Juniper SSL VPN

配置手册

目 录

一．初始化设置

1.1、通过 Console 连接 SSL VPN

SSL VPN 的初始化是通过设备的 Console 端口完成的，Console 的设置如下：9600,8,N,1。

在管理员的计算机上使用任意终端软件，包括 HyperTerminal，Crt，SecureCrt 等等都行。把设备的 Console 线连接至 SSL VPN 的 Console 端口，开启电源开关，通过终端软件就能观察到设备启动自检的过程。

1.2、填写初始化信息

当系统自检到如下信息时：

Welcome to the initial configuration of your server!

NOTE: Press 'y' if this is a stand-alone server or the first
machine in a clustered configuration.
If this is going to be a member of an already running cluster
press n to reboot. When you see the 'Hit TAB for clustering options'
message press TAB and follow the directions.
Would you like to proceed (y/n)?: ***y（选择 Y）***
Note that continuing signifies that you accept the terms
of the Neoteris license agreement. Type "r" to read the
license agreement (the text is also available at any time
from the License tab in the Administrator Console).
Do you agree to the terms of the license agreement (y/n/r)?: ***y（选择 Y）***

初始化网络信息：

Please provide ethernet configuration information
IP address: ***192.168.0.190***
Network mask: ***255.255.255.0***
Default gateway: ***192.168.0.254***
（填入用户需要的 IP 地址，掩码和网关等信息。
注意：所有网络信息都会设置到 SSL VPN 的 Internal Interface 上）
Link speed [Auto]:
0) Auto
1) 1000 Mb/s, Full Duplex

2) 1000 Mb/s, Half Duplex
3) 100 Mb/s, Full Duplex
4) 100 Mb/s, Half Duplex
5) 10 Mb/s, Full Duplex
6) 10 Mb/s, Half Duplex
*Select 0-6: **0**（选择用户需要的速率）*
Please provide DNS nameserver information:
Primary DNS server: 202.106.0.20
*Secondary (optional): 202.99.8.1（填入用户需要的**DNS** 地址，可以是内部的**DNS** 服务器的**IP** 地址）*
DNS domain(s): juniper.net（填入用户需要的域名，无特别限制）
Please provide Microsoft WINS server information:
WINS server (optional):

确认初始化信息：

Please confirm the following setup:
IP address: 192.168.0.190
Network mask: 255.255.255.0
Gateway IP: 192.168.0.254
Link speed: Auto
Primary DNS server: 202.106.0.20
Secondary DNS: 202.99.8.1
DNS domain(s): juniper.net
WINS server:
*Correct? (y/n): y（确认无误后，选择**Y**）*

初始化安全信息：

Admin username: admin
Password:
Confirm password:
The administrator was successfully created.（填入用户设定的管理员帐号和密码）

