H3C SecPath M9000 系列多业务安全网关

开局指导书

目 录

1 简述 1
1.1 产品介绍 1
1.2 系统介绍 1
1.2.1 M9000-AI-E 系列外观介绍 1
1.2.2 系统结构介绍 2
1.2.3 M9000 的管理 3
2 M9000-AI-E 系列的硬件限制和版本升级 4
2.1 硬件说明 4
2.2 版本升级的内容 7
2.3 M9000-AI-E8 主控升级过程 8
2.4 M9000-AI-E8 业务板升级过程 8
2.5 注意事项 14
3 防火墙基础配置 14
3.1 防火墙的几个基本概念 14
3.1.1 安全域 14
3.1.2 流和会话 14
4 M9000 系列多业务安全网关的远程管理概述 15
5 典型组网 16
5.1 IRF 和冗余组 16
5.1.1 组网需求 16
5.1.2 配置思路 16
5.1.3 配置步骤 17
5.2 注意事项 22
6 M9000 的安全策略基本配置 22
6.1 组网需求 27
6.2 配置思路 27
6.3 配置步骤 27
6.4 注意事项 28
7 M9000 的 NAT 基本功能 28
7.1 组网需求 28
7.2 配置思路 29
7.3 配置步骤 29

7.4 注意事项 30
8 内网用户通过 NAT 访问外网（静态地址转换） 31
8.1 组网需求 31
8.2 配置思路 31
8.3 配置步骤 31
8.4 注意事项 32
9 SSL VPN 32
9.1 SSL VPN 简介 32
9.2 配置 IP 接入方式 32
9.2.1 组网需求 32
9.2.2 配置思路 33
9.2.3 配置步骤 33
9.2.4 登录和注意事项 34
10 串行部署- IPS 模式基本功能 36
10.1 组网需求 36
10.2 配置思路 36
10.3 配置步骤 36
10.4 注意事项 38
11 AV 病毒防护基本功能 39
11.1 组网需求 39
11.2 配置思路 39
11.3 配置步骤 39
11.4 注意事项 41
12 M9000 的 VRRP+RBM 基本功能 22
12.1 组网需求 22
12.2 配置思路 23
12.3 配置步骤 23
12.4 注意事项 26
13 日志 41
13.1 日志简介 41
13.2 配置发送 syslog 日志 42
13.3 配置发送 customlog 日志 42
13.3.1 配置需求 42
13.3.2 配置思路 42
13.3.3 配置步骤 42

13.3.4 日志结果分析 ····· 43
13.4 配置发送 Userlog 日志 ····· 43
13.4.1 组网需求 ····· 43
13.4.2 配置思路 ····· 44
13.4.3 配置步骤 ····· 44
13.4.4 日志结果及分析 ····· 44
13.5 配置发送 Session 日志 ····· 45
13.5.1 组网需求 ····· 45
13.5.2 配置思路 ····· 45
13.5.3 配置步骤 ····· 45
13.5.4 日志结果及分析 ····· 45
13.6 注意事项 ····· 46

1 简述

1.1 产品介绍

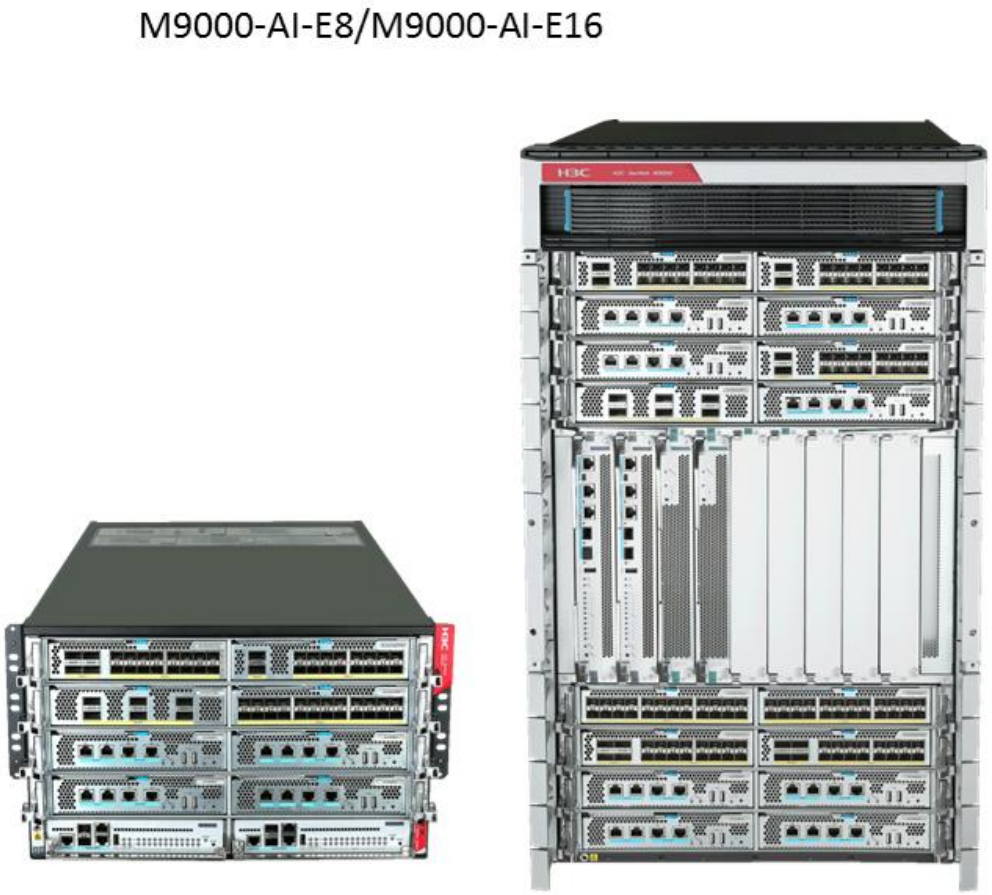
H3C SecPath M9000 系列多业务安全网关是 H3C 公司结合云计算、IPv6、大数据及高性能计算的发展趋势，针对云计算数据中心、运营商 CGN、大型企业及园区网出口等市场推出的新一代高性能多业务安全网关。

1.2 系统介绍

1.2.1 M9000-AI-E 系列外观介绍

H3C SecPath M9000 系列多业务安全网关包括 M9000 产品（M9006、M9010 和 M9014 三款产品）和 M9000-S 产品（M9008-S 和 M9012-S 两款产品）以及 M9000-AI-E 产品（M9000-AI-E16 和 M9000-AI-E8 两款产品），在不区分具体型号时，后续章节统称为 M9000 系列设备。M9000 产品特指 M9006、M9010 和 M9014 三款产品，M9000-S 产品特指 M9008-S 和 M9012-S 款产品。M9000-AI-E 产品特指 M9000-AI-E16 和 M9000-AI-E8 两款产品，下图 1-1 主要介绍 M9000-AI-E 的设备外观。

图1-1 M9000-AI-E 设备外观



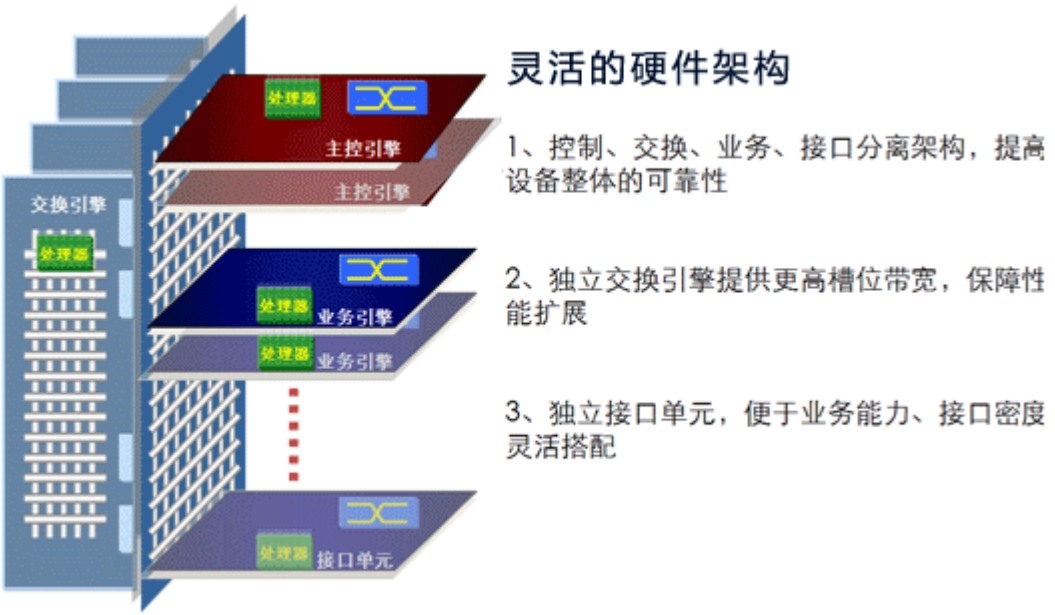
M9000/M9000-AI-E 产品主要由主控板区、接口板和业务板区、网板区、电源区、风扇区等几个部分组成，M9000-S 产品主要由主控板区、接口板和业务板区、电源区、风扇区等几个部分组成。

1.2.2 系统结构介绍

H3C SecPath M9000 系列多业务安全网关充分考虑网络应用对高可靠性的要求，采用领先的多核全分布式架构。主控引擎 1+1 冗余，提供整机统一配置管理，支持安全集群；业务引擎和接口单元支持混插，可以根据性能需求灵活进行选择；风扇模块冗余，风扇框支持风扇状态监控，风扇支持无级调速，可以根据环境温度、单板配置自动分组调速；电源模块 M+N 备份，交、直流电源模块支持热插拔，多电源模块负载分担，可灵活根据系统功耗配置模块数量，保证模块高效工作。设备所有单元均支持热插拔，充分满足网络维护、升级、优化的需求。

M9000 采用控制、业务、数据相分离的全分布式架构，控制引擎、交换引擎、业务引擎及接口单元硬件分离，解耦合系统关键部件，提高系统可靠性；独立的硬件交换引擎，支撑高性能安全业务无阻塞处理及转发。 独立的高性能控制引擎，实现系统统一配置管理和安全集群。

图1-2 硬件架构



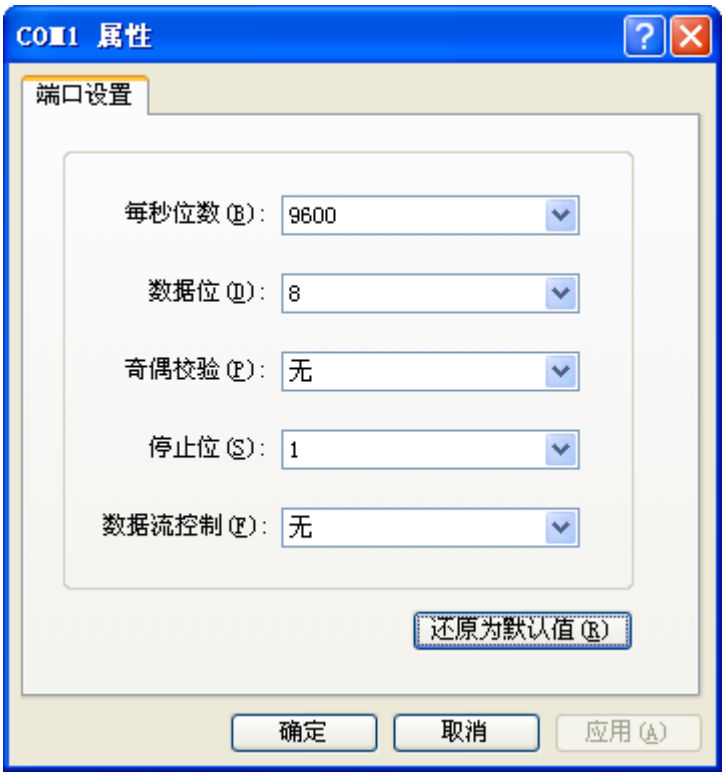
内置模块化软件系统，支持多进程的调度，进程间运行空间隔离，单个进程的异常不会影响系统其他部分，提高系统可靠性；支持权限管理功能，基于特性、命令行、系统资源、WEB 管理等级别定义用户读写权限，提高系统安全性；支持热补丁、支持 ISSU，不中断业务的情况下实现系统升级，提高系统易用性。

1.2.3 M9000 的管理

M9000 目前支持命令行管理，命令行可以提供全面的配置、信息查看、故障诊断等。

如 1-3 所示，M9000 主控板自带 Console 口，可以用串口线对 M9000 进行管理，其串口参数与管理 H3C 主网络设备设置相同。

图1-3 串口参数设置



在 M9000 中，业务板也有 Console 口，可以连接该 Console 口，对整台设备进行管理。在业务板启动过程中，业务板 Console 口显示的业务板的启动信息。

对业务板的 Console 口，主要用于业务板启动信息的查看，当业务板完全启动后，显示的信息为和主控板上的信息完全相同，为 M9000 的统一管理信息。

建议 Console 口采用主控板的 Console 口信息。

2 M9000-AI-E 系列的硬件和版本升级

2.1 硬件说明

M9000-AI-E 产品主要由主控板区、接口板和业务板区、网板区、电源区、风扇区等几个部分组成。下面两张图显示的是 M9000-AI-E8 和 M9000-AI-E16 的机箱的区域说明：

