Juniper防火墙简要实用手册

（版本号：V1.0）

目　　录

1 juniper中文参照手册重点章节导读

版本：Juniper防火墙5.0中文参照手册，内容非常庞大和繁杂，其中诸多简介和功能实际应用的也许性不大，为了让大家尽快用最短的时间内掌握Juniper防火墙的实际操作，下面简朴对参照手册中的重点章节进行一种总结和概括，掌握了这些内容大家就可以基本可以完毕安全布署和维护的工作。

1.1 第二卷：基本原理

1.1.1 第一章：ScreenOS 体系构造

- 安全区
- 安全区接口
- 方略

1.1.2 第二章：路由表和静态路由

- 配置静态路由

1.1.3 第三章：区段

- 安全区
- 配置安全区
- 功能区段：HA区段

1.1.4 第四章：接口

- 接口类型：安全区接口：物理
- 接口类型：安全区接口：功能区段接口
- 察看接口
- 配置安全区接口：将接口绑定到安全区、从安全区解除接口绑定、修改接口、跟踪IP地址
- 二级IP地址

1.1.5 第五章：接口模式

- 透明模式
- NAT模式
- 路由模式

1.1.6 第六章：为方略构建块

- 地址：地址条目、地址组
- 服务：预定义的服务、定制服务
- DIP池：端口地址转换、范例：创立带有PAT的DIP池、范例：修改DIP池、扩展接口和DIP
- 时间表

1.1.7 第七章：方略

- 三种类型的方略

- 方略定义
- 方略应用

1.1.8 第八章：地址转换

- 地址转换简介
- 源网络地址转换
- 目的网络地址转换
- 映射IP 地址
- 虚拟IP地址

1.1.9 第十一章：系统参数

- 下载/上传设置和固件
- 系统时钟

1.2 第三卷：管理

1.2.1 第一章：管理

- 通过WEB 顾客界面进行管理
- 通过命令行界面进行管理
- 管理的级别：根管理员、可读/

  写管理员、只读管理员、定义Admin顾客
- 保证管理信息流的安全：更改端口号、更改Admin

  登录名和密码、重置设备到出厂缺省设置、限制管理访问

1.2.2 监控NetScreen 设备

- 储存日志信息
- 事件日志
- 信息流日志
- 系统日志

1.3 第八卷：高可用性

1.3.1 NSRP

- NSRP 概述
- NSRP 和NETSCREEN 旳操作模式
- NSRP集群
- VSD组
- 同步

1.3.2 故障切换

- 设备故障切换(NSRP)
- VSD 组故障切换(NSRP)
- 为设备或VSD 组故障切换配置对象监控

Juniper防火墙初始化配置和操纵

对一台空配置的Juniper防火墙我们可以用两种措施去进行操纵：Console控制台和WEB。

1. Console控制台：使用Console线连接到Juniper的防火墙上的Console口，运用超级终端用CLI命令行界面进行配置。
2. 使用WEB界面：Juniper防火墙上默认状况下在E1接口（trust）口有一种初始管理IP地址192.168.1.1
   255.255.255.0；我们可以把自己的笔记本和防火墙的E1口用一根交叉线连接起来，然后把本机的地址配置为192.168.1.X
   255.255.255.0，之后我们就可以在本机上通过IE浏览器登陆192.168.1.1的地址通过WEB界面对设备进行配置了。

注意1：Juniper防火墙接口的WEB管理特性默认只在E1接口（trust）口才启用，也就是说我们有也许无法通过用WEB登陆其他接口进行操纵，除非我们提前已经打开了对应接口的WEB管理选项。

