Juniper SRX Branch 系列防火墙配置管理手册

Juniper 系统工程师

Juniper Networks, Inc.
上海市淮海中路333号瑞安广场1102-1104室
邮编:200021
电话:61415000
http://www.juniper.net

目录

Juniper SRX Branch 系列防火墙配置管理手册说明

SRX 系列防火墙是 Juniper 公司基于 JUNOS 操作系统的安全系列产品，JUNOS 集成了路由、交换、安全性和一系列丰富的网络服务。目前 Juniper 公司的全系列路由器产品、交换机产品和 SRX 安全产品均采用统一源代码的 JUNOS 操作系统，JUNOS 是全球首款将转发与控制功能相隔离，并采用模块化软件架构的网络操作系统。JUNOS 作为电信级产品的精髓是 Juniper 真正成功的基石，它让企业级产品同样具有电信级的不间断运营特性，更好的安全性和管理特性，JUNOS 软件创新的分布式架构为高性能、高可用、高可扩展的网络奠定了基础。基于 NP 架构的 SRX 系列产品产品同时提供性能优异的防火墙、NAT、IPSEC、IPS、UTM 等全系列安全功能，其安全功能主要来源于已被广泛证明的 ScreenOS 操作系统。

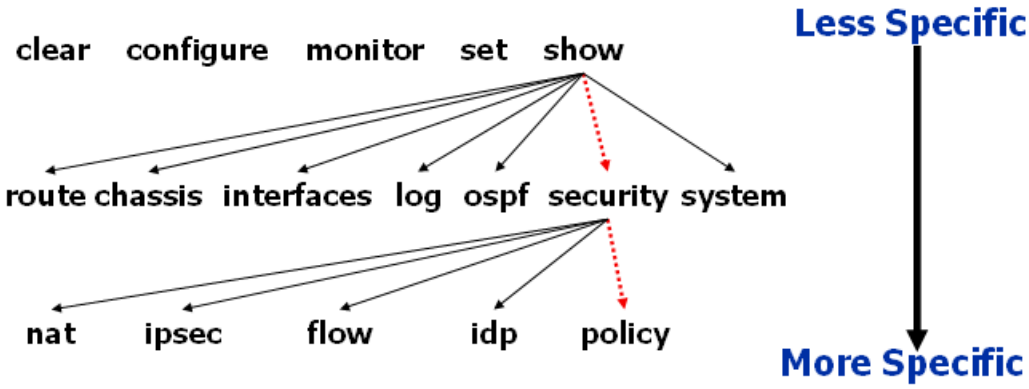
本文旨在为熟悉 Netscreen 防火墙 ScreenOS 操作系统的工程师提供 SRX 防火墙参考配置，以便于大家能够快速部署和维护 SRX 防火墙，文档介绍 JUNOS 操作系统，并参考 ScreenOS 配置介绍 SRX 防火墙配置方法，最后对 SRX 防火墙常规操作与维护做简要说明。

鉴于 SRX 系列防火墙低端<Branch>系列与高端 3K、5K 系列在功能配置与包处理流程有所差异，本人主要以低端系列功能配置介绍为主，Branch 系列型号目前包含：SRX100\210\240\650 将来会有新的产品加入到 Branch 家族，请随时关注官方网站动态，配置大同小异。

一、JUNOS 操作系统介绍

1.1 层次化配置结构

JUNOS 采用基于 FreeBSD 内核的软件模块化操作系统，支持 CLI 命令行和 WEBUI 两种接口配置方式，本文主要对 CLI 命令行方式进行配置说明。JUNOS CLI 使用层次化配置结构，分为操作（operational）和配置（configure）两类模式，在操作模式下可对当前配置、设备运行状态、路由及会话表等状态进行查看及设备运维操作，并通过执行 config 或 edit 命令进入配置模式，在配置模式下可对各相关模块进行配置并能够执行操作模式下的所有命令（run）。在配置模式下 JUNOS 采用分层分级模块下配置结构，如下图所示，edit 命令进入下一级配置（类似 unix cd 命令）,exit 命令退回上一级，top 命令回到根级。



1.2 JunOS 配置管理

JUNOS 通过 set 语句进行配置，配置输入后并不会立即生效，而是作为候选配置（**Candidate Config**）等待管理员提交确认，管理员通过输入 commit 命令来提交配置，配置内容在通过 SRX 语法检查后才会生效，一旦 commit 通过后当前配置即成为有效配置（Active config）。另外，JUNOS 允许执行 commit 命令时要求管理员对提交的配置进行两次确认，如执行 commit confirmed 2 命令要求管理员必须在输入此命令后 2 分钟内再次输入 commit 以确认提交，否则 2 分钟后配置将自动回退，这样可以避免远程配置变更时管理员失去对 SRX 的远程连接风险。

在执行 commit 命令前可通过配置模式下 show 命令查看当前候选配置（**Candidate Config**），在执行 commit 后配置模式下可通过 run show config 命令查看当前有效配置（Active config）。此外可通过执行 show | compare 比对候选配置和有效配置的差异。

SRX 上由于配备大容量存储器，缺省按先后 commit 顺序自动保存 50 份有效配置，并可通过执行 rolback 和 commit 命令返回到以前配置（如 rollback 0/commit 可返回到前一 commit 配置）；也可以直接通过执行 save *confignam.conf* 手动保存当前配置，并执行 load override *confignam.conf* / commit 调用前期手动保存的配置。执行 load factory-default / commit 命令可恢复到出厂缺省配置。

SRX 可对模块化配置进行功能关闭与激活，如执行 deactivate security nat/comit 命令可使 NAT 相关配置不生效，并可通过执行 activate security nat/commit 使 NAT 配置再次生效。

SRX 通过 set 语句来配置防火墙，通过 delete 语句来删除配置，如 delete security nat 和 edit security nat / delete 一样，均可删除 security 防火墙层级下所有 NAT 相关配置，删除配置和 ScreenOS 不同，配置过程中需加以留意。

1.3 SRX 主要配置内容

部署 SRX 防火墙主要有以下几个方面需要进行配置：
System：主要是系统级内容配置，如主机名、管理员账号口令及权限、时钟时区、Syslog、SNMP、系统级开放的远程管理服务（如 telnet）等内容。

Interface:接口相关配置内容。

Security: 是 SRX 防火墙的主要配置内容，安全相关部分内容全部在 Security 层级下完成配置，如 NAT、Zone、Policy、Address-book、Ipsec、Screen、Idp、UTM 等，可简单理解为 ScreenOS 防火墙安全相关内容都迁移至此配置层次下，除了 Application 自定义服务。

Application：自定义服务单独在此进行配置，配置内容与 ScreenOS 基本一致。

routing-options： 配置静态路由或 router-id 等系统全局路由属性配置。

二、SRX 防火墙配置操作举例说明

2.1 初始安装

2.1.1 设备登陆

Console口(通用超级终端缺省配置)连接SRX，root用户登陆，密码为空<初始第一次登陆>

login: root
Password:
--- JUNOS 9.5R1.8 built 2009-07-16 15:04:30 UTC
root% cli　　/***进入操作模式***/
root>
root> configure
Entering configuration mode　　/***进入配置模式***/
[edit]
Root#

2.1.2 设备恢复出厂介绍

首先根据上述操作进入到配置模式,执行下列命令：

root# load factory-default
warning: activating factory configuration　/***系统激活出厂配置***/
恢复出厂后,必须立刻设置 ROOT 帐号密码<默认密码至少 6 位数：字母加数字>
root# set system root-authentication plain-text-password
New password:
当设置完 ROOT 帐号密码以后,进行保存激活配置
root# commit
commit complete
在此需要提醒配置操作员注意，系统恢复出厂后并不代表没有任何配置,系统缺省配置有 Screen\DHCP\Policy 等相关配置,你如果需要完整的删除,可以执行命令 delete 删除相关配置。通过 show 来查看系统是否还有遗留不需要的配置,可以一一进行删除,直到符合你的要求,然后再重新根据实际需求进行配置。

2.1.3 设置 root 用户口令

设置root用户口令
root# set system root-authentication plain-text-password
root# new password : root123
root# retype new password: root123
密码将以密文方式显示
root# show system root-authentication
encrypted-password "1xavDeUe6$fNM6olGU.8.M7B62u05D6."; # SECRET-DATA

注意：强烈建议不要使用其它加密选项来加密root和其它user口令(如encrypted-password加密方式)，此配置参数要求输入的口令是经加密算法加密后的字符串，采用这种加密方式手工输入时存在密码无法通过验证风险。
注：root用户仅用于console连接本地管理SRX，不能通过远程登陆管理SRX，必须成功设置root口令后，才能执行commit提交后续配置命令。

2.1.4 设置远程登陆管理用户

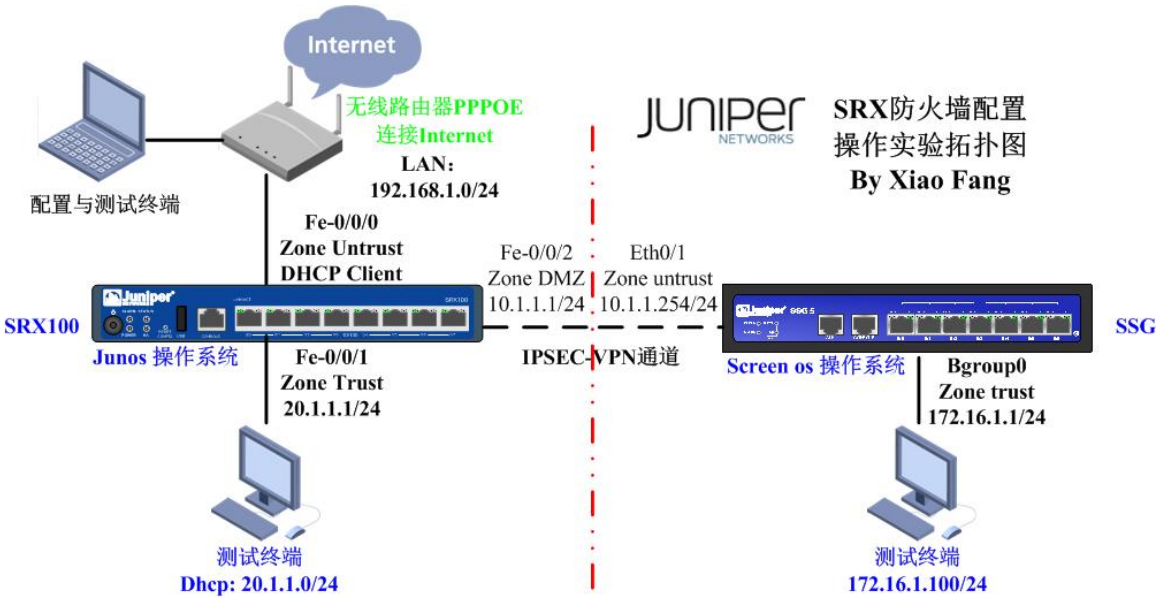
root# set system login user lab class super-user authentication plain-text-password
root# new password : lab123
root# retype new password: lab123
注：此 lab 用户拥有超级管理员权限，可用于 console 和远程管理访问，另也可自行灵活定义其它不同管理权限用户。

2.1.5 远程管理 SRX 相关配置

run set date YYYYMMDDhhmm.ss /***设置系统时钟***/
set system time-zone Asia/Shanghai /***设置时区为上海***/
set system host-name SRX-650-1 /***设置主机名***/
set system name-server 1.1.1.1 /***设置 DNS 服务器***/
set system services ftp
set system services telnet
set system services web-management http
/***在系统级开启 ftp/telnet/http 远程接入管理服务***/
set interfaces ge-0/0/0.0 family inet address 10.1.1.1/24
或
set interfaces ge-0/0/0 unit 0 family inet address 10.1.1.1/24
set interfaces ge-0/0/1 unit 0 family inet address 10.1.2.1/24
set routing-options static route 0.0.0.0/0 next-hop 192.168.1.1
/***配置逻辑接口地址及缺省路由，SRX 接口要求 IP 地址必须配置在逻辑接口下（类似 ScreenOS 的子接口），通常使用逻辑接口 0 即可***/
set security zones security-zone untrust interfaces ge-0/0/0.0
/***将 ge-0/0/0.0 接口放到安全区域中，类似 ScreenOS***/
set security zones security-zone untrust host-inbound-traffic system-services ping
set security zones security-zone untrust host-inbound-traffic system-services http
set security zones security-zone untrust host-inbound-traffic system-services telnet
/***在 untrust zone 打开允许远程登陆管理服务，ScreenOS 要求基于接口开放服务，SRX 要求基于 Zone 开放，从 SRX 主动访问出去流量开启服务，类似 ScreenOS***/

本次实验拓扑中使用的设备的版本如下：
SRX100-HM 系统版本与 J-WEB 版本均为：10.1.R2.8
SSG 防火墙版本为 6.1.0R7
测试客户端包含 WINDOWS7\XP

2.2 配置操作实验拓扑



2.3 策略相关配置说明

安全设备的缺省行为是拒绝安全区段之间的所有信息流（区段之间信息流）允许绑定到同一区段的接口间的所有信息流（区段内部信息流）。为了允许选定的区段之间信息流通过安全设备，必须创建覆盖缺省行为的区段之间策略。同样，为了防止选定的区段内部信息流通过安全设备，必须创建区段内部策略。

基本元素

允许、拒绝或设置两点间指定类型单向信息流通道的策略。信息流（或“服务”）的类型、两端点的位置以及调用的动作构成了策略的基本元素。尽管可以有其它组件，但是**共同构成策略核心部分的必要元素如下**:

策略名称 – 两个安全区段间（从源区段到目的区段）间信息流的方向 **/***必须配置***/**

源地址 – 信息流发起的地址 **/***必须配置***/**

目标地址 – 信息流发送到的地址 **/***必须配置***/**

服务 – 信息流传输的类型 **/***必须配置***/**

动作 – 安全设备接收到满足头四个标准的信息流时执行的动作 **/***必须配置***/**

这些动作为:deny、permit、reject 或 tunnel

注意tunnel、firewall-authentication、application-services<IDP\UAC\WX\UTM策略>在permit下一级,如下：

root# set security policies from-zone trust to-zone untrust policy t-u then permit ?

> Firewall-authentication

> tunnel　　另外还包括其他的策略元素,比如记录日志、流量统计、时间调度对象等

三种类型的策略

可通过以下三种策略控制信息流的流动:

通过创建区段之间策略，可以管理允许从一个安全区段到另一个安全区段的信息流的种类。

通过创建区段内部策略，也可以控制允许通过绑定到同一区段的接口间的信息流的类型。

通过创建全局策略，可以管理地址间的信息流，而不考虑它们的安全区段。

2.3.1 策略地址对象定义

SRX 服务网关地址对象需要自定义后才可以在策略中进行引用,默认只有 any 对象

自定义单个地址对象如下：

root# set security zones security-zone trust address-book address pc-1 20.1.1.200/32
root# set security zones security-zone trust address-book address pc-2 20.1.1.210/32

自定义单个地址组对象如下：

set security zones security-zone trust address-book address-set pc-group address pc-1
set security zones security-zone trust address-book address-set pc-group address pc-2

2.3.2 策略服务对象定义

SRX 服务网关部分服务对象需要自定义后才可以在策略中进行引用,默认仅有预定义常用服务对象

自定义单个服务对象如下：

set applications application tcp-3389 protocol tcp 定义服务对象协议<TCP\UDP\ICMP\OTHER>
set applications application tcp-3389 source-port 1-65535 定义服务对象源端口
set applications application tcp-3389 destination-port 3389-3389 定义服务对象目标地址
set applications application tcp-3389 inactivity-timeout never 可选定义服务对象 timeout 时长
set applications application tcp-8080 protocol tcp
set applications application tcp-8080 source-port 1-65535
set applications application tcp-8080 destination-port 8080-8080
set applications application tcp-8080 inactivity-timeout 3600

自定义单个服务组对象如下：

set applications application-set aaplications-group application tcp-8080
set applications application-set aaplications-group application tcp-3389

2.3.3 策略时间调度对象定义

SRX 服务网关时间调度对象需要自定义后才可以在策略中进行引用,默认没有预定义时间调度对象

自定义单个时间调度对象如下：

set schedulers scheduler **work-time** daily start-time 09:00:00 stop-time 18:00:00
set schedulers scheduler **happy-time** sunday start-time 00:00:00 stop-time 23:59:59
set schedulers scheduler **happy-time** saturday start-time 00:00:00 stop-time 23:59:59

注意：时间调度服务生效参考设备系统时间,所以需要关注设备系统时间是否正常。

2.3.4 策略配置举例

Policy 配置方法与 ScreenOS 基本一致，仅在配置命令上有所区别，其中策略的允许/拒绝的动作（Action）需要额外配置一条 then 语句(将 ScreenOS 的一条策略分解成两条及以上配置语句)。Policy 需要手动配置 policy name，policy name 可以是字符串，也可以是数字（与 ScreenOS 的 policy ID 类似,只不过需要手工指定)。

首先需要注意系统缺省策略配置：

root# show security policies default-policy　　查看当前系统缺省策略动作

root# set security policies default-policy ？ 设置系统缺省策略动作

Possible completions:

deny-all　　Deny all traffic if no policy match

permit-all　　Permit all traffic if no policy match

根据实验拓扑进行策略配置举例说明

set security zones security-zone trust address-book address pc1 20.1.1.200/32

set security zones security-zone untrust address-book address server1 192.168.1.200/32

/***与 ScreenOS 一样，在 trust 和 untrust zone 下分别定义地址对象便于策略调用，地址对象的名称可以是地址/掩码形式***/

set security zones security-zone trust address-book address-set addr-group1 address pc1

/***在 trust zone 下定义名称为 add-group1 的地址组，并将 pc1 地址放到该地址组中***/

Set security policies from-zone trust to-zone untrust policy 001 match source-address addr-group1 destination-address server1 application any

set security policies from-zone trust to-zone untrust policy 001 then permit

/***定义从 trust 到 untrust 方向 permit 策略,允许 addr-group1 组的源地址访问 server1 地址 any 服务***/

set security policies from-zone trust to-zone untrust policy 001 then log session-init

set security policies from-zone trust to-zone untrust policy 001 then log session-close

set security policies from-zone trust to-zone untrust policy 001 then count

<可选配置>/***定义从 trust 到 untrust 方向策略，针对当前策略记录日志并统计策略流量

root# set security policies from-zone trust to-zone untrust policy 001 scheduler-name happy-time

root# set security policies from-zone trust to-zone dmz policy 001 scheduler-name work-time

<可选配置>/***定义当前策略，引用时间调度对象，符合时间条件策略生效，否则策略将处于非工作状态

root# set security policies from-zone trust to-zone untrust policy t-u then permit application-services ?

Possible completions:

+ apply-groups　　Groups from which to inherit configuration data

+ apply-groups-except　Don't inherit configuration data from these groups

gprs-gtp-profile　　Specify GPRS Tunneling Protocol profile name

idp　　Intrusion detection and prevention

redirect-wx　　Set WX redirection

reverse-redirect-wx　Set WX reverse redirection

uac-policy　　Enable unified access control enforcement of policy

utm-policy　　Specify utm policy name

[edit]

<可选配置>/***定义当前策略，选择是否客气 IDP\UAC\UTM 等操作,如果针对策略开启相应的检查，请先定义好相应的功能。

2.4 地址转换

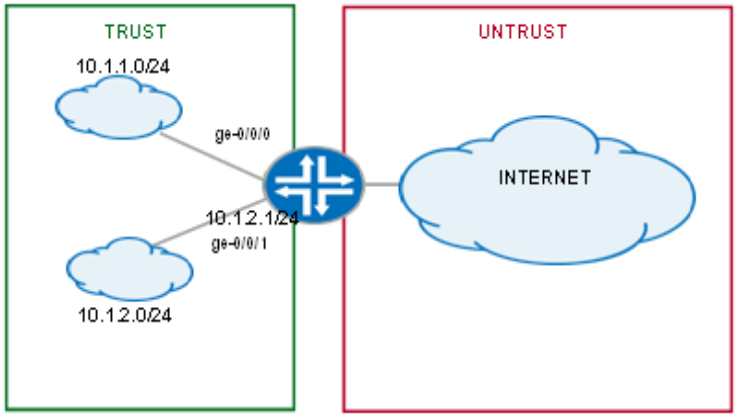
SRX NAT 较 ScreenOS 在功能实现方面基本保持一致，但在功能配置上有较大区别，配置的主要差异在于 ScreenOS 的 NAT 与 policy 是绑定的，无论是 MIP/VIP/DIP 还是基于策略的 NAT，在 policy 中均要体现出 NAT 内容（除了缺省基于 untrust 接口的 Souec-NAT 模式外），而 SRX 的 NAT 则作为网络层面基础内容进行独立配置（独立定义地址映射的方向、映射关系及地址范围），Policy 中不再包含 NAT 相关配置信息，这样的好处是易于理解、简化运维，当网络拓扑和 NAT 映射关系发生改变时，无需调整 Policy 配置内容。

SRX NAT 和 Policy 执行先后顺序为：目的地址转换－目的地址路由查找－执行策略检查－源地址转换，结合这个执行顺序，在配置 Policy 时需注意：**Policy 中源地址应是转换前的源地址，而目的地址应该是转换后的目的地址，换句话说，Policy 中的源和目的地址应该是源和目的两端的真实 IP 地址，**这一点和 ScreenOS 存在区别，需要加以注意。

SRX 中不再使用 MIP/VIP/DIP 这些概念，其中 MIP 被 Static 静态地址转换取代，两者在功能上完全一致；DIP 被 Source NAT 取代；基于 Policy 的目的地址转换及 VIP 被 Destination NAT 取代。ScreenOS 中基于 Untrust zone 接口的源地址转换被保留下来，但在 SRX 中不再是缺省模式（SRX 中 Trust Zone 接口没有 NAT 模式概念），需要手工配置。类似 ScreenOS，Static 属于双向 NAT，其他类型均属于单向 NAT。

此外，SRX 还多了一个 proxy-arp 概念，如果定义的 IP Pool（可用于源或目的地址转换）需配置 SRX 对这个 Pool 内的地址提供 ARP 代理功能，这样对端设备能够解析到 IP Pool 地址的 MAC 地址（使用接口 MAC 地址响应对方），以便于返回报文能够送达 SRX。下面是配置举例及相关说明：

2.4.1 Interface based NAT 基于接口的源地址转换



图片仅供参考，下列配置参考实验拓扑

NAT 配置：

set security nat source rule-set 1 from zone trust 指定源区域

set security nat source rule-set 1 to zone untrust 指定目标区域

set security nat source rule-set 1 rule rule1 match source-address 0.0.0.0/0 destination-address 0.0.0.0/0 指定源和目标匹配的地址或者地址段，0.0.0./0 代表所有

set security nat source rule-set 1 rule rule1 then source-nat interface 指定通过接口 IP 进行源翻译

上述配置定义 NAT 源地址映射规则，从 Trust Zone 访问 Untrust Zone 的所有流量用 Untrust Zone 接口 IP 做源地址转换。

Policy 配置:

set security policies from-zone trust to-zone untrust policy 1 match source-address pc-1

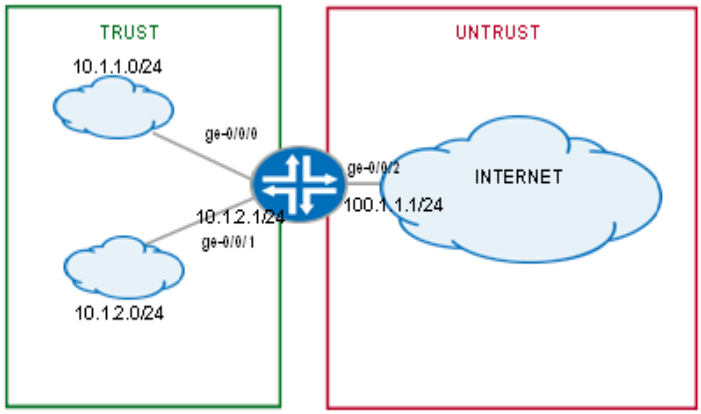
set security policies from-zone trust to-zone untrust policy 1 match destination-address any

set security policies from-zone trust to-zone untrust policy 1 match application any

set security policies from-zone trust to-zone untrust policy 1 then permit

上述配置定义 Policy 策略，允许 Trust zone 10.1.2.2 地址访问 Untrust 方向任何地址，根据前面的 NAT 配置，SRX 在建立 session 时自动执行接口源地址转换。

2.4.2 Pool based Source NAT 基于地址池的源地址转换



图片仅供参考,下列配置参考实验拓扑

NAT 配置：

set security nat source pool pool-1 address 192.168.1.50 to 192.168.1.150

set security nat source rule-set 1 from zone trust

set security nat source rule-set 1 to zone untrust

set security nat source rule-set 1 rule rule1 match source-address 0.0.0.0/0 destination-address 0.0.0.0/0

set security nat source rule-set 1 rule rule1 then source-nat pool pool-1

set security nat proxy-arp interface ge-0/0/0 address 192.168.1.50 to 192.168.1.150