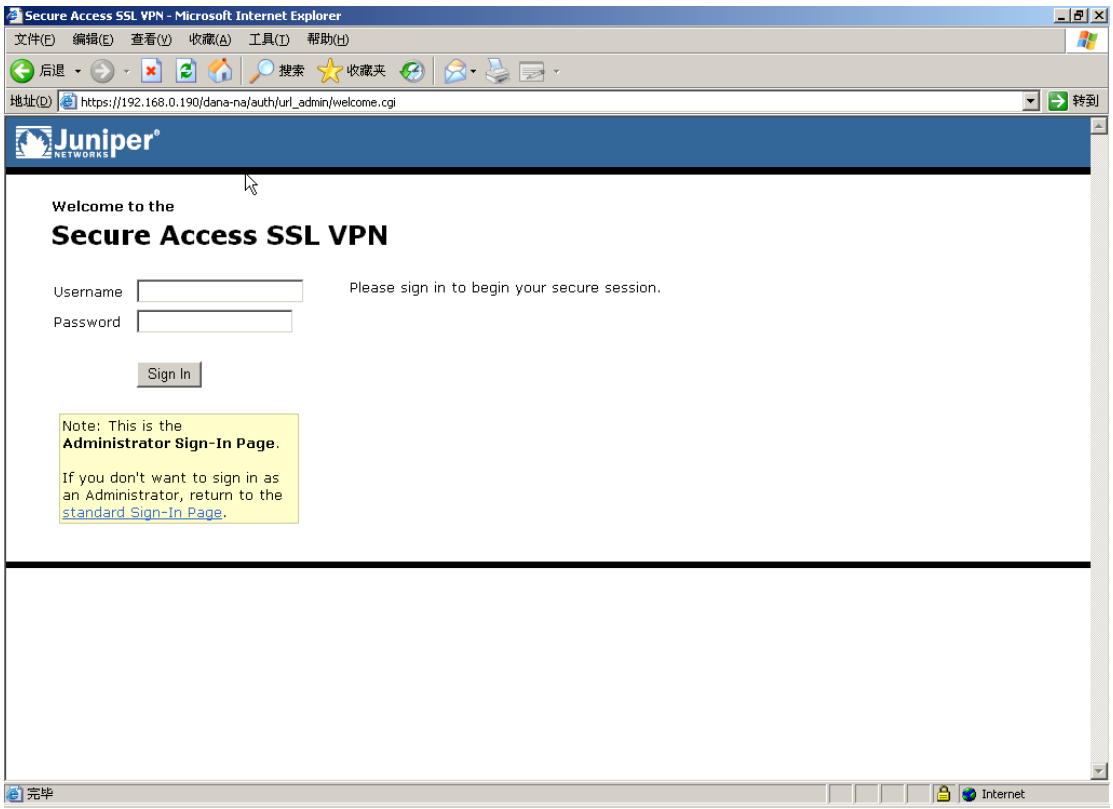
设置 SSL VPN 自签证书：

Please provide information to create a self-signed Web server digital certificate.
Common name (example: secure.company.com): timerwell.juniper.net
Organization name (example: Company Inc.): juniper
（这个部分输入用户的证书信息，无特殊限制）
Please enter some random characters to augment the system's random key generator.
We recommend that you enter approximatelythirty characters.
Random text (hit enter when done): dkfjlkkjffieejjkdnfkkfjiiiffoperjoootpqe454646
*（这个部分输入**30** 个左右的字符以产生证书）*
Creating self-signed digital certificate...
The self-signed digital certificate was successfully created.

Congratulations! You have successfully completed the initial set up of your server.
*（当您看到这句话时证明你已经成功的初始化 **SSL VPN** 了）*
https://<IVE-IP-Address>/admin (note the 's' in https://)
Example: https://10.10.22.34/admin
*（按照上述的提示，管理员可以通过 **URL https://192.168.0.190/admin** 来管理设备啦）*

1.3、使用浏览器连接 SSL VPN

如下图：



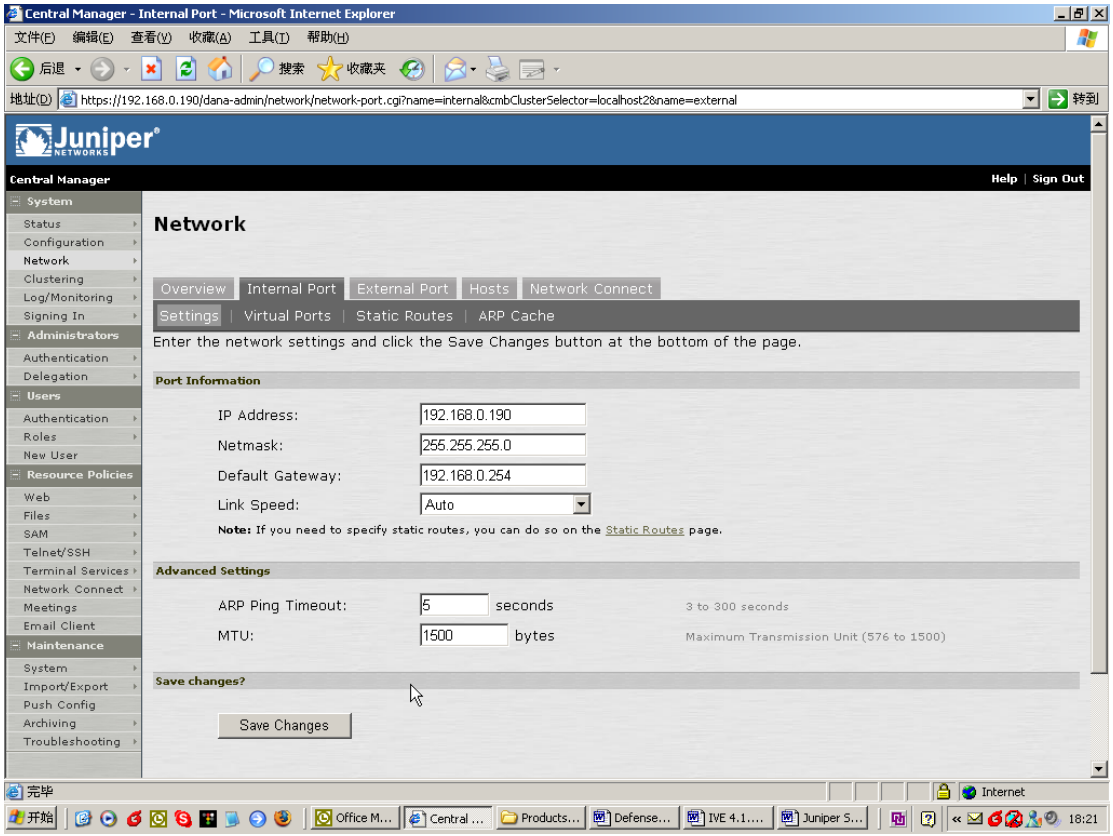
在这个 Web 页面中填入刚刚建好的管理员帐号和密码就可以登陆到 SSL VPN 进行管理啦，至此 SSL VPN 初始化过程完毕。

