JUNIPER SRX 售后培训

戴 勇

http://Bbs.vlan5.com

AGENDA TECHNICAL MODULE

1. **Architecture Samples**
2. JUNOS Introduction
3. Initial Configuration
4. Device Management
5. Interface Configuration
6. Spanning Tree
7. VLAN Configuration
8. Route setup
9. Virtual Chassis

PRESALES
JUNOS 初始化配置

课程内容

- 第一章 基本操作
- 第二章 初始化配置
- 第三章 接口配置及排错
- 第四章 协议无关的路由
- 第五章 路由策略
- 第六章 OSPF配置与排错
- 第七章 Firewall Filter

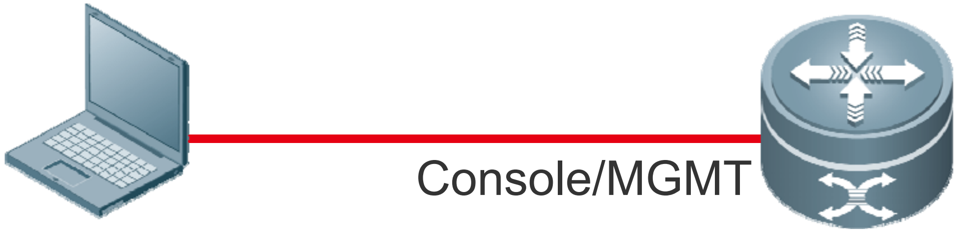
接入路由器管理端口

Console

- Db9 EIA-232 @ 9600 Bps, 8/N/1-pre-configured

MGMT, Telnet, SSH

- 需要配置



用户认证登录

本地

- 用户名密码
- 每一个用户都有一个单独的主目录
- 基于用户定义权限

RADIUS/TACACS+

- TACACS+ (只用于认证)
- RADIUS （认证授权均可）

RADIUS/TACACS+ 认证失败后返回本地认证

lab2 (ttyd0)

```
login: root

Password:
```

CLI模式

操作模式

- 监控与排错

```
root@lab2>
```

配置模式

- 配置接口、协议等

```
[edit]
root@lab2#
```

命令补全

空格补全

```
root@lab2> sh<space>ow i<space>
'i' is ambiguous.

Possible completions:
  igmp                 Show information about IGMP
  interfaces           Show interface information
  isis                 Show information about IS-IS

root@lab2> show i
```

Tab键补全

命令提示

```
lab@root> ?

Possible completions:
    clear          Clear information in the system
    configure      Manipulate software configuration information
    file           Perform file operations
    help           Provide help information
    …

lab@root> show ?

Possible completions:
    aps            Show APS information
    arp            Show system ARP table entries
    as-path        Show table of known AS paths
    …
```

Topical Help

help topic 提供 命令的说明信息

```
user@switch> help topic interfaces ?
Possible completions:
  accept-data          Accept packets destined for virtual address
  accept-source-mac    Policers for specific source MAC addresses
  accounting           Packet counts for destination and source classes
  accounting-profile   Accounting profile
  acknowledge-timer    Maximum time to wait for link acknowledgment message
  address              Interface address and destination prefix
  ...
user@switch> help topic interfaces address
                         Configuring the Interface Address

   You assign an address to an interface by specifying the address when
   configuring the protocol family. For the inet family, configure the
   interface's IP address. For the iso family, configure one or more
   addresses for the loopback interface. For the ccc, tcc, mpls, tnp, and
   vpls families, you never configure an address.
   ...
```

配置语法的帮助

用 **help reference** 命令查看配置语法

```
user@switch> help reference interfaces address
address

 Syntax

     address address {
         arp ip-address (mac | multicast-mac) mac-address <publish>;
         broadcast address;
         ...
  Hierarchy Level

     [edit interfaces interface-name unit logical-unit-number family family],
     [edit logical-routers logical-router-name interfaces interface-name unit
     logical-unit-number family family]

  Release Information

     Statement introduced before JUNOS Release 7.4.

  Description

     Configure the interface address.
  ...
```

配置模式

操作模式下输入configure或edit进入配置模式

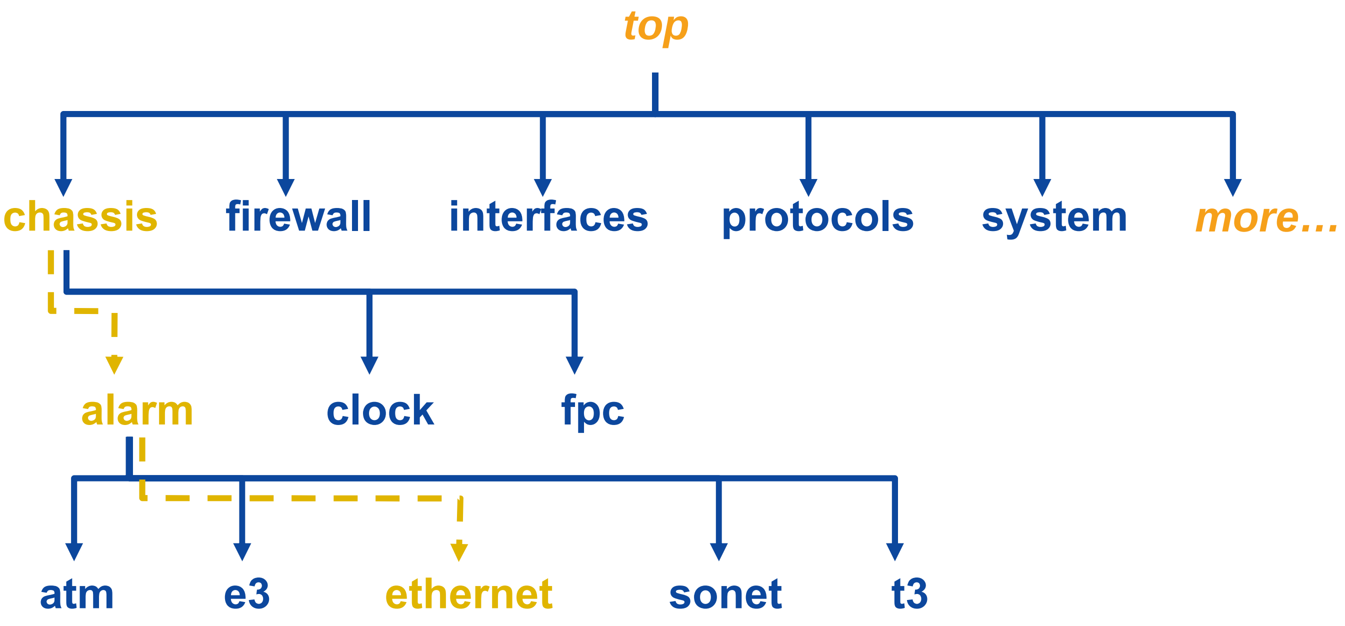
```
root@lab2> configure
Entering configuration mode
[edit]
root@lab2#
```

层次化的编辑方式

于各层次之间移动

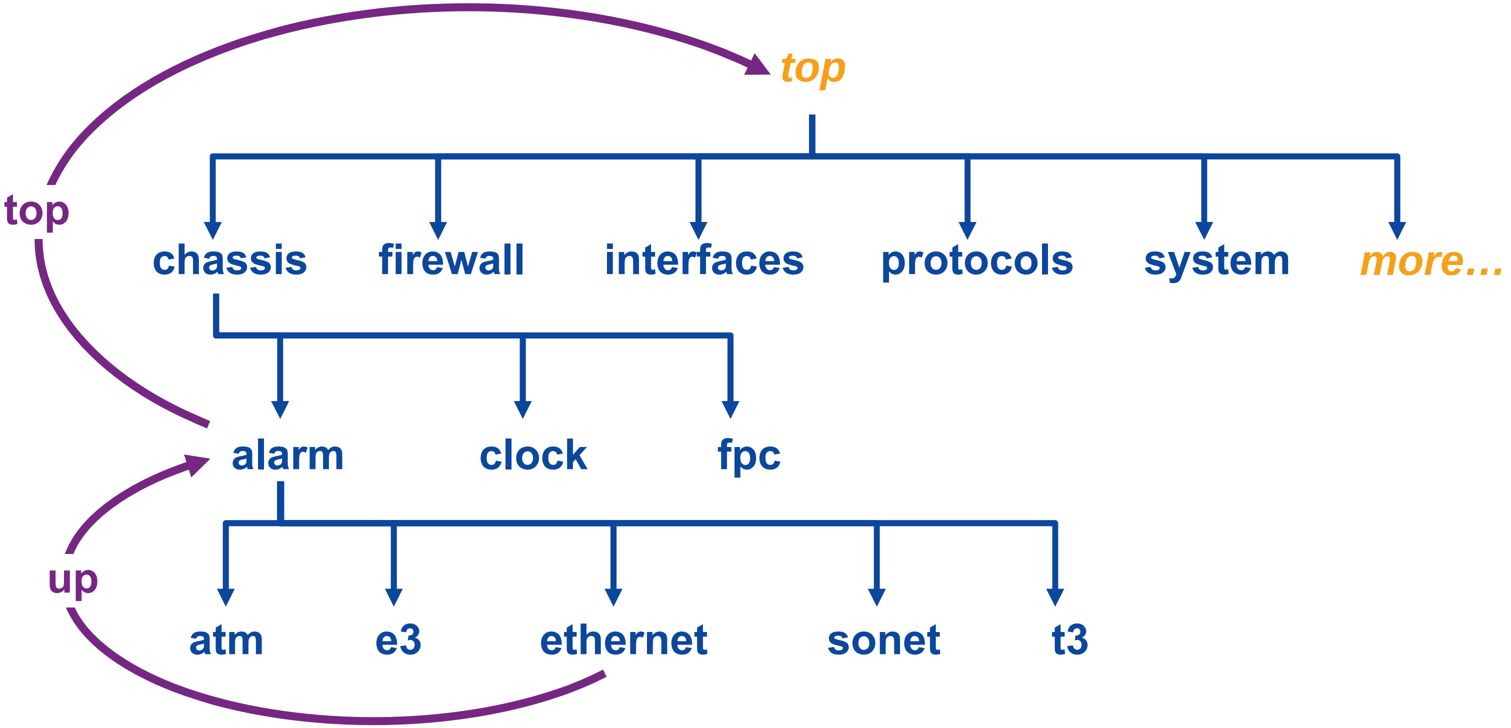
- Edit命令的工作方式类似于cd命令

```
[edit]
user@host# edit chassis alarm ethernet
[edit chassis alarm ethernet]
```



层次化的编辑方式

```
user@host# up
  [edit chassis alarm]
  user@host# top
  [edit]
```



检查配置

```
[edit]
    user@host# show chassis alarm
    sonet {
            lol red;
            pll yellow;
       }
    [edit]
    user@host# edit chassis alarm
    [edit chassis alarm]
    user@host# show
    sonet {
            lol red;
            pll yellow;
       }
    [edit chassis alarm]
```

对比配置文件

删除配置

```
user@host# set alarm sonet lol red
user@host# delete alarm sonet pll yellow
```

对比当前配置与实际运行配置的不同

```
[edit chassis]
user@host# show | compare
alarm {
   sonet {
+     lol red
      los red;
-     pll yellow;
   }
}
```

