

第一阶段-FW 评分标准

9. 为实现对防火墙的安全管理，在防火墙 DCFW 的 Trust 安全域开启 PING, HTTP, SNMP 功能（loopback 接口除外），Untrust 安全域开启 SSH、HTTPS 功能；

共 8 分，共 6 处。

1.1 分

接口配置

常规 属性 高级 RIP

名称: aggregate1.111

描述: (0~63)字符

绑定安全域: ☒ 三层安全域 ☐ 二层安全域 ☐ 无绑定

安全域: trust

IP配置

类型: ☒ 静态IP ☐ 自动获取IP ☐ PPPoE

IP地址: 10.1.0.254

网络掩码: 255.255.255.0

☐ 启用DNS代理 ☒ 代理 ☐ 透明代理

高级选项... DHCP... DDNS...

管理方式

☐ Telnet ☐ SSH ☒ Ping ☒ HTTP ☐ HTTPS ☒ SNMP

路由

逆向路由: ☐ 启用 ☐ 关闭 ☒ 自动

确定 取消

2.1 分

接口配置

常规

属性

高级

RIP

名称:

aggregate1.112

描述:

(0~63)字符

绑定安全域:

☒ 三层安全域

☐ 二层安全域

☐ 无绑定

安全域:

trust

IP配置

类型:

☒ 静态IP

☐ 自动获取IP

☐ PPPoE

IP地址:

10.2.0.254

网络掩码:

255.255.255.0

☐ 启用DNS代理

☒ 代理

☐ 透明代理

高级选项...

DHCP...

DDNS...

管理方式

☐ Telnet

☐ SSH

☒ Ping

☒ HTTP

☐ HTTPS

☒ SNMP

路由

逆向路由:

☐ 启用

☐ 关闭

☒ 自动

确定

取消

3.1 分

接口配置

常规

属性

高级

RIP

名称:

ethernet0/3

描述:

(0~63)字符

绑定安全域:

☒ 三层安全域

☐ 二层安全域

☐ 无绑定

安全域:

trust

IP配置

类型:

☒ 静态IP

☐ 自动获取IP

☐ PPPoE

IP地址:

10.3.0.254

网络掩码:

255.255.255.252

☐ 启用DNS代理

☒ 代理

☐ 透明代理

高级选项...

DHCP...

DDNS...

管理方式

☐ Telnet

☐ SSH

☒ Ping

☒ HTTP

☐ HTTPS

☒ SNMP

路由

逆向路由:

☐ 启用

☐ 关闭

☒ 自动

确定

取消

4.1 分

接口配置

常规属性高级RIP

名称：

ethernet0/4

描述：

(0~63)字符

绑定安全域：

三层安全域

二层安全域

无绑定

安全域：

trust

IP配置

类型：

静态IP

自动获取IP

PPPoE

IP地址：

10.4.0.254

网络掩码：

255.255.255.252

启用DNS代理

代理

透明代理

高级选项...

DHCP...

DDNS...

管理方式

Telnet

SSH

Ping

HTTP

HTTPS

SNMP

路由

逆向路由：

启用

关闭

自动

确定

取消

5.2 分

接口配置

常规属性高级RIP

名称：

ethernet0/5

描述：

(0~63)字符

绑定安全域：

三层安全域

二层安全域

无绑定

安全域：

untrust

IP配置

类型：

静态IP

自动获取IP

PPPoE

IP地址：

10.100.18.1

网络掩码：

255.255.255.224

启用DNS代理

代理

透明代理

高级选项...

DHCP...

DDNS...

管理方式

Telnet

SSH

Ping

HTTP

HTTPS

SNMP

路由

逆向路由：

启用

关闭

自动

确定

取消

6.2 分

接口配置

常规 属性 高级 RIP

名称: ethernet0/6

描述: (0~63)字符

绑定安全域: ☒ 三层安全域 ☐ 二层安全域 ☐ 无绑定

安全域: untrust

IP配置

类型: ☒ 静态IP ☐ 自动获取IP ☐ PPPoE

IP地址: 200.1.1.1

网络掩码: 255.255.255.0

☐ 启用DNS代理 ☒ 代理 ☐ 透明代理

高级选项... DHCP... DDNS...