二．SSL VPN 基本设置

2.1、网络接口设置

在初始化过程中我们设置了 SSL VPN 的 Internal Interface，接下来我们设置 External Interface。

在浏览器上点击“**Network--→External Port--→Setting**”得到下图：

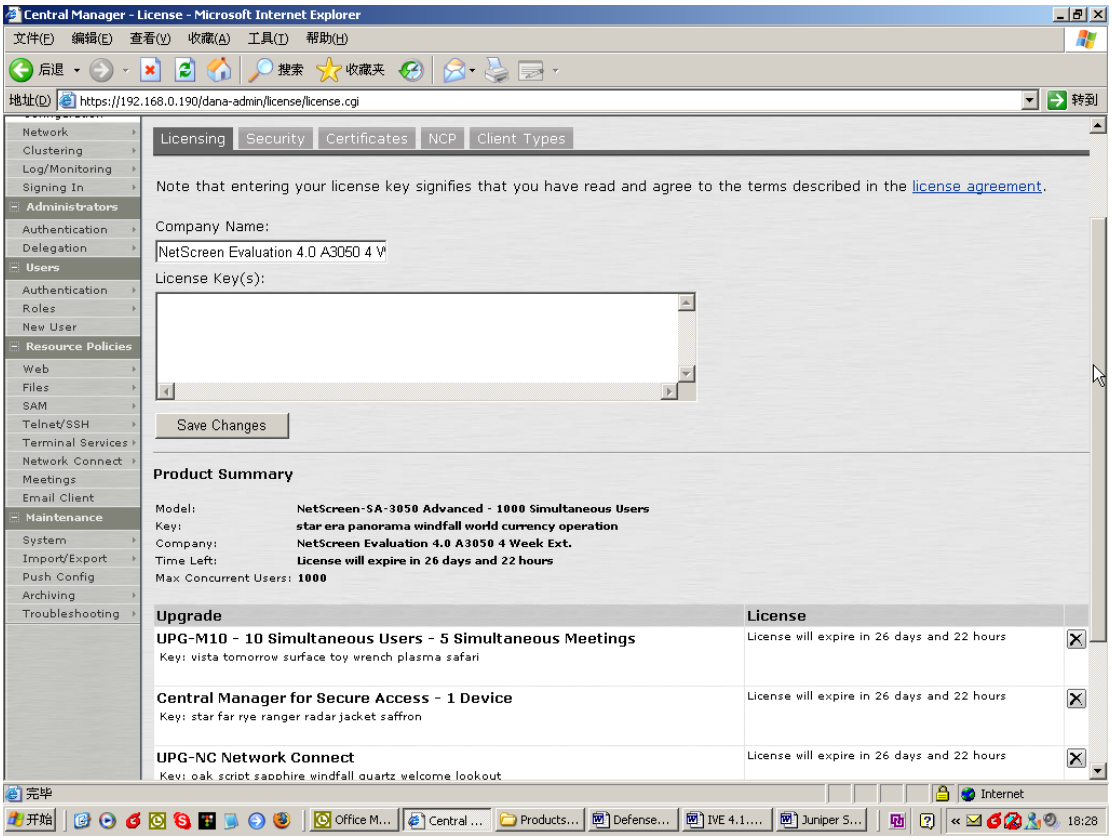


在上图中，填入相应的 External Port 设置，即完成了 SSL VPN 的网络初始设置。

2.2、设置 SSL VPN 的 License

SSL VPN 要正常工作，必须要有合适的 License，所以给 SSL VPN 添加 License 是必不可少的。

在浏览器上点击“**Configuration--→Licensing**”得到下图：



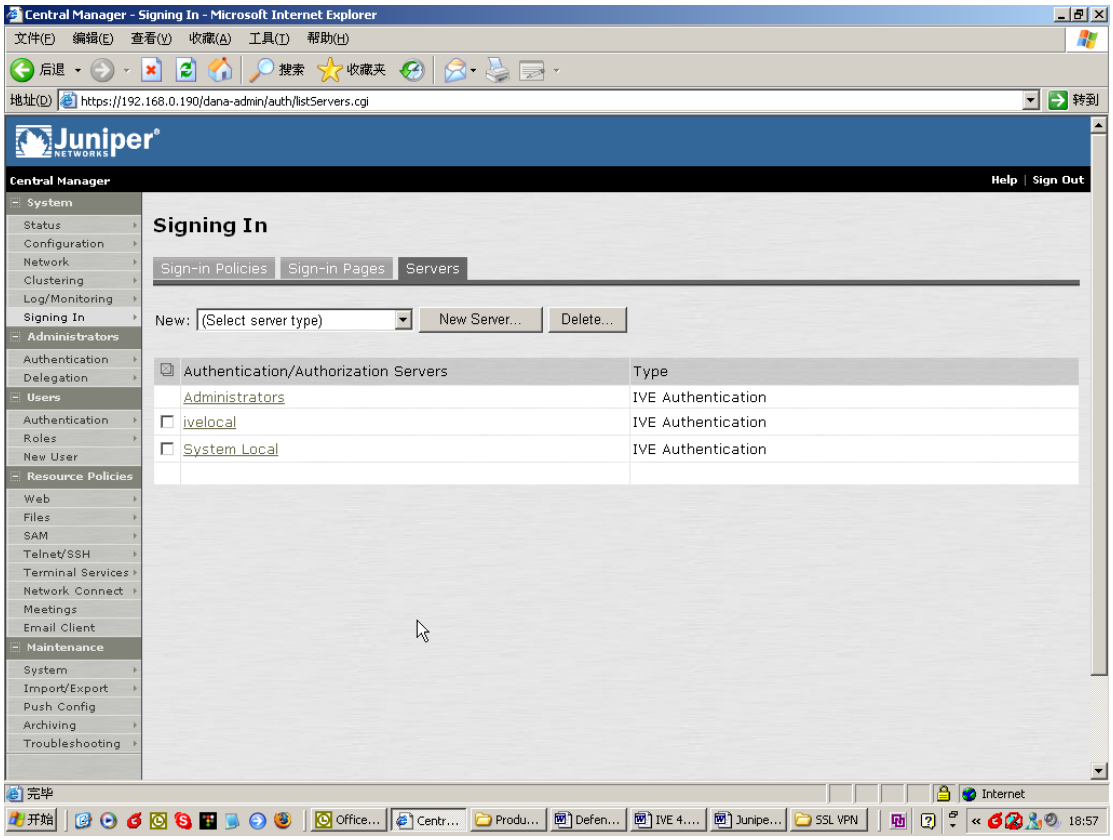
如上图所示，此设备拥有的是一个临时 License，包括了 1000 并发用户数和 4 周的试用期限等。