图2-1 M9000-AI-E8 前、后面板示意图

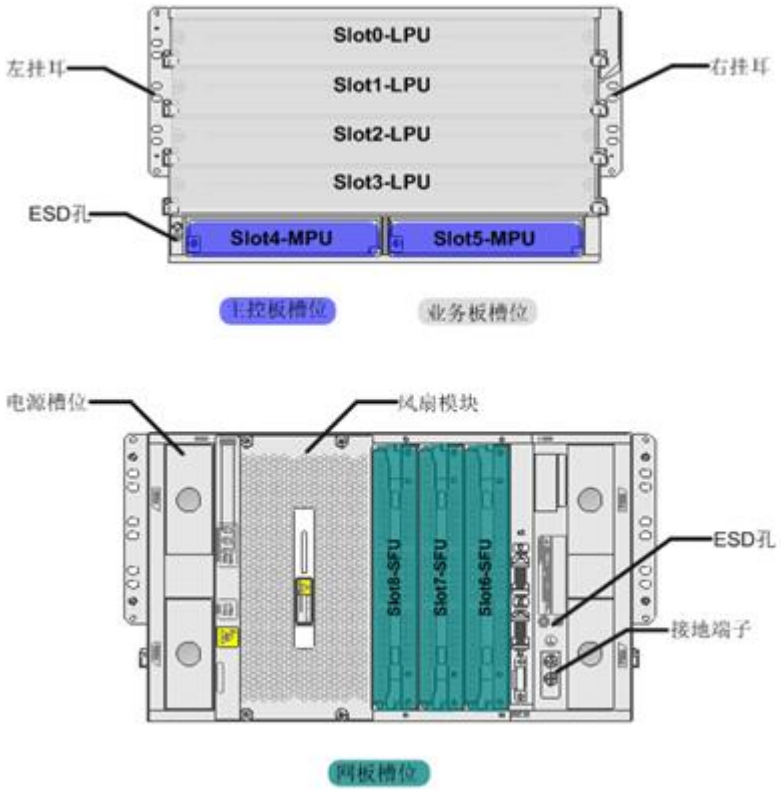


图2-2 M9000-AI-E16 前、后面板示意图

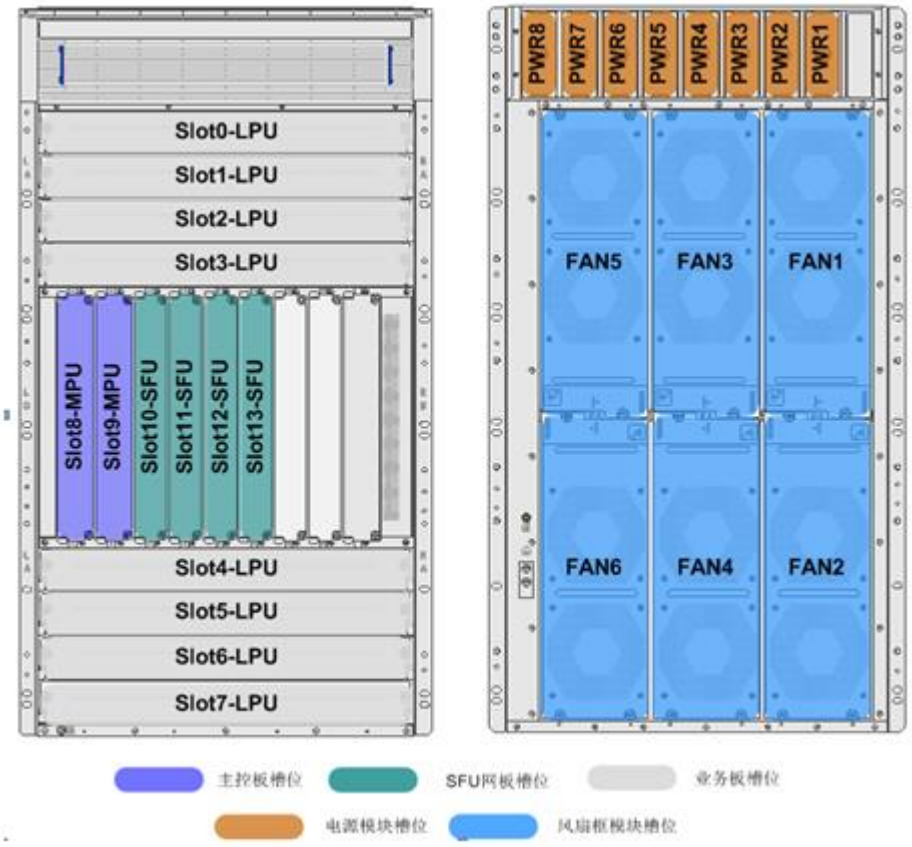


表2-1 机箱各区域说明

区域说明	选配情况
业务板槽位	该区域插入母板，母板可以插入业务子卡和接口子卡，母板、业务子卡、接口子卡必配（机箱发货时不带母板、接口子卡及业务子卡） 其中单个母板可插2张业务子卡或者2张接口子卡或者1张业务子卡和1张接口子卡
主控板槽位	主控板必配（机箱发货时不带主控板） M9000-AI-E8支持NSQM5SUP16A1 M9000-AI-E16支持NSQM5SUP08A1
电源模块的槽位	电源模块必配（机箱发货时不带电源模块），支持的电源模块型号有PSR2400-54A、PSR3000-54A、PSR2400-54D、PSR3000-54AHD四种类型 根据不同机箱的特点，电源的位置有所不同： M9000-AI-E8：电源位于机箱背面左右两侧 M9000-AI-E16：电源位于机箱背面上方
风扇框的槽位，位于机箱背面	风扇框必配（机箱发货时已安装好相应风扇框） 根据不同机箱的特点，风扇框的位置有所不同： M9000-AI-E8：风扇框位于机箱背面的左侧

区域说明	选配情况
	M9000-AI-E16：风扇框位于机箱背面的下方
SFU网板的槽位	网板必配（机箱发货时不带网板） M9000-AI-E8支持NSQM5FAB08A1 M9000-AI-E16支持NSQM5FAB16A1 M9000-AI-E8和M9000-AI-E16主机都提供4个网板槽位，但当前仅支持配置2个网板，且M9000-AI-E8不支持热插拔。

M9000-AI-E8 的 full-mesh 架构，slot0 与 slot1 一组， slot2 与 slot3 一组，组间带宽为 400G，跨组带宽是 200G。

M9000-AI-E16 注意高低速槽位，slot3 与 slot4 为高速槽位（800G），slot0-slot2，slot5-slot7 为低速槽位（400G）。

M9000-AI-E16 设备的转接板分上下两种（上：NSQ1M9ESL18UA；下：NSQ1M9ESL18LA），实际组装时可通过机框的插销间距和轨道槽来分辨，不可以硬插，并且不支持热插拔。转接板有毛边，轻拿轻放，小心割伤。组装时依照铜柱固定插销位置安装，如果风扇安装不上，请检查转接板是否连接正确。

表2-2 M9000-AI-E 产品支持的接口板和业务板

单板名称	单板类型	单板俗称	单板印丝名称	备注
NSQM5SUP16A1	主控板	E16主控	NSQM5SUP16A1	M9000-AI-E16支持
NSQM5SUP08A1	主控板	E8主控	NSQM5SUP08A1	M9000-AI-E8支持
NSQM5FAB16A1	网板	E16网板A类	NSQM5FAB16A1	M9000-AI-E16支持
NSQM5FAB08A1	网板	E8网板A类	NSQM5FAB08A1	M9000-AI-E8支持
NSQM5MBSHA1	母板	母板	NSQM5MBSHA1	接口交换A模块(SH)
NS-FWEMPA1	防火墙业务板	业务板子卡	NS-FWEMPA1	SecBlade V 下一代防火墙A模块(MP)
NS-C300-CGQ2TG16A1	接口子卡	2端口百G+16端口万兆子卡	NS-C300-CGQ2TG16A1	2端口100G以太网光接口(QSFP28)+16端口10G以太网光接口模块(SFP+)
NS-C600-CGQ6A1	接口子卡	6端口百G子卡	NS-C600-CGQ6A1	6端口100G以太网光接口模块(QSFP28)
NS-C300-QG4TG16A1	接口子卡	4端口40G+16端口万兆子卡	NS-C300-QG4TG16A1	4端口40G以太网光接口(QSFP+)+16端口10G以太网光接口模块(SFP+)
NS-C300-TG24A1	接口子卡	24端口万兆子卡	NS-C300-TG24A1	24端口10G以太网光接口模块(SFP+)

2.2 版本升级的内容

对 M9000 版本，要升级 2 个版本，主控版本和业务板软件版本。这两个版本要单独通过命令行升级。在升级时，需要指定主控、业务板所在的 Slot 号。下面以 M9000-AI-E8 为例，介绍升级过程。

2.3 M9000-AI-E8主控升级过程

- 在 V7 Comware 系统下升级，升级过程如下：

(1)首先把主控的.ipe 文件上传到 flash。上传操作可以通过 ftp 或者 tftp。

(2)上传成功后，设置该文件为某槽位主控的系统文件，如下：

```
<M9000-E8>boot-loader file flash:/M9000E.ipe chassis 1 slot 4 main
Verifying the file flash:/M9000E.ipe on chassis 1 slot
4.....
.....Done.
H3C SecPath M9000-AI-E8 images in IPE:
M9000E-CMW710-BOOT-E9001P12.bin
M9000E-CMW710-SYSTEM-E9001P12.bin
M9000E-CMW710-DEVKIT-E9001P12.bin
This command will set the main startup software images. Please do not reboot any MPU during
the upgrade. Continue? [Y/N]:y
Add images to chassis 1 slot 4.
File flash:/M9000E-CMW710-BOOT-E9001P12.bin already exists on chassis 1 slot 4.
File flash:/M9000E-CMW710-SYSTEM-E9001P12.bin already exists on chassis 1 slot 4.
File flash:/M9000E-CMW710-DEVKIT-E9001P12.bin already exists on chassis 1 slot 4.
Overwrite the existing files?[Y/N]:y
```

2.4 M9000-AI-E8业务板升级过程

- 在 V7 Comware 系统下升级：

(1)首先把业务板的.ipe 文件上传到主控的 flash

(2)上传成功后，设置该文件为某槽位业务板的系统文件，如下：

```
<M9000-E8>boot-loader file flash:/M9000e_fw.ipe chassis 1 slot 2 cpu 3 main
Verifying the file flash:/M9000e_fw.ipe on chassis 1 slot
4.....
..........Done.
Blade5fw images in IPE:
BLADE4FWM9000-E-CMW710-BOOT-E9001P12.bin
BLADE4FWM9000-E-CMW710-SYSTEM-E9001P12.bin
This command will set the main startup software images. Please do not reboot any MPU during
the upgrade. Continue? [Y/N]:y
Add images to chassis 1 slot 2.3.
File flash:/BLADE4FWM9000-E-CMW710-BOOT-E9001P12.bin already exists on chassis 1 slot 2.3.
File flash:/BLADE4FWM9000-E-CMW710-SYSTEM-E9001P12.bin already exists on chassis 1 slot 2.3.
Overwrite the existing files?[Y/N]:y
```

(3)加载版本完成后，检查版本是否是加载的版本，如下：

```
<M9000-E8>display boot-loader
Software images on chassis 1 slot 2.3:
Current software images:
  flash:/BLADE4FWM9000-E-CMW710-BOOT-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-SYSTEM-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-DEVKIT-E9001P12.bin
Main startup software images:
```

```
  flash:/BLADE4FWM9000-E-CMW710-BOOT-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-SYSTEM-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-DEVKIT-E9001P12.bin
Backup startup software images:
  None
Software images on chassis 1 slot 2.4:
Current software images:
  flash:/BLADE4FWM9000-E-CMW710-BOOT-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-SYSTEM-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-DEVKIT-E9001P12.bin
Main startup software images:
  flash:/BLADE4FWM9000-E-CMW710-BOOT-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-SYSTEM-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-DEVKIT-E9001P12.bin
Backup startup software images:
  None
Software images on chassis 1 slot 3.1:
Current software images:
  flash:/BLADE4FWM9000-E-CMW710-BOOT-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-SYSTEM-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-DEVKIT-E9001P12.bin
Main startup software images:
  flash:/BLADE4FWM9000-E-CMW710-BOOT-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-SYSTEM-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-DEVKIT-E9001P12.bin
Backup startup software images:
  None
Software images on chassis 1 slot 3.2:
Current software images:
  flash:/BLADE4FWM9000-E-CMW710-BOOT-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-SYSTEM-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-DEVKIT-E9001P12.bin
Main startup software images:
  flash:/BLADE4FWM9000-E-CMW710-BOOT-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-SYSTEM-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-DEVKIT-E9001P12.bin
Backup startup software images:
  None
Software images on chassis 1 slot 3.3:
Current software images:
  flash:/BLADE4FWM9000-E-CMW710-BOOT-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-SYSTEM-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-DEVKIT-E9001P12.bin
Main startup software images:
  flash:/BLADE4FWM9000-E-CMW710-BOOT-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-SYSTEM-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-DEVKIT-E9001P12.bin
Backup startup software images:
```

```
  None
Software images on chassis 1 slot 3.4:
Current software images:
  flash:/BLADE4FWM9000-E-CMW710-BOOT-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-SYSTEM-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-DEVKIT-E9001P12.bin
Main startup software images:
  flash:/BLADE4FWM9000-E-CMW710-BOOT-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-SYSTEM-E9001P12.bin
  flash:/BLADE4FWM9000-E-CMW710-DEVKIT-E9001P12.bin
Backup startup software images:
  None
Software images on chassis 1 slot 4:
Current software images:
  flash:/M9000E-CMW710-BOOT-E9001P12.bin
  flash:/M9000E-CMW710-SYSTEM-E9001P12.bin
  flash:/M9000E-CMW710-DEVKIT-E9001P12.bin
Main startup software images:
  flash:/M9000E-CMW710-BOOT-E9001P12.bin
  flash:/M9000E-CMW710-SYSTEM-E9001P12.bin
  flash:/M9000E-CMW710-DEVKIT-E9001P12.bin
Backup startup software images:
  None
Software images on chassis 1 slot 5:
Current software images:
  flash:/M9000E-CMW710-BOOT-E9001P12.bin
  flash:/M9000E-CMW710-SYSTEM-E9001P12.bin
  flash:/M9000E-CMW710-DEVKIT-E9001P12.bin
Main startup software images:
  flash:/M9000E-CMW710-BOOT-E9001P12.bin
  flash:/M9000E-CMW710-SYSTEM-E9001P12.bin
  flash:/M9000E-CMW710-DEVKIT-E9001P12.bin
```