上述配置表示从 trust 方向（any）到 untrust 方向(any)访问时提供源地址转换，源地址池为 pool1(192.168.1.50-192.168.1.150)，同时 fe-0/0/0 接口为此 pool IP 提供 ARP 代理。需要注意的是：定义 Pool 时不需要与 Zone 及接口进行关联。配置 proxy-arp 目的是让返回包能够送达 SRX，如果 Pool 与出接口 IP 不在同一子网，则对端设备需要配置指向 fe-0/0/0 接口的 Pool 地址路由。

Policy：

set security policies from-zone trust to-zone untrust policy 1 match source-address pc-1

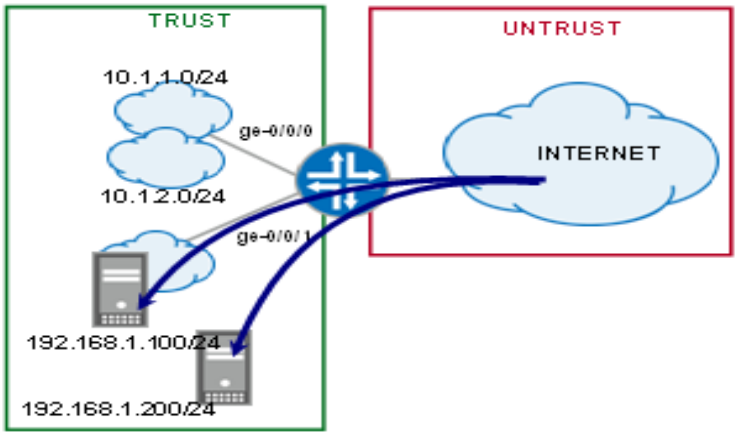
set security policies from-zone trust to-zone untrust policy 1 match destination-address any

set security policies from-zone trust to-zone untrust policy 1 match application any

set security policies from-zone trust to-zone untrust policy 1 then permit

上述配置定义 Policy 策略，允许 Trust zone 10.1.2.2 地址访问 Untrust 方向任何地址，根据前面的 NAT 配置，SRX 在建立 session 时自动执行源地址转换。

2.4.3 Pool base destination NAT 基于地址池的目标地址转换



图片仅供参考,下列配置参考实验拓扑

NAT 配置：

set security nat destination pool 111 address 20.1.1.200/32

set security nat destination rule-set 1 from zone untrust

set security nat destination rule-set 1 rule 111 match source-address 0.0.0.0/0

set security nat destination rule-set 1 rule 111 match destination-address 192.168.1.150/32

set security nat destination rule-set 1 rule 111 then destination-nat pool 111

上述配置将外网 any 访问 192.168.1.150 地址映射到内网 20.1.1.200 地址，**注意：定义的 Dst Pool 是内网真实 IP 地址，而不是映射前的公网地址**。这点和 Src-NAT Pool 有所区别。

Policy：

set security policies from-zone trust to-zone untrust policy 1 match source-address any

set security policies from-zone trust to-zone untrust policy 1 match destination-address PC-1

set security policies from-zone trust to-zone untrust policy 1 match application any

set security policies from-zone trust to-zone untrust policy 1 then permit

上述配置定义 Policy 策略，允许 Untrust 方向任何地址访问 Trust 方向 PC-1：20.1.1.200，根据前面的 NAT 配置，公网访问 192.168.1.150 时，SRX 自动执行到 20.1.1.200 的目的地址转换。

ScreenOS VIP 功能对应的 SRX Dst-nat 配置：

set security nat destination pool 222 address 20.1.1.200/32 port 8080

set security nat destination rule-set 1 from zone untrust

set security nat destination rule-set 1 rule 111 match source-address 0.0.0.0/0

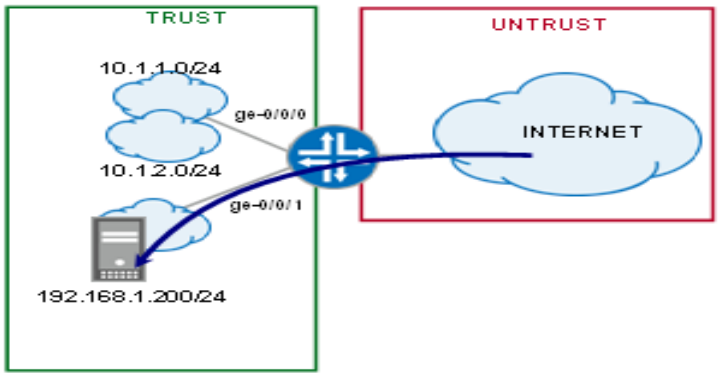
set security nat destination rule-set 1 rule 111 match destination-address 192.168.1.150/32

set security nat destination rule-set 1 rule 111 match destination-port 8080

set security nat destination rule-set 1 rule 111 then destination-nat pool 222

上述 NAT 配置定义:访问 192.168.1.150 地址 8080 端口映射至 20.1.1.200 地址 8080 端口,功能与 ScreenOS VIP 端口映射一致。

2.4.4 Pool base Static NAT 基于地址池的静态地址转换



图片仅供参考,下列配置参考实验拓扑

NAT：

set security nat static rule-set static-nat from zone untrust

set security nat static rule-set static-nat rule rule1 match destination-address 192.168.1.150

set security nat static rule-set static-nat rule rule1 then static-nat prefix 20.1.1.200

Policy:

set security policies from-zone trust to-zone untrust policy 1 match source-address any

set security policies from-zone trust to-zone untrust policy 1 match destination-address pc-1

set security policies from-zone trust to-zone untrust policy 1 match application any

set security policies from-zone trust to-zone untrust policy 1 then permit

Static NAT 概念与 ScreenOS MIP 一致，属于静态双向一对一 NAT，上述配置表示访问 192.168.1.150 时转换为 20.1.1.200，当 20.1.1.200 访问 Internet 时自动转换为 192.168.1.150，并且优先级比其他类型 NAT 高。

2.5 IPSEC VPN

SRX IPSEC VPN 支持 Site-to-Site VPN 和基于 NS-remote 的拨号 VPN 以及基于 IPSEC 的动态 VPN，访问方式通过 WEB 界面进行，和 ScreenOS 一样，site-to-site VPN 也支持路由模式和 Policy 模式，在配置方面也和 ScreenOS 基本一致。SRX 中的加密/验证算法在命名上和 ScreenOS 存在一些区别，配置过程中建议选择 ike 和 ipsec 的 proposal 为 standard 模式，standard 中包含 SRX 支持的全部加密/验证算法，只要对端设备支持其中任何一种即可。SRX 中通道接口使用 st0 接口，对应 ScreenOS 中的 tunnel 虚拟接口。

本次将列举如下配置案例：

1、 **基于策略的 LAN TO LAN IPSEC VPN**
2、 **基于路由的 LAN TO LAN IPSEC VPN**
3、 **基于 REMOTE VPN 客户端拨号 VPN**
4、 **基于 IPSEC 动态 VPN<通过 WEB 界面>**

注意在 REMOTE VPN 客户端拨号 VPN 中我们将列举 JUNIPER REMOTE VPN 客户端和第三方 ShrewSoft VPN Client,另外基于 IPSEC 动态 VPN 是通过 WEB 界面访问,初次登陆系统自动或人工下载一个 JAVA 客户端。

2.5.1 基于路由的 LAN TO LAN IPSEC VPN

SRX 配置：

下面是图中左侧 SRX 基于路由方式 Site-to-site VPN 配置：

set interfaces st0 unit 0 family inet address 1.1.1.1/24

set security zones security-zone untrust interfaces st0.0

set routing-options static route 172.16.1.0/24 next-hop st0.0

定义 st0 tunnel 接口地址/Zone 及通过 VPN 通道到对端网络路由

set security ike policy ABC mode main

set security ike policy ABC proposal-set standard

set security ike policy ABC pre-shared-key ascii-text *juniper*

定义 IKE Phase1 policy 参数，main mode，standard proposal 及预共享密钥方式

set security ike gateway gw1 ike-policy ABC

set security ike gateway gw1 address 10.1.1.254

set security ike gateway gw1 external-interface fe-0/0/2.0

定义 IKE gaeway 参数，预共享密钥认证，对端网关 10.1.1.254，出接口 fe-0/0/2（位于 dmz zone）

set security ipsec policy *AAA* proposal-set standard

set security ipsec vpn vpn1 bind-interface st0.0

set security ipsec vpn vpn1 ike gateway gw1

set security ipsec vpn vpn1 ike ipsec-policy *AAA*

set security ipsec vpn vpn1 establish-tunnels immediately

定义 ipsec Phase 2 VPN 参数：standard proposal、与 st0.0 接口绑定，调用 Phase 1 gw1 ike 网关。

set security policies from-zone untrust to-zone trust policy vpn-policy match source-address any

set security policies from-zone untrust to-zone trust policy vpn-policy match destination-address any

set security policies from-zone untrust to-zone trust policy vpn-policy match application any

set security policies from-zone untrust to-zone trust policy vpn-policy then permit

set security policies from-zone trust to-zone untrust policy vpn-policy match source-address any

set security policies from-zone trust to-zone untrust policy vpn-policy match destination-address any

set security policies from-zone trust to-zone untrust policy vpn-policy match application any

set security policies from-zone trust to-zone untrust policy vpn-policy then permit

两端设备策略开启双向 policy 以允许 VPN 流量通过

SSG 配置参考：

set ike gateway "abc" address 10.1.1.1 Main outgoing-interface "ethernet0/1" preshare "juniper" sec-level standard

set vpn "gw-1" gateway "abc" no-replay tunnel idletime 0 sec-level standard

set vpn "gw-1" monitor

set vpn "gw-1" id 0x1 bind interface tunnel.1

set interface tunnel.1 ip 1.1.1.2/24

set route 20.1.1.0/24 interface tunnel.1

set policy id 3 from "ssg-vpn" to "Trust" "Any-IPv4" "Any-IPv4" "ANY" permit log

set policy id 2 from "Trust" to "ssg-vpn" "Any-IPv4" "Any-IPv4" "ANY" permit log

SRX 设备端监控 VPN 状态

```
root# run show security ipsec security-associations
  Total active tunnels: 1
  ID    Gateway          Port  Algorithm       SPI      Life:sec/kb  Mon vsys
  <131073 10.1.1.254     500   ESP:3des/sha1   b5984553 3565/ unlim   U   0
  >131073 10.1.1.254     500   ESP:3des/sha1   e5075442 3565/ unlim   U   0

[edit]
root# run show security ike security-associations
Index   Remote Address  State  Initiator cookie  Responder cookie  Mode
2       10.1.1.254      UP     102cf6a03562f972  1e62de328dcc3fe1  Main

[edit]
root#
```

SSG 设备端监控 VPN 状态

```
screenos-> get sa
total configured sa: 1
HEX ID    Gateway         Port Algorithm     SPI      Life:sec kb Sta   PID vsys
00000001<         10.1.1.1  500 esp:3des/sha1 e5075442  2962 unlim A/U    -1 0
00000001>         10.1.1.1  500 esp:3des/sha1 b5984553  2962 unlim A/U    -1 0
screenos->
```

2.5.2 基于策略的 LAN TO LAN IPSEC VPN

要设置基于策略的LAN TO LAN IPSEC VPN通道，请在通道两端的安全设备上执行以下步骤:

1. 同样配置IKE\IPSEC参数<指定对方的IP地址、指定加密方式等>
2. 不需要配置通道接口
3. 为每个站点间通过的 VPN 流量设置策略,注意此时需要在策略中调用VPN IKE通道,如下命令：

SRX设备策略配置:

root# set security policies from-zone srx-vpn to-zone trust policy vpn-policy then permit tunnel ipsec-vpn vpn1

root# set security policies from-zone trust to-zone srx-vpn policy vpn-policy then permit tunnel ipsec-vpn vpn1

SSG设备策略配置:

set policy id 3 from ssg-vpn to trust 20.1.1.0/24 172.16.1.0/24 any tunnel vpn abc

set policy id 3 from trust to ssg-vpn 172.16.1.0/24 20.1.1.0/24 any tunnel vpn abc

特别提醒,基于策略的 LAN TO LAN IPSEC VPN 在建立策略的时候,两端设备的双向策略源地址、目标地址、服务必须一致对应。

2.5.3 基于 Remote VPN 客户端拨号 VPN

为了能够体现其配置真实性、可观性、此次配置将采用真实环境进行配置演示,具体如下：

第一步：定义分配给 VPN 拨号用户的 IP 地址池

set access address-pool xauth-pool address-range low 30.1.1.1

set access address-pool xauth-pool address-range high 30.1.1.100

第二步：定义 VPN 拨号用户

set access profile **xauth-users** authentication-order password

set access profile xauth-users client test1 firewall-user password "9qmQF69A01R/9M8xNbw"

set access profile xauth-users client test2 firewall-user password "9zPWq3Ct0BIcreOB-Vs2aJ"

第三步：定义 IKE Proposal

set security ike proposal **dialup-proposal** authentication-method pre-shared-keys

set security ike proposal dialup-proposal dh-group group2

set security ike proposal dialup-proposal authentication-algorithm sha1

set security ike proposal dialup-proposal encryption-algorithm aes-128-cbc

第四步：定义 IPSEC Proposal

set security ipsec proposal **dialup-proposal** protocol esp

set security ipsec proposal dialup-proposal authentication-algorithm hmac-sha1-96

set security ipsec proposal dialup-proposal encryption-algorithm aes-128-cbc

第五步： 定义 IKE policy

set security ike policy **dialup-policy** mode aggressive

set security ike policy dialup-policy proposals dialup-proposal

set security ike policy dialup-policy pre-shared-key ascii-text “JUNIPER-WXF1987”

第六步：定义 IKE gateway

set security ike gateway dialup-ike ike-policy **dialup-policy**

set security ike gateway dialup-ike dynamic **hostname juniper**

set security ike gateway dialup-ike dynamic connections-limit 100

set security ike gateway dialup-ike dynamic **ike-user-type shared-ike-id**

set security ike gateway dialup-ike **external-interface ge-0/0/8.0** 选择 VPN 接受从那个接口拨进来

set security ike gateway dialup-ike xauth access-profile **xauth-users**

第七步：定义 Ipsec policy

set security ipsec policy **dialup-policy2** proposals **dialup-proposal**

set security ipsec policy ipsec-pol perfect-forward-secrecy keys group2

set security ipsec policy ipsec-pol proposals phase2-prop

第八步：定义 ipsev vpn

set security ipsec vpn **dialup-vpn** ike gateway dialup-ike

set security ipsec vpn dialup-vpn ike ipsec-policy **dialup-policy2**

set security ipsec vpn dialup-vpn establish-tunnels on-traffic

第九步：定义 VPN 策略<内部允许访问的资源>

set security policies from-zone untrust to-zone dmz policy dialup-vpn match source-address any

set security policies from-zone untrust to-zone dmz policy dialup-vpn match destination-address 10.0.100.0/24-vlan_3

set security policies from-zone untrust to-zone dmz policy dialup-vpn match destination-address 10.0.110.0/24-vlan_4

set security policies from-zone untrust to-zone dmz policy dialup-vpn match destination-address 10.0.130.0/24-vlan_5

set security policies from-zone untrust to-zone dmz policy dialup-vpn match destination-address 10.0.140.0/24-vlan6

set security policies from-zone untrust to-zone dmz policy dialup-vpn match application any

set security policies from-zone untrust to-zone dmz policy dialup-vpn then permit tunnel ipsec-vpn dialup-vpn

set security policies from-zone untrust to-zone dmz policy dialup-vpn then log session-init

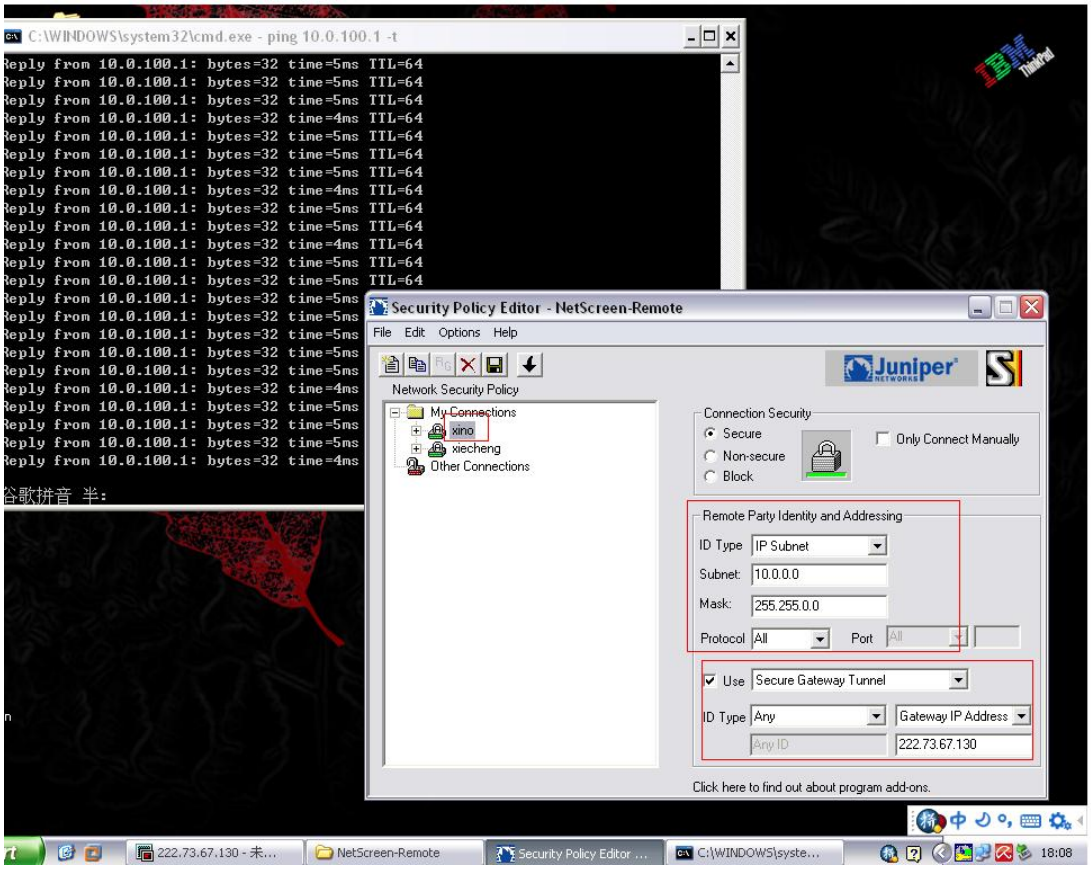
set security policies from-zone untrust to-zone dmz policy dialup-vpn then log session-close

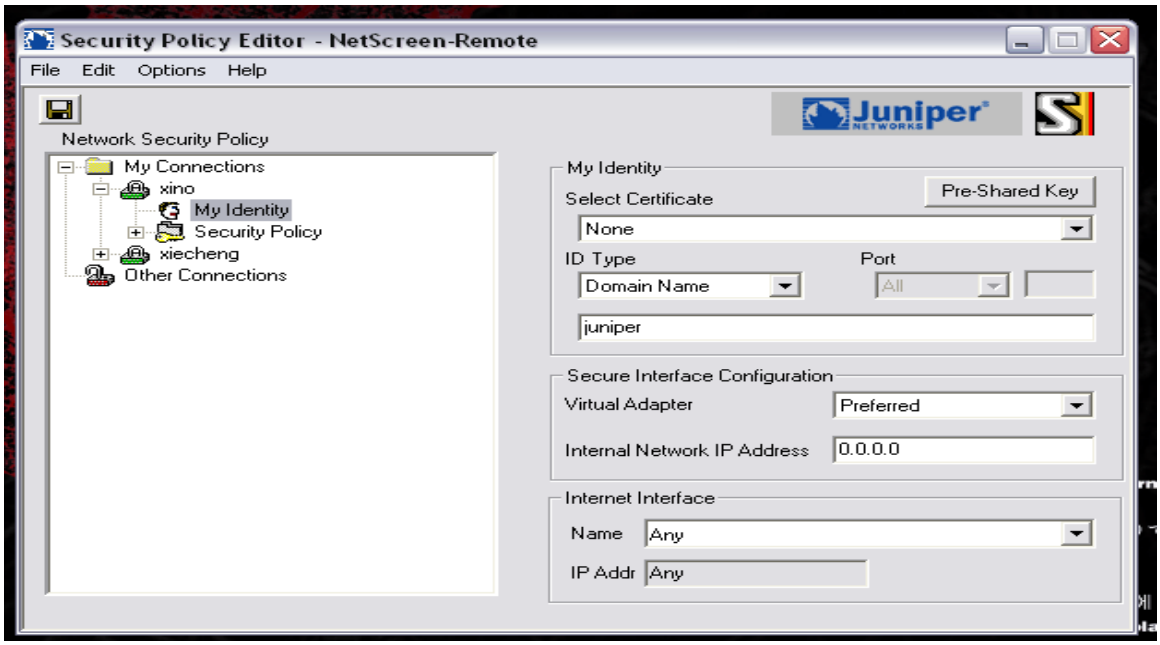
至此 ipsec 拨号 VPN 设备配置完成。

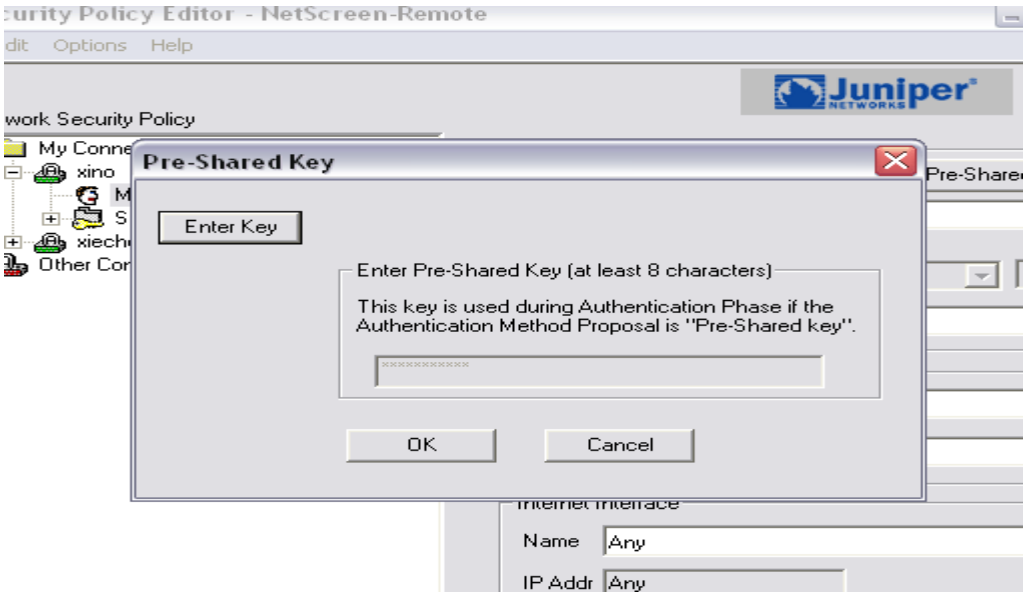
接下来我们将演示如何配置 Juniper Remote vpn 客户端<windows XP 系统>

