Deployment Guide
Jan-2017 rev. a

APV/SonicWall Layer 3 Firewall Cluster Deployment Guide

1 Introduction

In the age of big data, mobile, social and cloud, the longevity of today's data center is highly dependent on being agile, scalable, manageable, flexible, and most importantly secure against the ever-changing global threat environment. Enterprises, Carriers and ISPs demand network security solutions that can meet their massive data and capacity demands. This means that the network security layer must also be highly extensible to support the largest of data centers' bandwidth consumptions. Such requirements have made necessary networking security architectures that can be incrementally deployable and horizontally scalable. In other words, there might not be a single Next-Generation Firewall (NGFW) with the scale to meet the performance requirements of some deployments. An alternate way to scale the performance beyond capabilities of a single NGFW device is to combine multiple NGFW devices into a network cluster, leveraging the high-performance load balancing capabilities of Array's APV Series Application Delivery Controllers (ADCs). In this infinite scale-out model, adding additional security compute resources should ideally be a matter of easily adding more firewalls to the system in a very cost-effective way.

This document describes a Layer 3 cluster deployment that increases the performance and the capacity of the SonicWall NGFW for outbound traffic (LAN to WAN) through APV Series load balancing. The deployment supports traffic originated by the clients on the LAN and correctly routes dependent flows such as inbound SIP calls originated on the WAN.

In this network configuration, one APV Series Load Balancer distributes outbound traffic across multiple SonicWall NGFW nodes. Each node is configured with a unique WAN IP address and optionally a unique outbound NAT address range. Outbound traffic is Source IP NAT'ed. Return packets of the same flow and inbound packets from dependent flows are routed to the correct node based on the unique NAT'ed address.

2 Prerequisites

2.1 Hardware Requirements for this Example

- 1 Load Balancer - APV10650
- 1 Layer 2 Switch – Networking S4810
- 2-8 Firewall Nodes - SuperMassive 9800
- SonicWall Global Management System (GMS)

2.2 Array Networks APV Series Application Delivery Controllers

The APV appliance must be running version **ArrayOS TM 8.x** or later. For more information on deploying the APV appliance, please refer to the ArrayOS™ Web UI Guide, which is accessible through the product's Web User Interface. We assume that the APV Series appliance is already installed in the network with Management IP, interface IP, VLANs and default gateway configured.

3 Detailed Description

Fig.1 shows a detailed configuration of a Layer 3 cluster deployment (also called an L3 open sandwich).

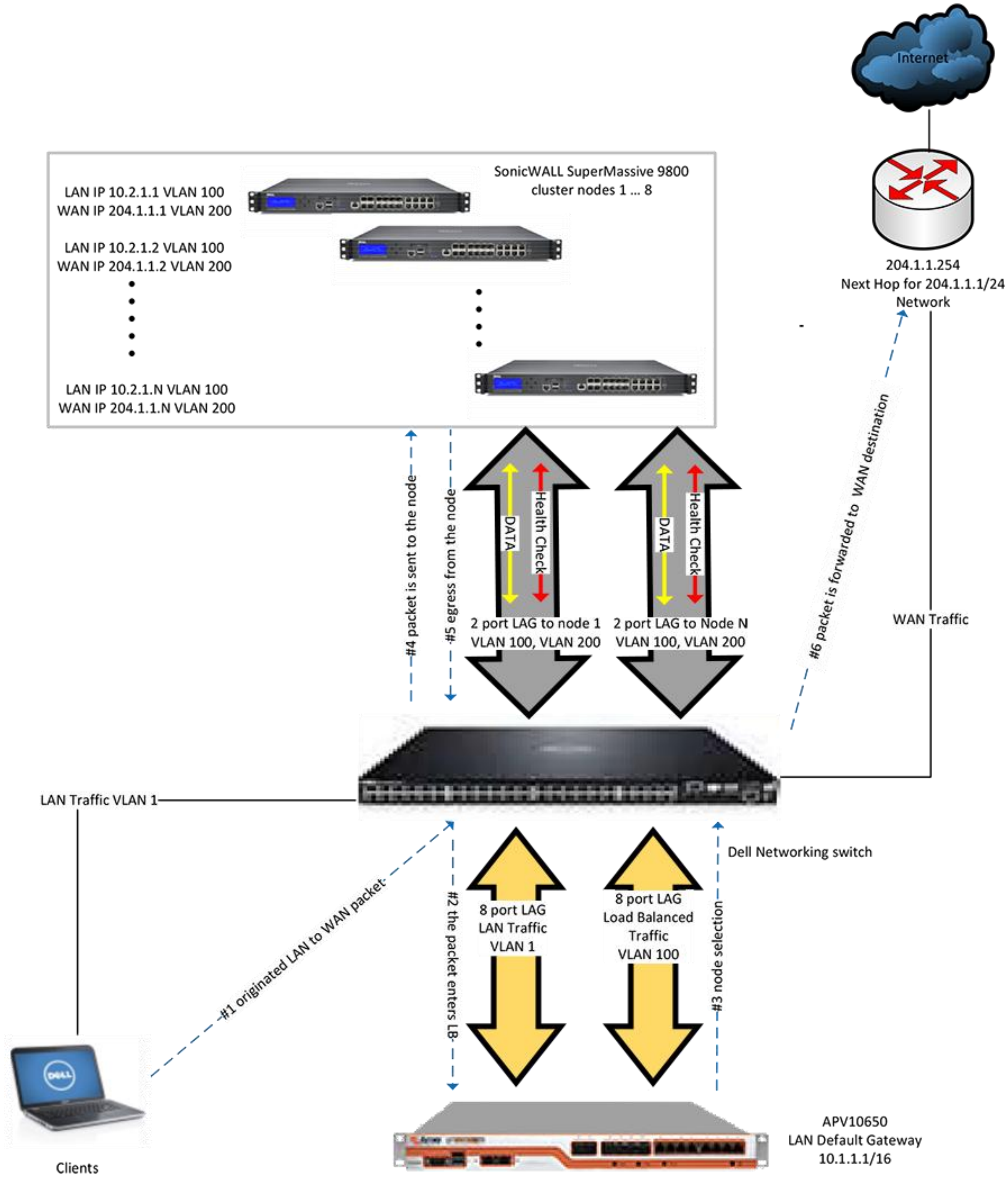


Figure 1: Deployment Details

In the sample deployment, the APV Series operating as an ingress load balancer is used to distribute outbound flows (LAN to WAN). The APV Series load balancer interface is configured as a gateway for the hosts on the LAN. On egress, the flows are NAT'ed to the individual node's WAN IP address or to an IP address from a NAT range that is unique on each node.

This configuration provides full redundancy for the SonicWall firewall nodes. Failure of a node is detected by the APV Series load balancer, at which point the load balancer stops sending the traffic to the failed node. The failover is not stateful and therefore existing flows will be disrupted. A configuration that provides redundancy for the switch and the APV Series load balancer is described in a later section.

3.1 Regular LAN to WAN traffic, e.g. HTTP

- A packet is originated by a host on the LAN and is sent to the gateway, which is the IP address of the ingress APV Series load balancer.
- The ingress APV Series load balancer receives the packet and selects the path through one of the nodes. 'Consistent Hash' of source and destination IP is used as a load balancing algorithm. This ensures that all outbound packets for the same session or application have complete session visibility and inspection.
- The packet is received by the selected node. The node performs all configured security functions – applies access rules, DPI, etc.
- If the packet is allowed, the packet source IP address is NAT'ed to the WAN interface IP address or to an IP from the WAN NAT pool range specific to the node.
- The response packet is routed back to the appropriate firewall node based on the packet's destination IP, ensuring symmetric routing and full session inspection from the same firewall node.

3.2 Active FTP

In the Active FTP case, the FTP data connection is established to a NAT'ed client's IP address thus ensuring that the data connections goes through the same node as the control connection.

3.3 Passive FTP

The passive FTP connection is established between the same pair of IP addresses as the control connection. Consistent Hash for Source+Destination IP will select the same node. Thus, the control and data connection will go through the same node.

3.4 SIP

Data connections are established to a NAT'ed client's IP address, ensuring that the data connections go through the same node as the control connection. Note that the existing optimization allowing two SIP clients on the same network to bypass the firewall does not work in cases when two clients' control connections are load balanced through two different nodes

4 Configuration Steps

4.1 Firewalls

In this deployment, each firewall is expected to handle traffic in excess of 10Gbps per node. That requires a two-port LAG for ingress and egress. Configuration steps are:

- Create a two-port LAG - Switching/Link Aggregation
- Create two VLAN subinterfaces for this LAG; one LAN - VLAN100 and one WAN - VLAN200
- A private network is used to connect the APV Series load balancer with the nodes. Assign a unique IP to each node LAN interface, i.e. 10.2.1.1 ... 10.2.1.N
- Assign a unique WAN interface IP to each node
- Optional - add a custom NAT policy for Source IP remap of outbound LAN connections

4.2 Configuring the Networking Switch

1. Configure the Load Balancer ingress LAG. This LAG uses LACP
    - (conf)#interface port-channel 69
    - (conf-if-po-69)#description "This port channel sends traffic from LAN to LB"
    - (conf-if-po-69)#switchport
    - (conf-if-po-69)#no spanning-tree
    - (conf-if-po-69)#lacp long-timeout
    - (conf-if-po-69)#no shutdown
    - (conf-if-po-69)#link-bundle-monitor enable
2. Add interfaces to the LAG
    - (conf)#interface Tengigabitethernet 0/0
    - (conf-if-te-0/0)#port-channel-protocol LACP
    - (conf-if-te-0/0-lacp)#port-channel 69 mode active
    - (conf-if-te-0/0-lacp)#exit
    - (conf-if-te-0/0)#no shutdown

    ... repeat for interfaces 0/1 through 0/7
3. Configure the Load Balancer egress LAG. This LAG uses LACP
    - (conf)#interface port-channel 86
    - (conf-if-po-86)#description "This port channel sends traffic from LB to all firewalls"
    - (conf-if-po-86)#switchport

- (conf-if-po-86)#no spanning-tree
- (conf-if-po-86)#lacp long-timeout
- (conf-if-po-86)#no shutdown
- (conf-if-po-86)#link-bundle-monitor enable

4. Add interfaces to the LAG
    - (conf)#interface Tengigabitethernet 0/8
    - (conf-if-te-0/0)#port-channel-protocol LACP
    - (conf-if-te-0/0-lacp)#port-channel 69 mode active
    - (conf-if-te-0/0-lacp)#exit
    - (conf-if-te-0/0)#no shutdown

    ... repeat for interfaces 0/9 through 0/15
5. Configure static LAG for each firewall node:
    - (conf)#interface port-channel 1
    - (conf-if-po-1)#description "This is ingress and egress traffic from node 1"
    - (conf-if-po-1)#switchport
    - (conf-if-po-1)#channel-member TenGigabitEthernet 0/16-17
    - (conf-if-po-1)#no shutdown

    ... repeat for other firewall nodes
6. Create VLAN 100 for forwarding load balanced traffic from LB to the firewalls
    - (conf)#interface vlan 100
    - (conf-if-vl-100)#description "LB to firewalls traffic"
    - (conf-if-vl-100)#no ip address
    - (conf-if-vl-100)#tagged Port-channel 1-8
    - (conf-if-vl-100)#untagged Port-channel 69
    - (conf-if-vl-100)#no shutdown
7. Create VLAN 200 for forwarding traffic from the firewalls to the WAN
    - (conf)#interface vlan200
    - (conf-if-vl-200)#description "Egress WAN Side Traffic"
    - (conf-if-vl-200)#no ip address
    - (conf-if-vl-200)#tagged Port-channel 1-8

