H3C EVPN安全纳管方案介绍

学习完本课程，您应该能够：

- 熟悉EVPN安全纳管的基本组网
- 掌握EVPN安全纳管的流量原理
- 掌握EVPN安全纳管的配置思路

目录

SDN Overlay安全方案比较

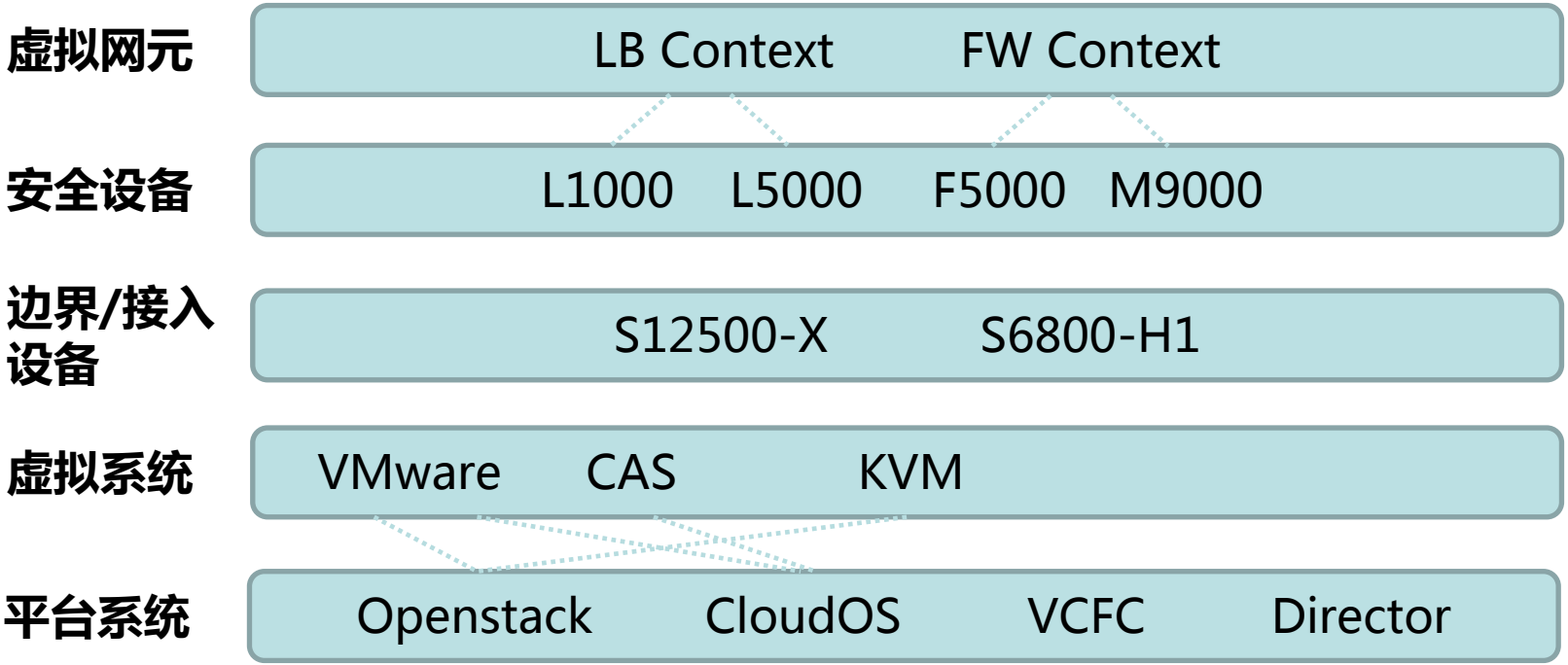
- **传统网络安全部署方式：**
  - 独立盒式或者框式安全设备，通过PBR、MQC、路由等引流方式至安全设备进行处理
  - 设备部署复杂，对网络运行影响大；流量牵引方式复杂，不容易掌握不同情况下引流的方式

- **SDN Overlay网络中安全部署方式：**
  - 安全策略
  - 服务链
  - 集中控制模式安全纳管
  - 分散控制模式（EVPN）安全纳管

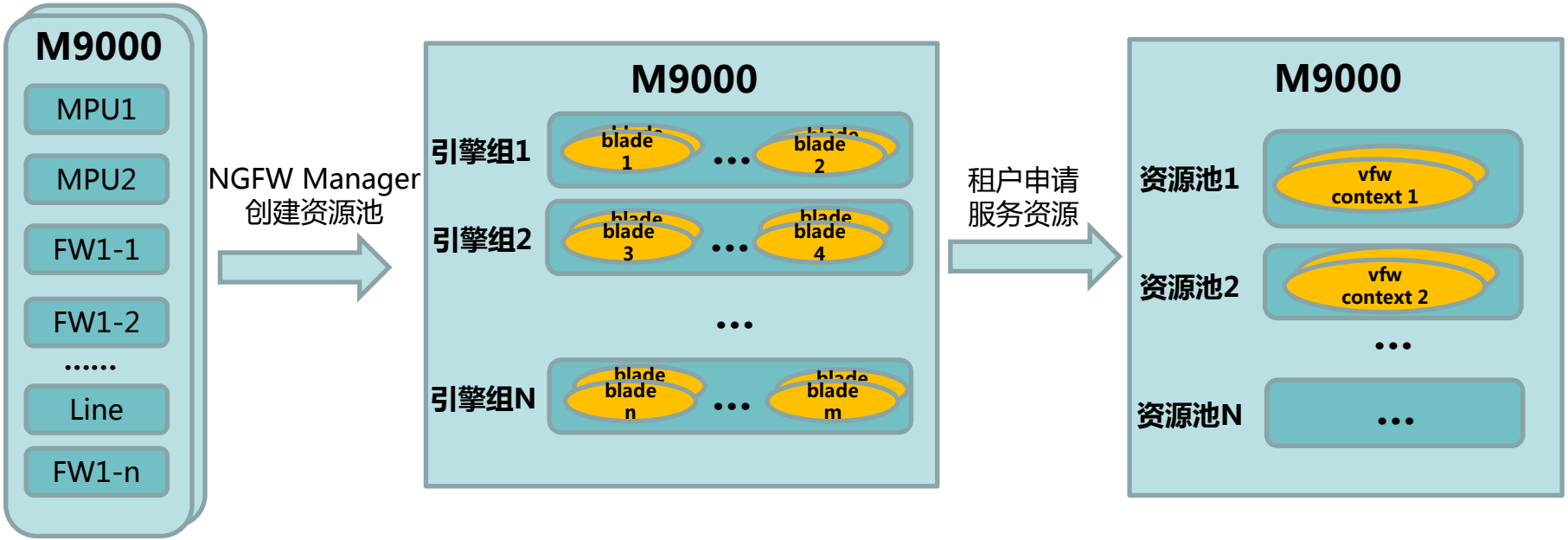
SDN Overlay安全方案比较

方案名	实现方式	缺点	优点
安全策略	Openflow流表实现，白名单功能，针对每个vport下发	局限性大，策略粒度太细，适用场景单一	使用方便，无需引流，性能高
服务链	NFV形态的VFW、VLB实现，流表引流，流量特征组匹配报文	需要NFVManager配合，NFV有性能瓶颈，网络overlay存在诸多限制	部署灵活，按需扩容，流量特征组+流表+PBR引流，可以控制策略颗粒度
集中控制模式安全纳管	在IP GW旁挂LB，串联FW，通过VCFC自动下发静态路由和PBR引流	流量必须上IP GW、实现较为复杂	性能较好，引流方式由控制器下发
EVPN安全纳管	Border旁挂LB，串联FW，通过VCFC自动下发静态路由和PBR引流	实现相对繁杂。组网必须是EVPN VXLAN组网。	性能好，自动引流。特性丰富。Border可与Leaf或Spine合一，组网灵活。

EVPN 安全纳管方案组成



安全资源池

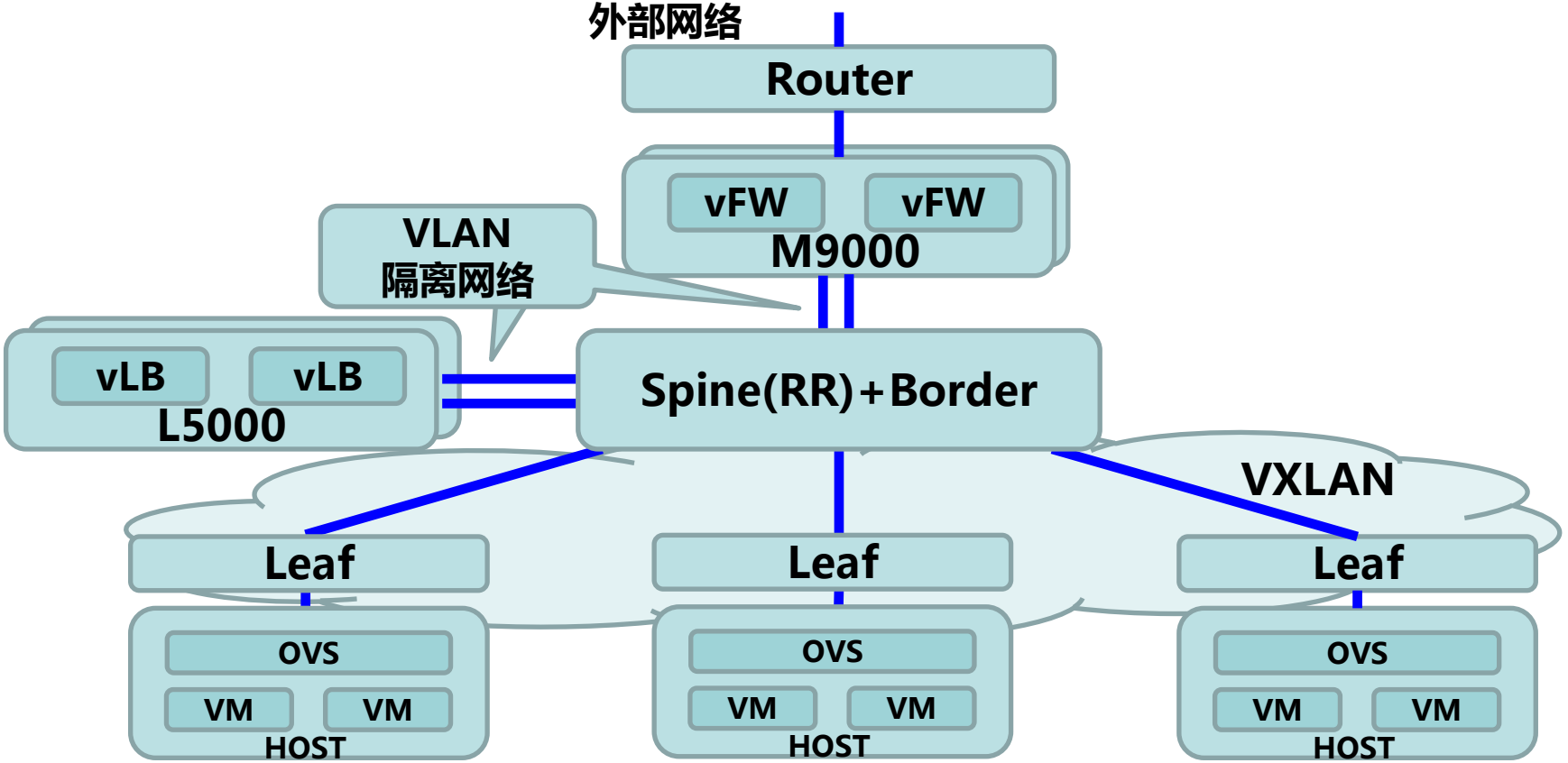


- M9000/F5000配置安全引擎组，VCFC NGFW Manager创建资源池，将引擎组分配给每个资源池，一个引擎组对应一个资源池；NEM在租户在申请服务资源时在用户选择的资源池里创建VFW context

