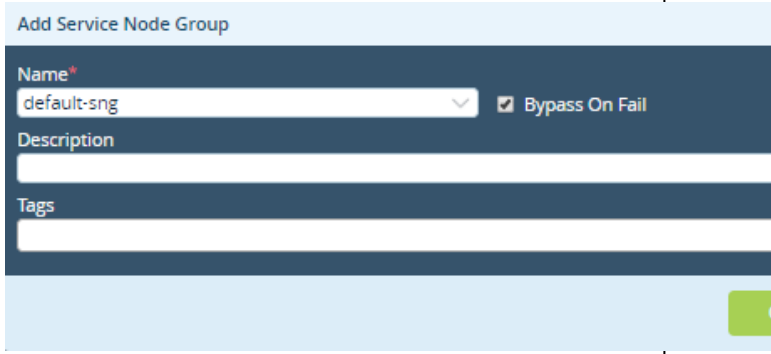
1

25

<input type="checkbox"/>	Name	Bypass On Fail
NO SERVICE NODE GROUP ADDED		

OK



Cancel

Field	Description
Name	Enter a name for the service chain.
Type	Select the service chain type Internal.
Description	Enter a text description for the service chain.
Tags	Enter tags to associate with the service chain.
Next Peer	<p>Select the type of next peer in the service chain, and then enter information for the specific peer in the field to the right:</p> <ul style="list-style-type: none"> ◦ ID ◦ Interface ◦ Layer 3 ◦ Back To Sender
Previous Peer	<p>Select the type of previous peer in the service chain, and then enter information for the specific peer in the field to the right:</p> <ul style="list-style-type: none"> ◦ ID ◦ Layer 3
Service Node Group	<p>Click the  Add icon to configure a service node group. Add information for the following fields.</p> 
◦ Name	Enter a name for the service node group.

◦ Bypass On Fail	Click to allow traffic to bypass the service node group when it fails
◦ Description	Enter a text description for the service node group.
◦ Tags	Enter tags to associate with the service node group.

- Click OK twice.

Configure a Service Chain Instance

- In Director view:
 - Select the Configuration tab in the top menu bar.
 - Select Devices > Devices in the horizontal menu bar.
 - Select an organization in the left menu bar.
 - Select a Controller in the main pane. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select Networking  > Service Chains > Service Chain Instances in the left menu bar
- Click the  Add icon to configure a service chain instance. Enter information for the following fields.

Add Service Chain Instance

Name*

Description

Tags

Service Chain*

Local Service Chain ID*

Local Service Index

Next Service Chain ID

Previous Service Chain ID

☐ Symmetric

☐ Reverse Traffic Symmetric



OK

Cancel

Field	Description
Name	Enter a name for the service chain instance.
Description	Enter a text description for the service chain instance.
Tags	Enter tags to associate with the service chain instance.
Service Chain	Select the service chain to use.
Local Service Chain ID	Enter an ID for the local service chain.
Local Service Index	Enter the index for the local service chain.
Next Service Chain ID	Enter the ID for the next service chain.
Previous Service Chain ID	Enter the ID for the previous service chain.
Symmetric	Select to enable traffic to flow symmetrically.
Reverse Traffic Symmetric	Select to enable traffic in the reverse direction to flow symmetrically.

5. Click OK.

Configure Service Filters

- In Director view:
 - Select the Configuration tab in the top menu bar.
 - Select Devices > Devices in the horizontal menu bar.
 - Select an organization in the left menu bar.
 - Select a Controller in the main pane. The view changes to Appliance view.
- Select the Configuration tab in the top menu bar.
- Select. Networking  > Service Chains > Service Filters in the left menu bar.
- Click the  Add icon to configure a service filter classifier. Enter information for the following fields.

Field	Description
Name	Enter a name for the service chain instance.
Description	Enter a text description for the service chain instance.
Tags	Enter tags to associate with the service chain instance.

5. Click OK.

6. In Rules, click the  Add icon to add a rule. In the General tab, enter information for the following fields.

Field	Description
Name	Enter a name for the service chain instance.
Description	Enter a text description for the service chain instance.
Tags	Enter tags to associate with the service chain instance.

7. In the Source/Destination tab, configure the source and/or destination addresses as matching criteria to capture traffic. Enter information for the following fields.