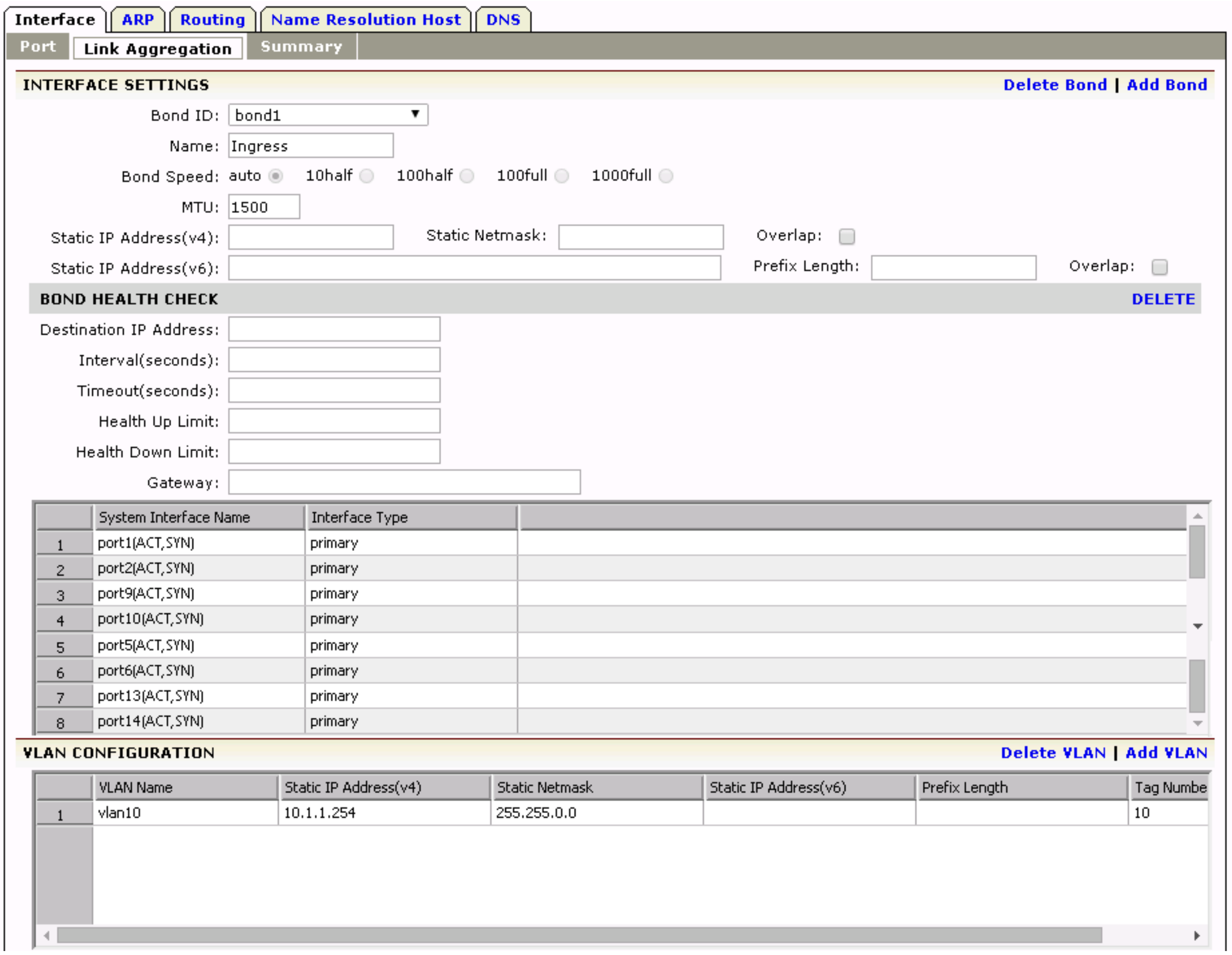
- (conf-if-vl-200)#untagged TenGigabitEthernet 0/32-39
- (conf-if-vl-200)#no shutdown

8. Connect LB ingress to port-channel 69 interfaces
9. Connect LB egress to port-channel 86 interfaces
10. Connect each firewall node to the interfaces of one of port-channel 1-8

4.3 Configuring the APV Series Load Balancer

The Load Balancer acts as the gateway for the LAN hosts.

1. Configure ingress and egress LAG
    - /System Configuration/Basic Networking/Link Aggregation
    - "Bond ID" = "bond1"
    - "Bond Name" = "Ingress"
    - "Static IP Address(v4)" = 10.1.1.254
    - Add ports 1,2,5,6,9,10,13,14



INTERFACE SETTINGS

Bond ID: bond1 ▼

Name: Ingress

Bond Speed: auto ● 10half ○ 100half ○ 100full ○ 1000full ○

MTU: 1500

Static IP Address(v4): Static Netmask: Overlap: □

Static IP Address(v6): Prefix Length: Overlap: □

BOND HEALTH CHECK

Destination IP Address:

Interval(seconds):

Timeout(seconds):

Health Up Limit:

Health Down Limit:

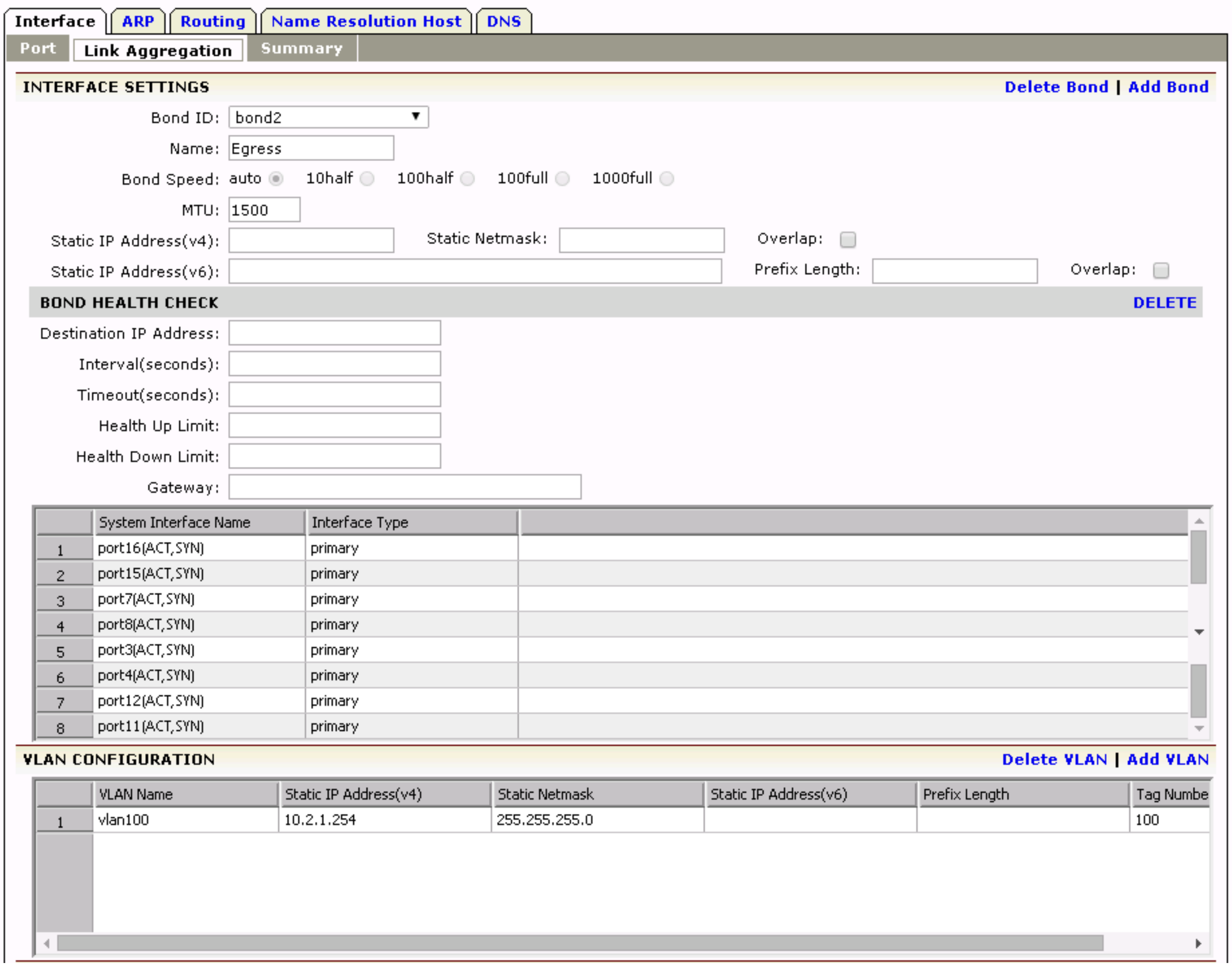
Gateway:

	System Interface Name	Interface Type	
1	port1(ACT,SYN)	primary	
2	port2(ACT,SYN)	primary	
3	port9(ACT,SYN)	primary	
4	port10(ACT,SYN)	primary	
5	port5(ACT,SYN)	primary	
6	port6(ACT,SYN)	primary	
7	port13(ACT,SYN)	primary	
8	port14(ACT,SYN)	primary	

VLAN CONFIGURATION

	VLAN Name	Static IP Address(v4)	Static Netmask	Static IP Address(v6)	Prefix Length	Tag Numbe
1	vlan10	10.1.1.254	255.255.0.0			10

- "Bond ID" = "bond2"
- "Bond Name" = "Egress"
- Add ports 3,4,7,8,11,12,15,16
- "Static IP Address(v4)" = 10.2.1.254



INTERFACE SETTINGS

Bond ID: bond2

Name: Egress

Bond Speed: auto ● 10half ○ 100half ○ 100full ○ 1000full ○

MTU: 1500

Static IP Address(v4): Static Netmask: Overlap: □

Static IP Address(v6): Prefix Length: Overlap: □

BOND HEALTH CHECK

Destination IP Address:

Interval(seconds):

Timeout(seconds):

Health Up Limit:

Health Down Limit:

Gateway:

	System Interface Name	Interface Type
1	port16(ACT,SYN)	primary
2	port15(ACT,SYN)	primary
3	port7(ACT,SYN)	primary
4	port8(ACT,SYN)	primary
5	port3(ACT,SYN)	primary
6	port4(ACT,SYN)	primary
7	port12(ACT,SYN)	primary
8	port11(ACT,SYN)	primary

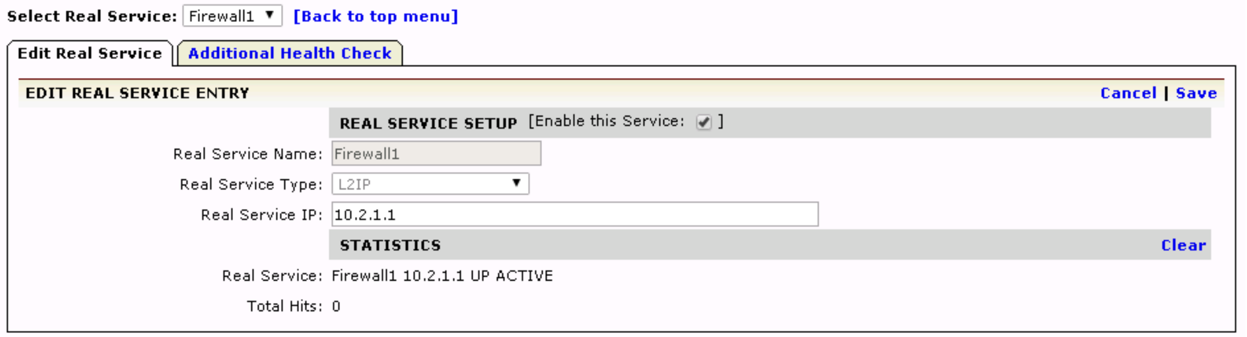
VLAN CONFIGURATION

	VLAN Name	Static IP Address(v4)	Static Netmask	Static IP Address(v6)	Prefix Length	Tag Numbe
1	vlan100	10.2.1.254	255.255.255.0			100

Note, ports are evenly distributed across two NUMA Domains for more efficient performance with symmetric load on the CPU for quicker processing .