在添加 License 过程中，只需要在 Company Name 和 License Key 两个空栏中填入相关信息即可。

2.3、添加用户认证服务器

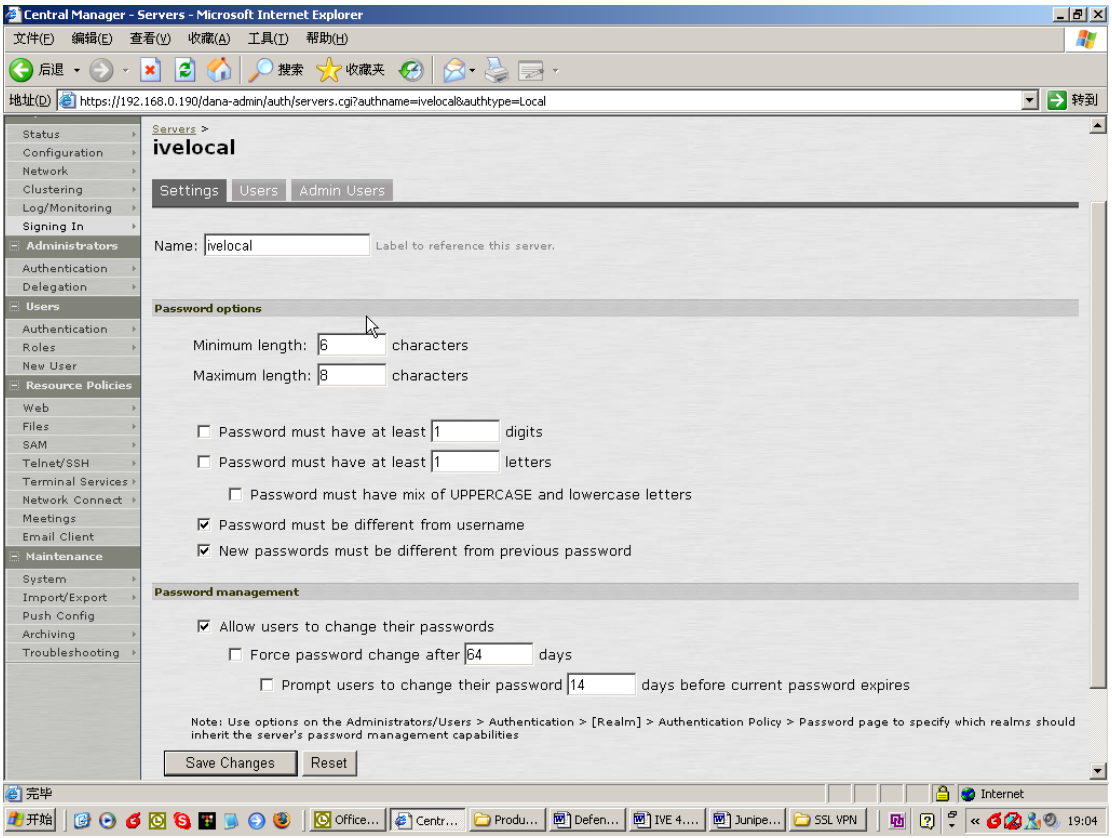
在配置完 SSL VPN 网络信息和 License 之后，就可以正常的使用 SSL VPN 了。为了让用户能够顺利的登入企业网，必须给用户进行身份认证。在身份认证的过程中，管理员可以选择使用 SSL VPN 内部的自建帐号认证用户，也可以结合企业内部的认证服务器进行认证。对于选择不同的认证服务器的帐号，他们将会属于不同的 SSL VPN 认证域。例如，我们可以利用一个 SSL VPN 自建的认证服务器，认证合作伙伴和分支机构的用户；利用内部的 LDAP 服务器认证总部本地的员工。