Add Rule

General

Source/Destination

Headers/Schedule

Enforce

Source Zone

+ New Zone

Destination Zone

+ New Zone

Source Site Name

Destination Site Name

Source Address

+ New Address Group

+ New Address

Destination Address

+ New Address Group

+ New Address

Source Address Negate

Destination Address Negate

Routing Instance





--Select--



Egress Routing Instance

--Select--

OK

Cancel

Field	Description
Source Zone	Click the  Add icon and select the zone that is the source of the traffic that the VOS device processes. For more information, see Configure Zones and Zone Protection Profiles .
Destination Zone	Click the  Add icon and select the zone that is the destination of the traffic that the VOS device processes. For more information, see Configure Zones and Zone Protection Profiles .
Source Site Name	Click the  Add icon and select the source site name.
Destination Site Name	Click the  Add icon and select the destination site

Field	Description
	name.
Source Address	<p>Click the  Add icon and select the originating address of incoming traffic. The address is classified based on:</p> <ul style="list-style-type: none"> ◦ Originating country ◦ Originating region ◦ IP address <p>For more information, see Configure Address Objects.</p>
Source Address Negate	Click to block traffic to the selected source addresses.
Destination Address	<p>Click the  Add icon and select the destination address of outgoing traffic. The address is classified based on:</p> <ul style="list-style-type: none"> ◦ Originating country ◦ Originating region ◦ IP address <p>For more information, see Configure Address Objects.</p>
Destination Address Negate	Click to block traffic to the selected destination addresses.
Routing Instance	Select a routing instance.
Egress Routing Instance	Select an egress routing instance.

8. In the Headers/Schedule tab configure matching criteria based on the IP packet header information. Enter information for the following fields.

Add Rule

GeneralSource/DestinationHeaders/ScheduleEnforce

IP

IP Version

--Select--

IP Flags

--Select--

DSCP

+

TTL

Condition

Greater than or equal to

Value

Others

Schedules

--Select--

+ Schedule

Services


Service List

+ New Service

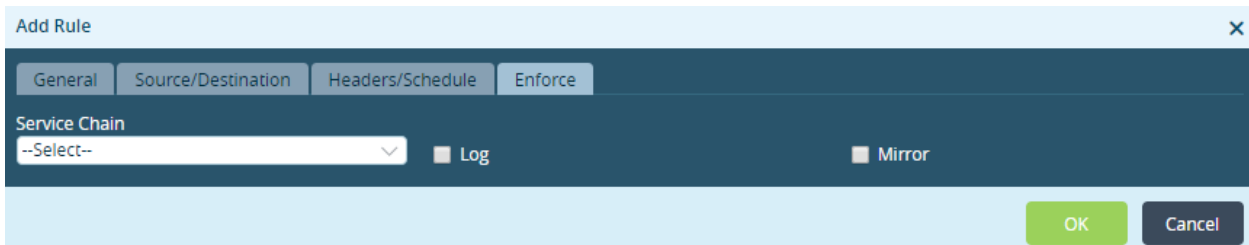
OK

Cancel

Field	Description
IP Address (Group of Fields)	
<ul style="list-style-type: none"> ◦ IP Version 	Select the IP header version to which the service chain rule applies.
<ul style="list-style-type: none"> ◦ IP Flags 	<p>For IPv4, select a fragmentation flag:</p> <ul style="list-style-type: none"> ◦ Don't Fragment ◦ More Fragment
<ul style="list-style-type: none"> ◦ DSCP 	Enter a DSCP value to classify how the IP packet is placed in the forwarding queue and thuse to assign a value or cost to the policy.
TTL (Group of Fields)	
<ul style="list-style-type: none"> ◦ Condition 	<p>Select the TTL condition that the service chain rule uses to trigger the rule. The condition matches the traffic based on the selected IP version, IP flag and TTL match.</p> <ul style="list-style-type: none"> ◦ Greater than or equal to—TTL value must be greater than or equal to the specified value. ◦ Less than or equal to—TTL value must be less

Field	Description
	<p>than or equal to the specified value.</p> <ul style="list-style-type: none"> ◦ Equal to—TTL value must be equal to the specified value.
◦ Value	Enter the TTL value for the service chain rule to match with the TTL condition.
Others (Group of Fields)	
◦ Schedules	Select a schedule to use when the service chain rule is in effect.
Services (Group of Fields)	
◦ Service List	<p>Click the  Add icon and select one or more services that is allowed or blocked and apply the service chain rule to the configured services. This includes the predefined and user-defined services. Service is defined on the basis of the destination address and port. For more information, see Configure Service Objects.</p>

