1：虚拟防火墙

1.4 虚拟防火墙实验

1）实验拓扑

2）实验需求

2.1)首先完成交换网络的VLAN 和TRUNK 设置，保证连通性

2.2）ASA1 要求是HR 部分的主防火墙，ASA2 是备份  
 ASA2 要求是ENG 部分的主防火墙，ASA1 是备份

2.3）要求R1 R2 身后的网络可以自如的访问3.3.3.3

3）实验步骤

步骤1：完成所有路由器的配置

步骤2：完成交换机的VLAN 和TRUNK 设置

SW1

1 VLAN 10

2 VLAN 20

3 4 TRUNK

57 VLAN 22

68 VLAN 33

SW2

1 2 3 TRUNK

步骤3：防火墙上输入序列号，激活故障倒换和虚拟防火墙

activation-key 0x4a3ec071 0x0d86fbf6 0x7cb1bc48 0x8b48b8b0 0xf317c0b5

步骤4：将防火墙的模式切换到多模式

ciscoasa(config)# mode multiple

步骤5：将防火墙所有接口全部激活

不要命名，不要添加IP

步骤6：在防火墙上设置逻辑子接口

不添加IP

步骤7：完成虚拟防火墙配置

7.1 查看现存的虚拟防火墙信息

ciscoasa# show context

Context Name Class Interfaces URL

\*admin default disk0:/admin.cfg

Total active Security Contexts: 1

!!注意

系统自建的ADMIN 虚拟防火墙实际上是用来管理所有其它虚拟防火墙的

7.2 创建虚拟防火墙

ASA1/ ASA2

context ENG

allocate-interface GigabitEthernet0.100 outside

allocate-interface GigabitEthernet1.10 inside

config-url disk0:/ENG.cfg

!

context SALE

allocate-interface GigabitEthernet0.200 outside

allocate-interface GigabitEthernet1.20 inside

config-url disk0:/SALE.cfg

7.3 进入虚拟防火墙完成防火墙常规配置

ASA1 ENG 虚拟防火墙

!

hostname ENG

!

interface inside

nameif inside

security-level 100

ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2

!

interface outside

nameif outside

security-level 0

ip address 100.100.100.1 255.255.255.0 standby 100.100.100.2

!

object network INSIDE

subnet 10.1.1.0 255.255.255.0

object-group network G

network-object object INSIDE

nat (inside,outside) source dynamic G interface

access-list FO extended permit icmp any any echo-reply

access-group FO in interface outside

route outside 0.0.0.0 0.0.0.0 100.100.100.3 1

route inside 10.1.1.0 255.255.255.0 192.168.1.3 1

ASA1 SALE

!

hostname SALE

!

interface inside

nameif inside

security-level 100

ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2

!

interface outside

nameif outside

security-level 0

ip address 200.200.200.1 255.255.255.0 standby 200.200.200.2

!

object network INSIDE

subnet 20.2.2.0 255.255.255.0

object-group network G

network-object object INSIDE

nat (inside,outside) source dynamic G interface

access-list FO extended permit icmp any any echo-reply

access-group FO in interface outside

route outside 0.0.0.0 0.0.0.0 200.200.200.3

route inside 20.2.2.0 255.255.255.0 192.168.2.3

此时R1 R2 带着源PING 3.3.3.3 流量经过ASA 1 的两个虚拟防火墙都是可达的。

7.4 故障倒换的配置，实现虚拟防火墙的AA 故障倒换

！！注意

故障倒换并不是配置在自创的虚拟防火墙下的，

是在ADMIN 下配置

ASA1

failover lan unit primary

failover lan interface LAN GigabitEthernet2

failover link LINK GigabitEthernet3

failover interface ip LAN 172.16.12.1 255.255.255.0 standby 172.16.12.2

failover interface ip LINK 172.16.21.1 255.255.255.0 standby 172.16.21.2

failover group 1

preempt

failover group 2

secondary

preempt

!

context ENG

join-failover-group 1

context SALE

join-failover-group 2

ASA2

failover lan unit secondary

failover lan interface LAN GigabitEthernet2

failover link LINK GigabitEthernet3

failover interface ip LAN 172.16.12.1 255.255.255.0 standby 172.16.12.2

failover interface ip LINK 172.16.21.1 255.255.255.0 standby 172.16.21.2

7.5 启用故障倒换，确认A/A 模式虚拟防火墙工作

ASA1 ASA 2

(config)# failover

此时校验是否实现了A/A

ASA1

ciscoasa# show failover

……………………………………

This host: Primary

**Group 1 State: Active**

**Active time: 86 (sec)**

**Group 2 State: Standby Ready**

**Active time: 0 (sec)**

………………………………………………

ASA2

ciscoasa# show failover

………………………………

**This host: Secondary**

**Group 1 State: Standby Ready**

**Active time: 0 (sec)**

**Group 2 State: Active**

**Active time: 126 (sec)**

……………………………………