(4)重启设备，变为升级以后的版本，检查版本信息如下。

```
<M9000-E8>display version
H3C Comware Software, Version 7.1.064, Ess 9001P12
Copyright (c) 2004-2019 New H3C Technologies Co., Ltd. All rights reserved.
H3C SecPath M9000-AI-E8 uptime is 0 weeks, 0 days, 21 hours, 41 minutes
Last reboot reason : User reboot

Boot image: flash:/M9000E-CMW710-BOOT-E9001P12.bin
Boot image version: 7.1.064, Ess 9001P12
  Compiled Jan 03 2019 15:00:00, DEBUG SOFTWARE
System image: flash:/M9000E-CMW710-SYSTEM-E9001P12.bin
System image version: 7.1.064, Ess 9001P12
  Compiled Jan 03 2019 15:00:00, DEBUG SOFTWARE
Feature image(s) list:
  flash:/M9000E-CMW710-DEVKIT-E9001P12.bin, version: 7.1.064
    Compiled Jan 03 2019 15:00:00, DEBUG SOFTWARE
```

```
LPU Chassis 1 Slot 1:
Uptime is 0 weeks,0 days,21 hours,38 minutes
H3C SecPath M9000-AI-E8 LPU with 1 ARM Processor
BOARD TYPE:         NSQM5MBSHA1
DRAM:               2048M bytes
PCB 1 Version:      VER.A
SUBCARD 1 PCB Version:VER.A
SUBCARD 2 PCB Version:VER.A
Bootrom Version:    312
CPLD 1 Version:     002
SUBCARD 1 CPLD Version:001
SUBCARD 2 CPLD Version:001
Release Version:    H3C SecPath M9000-AI-E8-9001P12
Patch Version  :    None
Reboot Cause   :    UserReboot
PowChip Version:    001

LPU Chassis 1 Slot 2:
Uptime is 0 weeks,0 days,21 hours,27 minutes
H3C SecPath M9000-AI-E8 LPU with 1 ARM Processor
BOARD TYPE:         NSQM5MBSHA1
DRAM:               2048M bytes
PCB 1 Version:      VER.A
SUBCARD 1 PCB Version:VER.A
SUBCARD 2 PCB Version:VER.A
Bootrom Version:    312
CPLD 1 Version:     002
SUBCARD 1 CPLD Version:001
SUBCARD 2 CPLD Version:002
Release Version:    H3C SecPath M9000-AI-E8-9001P12
Patch Version  :    None
Reboot Cause   :    UserReboot
PowChip Version:    001
Chassis 1 Slot 2 CPU 3
CPU type:           Multi-core CPU
DDR4 :              32752M bytes
FLASH:              7296M bytes
Board PCB Version:  Ver.A
CPLD Version:       2.0
Release Version:    SecBlade FW Enhanced-9001P12
Basic  BootWare Version:1.01
Extend BootWare Version:1.01
Chassis 1 Slot 2 CPU 4
CPU type:           Multi-core CPU
DDR4 :              32752M bytes
FLASH:              7296M bytes
```

```
Board PCB Version:  Ver.A
CPLD Version:       2.0
Release Version:    SecBlade FW Enhanced-9001P12
Basic  BootWare Version:1.01
Extend BootWare Version:1.01

LPU Chassis 1 Slot 3:
Uptime is 0 weeks,0 days,21 hours,27 minutes
H3C SecPath M9000-AI-E8 LPU with 1 ARM Processor
BOARD TYPE:         NSQM5MBSHA1
DRAM:               2048M bytes
PCB 1 Version:      VER.A
SUBCARD 1 PCB Version:VER.E
SUBCARD 2 PCB Version:VER.A
Bootrom Version:    100
CPLD 1 Version:     001
SUBCARD 1 CPLD Version:004
SUBCARD 2 CPLD Version:002
Release Version:    H3C SecPath M9000-AI-E8-9001P12
Patch Version  :    None
Reboot Cause   :    UserReboot
PowChip Version:    001
Chassis 1 Slot 3 CPU 1
CPU type:           Multi-core CPU
DDR4 :              32752M bytes
FLASH:              7296M bytes
Board PCB Version:  Ver.A
CPLD Version:       4.0
Release Version:    SecBlade FW Enhanced-9001P12
Basic  BootWare Version:1.01
Extend BootWare Version:1.01
Chassis 1 Slot 3 CPU 2
CPU type:           Multi-core CPU
DDR4 :              32752M bytes
FLASH:              7296M bytes
Board PCB Version:  Ver.A
CPLD Version:       4.0
Release Version:    SecBlade FW Enhanced-9001P12
Basic  BootWare Version:1.01
Extend BootWare Version:1.01
Chassis 1 Slot 3 CPU 3
CPU type:           Multi-core CPU
DDR4 :              32752M bytes
FLASH:              7296M bytes
Board PCB Version:  Ver.A
CPLD Version:       2.0
Release Version:    SecBlade FW Enhanced-9001P12
Basic  BootWare Version:1.01
```

```
Extend BootWare Version:1.01
Chassis 1 Slot 3 CPU 4
CPU type:           Multi-core CPU
DDR4 :              32752M bytes
FLASH:              7296M bytes
Board PCB Version:  Ver.A
CPLD Version:       2.0
Release Version:    SecBlade FW Enhanced-9001P12
Basic  BootWare Version:1.01
Extend BootWare Version:1.01

MPU(M) Chassis 1 Slot 4:
Uptime is 0 weeks,0 days,21 hours,41 minutes
H3C SecPath M9000-AI-E8 MPU(M) with 1 XLP316 Processor
BOARD TYPE:         NSQM5SUP08A1
DRAM:               16384M bytes
FLASH:              1024M bytes
PCB 1 Version:      VER.A
Bootrom Version:    158
CPLD 1 Version:     002
CPLD 2 Version:     001
Release Version:    H3C SecPath M9000-AI-E8-9001P12
Patch Version  :    None
Reboot Cause   :    UserReboot

MPU(S) Chassis 1 Slot 5:
Uptime is 0 weeks,0 days,21 hours,41 minutes
H3C SecPath M9000-AI-E8 LPU with 1 XLP316 Processor
BOARD TYPE:         NSQM5SUP08A1
DRAM:               16384M bytes
FLASH:              1024M bytes
PCB 1 Version:      VER.A
Bootrom Version:    158
CPLD 1 Version:     002
CPLD 2 Version:     001
Release Version:    H3C SecPath M9000-AI-E8-9001P12
Patch Version  :    None
Reboot Cause   :    UserReboot

NPU Chassis 1 Slot 6:
BOARD TYPE:         NSQM5FAB08A1
PCB Version:        VER.A
CPLD Version:       200


NPU Chassis 1 Slot 7:
BOARD TYPE:         NSQM5FAB08A1
PCB Version:        VER.A
```

```
CPLD Version:       200
```

2.5 注意事项

- 如果系统为双主控，另外一块主控需要单独设置。如另外一块主控在 slot 5，则应键入命令：boot-loader file flash:/m9000.ipe slot 5 main。也可以同时设置两块主控，设置如下：boot-loader file flash:/m9000.ipe all main。
- IRF 环境下，升级主控时，要添加框号，如 boot-loader file flash:/m9000.ipe chassis 1 slot 0 main，这里 chassis 指的是框号。
- 如果设备有多块业务板卡，需要对每一块业务板卡升级且 slot 号要设置正确。
- M9000-AI-E 的 blade 子卡上的每个 cpu 需单独升级版本。

3 防火墙基础配置

3.1 防火墙的几个基本概念

3.1.1 安全域

防火墙作为网络安全设备，按照业务的重要性高低，将网络分为若干个安全域，安全域以防火墙接口为边界。引入安全域的概念之后，安全管理员将安全需求相同的接口进行分类（划分到不同的安全域），能够实现策略的分层管理。

目前，M9000 系列的缺省安全域为 Management、Local、Trust、Untrust、DMZ 域。默认管理接口属于 Management 安全域中。

创建安全域后，设备上各接口的报文转发遵循以下规则：

- 一个安全域中的接口与一个不属于任何安全域的接口之间的报文，会被丢弃。
- 属于同一个安全域的各接口之间的报文缺省会被丢弃。
- 安全域之间的报文由安全策略进行安全检查，并根据检查结果放行或丢弃。若安全策略不存在或不生效，则报文会被丢弃。
- 非安全域的接口之间的报文被丢弃。
- 目的地址或源地址为本机的报文，缺省会被丢弃，若该报文与安全策略匹配，则由安全策略进行安全检查，并根据检查结果放行或丢弃。

3.1.2 流和会话

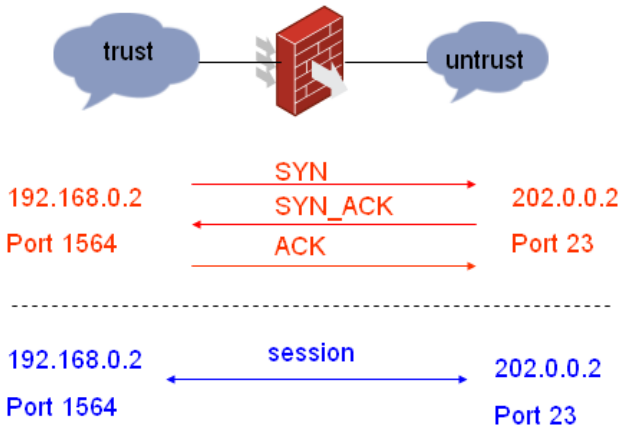
流（Flow）是一个单方向的概念，根据报文所携带的三元组或者五元组唯一标识。根据 IP 层协议的不同，流分为四大类：

- TCP 流：通过五元组唯一标识。
- UDP 流：通过五元组唯一标识。
- ICMP 流：通过三元组 + ICMP type + ICMP code 唯一标识。
- RAW IP 流：不属于上述协议，通过三元组标识。

会话（Session）是一个双向的概念，一个会话通常关联两个方向的流，一个为会话发起方（Initiator），另外一个为会话响应方（Responder）。通过会话所属的任一方向的流特征都可以唯一确定该会话以及方向。

对于 TCP/UDP/ICMP/RAW IP 流，首包进入防火墙时开始创建会话，后续相同的报文或者返回报文可以匹配该会话。以 TCP 三次握手为例：

图3-1 会话建立



如图 3-1 所示，Trust 域的 192.168.0.2:1564 访问 Untrust 域的 202.0.0.2 的 23 端口，首包 syn 报文开始创建一个双向会话（192.168.0.2:1564<---->202.0.0.2:23），后续 SYN_ACK 和 ACK 报文都匹配到此会话后，完整的会话创建完成。后续数据流如果匹配到此会话则放行通过。

4 M9000 系列多业务安全网关的远程管理概述

对 M9000 系列设备，可以通过 Telnet、SSH、MIB 进行远程管理。缺省情况下，系统是无法通过 Telnet 远程登录的。系统默认的启动配置如下：

- 缺省用户为 admin,密码 admin。
- 终端 VTY 用户登录方式为 password 方式，但是没有设置登录 password。
- Telnet、SSH、SNMP 服务关闭。
- 管理口默认绑定 management vpn-instance，存在默认地址。
- 管理口默认加入 management 域中。
- 没有任何安全策略。

5 典型组网

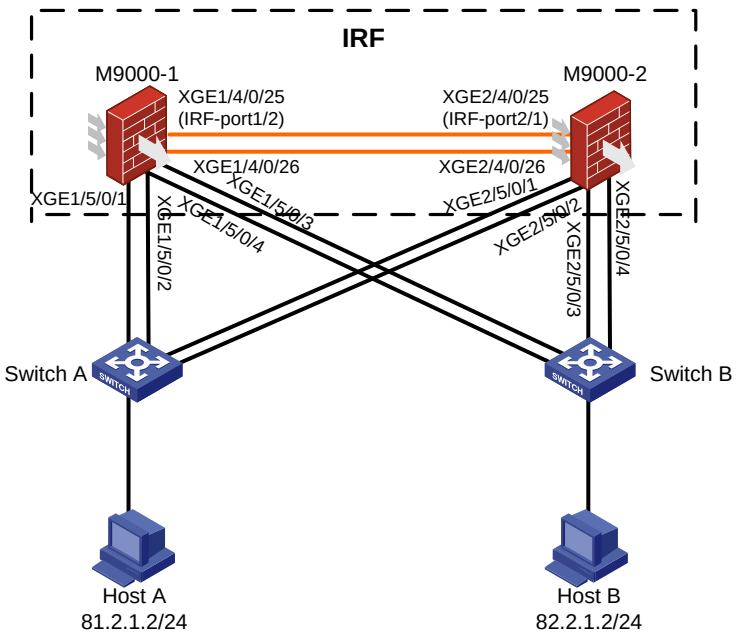
5.1 IRF和冗余组

5.1.1 组网需求

如图 5-1 所示，组网需求如下：

- 两台 M9000 设备：M9000-1 和 M9000-2，构成 IRF 设备。
- 聚合口为 Route-Aggregation1、Route-Aggregation2、Route-Aggregation3、Route-Aggregation4，这四个聚合口每个端口包含 2 个成员口。
- 冗余口 RETH1 的成员口为 Route-Aggregation1、Route-Aggregation2，主端口为 Route-Aggregation1。
- 冗余口 RETH2 的成员口为 Route-Aggregation3、Route-Aggregation4，主端口为 Route-Aggregation3。
- Host A 和 Host B 互相可以 ping 通。当 M9000-1 工作正常时，会话建立在 M9000-1 上。当 M9000-1 异常时（可以通过 shutdown Route-Aggregation1 来实现异常），会话建立在 M9000-2 上。
- 配置 BFD 检测，两台设备各取一个物理口直连加入聚合口 Route-Aggregation 999
- 堆叠双机的时候如果需要业务热备份必须要开启会话备份