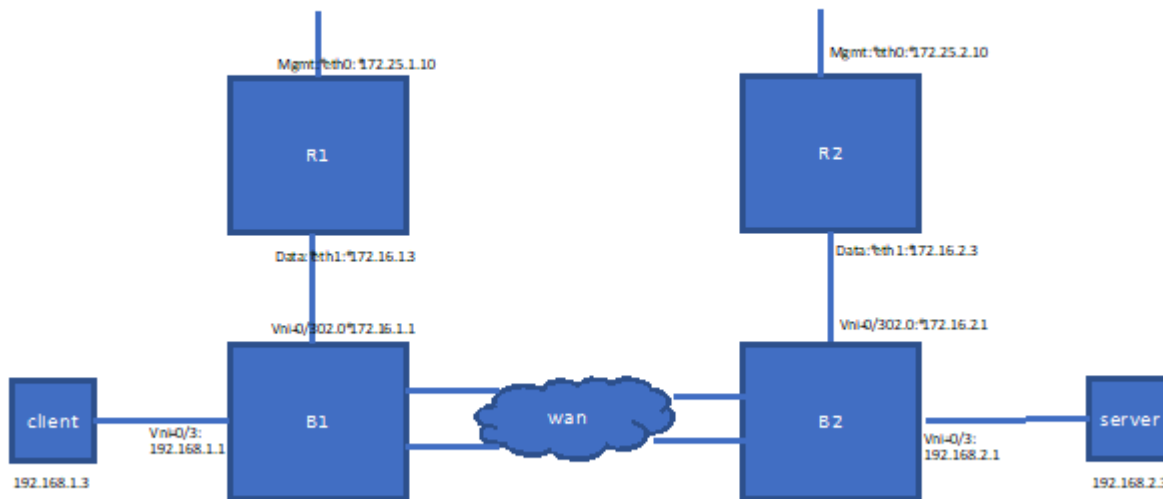
9. Select the Enforce tab to apply the service chain to the service filter rule. Enter information for the following fields.



Field	Description
Service Chain	Select a service chain.
Log	Click to enable log reporting.
Mirror	Click to enable mirroring.

Service Chaining with Replify Nodes Example

This section discusses how to configure service chaining in topologies that contain Replify nodes. The following figure illustrates the sample topology used in this example. Here, traffic from a client at Branch B1 to a server at Branch B2 is optimized through the Replify nodes R1 and R2. Each of these Replify nodes has two interfaces: a management interface and a data interface. The management interface is in the organization's control virtual router, which allows the Replify nodes to access them, through the Director node, using HTTP and ssh. The data interface is in the LAN virtual router, and the Replify nodes are service-chained in Layer 3 mode.



The following table lists the interfaces, virtual routers, and zones of the two branches.

Branch	Interface Description	Interface	IP Address	Virtual Router	Zone
Branch 1					
	LAN interface	vni-0/3.0	192.168.1.1/24	LAN VR	Intf-LAN-Zone
	Management interface	vni-0/300.0	172.25.1.1/24	Control VR	—
	Interface for Replify data	vni-0/302.0	172.165.1.1/24	LAN VR	Replify-Zone
Branch 2					
	LAN interface	vni-0/3.0	192.168.2.1/24	LAN VR	Intf-LAN-Zone

Branch	Interface Description	Interface	IP Address	Virtual Router	Zone
	Management interface	vni-0/300.0	172.25.2.1/24	Control VR	—
	Interface for Replify data	vni-0/302.0	172.165.2.1/24	LAN VR	Replify-Zone

Replify Configuration

When you create a Replify VNF, DHCP IP is assigned to eth0. This address belongs to the management network.

Apply License

To apply license, log in to Replify through the web console of Versa Director as the user Administrator, with the password default.

Configure the Data Interface

To configure eth1 as the data interface, log in to the Director node as the user root, with the password default, using either the web or the ssh interface.

Configure Routes

For this example, we assume that all the LAN VRs hosted behind SD-WAN branches fall in the IP prefix range 192.0.0.0/8 and that all the peer Replify nodes are configured in the IP prefix range 172.16.0.0/16. You need to configure routes such that the default route is through the management interface, and the Replify subnets and host subnets are routed through the data interface.

To view the routes on the R2 Replify node:

```
root@Replify-ucpe2:~# route -n
Kernel IP routing table
Destination Gateway  Genmask      Flags Metric Ref Use Iface
0.0.0.0     172.25.2.1  0.0.0.0      UG  0     0  0 eth0
172.16.0.0   172.16.2.1  255.255.0.0  UG  0     0  0 eth1
172.16.2.0   0.0.0.0     255.255.255.0 U  0     0  0 eth1
172.25.2.0   0.0.0.0     255.255.255.0 U  0     0  0 eth0
192.0.0.0    172.16.2.1  255.0.0.0    UG  0     0  0 eth1
```

Verify Communication between Replify Nodes

To verify that the two Replify nodes can communicate with each other over the SD-WAN VPN, ping the R2 data interface from the ssh terminal of R1.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_Servic...