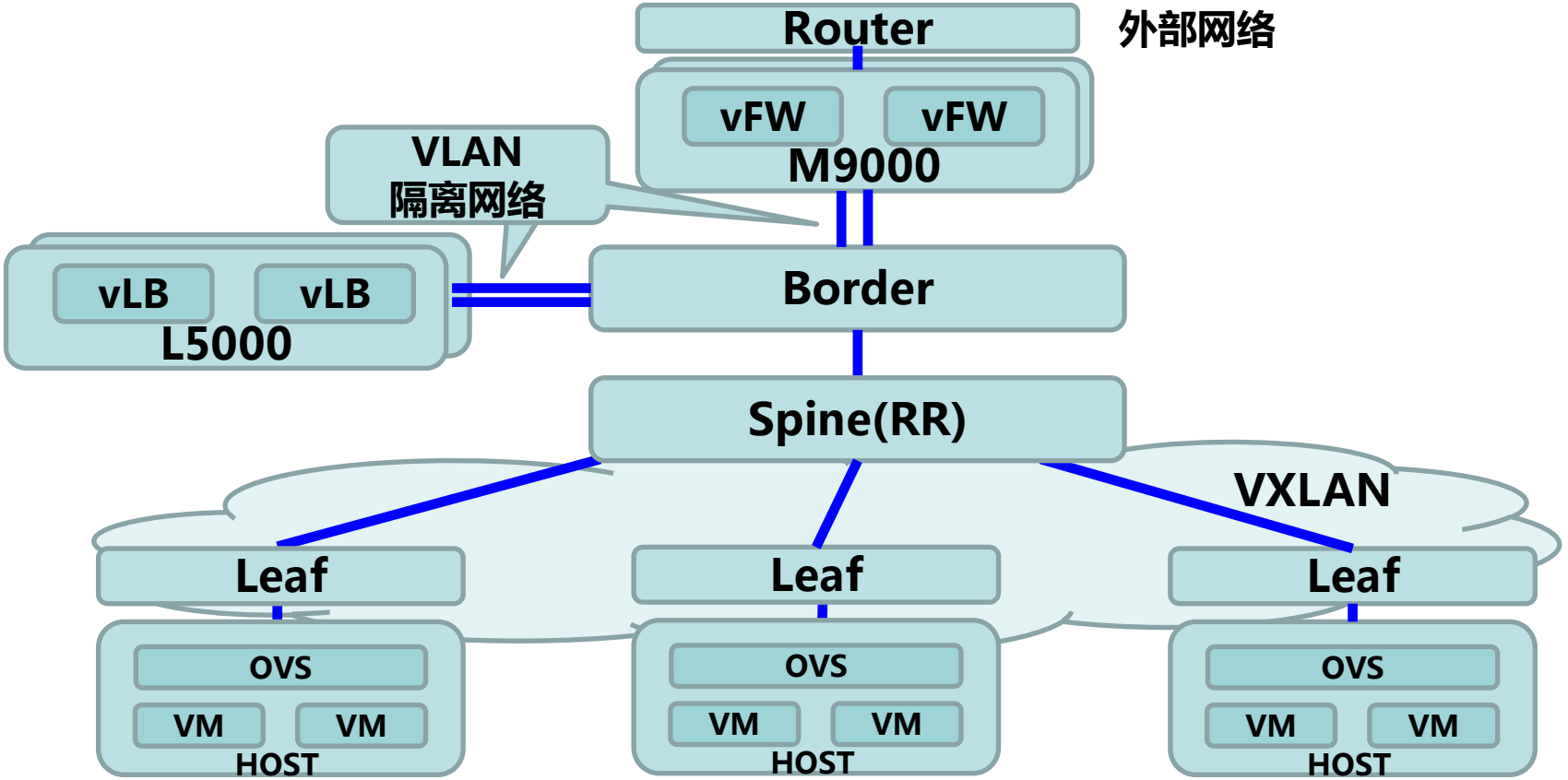
EVPN安全纳管特性

安全特性	VCFC	CloudOS	Openstack
防火墙	Yes	Yes	Yes
NAT	Yes	Yes	Yes
浮动IP	Yes	Yes	Yes
防病毒	Yes		
IPS	Yes		
攻击检测及防范	Yes		
URL过滤	Yes		
连接数限制	Yes		
SSL VPN	Yes		
IPSEC VPN	Yes		
负载均衡V1	Yes	Yes	Yes
负载均衡V2	Yes		

EVPN安全纳管逻辑拓扑1



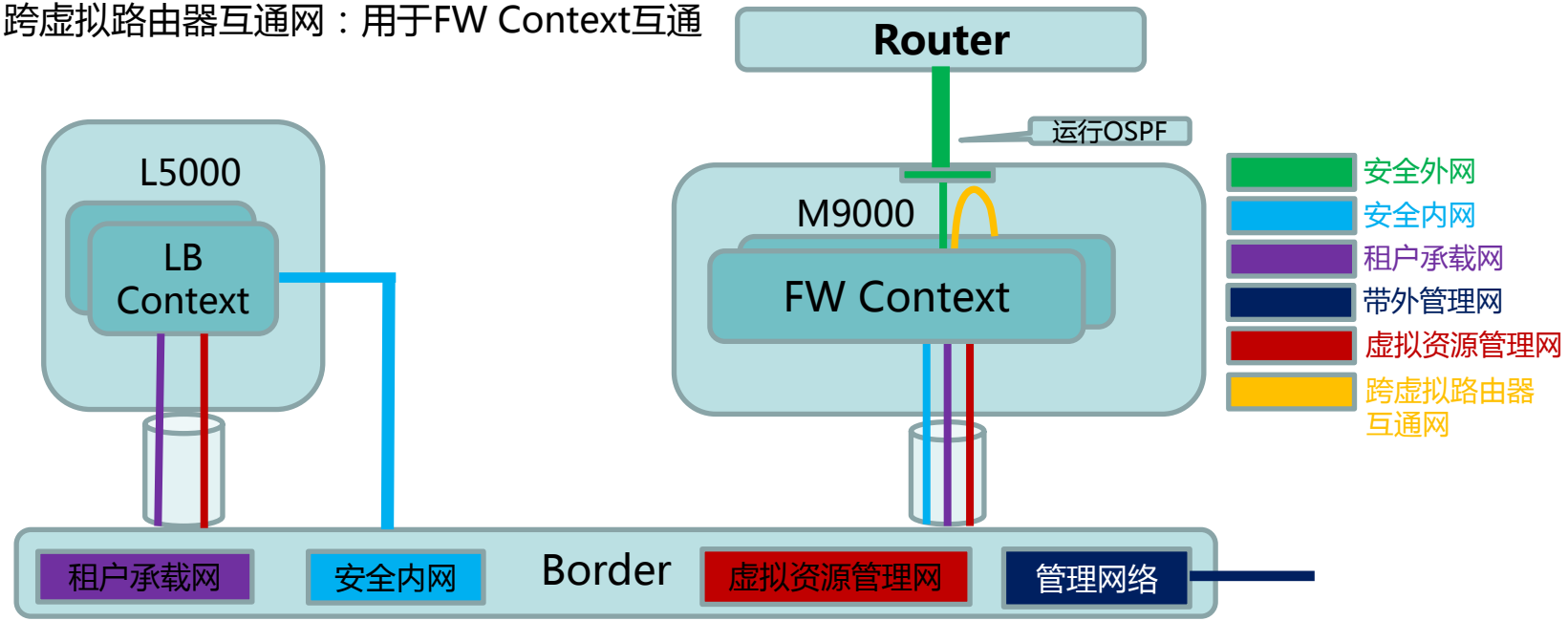
EVPN安全纳管逻辑拓扑2



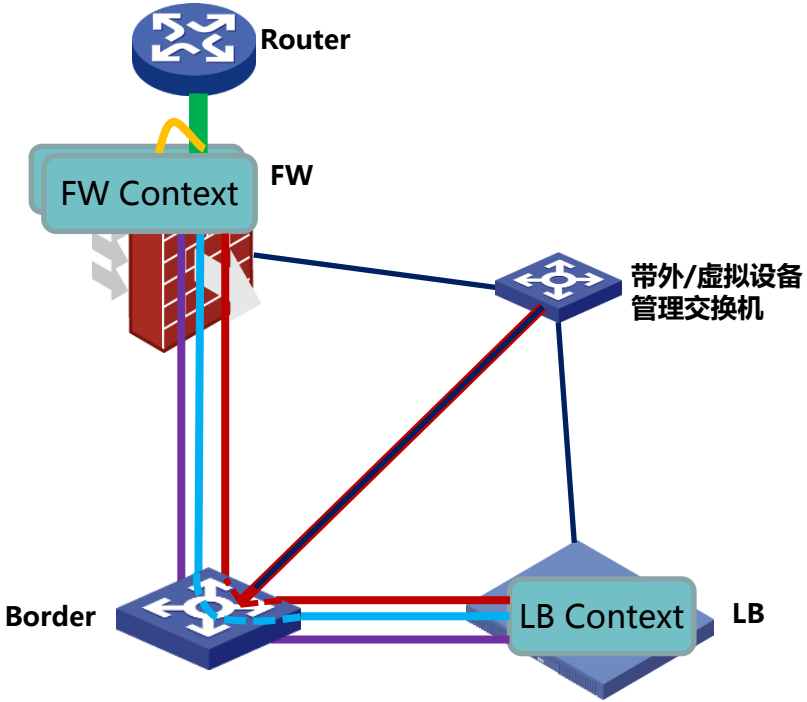
目录

EVPN安全纳管VLAN同网段组网

- 安全外网：用于FW与外网之间流量
- 安全内网：用于FW和LB之间流量，占用一个VLAN
- 租户承载网：用于FW和LB与租户VXLAN/VLAN网络之间流量，占用一个VLAN
- 虚拟资源管理网：用于FW和LB与VCFC之间流量
- 跨虚拟路由器互通网：用于FW Context互通



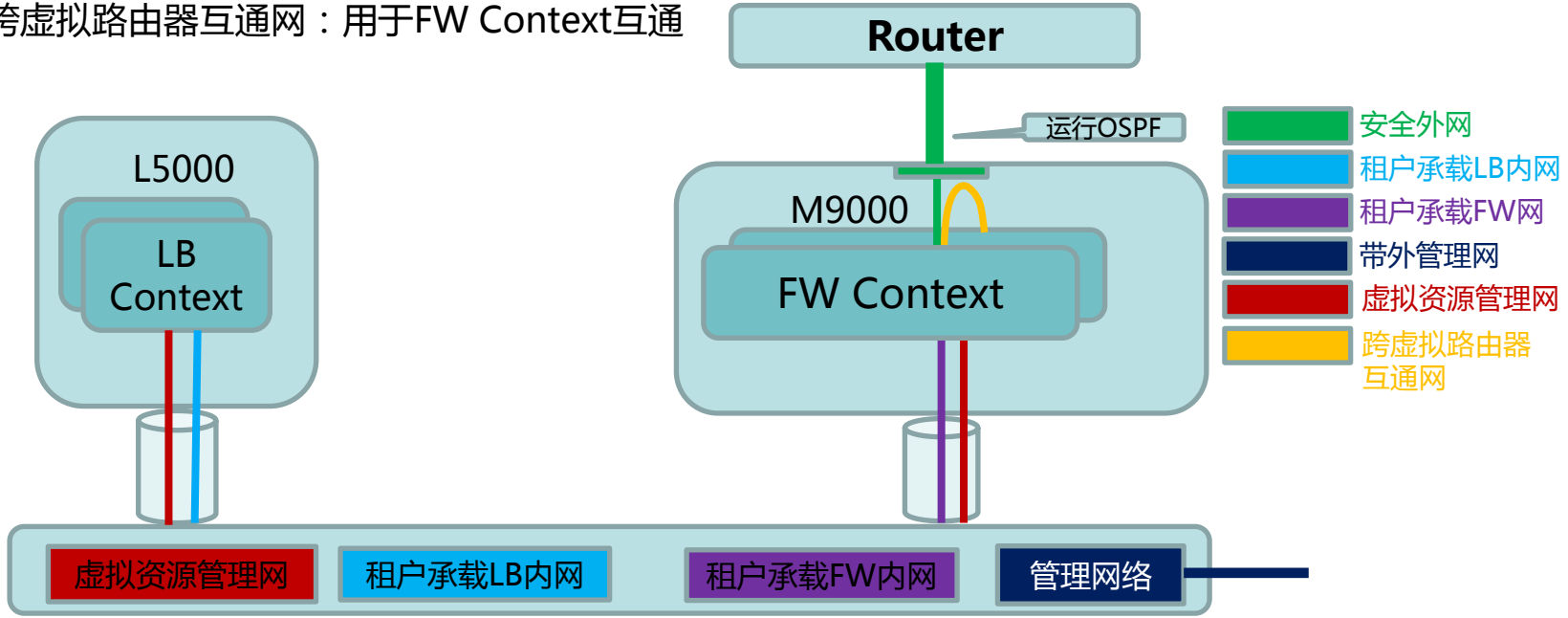
VLAN同网段典型组网



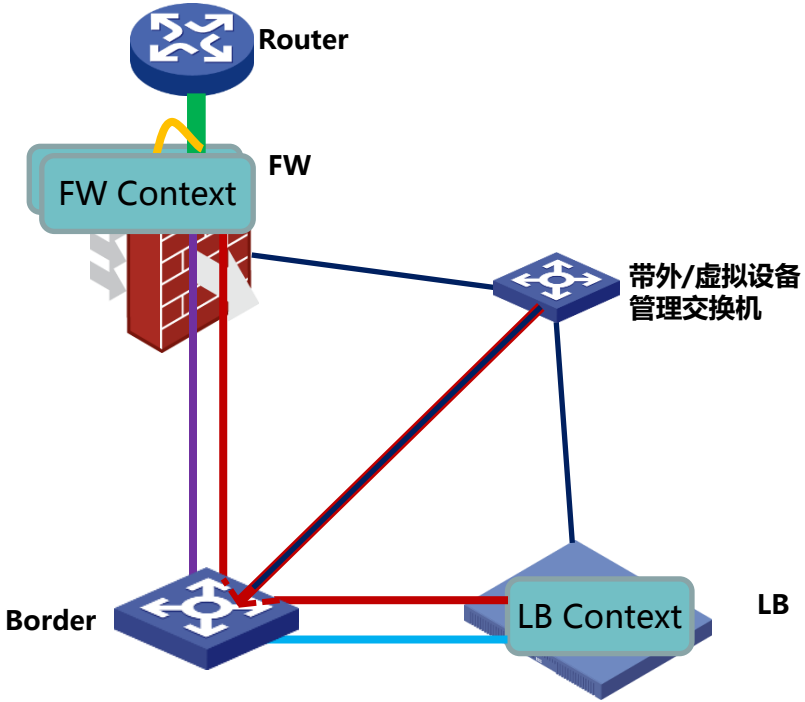
安全外网
安全内网
租户承载网
带外管理网
虚拟资源管理网
跨虚拟路由器
互通网