图5-1 IRF 和冗余组组网图



5.1.2 配置思路

- 创建聚合口，并把相应端口加入到聚合口。
- 创建冗余口 reth1 和 reth2。

- 创建冗余组，包含冗余成员：reth1 和 reth2。
- 将冗余口 reth1 和 reth2 加入到安全域 Trust。
- 创建安全策略。
- 配置 BFD 检测，两台设备各取一个物理口直连加入聚合口 Route-Aggregation 999
- 堆叠双机的时候如果需要业务热备份必须要开启会话备份

5.2 配置步骤

1. M9000-1 的配置

1．配置 IRF

配置成员号和优先级。

```
[M9000-1]irf member 1
[M9000-1]irf priority 32
```

将设备切换到 IRF 模式。

```
[M9000-1]chassis convert mode irf
The device will switch to IRF mode and reboot.
You are recommended to save the current running configuration and specify the configuration
file for the next startup. Continue? [Y/N]:y
```

重启后，可以看到设备接口已变成四维模式，将 IRF 物理端口手动 shutdown。

```
[M9000-1] interface Ten-GigabitEthernet 1/4/0/25
[M9000-1-Ten-GigabitEthernet1/4/0/25] shutdown
[M9000-1] interface Ten-GigabitEthernet 1/4/0/26
[M9000-1-Ten-GigabitEthernet1/4/0/25] shutdown
```

将 IRF 物理端口加入到堆叠组中。

```
[M9000-1] irf-port 1/2
[M9000-1-irf-port1/2] port group interface ten-gigabitethernet 1/4/0/25
You must perform the following tasks for a successful IRF setup:
Save the configuration after completing IRF configuration.
Execute the "irf-port-configuration active" command to activate the IRF ports.
[M9000-1-irf-port1/2] port group interface ten-gigabitethernet 1/4/0/26
[M9000-1-irf-port1/2] quit
[M9000-1]irf-port-configuration active
```

将 irf 物理端口手动 undo shutdown（该配置操作在 M9000-2 的 irf 端口手动 undo shutdown 完成后操作）

```
[M9000-1] interface Ten-GigabitEthernet 1/4/0/25
[M9000-1-Ten-GigabitEthernet1/4/0/25] undo shutdown
[M9000-1] interface Ten-GigabitEthernet 1/4/0/26
[M9000-1-Ten-GigabitEthernet1/4/0/25] undo shutdown
```

该步骤操作完成后，备框将自动重启。

2．配置聚合口(以下配置在完成 2. M9000-2 堆叠配置后进行)

创建三层聚合口 Route-Aggregation1，并把端口加入到聚合组。

```
[M9000-1] interface Route-Aggregation1
[M9000-1-Route-Aggregation1] quit
```

```
[M9000-1] interface ten-gigabitethernet 1/5/0/1
[M9000-1-Ten-GigabitEthernet1/5/0/1] port link-aggregation group 1
[M9000-1-Ten-GigabitEthernet1/5/0/1] quit
[M9000-1] interface ten-gigabitethernet 1/5/0/2
[M9000-1-Ten-GigabitEthernet1/5/0/2] port link-aggregation group 1
[M9000-1-Ten-GigabitEthernet1/5/0/2] quit
```

创建三层聚合口 Route-Aggregation3，并把 M9000-1 上的端口加入到聚合组中。

```
[M9000-1] interface Route-Aggregation3
[M9000-1-Route-Aggregation3] quit
[M9000-1] interface ten-gigabitethernet 1/5/0/3
[M9000-1-Ten-GigabitEthernet1/5/0/3] port link-aggregation group 3
[M9000-1-Ten-GigabitEthernet1/5/0/3] quit
[M9000-1] interface ten-gigabitethernet 1/5/0/4
[M9000-1-Ten-GigabitEthernet1/5/0/4] port link-aggregation group 3
[M9000-1-Ten-GigabitEthernet1/5/0/4] quit
```

3．配置冗余组【冗余主备组网】

创建冗余口 1，并配置冗余口成员。

```
[M9000-1] interface reth 1
[M9000-1-Reth1] ip address 81.2.1.1 24
[M9000-1-Reth1] member interface Route-Aggregation 1 priority 100
[M9000-1-Reth1] member interface Route-Aggregation 2 priority 1
[M9000-1-Reth1] quit
```

创建冗余口 2，并配置冗余口成员。

```
[M9000-1] interface reth 2
[M9000-1-Reth2] ip address 82.2.1.1 24
[M9000-1-Reth2] member interface Route-Aggregation 3 priority 100
[M9000-1-Reth2] member interface Route-Aggregation 4 priority 1
[M9000-1-Reth2] quit
```

配置 Track，用于冗余联动。

```
[M9000-1] track 11 interface Route-Aggregation1
[M9000-1] track 12 interface Route-Aggregation3
[M9000-1] track 21 interface Route-Aggregation2
[M9000-1] track 22 interface Route-Aggregation4
[M9000-1] track 31 interface Blade 1/3/0/1 physical
[M9000-1] track 32 interface Blade 2/3/0/1 physical
```

配置备份组，并指定 M9000-1 上的安全引擎为主，M9000-2 上的安全引擎为备。

```
[M9000-1] failover group Group1
[M9000-1-failover-group-Group1] bind chassis 1 slot 3 cpu 1 primary
[M9000-1-failover-group-Group1] bind chassis 2 slot 3 cpu 1 secondary
[M9000-1-failover-group-Group1] quit
```

创建 Node 1，Node 1 和 M9000-1 绑定，为主节点。关联的 Track 项为 11、12 和 31。

```
[M9000-1] redundancy group 1
[M9000-1-redundancy-group-1] node 1
[M9000-1-redundancy-group-1-node-1] bind chassis 1
[M9000-1-redundancy-group-1-node-1] priority 100
[M9000-1-redundancy-group-1-node-1] track 11 interface Route-Aggregation 1
```

```
[M9000-1-redundancy-group-1-node-1] track 12 interface Route-Aggregation 3
[M9000-1-redundancy-group-1-node-1] track 31
[M9000-1-redundancy-group-1-node-1] quit
```

创建 Node 2，Node 2 和 M9000-2 绑定，为备节点，关联的 Track 项为 21、22 和 32。

```
[M9000-1-redundancy-group-1] node 2
[M9000-1-redundancy-group-1-node-2] bind chassis 2
[M9000-1-redundancy-group-1-node-2] priority 50
[M9000-1-redundancy-group-1-node-2] track 21 interface Route-Aggregation 2
[M9000-1-redundancy-group-1-node-2] track 22 interface Route-Aggregation 4
[M9000-1-redundancy-group-1-node-2] track 32
[M9000-1-redundancy-group-1-node-2] quit
[M9000-1-redundancy-group-1] member interface reth 1
[M9000-1-redundancy-group-1] member interface reth 2
[M9000-1-redundancy-group-1] member failover group Group1
[M9000-1-redundancy-group-1] quit
```

4．配置安全域和安全策略

将 Reth1、Reth2 加入到安全域 Trust。

```
[M9000-1] security-zone name trust
[M9000-1-security-zone-Trust] import interface reth 1
[M9000-1-security-zone-Trust] import interface reth 2
[M9000-1-security-zone-Trust] quit
```

配置对象组。

```
[M9000-1]object-group ip address A
[M9000-1-obj-grp-ip-A]network subnet 81.2.1.0 24
[M9000-1-obj-grp-ip-A]quit
[M9000-1]object-group ip address B
[M9000-1-obj-grp-ip-B]network subnet 82.2.2.0 24
[M9000-1-obj-grp-ip-B]quit
```

配置 Trust 到 Trust 域之间的安全策略。

```
[M9000-1]security-policy ip
[M9000-1-security-policy-ip]rule name trust-trust
[M9000-1-security-policy-ip-8-trust-trust]source-ip A
[M9000-1-security-policy-ip-8-trust-trust]source-ip B
[M9000-1-security-policy-ip-8-trust-trust]action pass
[M9000-1-security-policy-ip-8-trust-trust]quit
[M9000-1-security-policy-ip]quit
```

5．配置 BFD 检测

把两框的 32 口直连并加入聚合口 Route-Aggregation 999，接口下使能 BFD。

```
[m9000]interface Route-Aggregation999
[m9000-Route-Aggregation999]mad bfd enable
[m9000-Route-Aggregation999]mad ip address 192.168.1.254 255.255.255.0 member 1
[m9000-Route-Aggregation999]mad ip address 192.168.1.253 255.255.255.0 member 2
[m9000-Route-Aggregation999]interface Ten-GigabitEthernet1/2/0/31
[m9000-Ten-GigabitEthernet1/2/0/31]port link-mode route
[m9000-Ten-GigabitEthernet1/2/0/31]port link-aggregation group 999
```

```
[m9000-Ten-GigabitEthernet1/2/0/31]interface Ten-GigabitEthernet2/2/0/31
[m9000-Ten-GigabitEthernet2/2/0/31]port link-mode route
[m9000-Ten-GigabitEthernet1/2/0/31]port link-aggregation group 999
```

6. 堆叠双机的时候如果需要业务热备份必须要开启会话备份

```
[m9000] session synchronization  enable
[m9000] session synchronization  dns
[m9000] session synchronization  http
```

2. M9000-2 的配置

1．配置 IRF

配置成员号和优先级。

```
[M9000-2]irf member 2
[M9000-2]irf priority 1
```

将设备切换到 IRF 模式。

```
[M9000-2]chassis convert mode irf
The device will switch to IRF mode and reboot.
You are recommended to save the current running configuration and specify the configuration
file for the next startup. Continue? [Y/N]:y
Now rebooting, please wait...
```

重启后，可以看到设备接口已变为四维模式，将 IRF 物理端口手动 shutdown。

```
[M9000-2] interface Ten-GigabitEthernet 2/4/0/25
[M9000-2-Ten-GigabitEthernet2/4/0/25] shutdown
[M9000-2] interface Ten-GigabitEthernet 2/4/0/26
[M9000-2-Ten-GigabitEthernet2/4/0/25] shutdown
```

将 IRF 物理端口加入到 IRF 端口中。

```
[M9000-2] irf-port 2/1
[M9000-2-irf-port2/1] port group interface ten-gigabitethernet 2/4/0/25
You must perform the following tasks for a successful IRF setup:
Save the configuration after completing IRF configuration.
Execute the "irf-port-configuration active" command to activate the IRF ports.
[M9000-2-irf-port2/1] port group interface ten-gigabitethernet 2/4/0/26
[M9000-2-irf-port2/1] quit
[M9000-2] irf-port-configuration active
```

将 irf 物理端口手动 undo shutdown 后，保存当前配置

```
[M9000-2] interface ten-gigabitethernet 2/4/0/25
[M9000-2- Ten-GigabitEthernet2/4/0/25] undo shutdown
[M9000-2] interface ten-gigabitethernet 2/4/0/26
[M9000-2-Ten-GigabitEthernet2/4/0/26] undo shutdown
[M9000-2] save
The current configuration will be written to the device. Are you sure? [Y/N]:y
Please input the file name(*.cfg)[flash:/startup.cfg]
(To leave the existing filename unchanged, press the enter key):
Validating file. Please wait...
The current configuration adds 42 commands and deletes 350 commands.
The flash:/startup.cfg file already exists. The save operation will overwrite the file.
Are you sure you want to continue the save operation? [Y/N]:y
```

创建三层聚合口 Route-Aggregation4，并把 M9000-2 上的端口加入到聚合组中。

```
[M9000-2] interface Route-Aggregation4
[M9000-2-Route-Aggregation4] quit
[M9000-2] interface ten-gigabitethernet 2/5/0/3
[M9000-2-Ten-GigabitEthernet2/5/0/3] port link-aggregation group 4
[M9000-2-Ten-GigabitEthernet2/5/0/3] quit
[M9000-2] interface ten-gigabitethernet 2/5/0/4
[M9000-2-Ten-GigabitEthernet2/5/0/4] port link-aggregation group 4
[M9000-2-Ten-GigabitEthernet2/5/0/4] quit
```

2．其他配置

IRF 建立起来后，原来的 2 台设备变成 1 台设备了，其他配置在 M9000-1 上进行。

3. Switch A 的配置

配置连接 Host A 的接口。

```
<SwitchA> system-view
[SwitchA] interface GigabitEthernet 1/0/3
[SwitchA-GigabitEthernet1/0/3] port access vlan 1120
[SwitchA-GigabitEthernet1/0/3] quit
```

配置出接口（与 M9000-1 连接的聚合接口）。

```
[SwitchA] interface Bridge-Aggregation1
[SwitchA-Bridge-Aggregation1] port access vlan 1120
[SwitchA-Bridge-Aggregation1] quit
```

配置出接口（与 M9000-2 连接的聚合接口）。

```
[SwitchA] interface Bridge-Aggregation2
[SwitchA-Bridge-Aggregation1] port access vlan 1120
[SwitchA-Bridge-Aggregation1] quit
```

把端口加入到聚合组中（该配置略）。

4. Switch B 的配置步骤

配置连接 Host B 的接口。

```
<SwitchB> system-view
[SwitchB] interface GigabitEthernet 1/0/3
[SwitchB-GigabitEthernet1/0/3] port access vlan 1121
[SwitchB-GigabitEthernet1/0/3] quit
```

配置出接口（与 M9000-1 连接的聚合接口）。

```
[SwitchB] interface Bridge-Aggregation3
[SwitchB-Bridge-Aggregation1] port access vlan 1121
[SwitchB-Bridge-Aggregation1] quit
```