Updated: Wed, 23 Oct 2024 08:26:24 GMT

Copyright © 2024, Versa Networks, Inc.

```

root@Replify-ucpe1:~# ping 172.16.2.3
PING 172.16.2.3 (172.16.2.3) 56(84) bytes of data.
64 bytes from 172.16.2.3: icmp_seq=1 ttl=62 time=3.04 ms
64 bytes from 172.16.2.3: icmp_seq=2 ttl=62 time=2.67 ms

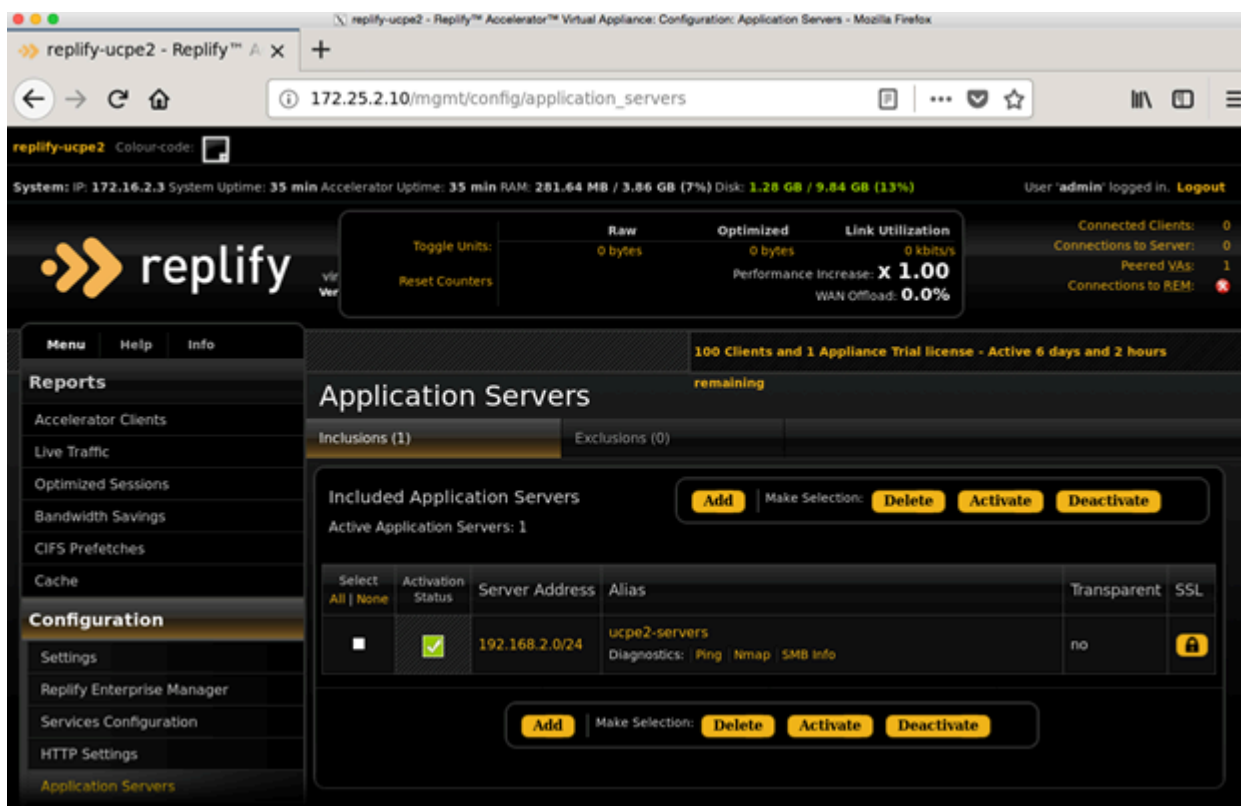
```