EVPN安全纳管VLAN跨网段组网

- 安全外网：用于FW与外网之间流量
- 租户承载防火墙内网：用于FW和Border之间流量，占用一个VLAN
- 租户承载负载均衡内网：用于LB与Border之间流量，占用一个VLAN
- 虚拟资源管理网：用于FW和LB与VCFC之间流量
- 跨虚拟路由器互通网：用于FW Context互通

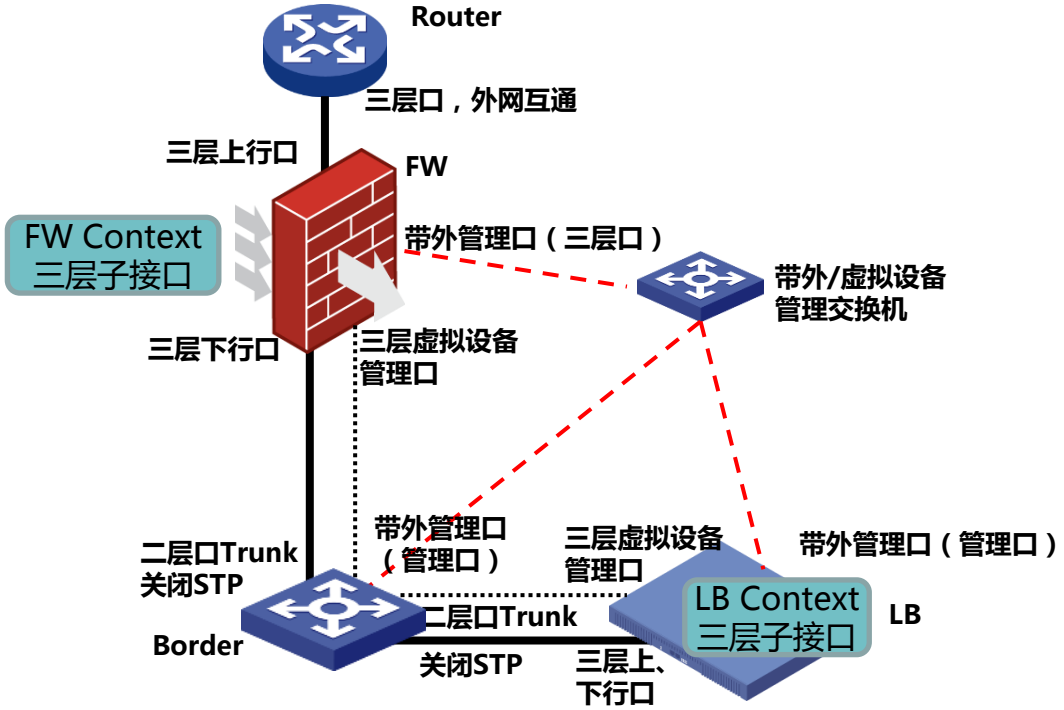


VLAN跨网段典型组网

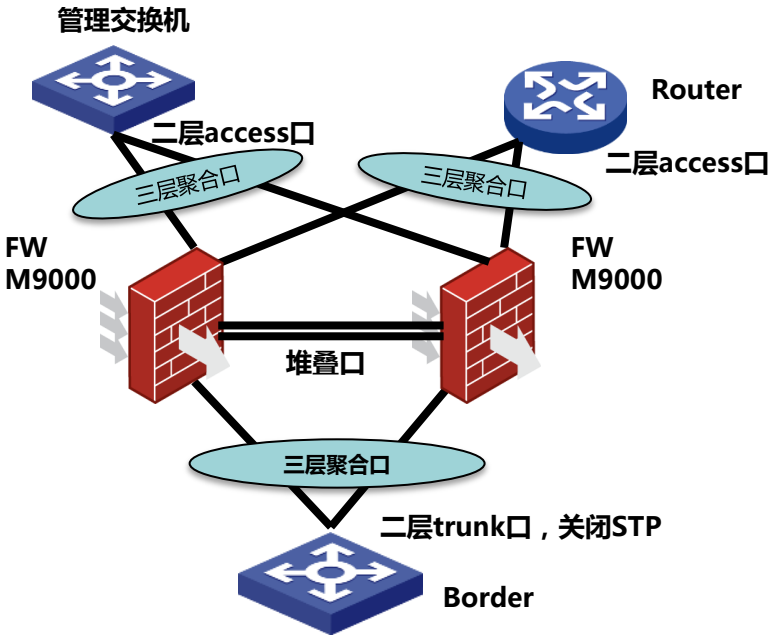


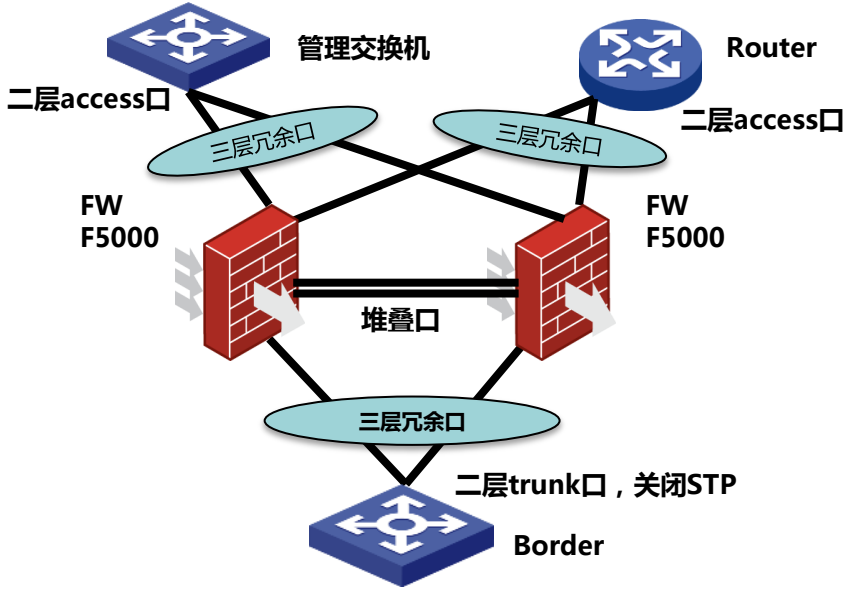
安全外网
租户承载LB内网
租户承载FW网
带外管理网
虚拟资源管理网
跨虚拟路由器
互通网