配置出接口（与 M9000-2 连接的聚合接口）。

```
[SwitchB] interface Bridge-Aggregation4
[SwitchB-Bridge-Aggregation1] port access vlan 1121
[SwitchB-Bridge-Aggregation1] quit
```

把端口加入到聚合组中（该配置略）。

5.2.2 注意事项

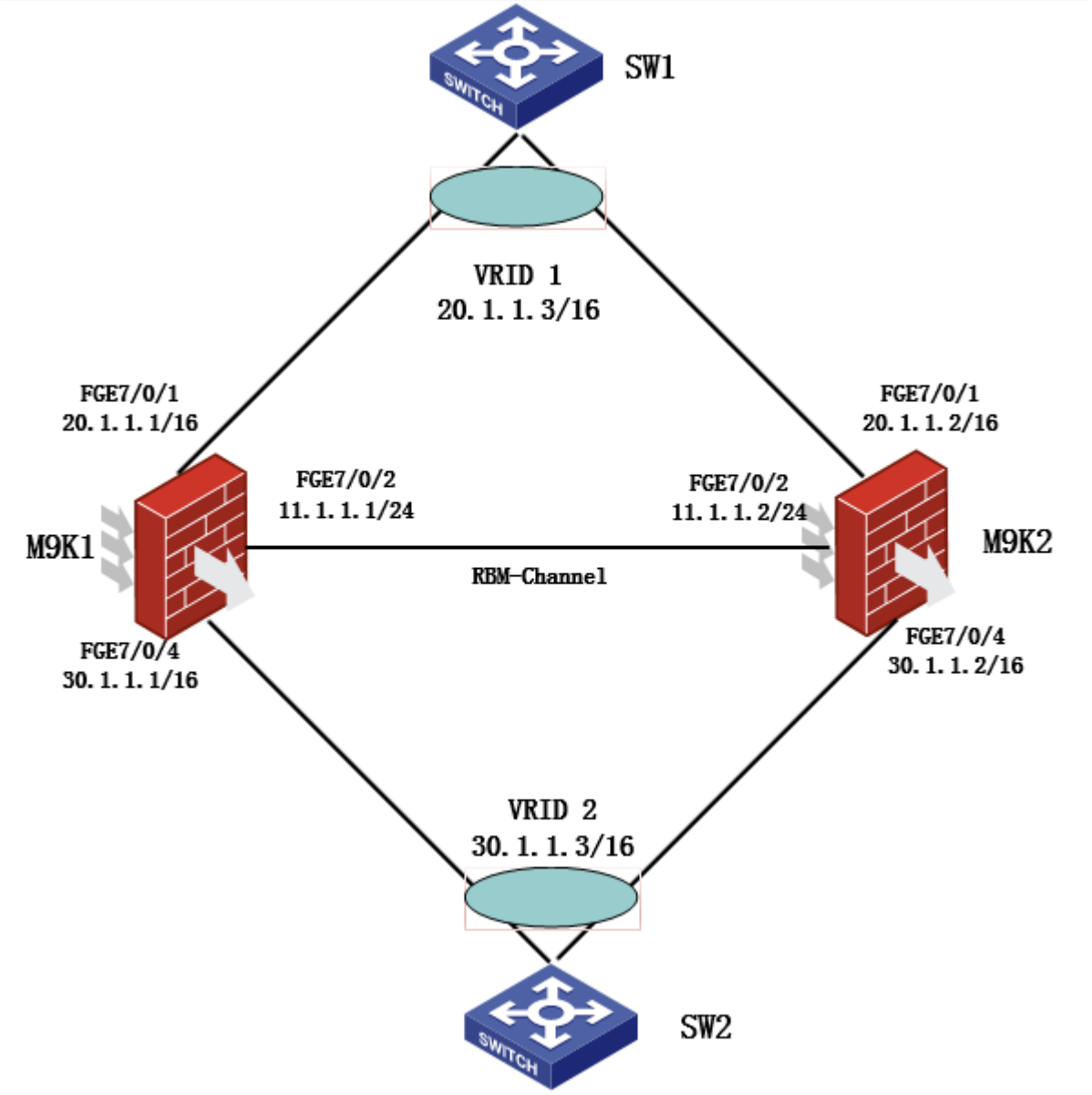
- 对于 IRF 来说，先启动的设备为主设备。
- 冗余口成员只能是物理口、物理子接口、聚合口、聚合子接口。
- IRF 双机组网中，对于备份组的要求是每个框的业务引擎槽位和 CPU 需要一一对应。

5.3 M9000的VRRP+RBM基本功能

5.3.1 组网需求

如图 5-2 所示，2 台 M9K 通过三层口连接到内部网络和外部网络，防火墙分别和上下行交换机连接。

图5-2 VRRP+RBM 基本功能组网图



5.3.2 配置思路

- 配置接口地址并加入安全域，保证传输可达
- 配置 VRRP 备份组
- 主备防火墙上配置 RBM 组，包含控制通道和数据通道

5.3.3 配置步骤

(1) 确保主备设备的软硬件环境一致

在配置远端备份管理功能之前，请先保证主/备设备的硬件环境和软件环境的一致性。

(2) 配置 M9K1

配置接口 IP 地址、路由、安全域及安全策略保证网络可达。

```
[M9K1-FortyGigE7/0/2] ip address 11.1.1.1 255.255.255.0
[M9K1-FortyGigE7/0/1] ip address 20.1.1.1 255.255.0.0
[M9K1-FortyGigE7/0/4] ip address 30.1.1.1 255.255.0.0
[M9K1-security-zone-Untrust]import interface FortyGigE7/0/1
[M9K1-security-zone-Trust]import interface FortyGigE7/0/4
[M9K1-security-zone-RMB]import interface FortyGigE7/0/2
[M9K1-security-policy-ip]rule name Trust-Untrust
[M9K1-security-policy-ip-5-Trust-Untrust]source-zone Trust
[M9K1-security-policy-ip-5-Trust-Untrust]destination-zone Untrust
[M9K1-security-policy-ip-5-Trust-Untrust]action pass
```

配置安全策略使安全域 RBM 与安全域 Local 之间的报文互通，保证 RBM 通道建立成功

```
[M9K1-security-policy-ip]rule name Local-RBM
[M9K1-security-policy-ip-7-Local-RBM]source-zone Local
[M9K1-security-policy-ip-7-Local-RBM]destination-zone RBM
[M9K1-security-policy-ip-7-Local-RBM]action pass
[M9K1-security-policy-ip]rule name RBM-Local
[M9K1-security-policy-ip-8-RBM-Local]source-zone RBM
[M9K1-security-policy-ip-8-RBM-Local]destination-zone Local
[M9K1-security-policy-ip-8-RBM-Local]action pass
```

配置 RBM 控制通道的对端 IP 地址为 11.1.1.2，端口号使用默认的 66064。

```
<M9K1> system-view
[M9K1] remote-backup group
[M9K1-remote-backup-group] remote-ip 11.1.1.2
```

配置 RBM 控制通道的本端 IP 地址为 11.1.1.1。

```
[M9K1-remote-backup-group] local-ip 11.1.1.1
```

配置 RBM 的数据通道，本举例使用控制通道的物理链路建立。

```
[M9K1-remote-backup-group] data-channel interface FortyGigE7/0/2
```

配置设备的管理角色为主管理设备。

```
[M9K1-remote-backup-group] device-role primary
```

配置 RBM 双机热备的模式为主备模式。（默认是主备模式）

```
[M9K1-remote-backup-group] undo backup-mode
```

开启 RBM 热备功能。

```
[M9K1-remote-backup-group] hot-backup enable
```

开启配置信息自动备份功能。

```
[M9K1-remote-backup-group] configuration auto-sync enable
```

开启配置信息一致性检查功能，并设置周期为 12 小时。

```
[M9K1-remote-backup-group] configuration sync-check interval 12
[M9K1-remote-backup-group] quit
```

配置 RBM 与 VRRP 关联。在接口 FortyGigE7/0/1 建 VRRP 备份组 1，其虚拟 IP 地址为 20.1.1.3，并配置其属于 VRRP ative 组。

```
[M9K1] interface FortyGigE7/0/1
[M9K1-FortyGigE7/0/1] vrrp vrid 1 virtual-ip 20.1.1.3 active
```

配置 RBM 与 VRRP 关联。在接口 FortyGigE7/0/4 创建 VRRP 备份组 2，其虚拟 IP 地址为 30.1.1.3，并配置其属于 VRRP ative 组。

```
[M9K1] interface FortyGigE7/0/4
[M9K1-FortyGigE7/0/4] vrrp vrid 2 virtual-ip 30.1.1.3 active
```

#配置动态 NAT

#在此配置举例中，仅需要在主管理设备 M9K1 上配置 NAT 的相关配置，M9K1 上的 NAT 配置会自动同步到从管理设备 M9K2。

配置 NAT 地址组 1，其地址成员范围为 2.1.1.5 到 2.1.1.10。

```
<M9K1> system-view
[M9K1] nat address-group 1
[M9K1-address-group-1] address 2.1.1.5 2.1.1.10
```

配置 NAT 地址组 1 与 VRRP 备份组 1 绑定。

```
[M9K1-address-group-1] vrrp vrid 1
[M9K1-address-group-1] quit
```

在接口上配置出方向动态地址转换，允许使用地址组 1 中的地址进行源地址转换，并在转换过程中使用端口信息。

```
[M9K1] interface FortyGigE7/0/1
[M9K1-FortyGigE7/0/1] nat outbound address-group 1
```

指定远端备份组中主备设备可以使用的 NAT 端口块范围（RBM 角色主配置下面的 primary 命令后，RBM 角色备会自动配置 secondary 命令）

```
<M9K1> system
[M9K1] nat remote-backup port-alloc primary
```

若存在 HTTP 或 DNS 应用协议的流量，还需开启对应的会话备份功能。

```
<M9K1> system
[M9K1] session synchronization http
[M9K1] session synchronization dns
```

(3) 配置 M9K2

配置接口 IP 地址、路由、安全域及安全策略保证网络可达。

```
[M9K2-FortyGigE7/0/2] ip address 11.1.1.2 255.255.255.0
[M9K2-FortyGigE7/0/1] ip address 20.1.1.2 255.255.0.0
[M9K2-FortyGigE7/0/4] ip address 30.1.1.2 255.255.0.0
[M9K2-security-zone-Untrust]import interface FortyGigE7/0/1
[M9K2-security-zone-Trust]import interface FortyGigE7/0/4
[M9K2-security-zone-RMB]import interface FortyGigE7/0/2
[M9K2-security-policy-ip]rule name Trust-Untrust
[M9K2-security-policy-ip-5-Trust-Untrust]source-zone Trust
[M9K2-security-policy-ip-5-Trust-Untrust]destination-zone Untrust
[M9K2-security-policy-ip-5-Trust-Untrust]action pass
```

配置安全策略使安全域 RBM 与安全域 Local 之间的报文互通，保证 RBM 通道建立成功

```
[M9K2-security-policy-ip]rule name Local-RBM
[M9K2-security-policy-ip-7-Local-RBM]source-zone Local
[M9K2-security-policy-ip-7-Local-RBM]destination-zone RBM
[M9K2-security-policy-ip-7-Local-RBM]action pass
[M9K2-security-policy-ip]rule name RBM-Local
[M9K2-security-policy-ip-8-RBM-Local]source-zone RBM
[M9K2-security-policy-ip-8-RBM-Local]destination-zone Local
[M9K2-security-policy-ip-8-RBM-Local]action pass
```

配置 RBM 控制通道的对端 IP 地址为 11.1.1.1，端口号使用默认的 66064。

```
<M9K2> system-view
[M9K2] remote-backup group
[M9K2-remote-backup-group] remote-ip 11.1.1.1
```

配置 RBM 控制通道的本端 IP 地址为 11.1.1.2。

```
[M9K2-remote-backup-group] local-ip 11.1.1.2
```

配置 RBM 的数据通道，本举例使用控制通道的物理链路建立。

```
[M9K2-remote-backup-group] data-channel interface FortyGigE7/0/2
```

配置设备的管理角色为备管理设备。

```
[M9K2-remote-backup-group] device-role secondary
```

配置 RBM 双机热备的模式为主备模式。（默认是主备模式）

```
[M9K2-remote-backup-group] undo backup-mode
```

开启 RBM 热备功能。

```
[M9K2-remote-backup-group] hot-backup enable
```

开启配置信息自动备份功能。

```
[M9K2-remote-backup-group] configuration auto-sync enable
```

开启配置信息一致性检查功能，并设置周期为 12 小时。

```
[M9K2-remote-backup-group] configuration sync-check interval 12
[M9K2-remote-backup-group] quit
```

配置 RBM 与 VRRP 关联。在接口 FortyGigE7/0/1 创建 VRRP 备份组 1，其虚拟 IP 地址为 20.1.1.3，并配置其属于 VRRP standby 组。

```
[M9K2] interface FortyGigE7/0/1
[M9K2-FortyGigE7/0/2] vrrp vrid 1 virtual-ip 20.1.1.3 standby
```

配置 RBM 与 VRRP 关联。在接口 FortyGigE7/0/4 创建 VRRP 备份组 2，其虚拟 IP 地址为 30.1.1.3，并配置其属于 VRRP standby 组。

```
[M9K2] interface FortyGigE7/0/4
[M9K2-FortyGigE7/0/2] vrrp vrid 2 virtual-ip 30.1.1.3 standby
```

若存在 HTTP 或 DNS 应用协议的流量，还需开启对应的会话备份功能。

```
<M9K1> system
[M9K1] session synchronization http
[M9K1] session synchronization dns
```