在浏览器上点击“**Signing--→Authentication/Authorization**”得到下图



在这个页面中，管理员将看到两个内置的认证服务器，Administrators 和 System Local。其中 Administrator 是添加 SSL VPN 管理员帐号的，而 System Local 是 SSL VPN 内建的一个普通用户的认证服务器。

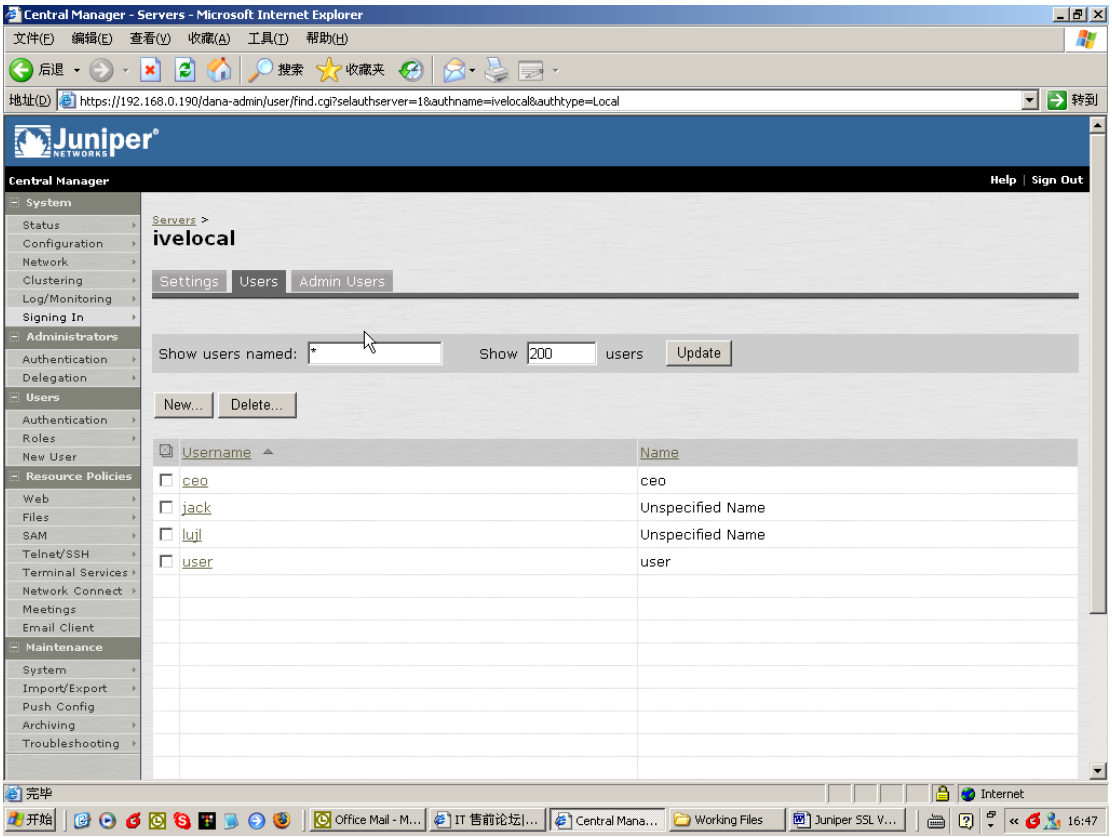
这是如果我们想添加一个新认证服务器及认证域时，点击页面上的**“New Server”**，并在 New 的选栏中选择“**IVE Authentication**”得到下图：