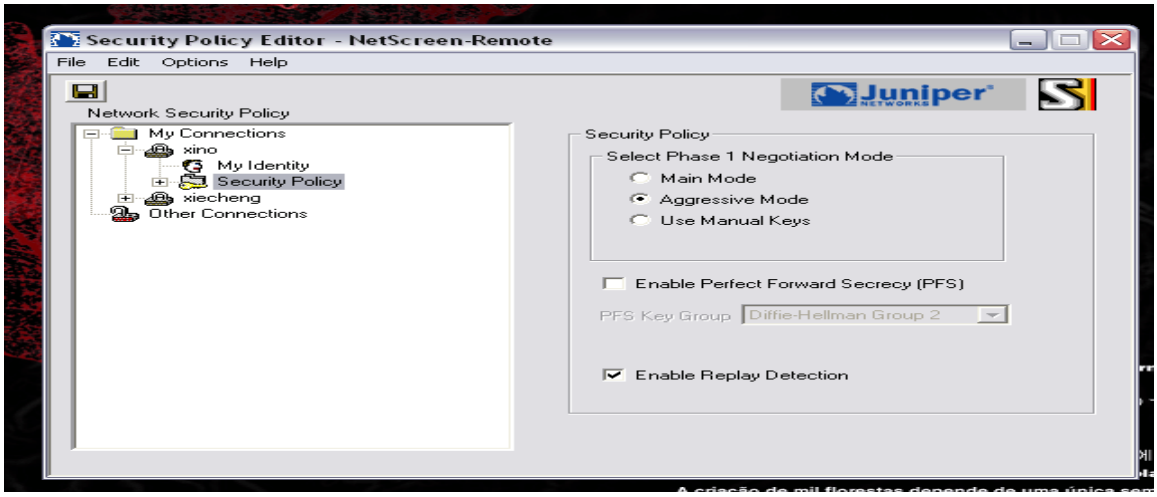
如何配置第三方 ShrewSoft VPN Client<windows 7>

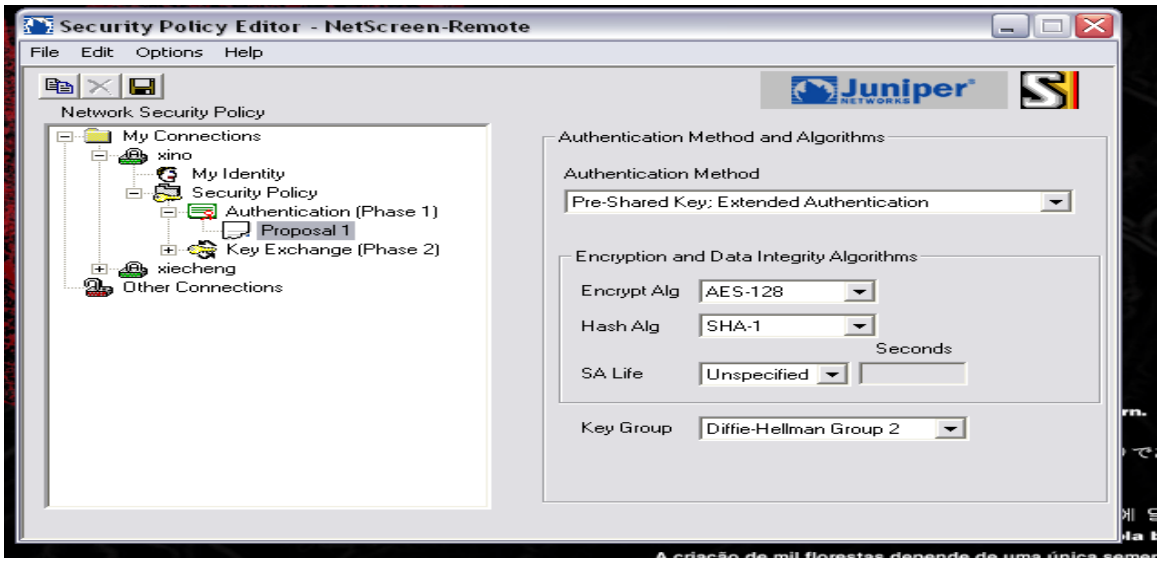
首先我们介绍 Juniper Remote vpn 客户端配置，参考如下截图配置<依据上述配置进行>：

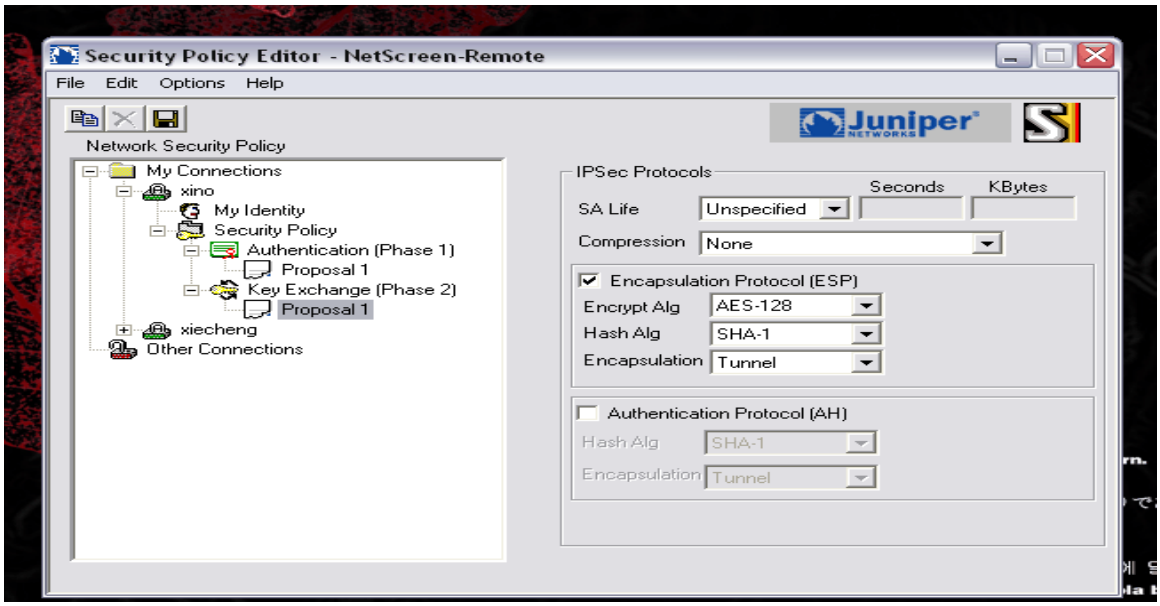


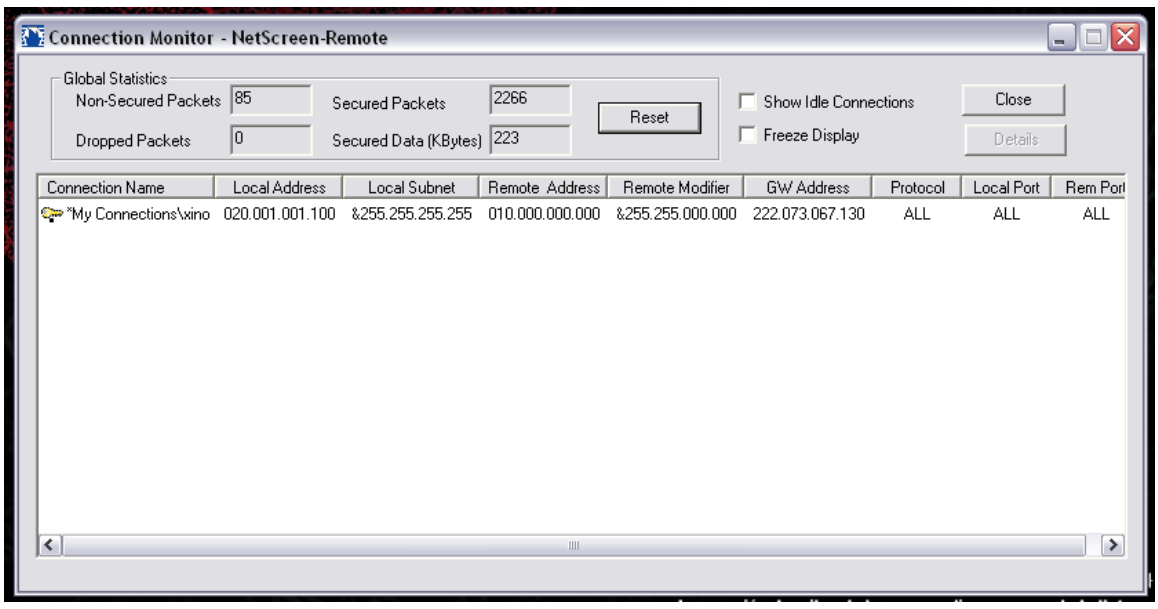

Security Policy Editor - NetScreen-Remote
File Edit Options Help
Juniper
Network Security Policy
My Connections
xino
My Identity
Security Policy
xiecheng
Other Connections
My Identity
Select Certificate
Pre-Shared Key
None
ID Type
Port
Domain Name
All
juniper
Secure Interface Configuration
Virtual Adapter
Preferred
Internal Network IP Address
0.0.0.0
Internet Interface
Name
Any
IP Addr
Any


Pre-Shared Key
Enter Key
Enter Pre-Shared Key (at least 8 characters)
This key is used during Authentication Phase if the Authentication Method Proposal is "Pre-Shared key".
OK
Cancel
Name
Any
IP Addr
Any


Security Policy Editor - NetScreen-Remote
File Edit Options Help
Juniper
Network Security Policy
My Connections
xino
My Identity
Security Policy
xiecheng
Other Connections
Security Policy
Select Phase 1 Negotiation Mode
Main Mode
Aggressive Mode
Use Manual Keys
Enable Perfect Forward Secrecy (PFS)
PFS Key Group
Diffie-Hellman Group 2
Enable Replay Detection


Security Policy Editor - NetScreen-Remote
File Edit Options Help
Juniper
Network Security Policy
My Connections
xino
My Identity
Security Policy
Authentication (Phase 1)
Proposal 1
Key Exchange (Phase 2)
xiecheng
Other Connections
Authentication Method and Algorithms
Authentication Method
Pre-Shared Key; Extended Authentication
Encryption and Data Integrity Algorithms
Encrypt Alg AES-128
Hash Alg SHA-1
Seconds
SA Life Unspecified
Key Group Diffie-Hellman Group 2


Security Policy Editor - NetScreen-Remote
File Edit Options Help
Juniper
Network Security Policy
My Connections
xino
My Identity
Security Policy
Authentication (Phase 1)
Proposal 1
Key Exchange (Phase 2)
Proposal 1
xiecheng
Other Connections
IPSec Protocols
Seconds KBytes
SA Life Unspecified
Compression None
Encapsulation Protocol (ESP)
Encrypt Alg AES-128
Hash Alg SHA-1
Encapsulation Tunnel
Authentication Protocol (AH)
Hash Alg SHA-1
Encapsulation Tunnel


Connection Monitor - NetScreen-Remote
Global Statistics
Non-Secured Packets 85
Secured Packets 2266
Dropped Packets 0
Secured Data (KBytes) 223
Reset
Show Idle Connections
Freeze Display
Close
Details
Connection Name Local Address Local Subnet Remote Address Remote Modifier GW Address Protocol Local Port Rem Port
"My Connections\xino 020.001.001.100 &255.255.255.255 010.000.000.000 &255.255.000.000 222.073.067.130 ALL ALL ALL

客户端查看连接状态如上，设备端查看连接状态如下：

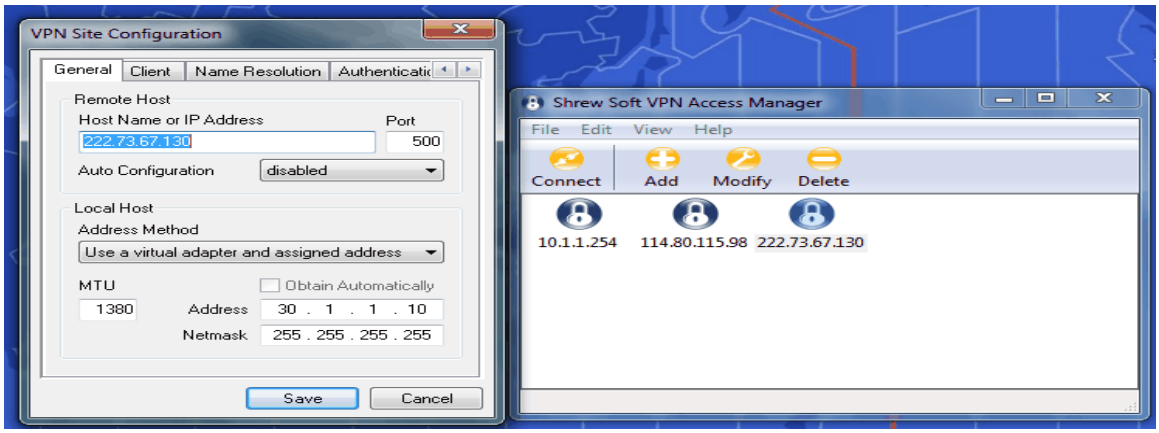
```
lab@SRX240_Firewell_01# run show security ipsec security-associations
  Total active tunnels: 1
  ID    Gateway          Port  Algorithm       SPI      Life:sec/kb  Mon vsys
  <133955786 58.41.57.6  52617 ESP:aes-128/sha1 48a147c8 2162/ unlim  -   0
  >133955786 58.41.57.6  52617 ESP:aes-128/sha1 86a2236c 2162/ unlim  -   0

[edit]
lab@SRX240_Firewell_01# run show security ipsec statistics
ESP Statistics:
  Encrypted bytes:        472465248
  Decrypted bytes:        223901168
  Encrypted packets:        1784869
  Decrypted packets:        1247746
AH Statistics:
  Input bytes:                    0
  Output bytes:                   0
  Input packets:                  0
  Output packets:                 0
Errors:
  AH authentication failures: 0, Replay errors: 0
  ESP authentication failures: 0, ESP decryption failures: 0
  Bad headers: 0, Bad trailers: 0

[edit]
lab@SRX240_Firewell_01# run show security ike security-associations
Index   Remote Address  State  Initiator cookie  Responder cookie  Mode
136     58.41.57.6      UP     92877b537201db6c  9a764b9f82bf438a  Aggressive
```

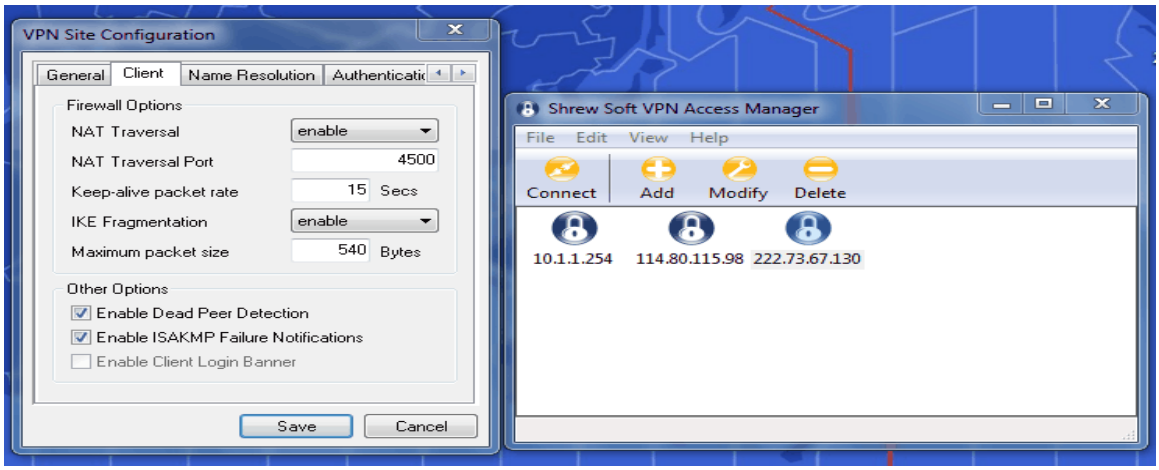
接下来我们介绍 ShrewSoft VPN Client<windows 7>客户端配置，参考如下截图配置<依据上述配置进行>：

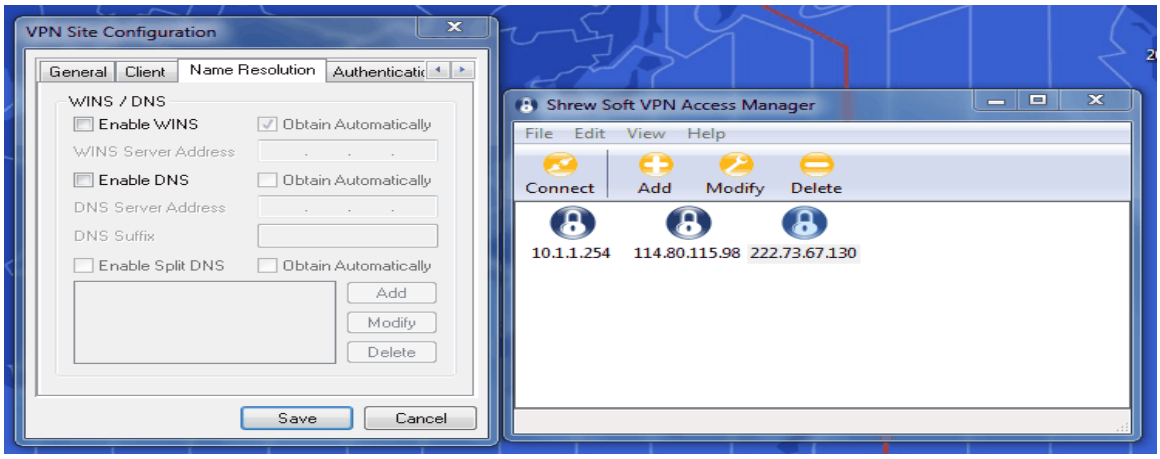
软件下载地址：http://www.shrewsoft.com/download

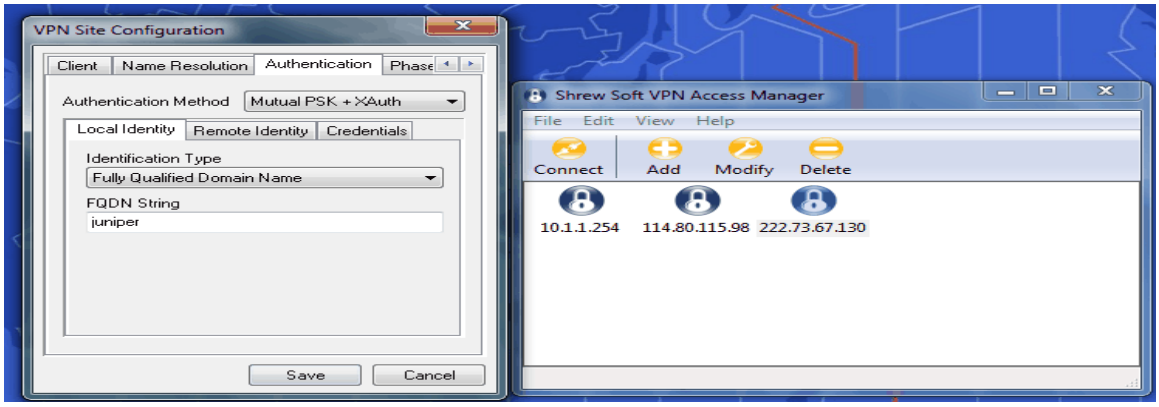
Please Select Your Download

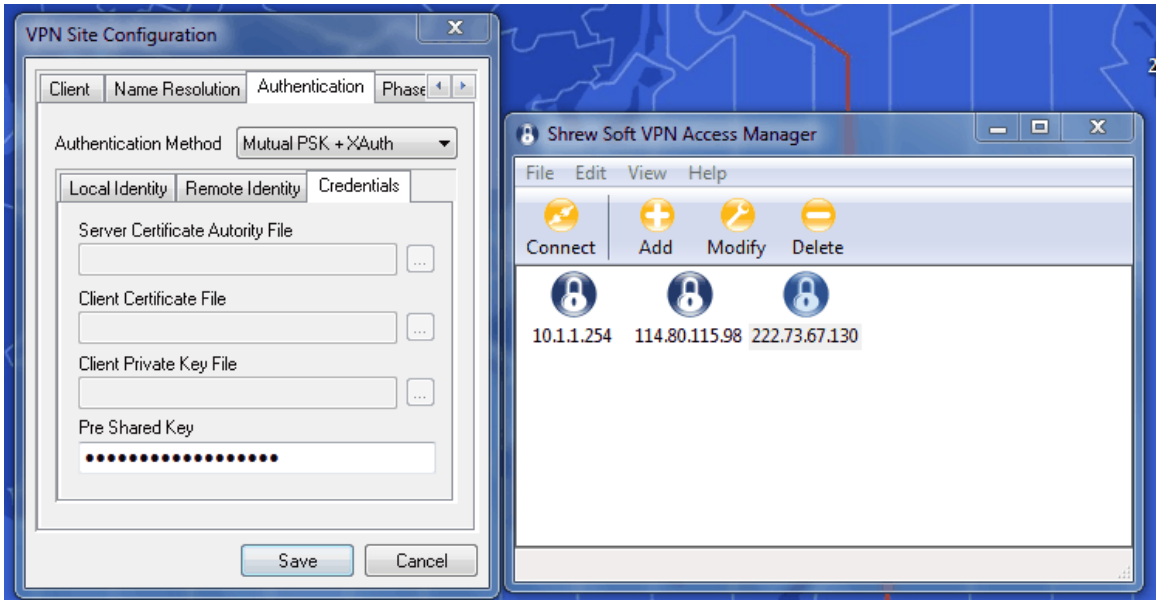
- VPN Client For Windows
- VPN Client For Linux and BSD

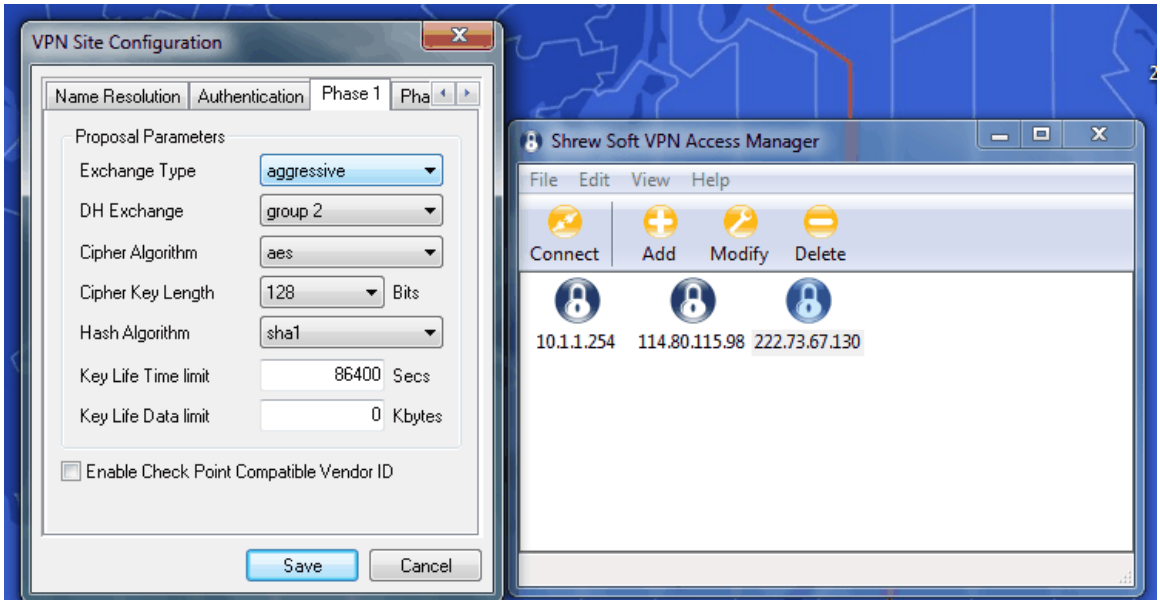


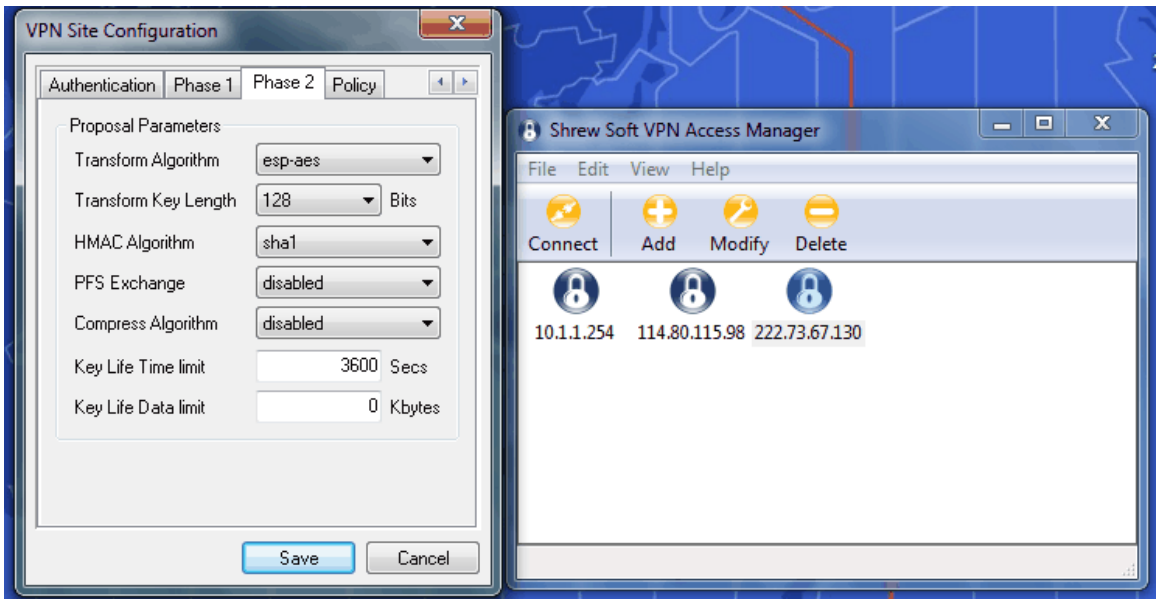

VPN Site Configuration
General
Client
Name Resolution
Authenticati
Firewall Options
NAT Traversal
enable
NAT Traversal Port
4500
Keep-alive packet rate
15
Secs
IKE Fragmentation
enable
Maximum packet size
540
Bytes
Other Options
Enable Dead Peer Detection
Enable ISAKMP Failure Notifications
Enable Client Login Banner
Save
Cancel
Shrew Soft VPN Access Manager
File
Edit
View
Help
Connect
Add
Modify
Delete
10.1.1.254
114.80.115.98
222.73.67.130