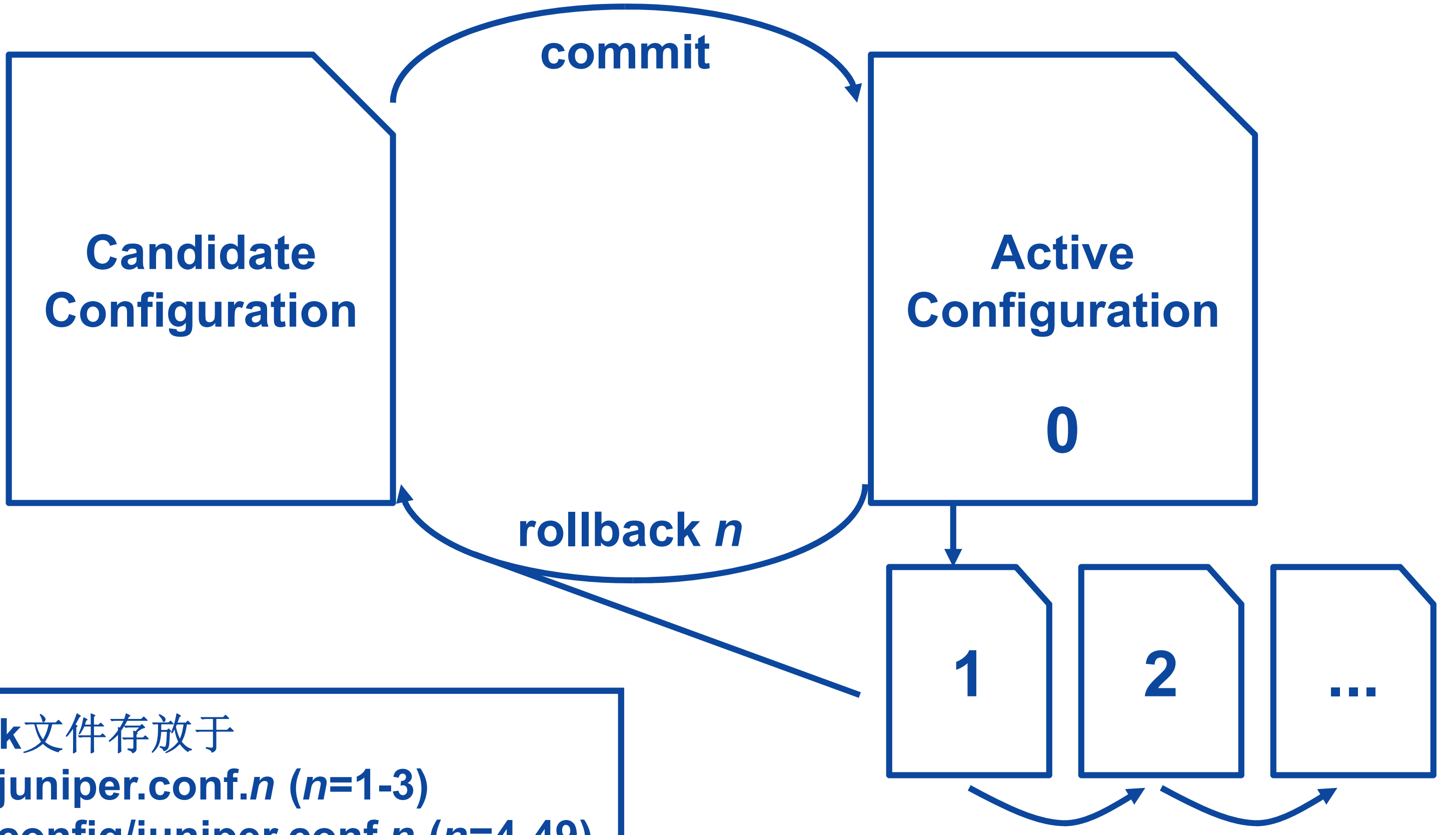
其他参数

```
user@host# show | compare filename
user@host# show | compare rollback number
```

删除配置

```
[edit]
user@host# edit chassis alarm sonet
[edit chassis alarm sonet]
user@host# delete lol
[edit chassis alarm sonet]
user@host# delete los
[edit chassis alarm sonet]
user@host#
```

提交配置



Rollback文件存放于
/config/juniper.conf.*n* (*n*=1-3)
/var/db/config/juniper.conf.*n* (*n*=4-49)

提交配置

远程配置的时候需要注意以下几点

- 路由器之间可能失去连接
- 可能失去与路由器的连接

使用命令 commit confirmed避免命令提交后出现问题

- 在一定时间内使提交的配置生效 (默认为10分钟)
- 如果10分钟内没有输入commit命令，就会自动回退到之前的配置
- 记时中一旦输入commit命令，记时就会停止

回退

使用rollback命令回退到上一次的正确配置

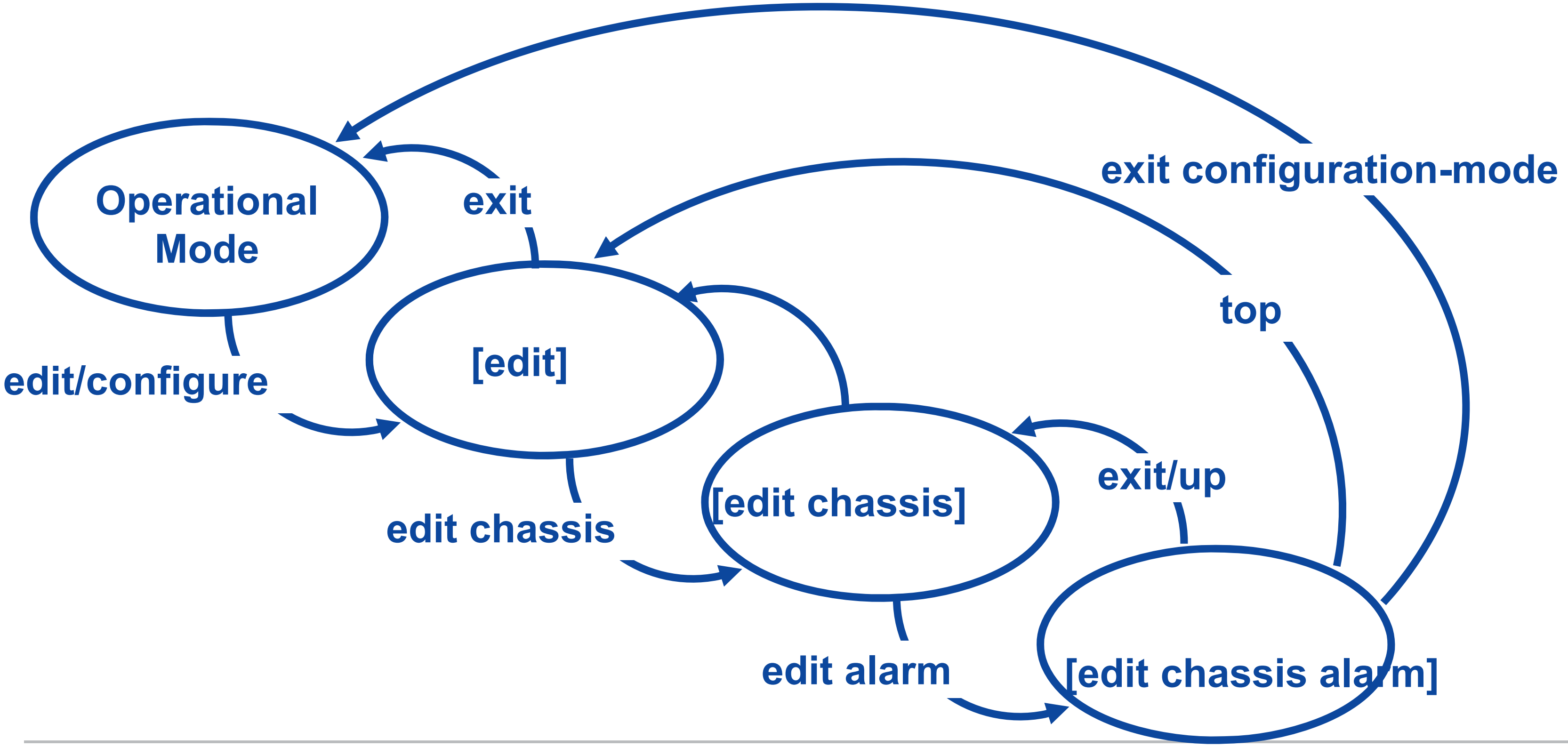
使用rollback(或rollback 0)命令将准备提交的命令重置到当前正在生效的命令(最后一次commit生效的命令)

- rollback 1 加载最后一次commit之前的第一次配置
- rollback n 加载最后一次commit之前的第N次配置

退出编辑模式

退出命令

- 使用exit向上跳一级
- 使用exit configuration-mode 退出到操作模式



保存配置文件

使用save命令保存当前层次下的配置

```
[edit]
cli# save filename
[edit]
cli#
```

可以指定文件保存的目录，否则就存放在用户的主目录下

加载配置

load 命令

- 覆盖当前的配置
  - load override *filename*
- 合并新的配置到当前配置中
  - load merge *filename*
- 提交命令
  - 使用命令commit提交后配置才能生效
- 提取终端输入的配置
  - load (merge | override) terminal

使用命令show system uptime查看系统最后一次更改配置的时间以及配置是由哪个用户提交的

排错

Craft Interface

- 红灯表示启动过程中有问题

日志

- 包括许多的细节问题
  - show log messages

CLI

- show chassis alarms
- monitor

关机重启

关机命令：lab# run request system halt

- 注意一定要先使用此条命令关机，然后方可关闭电源

重启命令：lab# run request system reboot

设备升级

第一步：使用命令set system services ftp 将设备配置为ftp server

第二步：使用flashfxp等工具将升级文件jinstall-8.2R1.7-domestic-signed.tgz上传至设备的/var/tmp目录下

第三步：#模式下使用命令run request system software add /var/tmp/jinstall-8.2R1.7-domestic-signed.tgz no-validate reboot 自动升级设备

升级过程中，通过console观察设备升级情况

升级完成后，>模式下使用show version命令查看升级后的版本情况

SALES
JUNIPER SWITCHING MARKETPLACE

课程内容

- 第一章 基本操作
- 第二章 初始化配置
- 第三章 接口配置及排错
- 第四章 协议无关的路由
- 第五章 路由策略
- 第六章 OSPF配置与排错
- 第七章 Firewall Filter

初始配置

设备第一次启动后:

- 配置root账号
  - root是默认账号
  - 出厂时没有密码
  - 必须通过console修改root密码
- 主机名
- 管理接口地址
- 远程登录
- 账号
- 时间

初始配置

以root用户登陆

```
root (ttyd0)

login: root
Last login: date on ttyd0
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
The Regents of the University of California. All rights reserved.
---JUNOS 5.3R1 built 2000-07-24 09:29:44 UTC
%
```

运行cli

```
% cli
root@root>
```

初始配置

进入配置模式

```
root@root> configure
[edit]
root@#
```

设置root密码

- 明文

```
root@root# set system root-authentication
    plain-text-password
```

- 密文

```
root@root# set system root-authentication
    encrypted-password encrypted-password
```

初始配置

设置主机名

```
[edit]
root@root# set system host-name lab2
```

提交

```
[edit]
root@# commit
commit complete

[edit]
root@lab2#
```

初始配置

设置管理接口地址

```
[edit]
root@lab2# set interfaces fxp0 unit 0 family inet
    address ip-address/prefix-length
```

远程登录

```
[edit]
root@lab2# set system services ssh
```

初始配置

建立账户

```
[edit system]
        login {
          user root {
                full-name “root”;
                uid 1001;
                class superuser;
                authentication {
                encrypted-password “$1$poPPeY”;
                }
        }
```

初始配置

配置时间

- set date *YYYYMMDDhhmm.ss*
- 时区 set system time-zone *time-zone*

日志与跟踪

跟踪数据包与路由器事件

系统日志

- UNIX的日志语法
- 监控系统事件

跟踪

- 常规路由行为
- 接口
- 协议信息
  - BGP
  - IS-IS
  - OSPF
  - RIP
  - MPLS

系统日志类别

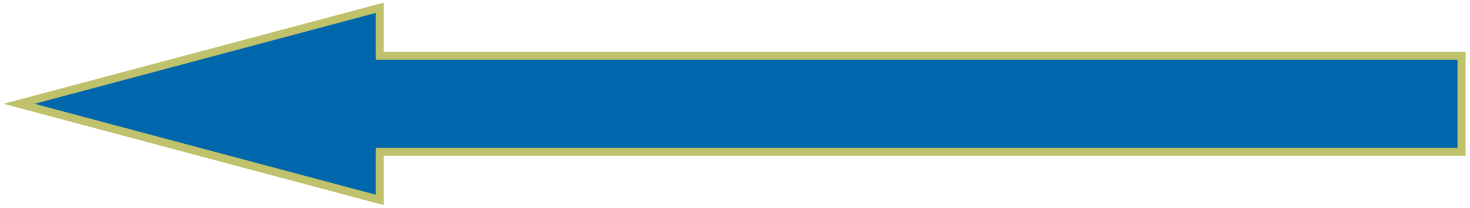
级别:

any	任意事件
authorization	系统授权
cron	定时后台程序
daemon	各种后台
interactive-commands	CLI命令
kernel	系统核心事件
user	用户事件

日志级别

向下兼容

emergency alert critical error warning notice info debug



写入日志

默认日志文件存放于硬盘的/var/log 目录下

```
file filename {
    facility level;
    archive {
        files number;
        size size;
        (world-readable | no-world-readable);
    }
}
```

写入远程设备

- 主机

```
host hostname {
   facility level;
}
```

- 用户

```
user (username | *) {
   facility level;
}
```

- console

```
console {
   facility level;
}
```

日志举例

```
syslog {
    file security {
      authorization info;
      interactive-commands info;
    }
    file messages {
      authorization notice;
      any warning;
    }
    user alex {
      any critical;
    }
    host hot-dog.juniper.net {
      daemon info;
      any warning;
    }
    console {
      any error;
    }
      }
```

跟踪

全局配置

```
[edit feature-name]
user@host# show
    traceoptions {
        file filename [replace] [size size] [files number] [no-stamp];
        flag flag [flag-modifier] [disable];
    }
```

- *feature-name* 在这两个级别下配置
  - [edit routing-options]
  - [edit protocols *protocol*] (OSPF, IS-IS, BGP, MPLS等等)

跟踪事件

常规事件:

all	所有事件
general	普通事件与路由表改变事件
normal	普通事件
policy	路由策略
route	路由表改变
state	状态转换
task	接口与进程转换
timer	时间