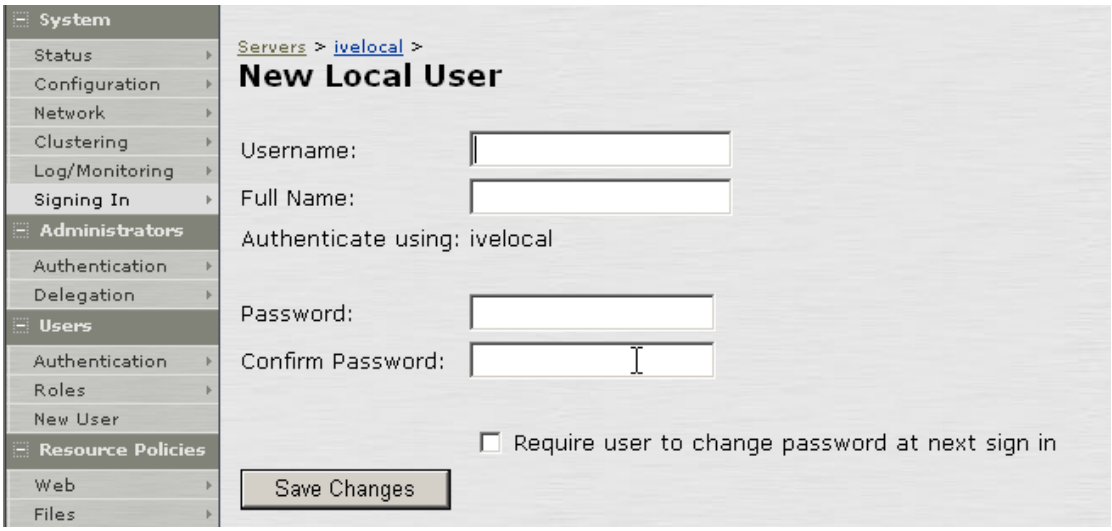
在该页面上的 **Name** 中输入认证服务器的名字（本例中是：IveLocal）等用户需要填入和勾选的其他选项，最后点击 **Save Changes** 即完成新加一个认证服务器的设置了。