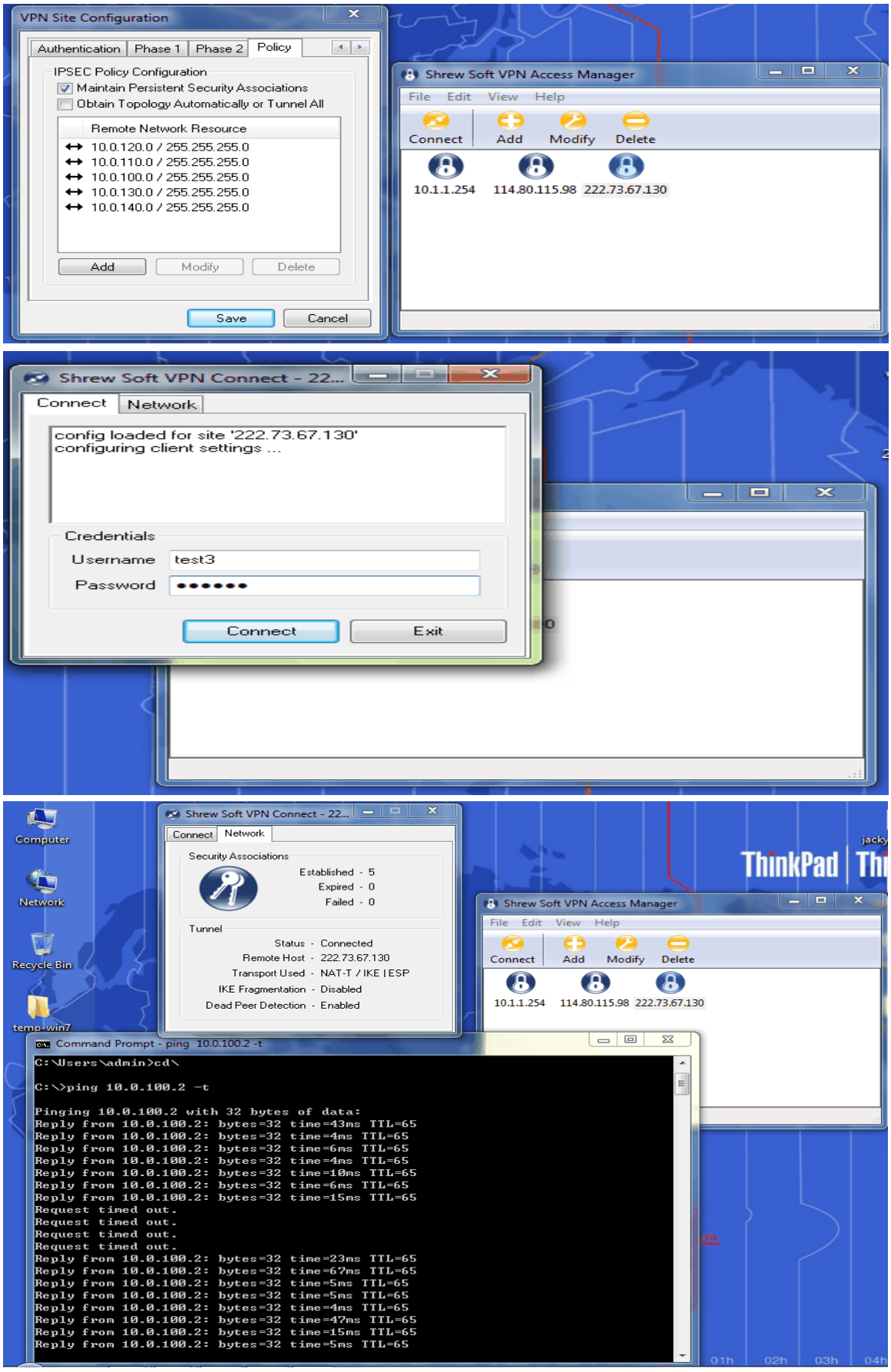

VPN Site Configuration
General
Client
Name Resolution
Authenticati
WINS / DNS
Enable WINS
Obtain Automatically
WINS Server Address
Enable DNS
Obtain Automatically
DNS Server Address
DNS Suffix
Enable Split DNS
Obtain Automatically
Add
Modify
Delete
Save
Cancel
Shrew Soft VPN Access Manager
File
Edit
View
Help
Connect
Add
Modify
Delete
10.1.1.254
114.80.115.98
222.73.67.130


VPN Site Configuration
Client
Name Resolution
Authentication
Phase
Authentication Method
Mutual PSK + XAuth
Local Identity
Remote Identity
Credentials
Identification Type
Fully Qualified Domain Name
FQDN String
juniper
Save
Cancel
Shrew Soft VPN Access Manager
File
Edit
View
Help
Connect
Add
Modify
Delete
10.1.1.254
114.80.115.98
222.73.67.130


VPN Site Configuration
Client
Name Resolution
Authentication
Phase
Authentication Method
Mutual PSK + XAuth
Local Identity
Remote Identity
Credentials
Server Certificate Autority File
Client Certificate File
Client Private Key File
Pre Shared Key
Save
Cancel
Shrew Soft VPN Access Manager
File
Edit
View
Help
Connect
Add
Modify
Delete
10.1.1.254
114.80.115.98
222.73.67.130


VPN Site Configuration
Name Resolution
Authentication
Phase 1
Pha
Proposal Parameters
Exchange Type
aggressive
DH Exchange
group 2
Cipher Algorithm
aes
Cipher Key Length
128
Bits
Hash Algorithm
sha1
Key Life Time limit
86400
Secs
Key Life Data limit
0
Kbytes
Enable Check Point Compatible Vendor ID
Save
Cancel
Shrew Soft VPN Access Manager
File
Edit
View
Help
Connect
Add
Modify
Delete
10.1.1.254
114.80.115.98
222.73.67.130


VPN Site Configuration
Authentication
Phase 1
Phase 2
Policy
Proposal Parameters
Transform Algorithm
esp-aes
Transform Key Length
128
Bits
HMAC Algorithm
sha1
PFS Exchange
disabled
Compress Algorithm
disabled
Key Life Time limit
3600
Secs
Key Life Data limit
0
Kbytes
Save
Cancel
Shrew Soft VPN Access Manager
File
Edit
View
Help
Connect
Add
Modify
Delete
10.1.1.254
114.80.115.98
222.73.67.130



至此 IPSEC VPN 客户端拨号两种类型客户端配置介绍到此为止，如有问题请联系文档编辑者。

2.5.4 基于 IPSEC 动态 VPN

为了能够体现其配置真实性、可观性、此次配置将采用真实环境进行配置演示,具体如下：

第一步：配置用户认证配置文件

set access profile **user-auth-profile** client partner firewall-user password "9E25hWLxNVw8LG "
set access profile user-auth-profile client wj firewall-user password "9qmQF69A01R/9M8xNbw"
set access profile user-auth-profile client wxf firewall-user password "9gdoUjk.PQ36q.1RcyKv"
set access **firewall-authentication web-authentication default-profile user-auth-profile**

第二步：配置 IKE Proposal

set security ike proposal **phase1-prop** authentication-method pre-shared-keys
set security ike proposal phase1-prop dh-group group2
set security ike proposal phase1-prop authentication-algorithm sha1
set security ike proposal phase1-prop encryption-algorithm 3des-cbc

第三步：配置 Ipsev Proposal

set security ipsec proposal **phase2-prop** protocol esp
set security ipsec proposal phase2-prop authentication-algorithm hmac-sha1-96
set security ipsec proposal phase2-prop encryption-algorithm 3des-cbc

第四步：配置 IKE policy

set security ike policy ike-pol mode aggressive
set security ike policy ike-pol proposals **phase1-prop**
set security ike policy ike-pol pre-shared-key ascii-text "9FmMq/pBRhrlMXz3REyMWxSr"

第五步：配置 IKE Gateway<分别对应不同的用户>

set security ike gateway dyn-gw-wxf ike-policy **ike-pol**
set security ike gateway dyn-gw-wxf dynamic hostname wxf
set security ike gateway dyn-gw-wxf **external-interface ge-0/0/8** **接受 VPN 流量请求端口**
set security ike gateway dyn-gw-wxf xauth access-profile **user-auth-profile**
set security ike gateway dyn-gw-partner ike-policy **ike-pol**
set security ike gateway dyn-gw-partner dynamic hostname partner
set security ike gateway dyn-gw-partner external-interface ge-0/0/8
set security ike gateway dyn-gw-partner xauth access-profile **user-auth-profile**

第六步：配置 Ipsec policy

set security ipsec policy **ipsec-pol** perfect-forward-secrecy keys group2
set security ipsec policy **ipsec-pol** proposals **phase2-prop**

第七步：配置 Ipsev VPN<分别对应不同的用户>

set security ipsec vpn dynamic-vpn-wxf ike gateway **dyn-gw-wxf**
set security ipsec vpn dynamic-vpn-wxf ike ipsec-policy **ipsec-pol**
set security ipsec vpn dynamic-vpn-partner ike gateway **dyn-gw-partner**
set security ipsec vpn dynamic-vpn-partner ike ipsec-policy **ipsec-pol**

第八步：配置动态 VPN<分别对应不同的用户>

set security dynamic-vpn access-profile **user-auth-profile**
set security dynamic-vpn clients client1 remote-protected-resources 10.0.0.0/16
set security dynamic-vpn clients client1 remote-exceptions 0.0.0.0/0
set security dynamic-vpn clients client1 ipsec-vpn **dynamic-vpn-wxf**
set security dynamic-vpn clients client1 user wxf

set security dynamic-vpn clients client3 remote-protected-resources 10.0.140.11/32
set security dynamic-vpn clients client3 remote-exceptions 0.0.0.0/0
set security dynamic-vpn clients client3 ipsec-vpn **dynamic-vpn-partner**
set security dynamic-vpn clients client3 user partner

第八步：配置 VPN 策略对应动态 VPN 用户

set security policies from-zone untrust to-zone dmz policy vpn-wxf-dy match source-address any
set security policies from-zone untrust to-zone dmz policy vpn-wxf-dy match destination-address 10.0.100.0/24-vlan_3
set security policies from-zone untrust to-zone dmz policy vpn-wxf-dy match destination-address 10.0.110.0/24-vlan_4
set security policies from-zone untrust to-zone dmz policy vpn-wxf-dy match destination-address 10.0.130.0/24-vlan_5
set security policies from-zone untrust to-zone dmz policy vpn-wxf-dy match destination-address 10.0.140.0/24-vlan6
set security policies from-zone untrust to-zone dmz policy vpn-wxf-dy match application any
set security policies from-zone untrust to-zone dmz policy vpn-wxf-dy then permit tunnel ipsec-vpn dynamic-vpn-wxf
set security policies from-zone untrust to-zone dmz policy vpn-wxf-dy then log session-init
set security policies from-zone untrust to-zone dmz policy vpn-wxf-dy then log session-close

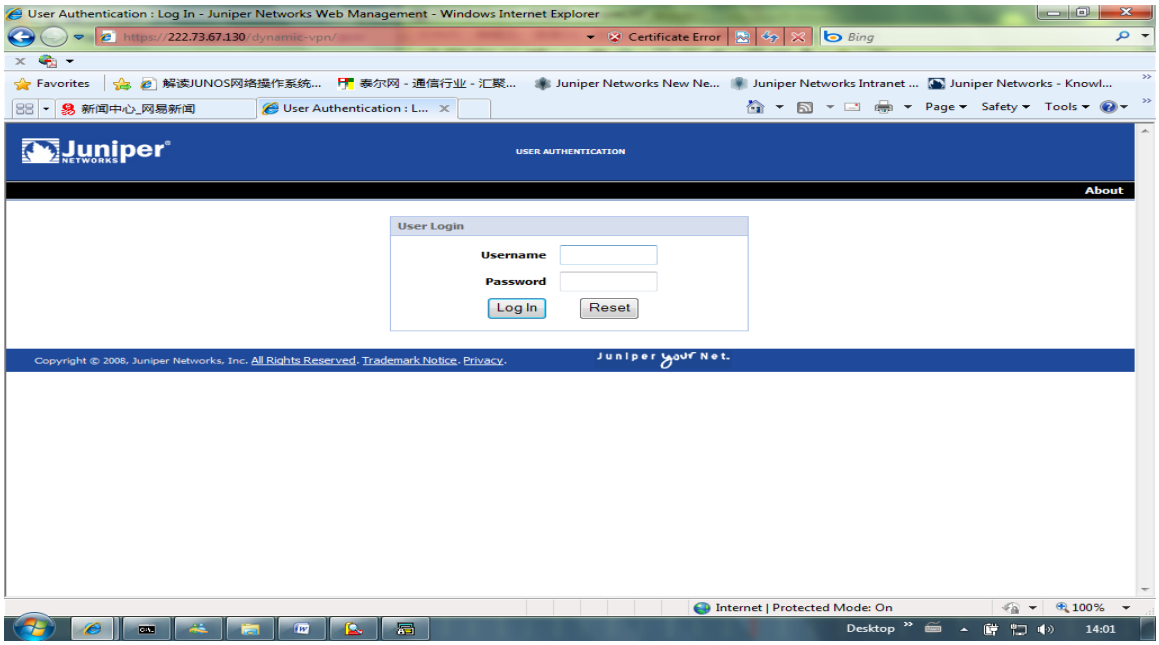
上面针对 WXF 用户、下面针对 Partner 用户

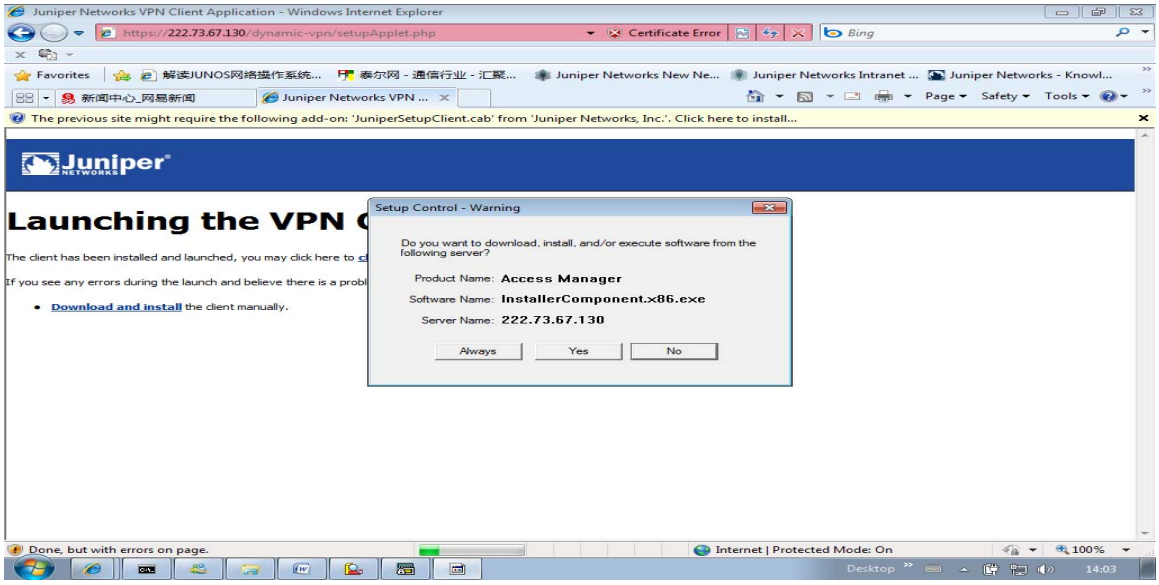
set security policies from-zone untrust to-zone dmz policy vpn-partner match source-address any
set security policies from-zone untrust to-zone dmz policy vpn-partner match destination-address 10.0.140.13/32
set security policies from-zone untrust to-zone dmz policy vpn-partner match destination-address 10.0.140.21/32
set security policies from-zone untrust to-zone dmz policy vpn-partner match destination-address 10.0.140.22/32
set security policies from-zone untrust to-zone dmz policy vpn-partner match application any
set security policies from-zone untrust to-zone dmz policy vpn-partner then permit tunnel ipsec-vpn dynamic-vpn-partner
set security policies from-zone untrust to-zone dmz policy vpn-partner then log session-init
set security policies from-zone untrust to-zone dmz policy vpn-partner then log session-close
set security policies from-zone untrust to-zone dmz policy vpn-partner then count

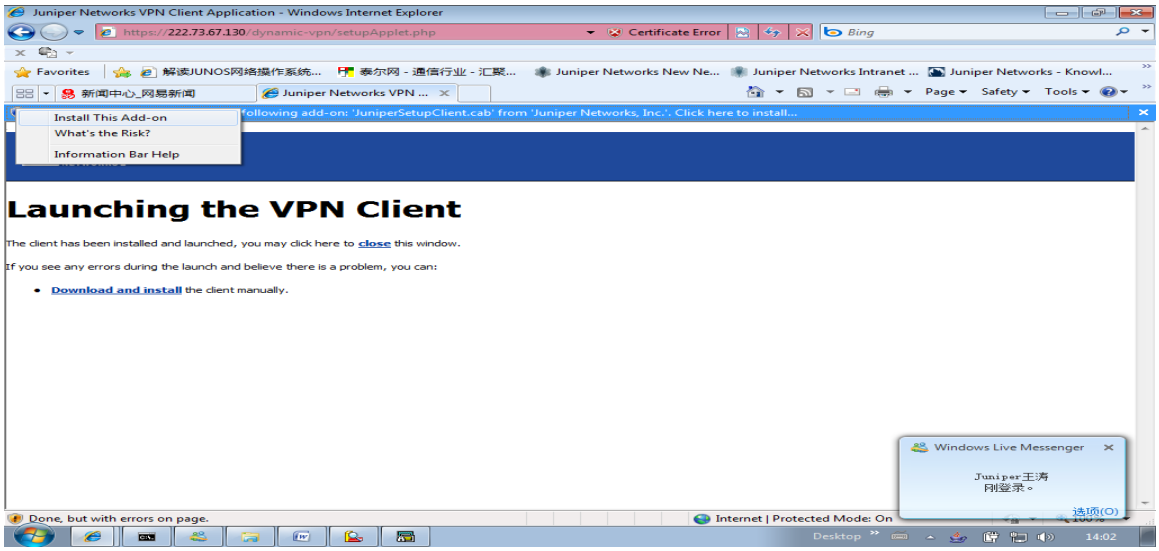
接下来我们介绍动态 VPN 客户端配置指导，参考如下截图配置<依据上述配置进行>：

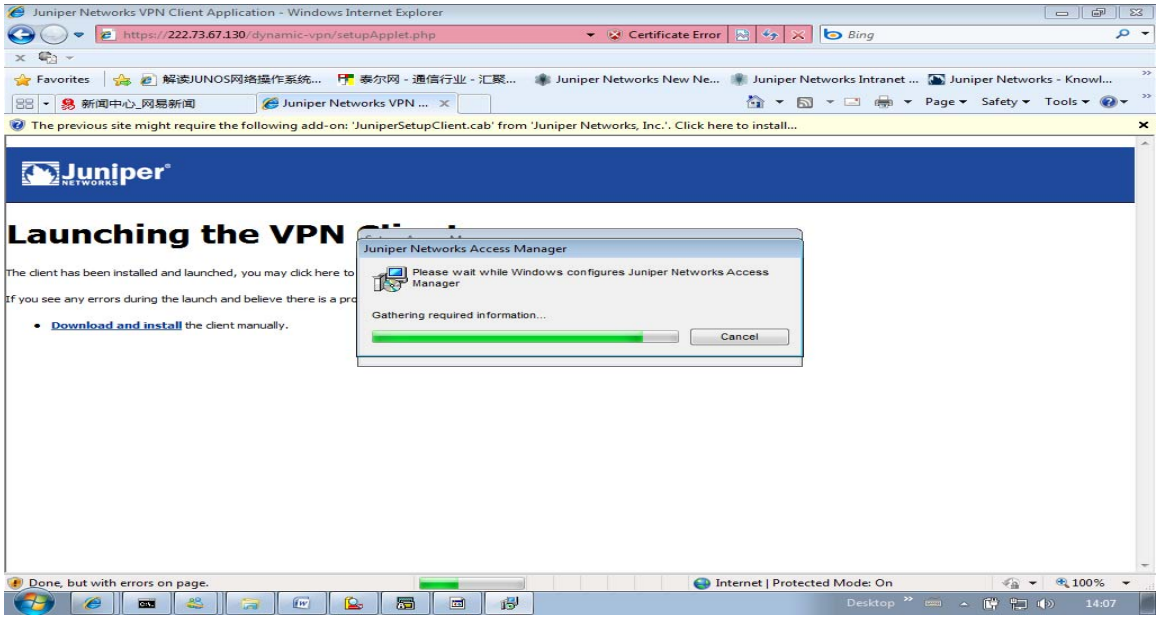
客户端通过 WEB-IE 访问地址：

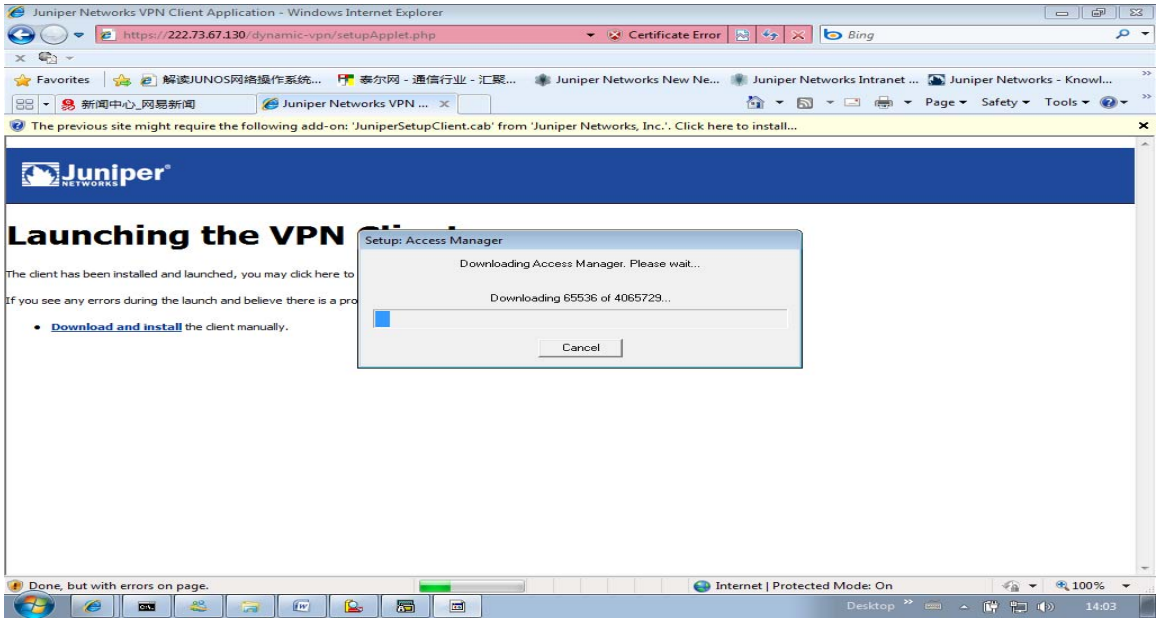
https://222.73.67.130/dynamic-vpn

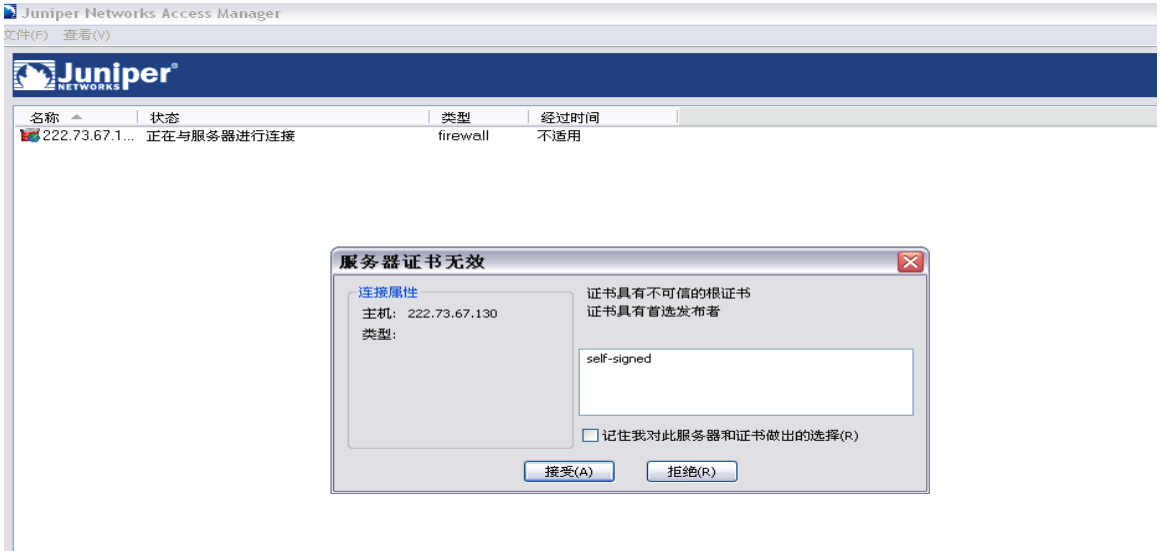

User Authentication : Log In - Juniper Networks Web Management - Windows Internet Explorer
https://222.73.67.130/dynamic-vpn/
Certificate Error
Bing
Favorites
User Authentication : L...
Page
Safety
Tools
Juniper
NETWORKS
USER AUTHENTICATION
About
User Login
Username
Password
Log In
Reset
Copyright © 2008, Juniper Networks, Inc. All Rights Reserved. Trademark Notice. Privacy.
Juniper your Net.
Internet | Protected Mode: On
100%
Desktop
14:01