其他参数:

detail	细节信息
receive	接受到的数据包
send	转发的数据包

查看

Log信息默认存储于 /var/log

```
user@host> show log
total 5778
-rw-r--r-- 1 root bin   1429        Feb 25 10:11        BGP-Events
-rw-r--r-- 1 root bin   17734       Feb 17 17:26        bgp.log
-rw-r--r-- 1 root bin   9265        Feb 25 10:51        cli-commands
-rw-r--r-- 1 root bin   486         Feb 25 10:11        critical
-rw-r--r-- 1 root bin   793495      Feb 25 10:11        dcd
-rw-r--r-- 1 root bin   999987      Feb  2 09:55        dcd.0
-rw-r--r-- 1 root bin   999956      Jan 15 11:35        dcd.1
-rw-r--r-- 1 root bin   41217       Feb 25 10:51        general-routing
-rw-rw-r-- 1 root wheel 56056       Feb 25 10:11        lastlog
-rw-rw-r-- 1 root wheel 20519       Jan  8 10:18        messages
-rw-r--r-- 1 root bin   4095        Feb 25 10:05        ospf-log
-rw-r--r-- 1 root bin   438         Feb 25 10:05        problem-neighbor
```

监控log信息

命令:

- **user@host>** monitor (start | stop) *filenames*
- 用Esc-Q 打开/关闭log信息输出
- monitor stop 关闭所有监控的log信息
- 关闭跟踪:

[edit protocols bgp traceoptions]

user@host# delete flag open

- 清空log文件:

user@host# clear log *filename*

课程内容

- 第一章 基本操作
- 第二章 初始化配置
- 第三章 接口配置及排错
- 第四章 协议无关的路由
- 第五章 路由策略
- 第六章 OSPF配置与排错
- 第七章 Firewall Filter

配置接口

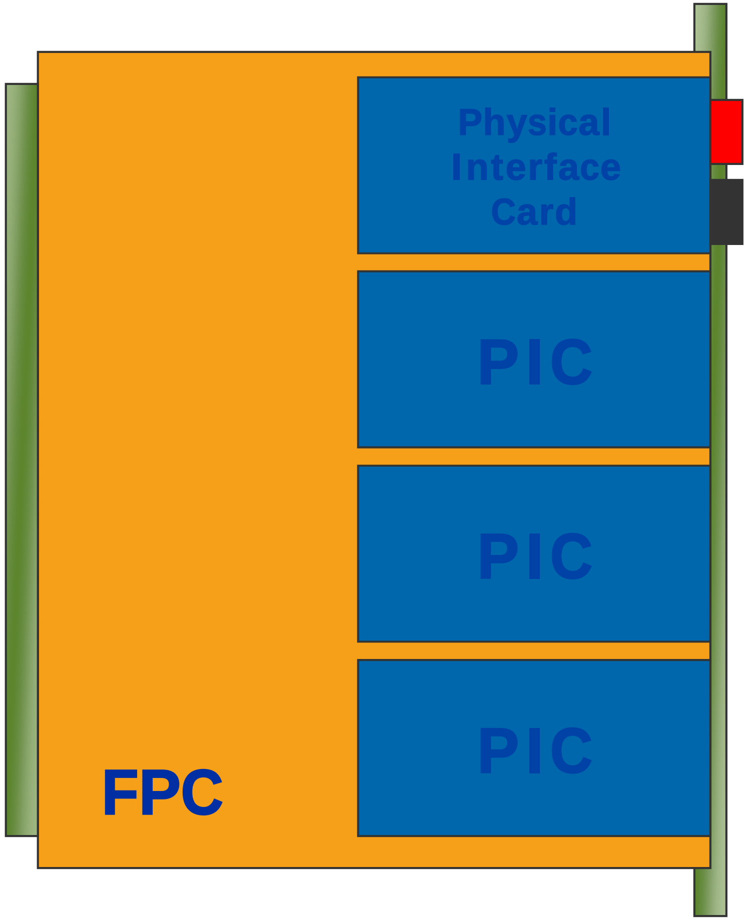
接口配置包括以下几点

- 标准接口
- 接口名
- 永久接口
- 物理参数
- 逻辑参数

标准接口

这些接口位于:

- 线卡上
- 线卡插在FPC上
  - FPC有4个线卡插槽
- FPC插在机箱上
- PIC-物理接口卡

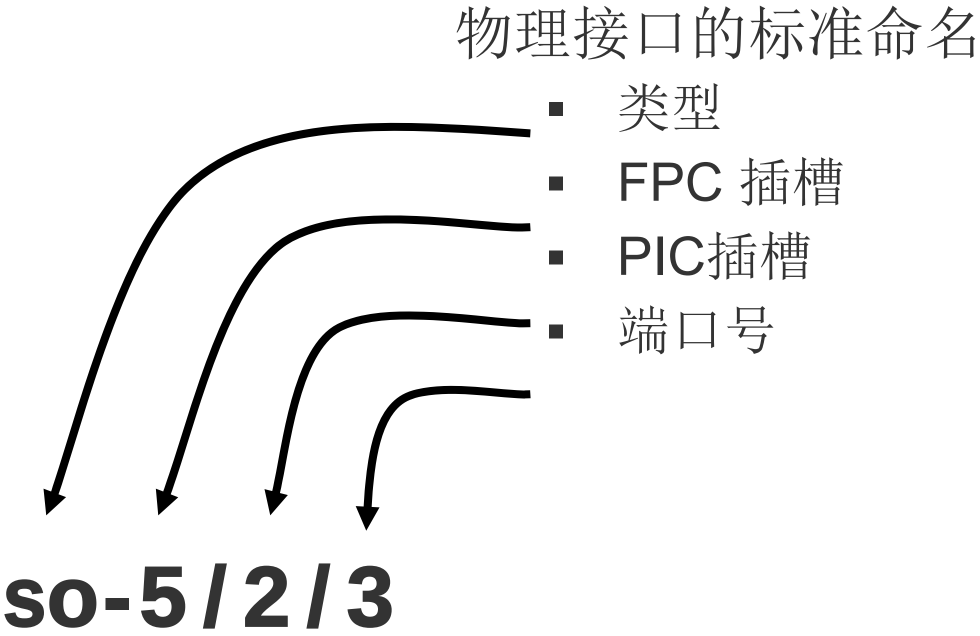


接口介质类型

介质类型:

- at—ATM over SONET/SDH ports
- e1—E1 ports
- fe—Fast Ethernet ports
- so—SONET/SDH ports
- ge—Gigabit Ethernet ports
- ae—Aggregated Ethernet ports

接口名



物理接口的标准命名

- 类型
- FPC 插槽
- PIC插槽
- 端口号

so-5/2/3

ge-2/1/0

JUNIPER SWITCHING MARKETPLACE

Overall Market size

Relevant APAC market numbers

Why you are here

Zones

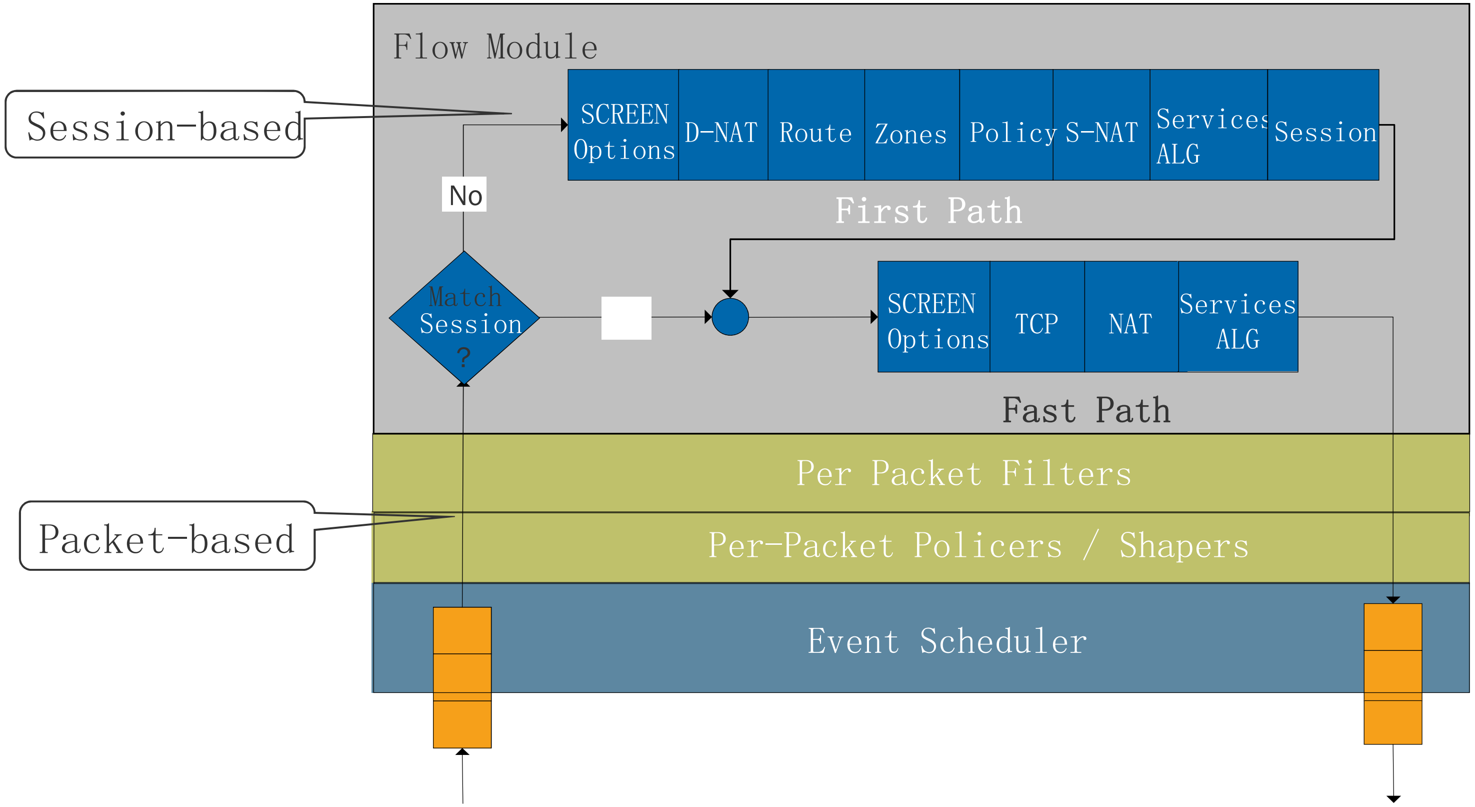
Zone（区域）是什么？

zone 是具有相同安全需求的一个或多个网络部分的集合。

区域之间的流量转发有安全策略来控制

- Null zone:
  - 系统默认zone
  - 丢弃所有流量
- 只有当接口属于non-Null zones时才能够接收和转发流量
  - 例外： fxp0

回顾: Packet Flow



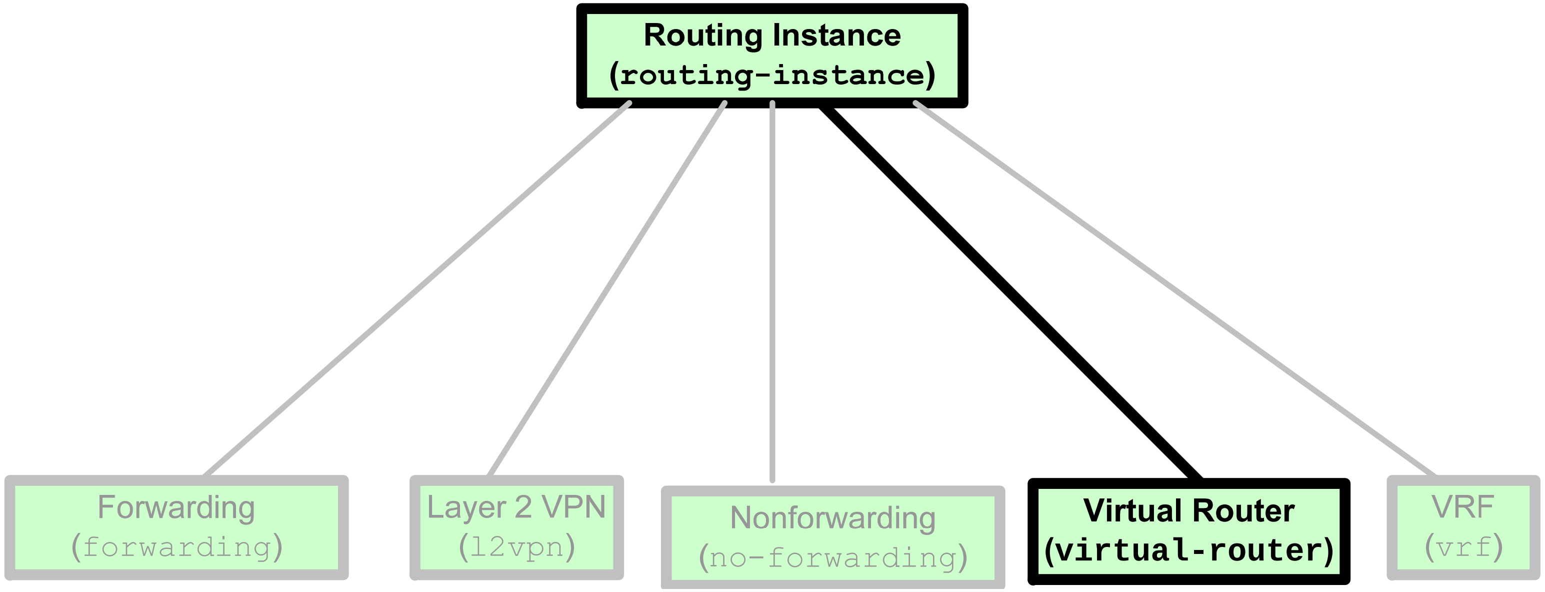
Zone 和 Interface 的分配

zones和interfaces之间存在严格的等级关系

- 一个逻辑接口属于一个区域
- 一个逻辑接口不能分配给多个区域
- 逻辑接口也可以分配给一个 routing instance
- 一个逻辑接口不能分配给多个routing instances
- 所有zone下的逻辑接口必须属于同一个 routing instance