Configure Optimization Services on Replify Nodes

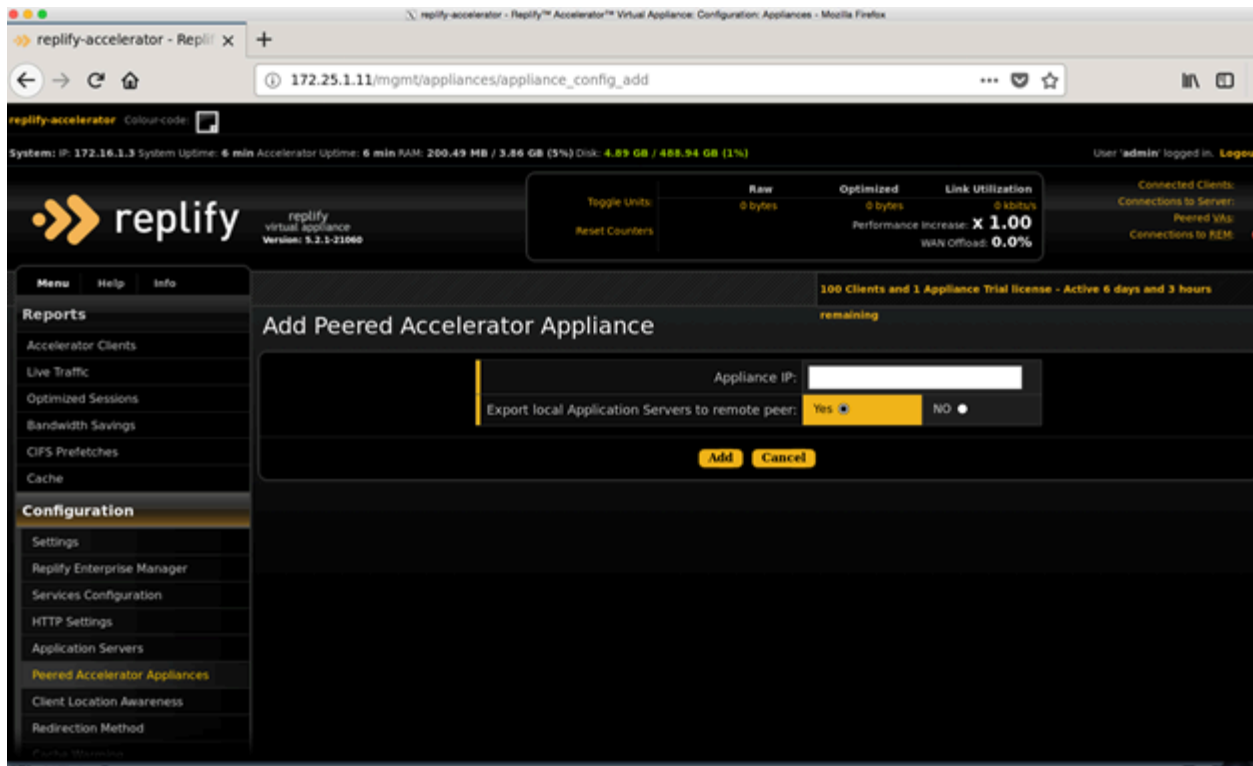
In this example, clients at Branch B1 access servers at Branch B2, and we want to optimize this traffic.

To configure optimization services on the Replify node:

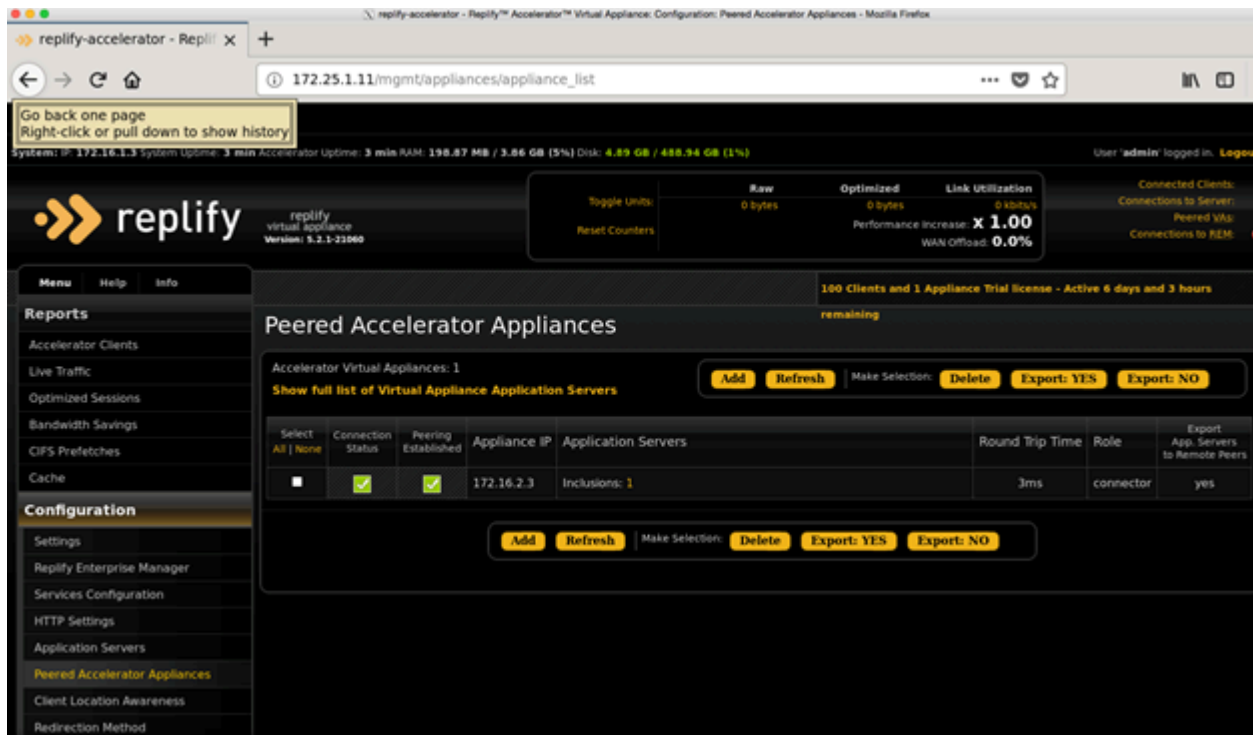
1. Configure application servers ucpe2-servers on Replify node R2, to optimize all traffic to these IP addresses.