2.4、添加认证用户

在 2.3 的图中选择 **Users**，即可进入到新建认证服务器的用户添加页面，如下图：



点击 **New**，即可加入在新建的认证服务器（本例的认证服务器是 IveLocal）中添加一个用户,如下图：

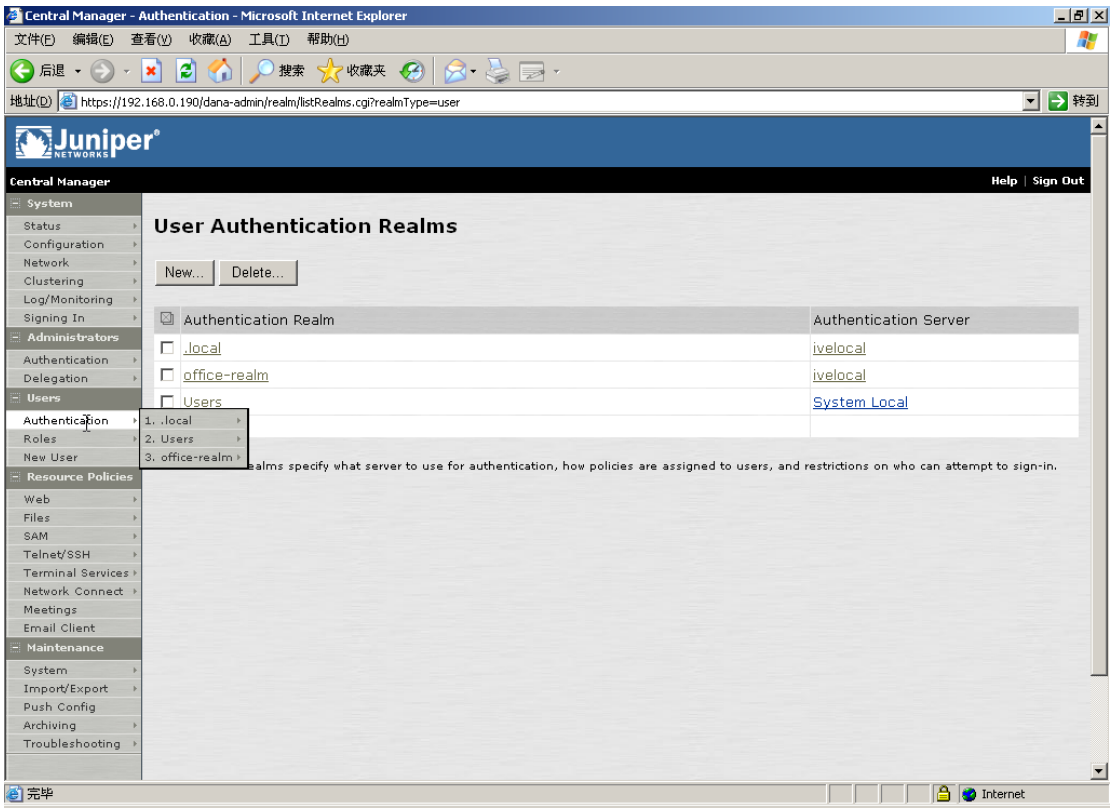


添加用户名和密码后，认证服务器 Ivelocal 就可以对这个新建用户进行身份的认证了。

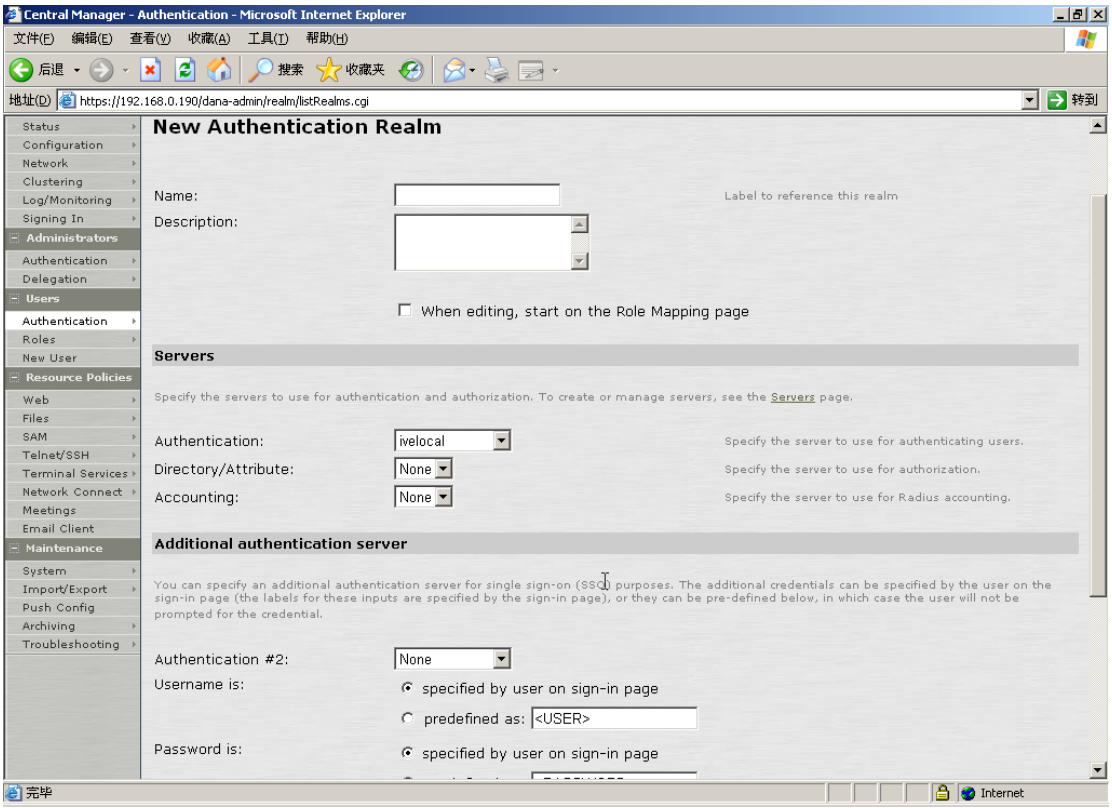
2.5、添加 SSL VPN 的认证域

每一个不同的认证服务器都可以有自己一套的用户数据库，无论使用的是 SSL VPN 内置机制建立的用户帐号数据库，还是使用集成企业内网的目录数据库，为了使认证机制更加合理和条理化，避免出现帐号重复和认证混乱的局面，Juniper