SRX中的Routing Instances

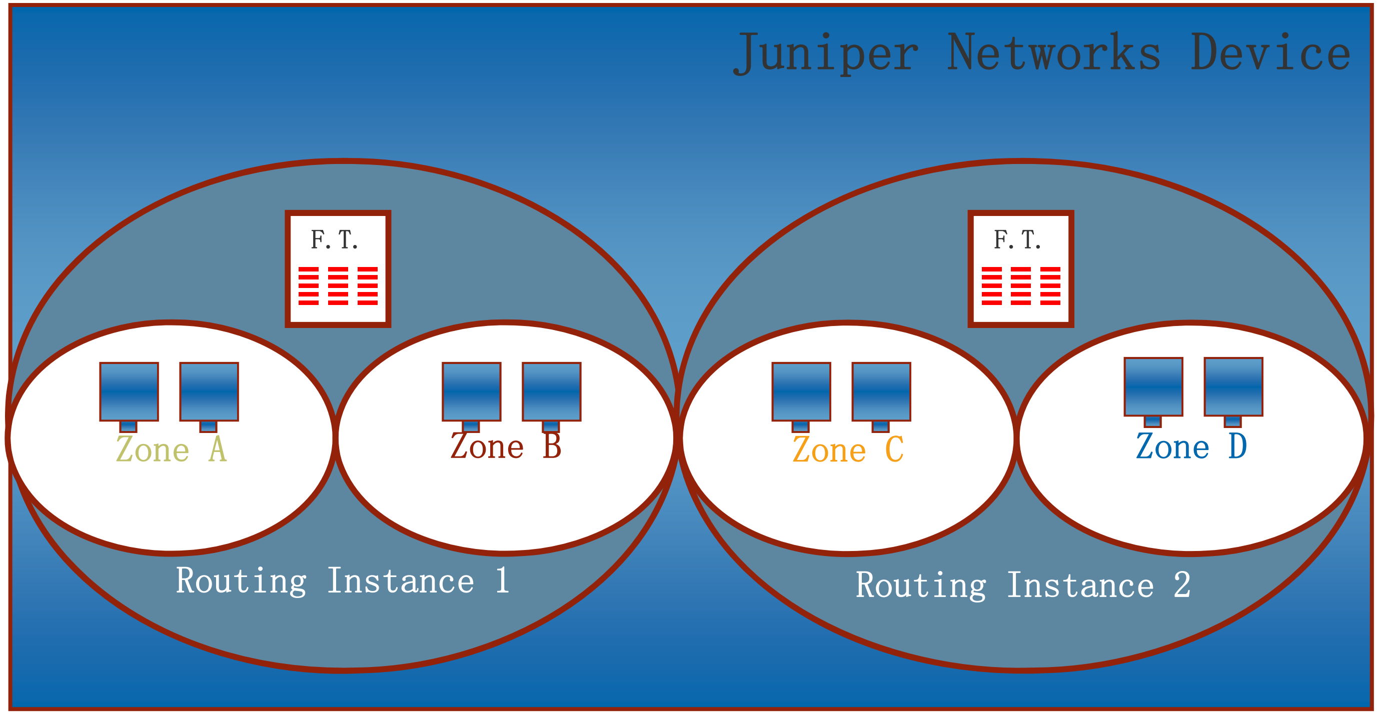
存在五种类型的Routing Instances



此次,我们涉及virtual router 类型

从属等级关系

interfaces, zones和routing instances之间的关系



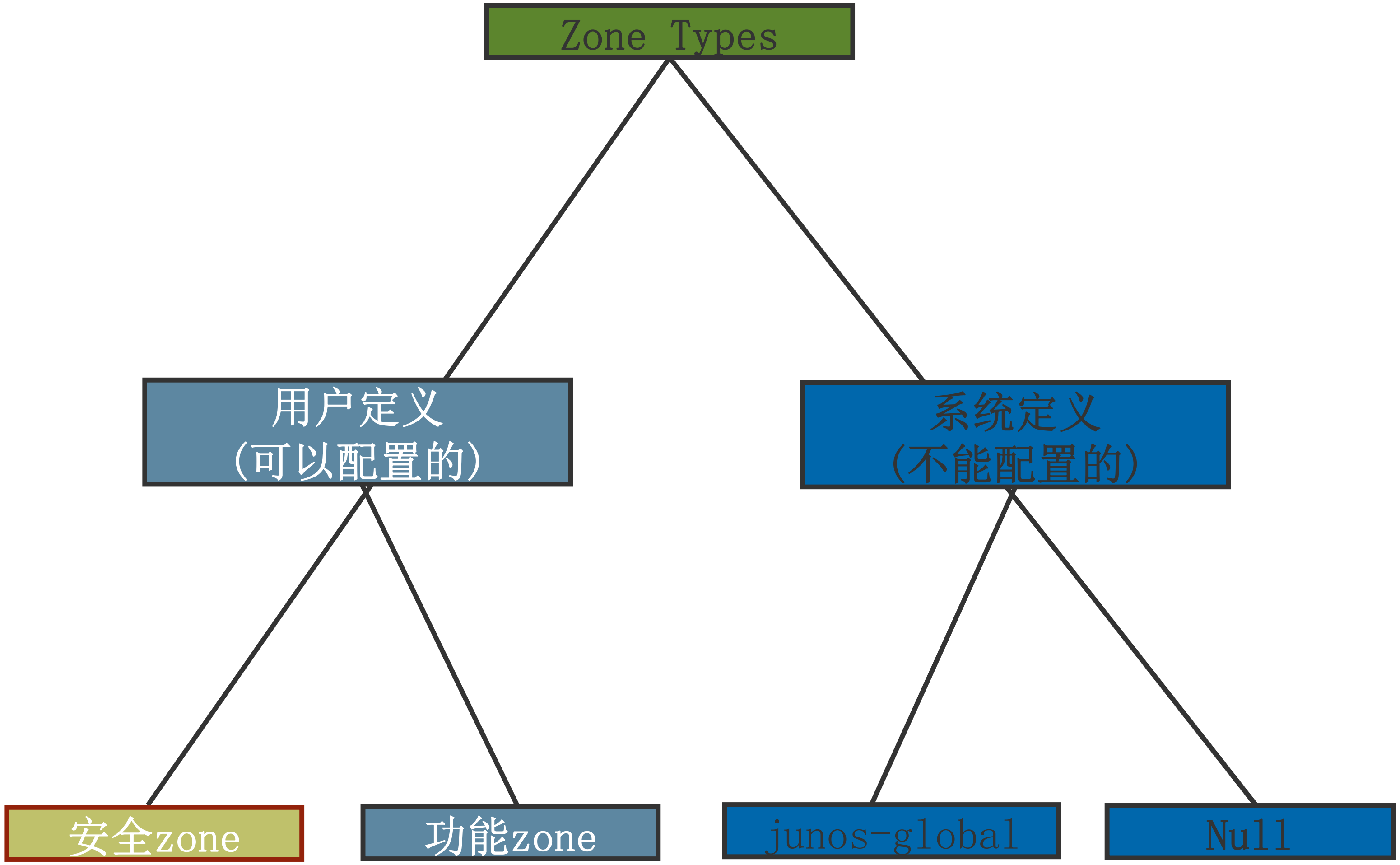
Interfaces

Zones

Routing Instance

Forwarding Table

Zone 的类型


Zone Types
用户定义
(可以配置的)
系统定义
(不能配置的)
安全zone
功能zone
junos-global
Null

用户定义的Zones

特点:

- 可以配置的
- 能够分配接口

两种类型:

- 安全zone
- 功能zone

安全 Zones

安全zones:

- 一个或多个网络部分的集合， 需要策略制定流量的进出规则
- 定义流量
- 传输流量
    - 区内和区间传输流量都必须要有安全策略
- 没有默认的安全策略
- 区属于专署的路由实例

Functional Zones

Functional zones 的功能

- 只用于—management zone
  - 设备的out-of-band管理
- 不能指定策略
- 流量不能穿越
- 只能定义一个管理的ZONE

System-Defined Zones

`junos-global` zone:

- 为 static NAT 地址提供一个存储区域
- 不能被配置
- 不能分配接口

Null zone:

- 不能被配置
- 默认情况下所有接口都属于 Null zone
- 当我们把接口从一个zone中删除, 它将进入Null zone
- JUNOS 拒绝属于Null zone接口的所有流量

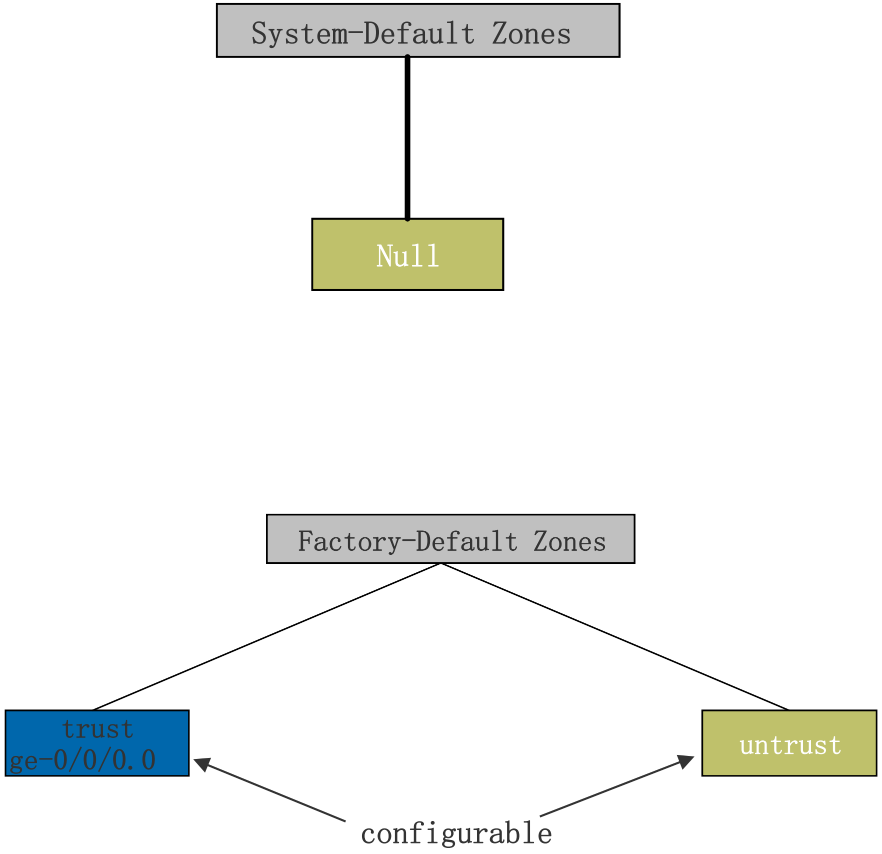
Default Zones

系统只定义了一个默认zone:

- Null

Factory-default 配置了两个安全 zones:

- trust：接口 ge-0/0/0.0 属于它
- untrust



Zone 配置方法

步骤:

- 定义安全区域或功能区域
- 添加逻辑接口
- 添加服务和协议允许通过区域内的接口进入SRX
  - 如果省略这步, 没有任何进入SRX的流量被允许

定义 Zone

进入配置模式:

```
user@host> configure
Entering configuration mode

[edit]
user@host#
```

定义一个安全区域或一个功能区域:

```
[edit]
user@host# set security zones security-zone zone-name
```

—或—

```
user@host# set security zones functional-zone management
```

功能区域说明:

- 有一种类型被定义—management
- 不能有用户定义的名字

在区域中添加逻辑接口

为zone添加逻辑接口

- 安全 zone:

```
[edit]
user@host# edit security zones

[edit security zones]
user@host# set security-zone HR interfaces ge-0/0/1.0
```

- 功能 zone:

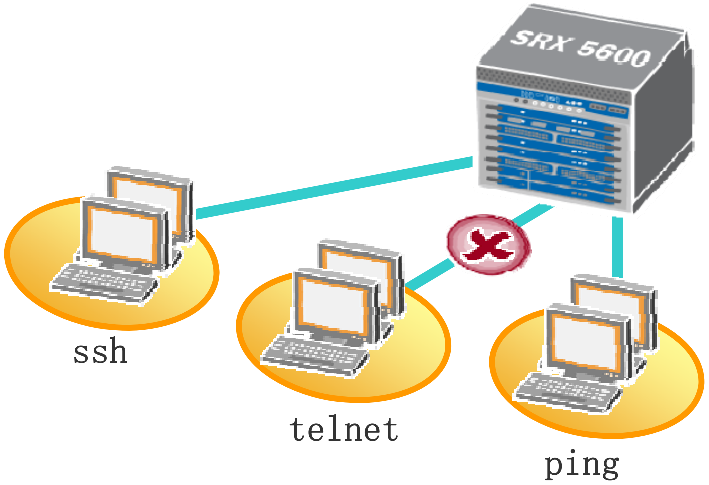
```
[edit]
user@host# edit security zones

[edit security zones]
user@host# set functional-zone management interfaces ge-0/0/1.100
```

详细指定允许哪种类型的流量进入SRX(1 of 3)

在SRX上默认是没有流量被允许

- 用 **host-inbound-traffic** 命令详细的指定从zone或interface进入SRX的流量
- 所有已SRX为原的出向的流量是被允许的



详细指定允许哪种类型的流量进入SRX(2 of 3)

Configurational 层级

- zone 下配置:

```
[edit security zones]
user@host# set security-zone HR host-inbound-traffic system-services all
```

- zone内接口下配置:

```
[edit security zones]
user@host# set security-zone HR interfaces ge-0/0/1 host-inbound-traffic system-
services http
```

- 接口下的配置覆盖zone下的配置

详细指定允许哪种类型的流量进入SRX (3 of 3)

host-inbound-traffic statement choices:

- **system-services:** 指定被允许从zone内接口进入SRX的服务:
  - Telnet, SSH, DNS, ping, SNMP, and others
- **protocols:** 指定被允许从zone内接口进入SRX的协议 :
  - BFD, BGP, LDP, OSPF, RIP, PIM, and others
- 可以使用 **except** 关键字 （除了……之外）

复习 (1 of 3)

下面的配置做些什么?

```
security {
    zones {
        security-zone HR {
            host-inbound-traffic {
                system-services {
                    telnet;
                    ftp;
                }
            }
            interfaces {
                ge-0/0/0.0;
                ge-0/0/1.0;
         }
     }
}
```

复习 (2 of 3)

下面的配置做些什么?

```
security {
    zones {
        security-zone HR {
            host-inbound-traffic {
                system-services {
                    telnet;
                    ftp;
                }
            }
            interfaces {
                ge-0/0/0.0;
                ge-0/0/1.0 {
                    host-inbound-traffic {
                        system-services {
                            snmp;
                        }
                    }
                }
            }
        }
    }
}
```

复习(3 of 3)

什么服务被允许通过接口
ge-0/0/0.0 和
ge-0/0/1.0进入SRX?

```
security {
    zones {
        security-zone zone1 {
            host-inbound-traffic {
                system-services {
                    all;
                    telnet {
                        except;
                    }
                }
            }
            interfaces {
                ge-0/0/0.0;
                ge-0/0/1.0 {
                    host-inbound-traffic {
                        system-services {
                            all;
                            http {
                                except;
                            }
                            ftp {
                                except;
                            }
                        }
                    }
                }
            }
          }
     }
}
```

监测 Zones

用**show security zones** 命令:

- Zone 类型
- Zone 名称
- 绑定接口的数量
- 接口绑定到对应的zones

```
user@host> show security zones

Functional zone: management
  Policy configurable: No
  Interfaces bound: 1
  Interfaces:
    ge-0/0/0.0
```

Functional management zone
with one interface—ge-0/0/0.0

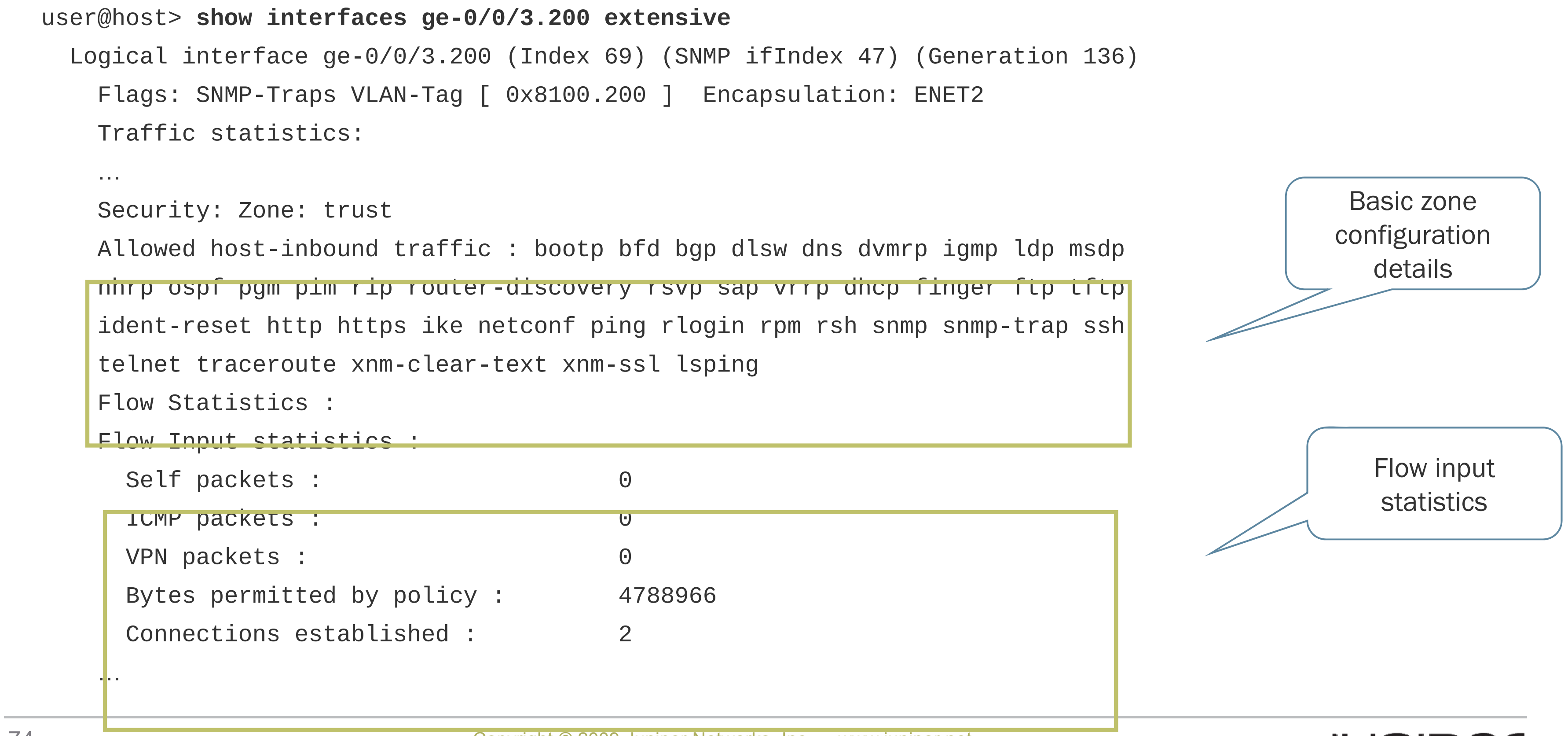
```
user@host> show security zones

Security zone: HR
  Send reset for non-SYN session TCP packets: Off
  Policy configurable: Yes
  Interfaces bound: 1
  Interfaces:
    ge-0/0/1.0
```

Security zone HR
with one interface—ge-0/0/1.0

监控允许进入接口的流量 (1 of 2)

查看接口详细信息用**show interfaces *interface-name* extensive** 命令:

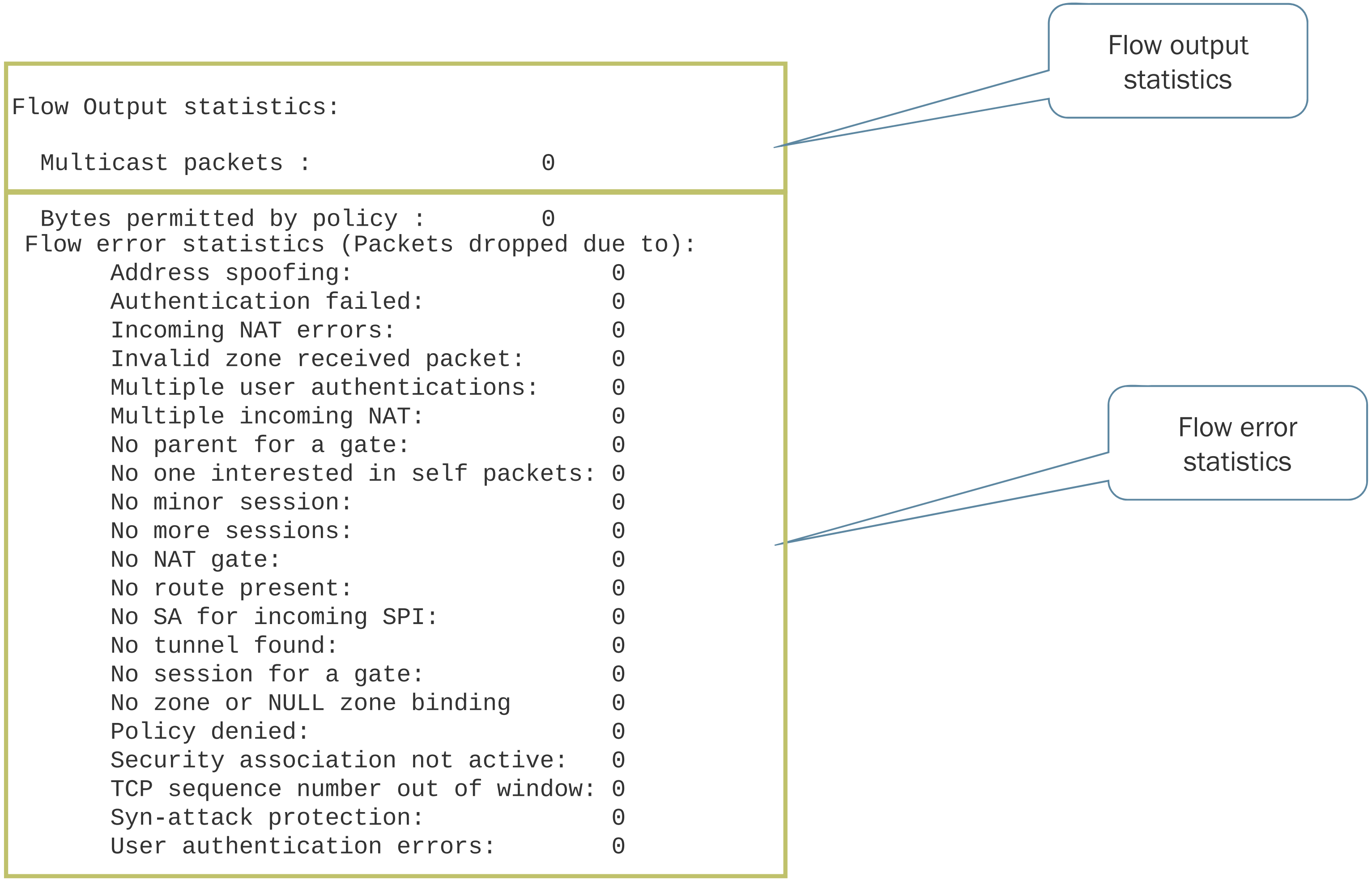


```
user@host> show interfaces ge-0/0/3.200 extensive
  Logical interface ge-0/0/3.200 (Index 69) (SNMP ifIndex 47) (Generation 136)
    Flags: SNMP-Traps VLAN-Tag [ 0x8100.200 ]  Encapsulation: ENET2
    Traffic statistics:
    …
    Security: Zone: trust
    Allowed host-inbound traffic : bootp bfd bgp dlsw dns dvmrp igmp ldp msdp
    nhrp ospf pgm pim rip router-discovery rsvp sap vrrp dhcp finger ftp tftp
    ident-reset http https ike netconf ping rlogin rpm rsh snmp snmp-trap ssh
    telnet traceroute xnm-clear-text xnm-ssl lsping
    Flow Statistics :
    Flow Input statistics :
      Self packets :                    0
      ICMP packets :                    0
      VPN packets :                     0
      Bytes permitted by policy :       4788966
      Connections established :         2
    …
```