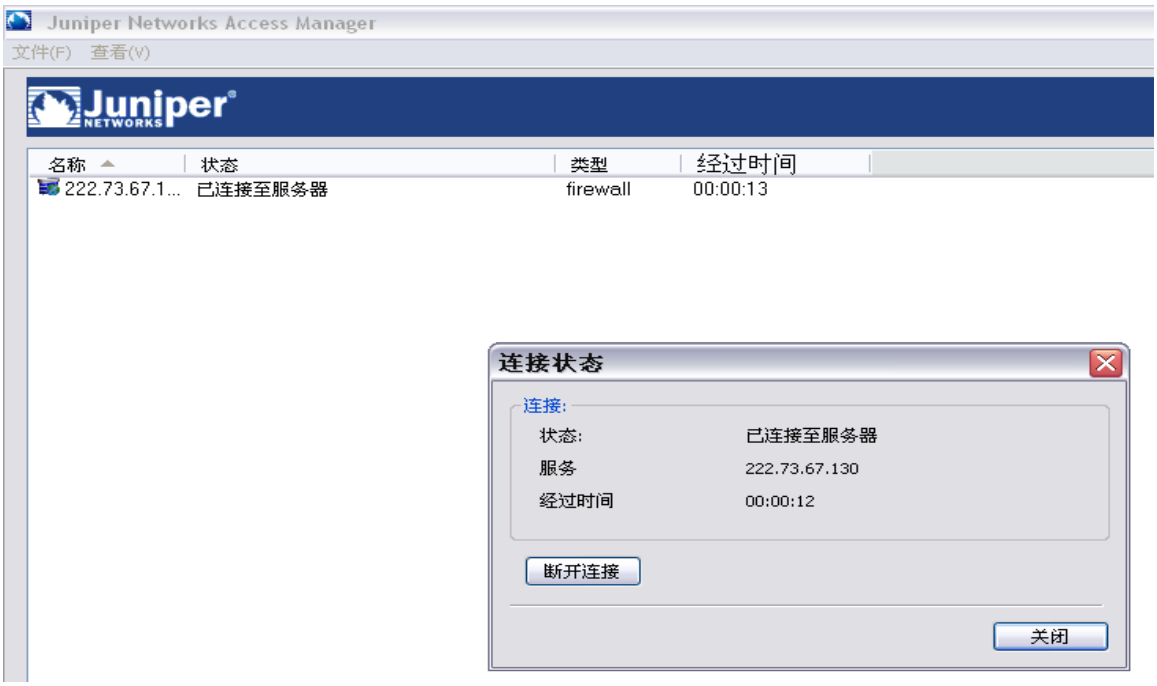

Juniper Networks VPN Client Application - Windows Internet Explorer
https://222.73.67.130/dynamic-vpn/setupApplet.php
Certificate Error
Bing
Favorites
Juniper Networks VPN ...
Page
Safety
Tools
The previous site might require the following add-on: 'JuniperSetupClient.cab' from 'Juniper Networks, Inc.'. Click here to install...
Juniper
NETWORKS
Launching the VPN C
The client has been installed and launched, you may click here to cl
If you see any errors during the launch and believe there is a probl
Download and install the client manually.
Setup Control - Warning
Do you want to download, install, and/or execute software from the following server?
Product Name: Access Manager
Software Name: InstallerComponent.x86.exe
Server Name: 222.73.67.130
Always
Yes
No
Done, but with errors on page.
Internet | Protected Mode: On
100%
Desktop
14:03


Juniper Networks VPN Client Application - Windows Internet Explorer
https://222.73.67.130/dynamic-vpn/setupApplet.php
Certificate Error
Bing
Favorites
Juniper Networks VPN ...
Page
Safety
Tools
Install This Add-on
What's the Risk?
Information Bar Help
following add-on: 'JuniperSetupClient.cab' from 'Juniper Networks, Inc.'. Click here to install...
Launching the VPN Client
The client has been installed and launched, you may click here to close this window.
If you see any errors during the launch and believe there is a problem, you can:
Download and install the client manually.
Windows Live Messenger
Juniper王涛
刚登录。
选项(O)
Done, but with errors on page.
Internet | Protected Mode: On
Desktop
14:02


Juniper Networks VPN Client Application - Windows Internet Explorer
https://222.73.67.130/dynamic-vpn/setupApplet.php
Certificate Error
Bing
Favorites
Juniper Networks VPN ...
The previous site might require the following add-on: 'JuniperSetupClient.cab' from 'Juniper Networks, Inc.'. Click here to install...
Juniper
Launching the VPN
The client has been installed and launched, you may click here to
If you see any errors during the launch and believe there is a pro
Download and install the client manually.
Juniper Networks Access Manager
Please wait while Windows configures Juniper Networks Access Manager
Gathering required information...
Cancel
Done, but with errors on page.
Internet | Protected Mode: On
100%
14:07


Juniper Networks VPN Client Application - Windows Internet Explorer
https://222.73.67.130/dynamic-vpn/setupApplet.php
Certificate Error
Bing
Favorites
Juniper Networks VPN ...
The previous site might require the following add-on: 'JuniperSetupClient.cab' from 'Juniper Networks, Inc.'. Click here to install...
Juniper
Launching the VPN
The client has been installed and launched, you may click here to
If you see any errors during the launch and believe there is a pro
Download and install the client manually.
Setup: Access Manager
Downloading Access Manager. Please wait...
Downloading 65536 of 4065729...
Cancel
Done, but with errors on page.
Internet | Protected Mode: On
100%
14:03


Juniper Networks Access Manager
文件(F) 查看(V)
Juniper
名称
状态
类型
经过时间
222.73.67.1...
正在与服务器进行连接
firewall
不适用
服务器证书无效
连接属性
主机: 222.73.67.130
类型:
证书具有不可信的根证书
证书具有首选发布者
self-signed
记住我对此服务器和证书做出的选择(R)
接受(A)
拒绝(R)



至此客户端配置完成,下面介绍设备端动态 VPN 状态

```
lab@SRX240_Firewell_01# run show security dynamic-vpn users detail
User: partner , Number of connections: 1
    Remote IP: 58.41.57.6
    IPSEC VPN: dynamic-vpn-partner
    IKE gateway: dyn-gw-partner
    IKE ID    : partner
    IKE Lifetime: 3600
    IPSEC Lifetime: 28800
    Status: CONNECTED


[edit]
lab@SRX240_Firewell_01# run show security dynamic-vpn client version
Juniper Access Manager version: 1.1.0.6475

[edit]
lab@SRX240_Firewell_01#
```

2.6 应用层网关 ALG 配置及说明

SRX 中自定义服务及 ALG 使用方法与 ScreenOS 保持一致，系统缺省开启 FTP ALG，为 TCP 21 服务提供 FTP 应用 ALG。自定义服务如果属于 FTP 类应用，需要将此自定义服务（非 TCP 21 端口）与 FTP 应用进行关联。下面举例定义一个 FTP 类服务 ftp-test，使用目的端口为 TCP 2100，服务超时时间为 3600 秒，并将此自定义服务与 FTP 应用关联（ALG），系统将识别此服务为 FTP 应用并开启 FTP ALG 来处理该应用流量。

set applications application ftp-test protocol tcp destination-port 2100 inactivity-timeout 3600
set applications application ftp-test application-protocol ftp

Branch 系统防火墙 ALG 状态如下（10.1R2.8 版本）

root# run show security alg status <默认配置下>

ALG Status :

DNS : Enabled FTP : Enable H323 : Enabled
MGCP : Enabled MSRPC : Enabled PPTP : Enabled
RSH : Enabled RTSP : Enabled SCCP : Enabled
SIP : Enabled SQL : Enabled SUNRPC : Enabled
TALK : Enabled TFTP : Enabled

建议不需要使用到的 ALG 可以关闭，以免影响正常应用，但是如果应用工作在 NAT 模式下则建议开启。

2.7 SRX Branch 系列 JSRP HA 高可用性配置及说明

JSRP 是 Juniper SRX 的私有 HA 协议，对应 ScreenOS 的 NSRP 双机集群协议，支持 A/P 和 A/A 模式，JSRP 对 ScreenOS NSRP 协议和 JUNOS Cluster 集群技术进行了整合集成，熟悉 NSRP 协议有助于对 JSRP 协议的理解。JSRP 和 NSRP 最大的区别在于 JSRP 是完全意义上的 Cluster 概念，两台设备完全当作一台设备来看待，两台设备的接口板卡顺序编号、运维变更将对两台设备同时进行操作，无需额外执行 ScreenOS 的配置和会话同步等操作，而 ScreenOS NSRP 可看作在同步配置和动态对象（session）基础上独立运行的两台单独设备。

JSRP 要求两台设备在软件版本、硬件型号、板卡数量、插槽位置及端口使用方面严格一一对应。由于 SRX 是转发与控制层面完全分裂架构，JSRP 需要控制层面（配置同步）和数据层面（Session 同步）两个平面的互联，高端系列 3K\5K 建议控制和数据层面互联链路使用光纤链路直连（部分平台强制要求光纤链路直连）。

在 Branch 系列则控制平面连接、带外管理接口必须使用设备规定的接口，而数据平面可以使用任何一个以太网口进行互连。

下面将介绍 SRX Branch 系列防火墙运行 HA 情况下，控制平面、带外接口连接示意图：

You must use the following ports to form the control link on the SRX Series branch

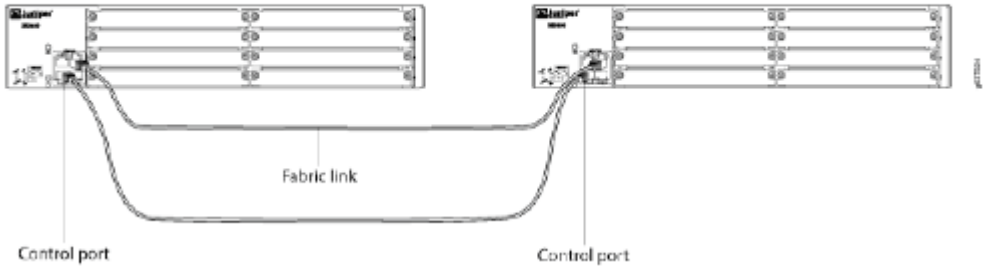
你必须使用下面设备指定端口来作为HA控制信号端口进行互连

设备型号:

- For SRX100 devices, connect the fe-0/0/7 port to the fe-1/0/7 port
- For SRX210 devices, connect the fe-0/0/7 port to the fe-2/0/7 port
- For SRX240 devices, connect the ge-0/0/1 port to the ge-5/0/1 port
- For SRX650 devices, connect the ge-0/0/1 port to the ge-9/0/1 port

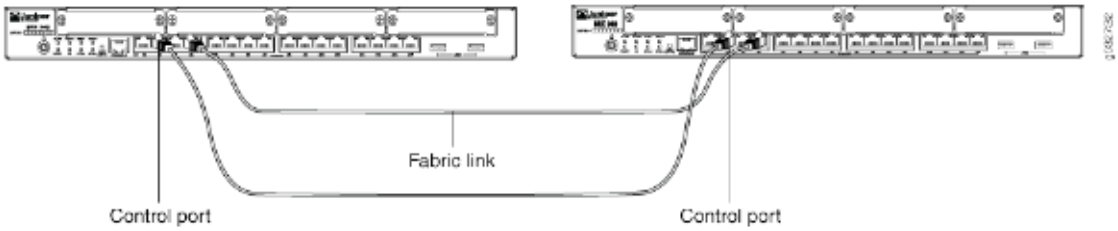
SRX650<标准配置 4 个千兆以太网 RJ-45 接口>SRX650 平台如果需要部署 HA 结构，则必须增加数据接口板卡<因为 HA 控制平面、数据平面和带外管理接口被占用了至少 3 个接口>

Figure 158: Connecting SRX Series Devices in a Cluster (SRX650 Devices)



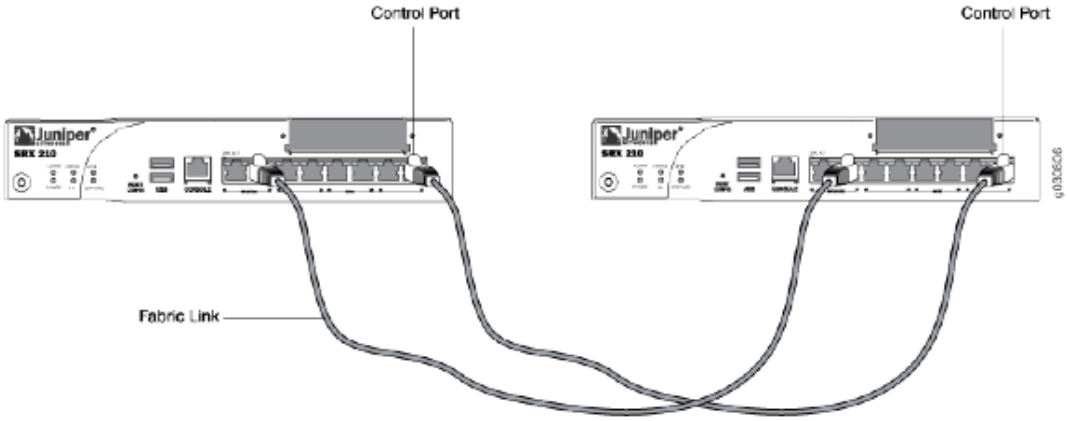
SRX240<标准配置 16 个千兆以太网 RJ-45 接口>

Figure 159: Connecting SRX Series Devices in a Cluster (SRX240 Devices)



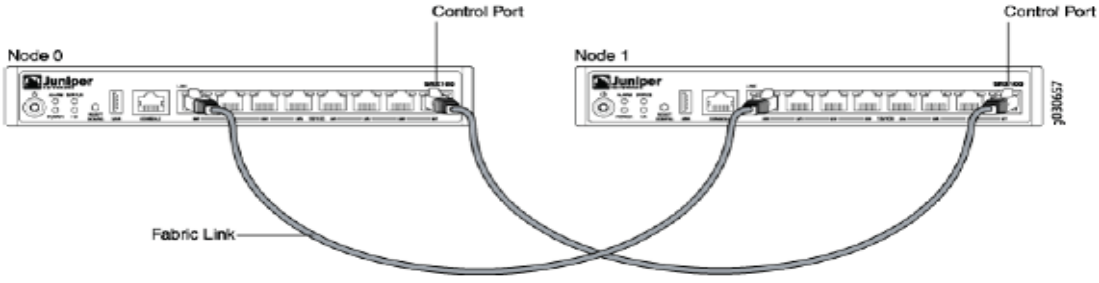
SRX210<标准配置 2 个千兆以太网 RJ-45 接口和 6 个百兆以太网 RJ-45 接口>

Figure 160: Connecting SRX Series Devices in a Cluster (SRX210 Devices)



SRX100<标准配置 8 个百兆以太网 RJ-45 接口>

Figure 161: Connecting SRX Series Devices in a Cluster (SRX100 Devices)



SRX Branch 系列接口规范<HA 控制接口、HA 带外管理接口以及 HA 数据接口>

Model	Chassis	Maximum Slots Per Node	Slot Numbering in a Cluster	Management Physical Port/Logical Interface	Control Physical Port/Logical Interface	Fabric Physical Port/Logical Interface
650	Node 0	9 (PIM slots)	0 — 8	ge-0/0/0	ge-0/0/1	Any Ethernet port
				fxp0	fxp1	fab0
	Node 1		9 — 17	ge-9/0/0	ge-9/0/1	Any Ethernet port
				fxp0	fxp1	fab1
240	Node 0	5 (PIM slots)	0 — 4	ge-0/0/0	ge-0/0/1	Any Ethernet port
				fxp0	fxp1	fab0
	Node 1		5 — 9	ge-5/0/0	ge-5/0/1	Any Ethernet port
				fxp0	fxp1	fab1
210	Node 0	2 (PIM slots)	0 and 1	fe-0/0/6	fe-0/0/7	Any Ethernet port
				fxp0	fxp1	fab0
	Node 1		2 and 3	fe-2/0/6	fe-2/0/7	Any Ethernet port
				fxp0	fxp1	fab1
100	Node 0	1(PIM slot)	0	fe-0/0/6	fe-0/0/7	Any Ethernet port
				fxp0	fxp1	fab0
	Node 1		1	fe-1/0/6	fe-1/0/7	Any Ethernet port
				fxp0	fxp1	fab1

JSRP 接口命名方式采用多个机箱抽象成一个逻辑机箱之后再统一为各个槽位进行编号，如上所示的每个机箱有几个业务槽位，节点 0 槽位号从 0 开始编号，节点 1 槽位号从节点 0 后面开始往后编。

整个 JSRP 配置过程包括如下 7 个步骤

- 配置 Cluster id 和 Node id（对应 ScreenOS NSRP 的 cluster id 并需手工指定设备使用节点 id）
- 指定 Control Port （指定控制层面使用接口，用于配置同步及心跳）
- 指定 Fabric Link Port （指定数据层面使用接口，主要 session 等 RTO 同步）
- 配置 Redundancy Group （类似 NSRP 的 VSD group，优先级与抢占等配置）
- 每个机箱的个性化配置 （单机无需同步的个性化配置，如主机名、带外管理口 IP 地址等）
- 配置 Redundant Ethernet Interface （类似 NSRP 的 Redundant 冗余接口）
- 配置 Interface Monitoring （类似 NSRP interface monitor，是 RG 数据层面切换依据）

SRX JSRP 配置样例<SRX240>：

- 配置 Cluster id 和 Node id

SRX-A>set chassis cluster cluster-id 1 node 0 reboot（注意该命令需在 operational 模式下输入，Cluster ID 取值范围为 1 - 15，当 Cluster ID = 0 时将 unsets the cluster）

SRX-B>set chassis cluster cluster-id 1 node 1 reboot

- 指定 Control Port（SRX Branch 系列，则无需指定,默认规定采用某一个接口作为控制接口，参考上一节）：
- 指定 Fabric Link Port

set interfaces fab0 fabric-options member-interfaces ge-0/0/2

set interfaces fab1 fabric-options member-interfaces ge-5/0/2

注：Fabric Link 中的 Fab0 固定用于 node 0，Fab1 固定用于 node 1

- 配置 Redundancy Group

RG0 固定用于主控板 RE 切换，RG1 以后用于 redundant interface 切换，RE 切换独立于接口切换

set chassis cluster reth-count 10 （指定整个 Cluster 中 redundant ethernet interface 最多数量）

set chassis cluster redundancy-group 0 node 0 priority 200 （高值优先，与 NSRP 相反）

set chassis cluster redundancy-group 0 node 1 priority 100

set chassis cluster redundancy-group 1 node 0 priority 200 （高值优先，与 NSRP 相反）

set chassis cluster redundancy-group 1 node 1 priority 100

- 每个机箱的个性化配置，便于对两台设备的区分与管理

set groups node0 system host-name SRX-A

set groups node0 interfaces fxp0 unit 0 family inet address 1.1.1.1/24 （带外网管口名称为 fxp0，区别 ScreenOS 的 MGT 口）

set groups node1 system host-name SRX-B

set groups node1 interfaces fxp0 unit 0 family inet address 1.1.1.2/24

set apply-groups ${node} （应用上述 groups 配置）

- 配置 Redundant Ethernet Interface

Redundant Ethernet Interface 类似 ScreenOS 里的 redundant interface，只不过 Redundant Ethernet interface 是分布在不同的机箱上（这一特性又类似 ScreenOS 的 VSI 接口）。

Set interface ge-0/0/8 gigether-options redundant-parent reth0 （node 0 的 ge-0/0/8 接口）

Set interface ge-5/0/8 gigether-options redundant-parent reth0 （node 1 的 ge-0/0/8 接口）

Set interface reth0 redundant-ether-options redundancy-group 1 （reth0 属于 RG1）

Set interface reth0 unit 0 family inet address 192.168.0.1/24

- 配置 Interface Monitoring，被监控的接口 Down 掉后，RG1 将自动进行主备切换（与 ScreenOS 类似），

Set cluster redundancy-group 1 interface-monitor ge-0/0/0 weight 255

Set cluster redundancy-group 1 interface-monitor ge-0/0/1 weight 255

Set cluster redundancy-group 1 interface-monitor ge-13/0/0 weight 255

Set cluster redundancy-group 1 interface-monitor ge-13/0/1 weight 255

- **JSRP 维护命令**

a) 手工切换 JSRP Master，RG1 原 backup 将成为 Master

root@srx240a> request chassis cluster failover redundancy-group 1 node 1

b) 手工恢复 JSRP 状态，按照优先级重新确定主备关系（高值优先）

root@srx240b> request chassis cluster failover reset redundancy-group 1

c) 查看 cluster interface

root@router> show chassis cluster interfaces

d) 查看 cluster 状态、节点状态、主备关系

lab@240a# run show chassis cluster status

e) 取消 cluster 配置

lab@Srx240a# set chassis cluster disable reboot

f) 升级 JSRP 软件版本

SRX 目前暂不支持软件在线升级（ISSU），升级过程会中断业务。

升级步骤如下：

1.升级 node 0，注意不要重启系统

2.升级 node 1，注意不要重启系统.

3.同时重启两个系统

g) 恢复处于 disabled 状态的 node

当 control port 或 fabric link 出现故障时，为避免出现双 master (split-brain)现象，JSRP 会把出现故障前状态为 secdonary 的 node 设为 disabled 状态,即除了 RE,其余部件都不工作。想要恢复必须 reboot 该 node。2.8 WEB 界面操作介绍 2.9 Screen 配置操作介绍

2.8 SRX Branch 系列 IDP、UTM 配置操作介绍

SRX Branch 系列产品提供一整套统一威胁管理 (UTM) 服务，包括：入侵防御系统 (IPS)、防病毒、防垃圾邮件、通过内容过滤实现的网页过滤以及防信息泄露，从而保护您的网络，防止最新的内容威胁。特定型号的产品还具有内容安全加速器以提供高性能 IPS 和防病毒性能。面向分支机构的 SRX 系列产品与其它的瞻博安全产品集成，从而提供企业级的统一接入控制和自适应威胁管理功能。这些功能为安全专家提供了与网络犯罪和数据丢失斗争的强大工具。

配置 IDP、UTM 功能之前,你首先需要知道你的设备是否购买了相关功能的 license，可以通过下面命令进行查看，由于测试中本人的设备 License 过期,相应的功能只是不能更新而已,功能测试使用没有问题。

由于当前测试过程没有 NSM 管理平台,故测试中的 IDP\UTM 等功能产生的日志无法收集分析。

root# run show system license 〈将会显示相应的功能 license 以及过期时间〉

如果 license 过去也可以通过相应的命令进行查看,如下：

root# run show system alarms

3 alarms currently active

Alarm time	Class	Description
2010-06-17 19:22:31 CST	Minor	License grace period for feature 28 expired
2010-06-17 19:22:31 CST	Minor	License grace period for feature 27 expired
2010-06-17 19:22:31 CST	Minor	License grace period for feature 25 expired

默认情况下,设备沟通过去将有提供一个月的试用期 license。

首先我们将介绍 IDP 配置

第一步：申请 license,此步骤必须保证设备本身能够访问 Internet

Root#run request system license update trial

第二步：查看 license 更新情况

root# run show system license

第三步：检查并下载安装 IDP 特征库更新包<需要设备本身能够访问 internet>

root# run request security idp security-package ? **下载并安装更新包**

Possible completions:

download	Download security package (Package includes detector and deltas for attack table)
install	Update attack database, active policy, detector with new package

第四步：检查下载状态、下载特征库版本、更新日期等信息

```
root# run request security idp security-package download status
In progress: Downloading ...
root# run request security idp security-package download status
Done;Successfully downloaded from(https://services.netscreen.com/cgi-bin/index.cgi).
Version info:1714(Wed Jun 16 14:41:19 2010, Detector=10.4.160100525)
root# run request security idp security-package download check-server
Successfully retrieved from(https://services.netscreen.com/cgi-bin/index.cgi).
Version info:1714(Detector=10.4.160100525, Templates=2)
```

第五步：当完成上述操作下载 IDP 特征库以后,需要进行对特征库的安装

```
root# run request security idp security-package install ?  特征库安装并查看安装状态
Possible completions:
  <[Enter]>                  Execute this command
  policy-templates           Update previously installed policy-templates with newly downloaded ones
  status                     Retrieve the status of security package load operation
  update-attack-database-only  Don't update/push active policy or detector to data plane
  |                          Pipe through a command
```

第六步：配置 IDP 策略与安装策略

```
root# show security idp    配置 IDP 策略与安全策略
idp-policy juniper-srx-idp-test {
    rulebase-ips {
        rule 1 {
            match {
                source-address any;
                destination-address any;
                attacks {
                    predefined-attack-groups [ HTTP DNS ICMP UDP TCP ];
                }
            }
            then {
                action {
                    ignore-connection;
                }
                notification {
                    log-attacks;
                }
            }
        }
    }
}
active-policy juniper-srx-idp-test;  激活 IDP 策略

[edit]
root# show security policies
```

```
from-zone dmz to-zone untrust {
    policy d-u {
        match {
            source-address any;
            destination-address any;
            application any;
        }
        then {
            permit {
                application-services {
                    idp;  针对当前策略开启 IDP 功能
                }
            }
            log {
                session-init;
```

第七步：查看 IDP 功能工作状态命令：

root# run show security idp ?