2. Add firewall nodes to 'Real Services'

- /Server Load Balance/Real Services/Add
- "Real Service Name" = "Firewall1"
- "Real Service Type" = L2IP
- "Real Service IP = 10.2.1.1



Select Real Service: Firewall1 [Back to top menu]

EDIT REAL SERVICE ENTRY — Cancel | Save

REAL SERVICE SETUP [Enable this Service: ☑]

Real Service Name: Firewall1

Real Service Type: L2IP

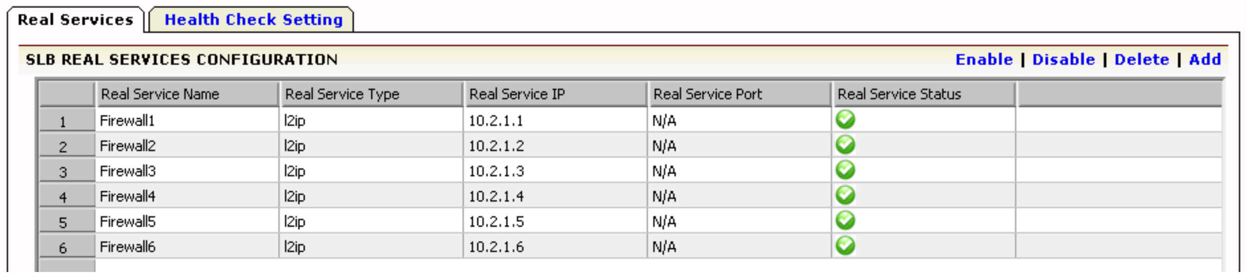
Real Service IP: 10.2.1.1

STATISTICS — Clear

Real Service: Firewall1 10.2.1.1 UP ACTIVE

Total Hits: 0

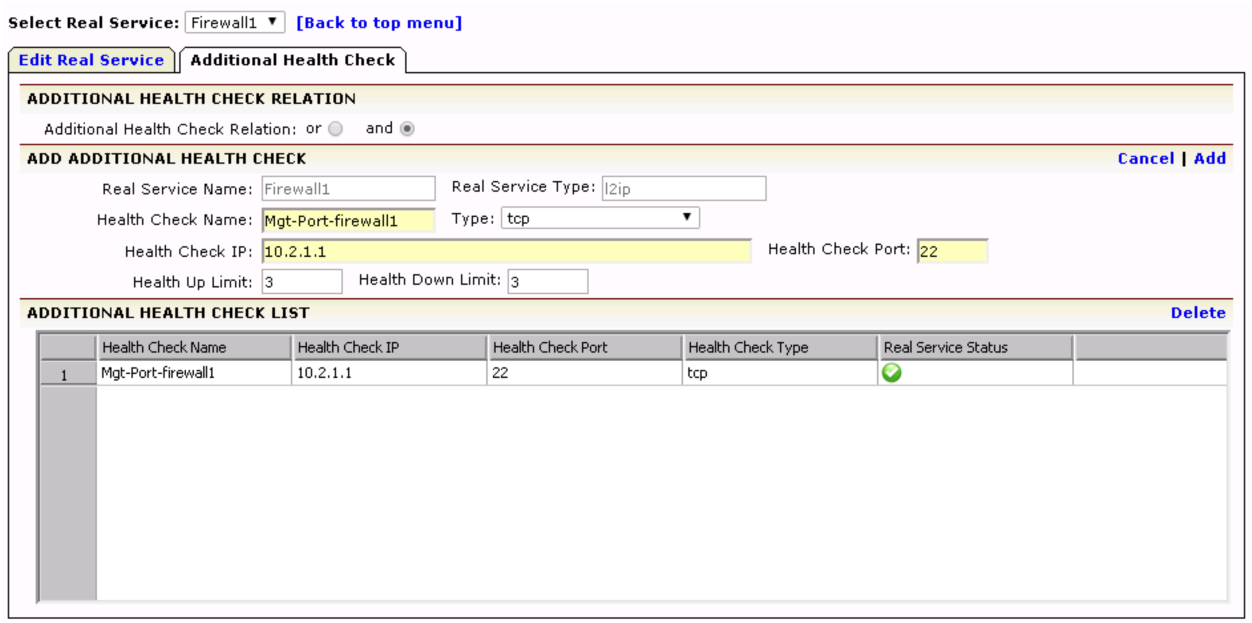
- Repeat for other nodes. The SLB Real Services Configuration screen will show all nodes.



SLB REAL SERVICES CONFIGURATION — Enable | Disable | Delete | Add

	Real Service Name	Real Service Type	Real Service IP	Real Service Port	Real Service Status
1	Firewall1	l2ip	10.2.1.1	N/A	✓
2	Firewall2	l2ip	10.2.1.2	N/A	✓
3	Firewall3	l2ip	10.2.1.3	N/A	✓
4	Firewall4	l2ip	10.2.1.4	N/A	✓
5	Firewall5	l2ip	10.2.1.5	N/A	✓
6	Firewall6	l2ip	10.2.1.6	N/A	✓

3. Enable Health Check for each firewall node in Real Services.



Select Real Service: Firewall1 [Back to top menu]

ADDITIONAL HEALTH CHECK RELATION

Additional Health Check Relation: or ○ and ●

ADD ADDITIONAL HEALTH CHECK — Cancel | Add

Real Service Name: Firewall1 Real Service Type: l2ip

Health Check Name: Mgt-Port-firewall1 Type: tcp

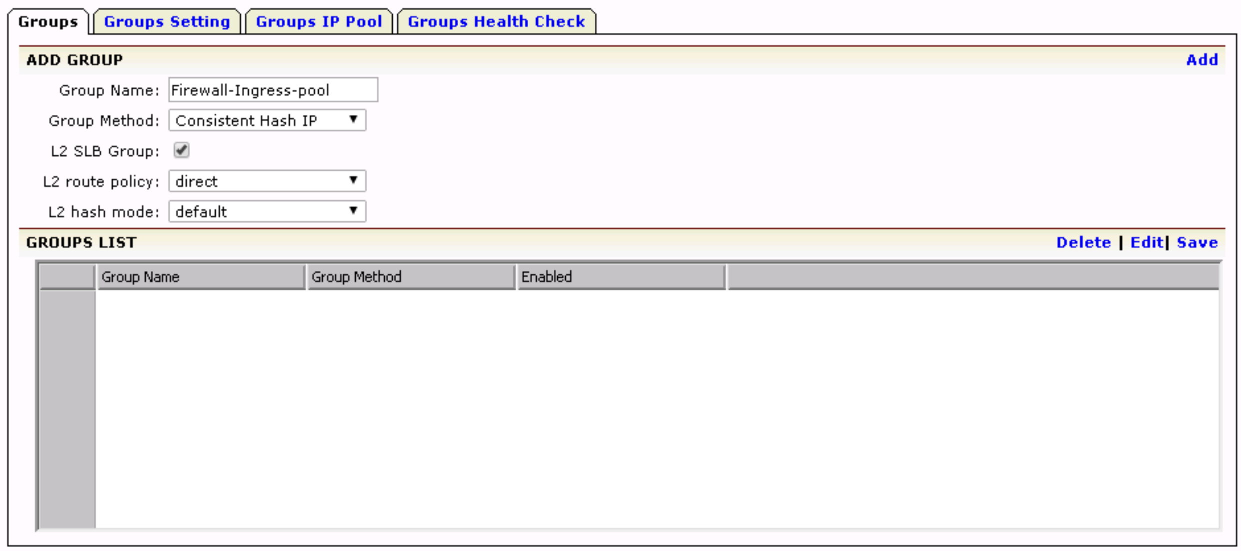
Health Check IP: 10.2.1.1 Health Check Port: 22

Health Up Limit: 3 Health Down Limit: 3

ADDITIONAL HEALTH CHECK LIST — Delete

	Health Check Name	Health Check IP	Health Check Port	Health Check Type	Real Service Status
1	Mgt-Port-firewall1	10.2.1.1	22	tcp	✓

4. Combine 'Real Services' into a group
   - /Server Load Balance/Groups
   - "Group Name" = "Firewall Ingress-pool"
   - "Group Method" = "Consistent Hash IP"
   - "L2 SLB Group" = ON
   - "L2 Route Policy" = "direct"
   - "L2 Hash Mode" = "default" (hashes both source and destination IP)



ADD GROUP

Group Name: Firewall-Ingress-pool

Group Method: Consistent Hash IP

L2 SLB Group: ☑

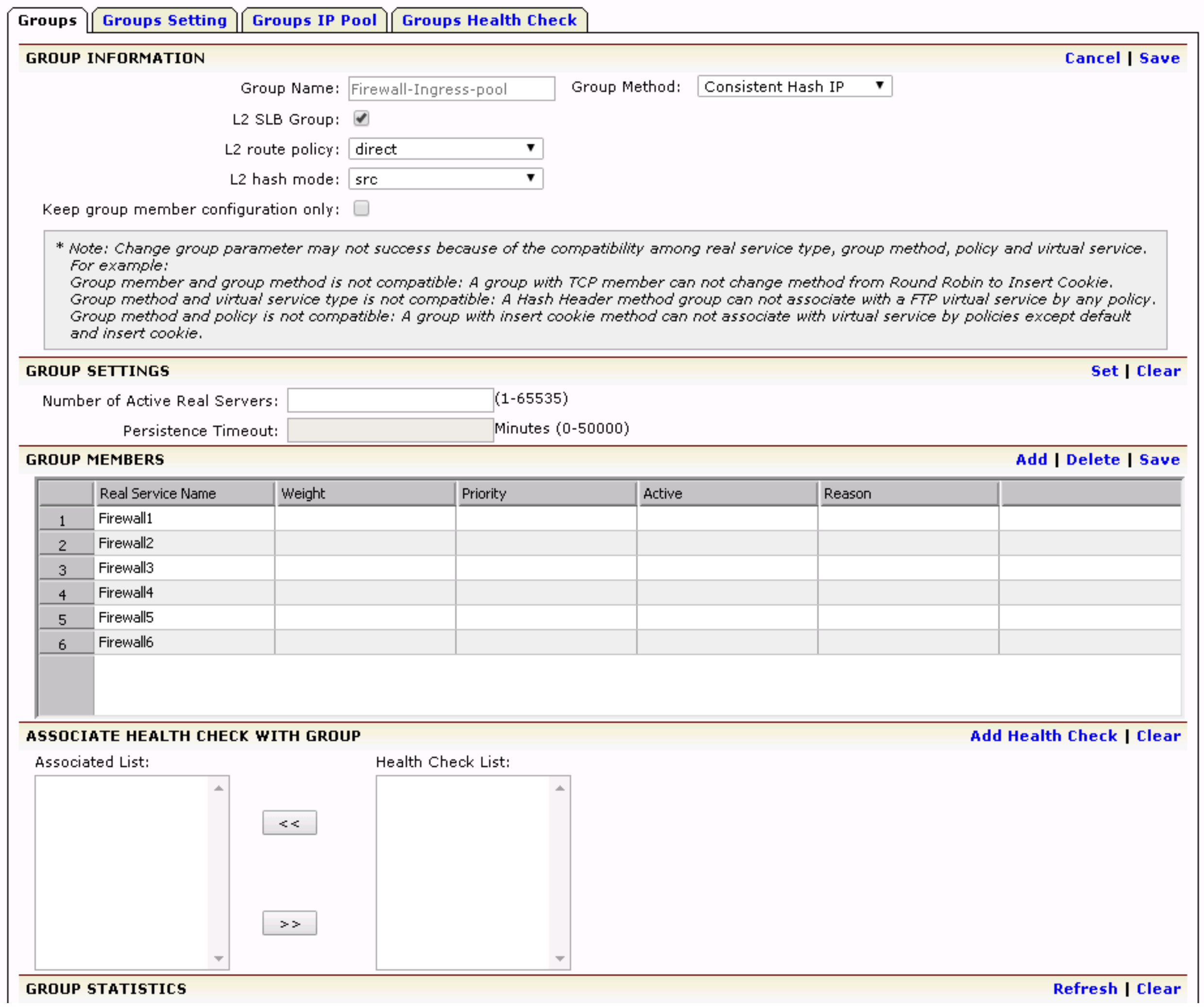
L2 route policy: direct

L2 hash mode: default

GROUPS LIST

Group Name	Group Method	Enabled

5. Add the remainder of the "Real Services" created at the previous step to the group. The Group Information screen will display them all.



GROUP INFORMATION

Group Name: Firewall-Ingress-pool Group Method: Consistent Hash IP

L2 SLB Group: ☑

L2 route policy: direct

L2 hash mode: src

Keep group member configuration only: □

* Note: Change group parameter may not success because of the compatibility among real service type, group method, policy and virtual service.
For example:
Group member and group method is not compatible: A group with TCP member can not change method from Round Robin to Insert Cookie.
Group method and virtual service type is not compatible: A Hash Header method group can not associate with a FTP virtual service by any policy.
Group method and policy is not compatible: A group with insert cookie method can not associate with virtual service by policies except default and insert cookie.