(4) 配置 SW1

在 SW1 上创建 VLAN 10，并将连接 M9K1、M9K2 的接口设置成工作在二层模式，接口链路类型为 Access，并将接口加入 VLAN 10。

(5) 配置 SW2

在 SW2 上创建 VLAN 10，并将连接 M9K1、M9K2 的接口设置成工作在二层模式，接口链路类型为 Access，并将接口加入 VLAN 10。

5.3.4 注意事项

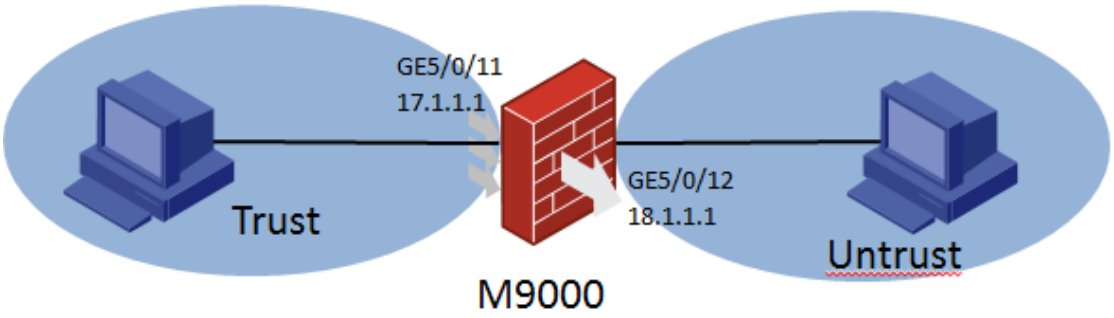
- 不支持会话引流；
- 不支持手动备份组；
- 要求进行双机热备份的两台设备主控板的数量相同，接口板的位置、类型和数量都相同，业务板的数量和位置相同，否则会出现主用设备备份过去的信息，与备用设备的物理配置无法兼容，导致主备切换后出现问题。
- 要求主备设备的对应接口必须加入到相同的安全区域。如主用设备的 GigabitEthernet1/0/0 接口加入了 Trust 区域，那么备用设备的 GigabitEthernet1/0/0 接口也必须加入 Trust 区域。
- 要求主备设备的 HASH 选板模式、HASH 因子配置一致。
- 热备口支持三层物理口和聚合口，聚合口最多支持 8 个成员口。
- 要求构成 vrrp 组网的两个 Context, Context ID 必须相同。
- VRRP 不支持 IPv6 与 rbm 联动功能。
- 配置同步功能只在主上生效，即：在配置主上敲的命令可以同步到配置备，在配置备上敲命令的话不会往主上同步，所以建议相关配置操作都在配置主上进行。
- AFT 业务功能不支持 VRRP 双主功能。
- VRRP 不支持 nat easyip。

6 M9000 的安全策略基本配置

6.1 组网需求

某公司以 Device 作为网络边界安全防护设备，配置安全策略，使得 Trust 域的用户可以访问 untrust 域内的用户，但 untrust 内的用户不能访问 trust 内用户。

图6-1 安全策略基本功能组网图



6.2 配置思路

- 配置接口地址，分别将接口加入 trust 和 untrust 域
- 配置地址对象组
- 配置服务对象组
- 配置安全策略，安全策略中引用地址对象组和服务对象组

6.3 配置步骤

配置接口 GigabitEthernet 5/0/11 的地址。

```
[m9k_C1]interface GigabitEthernet 5/0/11
[m9k_C1-GigabitEthernet5/0/11]ip address 17.1.1.1 24
[m9k_C1-GigabitEthernet5/0/11]quit
```

配置接口 GigabitEthernet 5/0/12 的地址

```
[m9k_C1]interface GigabitEthernet 5/0/12
[m9k_C1-GigabitEthernet5/0/12]ip address 18.1.1.1 24
[m9k_C1-GigabitEthernet5/0/12]quit
```

在命令行下将接口 GigabitEthernet 5/0/11 加入 Trust 域。

```
[m9k_C1]security-zone name Trust
[m9k_C1-security-zone-Trust]import interface GigabitEthernet 5/0/11
[m9k_C1-security-zone-Trust]quit
```

在命令行下将接口 GigabitEthernet 5/0/12 加入 Untrust 域。

```
[m9k_C1]security-zone name Untrust
[m9k_C1-security-zone-Untrust]import interface GigabitEthernet 5/0/12
[m9k_C1-security-zone-Untrust]quit
```

创建名称为 trust-untrust 的地址对象组，IP 地址范围从 17.1.1.2~17.1.1.200

```
[m9k_C1]object-group ip address trust-untrust
[m9k_C1-obj-grp-ip-trust-untrust]network range 17.1.1.2 17.1.1.200
[m9k_C1-obj-grp-ip-trust-untrust]quit
```

创建名称为 untrust-trust 的地址对象组，IP 地址范围从 18.1.1.2~18.1.1.200

```
[m9k_C1]object-group ip address untrust-trust
[m9k_C1-obj-grp-ip-untrust-trust]network range 18.1.1.2 18.1.1.200
[m9k_C1-obj-grp-ip-untrust-trust]quit
```

创建名称为 tcp 的服务对象组，并定义其支持的服务为 tcp

```
[m9k_C1]object-group service tcp
[m9k_C1-obj-grp-service-tcp]service tcp source gt 1023 destination gt 79
[m9k_C1-obj-grp-service-tcp]quit
```

创建安全策略 trust-untrust，过滤条件为：源 IP 地址为 trust-untrust 的地址对象组，目的地址为 untrust-trust 地址对象组，服务对象组为 tcp；开启日志记录和命中策略计数功能。

```
[m9k_C1]security-policy ip
[m9k_C1-security-policy-ip]rule 6 name trust-untrust
[m9k_C1-security-policy-ip-6-trust-untrust]source-ip trust-untrust
[m9k_C1-security-policy-ip-6-trust-untrust]destination-ip untrust-trust
[m9k_C1-security-policy-ip-6-trust-untrust]action pass
[m9k_C1-security-policy-ip-6-trust-untrust]service tcp
[m9k_C1-security-policy-ip-6-trust-untrust]logging enable
[m9k_C1-security-policy-ip-6-trust-untrust]counting enable
[m9k_C1-security-policy-ip-6-trust-untrust]quit
[m9k_C1-security-policy-ip-6]quit
```

6.4 注意事项

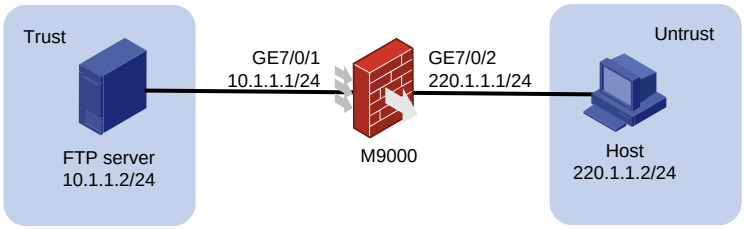
- 当安全策略与包过滤同时配置时，因为安全策略对报文的处理在包过滤之前，报文与安全策略规则匹配成功后，不再进行包过滤处理，所以请合理配置安全策略和包过滤，否则可能会导致配置的包过滤不生效。
- 配置安全策略时，请按照“深度优先”的原则（即控制范围小的、条件细化的在前，范围大的在后）进行配置。

7 M9000 的 NAT 基本功能

7.1 组网需求

如图 7-1 所示，M9000 连接内网和外网，FTP Server 处于内网，IP 地址为 10.1.1.2，Host 在外网，IP 地址为 220.1.1.2。现在 Host 以公网地址 220.1.1.1 访问 FTP Server，需要对 Host 地址进行 NAT Outbound 转换，转换地址池地址为 10.1.1.100～10.1.1.102。

图7-1 NAT 基本功能组网图



7.2 配置思路

- 配置接口地址。把接口 GigabitEthernet7/0/2 加入到 Untrust 域、GigabitEthernet7/0/1 加入到 Trust 域。
- 在接口 GigabitEthernet7/0/2 上配置 NAT Server，Server 地址为 220.1.1.1，私网地址为 10.1.1.1.2。
- 外网在 Untrust 域、内网在 Trust 域，创建 Untrust 域到 Trust 域的安全策略。

7.3 配置步骤

配置接口地址。

```
<Sysname> System-view
[Sysname] interface GigabitEthernet 7/0/2
[Sysname-GigabitEthernet7/0/2] ip address 10.1.1.1 24
[Sysname-GigabitEthernet7/0/2] quit
[Sysname] interface GigabitEthernet 7/0/2
[Sysname-GigabitEthernet7/0/2] ip address 220.1.1.1 24
```

在接口 GigabitEthernet7/0/2 上配置 NAT server。

```
[Sysname-GigabitEthernet7/0/2] nat server protocol tcp global 220.1.1.1 ftp inside 10.1.1.2
ftp
[Sysname-GigabitEthernet7/0/2] quit
```

创建 NAT 地址池。

```
[Sysname] nat address-group 0
[Sysname-address-group-0] address 10.1.1.100 10.1.1.102
[Sysname-address-group-0] quit
```

配置需要地址转换的 ACL。

```
[Sysname] acl basic 2999
[Sysname-acl-ipv4-basic-2999] rule 0 permit source 220.1.1.0 0.0.0.255
[Sysname-acl-ipv4-basic-2999] quit
```

在内网端口上配置 NAT Outbound。

```
[Sysname] interface GigabitEthernet 7/0/1
[Sysname-GigabitEthernet7/0/1] nat outbound 2999 address-group 0
[Sysname-GigabitEthernet7/0/1] quit
```

将接口 GigabitEthernet7/0/1 加入到 Trust 域。

```
[Sysname] security-zone name trust
```

```
[Sysname-security-zone-Trust] import interface GigabitEthernet 7/0/1
[Sysname-security-zone-Trust] quit
```

将接口 GigabitEthernet7/0/2 加入到 Untrust 域。

```
[Sysname] security-zone name untrust
[Sysname-security-zone-Untrust] import interface GigabitEthernet 7/0/2
[Sysname-security-zone-Untrust] quit
```

配置地址对象。

```
[Sysname] object-group ip address testSouAddr
[Sysname-obj-grp-ip-testSouAddr] network host address 220.1.1.2
[Sysname-obj-grp-ip-testSouAddr] quit
[Sysname] object-group ip address testDestAddr
[Sysname-obj-grp-ip-testDestAddr] network host address 10.1.1.2
[Sysname-obj-grp-ip-testDestAddr] quit
```

配置安全策略

```
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule name testObjPol
[Sysname-security-policy-ip-7-testObjPol] source-ip testSouAddr
[Sysname-security-policy-ip-7-testObjPol] destination-ip testDestAddr
[Sysname-security-policy-ip-7-testObjPol] service ftp
[Sysname-security-policy-ip-7-testObjPol] source-zone untrust
[Sysname-security-policy-ip-7-testObjPol] destination-zone trust
[Sysname-security-policy-ip-7-testObjPol] action pass
[Sysname-security-policy-ip-7-testObjPol] quit
[Sysname-security-policy-ip] quit
```

7.4 注意事项

- 对于 NAT Server 来说，在安全策略中规则匹配的目的地址为 NAT Server 转换后的私网地址。
- 对于 NAT Outbound 来说，在安全策略中，规则匹配的源地址为转换前的地址。
- 每个接口下可以配置的 NAT server，最多可支持 2048 个。
- 每个接口下配置 nat outbound，最多可支持 2048 个。
- NAT 地址池个数，最多可支持 256 个。
- 每个 NAT 地址池中的地址总数，最多可支持 65535 个。
- 每个地址池中地址条目，最多可支持 64 个。
- NAT 地址池配置注意事项

地址池的地址尽量配成一个完整的掩码地址，配置地址尽量为 0～2^n 或者 2^n～2^(n+1)-1，其中 n>0。

下面的地址段配置是正常最优的：

10.1.1.0~10.1.1.255

11.1.1.4~ 11.1.1.17

下面的地址段配置不可取：10.1.1.3~10.1.1.255

也就是说最好按照子网掩码去划分最优(要求包含子网的全零和全 1 地址)，如：

10.1.1.4-10.1.1.7(10.1.1.4/30)

10.1.1.8-10.1.1.11(10.1.1.8/30)

10.1.1.8-10.1.1.15(10.1.1.8/29)

10.1.1.16-10.1.1.31(10.1.1.16/28)

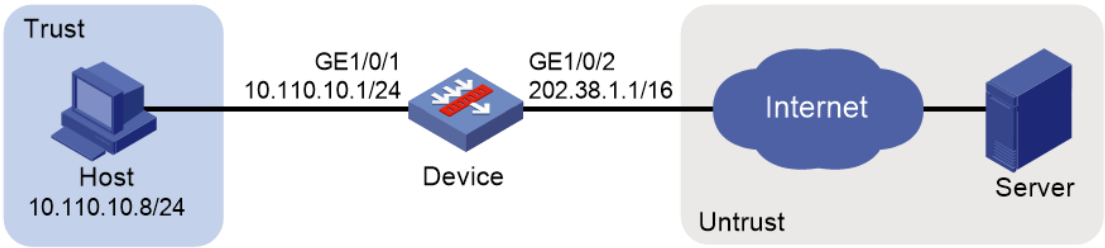
10.1.1.32-10.1.1.63(10.1.1.32/27)

8 内网用户通过 NAT 访问外网（静态地址转换）

8.1 组网需求

如图 8-1 所示，内部网络用户 10.110.10.8/24 使用外网地址 202.38.1.100 访问 Internet。

图8-1 NAT 基本功能组网图



8.2 配置思路

- 配置接口地址。把接口 GigabitEthernet1/0/2 加入到 Untrust 域、GigabitEthernet710/1 加入到 Trust 域。
- 配置内网 IP 地址 10.110.10.8 到外网地址 202.38.1.100 之间的一对一静态地址全局 nat 规则。
- 外网在 Untrust 域、内网在 Trust 域，创建 Untrust 域和 Trust 域的安全策略。

8.3 配置步骤

配置接口地址。

```
<Sysname> System-view
[Sysname] interface GigabitEthernet 1/0/2
[Sysname-GigabitEthernet1/0/2] ip address 202.38.1.1 16
[Sysname-GigabitEthernet1/0/2] quit
[Sysname] interface GigabitEthernet 1/0/1
[Sysname-GigabitEthernet1/0/1] ip address 10.110.10.1 24
```