2. Add the Branch B2 LAN subnet (192.168.2.0/24) as the server address.
3. On Replify node R1, configure R2 as a peer Replify. Provide the R2 data interface address (192.168.2.3) as the appliance IP address.



4. Verify that the R1 and R2 Replify nodes are peered properly. The peer connection status should be Up and green.



https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_Servic...

Updated: Wed, 23 Oct 2024 08:26:24 GMT

Copyright © 2024, Versa Networks, Inc.

Note that R1 and R2 establish a control connection between themselves. This connection is from R1 to port 32896 on the R2 data IP interface. An example of a control connection is a connection from 172.16.1.3:50247 to 172.16.2.3:32896. Ensure that this connection is allowed by any security rules. There is only one control connection, independent of the number of optimized connections flowing through the appliances.

At the completion of this process, R1 is configured to optimize any traffic to 192.168.2.0/24 with R2 as the peer. Also, if you select the Export Local Application Servers to Remote Peer checkbox is selected, R2 learns about any application servers configured on R1.

Configure Service Chaining on the Branches

To configure service chaining on the branch devices B1 and B2 to optimize TCP traffic that is sent from the LAN to the WAN on Branch B1:

1. Create the Replify service node group:

```
admin@UCPE-1-cli(config)% show service-node-groups
Replify-SNG
{
  id 2;
  type sfc-unaware-service-function;
  ingress-interface vni-0/302.0;
  egress-interface vni-0/302.0;
  service-function-egress-address 172.16.1.3;
  service-function-ingress-address 172.16.1.3;
}
```

2. Create the service chain. In this configuration, the service chain first goes to default-sng, which performs all Versa internal services, and then to the Replify node.

```
admin@UCPE-1-cli(config)% show orgs org uCPE service-chains
SC-Replify
{
  type internal;
  service-node-group default-sng;
  service-node-group Replify-SNG;
}
```

3. Create the service chain instance:

```
admin@UCPE-1-cli(config)% show orgs org-services uCPE service-chain-instances
SC-Replify
{
  service-chain SC-Replify;
  local-service-chain-id 503;
  reverse-traffic-symmetric enabled;
}
```

To configure service-chaining rules on Branch B1, only one rule is required, which service-chains all TCP traffic from the LAN and WAN to SC-Replify. Note that you do not need to configure service-chaining rules on B2, because Replify

nodes to not perform transparent service chaining.

```
admin@UCPE-1-cli(config)% show orgs org-services uCPE service-filters classifier
default-classifier
{
  rules
  {
    FromLAN
    {
      Match
      {
        Source
        {
          Zone
          {
            zone-list [ Intf-LAN-Zone ];
          }
        }
      }
    }
  }
  destination
  {
    Zone
    {
      zone-list [ ptvi ];
    }
  }
  services
  {
    predefined-services-list [ TCP ];
  }
}
se
{
  service-chain SC-Replify;
}
}
```

Traffic Flow

To understand traffic flows, let's consider a client 192.168.1.3 at Branch B1 that is downloading a file from server 192.168.2.3 at Branch B2. For this to happen, three sessions are established:

- Client to R1
- R1 to R2
- R2 to file server

In the forward direction:

1. The client establishes a connection to server port 80, specifically from 192.168.1.10:47511 to 192.168.2.10:80.

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_Service...