GROUP SETTINGS

Number of Active Real Servers: (1-65535)

Persistence Timeout: Minutes (0-50000)

GROUP MEMBERS

	Real Service Name	Weight	Priority	Active	Reason
1	Firewall1				
2	Firewall2				
3	Firewall3				
4	Firewall4				
5	Firewall5				
6	Firewall6				

ASSOCIATE HEALTH CHECK WITH GROUP

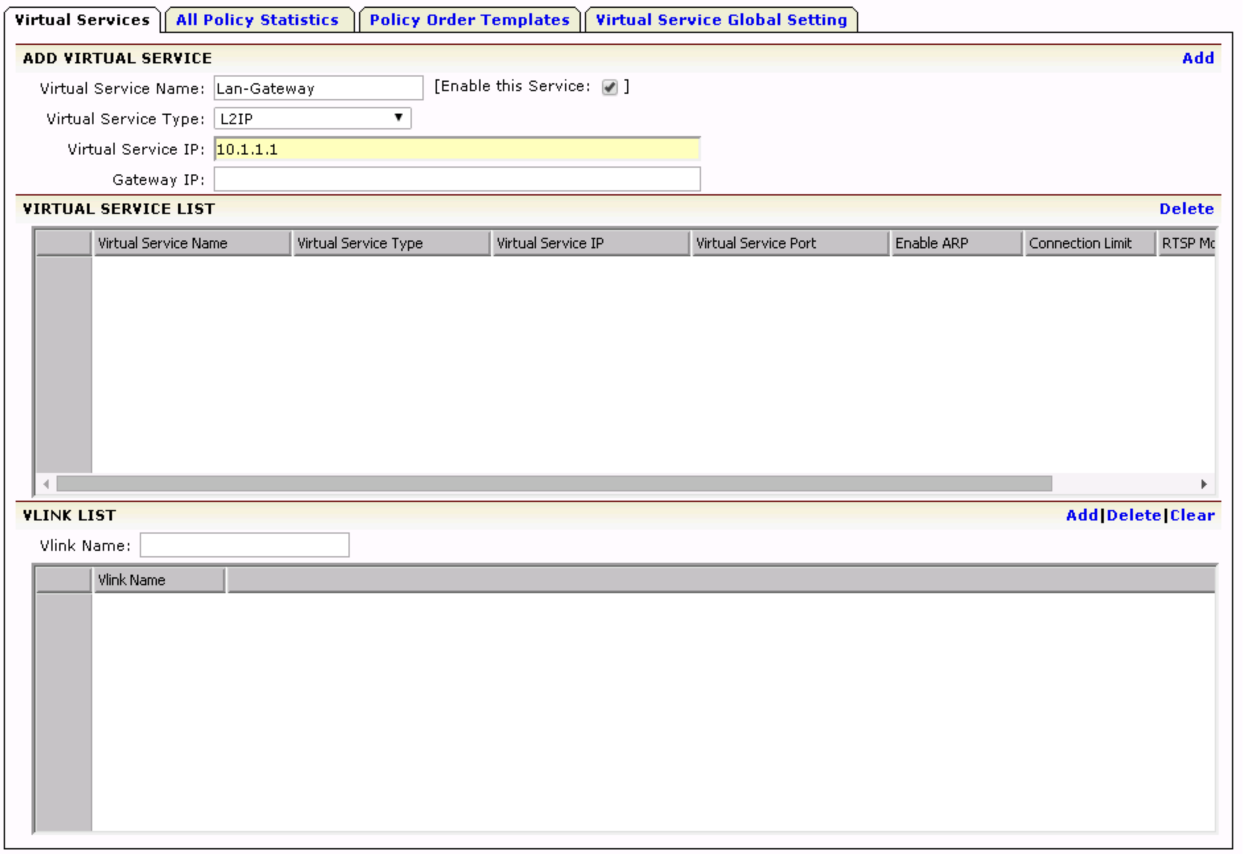
Associated List:

Health Check List:

GROUP STATISTICS

6. Add Virtual Service – that's the gateway for the LAN/Server Load Balance/Virtual Services

- "Virtual Service Name" = "LAN Gateway"
- "Virtual Service Type" = L2IP
- "Virtual Service IP" = 10.1.1.1



ADD VIRTUAL SERVICE

Virtual Service Name: Lan-Gateway [Enable this Service: ☑]

Virtual Service Type: L2IP

Virtual Service IP: 10.1.1.1

Gateway IP:

VIRTUAL SERVICE LIST

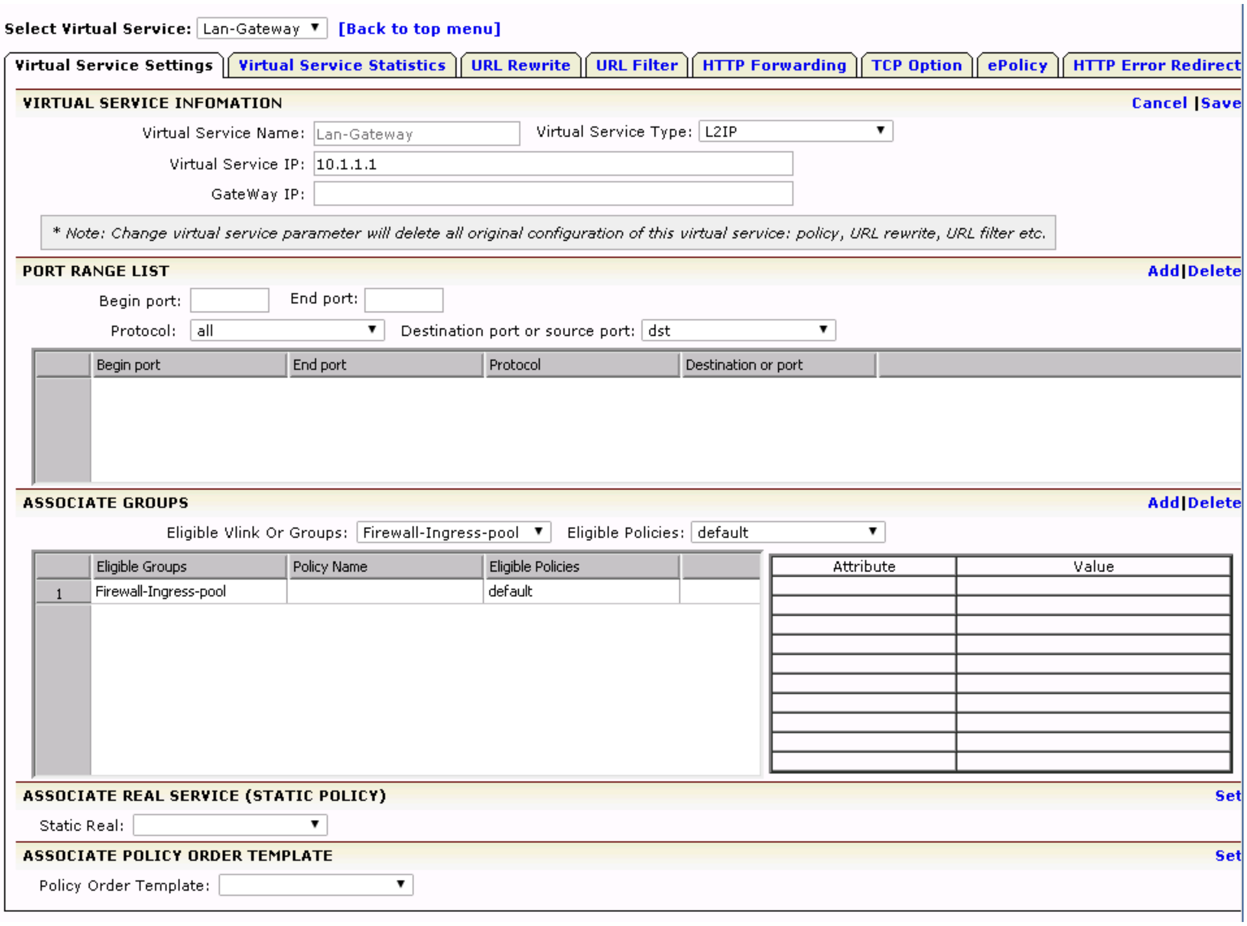
	Virtual Service Name	Virtual Service Type	Virtual Service IP	Virtual Service Port	Enable ARP	Connection Limit	RTSP Mc

VLINK LIST

Vlink Name:

	Vlink Name

- "Associate Group" - add "Firewall Group"



Select Virtual Service: Lan-Gateway

VIRTUAL SERVICE INFOMATION

Virtual Service Name: Lan-Gateway

Virtual Service Type: L2IP

Virtual Service IP: 10.1.1.1

GateWay IP:

Note: Change virtual service parameter will delete all original configuration of this virtual service: policy, URL rewrite, URL filter etc.

PORT RANGE LIST

Begin port:

End port:

Protocol: all

Destination port or source port: dst

	Begin port	End port	Protocol	Destination or port	

ASSOCIATE GROUPS

Eligible Vlink Or Groups: Firewall-Ingress-pool

Eligible Policies: default

	Eligible Groups	Policy Name	Eligible Policies	
1	Firewall-Ingress-pool		default	

Attribute	Value

ASSOCIATE REAL SERVICE (STATIC POLICY)

Static Real:

ASSOCIATE POLICY ORDER TEMPLATE

Policy Order Template:

5 Fully Redundant Configuration

The diagram below describes a fully redundant configuration – two load balancers and two switches cross-linked.

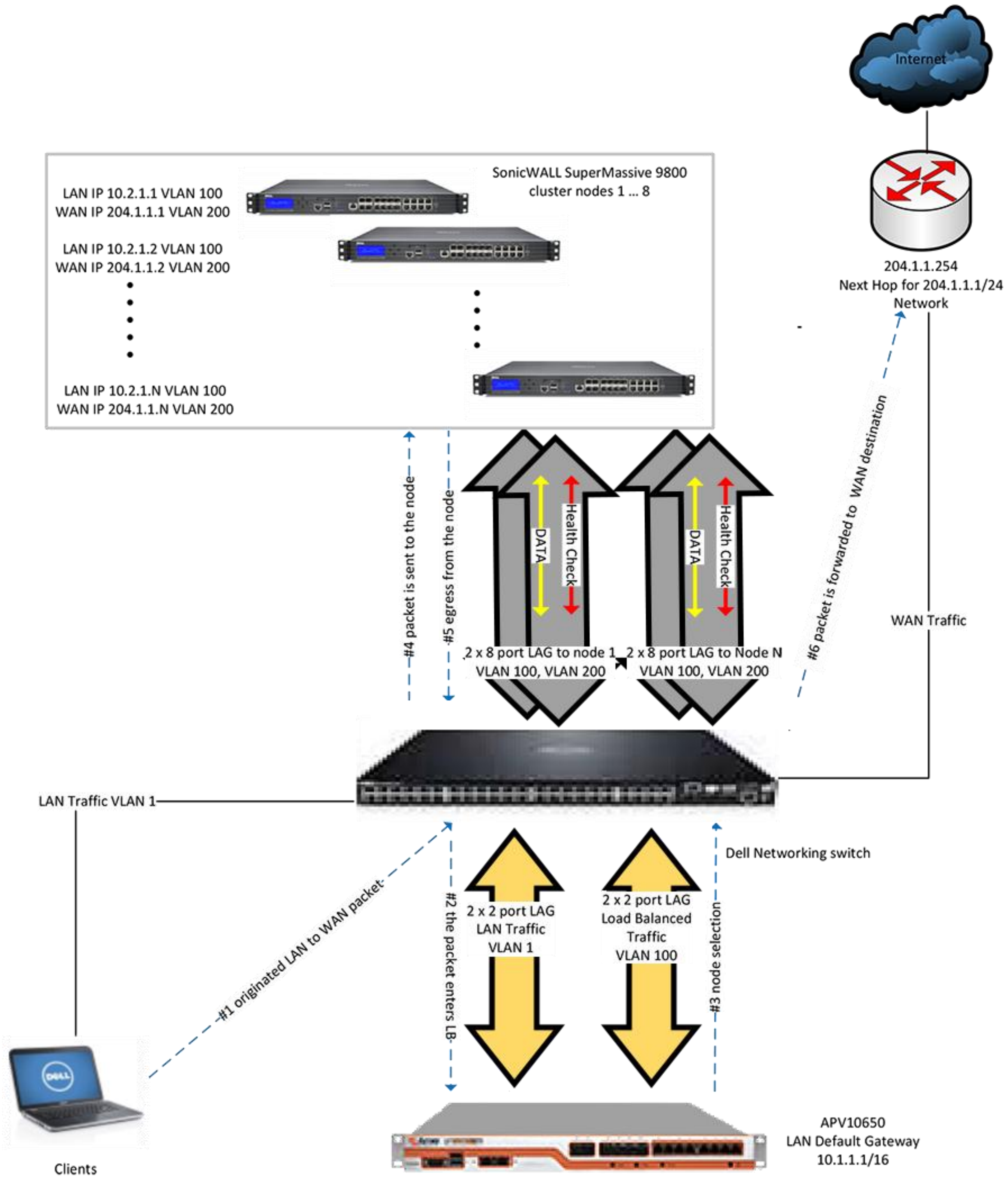


Figure 2: HA Configuration

6 Support for Multiple LANs

Multiple LAN support is illustrated on Fig. 3. Note that the WAN connection has been removed for clarity. What are the main differences?