管理方式

☐ Telnet ☒ SSH ☐ Ping ☐ HTTP ☒ HTTPS ☐ SNMP

路由

逆向路由: ☒ 启用 ☐ 关闭 ☐ 自动

确定 取消

10. 总部 VLAN 业务用户通过防火墙访问 Internet 时，复用公网 IP: 200.1.1.28/30, 保证每一个源 IP 产生的所有会话将被映射到同一个固定的 IP 地址，当有流量匹配本地址转换规则时产生日志信息，将匹配的日志发送至 10.52.0.100 的 UDP 2000 端口；

共 10 分，共 2 处。

1.5 分

新建

编辑

删除

优先级

优先级排序

导出 NAT444 静态映射

ID	源地址(原始)	目的地址(原始)	服务	出接口 / 下一跳虚拟路由器	转换为	模式	HA 组	日志
1	Any	Any		所有流量	200.1.1.28/30	动态端口-Sticky	0	开启

2.5 分

日志服务器配置

主机名称：

10.52.0.100

(A.B.C.D)/(1~255)字符

绑定方式：

☒ 虚拟路由器：

trust-vr

☐ 源接口：

协议：

UDP

端口：

2000

(1~65535),缺省值: 514

日志类型：

☐ 事件日志

☐ 配置日志

☐ 安全日志

☐ 网络日志

☐ 会话日志

☒ NAT日志

☐ 上网日志

☐ 调试日志

☐ NBC日志

确定

取消

11. 远程移动办公用户通过专线方式接入总部网络，在防火墙 DCFW 上配置，采用 SSL 方式实现仅允许对内网 VLAN 30 的访问，用户名密码均为 DCN2021，地址池参见地址表；

共 10 分，共 2 处。

1.5 分

网络信息

DCN | DigitalChina Secure Connect

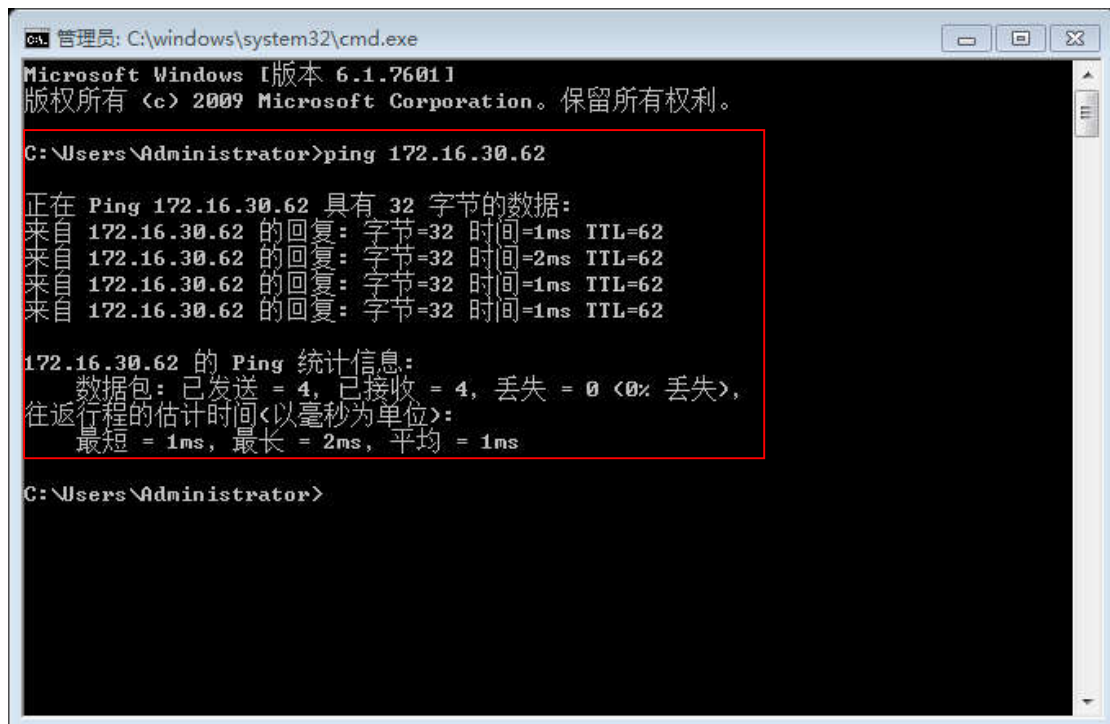
统计接口路由

本地路由

目的地址	子网掩码	网关	接口	距离
0.0.0.0	0.0.0.0	192.168.10.1	192.168.10.2	1
192.168.10.0	255.255.255.0	192.168.10.2	192.168.10.2	257
192.168.10.2	255.255.255.255	192.168.10.2	192.168.10.2	257
192.168.10.255	255.255.255.255	192.168.10.2	192.168.10.2	257
224.0.0.0	240.0.0.0	192.168.10.2	192.168.10.2	257
255.255.255.255	255.255.255.255	192.168.10.2	192.168.10.2	257

