V7防火墙context资源配置注意事项

Context　刘宏宇　2019-10-28 发表

问题描述

V7防火墙context资源配置注意事项

解决方法

引擎组的划分　//针对M9K

（1）如果没有进驻安全引擎，即使Context已经启动，Context也没有实际运行的环境，无法运行业务。 //在进行资源划分的时候要注意至少保留一个安全引擎给根墙，否则会导致根墙和虚墙都无法转发

（2）Context进驻安全引擎组后，才能使用安全引擎组中安全引擎上的资源，包括CPU、磁盘和内存。

（3）一个Context只能进驻一个安全引擎组。在不同的Context下进驻同一个安全引擎组。

（4）自定义引擎组内划分单个blade或者一个failover组，分配给不同的context还可以规避引流的相关问题。

接口的划分

（1）物理接口可以独占或共享方式分配给某个Context。

（2）逻辑接口支持以共享方式分配给某个Context，不支持独占分配。 //不需要单独再把逻辑口所包含的物理口添加上去，如聚合口下成员端口

（3）三层聚合子接口也支持共享给某个Context，规划好vlan后，在根墙下分配好不同vlan tag的子接口，这样也有利于在根墙下维护各虚墙的配置。 //推荐如下配置方法，防止组播、广播风暴

（4）二层聚合共享口与vlan划分配合，不同context下的vlan不同，虚墙下通过vlan虚接口进行转发

context二层共享聚合口推荐配置

根墙

```
interface Bridge-Aggregation2
 description ith
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 40 to 41 44 to 45 50 52 to 54 60 to 65 71 74 to 75 87 89 1211 to 1212
 port trunk permit vlan 1214 1217 1231 2205 to 2207 2209
interface Bridge-Aggregation3
 description internal-network
 port link-type trunk
 undo port trunk permit vlan 1
 port trunk permit vlan 2 12 to 13 98 to 99 103 105 124 400 to 417 420 to 434 500 to 518 601 to 602
 port trunk permit vlan 651 701 to 705 801 to 814 3017 3035 to 3047 3093 to 3094 4011 4017 to 4018 4023 4025
 port trunk permit vlan 4037 to 4038 4058 to 4064 4091
"
context WBHJ id 13
 context start
 location blade-controller-team 1
 allocate interface Bridge-Aggregation2 to Bridge-Aggregation3 share
 allocate vlan 400 to 417
 allocate vlan 420 to 434
 allocate vlan 40 74 103 105 651 1212
"
```

```
context WBHJ id 13
 context start
 location blade-controller-team 1
 allocate interface Bridge-Aggregation2 to Bridge-Aggregation3 share
 allocate vlan 400 to 417
 allocate vlan 420 to 434
 allocate vlan 40 74 103 105 651 1212
"
```

虚墙

```
 interface Vlan-interface40
  description wbhj-to:dcn-8905-5&6
  ip address 132.122.35.4 255.255.255.248
  nat outbound 2004 address-group 6
  nat server protocol icmp global 132.122.226.10 inside 172.42.3.10
  nat server protocol icmp global 132.122.226.11 inside 172.42.3.11
```

Context三层共享聚合口

根墙

```
context mdc32 id 32
 description [安阳移动市场部]
 context start
 location blade-controller-team 1
 allocate interface Route-Aggregation1.2 share
 allocate interface Route-Aggregation1.3132 share
#
context mdc33 id 33
 description To-[林州大峡谷-OA]
 context start
 location blade-controller-team 1
 allocate interface Route-Aggregation1.3 share
 allocate interface Route-Aggregation1.3133 share
```

虚墙

```
interface Route-Aggregation1.2
 ip address 172.16.1.23 255.255.255.0
 nat server protocol tcp global 112.53.100.66 80 inside 10.10.12.66 80
 nat server protocol tcp global 112.53.100.66 2000 inside 10.10.12.66 3389
```