F1000-AK系列透明部署案例（命令行）

透明 zhiliao_8mkdB 2018-11-24 发表

组网及说明

1 配置需求或说明

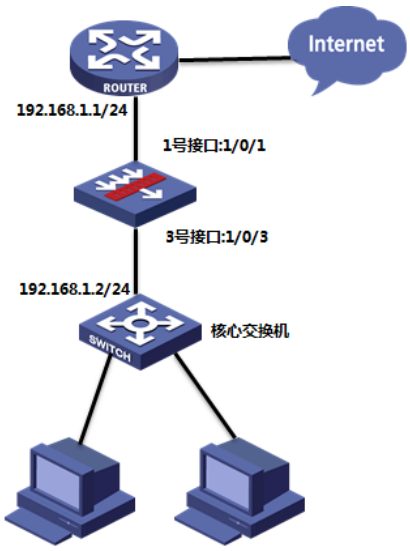
1.1 适用的产品系列

本案例适用于如F1000-AK180、F1000-AK170等F1000-AK系列的防火墙。

1.2 配置需求

如下组网图所示，在原有的网络中增加防火墙来提高网络安全性，但又不想对原有网络配置进行改动，所以需要防火墙采用透明模式部署；其中GigabitEthernet 1/0/1接口接原有路由器的下联口，GigabitEthernet 1/0/3接口接原有的交换机上联口。

2 组网图



配置步骤

3 配置步骤

3.1 配置连接路由器接口

#把1/0/1端口设置成二层模式

system-view

[H3C]interface GigabitEthernet 1/0/1

[H3C-GigabitEthernet1/0/1]port link-mode bridge

[H3C-GigabitEthernet1/0/1]quit

#将1/0/1端口加入到Untrust域

[H3C]security-zone name Untrust

[H3C-security-zone-Untrust]import interface GigabitEthernet1/0/1 vlan 1 to 4094

[H3C-security-zone-Untrust]quit

3.2 配置连接核心交换机接口

#把1/0/3端口设置成二层模式

[H3C]interface GigabitEthernet 1/0/3

[H3C-GigabitEthernet1/0/3]port link-mode bridge

[H3C-GigabitEthernet1/0/3]quit

#将1/0/3端口加入到Trust域

[H3C]security-zone name Trust

[H3C-security-zone-Trust]import interface GigabitEthernet1/0/3 vlan 1 to 4094

[H3C-security-zone-Trust]quit

3.3 配置连接核心交换机接口

#创建允许Trust访问Untrust的对象策略及规则

[H3C]object-policy ip Trust-Untrust

[H3C-object-policy-ip-Trust-Untrust]rule pass

[H3C-object-policy-ip-Trust-Untrust]quit

#放通源为Trust域，目的为Untrust的数据
[H3C]zone-pair security source Trust destination Untrust
[H3C-zone-pair-security-Trust-Untrust]object-policy apply ip Trust-Untrust
[H3C-zone-pair-security-Trust-Untrust]quit

3.4 保存配置
[H3C]save force

4 查看与验证
配置完成后终端可以上网，路由器和交换机不需要更改配置

配置关键点