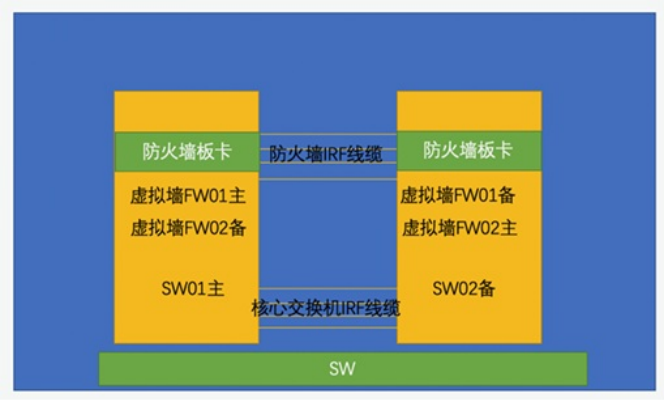
SecBlade IV NGFW防火墙插卡配置虚墙作为终端网关导致网速降低的经验案例

Context 叶靖 2020-03-25 发表

组网及说明

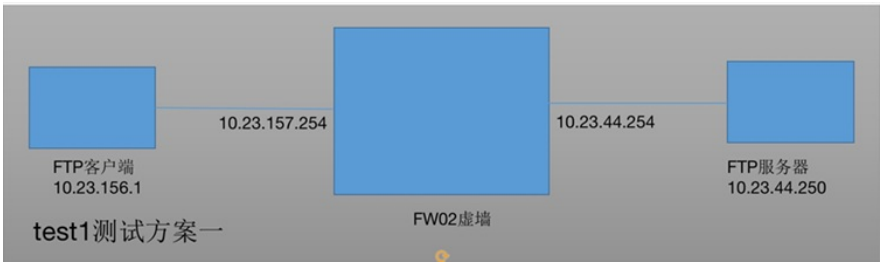
某局点购买了两台核心交换机和两台防火墙插卡(LSQM2FWDSC0)，现在每台核心交换机上都插了一块防火墙插卡,核心交换机和防火墙插卡都做了堆叠。然后现在还在防火墙上创建了两个虚墙FW01和FW02，每个虚墙都是采用冗余的方式进行配置。



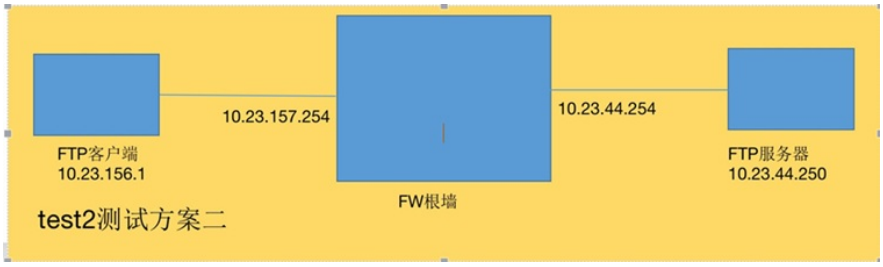
问题描述

现场对当前的网络情况进行测速，一共采用了两种组网进行测速，具体如下：

方案一：现场终端属于两个不同的网段，将终端的网关都放在在虚墙FW02上，这时通过终端windows共享文件复制的方式或者FTP下载的方式进行测速，测得网速大概在25MB/s



方案二：现场终端属于两个不同的网段，将终端的网关都放在防火墙根桥上，这时通过终端的windows共享文件复制的方式或者FTP下载的方式进行测试，测得网速大约为50MB/s（这时测得的速率是正常的）



经过多次测试，发现只要将终端的网关放在虚墙上，在这种组网下，内网终端之间互访的速率将会降

低。

过程分析

经过在实验室验证，将终端网关放在虚墙上，测得网速正常。

我们对比发现：在实验室测试的情况是采用物理口共享的方式，现场的配置冗余口的成员口是聚合子接口，然后将冗余口共享到context里。现场的配置大概如下：

```
#
context Admin id 1
#
context FW02 id 3
 context start
 allocate interface Reth101 to Reth103 share

#
interface Reth101
member interface Route-Aggregation1.101 priority 50
 member interface Route-Aggregation2.101 priority 100
#
interface Reth102
 member interface Route-Aggregation1.102 priority 50
 member interface Route-Aggregation2.102 priority 100
#
interface Reth103
member interface Route-Aggregation1.103 priority 50
 member interface Route-Aggregation2.103 priority 100
```

这种场景性能确实较低，这种场景研发以后尝试优化，实验室测试也复现了。

解决方法

现场可以将冗余口的成员口改成聚合口，然后配置冗余子接口共享到context里，下载速度差不多可达到根墙的速度。已经在实验室验证。

```
#
context Admin id 1
#
context FW01 id 2
 allocate interface Reth1.1 share
#
context FW02 id 3
 context start
 allocate interface Reth101.101 share
allocate interface Reth102.102 share
allocate interface Reth103.103 share

interface Reth101
member interface Route-Aggregation1 priority 50
 member interface Route-Aggregation2 priority 100
#
interface Reth102
 member interface Route-Aggregation1 priority 50
 member interface Route-Aggregation2 priority 100
#
interface Reth103
member interface Route-Aggregation1 priority 50
 member interface Route-Aggregation2 priority 100
#
interface Reth101.101
#
interface Reth102.102
#
interface Reth103.103
#
```