EVPN安全纳管基本组网一

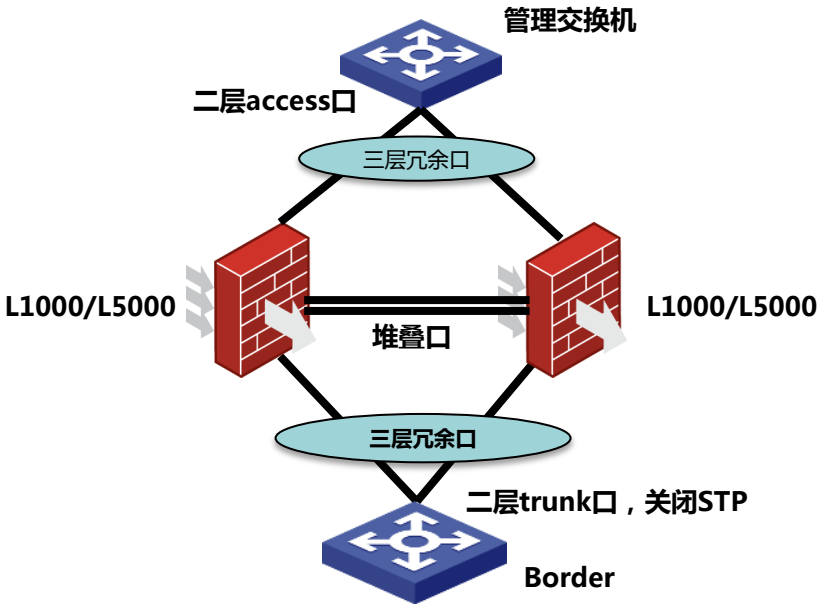


EVPN安全纳管基本组网一（续）

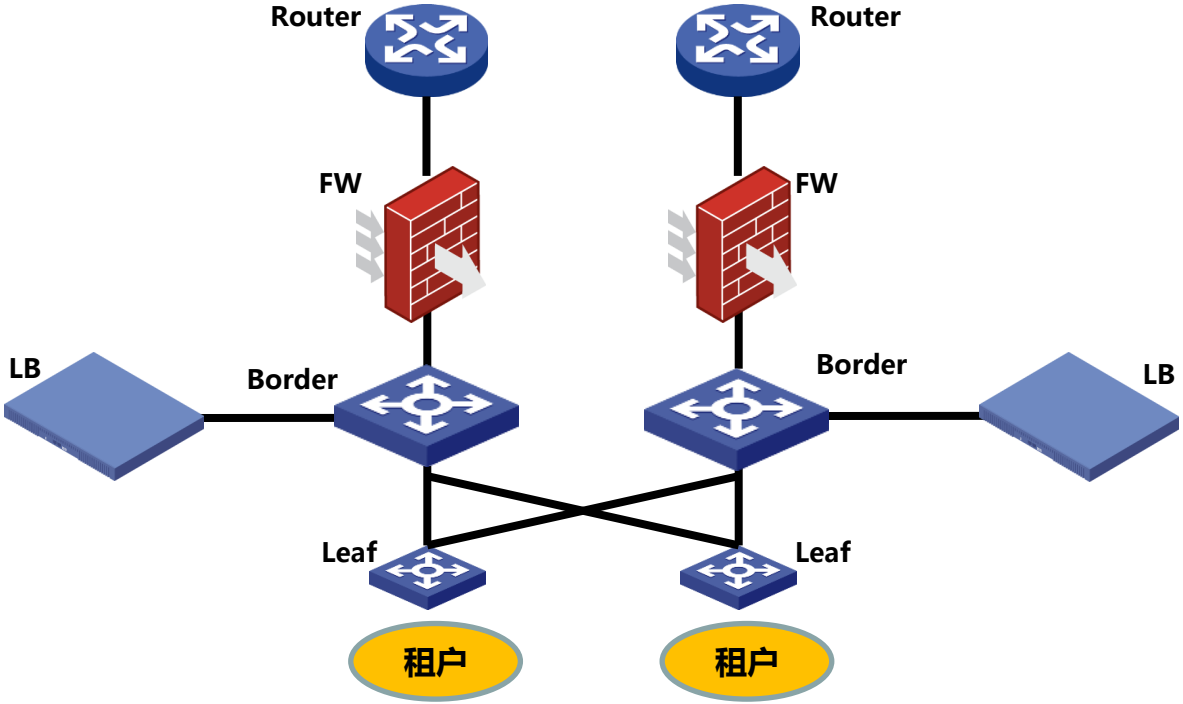




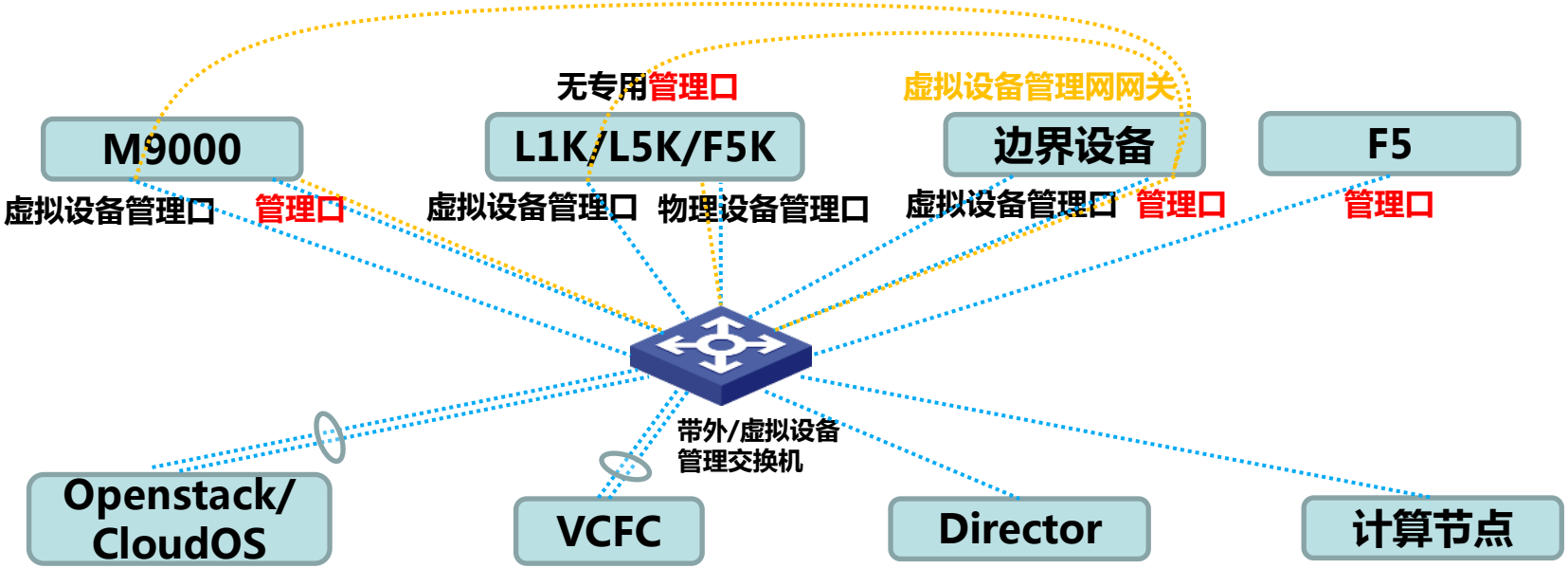
EVPN安全纳管基本组网一（续）



EVPN安全纳管基本组网二

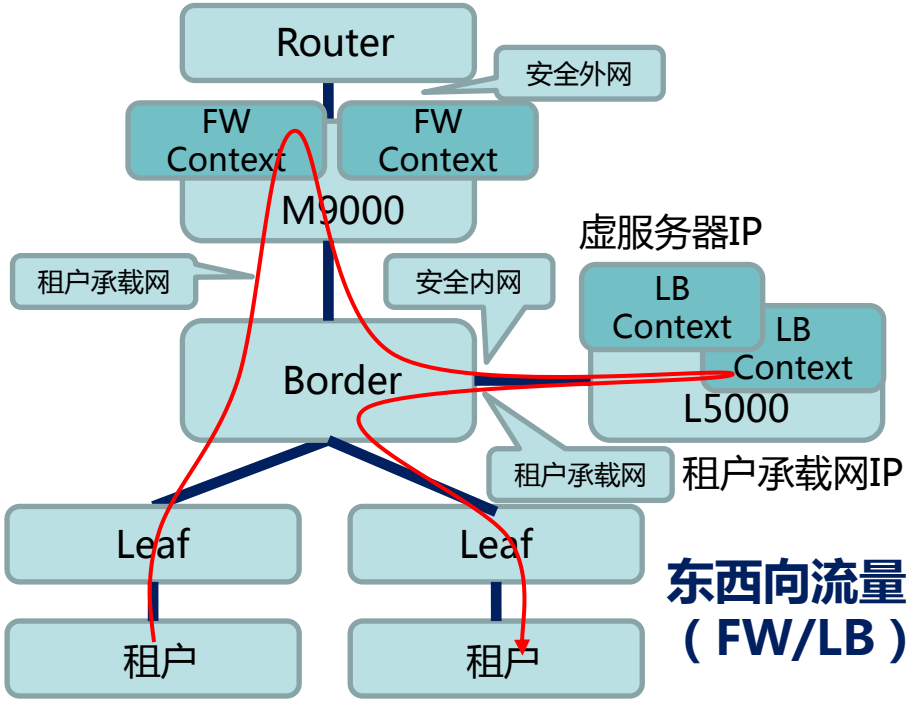


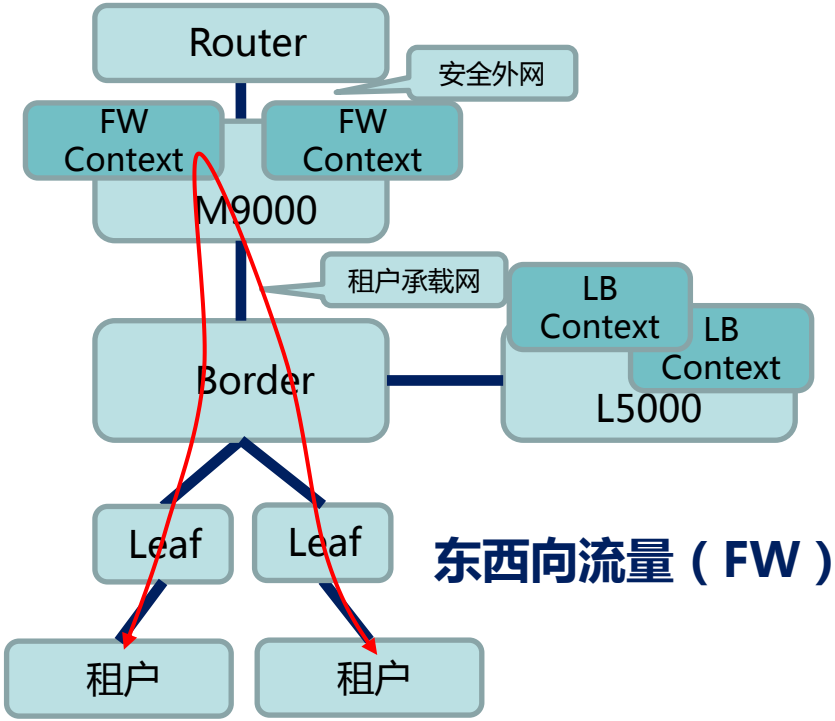
带外与虚拟设备管理网



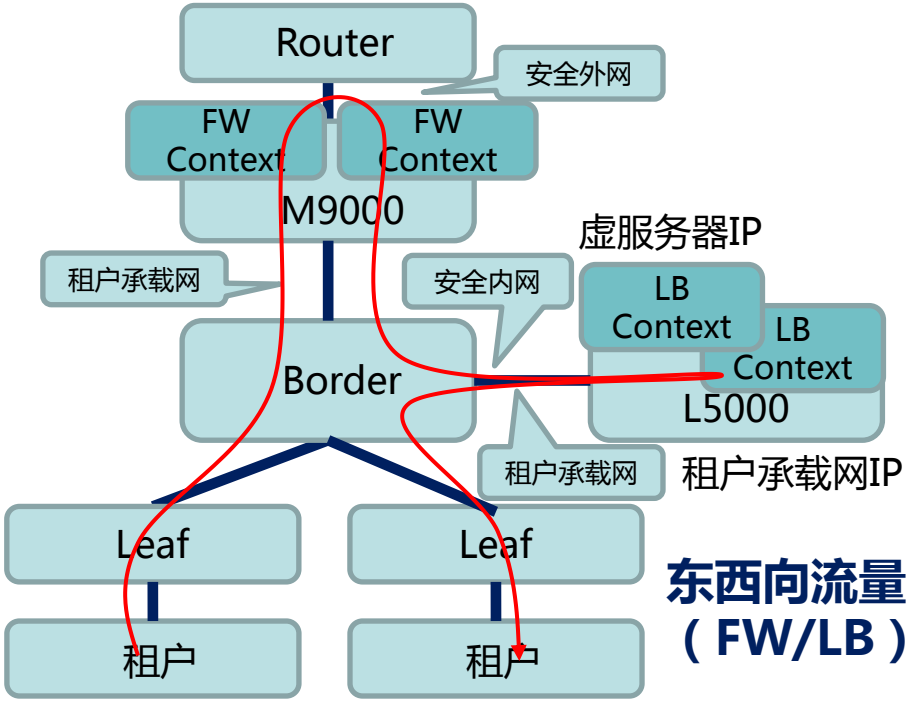
目录

东西向流量转发（同虚拟路由器）

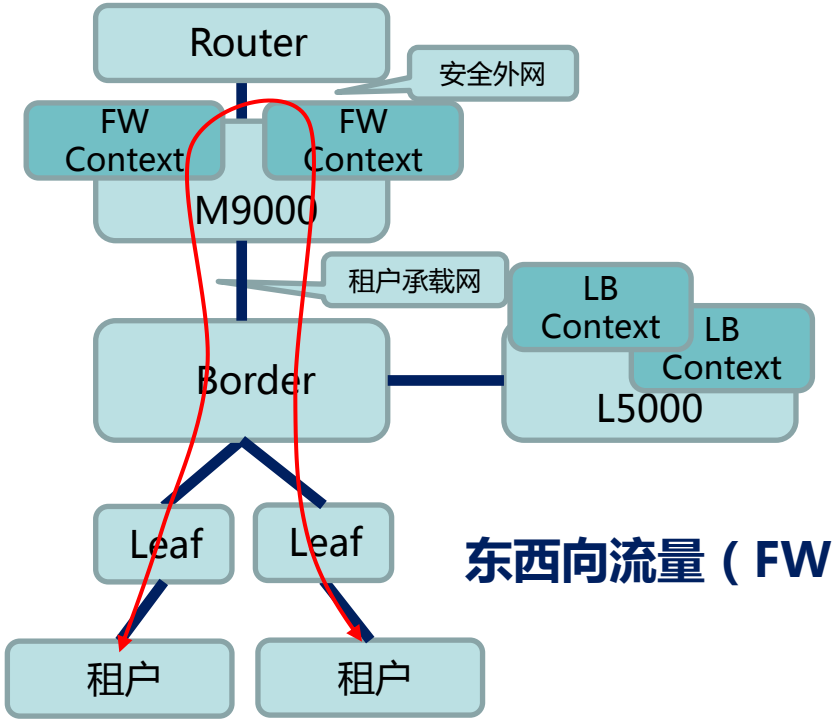




东西向流量转发（跨虚拟路由器）

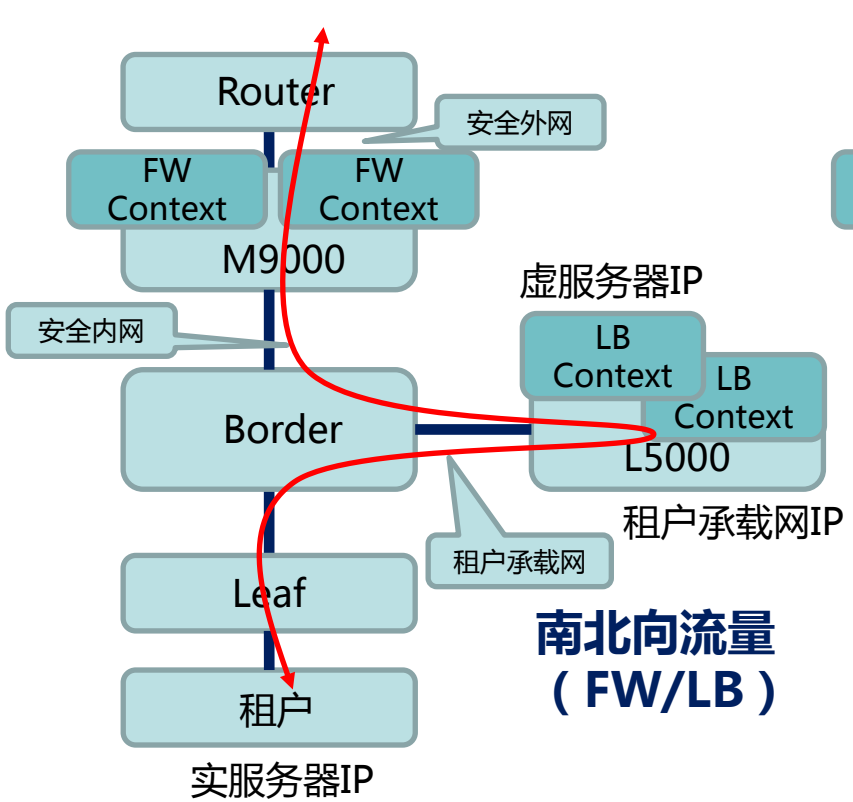


东西向流量（FW/LB）

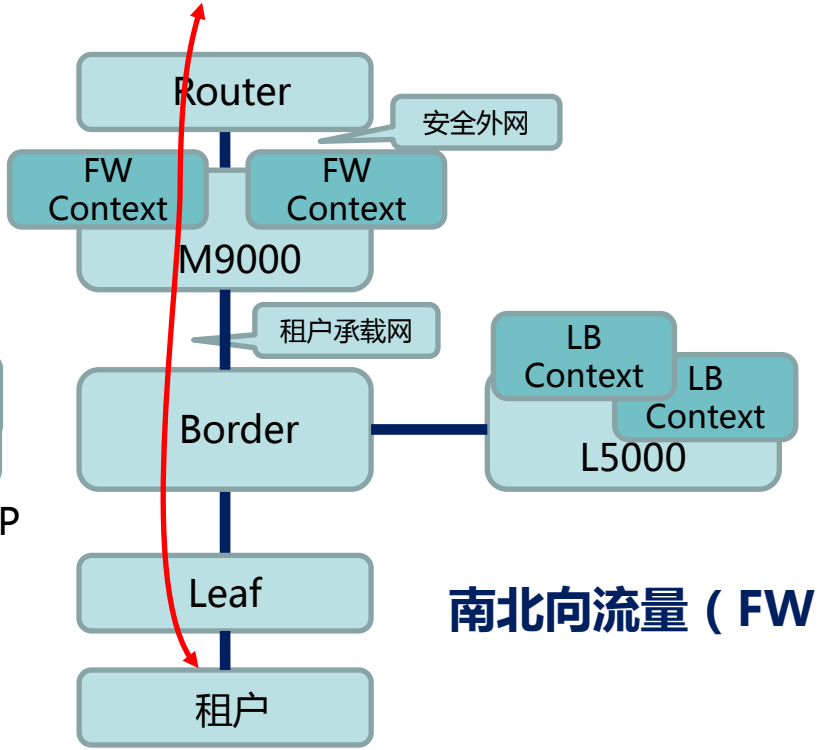


东西向流量（FW）

南北向流量转发



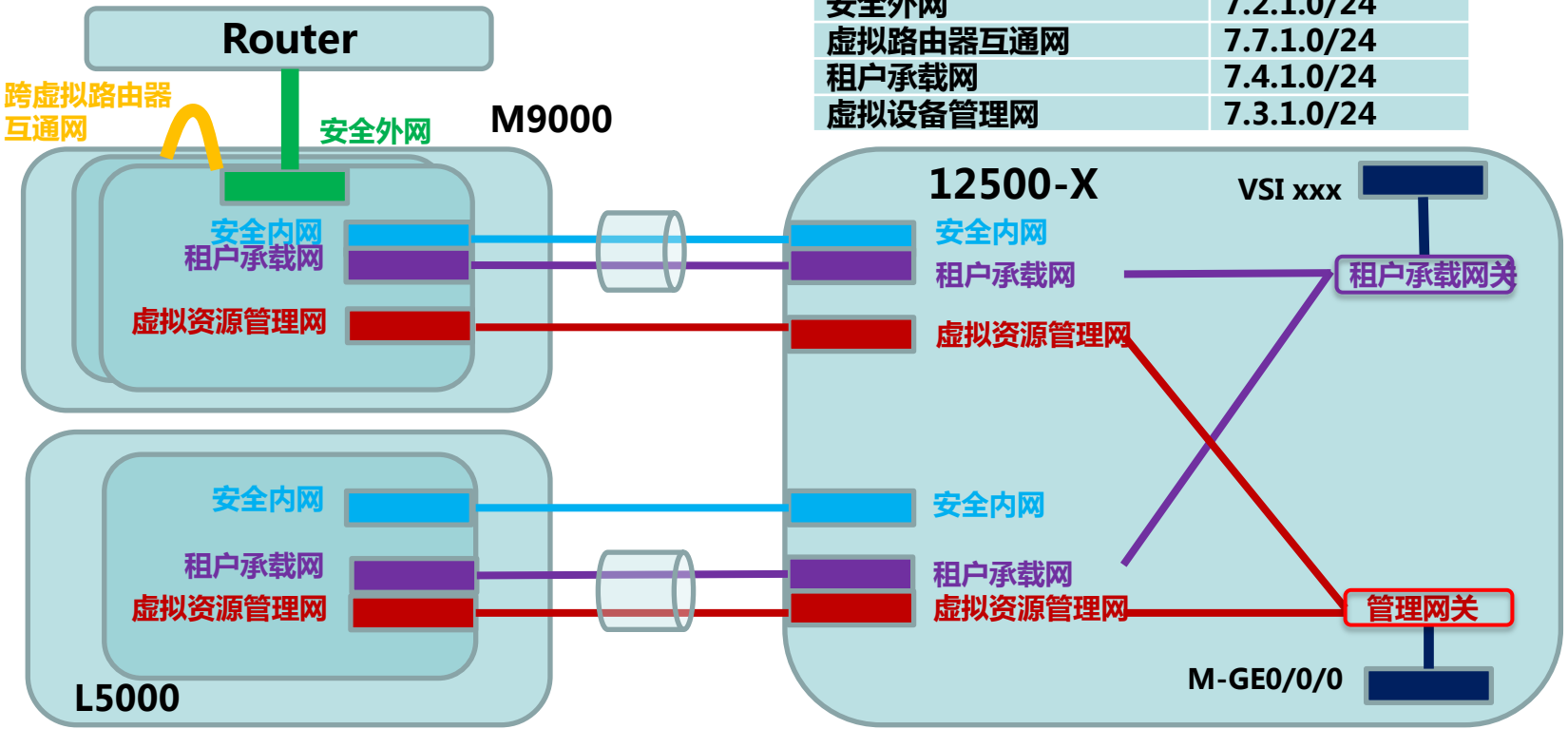
南北向流量（FW/LB）



南北向流量（FW）

EVPN安全纳管流量走向示例

安全内网	7.1.1.0/24
安全外网	7.2.1.0/24
虚拟路由器互通网	7.7.1.0/24
租户承载网	7.4.1.0/24
虚拟设备管理网	7.3.1.0/24



东西向过防火墙流量同虚拟路由器示例

- 东西向防火墙流量仅支持EVPN**集中式网关三层转发流量**。
- 举例：VM 202.0.0.2访问203.0.0.3

1、三层流量上Border后，在VSI口匹配VCFC自动下发的PBR。

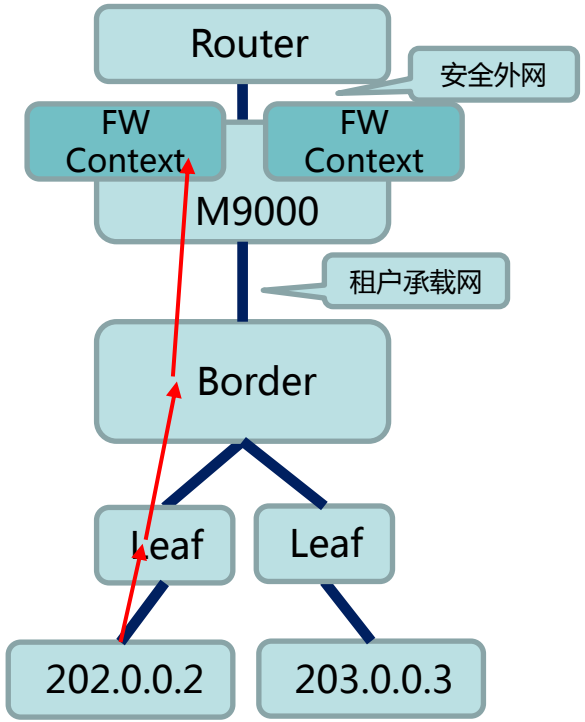
```
interface Vsi-interface3
 description SDN_VSI_Interface_2002
 ip binding vpn-instance 3000
 ip address 202.0.0.1 255.255.255.0 sub
 mac-address 3c8c-404e-dd46
 ip policy-based-route SDN_300
```

2、PBR会匹配ACL，并将下一跳设置为防火墙context内的租户承载网IP

```
policy-based-route SDN_300 permit node 100
 if-match acl name SDN_ACL_FW_3000