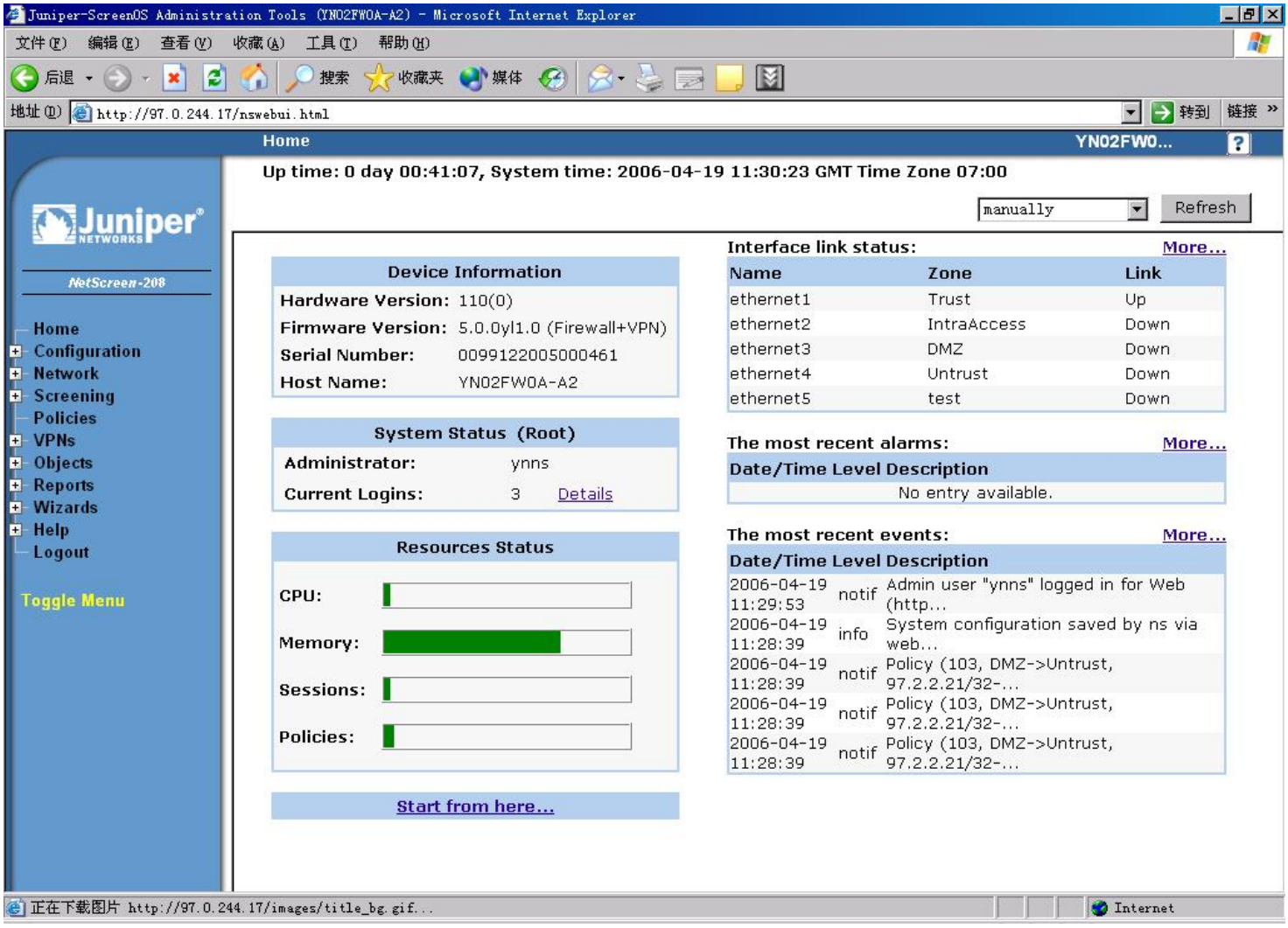
注意2：假如Juniper防火墙上有配置，我们不懂得目前E1接口的IP地址，我们可以先通过Console控制台用“get interface”的命令看一下目前E1口的IP地址。

注意3：Juniper防火墙OS 5.0以上的版本支持MDI和MDI

X自适应，也就是说我们的主机和E1口也可以用直通线进行互连，但这种方式有失效的时候，假如出现用交叉线互连物理也无法UP的状况，可以在Console控制台用“NS208-> delete file flash:/ns_sys_config”删除配置文献并重起防火墙的方式可以处理(Juniper的BUG)。