确定

2.5 分



The image shows a Windows command prompt window titled "管理员: C:\windows\system32\cmd.exe". The window displays the output of a ping command to the IP address 172.16.30.62. The output indicates that the ping was successful, with four packets sent and received, and a 0% loss rate. The round-trip times are listed as 1ms, 2ms, 1ms, and 1ms. The statistics section shows a minimum of 1ms, a maximum of 2ms, and an average of 1ms. The command prompt is running as Administrator, and the user is Administrator.

```
管理员: C:\windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
版权所有 (c) 2009 Microsoft Corporation。保留所有权利。

C:\Users\Administrator>ping 172.16.30.62

正在 Ping 172.16.30.62 具有 32 字节的数据:
来自 172.16.30.62 的回复: 字节=32 时间=1ms TTL=62
来自 172.16.30.62 的回复: 字节=32 时间=2ms TTL=62
来自 172.16.30.62 的回复: 字节=32 时间=1ms TTL=62
来自 172.16.30.62 的回复: 字节=32 时间=1ms TTL=62

172.16.30.62 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 1ms, 最长 = 2ms, 平均 = 1ms

C:\Users\Administrator>
```

12. 为了保证带宽的合理使用，通过流量管理功能将引流组应用数据流，上行最小带宽设置为 2M，下行最大带宽设置为 4M; 为净化上网环境，要求在防火墙 DCFW 做相关配置，禁止无线用户周一至周五工作时间 9：00-18：00 的邮件内容中含有“病毒”、“赌博”的内容，且记录日志；

共 8 分，共 6 处。

1.1 分

QoS配置

限流对象：

接口

ethernet0/6

所属安全域为untrust

应用QoS

IP QoS

白名单：

IP范围

起始IP

终止IP

时间表：

添加

删除

确定

取消

新建

编辑

删除

启用

禁用

优先级

提示:调整优先级请先选择接口/安全域

	绑定接口/安全域	规则名称	状态	匹配条件	带宽控制(Kbps)	细粒度控制
<input type="checkbox"/>	ethernet0/6	净网		应用: 引流组	下行最大带宽:4,000Kbps 上行最小带宽:2,000Kbps	

2.1 分

地址簿

名称

成员IP

描述:

搜索

清空

新建

编辑

删除

	地址簿名称	成员	描述
<input type="checkbox"/>	ipv4.loopback3_subnet	10.13.0.1/24	
<input type="checkbox"/>	ipv4.loopback4	10.14.0.1/32	
<input type="checkbox"/>	ipv4.loopback4_subnet	10.14.0.1/24	
<input type="checkbox"/>	ipv4.tunnel1	192.168.10.1/32	
<input type="checkbox"/>	ipv4.tunnel1_subnet	192.168.10.1/24	
<input type="checkbox"/>	VLAN30	172.16.30.0/26	
<input checked="" type="checkbox"/>	无线用户	10.80.1.0/26, 10.80...	

第 2 页, 总页数 2

每页显示条目数 20

显示表项 21 - 27 总数为 27

详情

关联项

地址簿名称:

无线用户

地址簿成员:

10.80.1.0/26, 10.80.0.0/24

描述:

3.1 分

时间表选择

新建

编辑

	名称	活跃	周期计划	时间范围
<input checked="" type="checkbox"/>	无线	非活跃	星期一 星期二 星期三 星期四 星期五 09:00 到 18:00	

第 1 页, 总页数 1

每页显示条目数 20

显示表项 1 - 1 总数为 1

时间表详情

时间表:

状态:

周期计划:

绝对计划:

确定

取消

4.1 分

关键字类别配置

类别名称: 无线

新建

删除

<input type="checkbox"/>	关键字	类型	信任值
<input type="checkbox"/>	赌博	完全匹配	100
<input type="checkbox"/>	病毒	完全匹配	100

确定

取消

5.2 分

邮件内容

系统会对内容含有如下关键字的邮件做指定控制

新建

编辑

关键字类别	<input type="checkbox"/> 阻止发送	<input type="checkbox"/> 记录日志
无线	<input type="checkbox"/>	<input checked="" type="checkbox"/>

确定

取消

6.2 分

邮件过滤规则配置

名称：

无线

当满足以下条件时

目的安全域：

untrust

用户：

无线

时间表：

无线

配置

配置

做如下控制

控制类型：

☐ 所有邮件

☒ 指定邮件控制内容

控制动作：

☐ 阻断/审计发件人

☐ 阻断/审计收件人

☒ 阻断/审计邮件内容

上述配置外邮件：

☐ 阻止发送

☐ 记录日志

例外

确定

取消