- Multiple Virtual Services are configured on the APV Series load balancer – one for each LAN
- Multiple forwarding networks are configured between the APV Series load balancer and the nodes – one for each LAN
- Multiple VLANs are added to the LAGs – one for each LAN

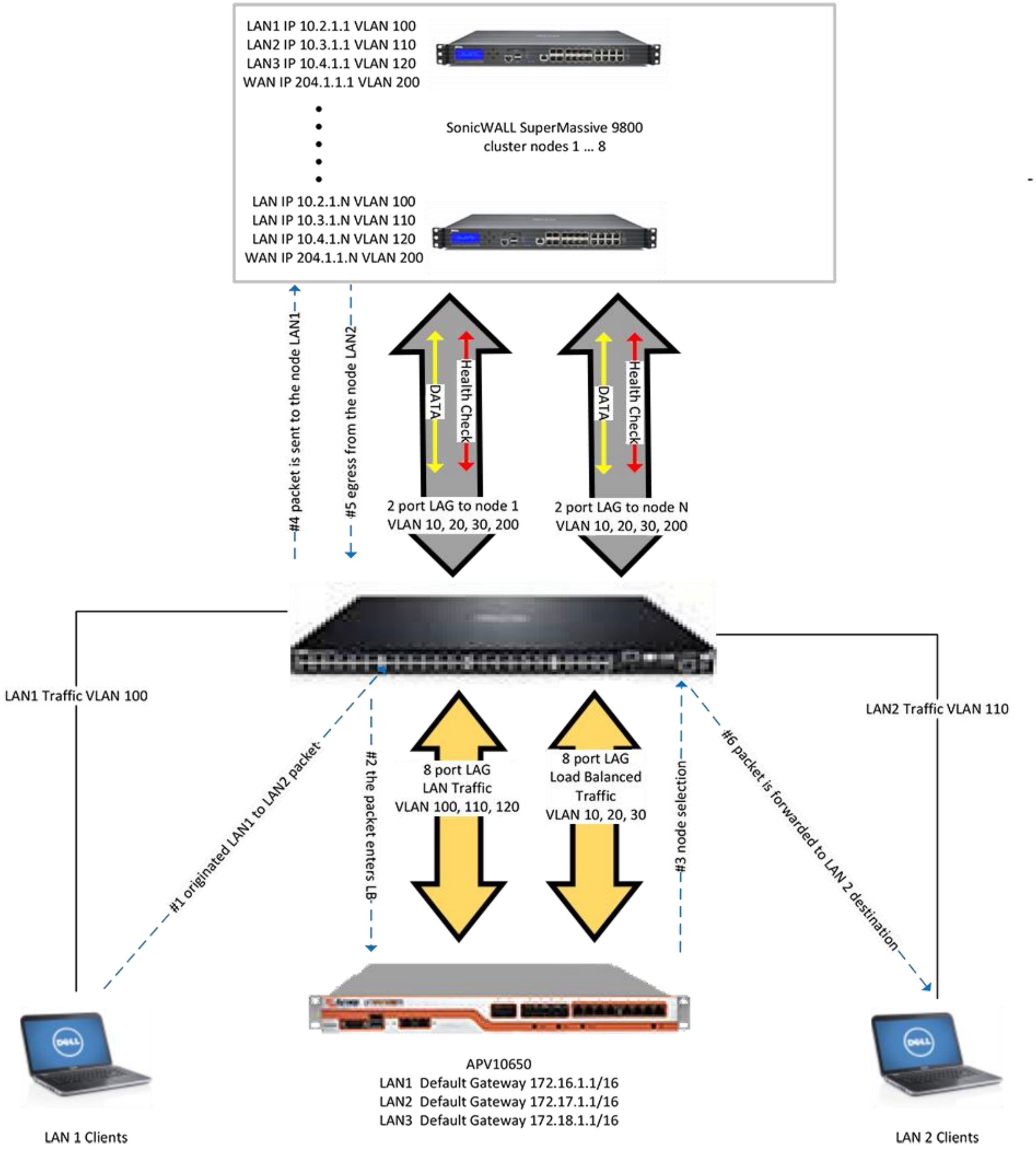


Figure 3: Support for Multiple LANs

6.1 Regular LAN1 to LAN2 Traffic, e.g. HTTP

- A packet is originated by a host on the LAN1 and is sent to the gateway, which is the IP address of the ingress APV Series load balancer.
- The APV Series ingress load balancer receives the packet and selects the path through one of the nodes. ‘Consistent Hash’ of source and destination IP is used as a load balancing algorithm. That ensures that all outbound packets from the same flow are routed through the same node.
- The packet is received by the selected node. The node performs all configured security functions – applies access rules, DPI, etc.
- The packet is sent to back to the load balancer because it is the next hop for LAN2
- The load balancer forwards the packet to the destination on LAN2
- A response packet is sent.
- The response packet is sent to the load balancer because it is the next hop for LAN1
- The load balancer selects the path through one of the nodes by using consistent hash of source and destination IP. Since HASH(source IP, destination IP) is the same as HASH(destination IP, source IP), the load balancer selects the same node as for LAN1-to-LAN2 packet.
- The response packet is forwarded to the node, back to the load balancer (next hop for LAN1) and finally to the destination on LAN1

6.2 Active FTP

Active FTP data connections are established between the same two IP addresses as the control connection; because HASH(source IP, destination IP) is the same as HASH(destination IP, source IP) the data connection is handled by the same node as control connection.

6.3 Passive FTP

The passive FTP connection is established between the same pair of IP addresses as the control connection. Consistent Hash for Source+Destination IP will select the same node. Thus the control and data connection will go through the same node.

6.4 SIP

6.4.1 SIP Server on the WAN

If the SIP Server is located on the WAN, calls between two clients on two different LANs works the same way as described in section 3.4, i.e. the caller connects to the NAT’ed address of the peer.

6.4.2 SIP Server on one of the LANs

This configuration might present challenges. An incoming call from a LAN client will not always be routed through the same node because: HASH(client 1 IP, SIP server IP) is not the same as HASH(client 2 IP, client 1 IP). Depending on the firewall rules between

LAN1 and LAN2 the connection may or may not go though and may not be classified as a SIP call.

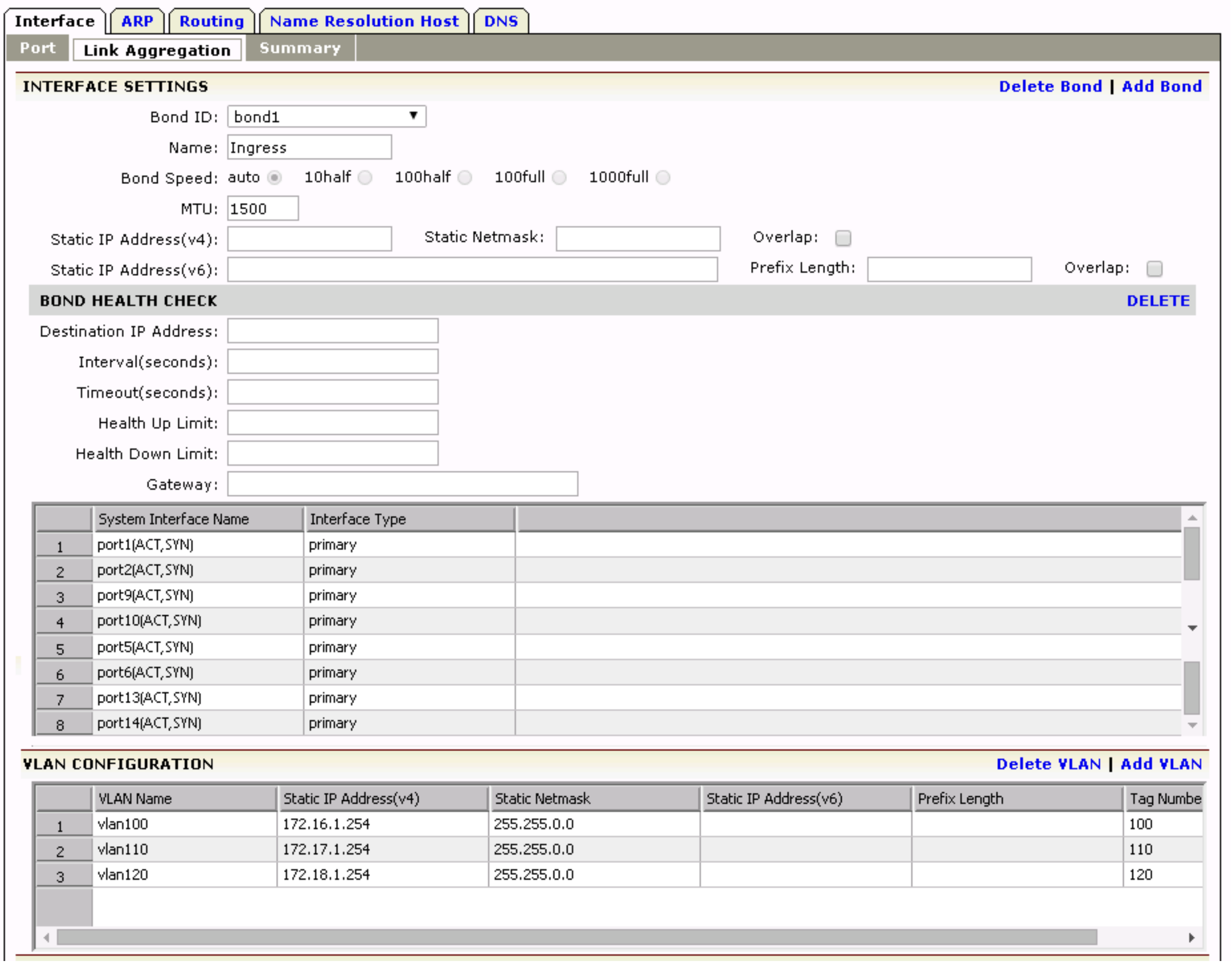
6.5 Additional Configuration Steps for Multi-LAN support

Multi-LAN support requires additional “Virtual Services” and additional “Real Services” on the APV Series load balancer, one for each additional LAN.

- Add LAN interfaces to each node but create VLAN subinterfaces – VLAN 100, VLAN110, VLAN120

Configure ingress and egress LAG:

- /System Configuration/Basic Networking/Link Aggregation
- "Bond ID" = "bond1"
- "Bond Name" = "Ingress"
- Add VLAN specific ips
- Add ports 1,2,5,6,9,10,13,14



INTERFACE SETTINGS

Bond ID: bond1

Name: Ingress

Bond Speed: auto ● 10half ○ 100half ○ 100full ○ 1000full ○

MTU: 1500

Static IP Address(v4): Static Netmask: Overlap: □

Static IP Address(v6): Prefix Length: Overlap: □

BOND HEALTH CHECK

Destination IP Address:

Interval(seconds):

Timeout(seconds):

Health Up Limit:

Health Down Limit:

Gateway:

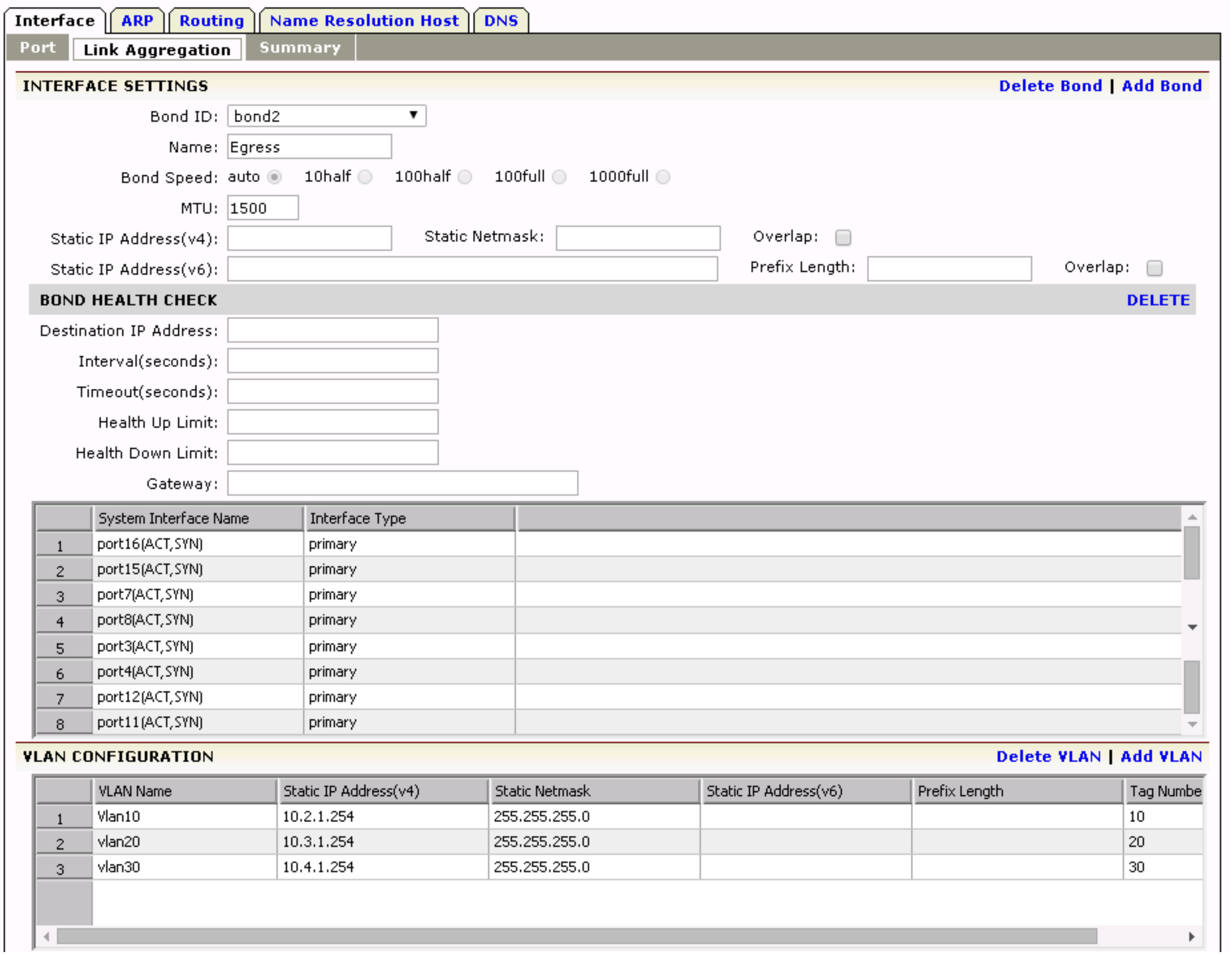
	System Interface Name	Interface Type
1	port1(ACT,SYN)	primary
2	port2(ACT,SYN)	primary
3	port9(ACT,SYN)	primary
4	port10(ACT,SYN)	primary
5	port5(ACT,SYN)	primary
6	port6(ACT,SYN)	primary
7	port13(ACT,SYN)	primary
8	port14(ACT,SYN)	primary