注：系统默认登陆顾客名和口令都是：“netscreen”。

2 查看系统概要信息



使用WEB登陆防火墙的管理地址，进入GUI管理界面，如上图所示。

- 左边是主配置菜单。

- 右边最上方是系统启动以及时间信息，右上角显示主机名。
- Device information：设备信息，显示设备硬软件版本、序列号以及主机名。
- Interface link status：接口链路状态，显示接口所属区和链路UP/DOWN信息。
- Resources Status：资源状况，显示系统CPU和内存使用率以及目前的会话和方略是系统满负荷的比例。（其中注意内存使用率是不真实的，在系统空负荷的状况下内存占用率也会很高，是系统自身设计的问题）。
- The most recent alarms：系统近来的报警信息
- The most recent events：系统近来的通告信息

3 主菜单常用配置选项导航

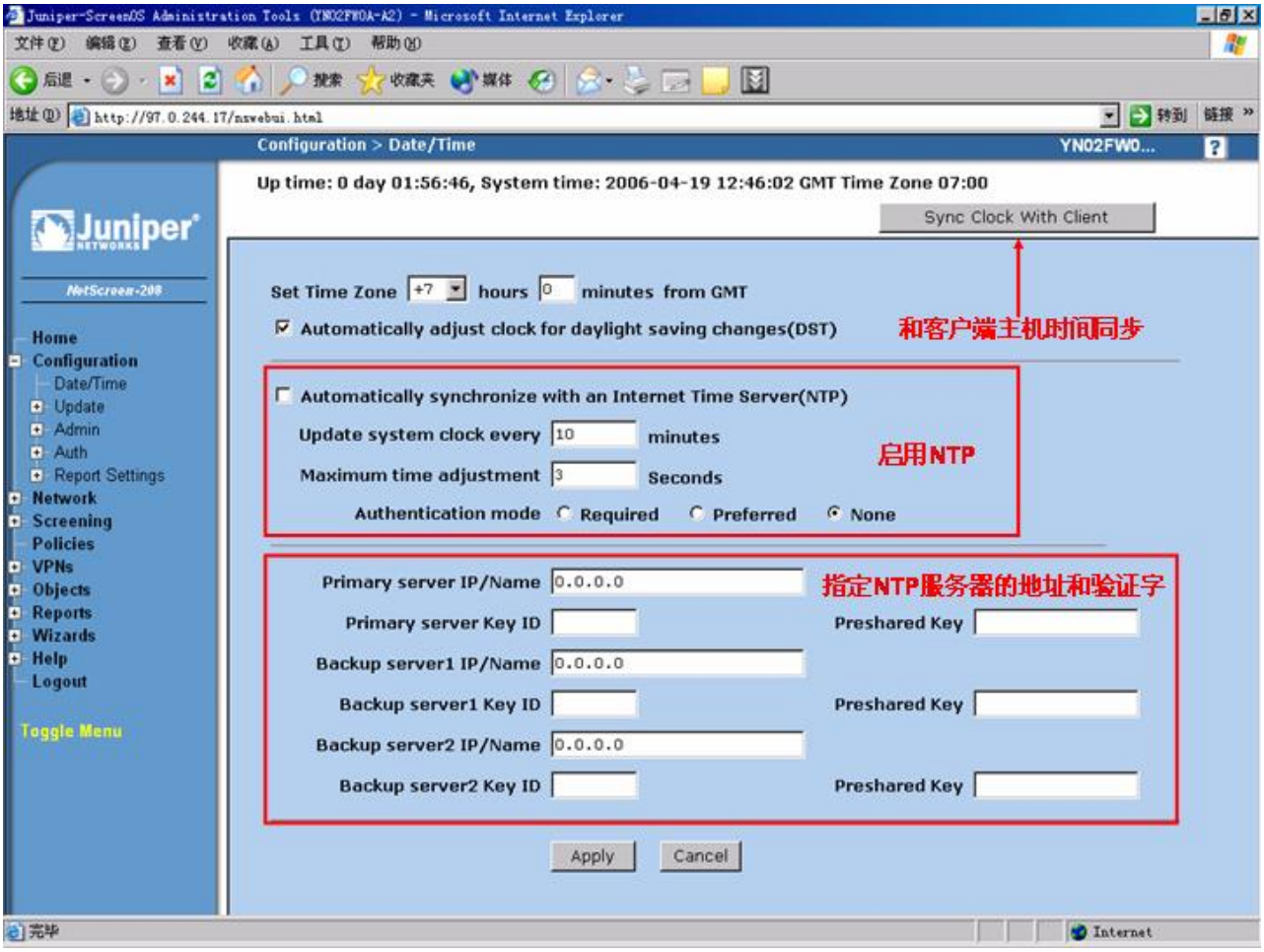
在主菜单中我们常常用到的配置菜单如下，背面将针对这些常用配置选项进行详细的简介。