 apply next-hop vpn-instance 3000 7.4.1.4
```

3、ACL匹配源sub网段：

```
acl advanced name SDN_ACL_FW_3000
 description SDN_ACL_DEC_FW_3000
 rule 10000 permit ip vpn-instance 3000 source 202.0.0.0 0.0.0.255
 rule 10001 permit ip vpn-instance 3000 source 203.0.0.0 0.0.0.255
```



东西向过防火墙同虚拟路由器流量示例

4、安全策略放通后，匹配控制器下发的静态网段路由，将流量送回租户承载网网关

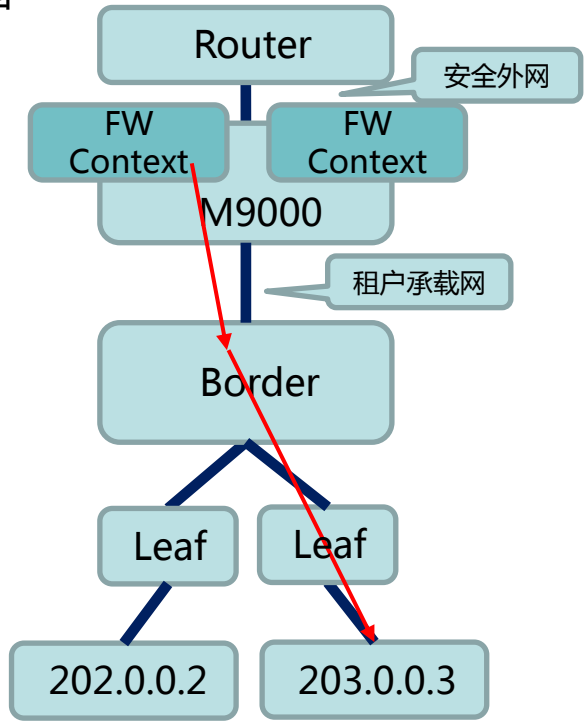
ip route-static vpn-instance 3000 202.0.0.0 24 7.4.1.1 description SDN_ROUTE

ip route-static vpn-instance 3000 203.0.0.0 24 7.4.1.1 description SDN_ROUTE

//到内网子网的网段路由指向租户承载网网关

5、Border上匹配VSI直连网段路由，查询流量通过VSI送给Leaf。

6、回程与去程的转发流程基本一致。



东西向过防火墙跨虚拟路由器流量示例

- 东西向防火墙流量仅支持**EVPN集中式网关跨虚拟路由器转发流量**。
- 举例：VM 202.0.0.2（VPN 3000）访问204.0.0.5（VPN 4000）

1、跨VPN流量上Border后，在VSI口匹配VCFC自动下发的PBR

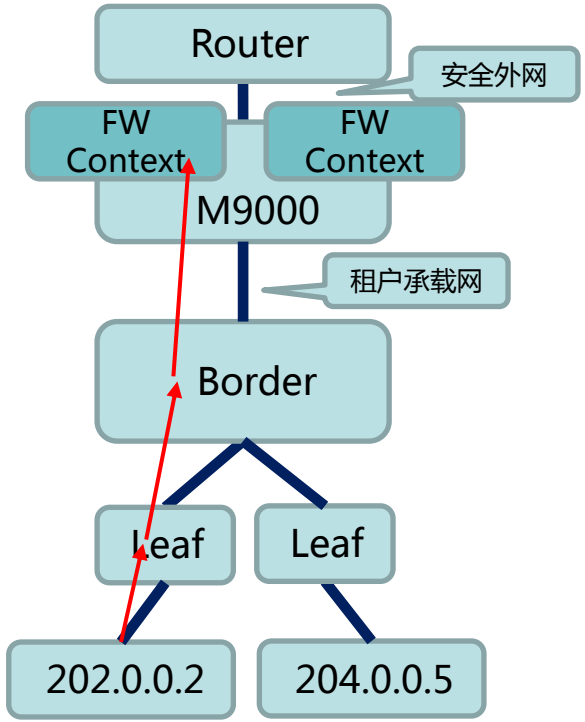
```
interface Vsi-interface3
 description SDN_VSI_Interface_2002
 ip binding vpn-instance 3000
 ip address 202.0.0.1 255.255.255.0 sub
 mac-address 3c8c-404e-dd46
 ip policy-based-route SDN_300
```

2、PBR会匹配ACL，并将下一跳设置为本虚拟路由器管理的防火墙context内的租户承载网IP

```
policy-based-route SDN_300 permit node 100
 if-match acl name SDN_ACL_FW_3000
 apply next-hop vpn-instance 3000 7.4.1.4
```