#配置内网 IP 地址 10.110.10.8 到外网地址 202.38.1.100 之间的一对一静态地址全局 nat 规则。

```
[Sysname] nat global-policy
[Sysname-nat-global-policy] rule name Rule_1
[Sysname-nat-global-policy-rule_Rule_1]source-ip host 10.110.10.8
[Sysname-nat-global-policy-rule_Rule_1]source-zone Trust
[Sysname-nat-global-policy-rule_Rule_1]destination-zone Untrust
[Sysname-nat-global-policy-rule_Rule_1]action snat static ip-address 202.38.1.1
```

将接口 GigabitEthernet1/0/1 加入到 Trust 域。

```
[Sysname] security-zone name Trust
[Sysname-security-zone-Trust] import interface GigabitEthernet 1/0/1
[Sysname-security-zone-Trust] quit
```

将接口 GigabitEthernet1/0/2 加入到 Untrust 域。

```
[Sysname] security-zone name Untrust
[Sysname-security-zone-Untrust] import interface GigabitEthernet 1/0/2
[Sysname-security-zone-Untrust] quit
```

配置安全策略。

```
[Sysname] security-policy ip
[Sysname-security-policy-ip]rule name Trust-Untrust
[Sysname-security-policy-ip-Trust-Untrust]action pass
[Sysname-security-policy-ip-Trust-Untrust]quit
[Sysname-security-policy-ip] rule name Untrust-Trust
[Sysname-security-policy-ip-Untrust-Trust]action pass
```

8.4 注意事项

- 对于全局 NAT 来说，匹配全局 NAT 中的规则才能进行地址转换
- 对于全局 NAT 要结合会话引流使用

9 SSL VPN

9.1 SSL VPN简介

SSL VPN 目前主要有如下几种：

- Web 接入方式：使用户能够通过 Web 接入方式访问企业内网资源。
- TCP 接入方式：使用户能够通过 TCP 接入方式访问企业内网资源。
- IP 接入方式：使用户能够通过 IP 接入方式访问企业内网资源。

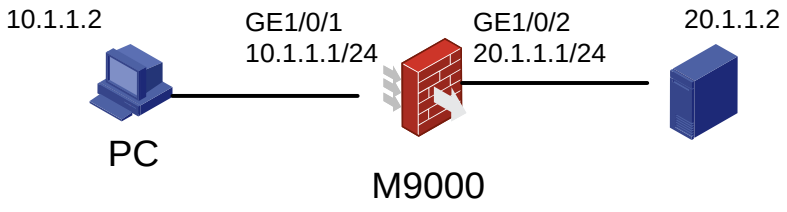
说明：目前 M9000 系列暂不支持 Web 和 TCP 的接入方式。

9.2 配置IP接入方式

9.2.1 组网需求

PC 通过 SSL VPN 网关设备安全地访问服务器端的特定 IP 资源。

图9-1 组网图



9.2.2 配置思路

- 配置接口地址，安全域及安全策略
- 配置 PKI domain。
- 导入 CA 证书和服务器证书。
- 配置 ssl 服务器端策略。
- 配置 SSL VPN 网关。
- 配置 SSL VPN 的 AC 口，以及地址池。
- 配置 SSL VPN 访问实例，并在实例下创建路由表项和策略组。
- 配置本地用户。

9.2.3 配置步骤

配置接口地址

```
<System> system-view
[System] interface GigabitEthernet1/0/1
[Sysname-GigabitEthernet1/0/1] ip address 10.1.1.1 255.255.255.0
[Sysname-GigabitEthernet1/0/1] quit
[System] interface GigabitEthernet1/0/2
[Sysname-GigabitEthernet1/0/2] ip address 20.1.1.1 255.255.255.0
[Sysname-GigabitEthernet1/0/2] quit
```

配置 PKI 域 sslvpn

```
[System] pki domain sslvpn
[System-pki-domain-sslvpn] public-key rsa general name sslvpn
[System-pki-domain-sslvpn] undo crl check enable
[System-pki-domain-sslvpn] quit
```

导入 CA 证书 ca.cer 和服务器证书 server.pfx。

```
[System] pki import domain sslvpn der ca filename ca.cer
[System] pki import domain sslvpn p12 local filename server.pfx
```

配置 SSL 服务器端策略 ssl。

```
[System] ssl server-policy ssl
[System-ssl-server-policy-ssl] pki-domain sslvpn
[System-ssl-server-policy-ssl] quit
```

配置 SSL VPN 网关 gw。

```
[System] sslvpn gateway gw
[System-sslvpn-gateway-gw] ip address 10.1.1.1 port 2000
[System-sslvpn-gateway-gw] ssl server-policy ssl
[System-sslvpn-gateway-gw] service enable
[System-sslvpn-gateway-gw] quit
```

创建 SSL VPN AC 接口 1，并创建地址池 ippool

```
[System] interface sslvpn-ac 1
[System-SSLVPN-AC1] ip address 1.1.1.100 24
[System-SSLVPN-AC1] quit
```

```
[System] sslvpn ip address-pool ippool 1.1.1.1 1.1.1.10
```

将 AC 口加入安全域

```
[System] security-zone name trust
[System-security-zone-Trust] import interface SSLVPN-AC 1
```

配置 SSL VPN 访问实例 ctx1，在实例下创建路由表项和策略组，开启服务。

```
[System] sslvpn context ctx1
[System-sslvpn-context-ctx1] gateway gw
[System-sslvpn-context-ctx1] ip-tunnel interface sslvpn-ac 1
[System-sslvpn-context-ctx1] ip-route-list rtlist
[System-sslvpn-context-ctx1-route-list-rtlist] include 2.1.1.0 255.255.255.0
[System-sslvpn-context-ctx1-route-list-rtlist] quit
[System-sslvpn-context-ctx1] policy-group pgroup
[System-sslvpn-context-ctx1-policy-group-pgroup] ip-tunnel address-pool ippool mask
255.255.255.0
[System-sslvpn-context-ctx1-policy-group-pgroup] ip-tunnel access-route ip-route-list
rtlist
[System-sslvpn-context-ctx1-policy-group-pgroup] filter  ip-tunnel acl 3000
[System-sslvpn-context-ctx1-policy-group-pgroup]quit
[System-sslvpn-context-ctx1] service enable
[System-sslvpn-context-ctx1] quit
[System]acl advanced 3000
[System-acl-ipv4-adv-3000]rule permit ip
[System-acl-ipv4-adv-3000]quit
```

创建高级 ACL，配置出方向 NAT 地址转换。

```
[System] nat address-group 1
[System -nat-address-group-1] address 20.1.1.10 20.1.1.20
[System -nat-address-group-1] quit
[System] interface GigabitEthernet1/0/2
[System-GigabitEthernet1/0/2] nat outbound 3000 address-group 1
```

创建本地 SSL VPN 用户 h3c，密码为 123456，授权用户的 SSL VPN 策略组为 pgroup。

```
[System] local-user h3c class network
[System-luser-network-h3c] password simple 123456
[System-luser-network-h3c] service-type sslvpn
[System-luser-network-h3c] authorization-attribute sslvpn-policy-group pgroup
[System-luser-network-h3c] quit
```

9.2.4 登录和注意事项

1. 登录

IP 接入方式需要在相应的客户端登录：

图9-2 iNode 客户端

2. 注意事项

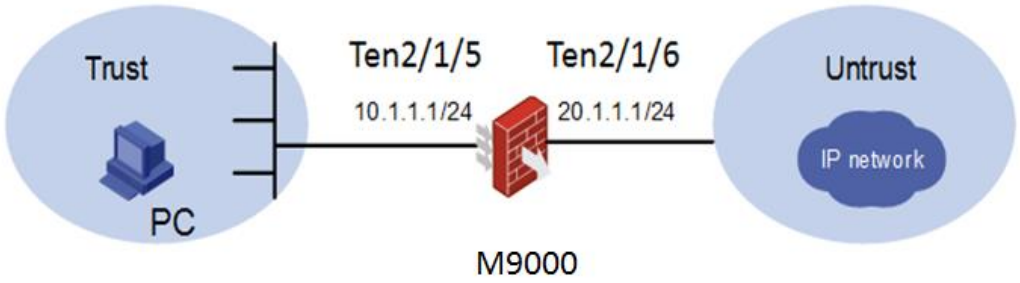
- AC 地址与 address-pool 不能有地址冲突，否则不能访问资源。
- 将接口 G1/0/1 和 G1/0/2 放入安全域。
- 配置安全策略为放行。
- 设备与 SSL VPN 客户端、Server 之间路由可达。
- Server 端有到 1.1.1.0/24 网段的路由。
- CA 证书 ca.cer 和服务器证书 server.pfx 须有效，且提前导入设备。
- 修改 sslvpn 配置后，需要在 sslvpn context 视图下先 undo service enable 再 service enable
- 需要在接口配置 nat outbound，M9K 设备当业务板数量大于等于 2 时连接服务器端的接口下需要配合使用 nat 来保证报文来回路径一致
- IP 接入方式时，AC 接口需要加入安全域并放通策略，地址池到内网资源的

PC 上需要安装 SSL VPN IP 接入的客户端，如 iNode 客户端（客户端的下载可以通过 web 访问网关去下载客户端）；

10 串行部署- IPS 模式基本功能

10.1 组网需求

图10-1 T9000 的三层 IPS 基本功能组网图



公司内部网络通过 Device 与 Internet 互连。内部网络属于 Trust 安全域，外部网络属于 Untrust 安全域。要求正确配置安全策略，使内外网所有流量都经 IPS 策略防护。

10.2 配置思路

- 配置接口 ip 并加入安全域
- 创建 IPS 策略
- 配置安全策略

10.3 配置步骤

配置接口 Ten-GigabitEthernet2/1/5 的地址。

```
[Sysname] interface Ten-GigabitEthernet 2/1/5
[Sysname-Ten-GigabitEthernet2/1/5] ip address 10.1.1.1 24
[Sysname-Ten-GigabitEthernet2/1/5] quit
```

配置接口 Ten-GigabitEthernet2/1/6 的地址。

```
[Sysname] interface Ten-GigabitEthernet 2/1/6
[Sysname-Ten-GigabitEthernet2/1/6] ip address 20.1.1.1 24
[Sysname-Ten-GigabitEthernet2/1/6] quit
```

将接口 Ten-GigabitEthernet 2/1/5 加入 Trust 域。

```
[Sysname] security-zone name trust
[Sysname-security-zone-Trust] import interface Ten-GigabitEthernet 2/1/5
[Sysname-security-zone-Trust] quit
```

在命令行下将接口 Ten-GigabitEthernet2/1/6 加入 Untrust 域。

```
[Sysname] security-zone name untrust
[Sysname-security-zone-Untrust] import interface Ten-GigabitEthernet 2/1/6
[Sysname-security-zone-Untrust] quit
```

创建 IPS 策略

```
[Sysname]ips policy ips
```

```
[Sysname-ips-policy-ips] quit
```

创建 app-profile ips，在 profile 中引用 ips 策略。

```
[Sysname] app-profile ips
[Sysname-profile-ips] ips apply policy ips mode protect
[Sysname-app-profile-ips] quit
```

创建安全策略,，并应用创建的 profile。

```
[Sysname] security-policy ip
[Sysname-security-policy-ip] rule 1 name ips
[Sysname-security-policy-ip-1-1] profile ips
[Sysname-security-policy-ip-1-1] source-zone trust
[Sysname-security-policy-ip-1-1] destination-zone untrus
[Sysname-security-policy-ip-1-1] action pass
[Sysname-security-policy-ip-1-1] quit
[Sysname-security-policy-ip] quit
```

Web 界面配置

创建 IPS 策略：对象——应用安全——入侵防御——配置文件——新建

在安全策略中应用 profile：策略—安全策略—新建—新建策略—内容安全中，IPS 策略中应用创建的 ips 策略。

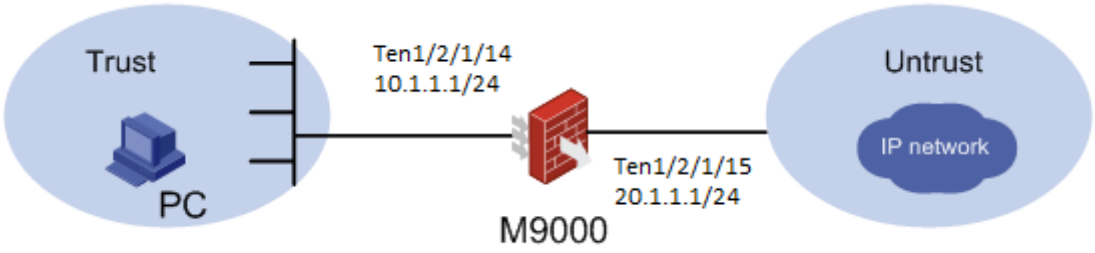
10.4 注意事项

默认情况下，创建自定义的 ips 策略同 default 策略中开启的特征状态保持一致，自定义策略中可以通过 override 命令改写具体特征的使能情况及动作。

11 AV 病毒防护基本功能

11.1 组网需求

图11-1 M9000 的 AV 基本功能组网图



公司内部网络通过 Device 与 Internet 互连。内部网络属于 Trust 安全域，外部网络属于 Untrust 安全域。要求正确配置安全策略，使内外网所有流量都经病毒防护。

11.2 配置思路

- 创建 AV 策略。
- 创建 app-profile。
- 创建安全策略。

11.3 配置步骤

配置接口 Ten-GigabitEthernet1/2/1/14 的地址。

```
[M9000-E8] interface Ten-GigabitEthernet1/2/1/14
[M9000-E8-Ten-GigabitEthernet1/2/1/14] ip address 10.1.1.1 24
[M9000-E8-Ten-GigabitEthernet1/2/1/14] quit
```