VLAN CONFIGURATION

	VLAN Name	Static IP Address(v4)	Static Netmask	Static IP Address(v6)	Prefix Length	Tag Numbe
1	vlan100	172.16.1.254	255.255.0.0			100
2	vlan110	172.17.1.254	255.255.0.0			110
3	vlan120	172.18.1.254	255.255.0.0			120

- Assign IP addresses to each new VLAN subinterface –VLAN 10, VLAN 20, VLAN 30
- "Bond ID" = "bond2"

- "Bond Name" = "Egress"
- Add ports 3,4,7,8,11,12,15,16
- " Add VLAN specific ips



INTERFACE SETTINGS

Bond ID: bond2 ▼

Name: Egress

Bond Speed: auto ● 10half ○ 100half ○ 100full ○ 1000full ○

MTU: 1500

Static IP Address(v4): Static Netmask: Overlap: □

Static IP Address(v6): Prefix Length: Overlap: □

BOND HEALTH CHECK

Destination IP Address:

Interval(seconds):

Timeout(seconds):

Health Up Limit:

Health Down Limit:

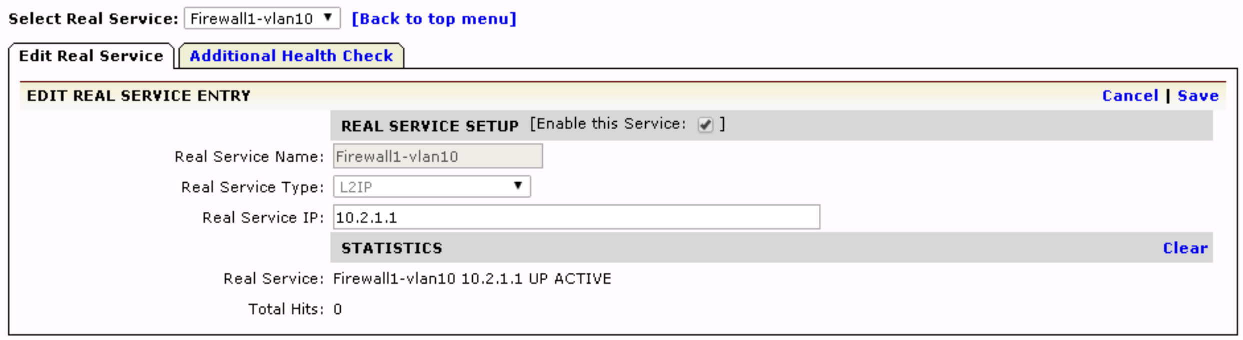
Gateway:

	System Interface Name	Interface Type
1	port16(ACT,SYN)	primary
2	port15(ACT,SYN)	primary
3	port7(ACT,SYN)	primary
4	port8(ACT,SYN)	primary
5	port3(ACT,SYN)	primary
6	port4(ACT,SYN)	primary
7	port12(ACT,SYN)	primary
8	port11(ACT,SYN)	primary

VLAN CONFIGURATION

	VLAN Name	Static IP Address(v4)	Static Netmask	Static IP Address(v6)	Prefix Length	Tag Numbe
1	Vlan10	10.2.1.254	255.255.255.0			10
2	vlan20	10.3.1.254	255.255.255.0			20
3	vlan30	10.4.1.254	255.255.255.0			30

- Create new ‘Real Services’ on the load balancer, one for each new VLAN network on the firewall side of load balancer



Select Real Service: Firewall1-vlan10 ▼

EDIT REAL SERVICE ENTRY

REAL SERVICE SETUP [Enable this Service: ☑]

Real Service Name: Firewall1-vlan10

Real Service Type: L2IP ▼

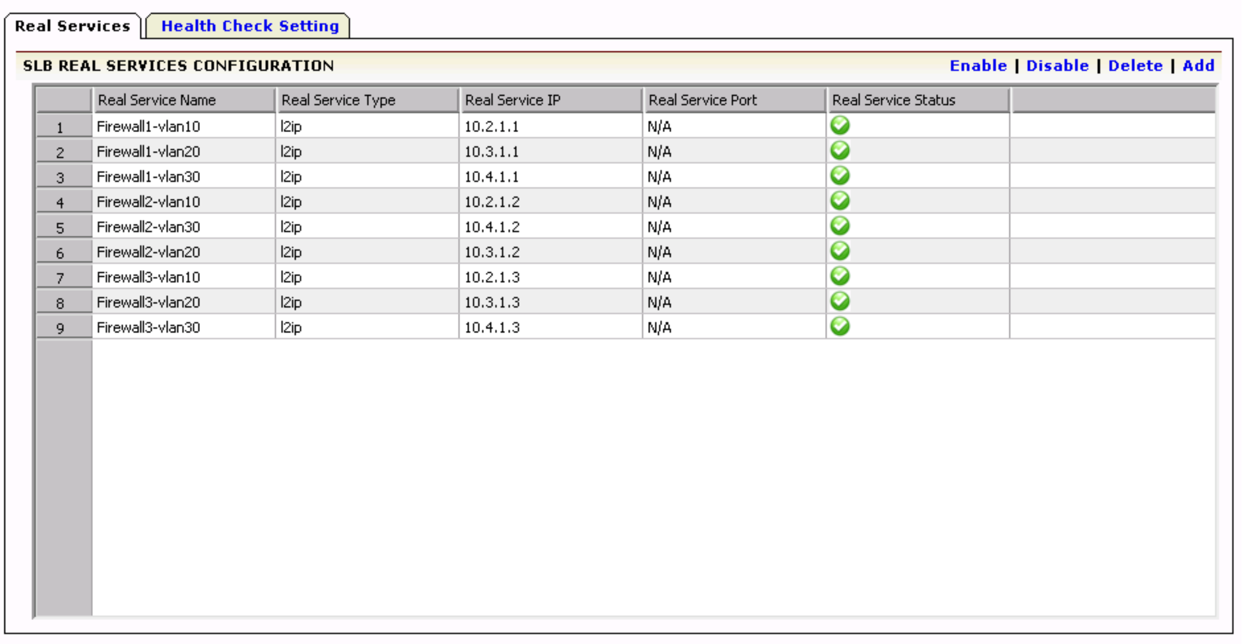
Real Service IP: 10.2.1.1

STATISTICS

Real Service: Firewall1-vlan10 10.2.1.1 UP ACTIVE

Total Hits: 0

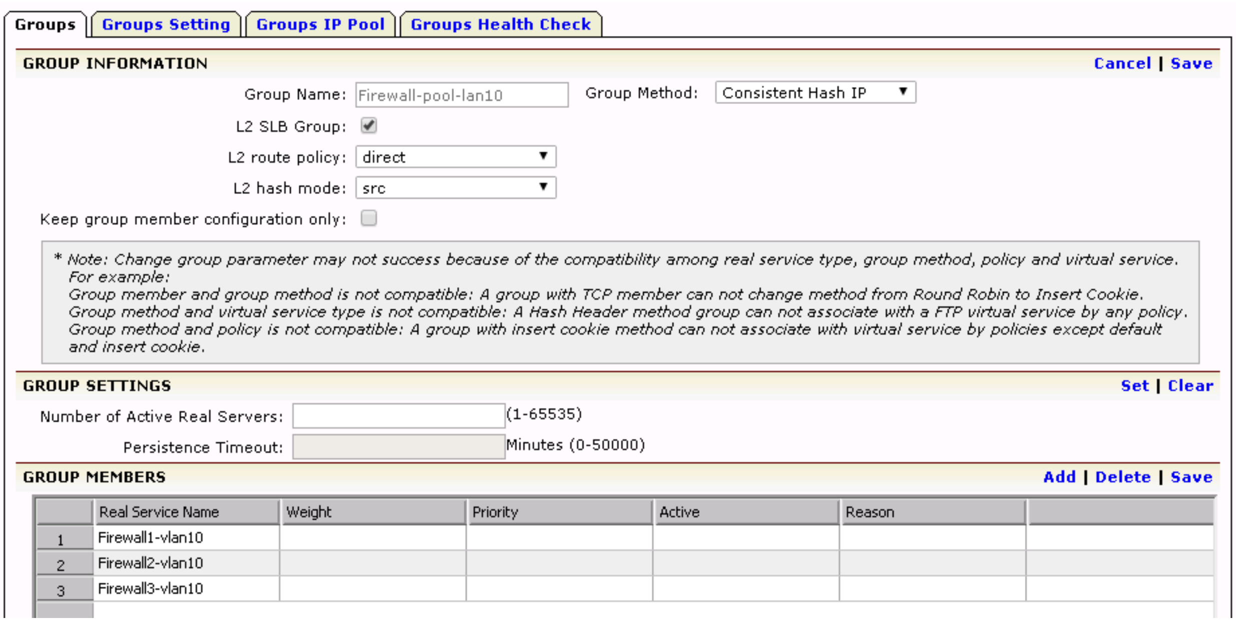
- The Real Services screen will display them all



SLB REAL SERVICES CONFIGURATION

	Real Service Name	Real Service Type	Real Service IP	Real Service Port	Real Service Status	
1	Firewall1-vlan10	l2ip	10.2.1.1	N/A	✓	
2	Firewall1-vlan20	l2ip	10.3.1.1	N/A	✓	
3	Firewall1-vlan30	l2ip	10.4.1.1	N/A	✓	
4	Firewall2-vlan10	l2ip	10.2.1.2	N/A	✓	
5	Firewall2-vlan30	l2ip	10.4.1.2	N/A	✓	
6	Firewall2-vlan20	l2ip	10.3.1.2	N/A	✓	
7	Firewall3-vlan10	l2ip	10.2.1.3	N/A	✓	
8	Firewall3-vlan20	l2ip	10.3.1.3	N/A	✓	
9	Firewall3-vlan30	l2ip	10.4.1.3	N/A	✓	

- For each new LAN, create a new group on the load balancer and add corresponding ‘Real Services’ to the group



GROUP INFORMATION

Group Name: Firewall-pool-lan10

Group Method: Consistent Hash IP

L2 SLB Group: ☑

L2 route policy: direct

L2 hash mode: src

Keep group member configuration only: □

** Note: Change group parameter may not success because of the compatibility among real service type, group method, policy and virtual service.*
For example:
Group member and group method is not compatible: A group with TCP member can not change method from Round Robin to Insert Cookie.
Group method and virtual service type is not compatible: A Hash Header method group can not associate with a FTP virtual service by any policy.
Group method and policy is not compatible: A group with insert cookie method can not associate with virtual service by policies except default and insert cookie.

