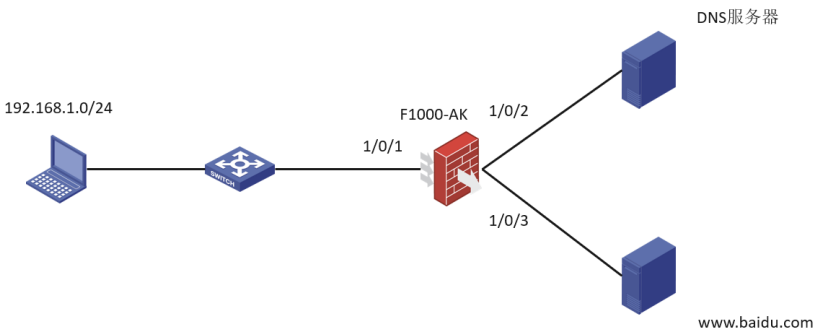
F1000-AK （版本V7 R8860P18）基于域名的安全策略配置案例

域间策略/安全域　zhiliao_VSoivy　2022-04-19 发表

组网及说明

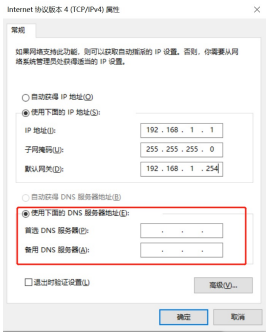


现场需要实现：限制网段为192.168.1.0/24的终端访问百度

配置步骤

1.终端和设备配置相同的DNS服务器

电脑侧：



2.设备侧配置

（1）配置接口IP地址

根据组网规划的信息，配置各接口的IP地址

（2） 配置接口加入安全域

创建安全域，并将接口加入对应的安全域

```
 security-zone name trust
   import interface gigabitethernet 1/0/1
security-zone name dns
   import interface gigabitethernet 1/0/2
security-zone name baidu
   import interface gigabitethernet 1/0/3
```

（3）配置对象

创建名为baidu的IP地址对象组，并定义其主机名称为www.baidu.com

```
object-group ip address baidu
   network host name www.baidu.com
```

（4）配置DNS服务器地址

指定DNS服务器的IP地址为114.114.114.114，确保设备可以获取到主机名对应的IP地址

```
 dns server 114.114.114.114
```

（5）配置安全策略

配置名称为dns的安全策略规则，允许设备访问DNS服务器

```
security-policy ip
  rule name dns
  source-zone local
  destination-zone dns
  destination-ip-host 114.114.114.114
  action pass
```

配置名称为host-dns的安全策略规则，允许内网主机访问DNS服务器

```
rule name host-dns
   source-zone trust
   destination-zone dns
   destination-ip-host 114.114.114.114
   service dns-udp
   action pass
```

配置名称为host-baidu的安全策略规则，禁止192.168.1.0/24的主机访问百度

```
 rule name host-baidu
   source-zone host
   destination-zone baidu
   source-ip-subnet 192.168.1.0 24
   destination-ip baidu
   action drop
```

（6）配置dns snooping ，此配置在新版本中必须配置

```
dns snooping enable
```

配置关键点

1.终端和设备侧配置同一个DNS服务器

2.8860P13及之后版本要配置dns snooping，并且不能配置dns代理

配置dns snooping需要注意：

1）DNS Snooping设备只有位于DNS客户端与DNS服务器之间，或DNS客户端与DNS代理设备之间时，DNS Snooping功能配置后才能正常工作。

2）DNS Snooping功能和DNS源地址透明代理功能不能同时使用。

说明：DNS Snooping功能适用于基于域名过滤用户流量的场景。基于域名过滤用户流量时，需要获取域名对应的IP地址才能真正实现流量过滤。开启DNS Snooping功能后，设备会监听过路的DNS请求报文和DNS应答报文，如果DNS请求报文中的域名与过滤规则中的域名相同，设备会在收到该域名的响应报文时记录域名解析结果，并上报给过滤规则，使得过滤规则可以基于此域名对应的IP地址实现流量过滤。如果DNS请求报文中的域名与过滤规则中的域名不同，设备不会记录域名解析结果。