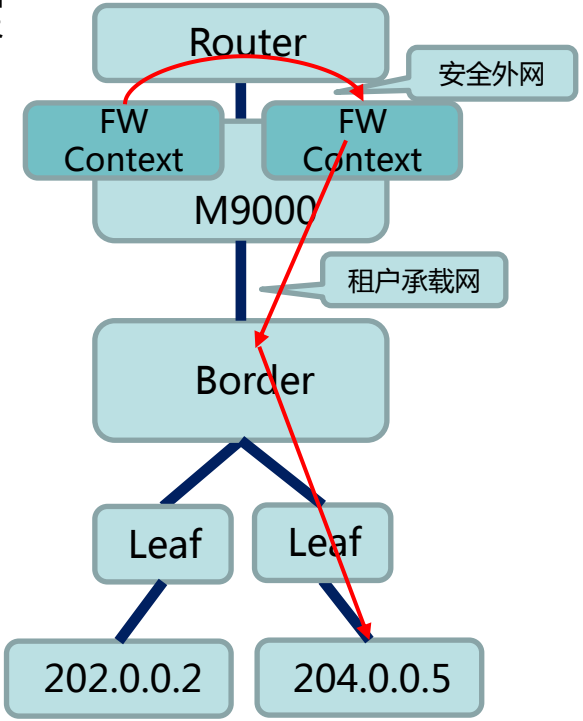
3、ACL匹配源sub网段：

```
acl advanced name SDN_ACL_FW_3000
 description SDN_ACL_DEC_FW_3000
 rule 10000 permit ip vpn-instance 3000 source 202.0.0.0 0.0.0.255
 rule 10001 permit ip vpn-instance 3000 source 203.0.0.0 0.0.0.255
```



东西向过防火墙跨虚拟路由器流量示例

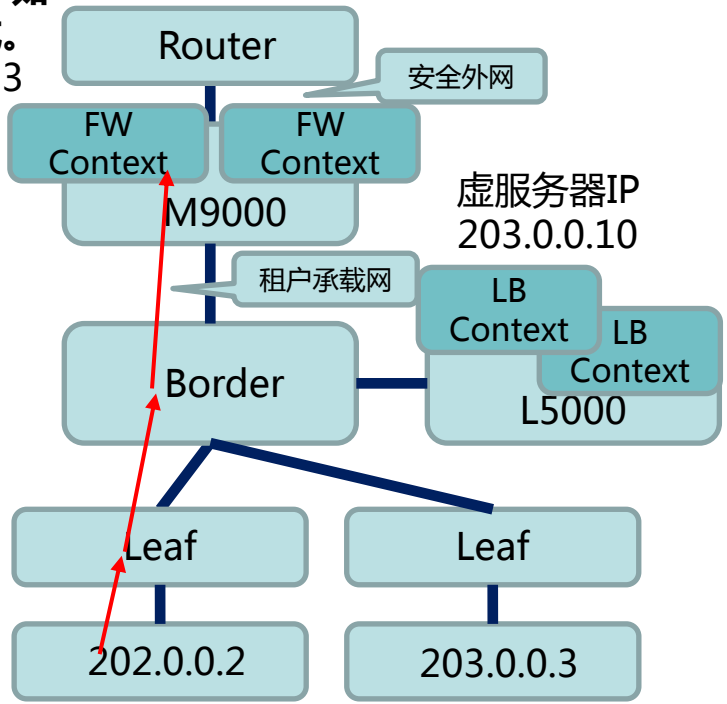
4、安全策略放通后，匹配控制器下发的静态网段路由，将流量到目的地址所属虚拟路由器的Context，下一跳为该Context的跨虚拟路由器互通网地址
ip route-static vpn-instance 3000 204.0.0.0 24 vpn-instance external_vpn 7.7.1.2 description SDN_ROUTE
5、到达目的Context后，如果安全策略放通，匹配VCFC下发的网段路由，将流量送给本VPN的租户承载网网关
ip route-static vpn-instance external_vpn 204.0.0.0 24 vpn-instance 4000 7.4.1.2 description SDN_ROUTE
6、Border上匹配VSI直连网段路由，查询流量通过VSI送给Leaf。
7、回程与去程的转发流程基本一致。



东西向过防火墙负载均衡分布式网关流量示例

- **当组网为EVPN分布式网关时，需开启虚服务源IP地址转换。如果虚服务IP与实服务IP同subnet，则必须使用ARP代理模式。**
- 举例：VM 202.0.0.2访虚IP203.0.0.10，对应实IP为203.0.0.3

1、Border发布VCFC下发的虚IP主机路由：
ip route-static vpn-instance 3000 203.0.0.10 32 7.4.1.3 description SDN_ROUTE
2、三层流量上Border后，在VSI口匹配VCFC自动下发的PBR。
interface Vsi-interface3
ip policy-based-route **SDN_300**
2、PBR会匹配ACL，并将下一跳设置为防火墙context内的租户承载网IP
policy-based-route **SDN_300** permit node 100
 if-match acl name **SDN_ACL_FW_3000**
 apply next-hop vpn-instance 3000 7.4.1.4
3、ACL匹配源sub网段：
acl advanced name **SDN_ACL_FW_3000**
rule 10001 permit ip vpn-instance 3000 source 203.0.0.0 0.0.0.255



东西向过防火墙负载均衡分布式网关流量示例

4、安全策略放通后，匹配控制器下发的虚IP主机路由，将流量送给负载均衡

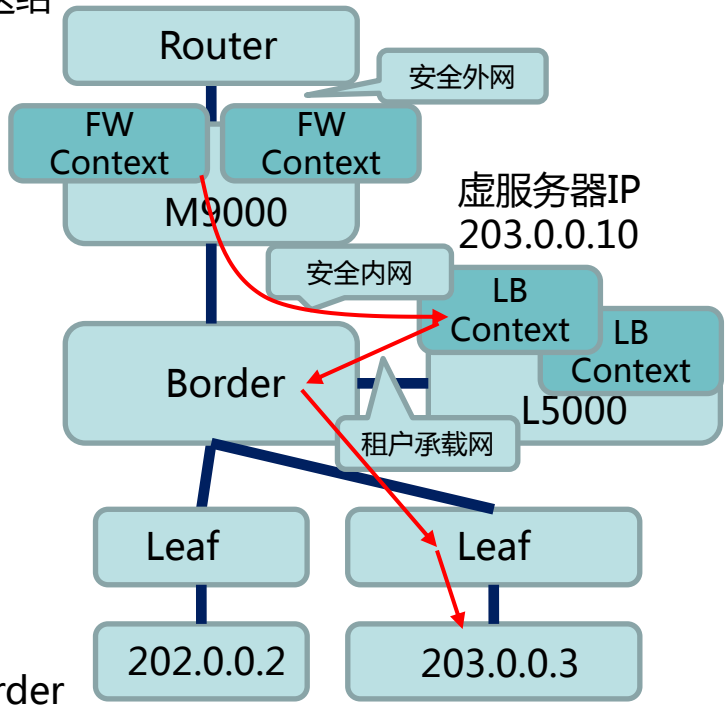
ip route-static vpn-instance 3000 203.0.0.10 32 **7.1.1.1**
description SDN_ROUTE//下一跳为LB安全内网IP

5、负载均衡上完成转换并生成会话，并且进行地址转换：

Initiator:
  Source   IP/port: **202.0.0.2/28884**
  Destination IP/port: **203.0.0.10/22**
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: 3000/-/-
Inbound interface: Ten-GigabitEthernet1/0/25.302
Responder:
  Source   IP/port: **203.0.0.3/22**
  Destination IP/port: **203.0.0.10/9085**
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: 3000/-/-
Inbound interface: Ten-GigabitEthernet1/0/24.300
State: TCP_ESTABLISHED
Application: SSH

6、负载均衡匹配控制器下发的网段路由，将转换后报文送给Border

ip route-static vpn-instance 3000 203.0.0.0 24 **7.4.1.1**
description SDN_ROUTE//下一跳为租户承载网网关



东西向过防火墙负载均衡分布式网关流量示例

7、回程流量由于是ARP代理模式，查询主机路由转发。到达Border后，匹配VSI接口上PBR首先送往负载均衡

interface Vsi-interface4

ip policy-based-route **SDN_300**

PBR会匹配ACL，并将下一跳设置为负载均衡context内的租户承载网IP

policy-based-route **SDN_300** permit node 50

 if-match acl name **SDN_ACL_LB_3000**

 apply next-hop vpn-instance 3000 7.4.1.3

ACL匹配源sub网段：

acl basic name **SDN_ACL_LB_3000**

 description SDN_ACL_DEC_LB_3000

 rule 10000 permit vpn-instance 3000 source **203.0.0.3 0**

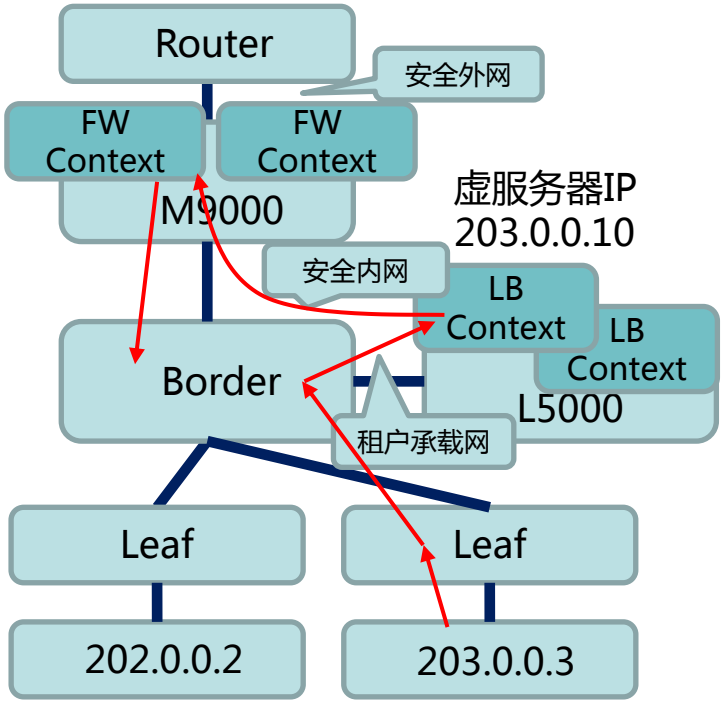
 rule 10001 permit vpn-instance 3000 source **203.0.0.4 0**

8、负载均衡上匹配会话，转换地址，将流量送回防火墙context

9、防火墙上匹配控制器下发的网段路由，将转换后报文送给Borde

ip route-static vpn-instance 3000 202.0.0.0 24 7.4.1.1

description SDN_ROUTE//下一跳为租户承载网网关



东西向过防火墙负载均衡集中式网关流量示例

- **当组网为EVPN集中式网关时，如果源IP与实服务器IP同subnet，需开启虚服务源IP地址转换。不支持源IP与需服务器IP同subnet。**
- 举例：VM 202.0.0.2访虚IP203.0.0.10，对应实IP为203.0.0.3