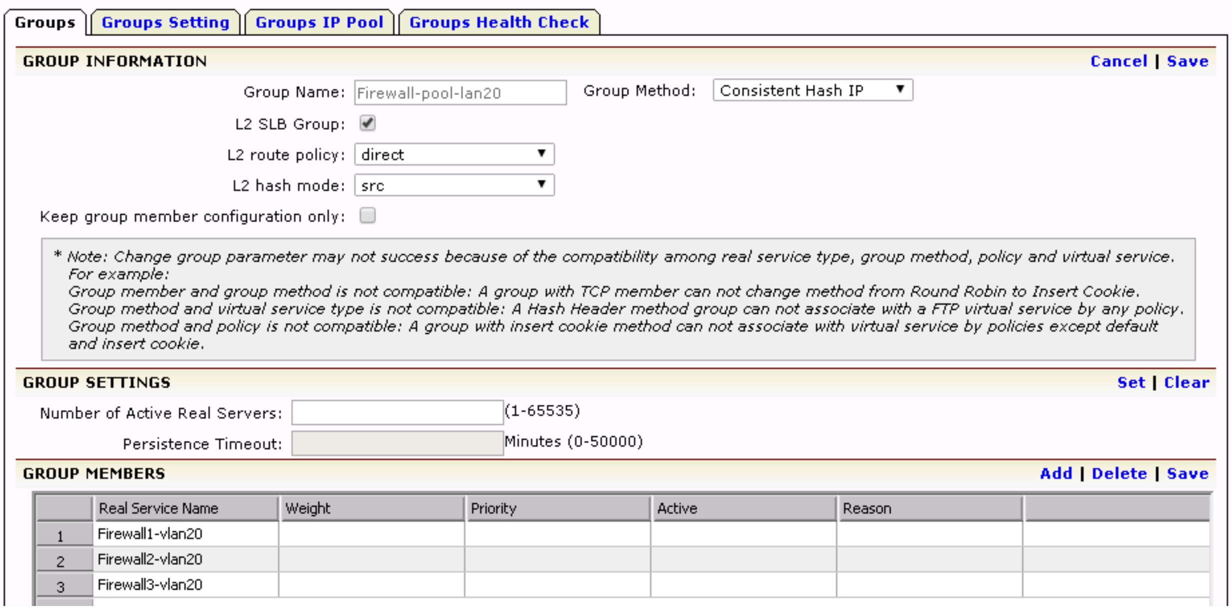
GROUP SETTINGS

Number of Active Real Servers: (1-65535)

Persistence Timeout: Minutes (0-50000)

GROUP MEMBERS

	Real Service Name	Weight	Priority	Active	Reason	
1	Firewall1-vlan10					
2	Firewall2-vlan10					
3	Firewall3-vlan10					



GROUP INFORMATION

Group Name: Firewall-pool-lan20

Group Method: Consistent Hash IP

L2 SLB Group: ☑

L2 route policy: direct

L2 hash mode: src

Keep group member configuration only: □

* Note: Change group parameter may not success because of the compatibility among real service type, group method, policy and virtual service.
For example:
Group member and group method is not compatible: A group with TCP member can not change method from Round Robin to Insert Cookie.
Group method and virtual service type is not compatible: A Hash Header method group can not associate with a FTP virtual service by any policy.
Group method and policy is not compatible: A group with insert cookie method can not associate with virtual service by policies except default and insert cookie.

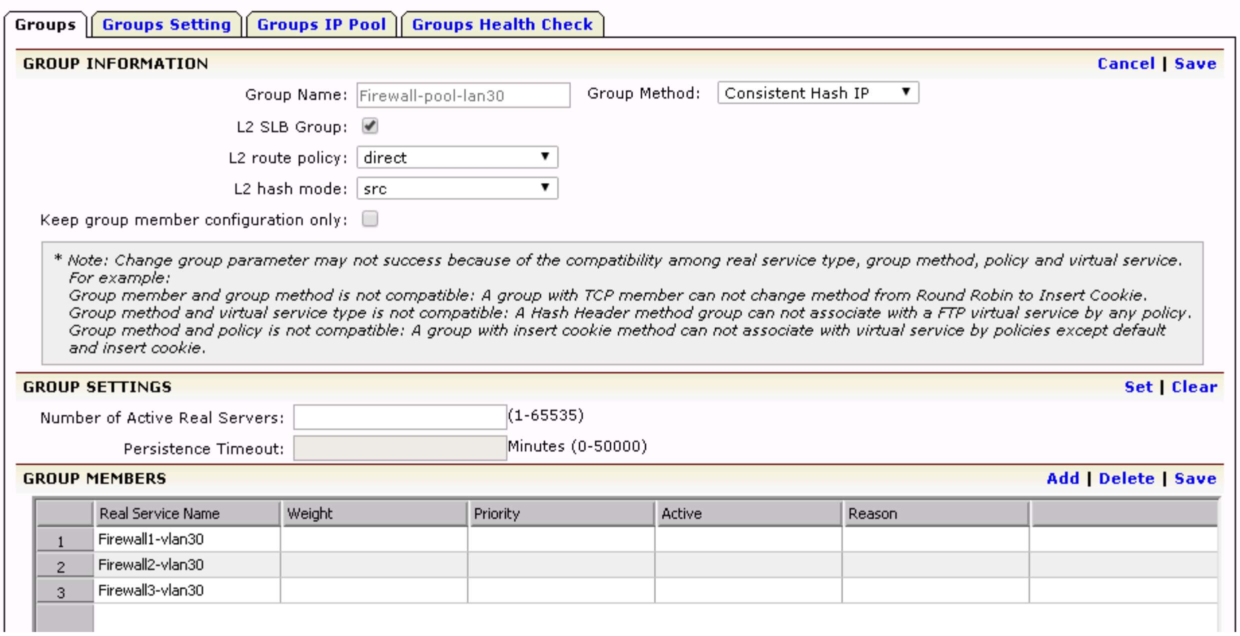
GROUP SETTINGS

Number of Active Real Servers: (1-65535)

Persistence Timeout: Minutes (0-50000)

GROUP MEMBERS

	Real Service Name	Weight	Priority	Active	Reason	
1	Firewall1-vlan20					
2	Firewall2-vlan20					
3	Firewall3-vlan20					



GROUP INFORMATION

Group Name: Firewall-pool-lan30

Group Method: Consistent Hash IP

L2 SLB Group: ☑

L2 route policy: direct

L2 hash mode: src

Keep group member configuration only: □

* Note: Change group parameter may not success because of the compatibility among real service type, group method, policy and virtual service.
For example:
Group member and group method is not compatible: A group with TCP member can not change method from Round Robin to Insert Cookie.
Group method and virtual service type is not compatible: A Hash Header method group can not associate with a FTP virtual service by any policy.
Group method and policy is not compatible: A group with insert cookie method can not associate with virtual service by policies except default and insert cookie.

GROUP SETTINGS

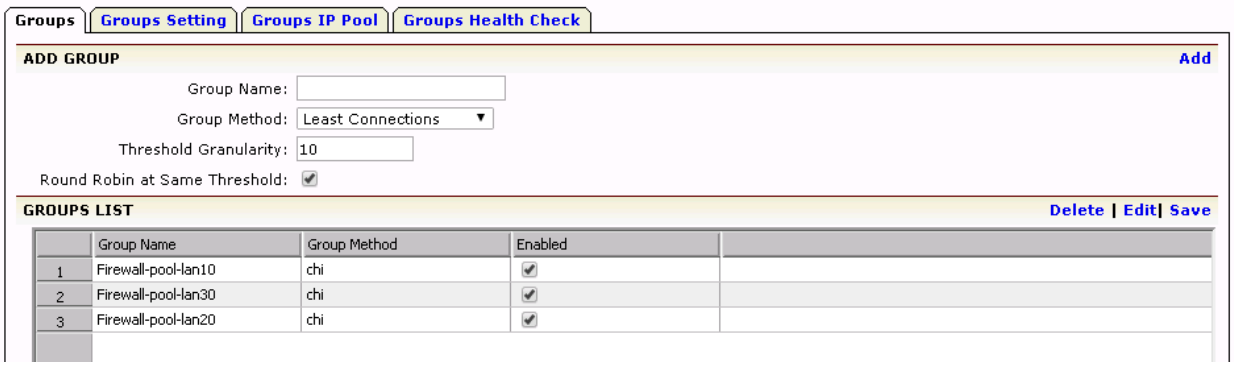
Number of Active Real Servers: (1-65535)

Persistence Timeout: Minutes (0-50000)

GROUP MEMBERS

	Real Service Name	Weight	Priority	Active	Reason	
1	Firewall1-vlan30					
2	Firewall2-vlan30					
3	Firewall3-vlan30					

- The Groups tab will display all groups created



ADD GROUP

Group Name:

Group Method: Least Connections

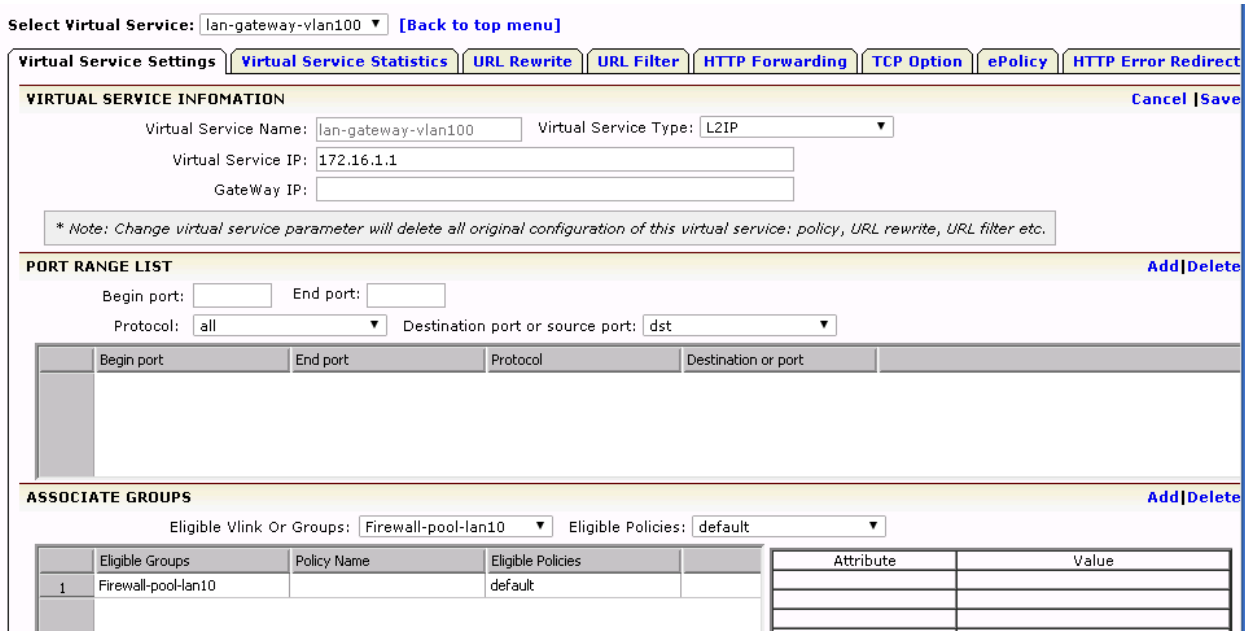
Threshold Granularity: 10

Round Robin at Same Threshold: ☑

GROUPS LIST

	Group Name	Group Method	Enabled	
1	Firewall-pool-lan10	chi	☑	
2	Firewall-pool-lan30	chi	☑	
3	Firewall-pool-lan20	chi	☑	

For each new LAN create a new ‘Virtual Service’



Select Virtual Service: lan-gateway-vlan100

VIRTUAL SERVICE INFOMATION

Virtual Service Name: lan-gateway-vlan100 Virtual Service Type: L2IP

Virtual Service IP: 172.16.1.1

GateWay IP:

* *Note: Change virtual service parameter will delete all original configuration of this virtual service: policy, URL rewrite, URL filter etc.*

PORT RANGE LIST

Begin port: End port:

Protocol: all Destination port or source port: dst

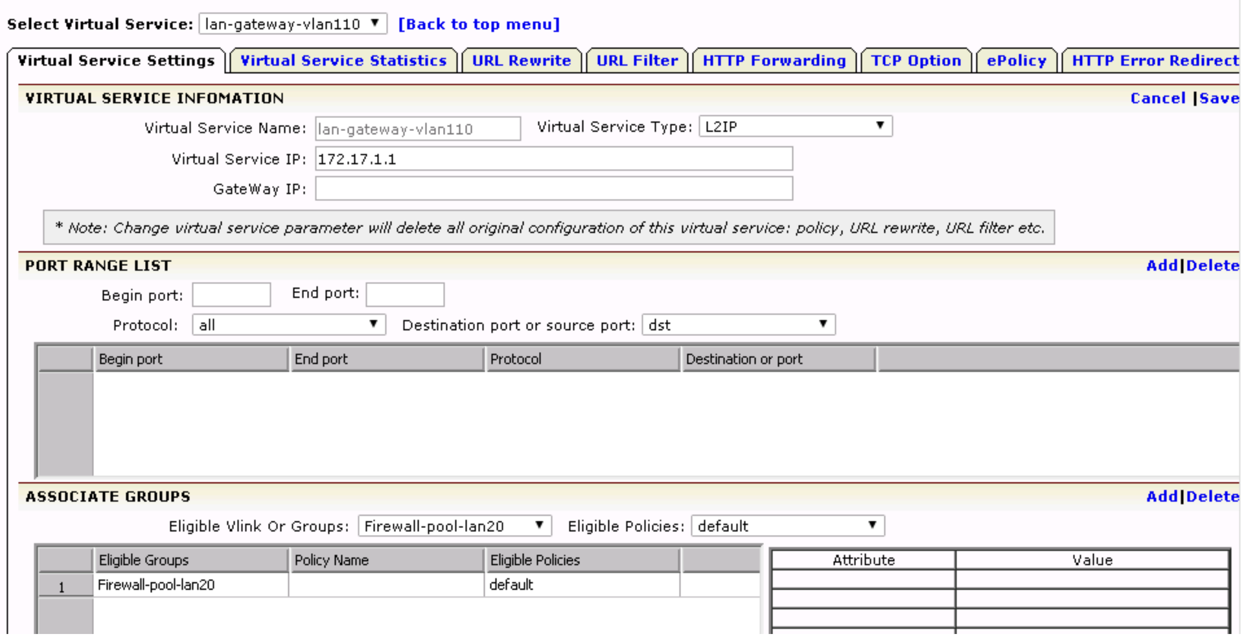
	Begin port	End port	Protocol	Destination or port	