Possible completions:

application-identification Show IDP application identification data
application-statistics Show IDP application statistics
attack Show IDP attack data
counters Show IDP counters
memory Show IDP data plane memory statistics
policies Show the list of currently installed policies
policy-templates-list Show available policy templates
security-package-version Show the version of currently installed security-package
status Show IDP status

root# run show security idp status

State of IDP: 2-default, Up since: 2010-01-19 23:23:21 CST (21:59:39 ago)
Packets/second: 281 Peak: 2703 @ 2010-01-20 20:15:34 CST
KBits/second : 280 Peak: 10097 @ 2010-01-20 20:15:34 CST
Latency (microseconds): [min: 0] [max: 0] [avg: 0]
Packet Statistics:
[ICMP: 2210497] [TCP: 11918] [UDP: 2419330] [Other: 0]
Flow Statistics:
ICMP: [Current: 1218] [Max: 2278 @ 2010-01-20 21:22:37 CST]
TCP: [Current: 40] [Max: 138 @ 2010-01-20 19:14:02 CST]
UDP: [Current: 16] [Max: 434 @ 2010-01-20 19:15:48 CST]
Other: [Current: 0] [Max: 0 @ 2010-01-19 23:23:21 CST]
Session Statistics:
[ICMP: 609] [TCP: 20] [UDP: 8] [Other: 0]
Policy Name : **juniper-srx-idp-tes**t v0 关键查看此处 IDP 策略是否激活工作状态
Running Detector Version : 10.2.160091104 运行中使用的检测版本

接下我们将介绍 UTM 中的 web-filtering 功能配置

Juniper SRX Branch 系列能够做到的 WEB 过滤内网包括如下：

Table 1: SurfControl Integrated Categories

CATEGORIES			
Adult Sexually Explicit	Advertisements	Arts Entertainment	Chat
Computing Internet	Criminal Skills	Drugs Alcohol Tobacco	Education
Finance Investment	Food Drink	Gambling	Glamour Intimate Apparel
Government Politics	Hacking	Hate Speech	Health Medicine
Hobbies Recreation	Hosting Sites	Job Search Career Development	Kids Sites
Lifestyle Culture	Motor Vehicles	News	Personals Dating
Photo Searches	Real Estate	Reference	Religion
Remote Proxies	Search Engines	Sex Education	Shopping
Sports	Streaming Media	Travel	Usenet News
Violence	Weapons	Web-Based Email	

可以通过 WEB 过滤功能过滤涉及上述信息的网站等,有效提高企业办公效率

列举一个简单的例子,不允许内网用户访问任何与新闻有关的网站， 但是可以访问 news.163.com,并且不允许访问开心网， 其他类型网站可以访问<体育、51JOB 等>

首先我们同样需要检查设备的 license 与特征库等是否最新<根据上述 IDP 操作,不再重复>

第一步：申请 license,此步骤必须保证设备本身能够访问 Internet

Root#run request system license update trial

第二步：查看 license 更新情况

root# run show system license

第三步：配置 UTM- web-filtering 策略和安全策略

```
root# show security utm
custom-objects {
    url-pattern {
        badsite-1 {
            value www.kaixin001.com;
        }
        goodsite-1 {
            value news.163.com;
        }
    }
    custom-url-category {
        bad-site {
            value badsite-1;
        }
        good-site {
            value goodsite-1;
        }
    }
}
feature-profile {
    web-filtering {
        url-whitelist good-site;
        url-blacklist bad-site;
```

```
            type surf-control-integrated;
            surf-control-integrated {
                profile block-selected-sites {
                    category {
                        News {
                            action block;
                        }
                    }
                    default log-and-permit;
                    custom-block-message "The site requested is not a work-related site! Go back to
work! If you have questions, Please contact technical, support This is the Juniper solution!";
                }
            }
        }
}
utm-policy web_filtering {
        web-filtering {
            http-profile block-selected-sites;
        }
}

[edit]
root# show security policies from-zone trust to-zone untrust policy t-u
match {
        source-address any;
        destination-address any;
        application any;
}
then {
        permit {
            application-services {
                utm-policy web_filtering;针对此条策略开启 WEB_Fitering

[edit]
第四步：查看 WEB-过滤功能工作状态命令：
root# run show security utm web-filtering ?
Possible completions:
  statistics           Show web-filtering statistics
  status               Show web-filtering status
[edit]
root# run show security utm web-filtering
```

2.9 SRX Branch 系列与 UAC 联动配置说明

JUNIPER SRX Branch 系列防火墙可以与 Juniper 统一接入控制器 UAC 进行 3 层访问控制联动工作,下面将具体介绍 UAC、SRX 配置,主要通过截图来进行说明:

主要事项:

1、 SRX 与 UAC 设备系统时间必须一致

2、 SRX 设备与 UAC 设备证书必须来自同一个根证书颁发

3、 SRX 与 UAC 之间通过 SSL 连接<如果通过防火墙或者 ACL 等控制>必须将其 443 端口放开

第一步:生成并获取 UAC 设备证书,并导入设备证书和根服务器证书<由于此操作需要通过第三方证书服务器来完成>为此我单独有 WORD 文档来介绍。

第二步:生成并获取 SRX 设备证书,具体步骤如下:

user@host> request security pki generate-key-pair certificate-id uac 手工生成 **certificate-id**

user@host> request security pki generate-certificate-request certificate-id uac domain-name juniper.net subject CN=abc 手工生成证书信息

The following certificate request is displayed in PEM format.

Generated certificate request

-----BEGIN CERTIFICATE REQUEST-----

MIHxMIGcAgEAMA4xDDAKBgNVBAMTA2htMTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgC

QQCbhaiWzmctH0ZDldCn+mSNM62kyiSgc4cmN68U/j9El09/DgGoMNy2y+RYA1xU

sr4B0NedGrZZJx5L1sIYjHr/AgMBAAGgKTAnBgkqhkiG9w0BCQ4xGjAYMBYGA1Ud

EQQPMA2CC2p1bmlwZXIubmV0MA0GCSqGSIb3DQEBBQUAA0EAleLR6Hp2ity8Dugs

MW4HI6SxfwMc2eYM5Nj2UhwpEEpsce77dUBZriKdehAgli7vwNsHGIuhHjEaFzfO

hpM3tA==

-----END CERTIFICATE REQUEST----- 通过 windows 证书服务器或者 OPENSSL 生成并获取证书

Fingerprint:

9e:d5:7d:44:e8:e7:b6:d7:4b:58:d4:4e:2b:fb:c6:b2:4b:b7:8b:82 (sha1)

b0:8d:c7:6d:41:d5:58:61:dc:a0:3e:4e:d6:39:02:d7 (md5)

user@host> request security pki local-certificate load certificate-id uac filename /var/tmp/device.cer 手工加载证书到设备

此证书是通过证书服务器生成后由 FTP 等方式传入到设备中。

lab# run show security pki local-certificate detail 查看当前证书信息

Certificate identifier: uac

Certificate version: 3

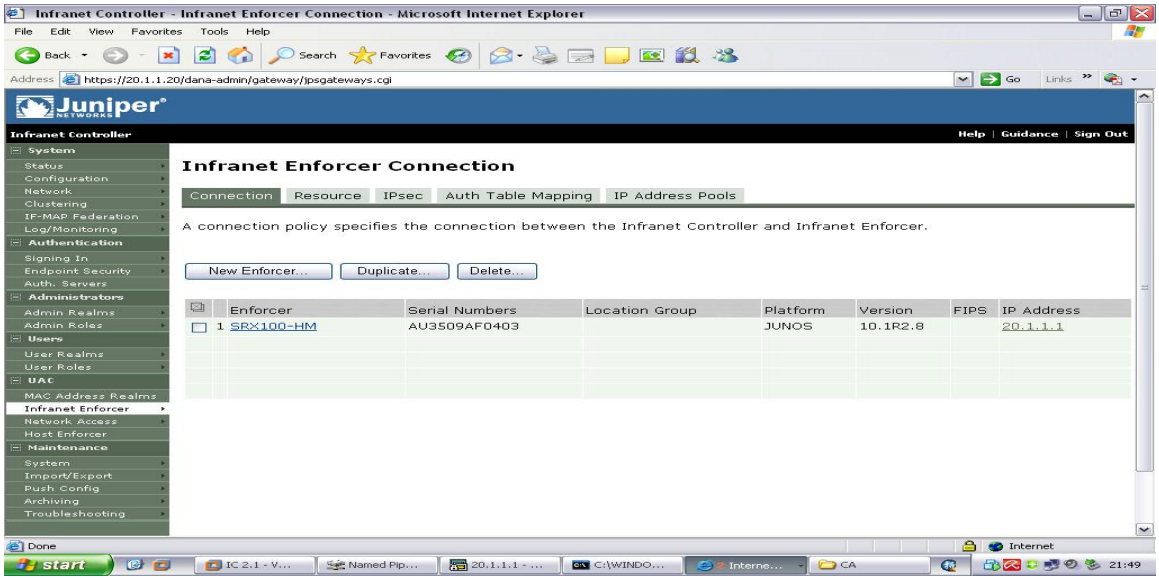
Serial number: 61069676000000000006

Issuer:

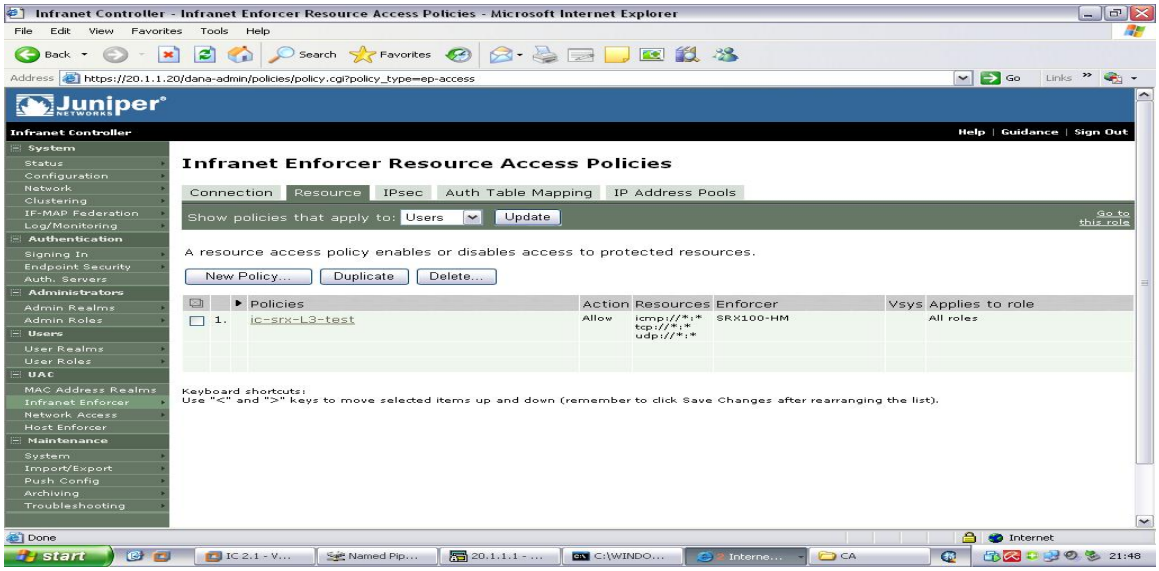
Common name: srx *** 部分显示信息省略***\\\\

第三步:配置 UAC 设备 Infranet enforcer connection,根据截图配置步骤如下:

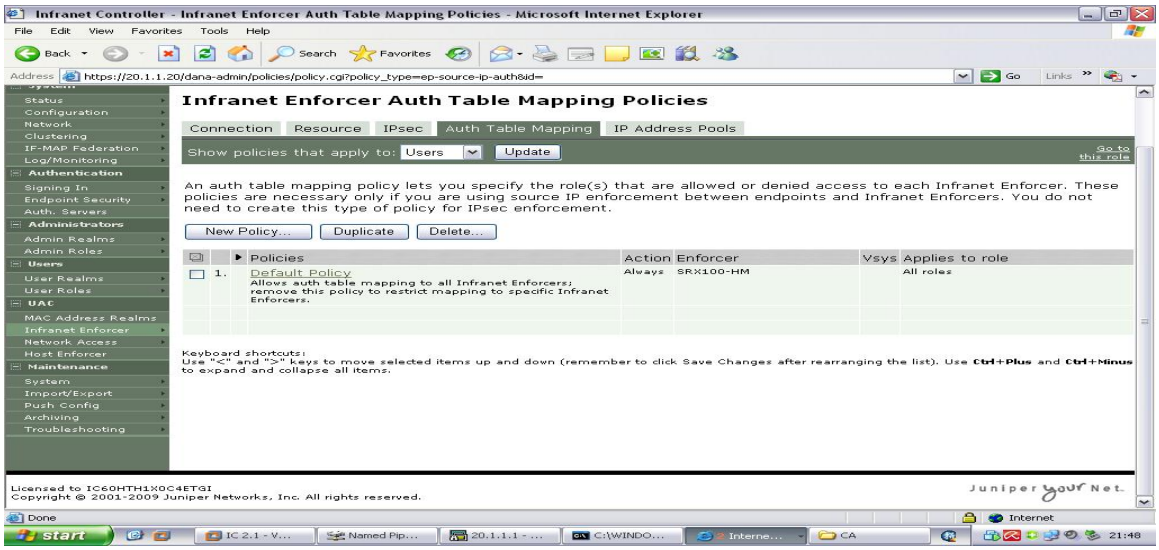
定义 Infranet enforcer connection 连接参数<设备序列号、共享密钥等>



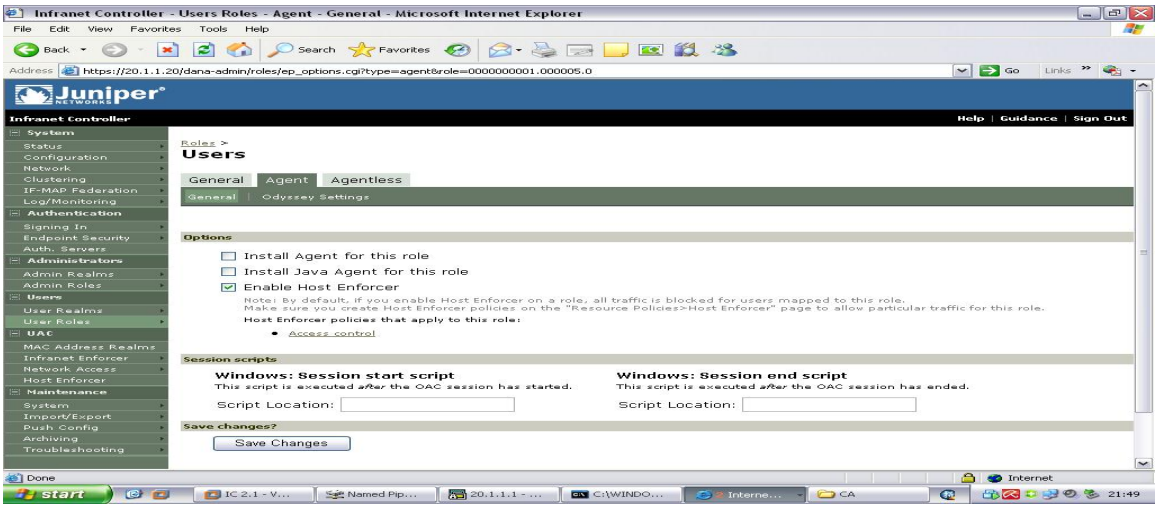
定义 Resource 内部资源



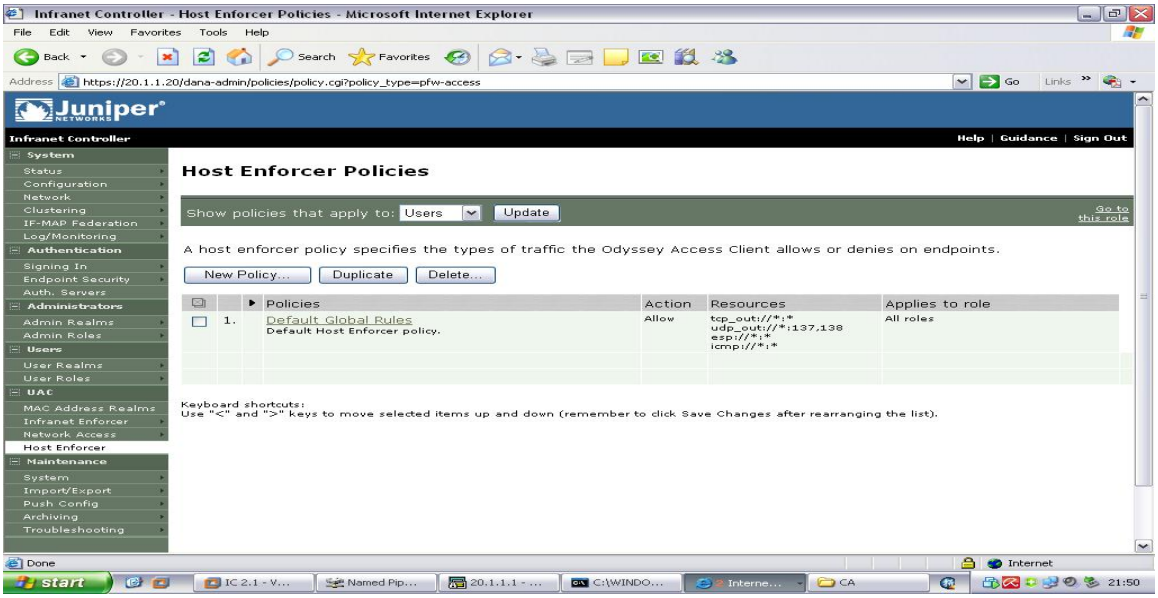
定义认证列表匹配到的 enforcer



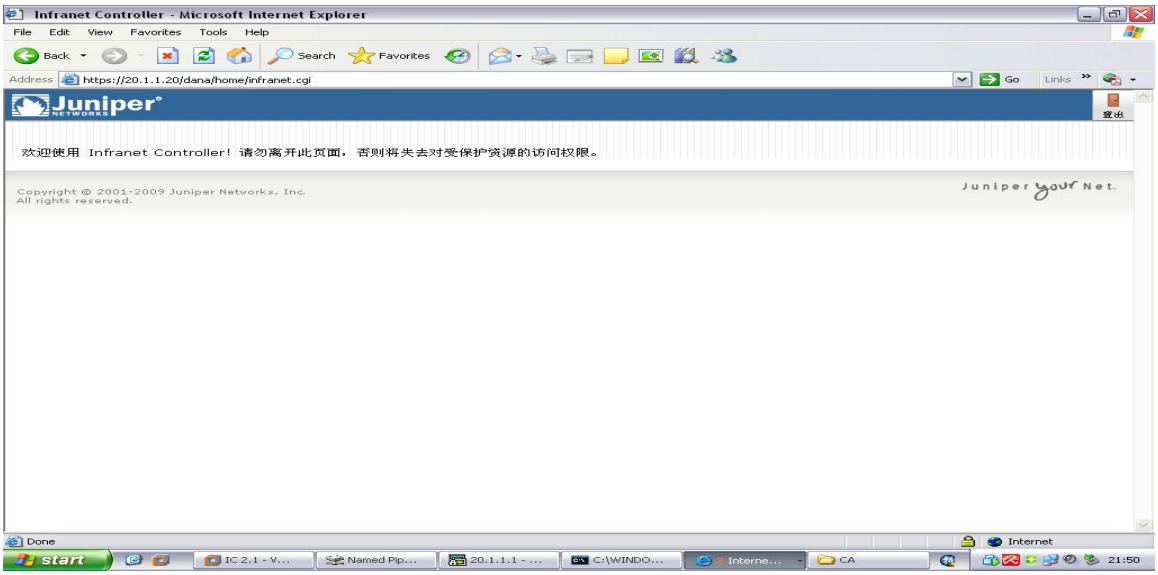
定义 roles〈注意 enable host enforcer 选项〉



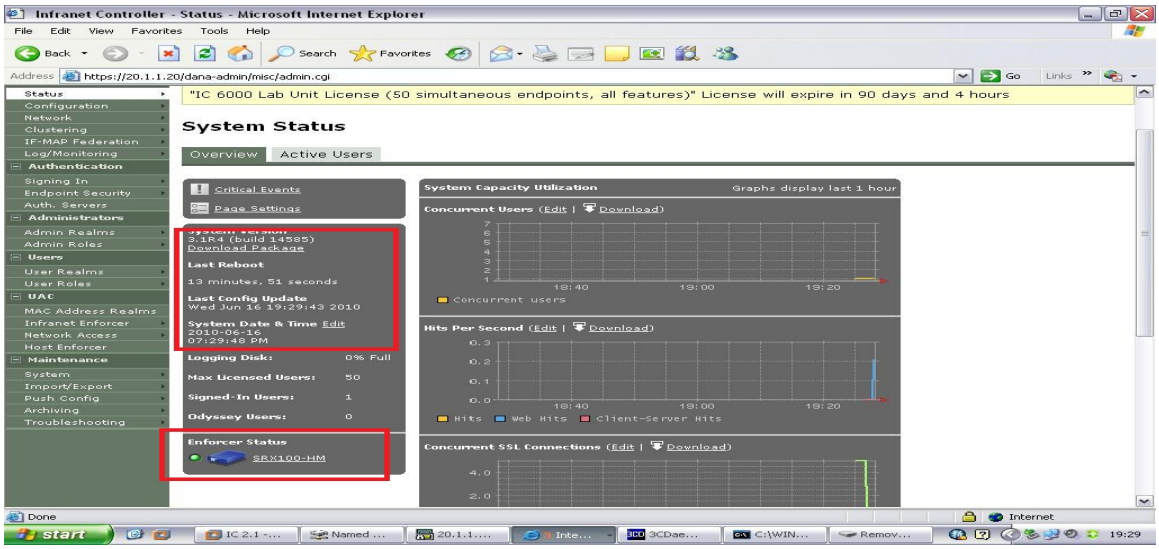
定义 Host enforcer policys



客户端尝试登陆,输入用户名和密码<UAC 本地系统或者远程认证服务器提供>



联动正常,UAC 首页显示如下：



第四步：配置 SRX 设备 unified-access-control,具体内容如下：

```
lab# show services
unified-access-control {
    infranet-controller ic-1 {
        address 20.1.1.20; UAC 设备 IP 地址
        interface fe-0/0/1.0; 与 UAC 设备进行通信的端口
        password "$9$hBVSKMLxNbYgXxHqP5F3KMW8dbZUj"; ## SECRET-DATA 与 UAC 设备联动的共享密钥
    }
```

第五步：SRX 设备针对需要进行与 UAC 设备联动的策略开启 UAC 认证策略功能：

set security policies from-zone trust to-zone untrust policy t-u then permit application-services uac-policy

第六步：查看 SRX 设备 unified-access-control 状态,具体内容如下：

```
lab# run show services unified-access-control authentication-table      用户认证表
Id     Source IP       Username      Age       Role identifier
2      20.1.1.100      test2         0         0000000001.000005.0
Total: 1
[edit]
lab# run show services unified-access-control policies detail          UAC 下发到设备的策略
Identifier: 1
  Resource: icmp://*:*
  Resource: tcp://*:*
  Resource: udp://*:*
  Action: allow
  Apply: all
Total: 1
[edit]
lab# run show services unified-access-control status                   SRX 设备与 UAC 设备连接的状态
Host            Address          Port    Interface      State
ic-1            20.1.1.20        11123   fe-0/0/1.0     connected
```