1、Border发布VCFC下发的虚IP主机路由：

ip route-static vpn-instance 3000 203.0.0.10 32 7.4.1.3 description SDN_ROUTE

2、三层流量上Border后，在VSI口匹配VCFC自动下发的PBR。

interface Vsi-interface3

ip policy-based-route **SDN_300**

2、PBR会匹配ACL，并将下一跳设置为防火墙context内的租户承载网IP

policy-based-route **SDN_300** permit node 100

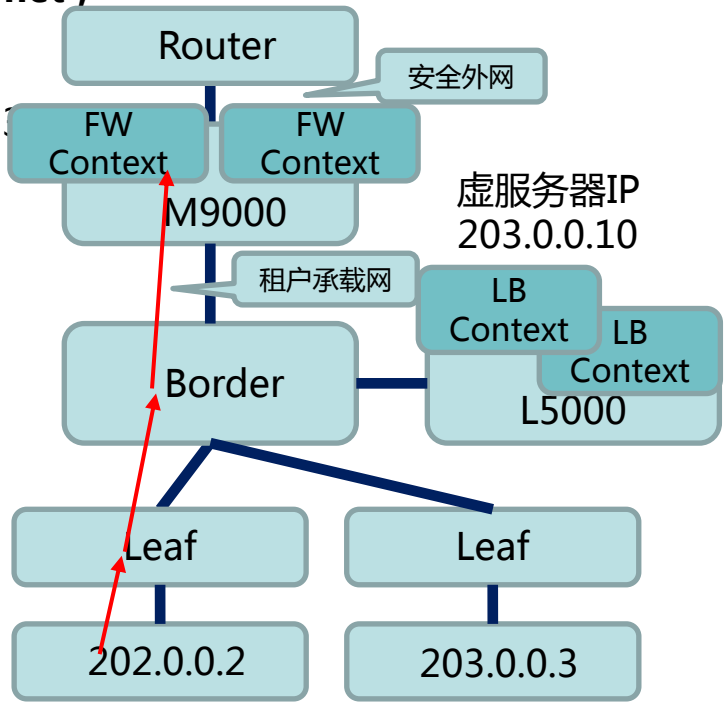
if-match acl name **SDN_ACL_FW_3000**

apply next-hop vpn-instance 3000 7.4.1.4

3、ACL匹配源sub网段：

acl advanced name **SDN_ACL_FW_3000**

rule 10001 permit ip vpn-instance 3000 source 203.0.0.0 0.0.0.255



东西向过防火墙负载均衡集中式网关流量示例

4、安全策略放通后，匹配控制器下发的虚IP主机路由，将流量送给负载均衡

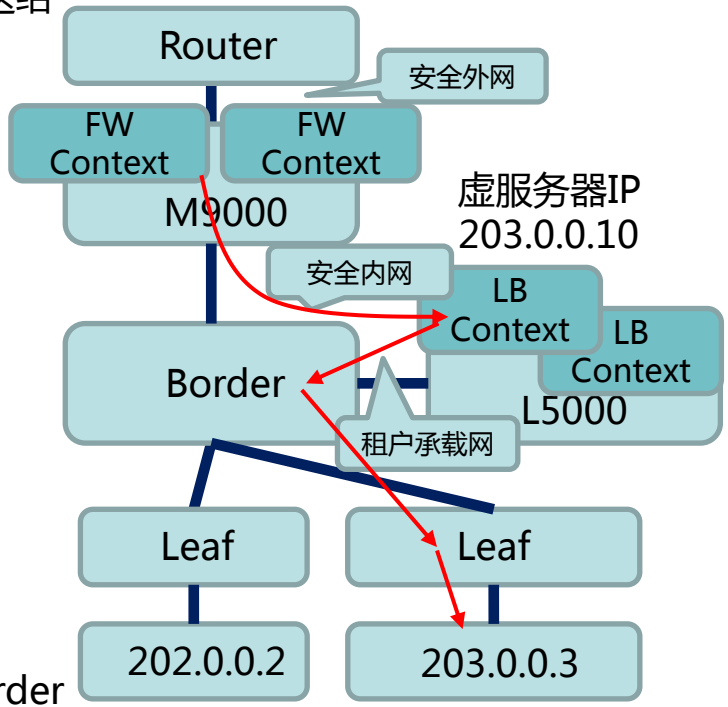
ip route-static vpn-instance 3000 203.0.0.10 32 **7.1.1.1**
description SDN_ROUTE//下一跳为LB安全内网IP

5、负载均衡上完成转换并生成会话：

Initiator:
  Source   IP/port: **202.0.0.2/28878**
  Destination IP/port: **203.0.0.10/22**
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: 3000/-/-
Inbound interface: Ten-GigabitEthernet1/0/25.302
Responder:
  Source   IP/port: 203.0.0.3/22
  Destination IP/port: 202.0.0.2/28878
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: 3000/-/-
Inbound interface: Ten-GigabitEthernet1/0/24.300
State: TCP_ESTABLISHED
Application: SSH

6、负载均衡匹配控制器下发的网段路由，将转换后报文送给Border

ip route-static vpn-instance 3000 203.0.0.0 24 **7.4.1.1**
description SDN_ROUTE//下一跳为租户承载网网关



东西向过防火墙负载均衡集中式网关流量示例

7、回程流量到达Border后，匹配VSI接口上PBR首先送往负载均衡

interface Vsi-interface4

ip policy-based-route **SDN_300**

PBR会匹配ACL，并将下一跳设置为负载均衡context内的租户承载网IP

policy-based-route **SDN_300** permit node 50

 if-match acl name **SDN_ACL_LB_3000**

 apply next-hop vpn-instance 3000 7.4.1.3

ACL匹配源sub网段：

acl basic name **SDN_ACL_LB_3000**

 description SDN_ACL_DEC_LB_3000

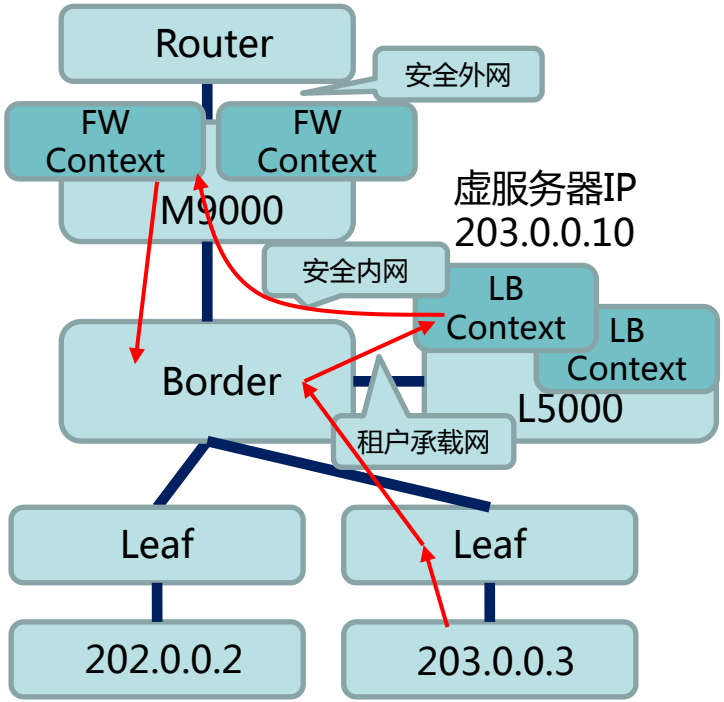
 rule 10000 permit vpn-instance 3000 source **203.0.0.3 0**

 rule 10001 permit vpn-instance 3000 source **203.0.0.4 0**

8、负载均衡上匹配会话，将流量送回防火墙context。

9、防火墙上匹配控制器下发的网段路由，将转换后报文送给Border

ip route-static vpn-instance 3000 202.0.0.0 24 7.4.1.1 description SDN_ROUTE//下一跳为租户承载网网关

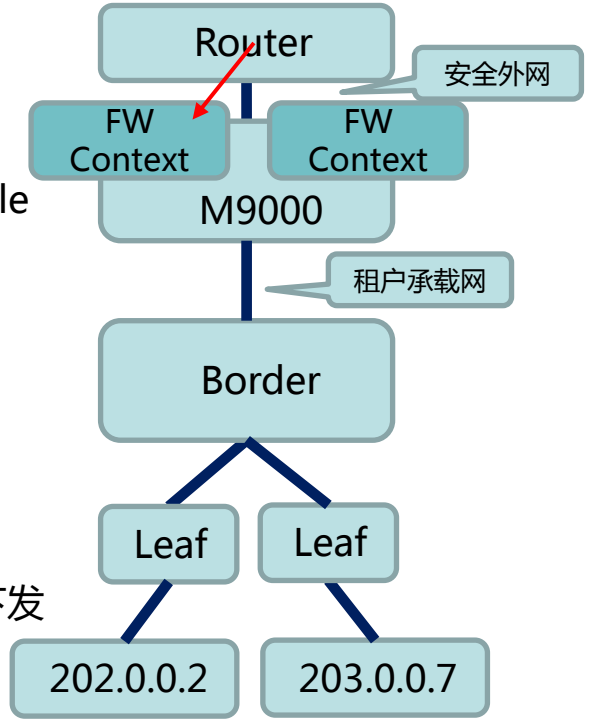


南北向过防火墙流量示例

- 南北向防火墙流量可选择是否使能**浮动IP**，如果不使能浮动IP，则需**南向主动访问北向**。
- 举例：外网4.1.1.1访问203.0.0.7，对应浮动IP为5.1.1.3

1、北向流量到达FW Context后，在外网口匹配静态NAT。

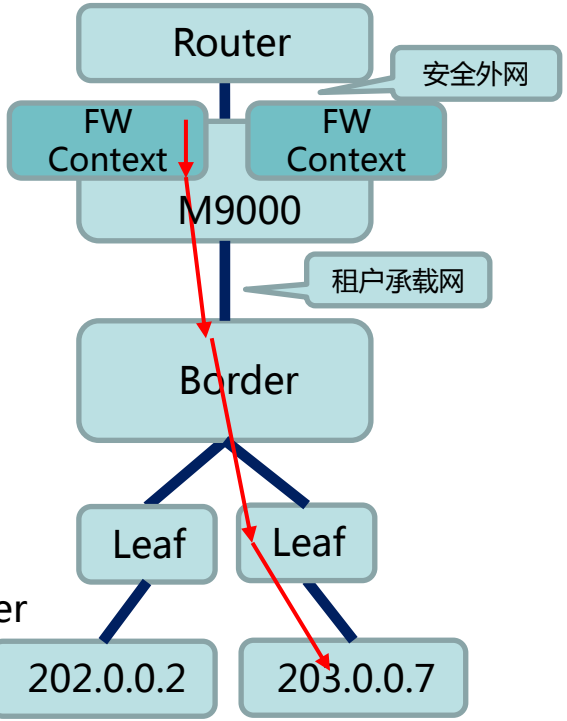
```
 nat static outbound 203.0.0.7 vpn-instance 3000 5.1.1.3
vpn-instance external_vpn acl name SDN_NAT_ACL_3000 reversible
//浮动IP NAT配置，将内网IP映射为外网IP 5.1.1.3
interface GigabitEthernet2/0/17
 description external
 ip binding vpn-instance external_vpn
 ip address 7.2.1.2 255.255.255.0  //安全外网IP
 ip address 7.7.1.1 255.255.255.0 sub //跨虚拟路由器互通网IP
 ospf 1 area 0.0.0.0
 nat outbound name SDN_NAT_ACL_3000 address-group name
SDN_ADDR_3000 vpn-instance external_vpn //外网网络使能SNAT下发
 nat static enable//用于浮动IP NAT的静态NAT
acl advanced name SDN_NAT_ACL_3000
rule 10000 permit ip vpn-instance 3000
//匹配ACL，用于内外到外网的访问
```



南北向过防火墙流量示例

2、防火墙Context上生成NAT 会话，完成地址转换和VPN转换

Initiator:
  Source IP/port: **7.2.1.1/699**
  Destination IP/port: **5.1.1.3/2048**
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: **external_vpn**/-/-
  Protocol: ICMP(1)
  Inbound interface: GigabitEthernet2/0/17
  Source security zone: EXTERNAL
Responder:
  Source IP/port: **203.0.0.7/699**
  Destination IP/port: **7.2.1.1/0**
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: **3000**/-/-
  Protocol: ICMP(1)
  Inbound interface: Ten-GigabitEthernet2/0/26.300
  Source security zone: T5ZKOYLFGTWEAJE3YF3QP22HCY
State: ICMP_REPLY
Application: ICMP



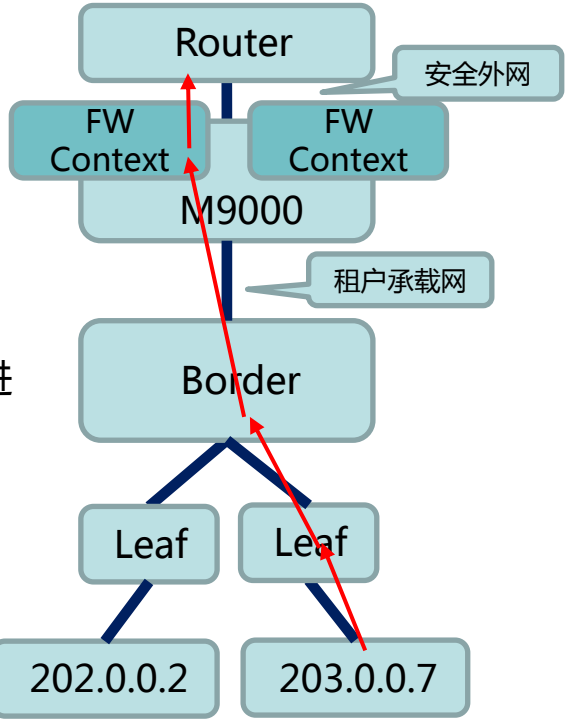
3、防火墙Context上匹配控制器下发的网段路由，将流量送给Border

ip route-static vpn-instance 3000 203.0.0.0 24 7.4.1.1 description SDN_ROUTE//下一跳为租户承载网网关IP

4、Border查询EVPN BGP主机路由进行转发

南北向过防火墙流量示例

5、回程流量匹配控制器下发的默认路由(通过EVPN发布给Leaf)，将流量送给Border，再匹配PBR流量送给防火墙Context
ip route-static vpn-instance 3000 0.0.0.0 0 7.4.1.4 description SDN_ROUTE//下一跳为FW租户承载网IP
6、防火墙上匹配NAT会话，完成VPN和地址转换后，匹配控制器下发的外网VPN静态路由将流量送回Router
ip route-static vpn-instance external_vpn 0.0.0.0 0 7.2.1.1 description SDN_ROUTE
//下一跳地址为安全外网网关IP
如果是南向北主动访问，则会匹配控制器下发的内网VPN静态路由进行VPN转换并将流量送给Router
ip route-static vpn-instance 3000 0.0.0.0 0 vpn-instance external_vpn 7.2.1.1 description SDN_ROUTE