1. Configuration：Date/Time；Update；Admin；Auth；Report Settings
2. Network：Zones；Interfaces；Routing；NSRP
3. Polices
4. Objects：Addresses；Services
5. Reports：Polices

只要可以纯熟掌握以上设置选项，就足以应对外网改造和平常维护的工作。

Configration配置菜单

3.1 Date/Time:日期和时间

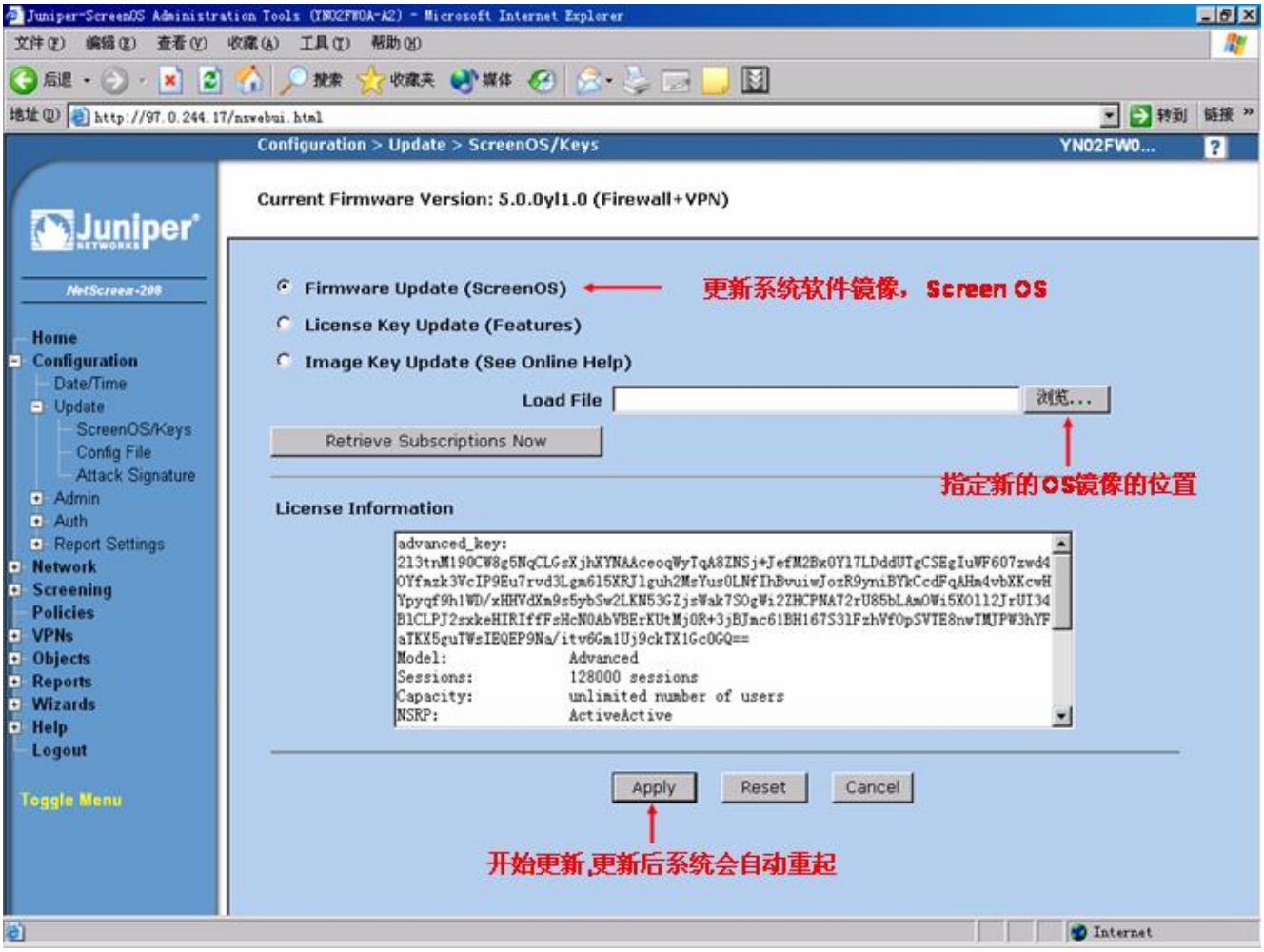


精确设置Juniper防火墙的时钟重要是为了使LOG信息都带有对的的时间以便于分析和排错，设置时钟重要有三种措施。

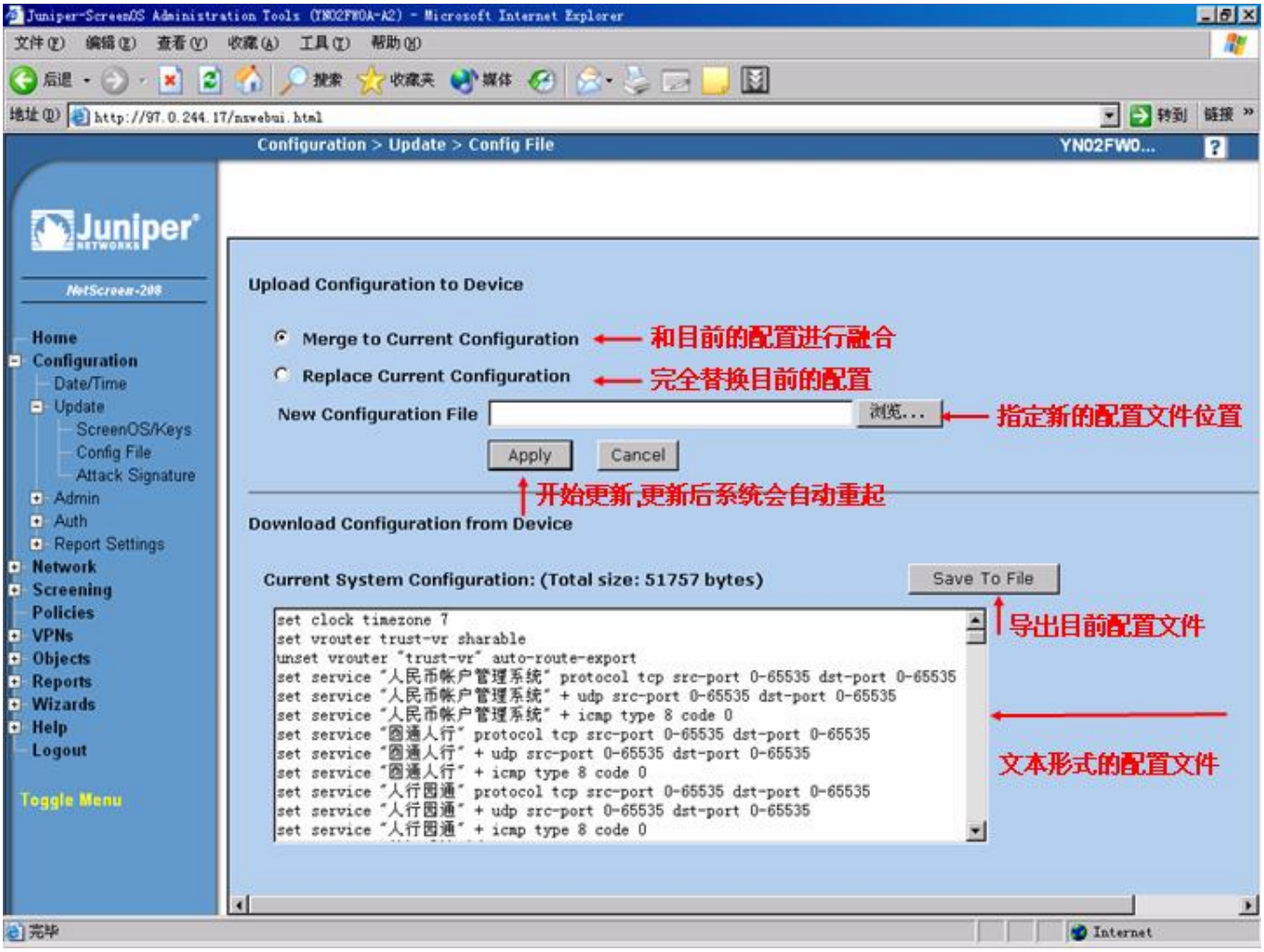
1. 用CLI命令行设置：set clock mm/dd/yyyy hh:mm:ss 。
2. 用WEB界面使用和客户端本机的时钟同步：简朴实用。
3. 用WEB界面配置NTP和NTP服务器的时钟同步。