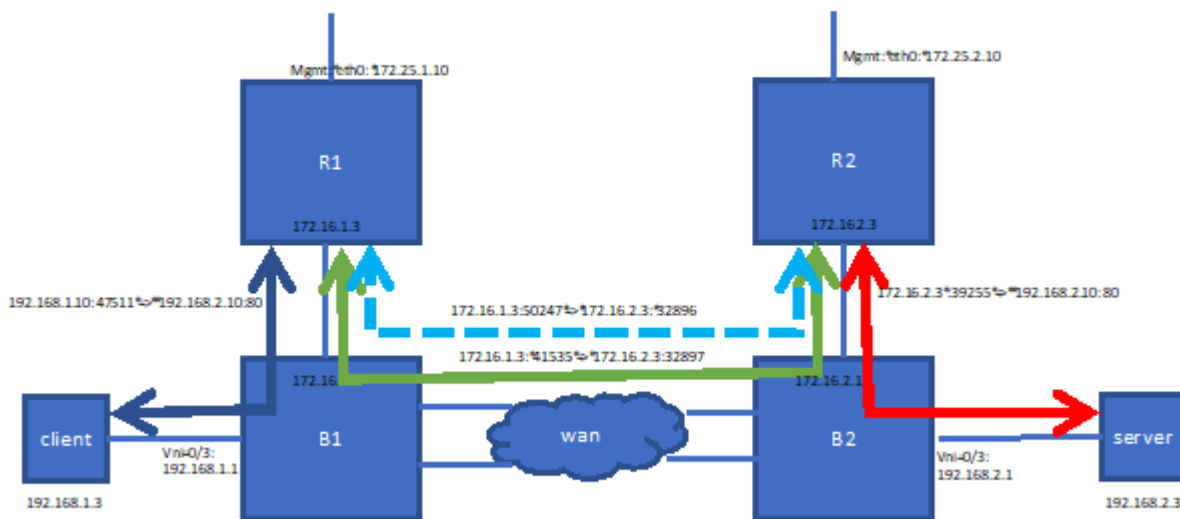
Updated: Wed, 23 Oct 2024 08:26:24 GMT

Copyright © 2024, Versa Networks, Inc.

Forward direction packets that match the service chaining rule from LAN are redirected to the Replify R1 data interface.

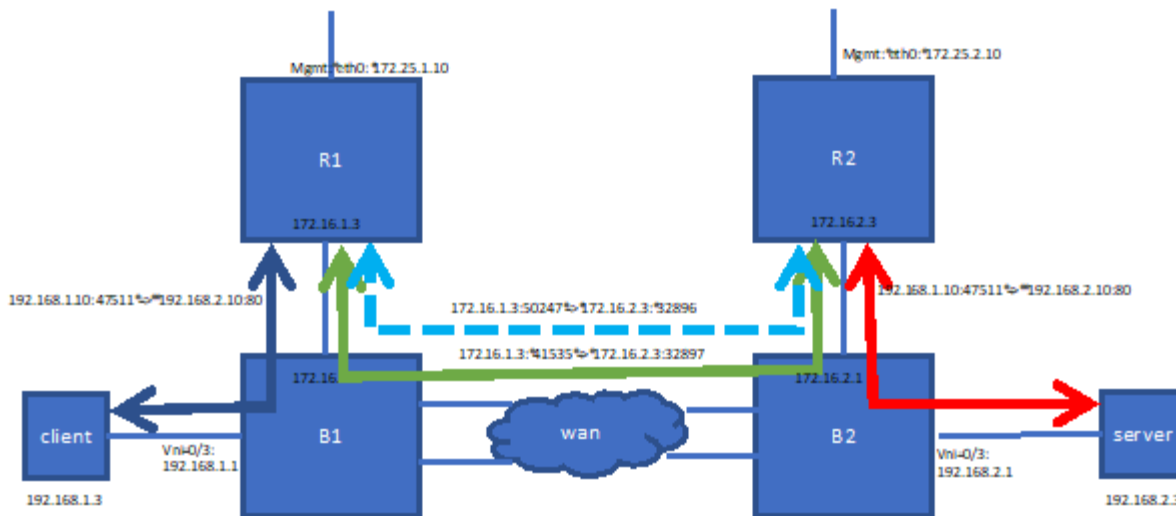
2. R1 looks up the peer Replify corresponding to the application server 192.168.2.3 (ucpe2-servers). It initiates a connection to the R2 using its own IP address. The connection is always established from an ephemeral port to port 32897, for example, from 172.16.1.3:51435 to 172.16.2.3:32897. Forward direction packets of this session are sent over the WAN and reach B2. Here, they are forwarded to R2, because the destination IP address is the R2 data interface. Note that because no service chaining is configured on R2, the traffic is not service-chained
3. R2 establishes a connection to the server using its own IP address as the source, for example, 172.16.2.3:39255 to 192.168.2.10:80.

In the reverse direction, the server sends reverse direction packets back to R2. R2 sends reverse direction packets to R1. R1 sends packets to the client using the server's IP address as source address. Only packets belonging to the original client > server flow on Branch 1 get service chained. The following figure illustrates the traffic flow.