ASSOCIATE GROUPS

Eligible Vlink Or Groups: Firewall-pool-lan10 Eligible Policies: default

	Eligible Groups	Policy Name	Eligible Policies	
1	Firewall-pool-lan10		default	

Attribute	Value



Select Virtual Service: lan-gateway-vlan110

VIRTUAL SERVICE INFOMATION

Virtual Service Name: lan-gateway-vlan110 Virtual Service Type: L2IP

Virtual Service IP: 172.17.1.1

GateWay IP:

* *Note: Change virtual service parameter will delete all original configuration of this virtual service: policy, URL rewrite, URL filter etc.*

PORT RANGE LIST

Begin port: End port:

Protocol: all Destination port or source port: dst

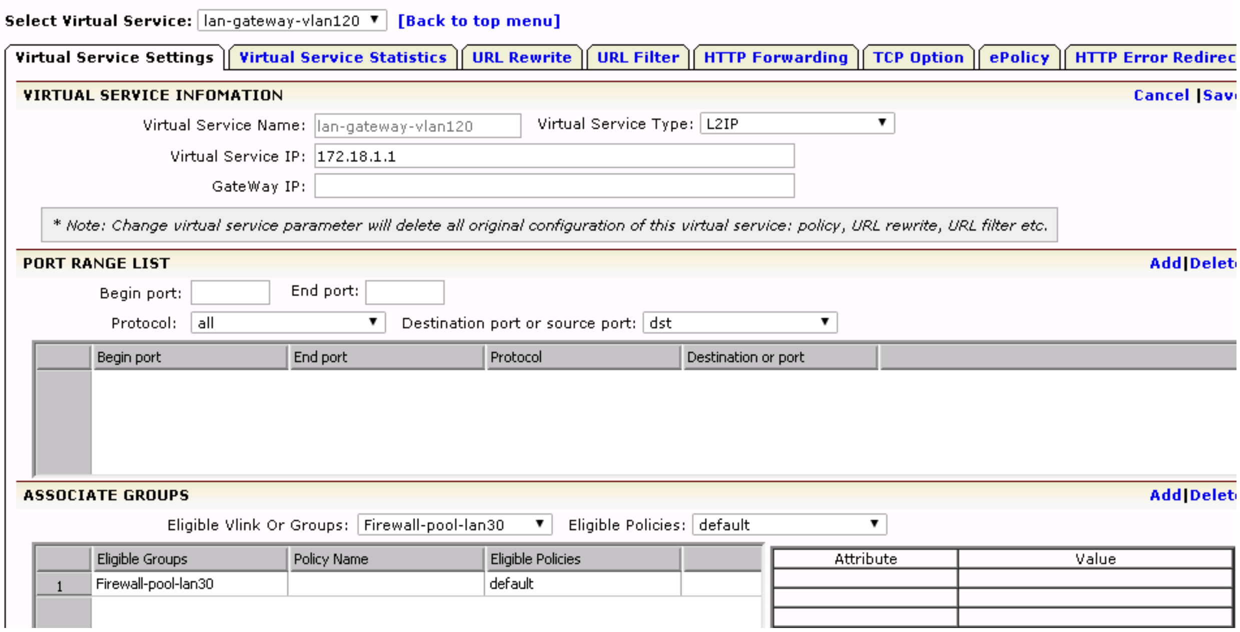
	Begin port	End port	Protocol	Destination or port	

ASSOCIATE GROUPS

Eligible Vlink Or Groups: Firewall-pool-lan20 Eligible Policies: default

	Eligible Groups	Policy Name	Eligible Policies	
1	Firewall-pool-lan20		default	

Attribute	Value



Select Virtual Service: lan-gateway-vlan120 ▼ [Back to top menu]

VIRTUAL SERVICE INFOMATION

Virtual Service Name: lan-gateway-vlan120

Virtual Service Type: L2IP ▼

Virtual Service IP: 172.18.1.1

GateWay IP:

* Note: Change virtual service parameter will delete all original configuration of this virtual service: policy, URL rewrite, URL filter etc.

PORT RANGE LIST

Begin port: End port:

Protocol: all ▼ Destination port or source port: dst ▼

	Begin port	End port	Protocol	Destination or port

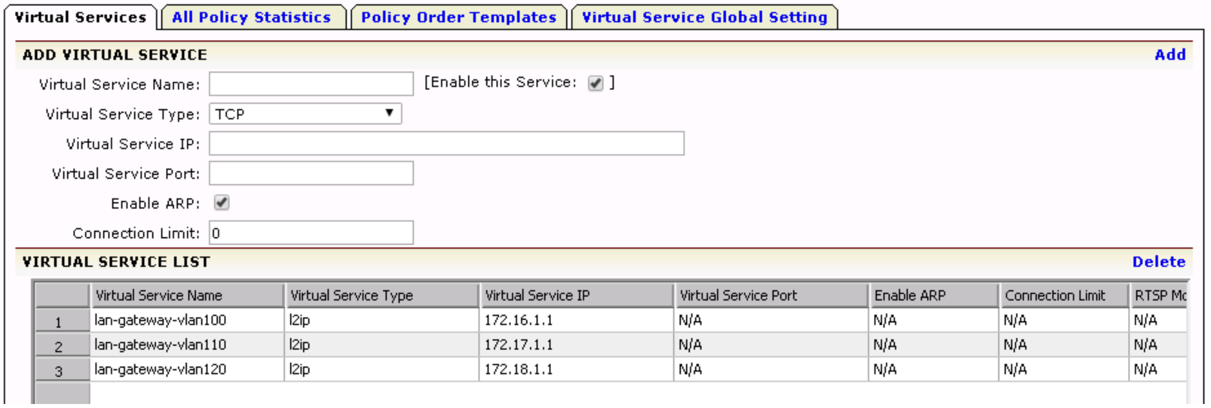
ASSOCIATE GROUPS

Eligible Vlink Or Groups: Firewall-pool-lan30 ▼ Eligible Policies: default ▼

	Eligible Groups	Policy Name	Eligible Policies
1	Firewall-pool-lan30		default

Attribute	Value

- The Virtual Services tab will display all Virtual Services created



ADD VIRTUAL SERVICE

Virtual Service Name: [Enable this Service: ☑]

Virtual Service Type: TCP ▼

Virtual Service IP:

Virtual Service Port:

Enable ARP: ☑

Connection Limit: 0

VIRTUAL SERVICE LIST

	Virtual Service Name	Virtual Service Type	Virtual Service IP	Virtual Service Port	Enable ARP	Connection Limit	RTSP Mc
1	lan-gateway-vlan100	l2ip	172.16.1.1	N/A	N/A	N/A	N/A
2	lan-gateway-vlan110	l2ip	172.17.1.1	N/A	N/A	N/A	N/A
3	lan-gateway-vlan120	l2ip	172.18.1.1	N/A	N/A	N/A	N/A

7 Support for Multiple LANs in a Fully Redundant Configuration

Combine the steps detailed in sections 5 and 6 together.

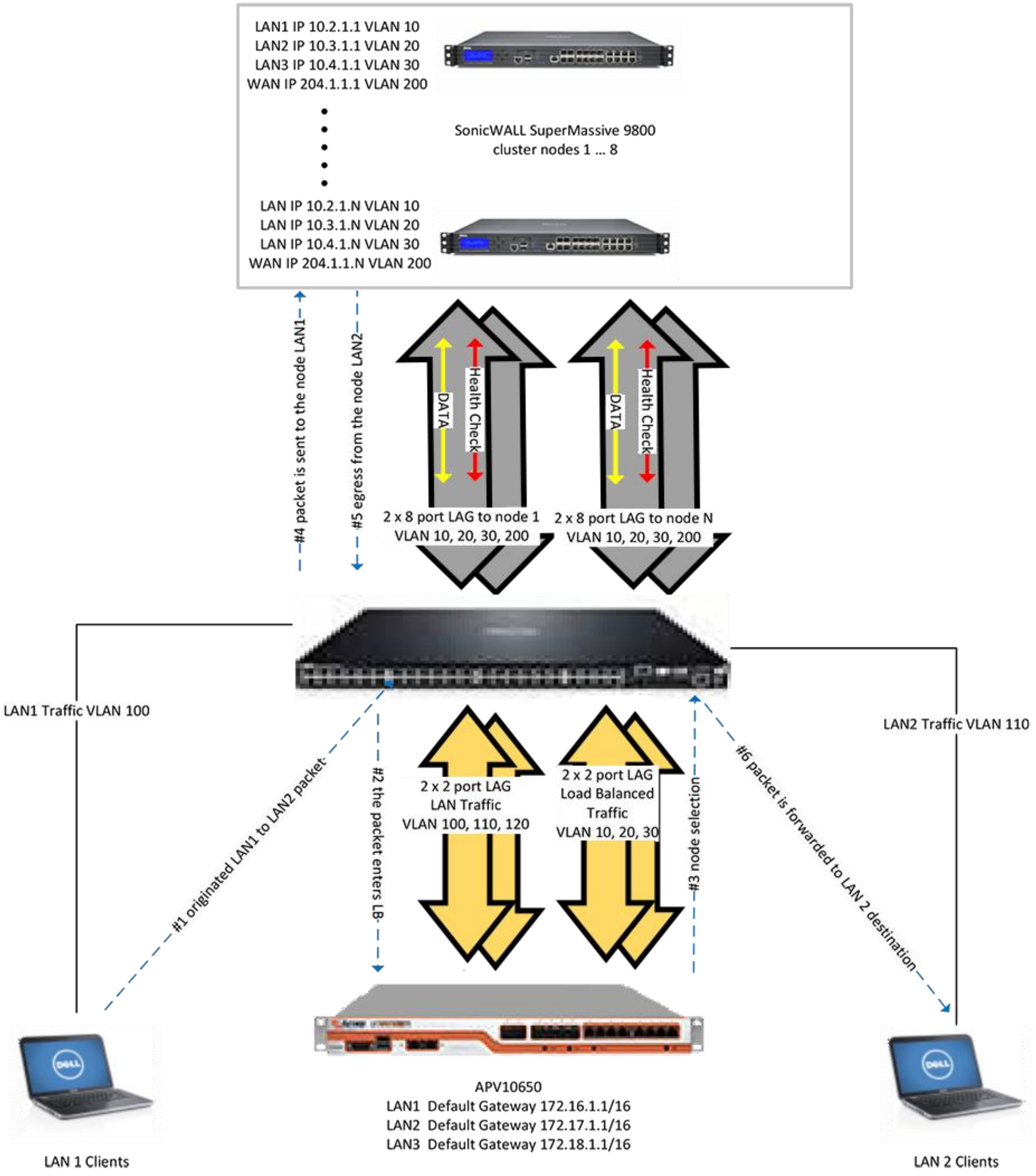


Figure 4: Supporting Multiple VLANs in a Fully Redundant Configuration

About Array Networks

Array Networks is a global leader in application delivery networking with over 5000 worldwide customer deployments. Powered by award-winning SpeedCore software, Array application delivery, WAN optimization and secure access solutions are recognized by leading enterprise, service provider and public sector organizations for unmatched performance and total value of ownership. Array is headquartered in Silicon Valley, is backed by over 250 employees worldwide and is a profitable company with strong investors, management and revenue growth. Poised to capitalize on explosive growth in the areas of mobile and cloud computing, analysts and thought leaders including Deloitte, IDC and Frost & Sullivan have recognized Array Networks for its technical innovation, operational excellence and market opportunity.

Corporate Headquarters
info@arraynetworks.com
408-240-8700
1 866 MY-ARRAY
www.arraynetworks.com

EMEA
rschmit@arraynetworks.com
+32 2 6336382

China
support@arraynetworks.com.cn
+010-84446688

France and North Africa
infosfrance@arraynetworks.com
+33 6 07 511 868

India
isales@arraynetworks.com
+91-080-41329296

Japan
sales-japan@
arraynetworks.com
+81-44-589-8315

To purchase Array Networks Solutions, please contact your Array Networks representative at 1-866-MY-ARRAY (692-7729) or authorized reseller

Jan-2017 rev. a