Update更新系统镜像和配置文献

3.1.1 更新ScreenOS系统镜像

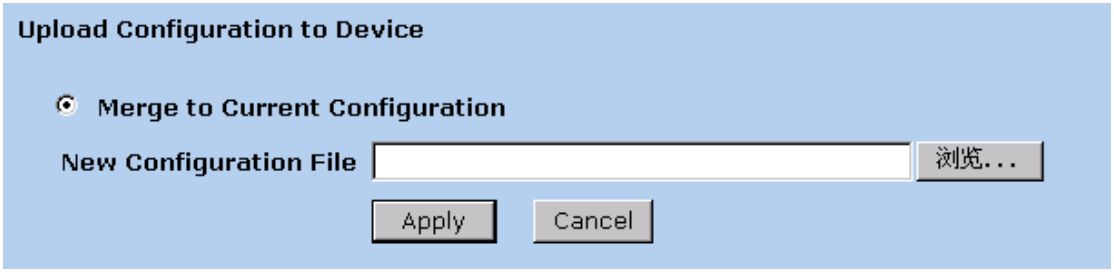


更新config file配置文献



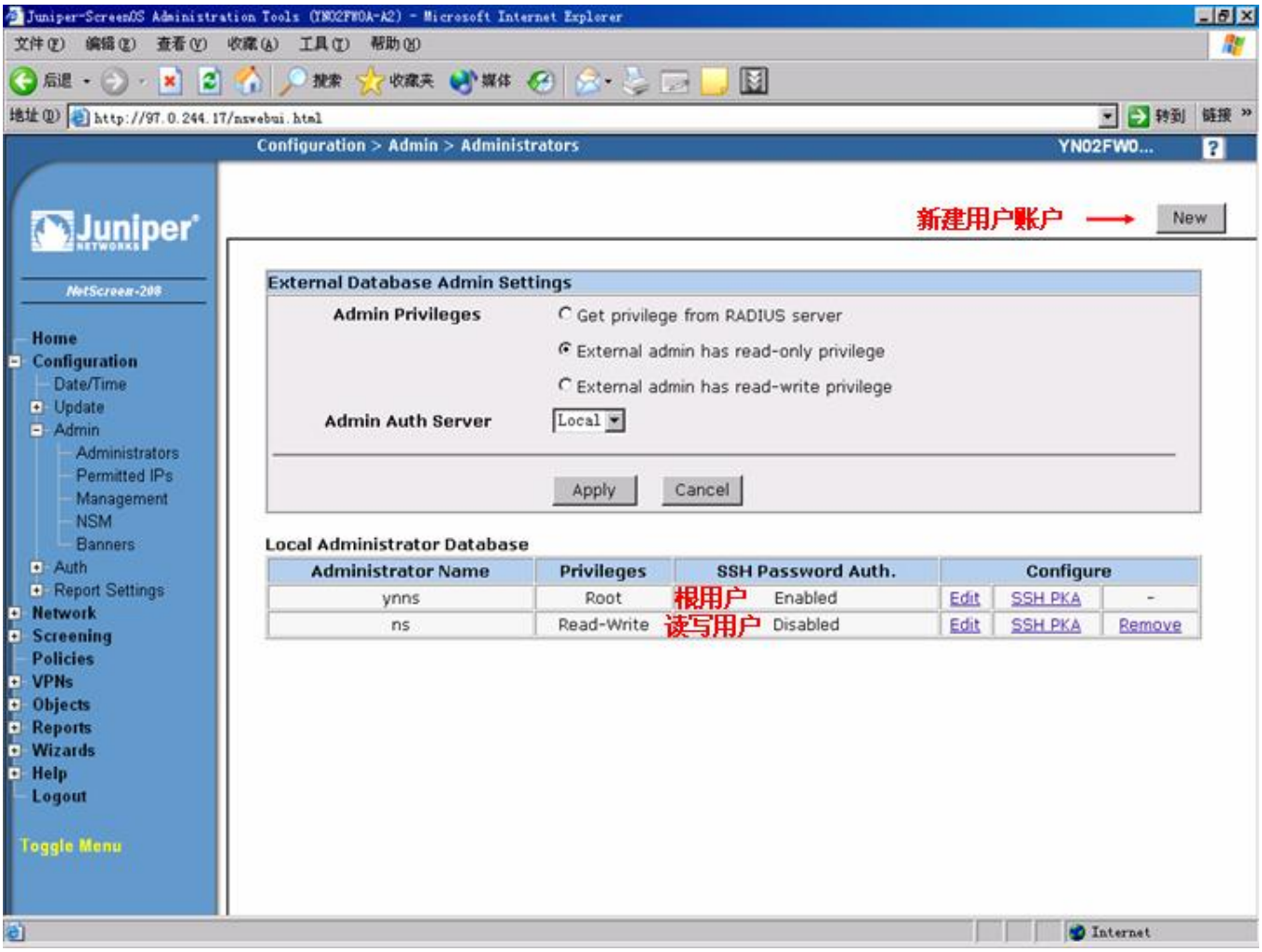
- 在这个菜单中我们可以查看目前文本形式的配置文献，把目前的配置文献导出进行备份，以及替代和更新目前的配置。
- 注意单项选择框默认是点选在“Merge to Current Configration”即和目前配置融合的位置，而我们一般是要完全替代目前的配置文献的，因此一定要注意把单项选择框点击到“Replace Current Configration”。
- 当进行配置替代的之后系统会自动重起使新配置生效。

TIP：进行配置旳替代必须用ROOT顾客进行登陆，用Read－Write顾客进行登陆是无法进行配置旳替代操纵旳，只有融合配置旳选项，替代目前配置旳选项将会隐藏不可见，如下图所示：

- 

Admin管理

3.1.2 Administrators管理员账户管理



- 只有用根ROOT顾客才可以创立管理员账户。
- 可以进行ROOT顾客账户顾客名和密码旳更改，但此账户不能被删除。
- 可以创立只读账户和读写账户，其中读写账户可以对设备旳大部分派置进行更改。