Basic zone configuration details

Flow input statistics

监控允许进入接口的流量 (2 of 2)



```
Flow Output statistics:

  Multicast packets :                  0

  Bytes permitted by policy :          0
 Flow error statistics (Packets dropped due to):
       Address spoofing:                    0
       Authentication failed:               0
       Incoming NAT errors:                 0
       Invalid zone received packet:        0
       Multiple user authentications:       0
       Multiple incoming NAT:               0
       No parent for a gate:                0
       No one interested in self packets:   0
       No minor session:                    0
       No more sessions:                    0
       No NAT gate:                         0
       No route present:                    0
       No SA for incoming SPI:              0
       No tunnel found:                     0
       No session for a gate:               0
       No zone or NULL zone binding         0
       Policy denied:                       0
       Security association not active:     0
       TCP sequence number out of window:   0
       Syn-attack protection:               0
       User authentication errors:          0
```

Flow output statistics

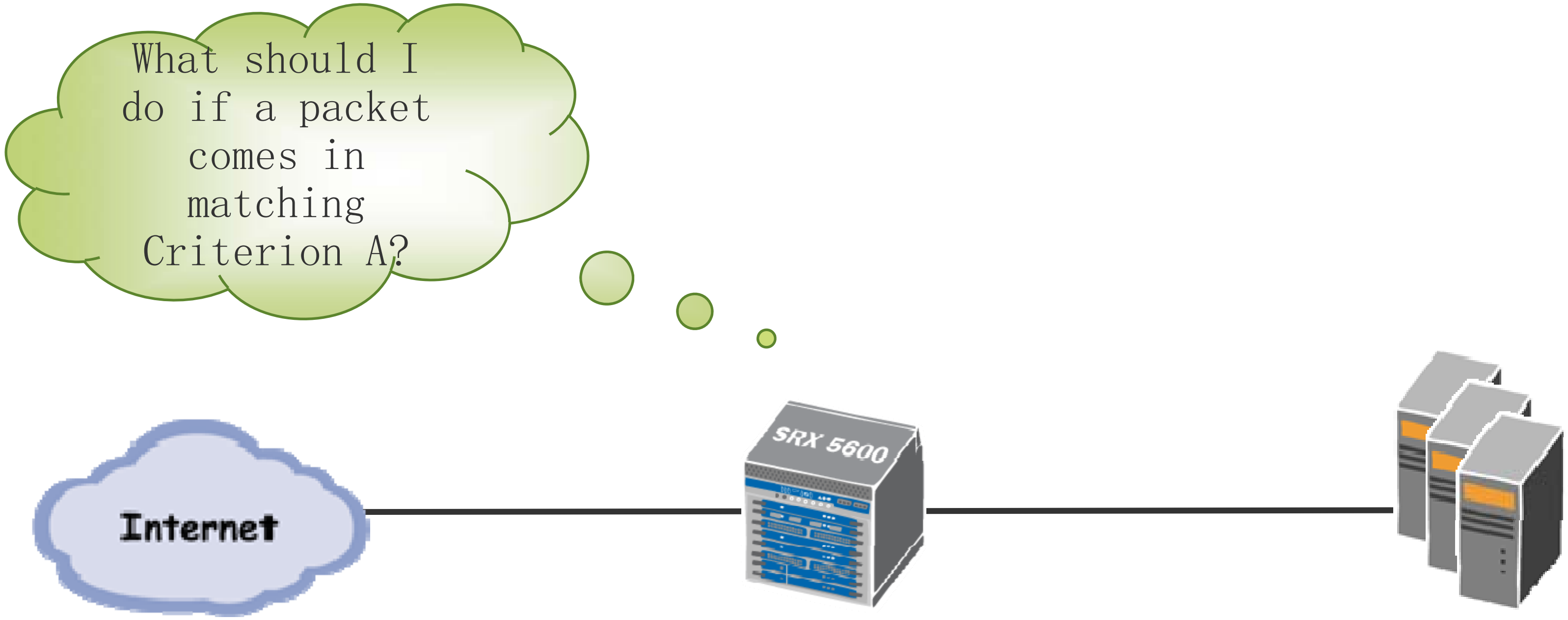
Flow error statistics

Security Policies

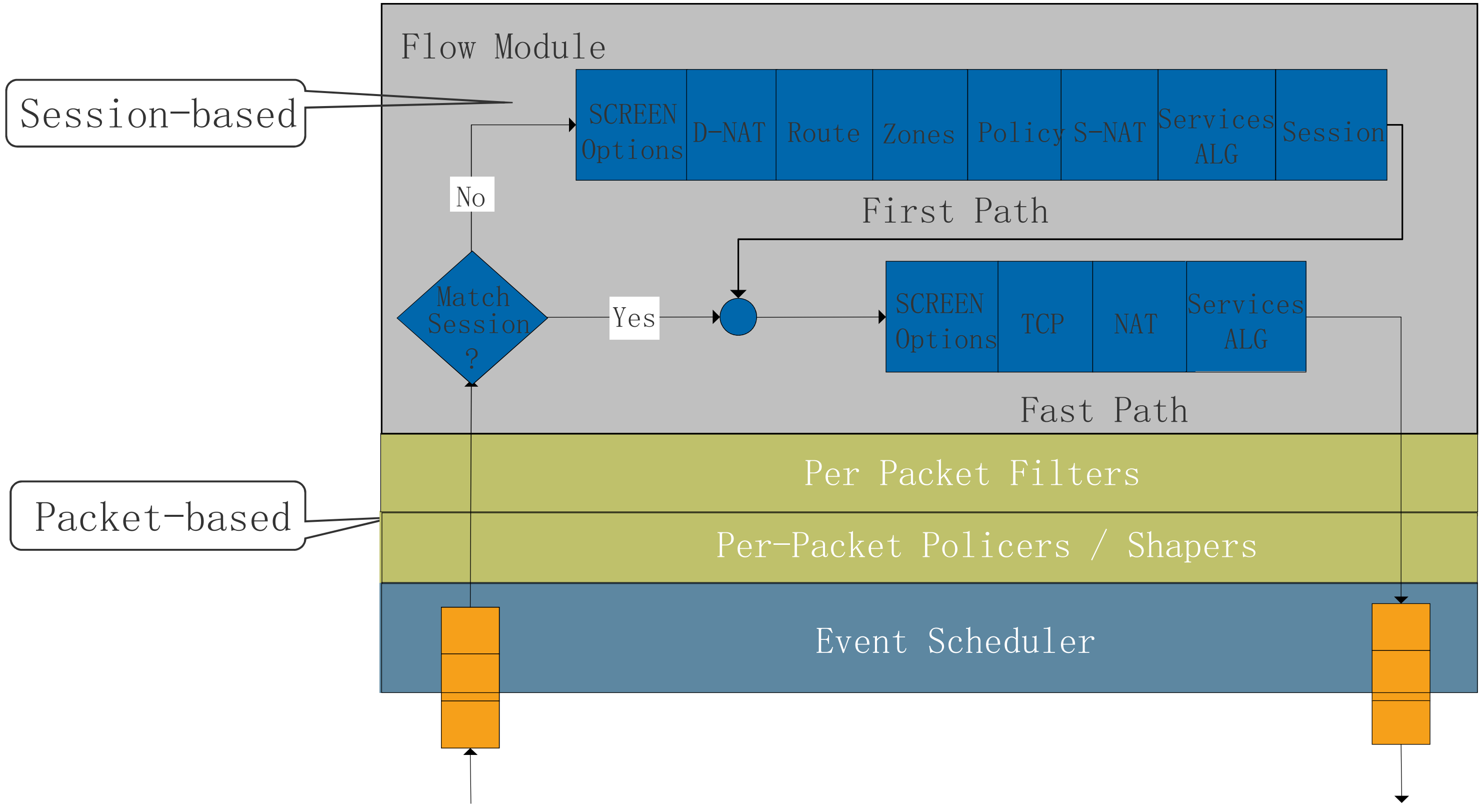
安全策略的定义

What is a security policy?

- 流量在zone间或zone内传输流量的一组规则

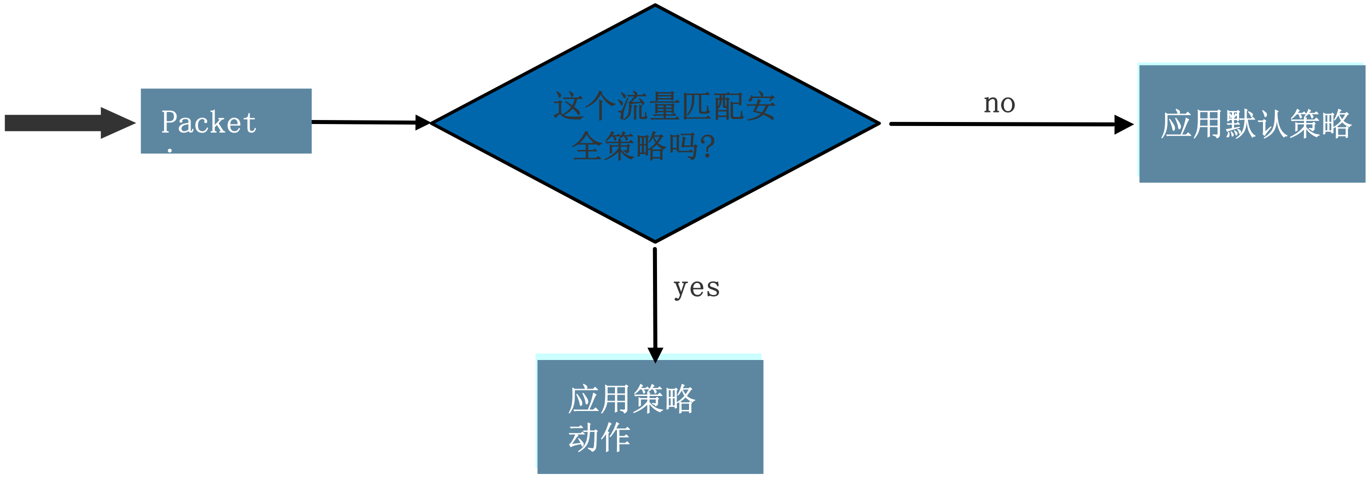


回顾: Packet Flow



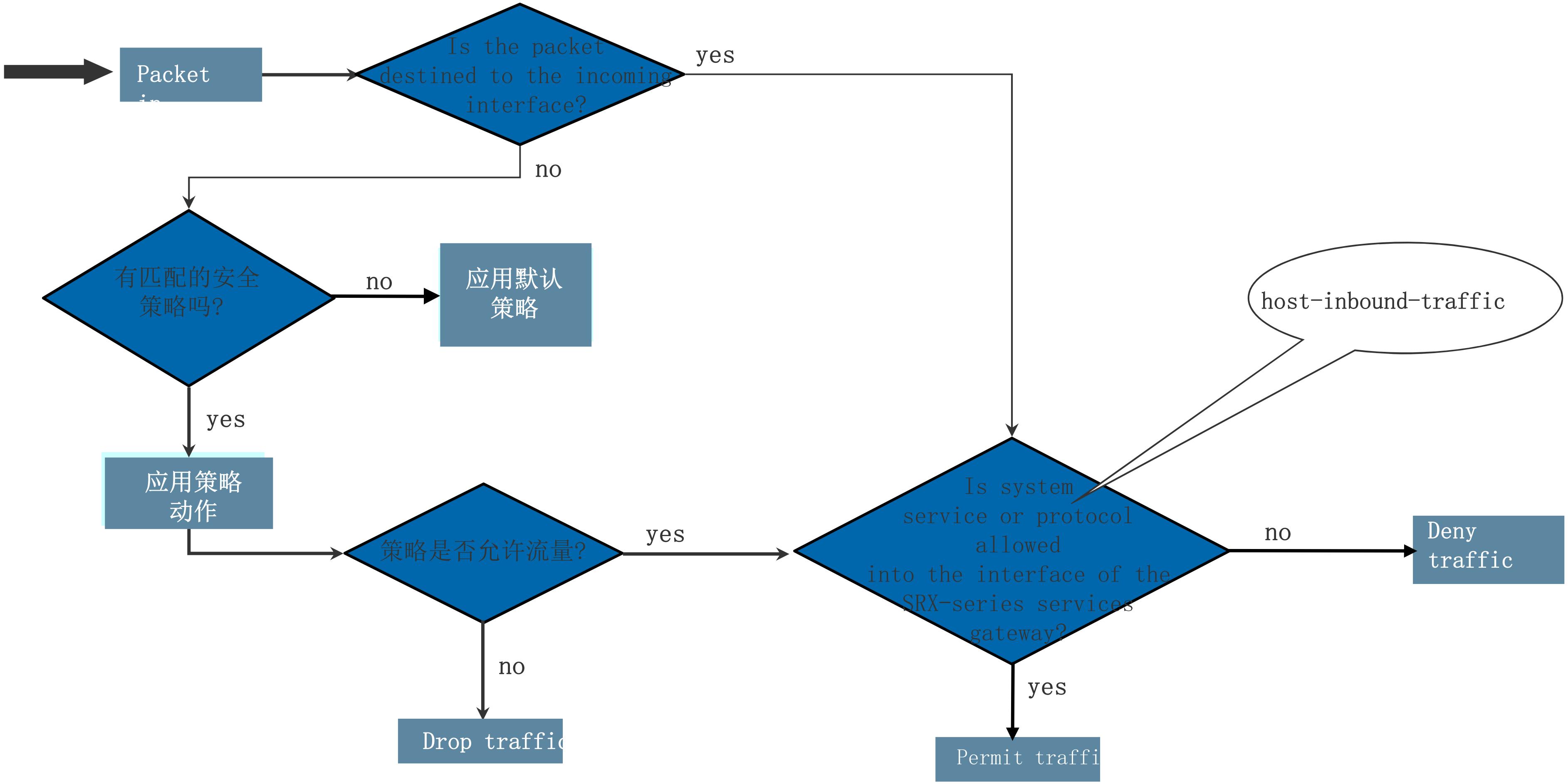
流量传输检查

SRX系列JUNOS 利用安全策略检查流量



本地Inbound 流量检查

`host-inbound-traffic` follows this process:



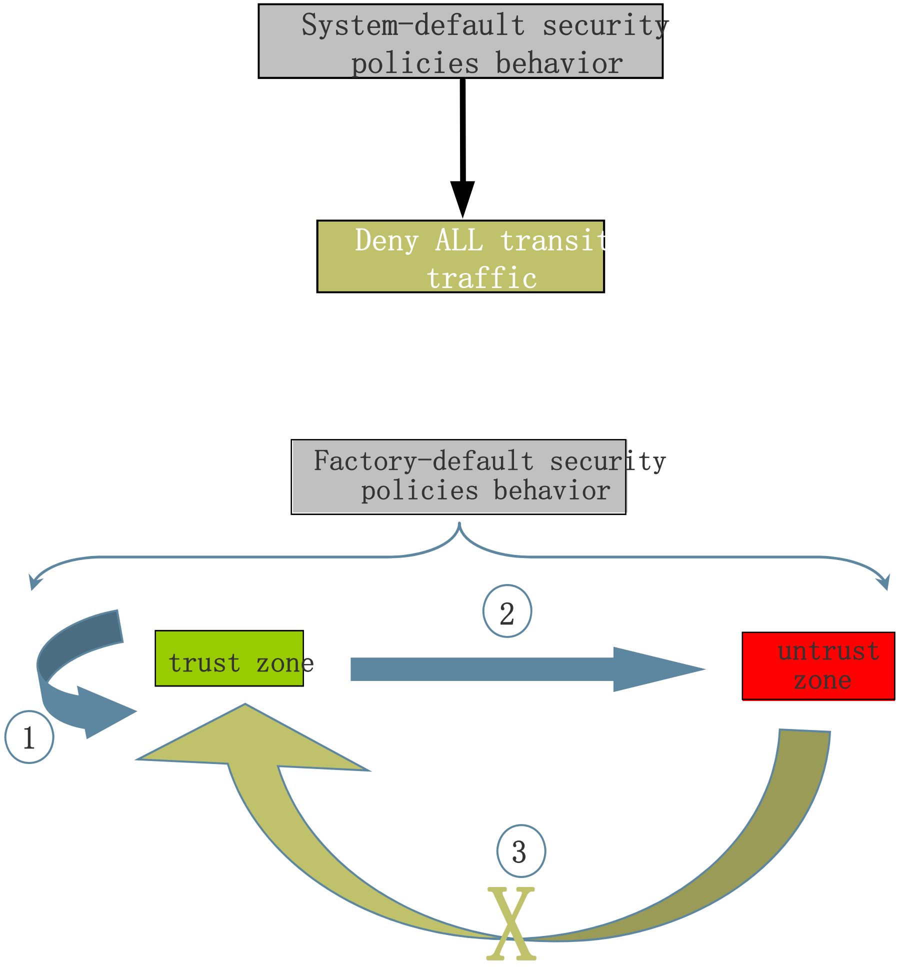
默认安全策略

默认策略拒绝所有流量穿越

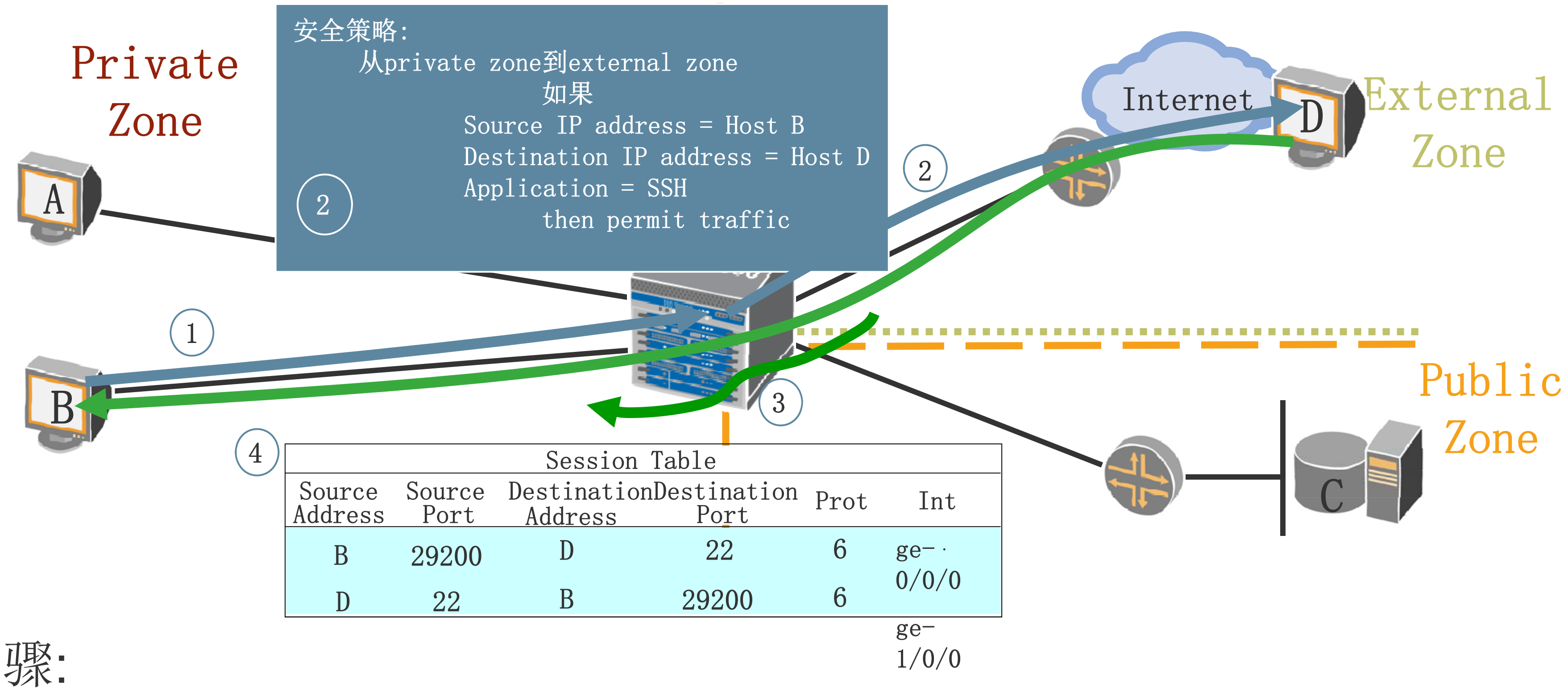
- 你可以改变默认策略为允许

出厂默认配置了三条策略:

- Trust to trust: permit all
- Trust to untrust: permit all
- Untrust to trust: deny all


System-default security policies behavior
Deny ALL transit traffic
Factory-default security policies behavior
trust zone
untrust zone
1
2
3
X

安全策略概念（实例）



安全策略:
从private zone到external zone
如果
Source IP address = Host B
Destination IP address = Host D
Application = SSH
then permit traffic

Session Table

Source Address	Source Port	Destination Address	Destination Port	Prot	Int
B	29200	D	22	6	ge-0/0/0
D	22	B	29200	6	ge-1/0/0

步骤:

1. 主机B 发起SSH访问到主机 D—Flow B → D
2. 安全策略允许这个访问
3. 这个流触发了一个反向的流; 两个流共同产生session
4. 反向流, 主机D → 主机 B, 同样的被允许

策略顺序

顺序:

- 顺序在防火墙中尤为重要!
- 默认情况下, 新建立的策略排在策略列表的最后
- 能用**insert** 命令改变顺序
- 记住系统默认策略!

```
insert security policies from-zone name to-zone name policy name
[before | after] policy name
```

编辑安全策略的配置

和其他JUNOS 配置一样分层, 安全策略的组成:

- Deleted
- Deactivated
- Activated
- Inserted
- Annotated
- Copied
- Renamed
- Searched and replaced

策略的语法

按下面的文本进行创建

- `from-zone` *zone-name* `to-zone` *zone-name*
- 在 `[edit security policies]`层下设置

每一个策略:

- 用户定义的策略名
- 由*match* 状态和 *then* 状态组成
  - Match 标准 必须包含原地址, 目标地址, 还有应用（服务）
  - 动作可以是permit, deny, reject, log, or count (或是他们的组合)
- 高级策略动作包含以下内容:
  - Scheduling
  - Rematching
  - IDP
  - Firewall authentication

策略匹配标准

策略匹配标准:

- Source addresses
  - 单个 （address）
  - 地址集（Address set）
- Destination addresses
  - 单个（address）
  - 地址集（Address set）
- Applications 或是 application sets
  - 用户定义的
  - 系统定义的

Configured within a zone’ s address book

Configured within a zone’ s address book

创建地址条目

命令:

- 添加一个地址到地址本中:

- 创建一个地址组（address sets）:

```
[edit security zones]
security-zone name {
     address-book {
          address name1 X.X.X.X / mask;
          address name2 X.X.X.X / mask;
          …
     }
}
```

```
[edit security zones]
security-zone name {
     address-book {
          address-set name {
               address name1;
               address name2;
               …
          }
     }
}
```

定义 Applications

Specifics of implementation:

- There are many built-in applications (`junos-rsh`, `junos-sip`, `junos-bgp`, `junos-tacacs`, and so forth)
- 可以添加applications, application sets, 或者两者到预定义的列表中
  - 名称没有限制
  - 可以改变protocols, ports, 超时时间, and so forth

```
[edit applications]
application name {
    protocol protocol;
    source-port source-port;
    destination-port destination-port;
}
...
```

```
[edit applications]
application-set name {
    application name1;
    application name2;
    ...
}
```

创建策略的匹配条目

详细说明:

- Group all policies together in the proper order, ensuring proper order of execution
- Apply defined matching parameters

```
[edit security policies]
from-zone zone-name to-zone zone-name {
        policy name1 {
            match {
                  source-address address-name1;
                  destination-address address-name1;
                  application application-name1;
             }
            …
         }
        policy name2 {
            match {
                  source-address address-name2;
                  destination-address address-name2;
                  application application-name2;
             }
            …
         }
        …
}
```

基本策略动作

策略动作:

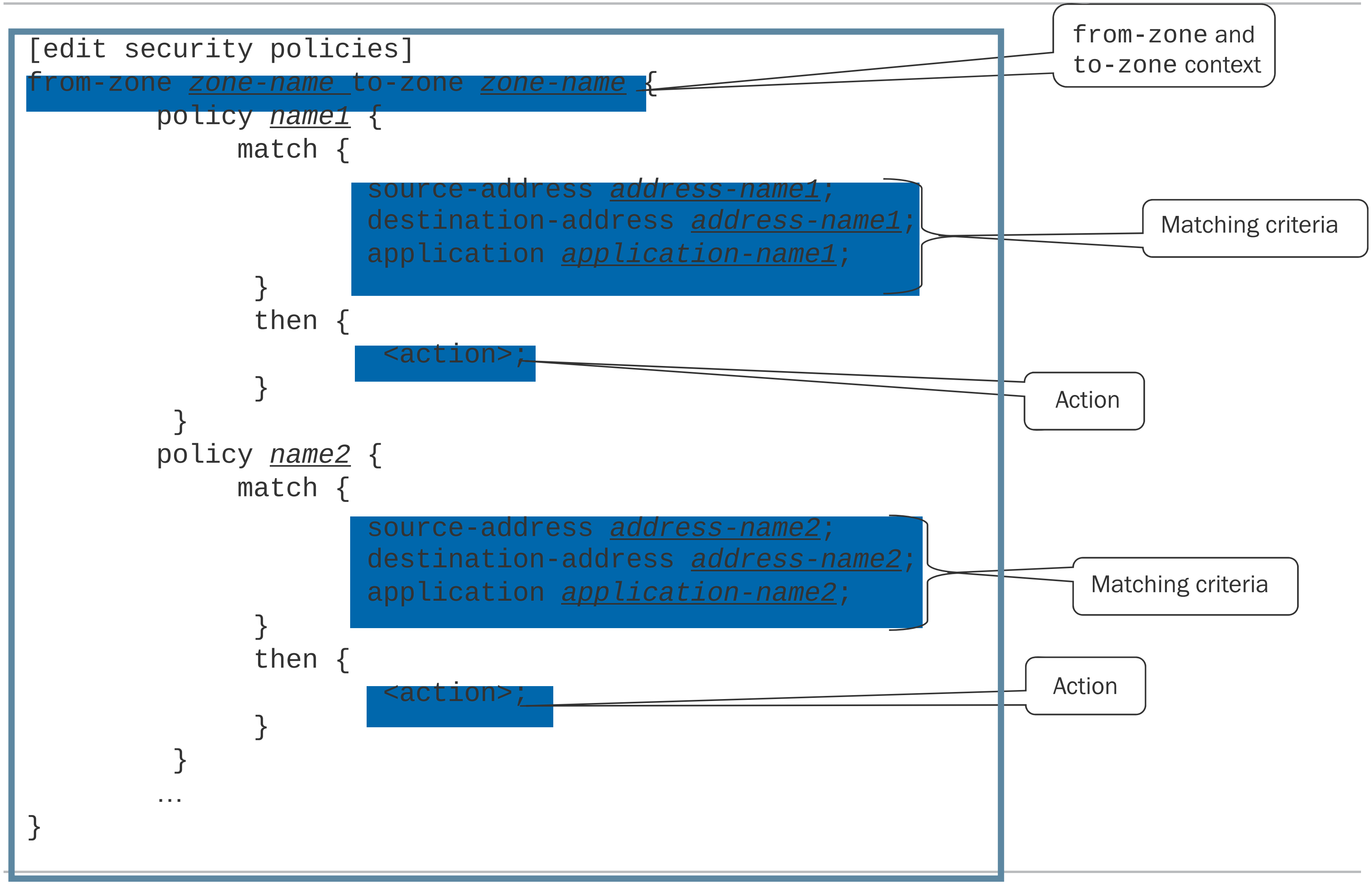
- `permit`: 允许
- `deny`: 拒绝
  - 可选 logs 和counts
- `reject`: 丢弃包并发送icmp不可达消息给UCP 流量或发送TCP (RST) 信息给TCP 流量
  - 可选 logs和counts