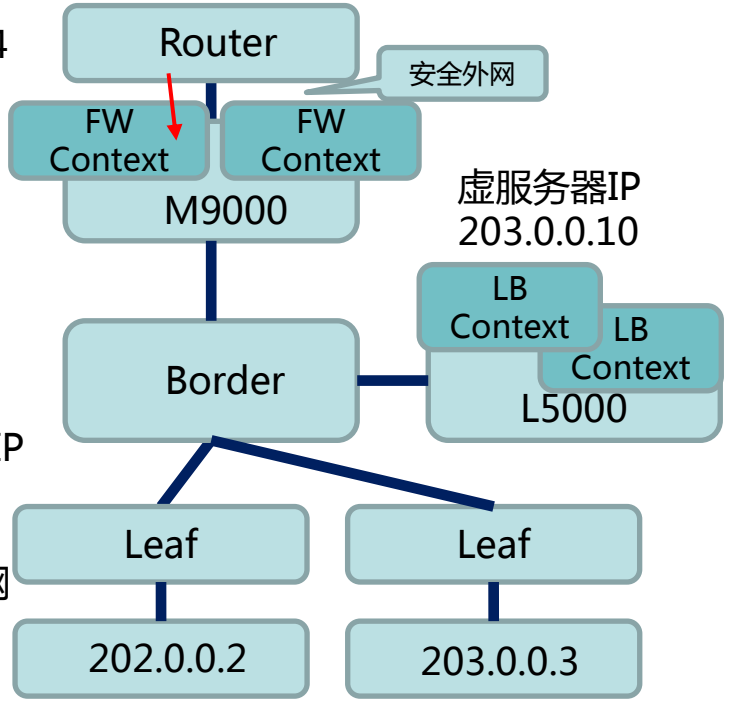


南北向过防火墙负载均衡流量示例

- 南北向防火墙流量可选择是否使能**浮动IP**，如果不使能浮动IP，则需**南向主动访问北向**。
- 举例：外网4.1.1.1访问虚IP 203.0.0.7，对应浮动IP为5.1.1.4

1、北向流量到达FW Context后，在外网口匹配静态NAT。

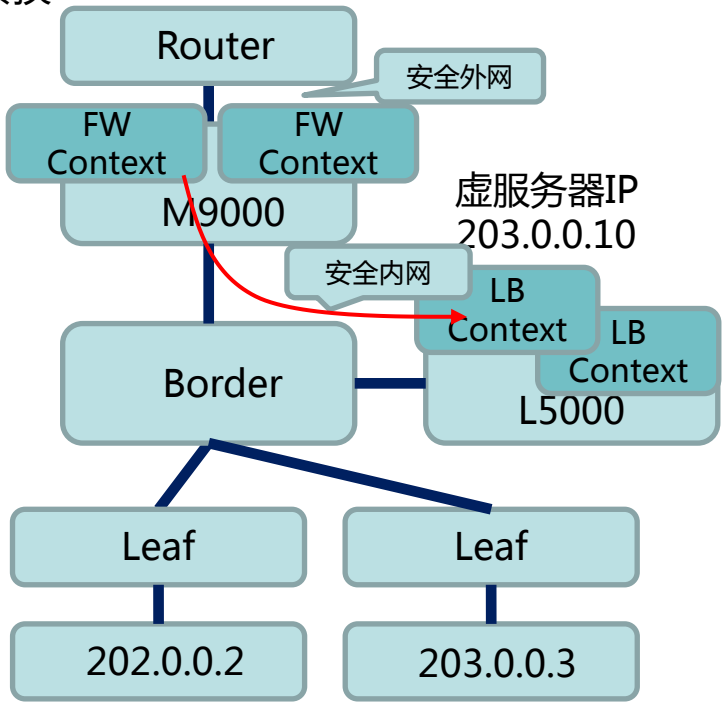
```
 nat static outbound 203.0.0.10 vpn-instance 3000 5.1.1.4
vpn-instance external_vpn acl name SDN_NAT_ACL_3000
reversible //浮动IP 静态NAT配置
interface GigabitEthernet2/0/17
 description external
 ip binding vpn-instance external_vpn
 ip address 7.2.1.2 255.255.255.0  //安全外网IP
 ip address 7.7.1.1 255.255.255.0 sub //跨虚拟路由器互通网IP
 ospf 1 area 0.0.0.0
 nat outbound name SDN_NAT_ACL_3000 address-group
name SDN_ADDR_3000 vpn-instance external_vpn //外网网络使能SNAT下发
 nat static enable//用于浮动IP NAT的静态NAT
```



南北向过防火墙负载均衡流量示例

2、防火墙Context上生成NAT 会话，完成地址转换和VPN转换

Initiator:
  Source IP/port: **4.1.1.1/13840**
  Destination IP/port: **5.1.1.4/22**
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: **external_vpn**/-/-
  Protocol: TCP(6)
  Inbound interface: GigabitEthernet2/0/17
  Source security zone: EXTERNAL
Responder:
  Source IP/port: **203.0.0.10/22**
  Destination IP/port: **4.1.1.1/13840**
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: **3000**/-/-
  Protocol: TCP(6)
  Inbound interface: Ten-GigabitEthernet2/0/26.302
  Source security zone: T5ZKOYLFGTWEAJE3YF3QP22HCY
State: TCP_ESTABLISHED
Application: SSH



3、防火墙Context上匹配控制器下发的主机路由，将流量送给LB Context

ip route-static vpn-instance 3000 203.0.0.10 32 7.1.1.1 description SDN_ROUTE//下一跳为LB Context安全内网IP

南北向过防火墙负载均衡流量示例

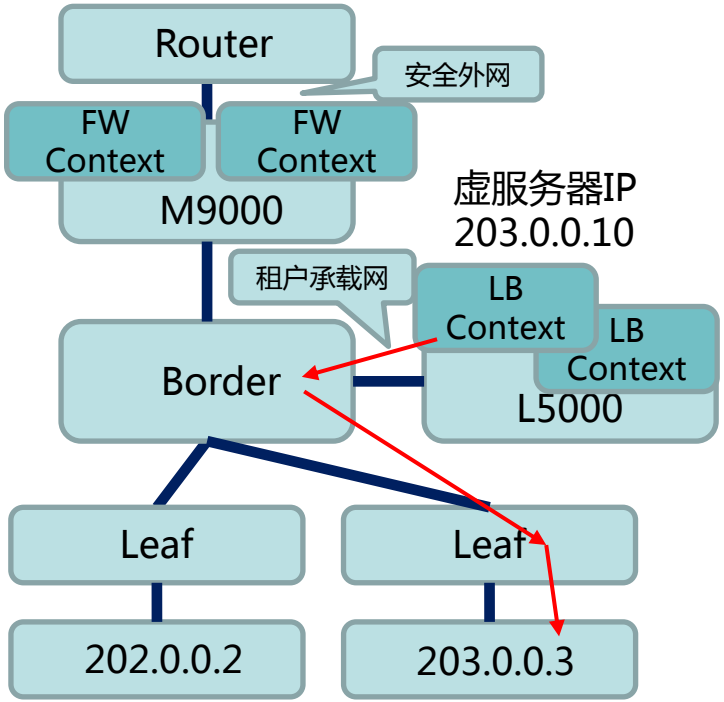
4、负载均衡上完成转换并生成会话：

Initiator:
  Source IP/port: **4.1.1.1/13840**
  Destination IP/port: **203.0.0.10/22**
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: **3000**/-/-
  Protocol: TCP(6)
  Inbound interface: Ten-GigabitEthernet1/0/25.302
Responder:
  Source IP/port: **203.0.0.4/22**
  Destination IP/port: **203.0.0.10/19160**
  DS-Lite tunnel peer: -
  VPN instance/VLAN ID/Inline ID: **3000**/-/-
  Protocol: TCP(6)
  Inbound interface: Ten-GigabitEthernet1/0/24.300
State: TCP_ESTABLISHED
Application: SSH

5、负载均衡匹配控制器下发的网段路由，将转换后报文送给Border

ip route-static vpn-instance 3000 203.0.0.0 24 **7.4.1.1** description SDN_ROUTE//下一跳为租户承载网网关

6、Border查询EVPN BGP主机路由进行转发



南北向过防火墙负载均衡流量示例

7、回程流量匹配控制器下发的主机路由(通过EVPN发布给Leaf)，将流量送给Border，匹配VSI接口上PBR首先送往负载均衡

interface Vsi-interface4
ip policy-based-route **SDN_300**

PBR会匹配ACL，并将下一跳设置为负载均衡context内的租户承载网IP

policy-based-route **SDN_300** permit node 50
 if-match acl name **SDN_ACL_LB_3000**
 apply next-hop vpn-instance 3000 7.4.1.3

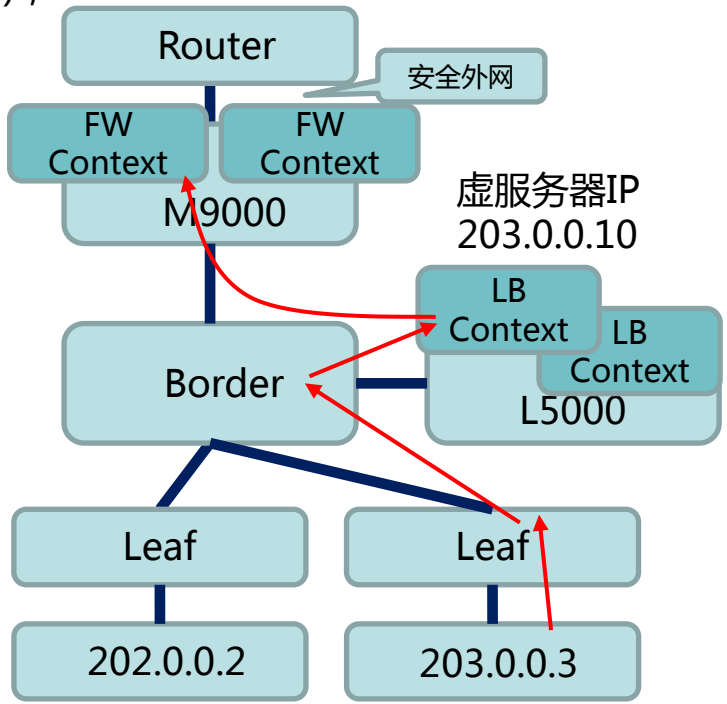
ACL匹配源sub网段：

acl basic name **SDN_ACL_LB_3000**
 description SDN_ACL_DEC_LB_3000
 rule 10000 permit vpn-instance 3000 source **203.0.0.3 0**

8、负载均衡上匹配会话，将流量送回防火墙context。

9、防火墙上匹配NAT会话，完成VPN和地址转换后，匹配控制器下发的外网VPN静态路由将流量送回Router

ip route-static vpn-instance external_vpn 0.0.0.0 0 7.2.1.1 description SDN_ROUTE
//下一跳地址为安全外网网关IP



安全纳管流量走向小结

- 东西向流量：
  - 在网关交换机上匹配源subnet策略路由，通过租户承载网向防火墙转发
  - 防火墙根据VCFC下发的安全策略放通流量，并根据静态主机路由，通过安全内网转发至负载均衡
  - 负载均衡根据VCFC下发的负载策略替换目的ip，并依据subnet静态路由，通过租户承载网发给Border的租户承载网关
  - 回程流量通过PBR上负载均衡
- 南北向流量：
  - 北向南流量报文先到防火墙做NAT，安全策略放通后，匹配主机静态路由，通过安全内网转发至负载均衡
  - 负载均衡策略替换目的ip后，匹配subnet静态路由通过租户承载网转发至租户承载网关
  - Border通过主机路由转发至虚机
  - 回程流量通过PBR上负载均衡

目录

EVPN安全纳管配置思路

- 规划各类网络好各个网络的地址范围、VLAN范围、接口连接、路由规划等
- 完成 Leaf、Border、Spine设备EVPN BGP和Underlay相关配置。
- 配置好M9K/F5K/L5K等安全硬件设备的Underlay相关配置和板卡模式。
- 完成虚拟机上线和Overlay二三层互通。
- M9K/F5K/L5K等安全硬件设备由VCFC NGFW Manager模块负责管理，VCFC通过NEM模块为租户申请网关资源或者服务资源。
- 为NGFWM模块添加硬件安全设备，配置资源池和每个资源池的配置模板。
- 在NEM模块网关组中添加服务网关组，配置相应的地址池和VLAN范围。
- 为租户创建服务资源，并在虚拟路由器上绑定服务资源，此时由VCFC创建好五张网络。
- 在网络服务里面配置防火墙和负载均衡相关策略,并由VCFC下发相关策略。

课程总结

- 熟悉EVPN安全纳管的基本组网
- 掌握EVPN安全纳管的流量原理
- 掌握EVPN安全纳管的配置思路

新IT解决方案领导者

THANK YOU

www.h3c.com

官方微信

官方微博