2.10 SRX Branch 系列 FLOW 配置说明

root# set security flow ?
Possible completions:
> aging Aging configuration
allow-dns-reply Allow unmatched incoming DNS reply packet
+ apply-groups Groups from which to inherit configuration data
+ apply-groups-except Don't inherit configuration data from these groups
route-change-timeout Timeout value for route change to nonexistent route (6..1800 seconds)
syn-flood-protection-mode TCP SYN flood protection mode
> tcp-mss TCP maximum segment size configuration
> tcp-session Transmission Control Protocol session configuration
> traceoptions Trace options for flow services
[edit]
root# set security flow syn-flood-protection-mode ? 设置 SYN-FLOOD 攻击防护
Possible completions:
syn-cookie Enable SYN cookie protection
syn-proxy Enable SYN proxy protection
[edit]
root# set security flow tcp-session ? 设置 tcp-session 相关参数
Possible completions:
+ apply-groups Groups from which to inherit configuration data
+ apply-groups-except Don't inherit configuration data from these groups
no-sequence-check Disable sequence-number checking
no-syn-check Disable creation-time SYN-flag check
no-syn-check-in-tunnel Disable creation-time SYN-flag check for tunnel packets
rst-invalidate-session Immediately end session on receipt of reset (RST) segment
rst-sequence-check Check sequence number in reset (RST) segment
strict-syn-check Enable strict syn check
tcp-initial-timeout Timeout for TCP session when initialization fails (20..300 seconds)
[edit]
root# set security flow tcp-mss ? 设置 TCP-MSS 相关参数
Possible completions:
> all-tcp Enable MSS override for all packets
+ apply-groups Groups from which to inherit configuration data
+ apply-groups-except Don't inherit configuration data from these groups
> gre-in Enable MSS override for all GRE packets coming out of an IPSec tunnel
> gre-out Enable MSS override for all GRE packets entering an IPsec tunnel
> ipsec-vpn Enable MSS override for all packets entering IPSec tunnel
[edit]

2.11 SRX Branch 系列 SCREEN 攻击防护配置说明

Juniper SRX 系列 防火墙用于保护网络的安全，具体做法是先检查要求从一个安全区段到另一区段的通路的所有连接尝试，然后予以允许或拒绝。对于每个安全区段和 MGT 区段，可启用一组预定义的 SCREEN 选项，检测并阻塞安全设备将其确定为具有潜在危害的各种信息流。

SCREEN 选项用于保护区段的安全，具体做法是先检查要求经过绑定到该区域的某一接口的所有连接尝试，然后予以准许或拒绝。然后安全设备应用防火墙策略，在这些策略中，可能包含针对通过 SCREEN 过滤器的信息流的内容过滤和入侵检测及防护（IDP）组件。

下面我们将举例配置一个 SCREEN 应用在外网 Untrust 区域：

具体配置命令如下：

```
root# show security screen
ids-option juniper-srx-screen-test {
    alarm-without-drop; 此动作表示仅记录攻击信息到日志，但是不拒绝攻击<可选设置>
    icmp {
        ip-sweep threshold 1000;
        fragment;
        flood threshold 100;
    }
    ip {
        bad-option;
        spoofing;
        tear-drop;
    }
    tcp {
        syn-frag;
        port-scan threshold 1000;端口扫描触发值为 1000<每秒 1000 个扫描动作>
        land;
        winnuke;
    }
    udp {
        flood threshold 100; UDP FLOOD 触发值为 100<每秒 100 个>
    }
    limit-session {
        source-ip-based 128;会话数限制<针对源 IP 地址>
        destination-ip-based 128;会话数限制<针对目标 IP 地址>
    }
}

[edit]
root# show security zones security-zone untrust
screen juniper-srx-screen-test; 将上述定义的 screen 配置应用到 untrust 区域
```

2.12 SRX Branch 系列 J-WEB 操作配置简要说明

Juniper SRX 系列防火墙提供 WEB 操作界面,WEB 操作界面主要包括如下几个大类：

1、 首页<监控实时系统状态>

2、 配置页面<防火墙功能配置，比如策略、VPN、NAT、路由等>

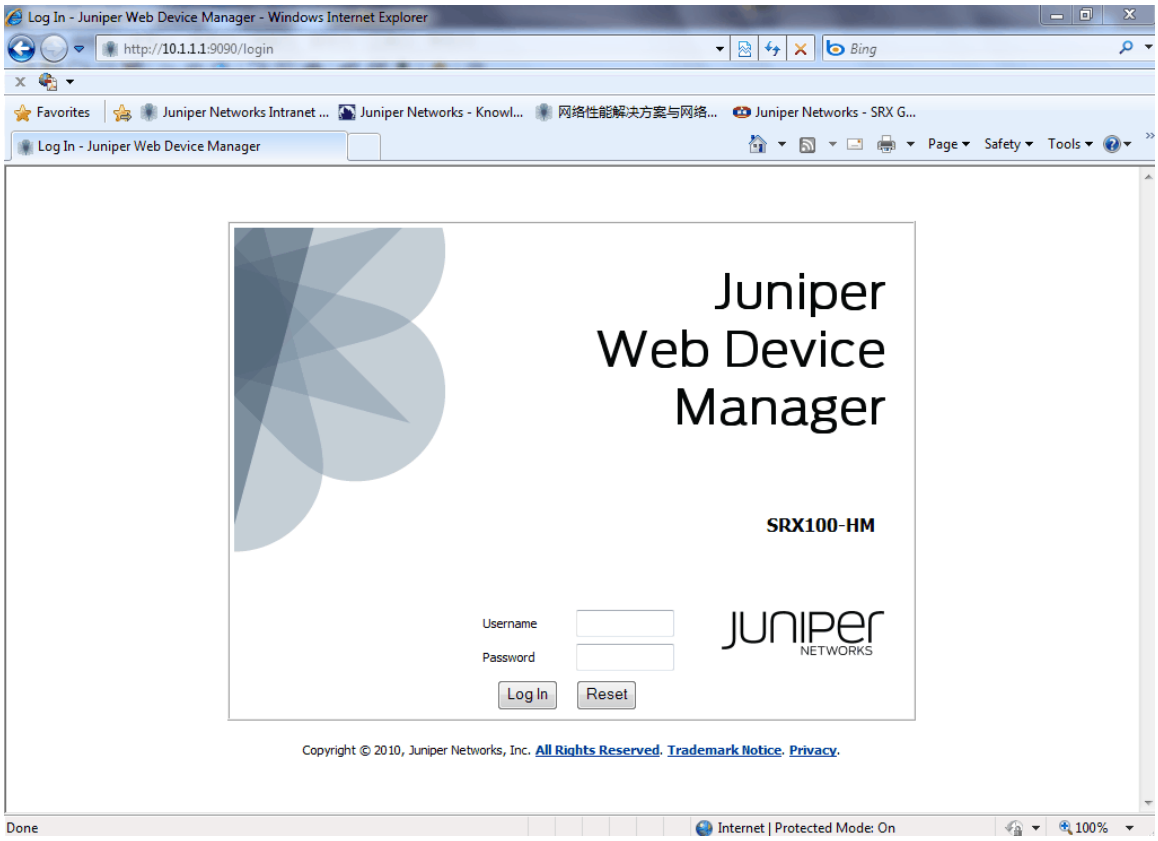
3、 监控页面<防火墙各项功能状态监控、接口流量监控等>

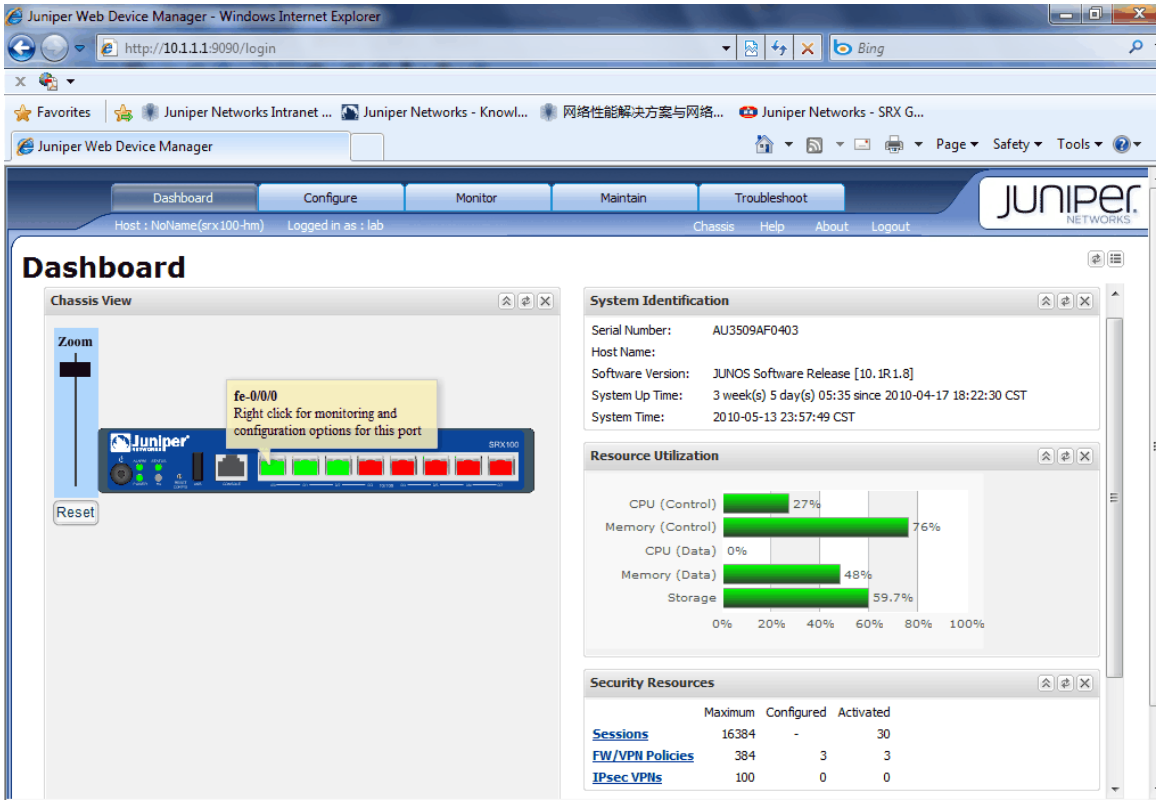
4、 系统维护页面<防火墙日常维护，比如升级等>

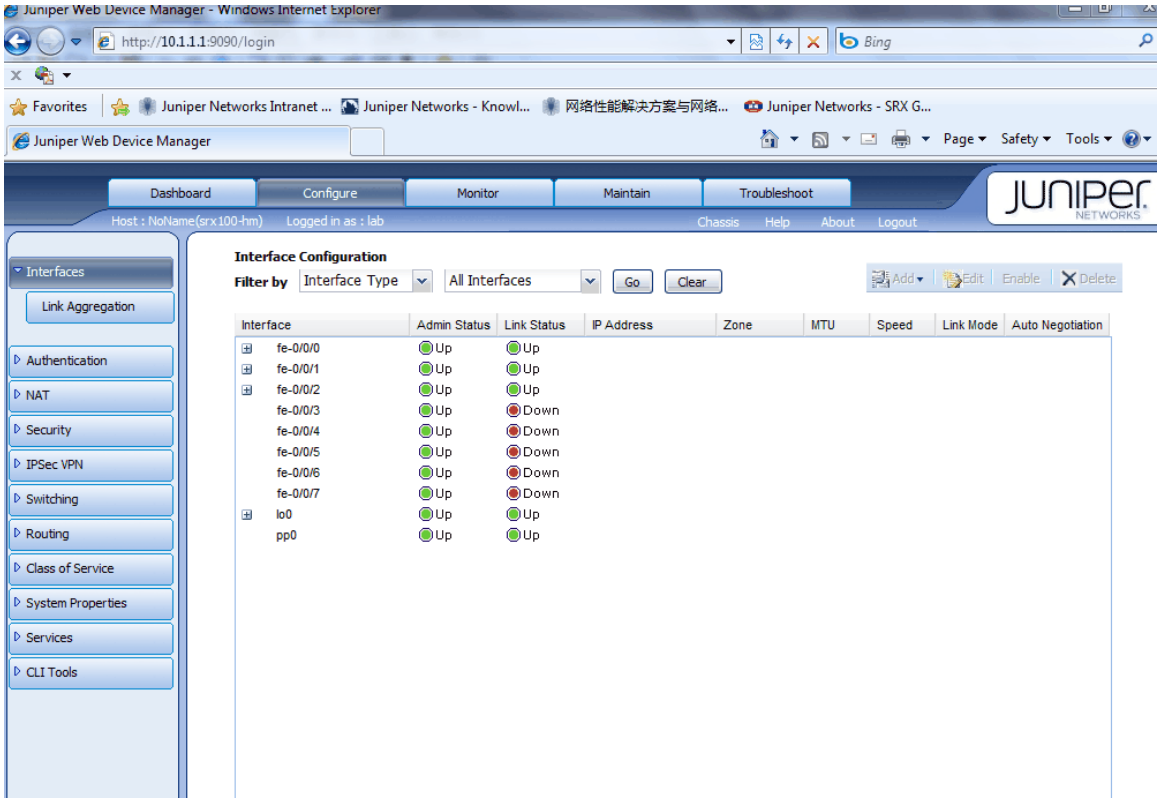
5、 系统故障排查页面<防火墙日常维护故障排查，比如抓包、PING、tracert route 等>

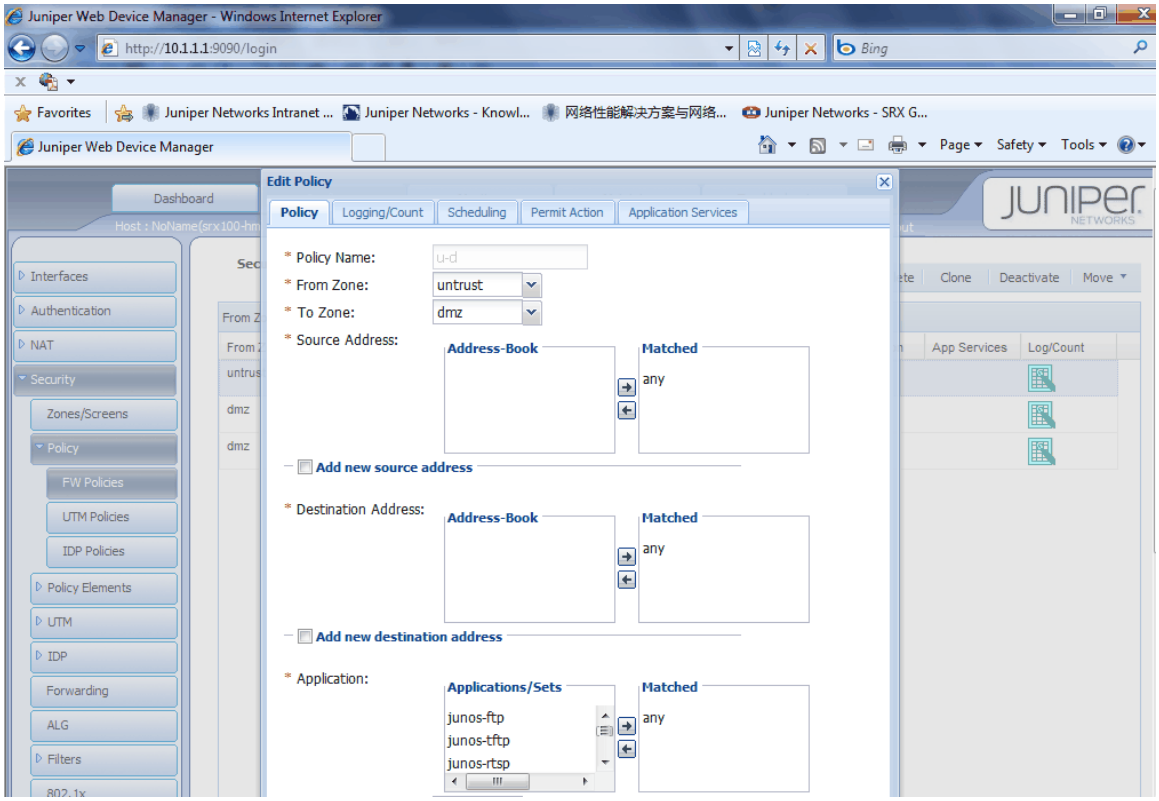
功能分类页面截图如下：

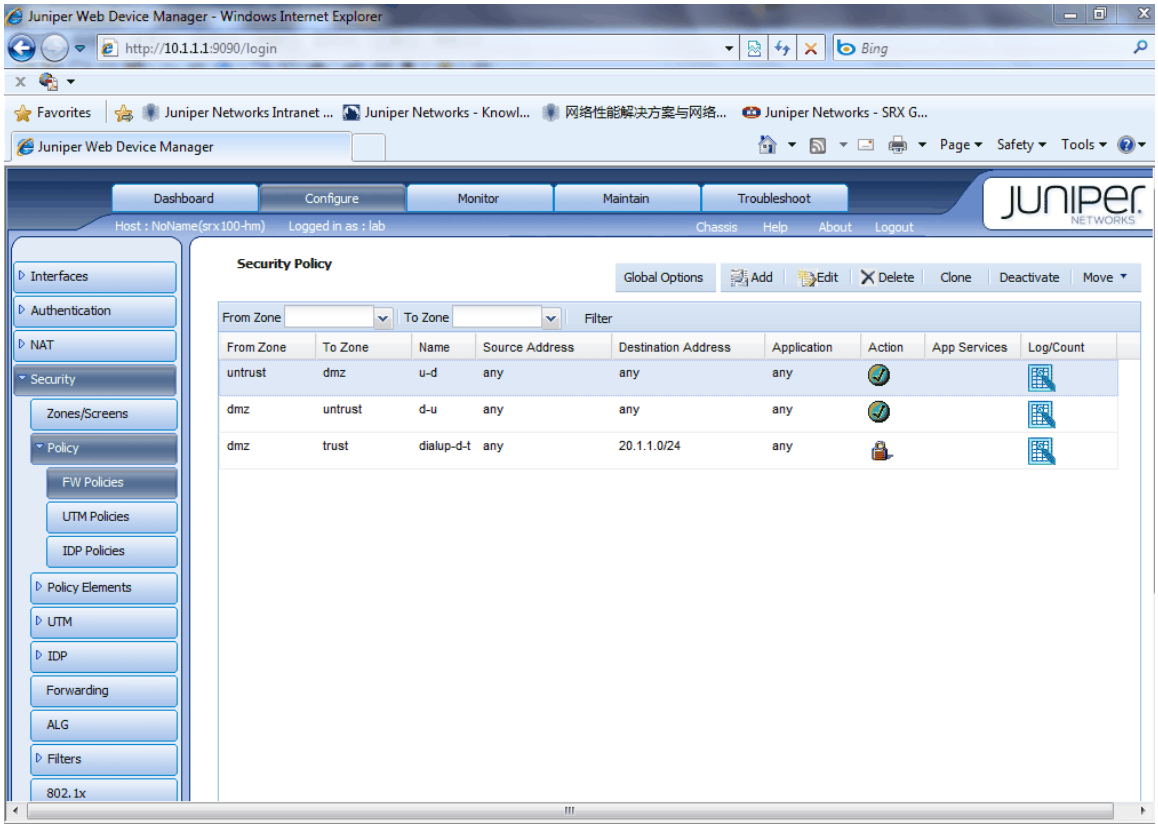
登录页面

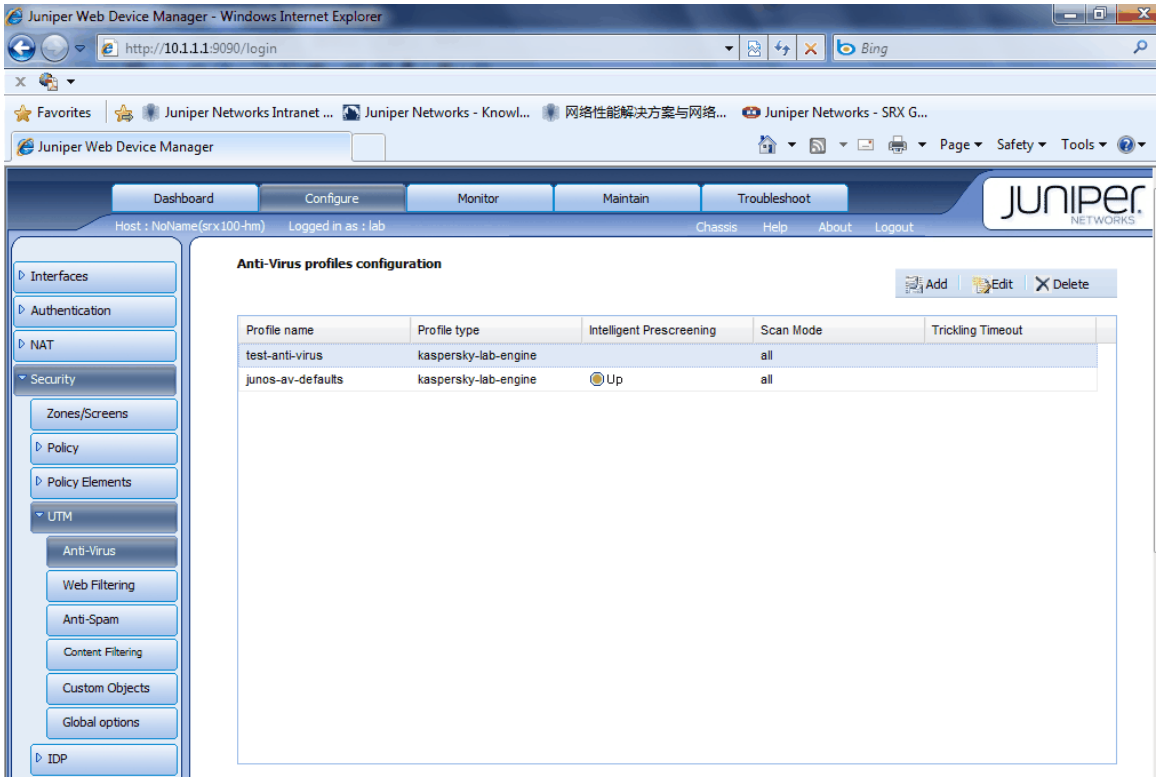


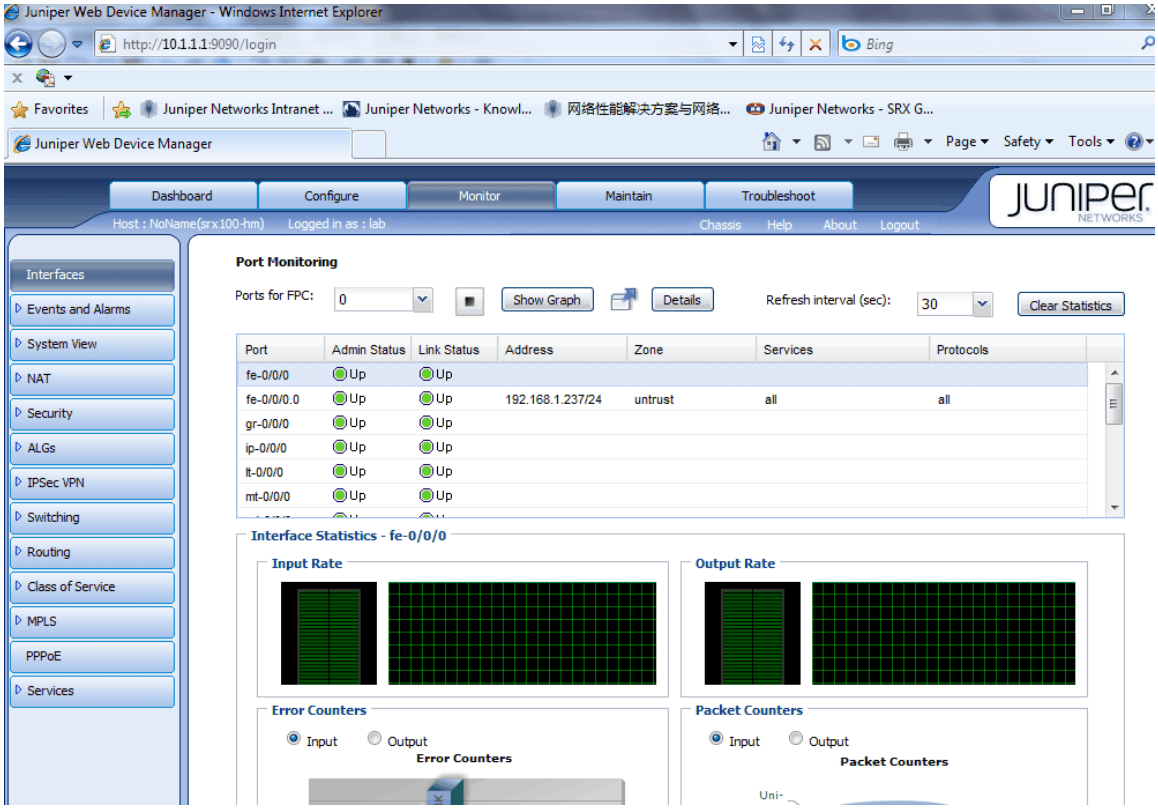

Juniper Web Device Manager - Windows Internet Explorer
http://10.1.1.1:9090/login
Juniper Web Device Manager
Dashboard
Configure
Monitor
Maintain
Troubleshoot
Host : NoName(srx100-hm)
Logged in as : lab
Chassis
Help
About
Logout
Dashboard
Chassis View
Zoom
Reset
fe-0/0/0
Right click for monitoring and configuration options for this port
System Identification
Serial Number: AU3509AF0403
Host Name:
Software Version: JUNOS Software Release [10.1R1.8]
System Up Time: 3 week(s) 5 day(s) 05:35 since 2010-04-17 18:22:30 CST
System Time: 2010-05-13 23:57:49 CST
Resource Utilization
CPU (Control) 27%
Memory (Control) 76%
CPU (Data) 0%
Memory (Data) 48%
Storage 59.7%
0% 20% 40% 60% 80% 100%
Security Resources
Maximum Configured Activated
Sessions 16384 - 30
FW/VPN Policies 384 3 3
IPsec VPNs 100 0 0