Advanced Permit Settings

If traffic is allowed to pass the security policy, you can also configure the following actions:

- Firewall authentication: authenticate the client prior to forwarding the traffic
  - Pass-through: access profile and client match
  - Web authentication: client match
- IPsec VPN: perform encryption and decryption of permitted transit traffic
- IDP: perform IDP policy evaluation

策略组成汇总



```
[edit security policies]
from-zone zone-name to-zone zone-name {
        policy name1 {
             match {
                     source-address address-name1;
                     destination-address address-name1;
                     application application-name1;
              }
              then {
                      <action>;
              }
         }
        policy name2 {
             match {
                     source-address address-name2;
                     destination-address address-name2;
                     application application-name2;
              }
              then {
                      <action>;
              }
         }
        ...
}
```

检测Policies (1 of 3)

show 命令:

- 用**show security policies**命令显示详细信息:

```
user@host> show security policies ?
Possible completions:
  <[Enter]>            Execute this command
  detail               Show the detailed information
  from-zone            Show the policy information matching the given source zone
  policy-name          Show the policy information matching the given policy name
  to-zone              Show the policy information matching the given destination zone
  |                    Pipe through a command
```

  - 用 detail 选项 显示状态
  - Policy must have a counter configured
- **show security flow session**
  - 查看流与 policy names 和 index numbers的关联

监测 Policies (2 of 3)

用log 动作发送到外部的log服务器

```
[edit security policies from-zone trust to-zone untrust]
user@host# set policy 812 then log ?
Possible completions:
+ apply-groups         Groups from which to inherit configuration data
+ apply-groups-except  Don't inherit configuration data from these groups
  session-close        Log at session close time
  session-init         Log at session init time
[edit security log]
user@host# show
format sd-syslog;
source-address address;
stream name {
    severity debug;
    host {
        address;
    }
}
```

- Logs直接发送到外部 syslog 服务器
- 外部syslog 服务器 必须配置并且可达

检测 Policies (3 of 3)

详细的troubleshooting用traceoptions:

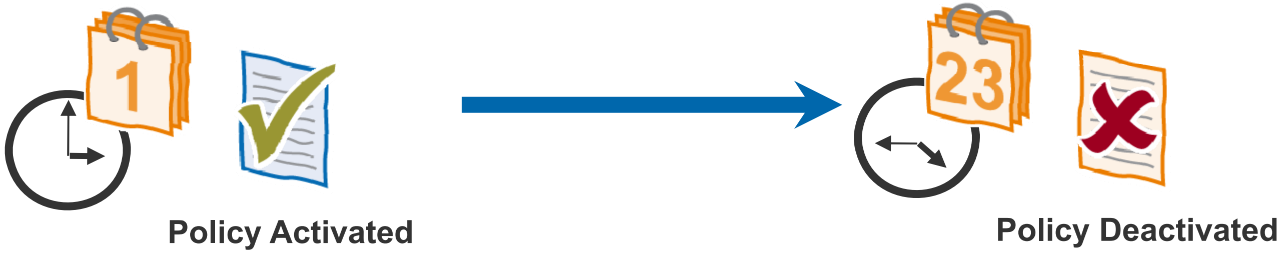
```
[edit security]
user@host# show
policies {
    traceoptions {
        file name;
        flag all;
    }
flow {
    traceoptions {
        file name;
        flag basic-datapath;
        flag session;
        packet-filter name {
            source-prefix address-prefix;
            destination-prefix address-prefix;
        }
      }
```

Policy Scheduling Overview

A *scheduled* policy is a policy that uses a configured scheduler to make the policy active at specific times

Policy and scheduler relationship:

- A policy can refer to only one scheduler
- Multiple policies can refer to the same scheduler
- If scheduler is not applied, a policy is always active



Policy Scheduler Components

Policy scheduler can be configured with:

- Slot schedule:
    - Start date and time
    - Stop date and time
- Daily schedule:
    - Start time
    - Stop time
    - All day
    - Exclude option

Policy Scheduler Details

Scheduler:

- Set up the schedule for policy execution, including time and date:

```
set schedulers scheduler name [day-of-the-week | daily] [specifics of time]
```

- Apply the scheduler
- Default behavior:
  - Policies that do not have schedulers are *always* active and in force

```
[edit security policies]
from-zone name to-zone name {
    policy name {
          match {
              ...
              ...
          }
          then {
             ...
          }
          scheduler-name name;
    }
}
```

Apply the scheduler

`policy-rematch` Statement

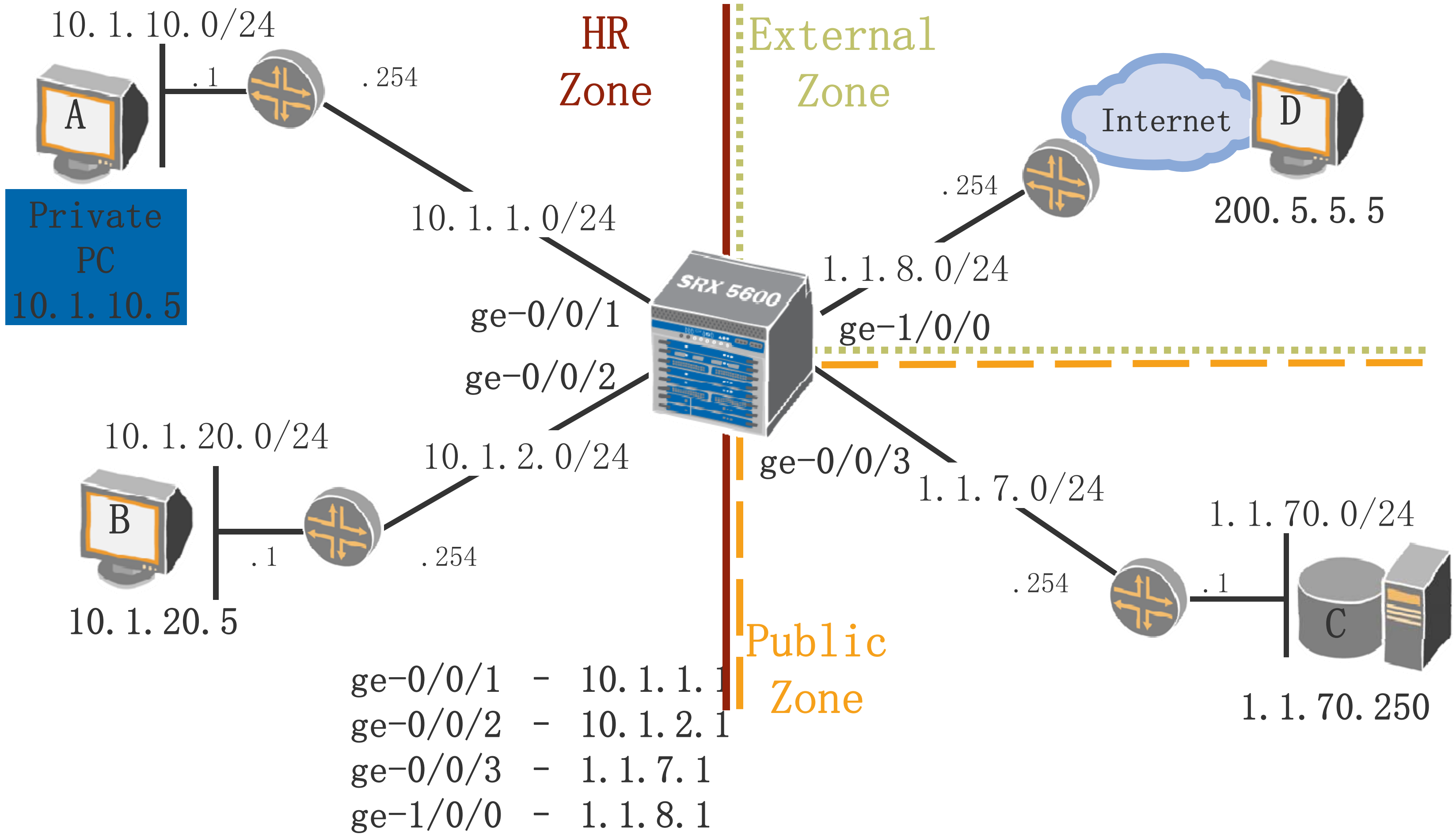
`policy-rematch` statement: signals the application of policy configuration changes to existing sessions

```
set security policies policy-rematch
```

- Default behavior:
  - Deletion of policies cause drops of impacted sessions
  - Configuration changes to existing policies do not impact sessions in progress

Action on Policy	Description	Rematch Flag	
		Enable	Disable (default)
Delete	Policy is deleted	All existing sessions are dropped	All existing sessions are dropped
Modify action	Action field of policy is modified from permit to deny or reject, or vice versa	All existing sessions are dropped	All existing sessions continue
Modify address	Source or destination address is modified	Policy lookup will be re-evaluated	All existing sessions continue
Modify application	Application is modified	Policy lookup will be re-evaluated	All existing sessions continue

Case Study: Creating Policies Between HR and Public Zones



Case Study: Entering Host Addresses into the HR Zone

```
[edit security]
user@host# show zones security-zone HR

address-book {
    address PC_A 10.1.10.5/32;
    address PC_B 10.1.20.5/32;
    address other-10-1 10.1.0.0/16;
    address-set HR_PCs {
          address PC_A;
          address PC_B;
    }
}
interfaces {
    ge-0/0/1.0;
    ge-0/0/2.0;
}
```

Case Study: Entering Host Addresses into the Public Zone

```
[edit security]
user@host# show zones security-zone Public

address-book {
     address Server_C 1.1.70.250/32;
     address other-1-1-70 1.1.70/24;
     address-set address-Public {
         address Server_C;
     }
}
interfaces {
       ge-0/0/3.0;
}
```

Case Study: Adding New Applications

```
[edit applications]
user@host# show
application HR-telnet {
    protocol tcp;
    source-port 1024-5000;
    destination-port telnet;
}
application-set HR-Public-applications {
    application junos-ftp;
    application junos-ike;
    application HR-telnet;
}
```

Case Study: Creating Policy Entries (1 of 2)

```
[edit security]
user@host# show policies
from-zone HR to-zone Public {
    policy HR-to-Public {
        match {
            source-address HR_PCs;
            destination-address address-Public;
            application HR-Public-applications;
        }
        then {
            permit;
        }
    }
```

Case Study: Creating Policy Entries (2 of 2)

```
  policy otherHR-to-Public {
          match {
              source-address other-10-1;
              destination-address other-1-1-70;
              application junos-ftp;
          }
          then {
              deny;
              log {
                  session-init;
                  session-close;
              }
              count;
          }
   }
}
```

Case Study: Creating a Scheduler

```
[edit]
user@host# show schedulers
scheduler schedulerHR {
    daily {
        start-time 09:00:00 stop-time 17:00:00;
    }
    sunday exclude;
    saturday exclude;
}
```

Example: Applying a Scheduler

```
[edit]
user@host# show security policies
from-zone HR to-zone Public {
    policy HR-to-Public {
        match {
            source-address HR-PCs;
            destination-address address-Public;
            application HR-Public-applications;
        }
        then {
            permit;
        }
        scheduler-name schedulerHR;
    }
```