本电子书由CyberArticle制作。点击这里下载CyberArticle。注册版本不会显示该信息。 删除广告

防火墙透明部署案例

目录

1 配置需求或说明

1.1 适用的产品系列

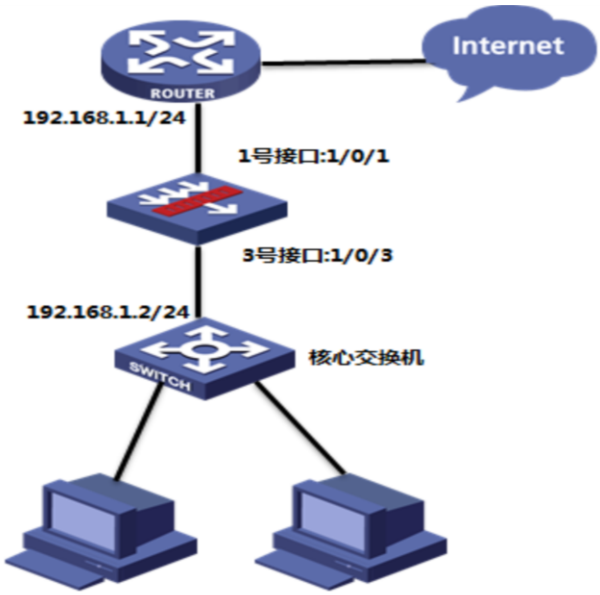
本案例适用于软件平台为Comware V7系列防火墙 ： F100-X-G2、F1000-X-G2、F100-WiNet、F1000-AK、F10X0等

注：本案例是在F100-C-G2的Version 7.1.064, Release 9510P08版本上进行配置和验证的。

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



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

```
<H3C>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
```

3.1 安全策略配置

防火墙目前版本存在两套安全策略，请在放通安全策略前确认设备运行那种类型的安全策略？以下配置任选其一。

1. 通过命令“display cu | in security-policy”如果查到命令行存在“security-policy disable”或者没有查到任何信息，则使用下面策略配置。

[H3C]display cu | in security-policy
security-policy disable

配置安全策略将Trust到Untrust域内网数据放通

#创建对象策略pass。

```
[H3C]object-policy ip pass
[H3C-object-policy-ip-pass] rule 0
pass
[H3C-object-policy-ip-pass]quit
```

创建Trust到Untrust域的域间策略调用pass策略。

```
[H3C]zone-pair security source Trust
```

```
destination Untrust
[H3C-zone-pair-security-Trust-
Untrust]object-policy apply ip pass
[H3C-zone-pair-security-Trust-
Untrust]quit
```

配置安全策略将Trust到Local域、Local到Trust、Local到Untrust域数据全放通策略

#创建Trust到Local域的域间策略调用pass策略。

```
[H3C]zone-pair security source Trust
destination Local
[H3C-zone-pair-security-Trust-Local]
object-policy apply ip pass
[H3C-zone-pair-security-Trust-Local]
quit
```

#创建Local到Trust域的域间策略调用pass策略。

```
[H3C]zone-pair security source Local
destination Trust
[H3C-zone-pair-security-Local-Trust]
object-policy apply ip pass
[H3C-zone-pair-security-Local-Trust]
quit
```

#创建Local到Untrust域的域间策略调用pass策略。

```
[H3C]zone-pair security source Local
destination Untrust
```

```
[H3C-zone-pair-security-Local-
Untrust]object-policy apply ip pass
[H3C-zone-pair-security-Local-
Untrust]quit
```

2. 通过命令“display cu | in security-policy”如果查到命令行存在“security-policy ip”并且没有查到“security-policy disable”，则使用下面策略配置。

```
[H3C]display cu | in security-policy
security-policy ip
```

创建安全策略并放通local到trust和trust到local的安全策略。

```
[H3C]security-policy ip
[H3C-security-policy-ip]rule 10 name
test
[H3C-security-policy-ip-10-test]
action pass
[H3C-security-policy-ip-10-test]
source-zone local
[H3C-security-policy-ip-10-test]
source-zone Trust
[H3C-security-policy-ip-10-test]
source-zone Untrust
```

```
[H3C-security-policy-ip-10-test]
destination-zone local
[H3C-security-policy-ip-10-test]
destination-zone Trust
[H3C-security-policy-ip-10-test]
destination-zone Untrust
[H3C-security-policy-ip-10-test]quit
```

3.4保存配置

```
<H3C>save force
```

3.5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