Configure Transparency on a Replify Node

You can configure the R2 Replify node to be transparent to the server. When it is transparent, instead of opening connection 3 from its own data IP address, it uses the client's IP address and port. To enable this, you configure a packet-based forwarding symmetric Layer 2 forwarding rule on B2. This rule ensures that reverse direction packets from the server to the client are redirected to R2.



```
admin@UCPE-2-cli(config)% show orgs org-services uCPE pbf
```

```
policies {
  p1 {
    rules {
      r1 {
        match {
          source {
            zone {
              zone-list [ Replify-LAN-Zone ];
            }
          }
          destination {
            address {
              address-list [ server_addrs ]; // 192.168.2.0/24
            }
          }
        }
        set {
          enforce-symmetric-l2;
        }
      }
    }
  }
}
```

Debug Replify Service Chaining

If a session is not able to pass traffic, verify that:

https://docs.versa-networks.com/Secure_SD-WAN/01_Configuration_from_Director/Common_Configuration/Configure_Servic...

Updated: Wed, 23 Oct 2024 08:26:24 GMT

Copyright © 2024, Versa Networks, Inc.

- The two Replify nodes can communicate with each other over their data interfaces. To do this, use the **ping** command.
- The two Replify nodes are peered properly.

To determine whether packets are being service-chained properly, use the **show session** CLI command.

For example, add a session display filter to isolate the client's connections on R1, as well as the R1 data connection to R2:

```
// client->server connection
admin@UCPE-1-cli(config)% request orgs org uCPE filter-add filter-name f1 destination-port 80
// R1 -> R2 data connection
admin@UCPE-1-cli(config)% request orgs org uCPE filter-add filter-name f2 destination-port 32897
```

Check whether packets are being dropped on these sessions and whether they are being service-chained properly. Remember that only client-server session packets are service-chained on R1.

```
admin@UCPE-1-cli(config)% run show orgs org uCPE sessions filter f1 extensive
extensive 0 2 173032
source-ip          192.168.1.10
destination-ip      192.168.2.10
source-port        47512
destination-port    80
protocol           6
natted             No
sdwan              Yes
application         http
forward-pkt-count   14194
forward-byte-count  738248
reverse-pkt-count   84103
reverse-byte-count  125511132
dropped-forward-pkt-count 0
dropped-forward-byte-count 0
dropped-reverse-pkt-count 0
dropped-reverse-byte-count 0
session-age        00:01:01
idle-for           00:00:00
idle-timeout       131
pbf-enabled        false
forward-egress-vrf  uCPE-LAN-VR
reverse-egress-vrf  uCPE-LAN-VR
session-provider-zone 0
forward-offload     false
reverse-offload     false
forward-ingress-interface vni-0/3.0
forward-egress-interface ptvi-0/37
reverse-ingress-interface vni-0/302.0
reverse-egress-interface vni-0/3.0
forward-fc          fc_be
reverse-fc          fc_be
forward-plp         low
reverse-plp         low
```

```

external-service-chaining true
rx-wan-ckt -
tx-wan-ckt Broadband:Broadband
tx-branch -
pbf-wan-ack-enc (P,E)
forward-ingress-ckt vni-0/3.0
forward-egress-branch UCPE-2
forward-egress-ckt Broadband:Broadband
reverse-ingress-ckt vni-0/302.0
reverse-egress-ckt vni-0/3.0
sdwan-rule-name Default-Rule

sng-1 sng-name Replify-FromLAN-SNG
sng-1 forward-tx-pkts 14194 // client to server packets sent to R1
sng-1 forward-tx-bytes 738248 sng-1 forward-rx-pkts 0 // no packets are returned by R1 since it forwards the
packets on the R1 -> R2 connection
sng-1 forward-rx-bytes 0
sng-1 reverse-tx-pkts 0
sng-1 reverse-tx-bytes 0
sng-1 reverse-rx-pkts 84103 // reverse direction packets for client->server connection received from R1
sng-1 reverse-rx-bytes 125511132
sng-1 forward-bypass-pkts 0
sng-1 forward-bypass-bytes 0
sng-1 reverse-bypass-pkts 0
sng-1 reverse-bypass-bytes 0

```

To debug the Replify node, if data transfer through the Replify node is slow, it may be because the cache is being bypassed. Ensure that the cache size is big enough to accommodate the largest file being downloaded. For example, if the cache size is 256 MB and the size of a downloaded file is 400 MB, the file is not be optimized or cached, because it is larger than the cache.

Supported Software Information

Releases 20.2 and later support all content described in this article.

Additional Information

[Configure Address Objects](#)

[Configure Layer 7 Objects](#)

[Configure Service Objects](#)

[Configure uCPE on a VOS Device](#)

[Configure Zones and Zone Protection Profiles](#)