配置接口 Ten-GigabitEthernet1/2/1/15 的地址。

```
[M9000-E8] interface Ten-GigabitEthernet1/2/1/15
[M9000-E8-Ten-GigabitEthernet1/2/1/15] ip address 20.1.1.1 24
[M9000-E8-Ten-GigabitEthernet1/2/1/15] quit
```

将接口 Ten-GigabitEthernet1/2/1/14 加入 Trust 域。

```
[M9000-E8] security-zone name Trust
[M9000-E8-security-zone-Trust] import interface Ten-GigabitEthernet 1/2/1/14
[M9000-E8-security-zone-Trust] quit
```

在命令行下将接口 Ten-GigabitEthernet1/2/1/15 加入 Untrust 域。

```
[M9000-E8]security-zone name Untrust
[M9000-E8-security-zone-Untrust] import interface Ten-GigabitEthernet 1/2/1/15
[M9000-E8-security-zone-Untrust] quit
```

创建病毒策略 AV。

```
[M9000-E8] anti-virus policy AV
```

```
[M9000-E8-anti-virus-policy-av] quit
```

创建 app-profile AV，在 profile 中引用 AV 策略。

```
[M9000-E8] app-profile AV
[M9000-E8-app-profile-AV] anti-virus apply policy AV mode protect
[M9000-E8-app-profile-AV] quit
```

创建安全策略,，并应用创建的 profile。

```
[M9000-E8] security-policy ip
[M9000-E8-security-policy-ip] rule 1 name 1
[M9000-E8-security-policy-ip-1-1] profile AV
[M9000-E8-security-policy-ip-1-1] source-zone trust
[M9000-E8-security-policy-ip-1-1] destination-zone untrus
[M9000-E8-security-policy-ip-1-1] action pass
[M9000-E8-security-policy-ip-1-1] quit
[M9000-E8-security-policy-ip] quit
```

Web 界面配置

创建 AV 策略：对象——应用安全——防病毒——创建 AV 策略

在安全策略中应用 profile：策略—安全策略—新建—新建策略—内容安全中，防病毒配置文件中应用 AV 策略。

11.4 注意事项

默认情况下，创建自定义的 AV 策略同 anti-virus default 策略中开启的应用检测状态保持一致，自定义策略中可以自定义需要检测的协议及方向，并且可以配置例外策略，用户可以根据实际使用情况进行开启关闭。

12 日志

12.1 日志简介

M9000 当前支持的日志主要有如下几种：

- Syslog 日志：主要包含系统命令操作日志，日志只能以 Syslog 格式发送。
- Customlog 日志： Customlog 日志是一种快速发送日志的方式，有专门的通道；主要包含 NAT444 日志、域间策略日志、DPI 日志和 AFT 日志。对于 AFT 日志，目前仅支持 AFT 端口块日志。如果系统中配置了 NAT，也可以发送 NAT 日志，但格式为 NAT444 格式。

- Userlog 日志：NAT 日志，可以以二进制方式发送。

12.2 配置发送syslog日志

这里假定我们的日志服务器地址为：192.168.96.40，发送日志到该服务器上的配置如下：

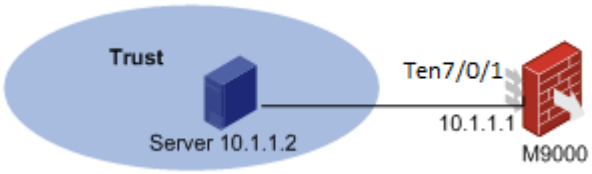
```
<Sysname> system-view
[Sysname] info-center enable
[Sysname] info-center loghost 192.168.96.40
```

12.3 配置发送customlog日志

12.3.1 配置需求

如图 12-1 所示，开启 NAT 日志功能，并设置以 customlog 格式发送各种 NAT444 日志到日志服务器 10.1.1.2 中。

图12-1 发送 customlog 日志组网图



12.3.2 配置思路

- 开启 NAT 日志功能。
- 配置 customlog 日志格式。
- 配置接口地址。

12.3.3 配置步骤

开启 NAT 日志功能。

```
<Sysname> system-view
[Sysname] nat log enable
```

配置日志格式为电信格式 NAT444 日志。

```
[Sysname] customlog format nat telecom
```

配置以电信格式将日志输出到日志服务器 10.1.1.2。

```
[Sysname] customlog host 10.1.1.2 export telecom-userlog telecom-sessionlog
```

配置 user 分配端口块日志。

```
[Sysname] nat log port-block-assign
```

配置 user 回收端口块日志。

```
[Sysname] nat log port-block-withdraw
```

配置 session 创建时，产生日志。

```
[Sysname] nat log flow-begin
```

配置 session 结束时，产生日志。

```
[Sysname] nat log flow-end
```

端口块端口占用完的告警日志。

```
[Sysname] nat log alarm
```

配置接口地址。

```
[Sysname] interface Ten-GigabitEthernet 7/0/1
[Sysname-Ten-GigabitEthernet7/0/1] ip address 10.1.1.1 24
[Sysname-Ten-GigabitEthernet7/0/1] quit
```

12.3.4 日志结果分析

(1) user 分配端口块日志格式如下

```
Jan 05 15:50:39 192.168.210.20  1 Jan 05 15:48:17 - Sysname - NAT444:userbasedA [0 45.0.0.10
- 200.0.2.202 - 6025 6536]
```

(2) user 回收端口块日志格式

```
Jan 05 15:51:09 192.168.210.20  1 Jan 05 15:48:47 - Sysname - NAT444:userbasedW [0 45.0.0.10
- 200.0.2.202 - 6025 6536]
```

(3) session 开始日志格式如下

```
Jan 05 15:50:39 192.168.210.20  1 Jan 05 15:48:17 - Sysname - NAT444:sessionbasedA [17
45.0.0.10 - 200.0.2.202 4097 6025 -]
Jan 05 15:50:39 192.168.210.20  1 Jan 05 15:48:17 - Sysname - NAT444:sessionbasedA [17
45.0.0.10 - 200.0.2.202 4096 6026 -]
```

(4) session 结束日志格式如下

```
Jan 05 15:51:05 192.168.210.20  1 Jan 05 15:48:43 - Sysname - NAT444:sessionbasedW [17
45.0.0.10 - 200.0.2.202 4096 6026 -]
Jan 05 15:51:05 192.168.210.20  1 Jan 05 15:48:43 - Sysname - NAT444:sessionbasedW [17
45.0.0.10 - 200.0.2.202 4097 6025 -]
```

(5) 端口块端口占用完的告警日志

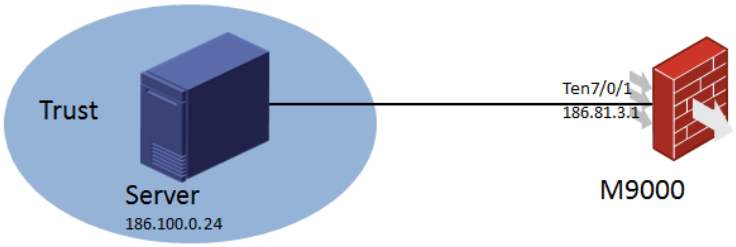
```
Jan 05 16:28:46 192.168.210.20  1 Jan 05 16:26:24 - Sysname - NAT444:userbasedF [17 45.0.0.10
- 200.0.2.202 - - -]
```

12.4 配置发送Userlog日志

12.4.1 组网需求

如图 12-2 所示，开启 NAT 日志功能，并发送 Userlog 日志到日志服务器 186.100.0.24 中。Userlog 日志用来发送 NAT 转换的日志。

图12-2 发送 Userlog 日志组网图



12.4.2 配置思路

- 开启 NAT 日志功能。
- 配置 userlog 服务器。
- 把连接日志服务器的端口加入到安全域中，并配置安全策略。

12.4.3 配置步骤

开启 NAT 日志功能。

```
<Sysname> System-view
[Sysname] nat log enable
[Sysname] nat log flow-end
```

配置日志发送主机

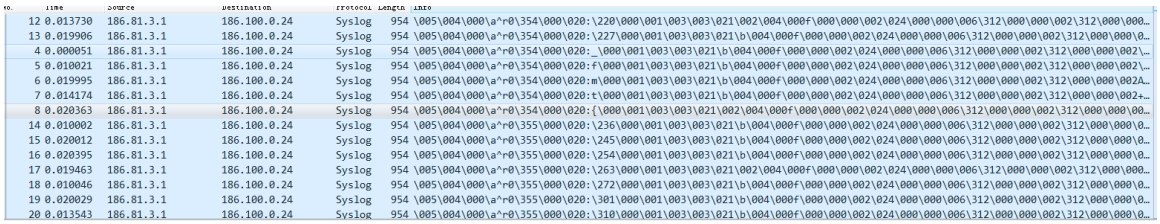
```
[Sysname] userlog flow export host 186.100.0.24 port 514
```

配置接口 IP 地址。

```
[Sysname] interface Ten-GigabitEthernet 7/0/1
[Sysname-Ten-GigabitEthernet7/0/1] ip address 186.81.3.1 16
[Sysname-Ten-GigabitEthernet7/0/1] quit
```

12.4.4 日志结果及分析

如下是 userlog 以二进制方式产生的日志：



No.	Time	Source	Destination	Protocol	Length	Info
12	0.013730	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\354\000\020:\220\000\001\003\003\021\002\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000…
13	0.019906	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\354\000\020:\227\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\0…
4	0.000051	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\354\000\020:_\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\002\…
5	0.010021	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\354\000\020:f\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\002\…
6	0.019995	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\354\000\020:m\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\002A…
7	0.014174	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\354\000\020:t\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\002+…
8	0.020363	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\354\000\020:{\000\001\003\003\021\002\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\00…
14	0.010002	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\355\000\020:\236\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\0…
15	0.020012	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\355\000\020:\245\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\0…
16	0.020395	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\355\000\020:\254\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\0…
17	0.019463	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\355\000\020:\263\000\001\003\003\021\002\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000…
18	0.010046	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\355\000\020:\272\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\0…
19	0.020029	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\355\000\020:\301\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\0…
20	0.013543	186.81.3.1	186.100.0.24	Syslog	954	\005\004\000\a^r0\355\000\020:\310\000\001\003\003\021\b\004\000f\000\000\002\024\000\000\006\312\000\000\002\312\000\000\0…

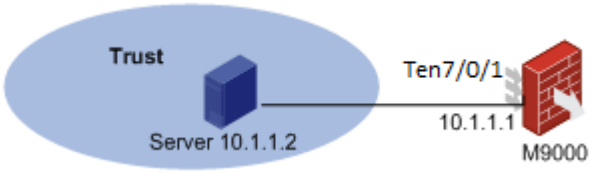
将 userlog 直接以二进制的方式输出到流日志主机上，在日志主机 wireshark 抓包，可观察到相关消息，但因为是二进制，无法直观查看消息内容(\005\004\000\a 代表日志类型为 5.0，\003\004\000\016 代表 3.0，\001\004\000$代表 1.0)

12.5 配置发送Session日志

12.5.1 组网需求

如图 12-3 所示，配置在会话建立时，产生会话日志，并发送到日志服务器 10.1.1.2。

图12-3 发送 Session 日志组网图



12.5.2 配置思路

- 配置会话产生流量阈值
- 配置会话产生的时间阈值
- 在接口下配置会话日志
- 配置日志发送的服务器

12.5.3 配置步骤

配置会话产生的字节数阈值。

```
<Sysname> System-view
[Sysname] session log bytes-active 2
```

配置会话产生的报文数阈值。

```
[Sysname] session log packets-active 1
```

配置会话产生的时间阈值。

```
[Sysname] session log time-active 10
```

在接口下配置会话日志。

```
[Sysname] interface ten-gigabitethernet7/0/1
[Sysname-Ten-GigabitEthernet7/0/1] session log enable ipv4 inbound
[Sysname-Ten-GigabitEthernet7/0/1] session log enable ipv4 outbound
[Sysname-Ten-GigabitEthernet7/0/1] quit
```

配置需要发送的日志服务器。

```
[Sysname] info-center loghost 10.1.1.2
```

12.5.4 日志结果及分析

如下是 Session 日志显示信息：

```
Jan  7 10:48:17 2014 Sysname %%10SESSION/6/SESSION_IPV4_FLOW: -Slot=3.1;
Protocol(1001)=UDP;SrcIPAddr(1003)=10.1.1.2;SrcPort(1004)=1701;NatSrcIPAddr(1005)=10.1.1
.65;NatSrcPort(1006)=5003;DstIPAddr(1007)=10.1.1.1;DstPort(1008)=1701;NatDstIPAddr(1009)
=10.1.1.1;NatDstPort(1010)=1701;InitPktCount(1044)=137;InitByteCount(1046)=6576;RplyPktC
ount(1045)=0;RplyByteCount(1047)=0;RcvVPNInstance(1042)=;SndVPNInstance(1043)=re10;RcvDS
```

```
LiteTunnelPeer(1040)=;SndDSLiteTunnelPeer(1041)=;BeginTime_e(1013)=01072014093531;EndTim
e_e(1014)=;Event(1048)=(6)Active data flow timeout;
```

12.6 注意事项

- 如果要把日志发送到日志服务器，要确保有去往服务器的路由可达。
- 配置业务口为日志发送口，不建议使用管理口作为日志发送口。
- customlog 和 userlog 不能共存。
- customlog 主要用于 NAT444 日志。Userlog 主要用于 NAT 日志。
- customlog 与 syslog 两种日志，优先配置 customlog 的日志发送方式。
- NAT日志支持userlog日志和customlog日志两种输出方式，缺省为userlog日志。
- 配置userlog以二进制方式发出时，需要在接口下配置会话日志；并且日志主机端口号为514端口；如果日志主机用其它端口，产生的信息将以UDP报文方式输出。