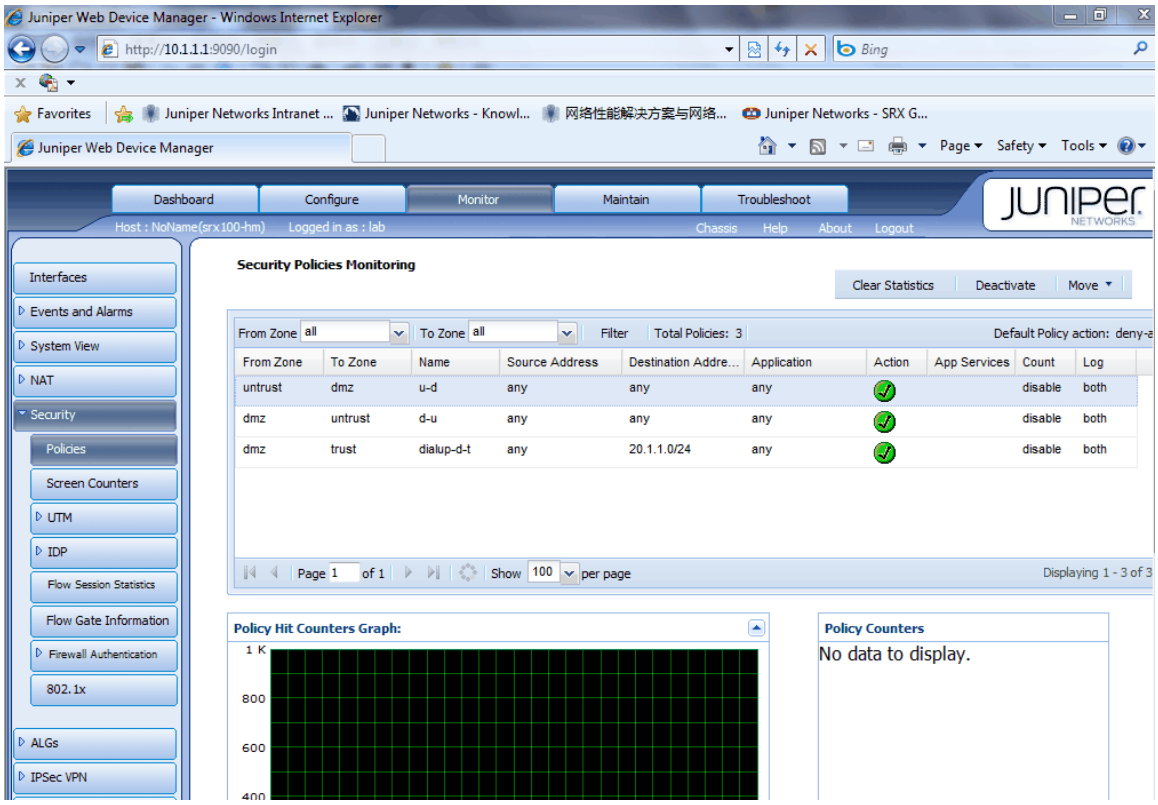

Juniper Web Device Manager - Windows Internet Explorer
http://10.1.1.1:9090/login
Juniper Web Device Manager
Dashboard
Configure
Monitor
Maintain
Troubleshoot
Host : NoName(srx100-hm)
Logged in as : lab
Chassis
Help
About
Logout
Interfaces
Link Aggregation
Authentication
NAT
Security
IPSec VPN
Switching
Routing
Class of Service
System Properties
Services
CLI Tools
Interface Configuration
Filter by Interface Type All Interfaces Go Clear
Add Edit Enable Delete
Interface Admin Status Link Status IP Address Zone MTU Speed Link Mode Auto Negotiation
fe-0/0/0 Up Up
fe-0/0/1 Up Up
fe-0/0/2 Up Up
fe-0/0/3 Up Down
fe-0/0/4 Up Down
fe-0/0/5 Up Down
fe-0/0/6 Up Down
fe-0/0/7 Up Down
lo0 Up Up
pp0 Up Up

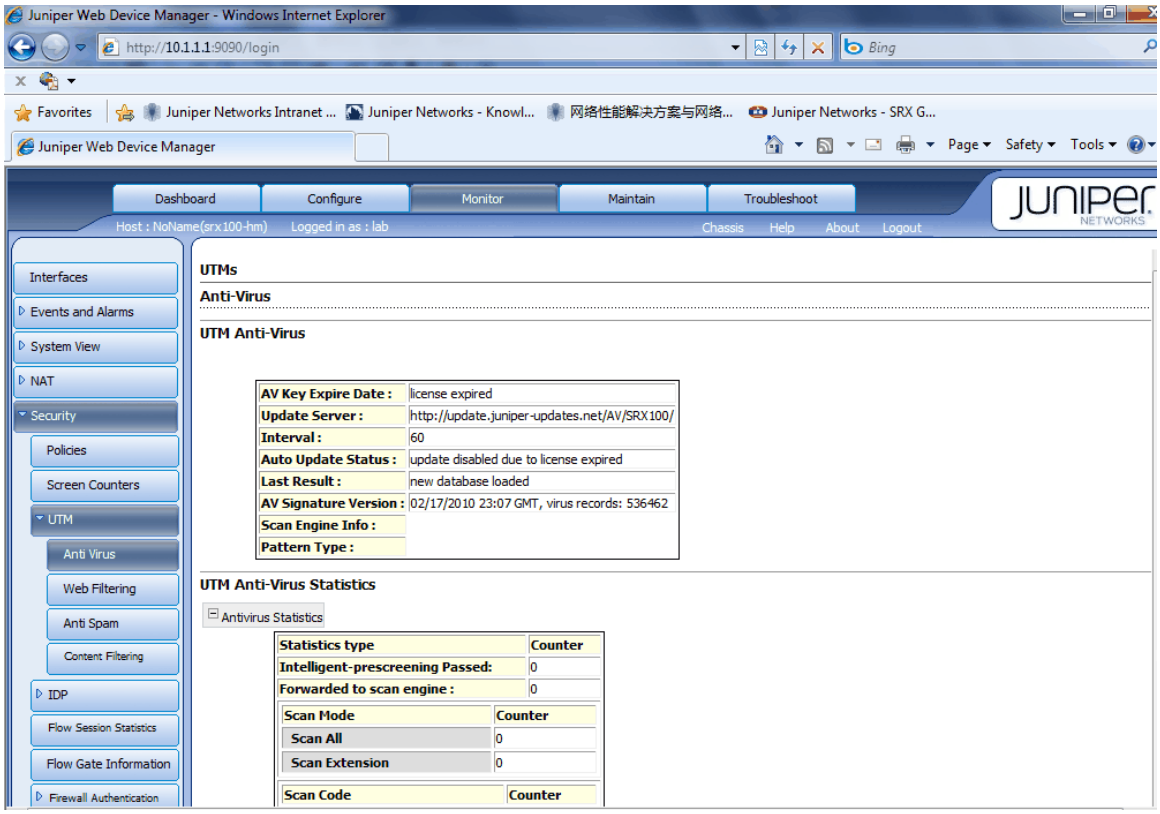

Juniper Web Device Manager - Windows Internet Explorer
http://10.1.1.1:9090/login
Juniper Web Device Manager
Edit Policy
Policy
Logging/Count
Scheduling
Permit Action
Application Services
Policy Name:
From Zone:
untrust
To Zone:
dmz
Source Address:
Address-Book
Matched
any
Add new source address
Destination Address:
Address-Book
Matched
any
Add new destination address
Application:
Applications/Sets
Matched
any
junos-ftp
junos-tftp
junos-rtsp
Dashboard
Interfaces
Authentication
NAT
Security
Zones/Screens
Policy
FW Policies
UTM Policies
IDP Policies
Policy Elements
UTM
IDP
Forwarding
ALG
Filters
802.1x
Clone
Deactivate
Move
App Services
Log/Count

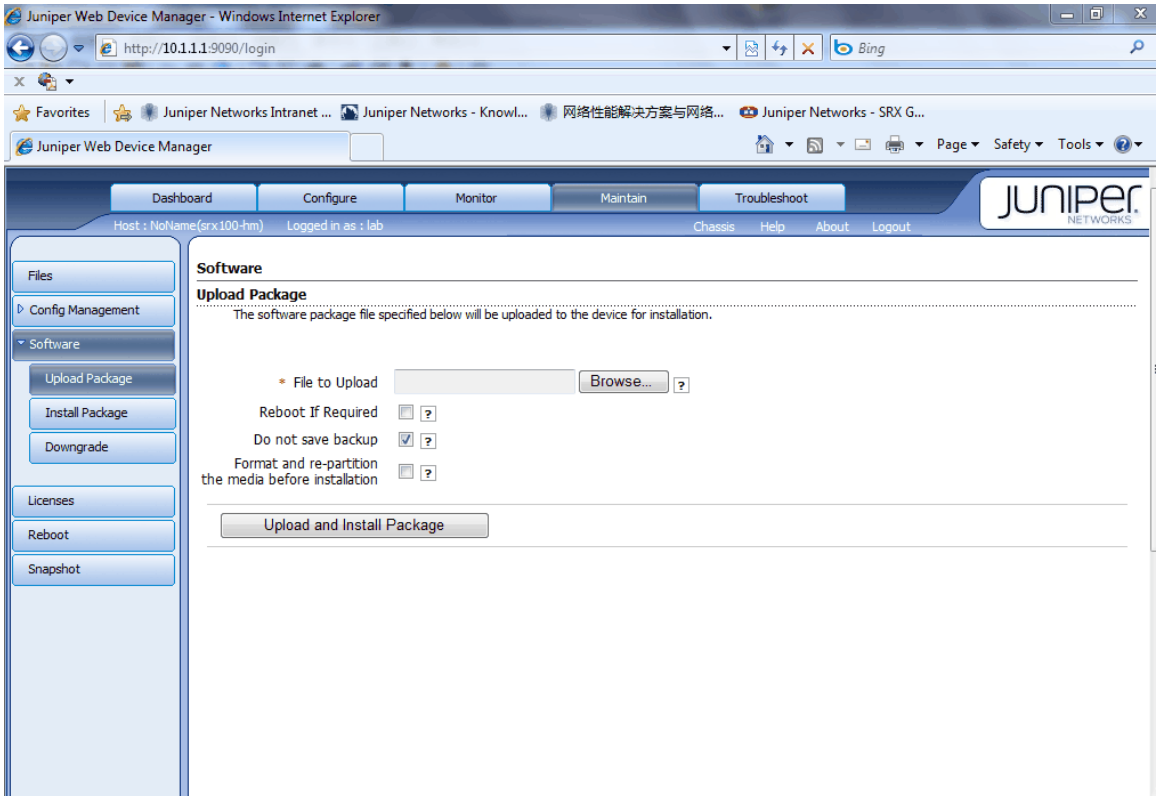

Juniper Web Device Manager - Windows Internet Explorer
http://10.1.1.1:9090/login
Juniper Web Device Manager
Dashboard
Configure
Monitor
Maintain
Troubleshoot
Host : NoName(srx100-hm)
Logged in as : lab
Chassis
Help
About
Logout
Security Policy
Global Options
Add
Edit
Delete
Clone
Deactivate
Move
From Zone
To Zone
Filter
From Zone
To Zone
Name
Source Address
Destination Address
Application
Action
App Services
Log/Count
untrust
dmz
u-d
any
any
any
dmz
untrust
d-u
any
any
any
dmz
trust
dialup-d-t
any
20.1.1.0/24
any
Interfaces
Authentication
NAT
Security
Zones/Screens
Policy
FW Policies
UTM Policies
IDP Policies
Policy Elements
UTM
IDP
Forwarding
ALG
Filters
802.1x

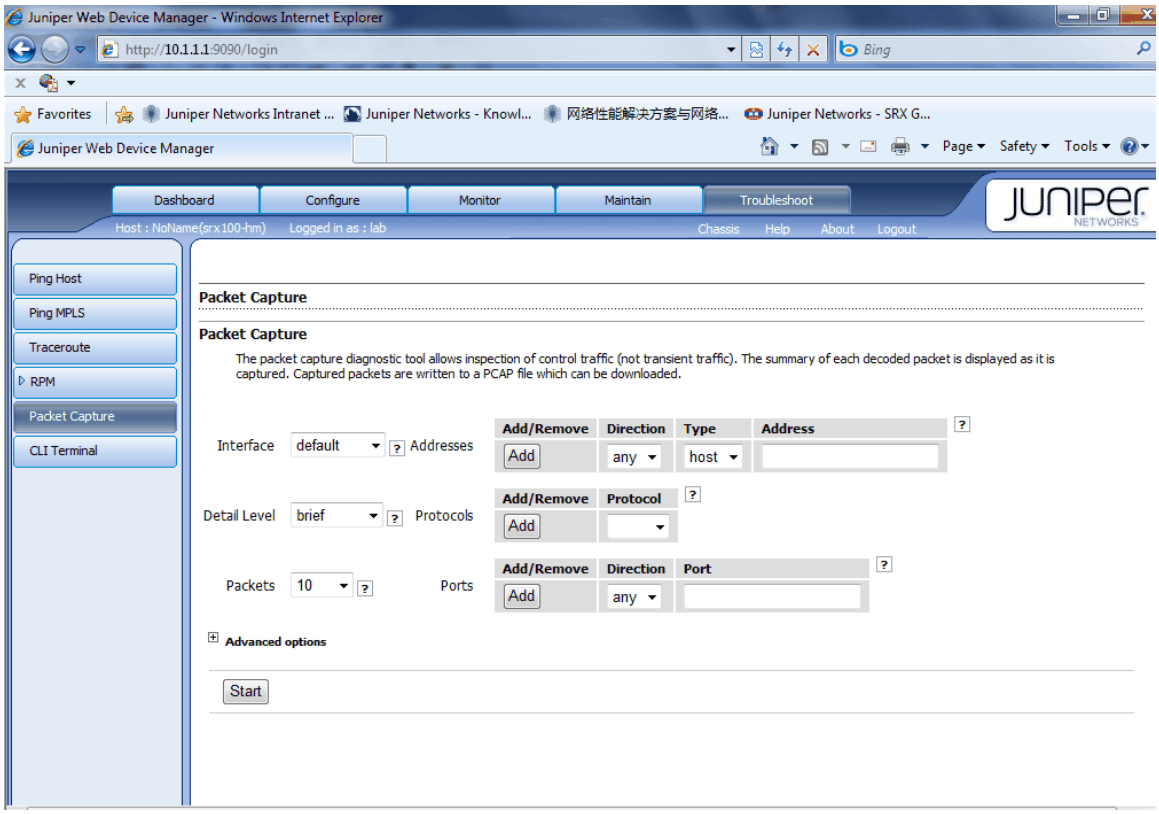

Juniper Web Device Manager - Windows Internet Explorer
http://10.1.1.1:9090/login
Juniper Web Device Manager
Dashboard
Configure
Monitor
Maintain
Troubleshoot
Host : NoName(srx100-hm)
Logged in as : lab
Chassis
Help
About
Logout
Interfaces
Authentication
NAT
Security
Zones/Screens
Policy
Policy Elements
UTM
Anti-Virus
Web Filtering
Anti-Spam
Content Filtering
Custom Objects
Global options
IDP
Anti-Virus profiles configuration
Add
Edit
Delete
Profile name
Profile type
Intelligent Prescreening
Scan Mode
Trickling Timeout
test-anti-virus
kaspersky-lab-engine
all
junos-av-defaults
kaspersky-lab-engine
Up
all


Juniper Web Device Manager - Windows Internet Explorer
http://10.1.1.1:9090/login
Juniper Web Device Manager
Dashboard
Configure
Monitor
Maintain
Troubleshoot
Host : NoName(srx100-hm)
Logged in as : lab
Chassis
Help
About
Logout
Interfaces
Events and Alarms
System View
NAT
Security
ALGs
IPSec VPN
Switching
Routing
Class of Service
MPLS
PPPoE
Services
Port Monitoring
Ports for FPC:
Show Graph
Details
Refresh interval (sec):
Clear Statistics
Port
Admin Status
Link Status
Address
Zone
Services
Protocols
fe-0/0/0
fe-0/0/0.0
192.168.1.237/24
untrust
gr-0/0/0
ip-0/0/0
lt-0/0/0
mt-0/0/0
Interface Statistics - fe-0/0/0
Input Rate
Output Rate
Error Counters
Input
Output
Packet Counters


Juniper Web Device Manager - Windows Internet Explorer
http://10.1.1.1:9090/login
Juniper Web Device Manager
Dashboard
Configure
Monitor
Maintain
Troubleshoot
Host : NoName(srx100-hm)
Logged in as : lab
Chassis
Help
About
Logout
Interfaces
Events and Alarms
System View
NAT
Security
Policies
Screen Counters
UTM
IDP
Flow Session Statistics
Flow Gate Information
Firewall Authentication
802.1x
ALGs
IPSec VPN
Security Policies Monitoring
Clear Statistics
Deactivate
Move
From Zone all
To Zone all
Filter
Total Policies: 3
Default Policy action: deny-a
From Zone | To Zone | Name | Source Address | Destination Addre... | Application | Action | App Services | Count | Log
untrust | dmz | u-d | any | any | any | disable | both
dmz | untrust | d-u | any | any | any | disable | both
dmz | trust | dialup-d-t | any | 20.1.1.0/24 | any | disable | both
Page 1 of 1
Show 100 per page
Displaying 1 - 3 of 3
Policy Hit Counters Graph:
1 K
800
600
400
Policy Counters
No data to display.


Juniper Web Device Manager - Windows Internet Explorer
http://10.1.1.1:9090/login
Juniper Web Device Manager
Dashboard
Configure
Monitor
Maintain
Troubleshoot
Host : NoName(srx100-hm)
Logged in as : lab
Chassis
Help
About
Logout
Interfaces
Events and Alarms
System View
NAT
Security
Policies
Screen Counters
UTM
Anti Virus
Web Filtering
Anti Spam
Content Filtering
IDP
Flow Session Statistics
Flow Gate Information
Firewall Authentication
UTMs
Anti-Virus
UTM Anti-Virus
AV Key Expire Date : license expired
Update Server : http://update.juniper-updates.net/AV/SRX100/
Interval : 60
Auto Update Status : update disabled due to license expired
Last Result : new database loaded
AV Signature Version : 02/17/2010 23:07 GMT, virus records: 536462
Scan Engine Info :
Pattern Type :
UTM Anti-Virus Statistics
Antivirus Statistics
Statistics type | Counter
Intelligent-prescreening Passed: 0
Forwarded to scan engine : 0
Scan Mode | Counter
Scan All 0
Scan Extension 0
Scan Code | Counter


Juniper Web Device Manager - Windows Internet Explorer
http://10.1.1.1:9090/login
Juniper Web Device Manager
Dashboard
Configure
Monitor
Maintain
Troubleshoot
Host : NoName(srx100-hm)
Logged in as : lab
Chassis
Help
About
Logout
Files
Config Management
Software
Upload Package
Install Package
Downgrade
Licenses
Reboot
Snapshot
Software
Upload Package
The software package file specified below will be uploaded to the device for installation.
* File to Upload
Browse...
Reboot If Required
Do not save backup
Format and re-partition the media before installation
Upload and Install Package


Juniper Web Device Manager - Windows Internet Explorer
http://10.1.1.1:9090/login
Juniper Web Device Manager
Dashboard
Configure
Monitor
Maintain
Troubleshoot
Host : NoName(srx100-hm)
Logged in as : lab
Chassis
Help
About
Logout
Ping Host
Ping MPLS
Traceroute
RPM
Packet Capture
CLI Terminal
Packet Capture
Packet Capture
The packet capture diagnostic tool allows inspection of control traffic (not transient traffic). The summary of each decoded packet is displayed as it is captured. Captured packets are written to a PCAP file which can be downloaded.
Interface
default
Addresses
Add/Remove
Direction
Type
Address
Add
any
host
Detail Level
brief
Protocols
Add/Remove
Protocol
Add
Packets
10
Ports
Add/Remove
Direction
Port
Add
any
Advanced options
Start

三、SRX 防火墙常规操作与维护

3.2 设备关机

SRX 因为主控板上有大容量存储，为防止强行断电关机造成硬件故障，要求设备关机必须按照下面的步骤进行操作：

1. 管理终端连接 SRX console 口。
2. 使用具有足够权限的用户名和密码登陆 CLI 命令行界面。
3. 在提示符下输入下面的命令：

   ```
   user@host> request system halt
   ...
   The operating system has halted.
   Please press any key to reboot
   ```

   (除非需要重启设备，此时不要敲任何键，否则设备将进行重启)
4. 等待 console 输出上面提示信息后，确认操作系统已停止运行，关闭机箱背后电源模块电源。

3.3 设备重启

SRX 重启必须按照下面的步骤进行操作：

1. 管理终端连接 SRX console 口。
2. 使用具有足够权限的用户名和密码登陆 CLI 命令行界面。
3. 在提示符下输入下面的命令：

   ```
   user@host> request system reboot
   ```
4. 等待 console 设备的输出，操作系统已经重新启动。

3.4 操作系统升级

SRX 操作系统软件升级必须按照下面的步骤进行操作：

1. 管理终端连接 SRX console 口，便于升级过程中查看设备重启和软件加载状态。
2. SRX 上开启 FTP 服务，并使用具有超级用户权限的非 root 用户通过 FTP 客户端将下载的升级软件介质上传到 SRX 上。
3. 升级前，执行下面的命令备份旧的软件及设定：

   ```
   user@host> request system snapshot
   ```
4. 加载新的 SRX 软件：

```
user@host> request system software add validate filename.tgz
reboot
```

5. 软件加载成功后， SRX 将自动重启，重启完成后检查系统当前软件版本号：

```
user@host> show system software
```

3.5 密码恢复

SRX Root 密码丢失，并且没有其他的超级用户权限，那么就需要执行密码恢复，该操作需要中断设备正常运行，但不会丢失配置信息，这点与 ScreenOS 存在区别。

要进行密码恢复，请按照下面操作进行：

1. Console 口连接 SRX，然后重启 SRX。
2. 在启动过程中，console 上出现下面的提示的时候，按**空格键**中断正常启动方式，然后再进入单用户状态，并输入：**boot -s**

```
Loading /boot/defaults/loader.conf
/kernel data=… … syms=[… …]
Hit [Enter] to boot immediately, or space bar for command prompt.
loader>
loader> boot -s
```

3. 执行密码恢复：在以下提示文字后输入 **recovery，**设备将自动进行重启

```
Enter full pathname of shell or 'recovery' for root password
recovery or RETURN for /bin/sh: recovery
```

4. 进入配置模式，删除 root 密码，并重现设置 root 密码：

```
user@host> configure
Entering configuration mode
user@host#delete system root-authentication
user@host#set system root-authentication plain-text-password
user@host#New password:
user@host#Retype new password:
user@host# commit
commit complete
```

3.6 常用监控维护命令

下列操作命令在操作模式下使用，或在配置模式下 run show…

- Show system software 查看当前软件版本号
- show system uptime 查看系统启动时间
- Show chassis haredware 查看硬件板卡及序列号
- show chassis environment 查看硬件板卡当前状态
- show chassis routing-engine 查看主控板（RE）资源使用及状态
- show route 查看路由表

- show arp 查看 ARP 表
- show log messages 查看系统日志
- show interface terse 查看所有接口运行状态
- show interface ge-x/y/z detail 查看接口运行细节信息
- monitor interface ge-x/y/z 动态统计接口数据包转发信息
- monitor traffic interface ge-x/y/z 动态报文抓取（Tcpdump，类似 ScreenOS snoop 命令）
- show security flow session summary 查看当前防火墙并发会话数
- show security flow session 查看当前防火墙具体并发会话
- clear security flow session all 清除当前 session
- show security alg status 检查全局 ALG 开启情况
- SRX 对应 ScreenOS **debug flow basic** 跟踪报文处理路径的命令：
  - set security flow traceoptions flag basic-datapath 开启 SRX 基本报文处理 Debug
  - set security flow traceoptions file *filename.log* 将输出信息记录到指定文件中
  - set security flow traceoptions file *filename.log* size <file-size> 设置该文件大小，缺省 128k
  - set security flow traceoptions packet-filter filter1 destination-prefix 5.5.5.2 设置报文跟踪过滤器
  - run file show *filename.log* 查看该 Log 输出信息
- SRX 对应 ScreenOS **get tech** 命令，开 Case 时需要抓取的信息：request support information

End date 2010-06-17

By wang xiao fang
Email:van_wang@junipernetwork.cn
Mobile:12345678900