SSL VPN 引入了认证域的功能，在 SSL VPN 上把不同的认证服务器加入到不同的域，来认证不同域上的用户，同时也方便用户了解自己登陆时应该选择哪一个认证域和哪一个认证帐号。

点击“**Authentication**”，得到下图：



点击“**new**”，得到下图：



在“**Name**”中，填入用户希望填入的认证域名。

在“**Authentication**”中，选择使用认证服务器 Ivelocal 来认证用户，最后点击“**Save Changes**”即完成了认证域的添加。

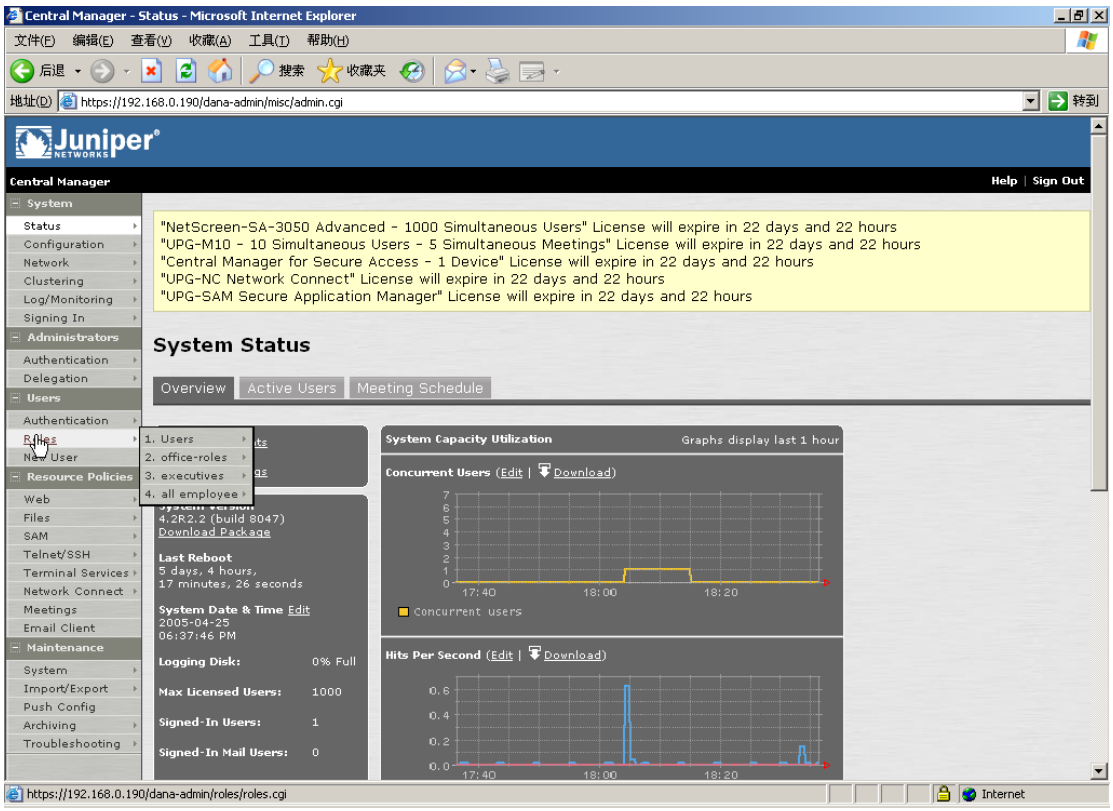
至此，Juniper SSL VPN 的基本配置，包括添加 License 和身份认证等设置都已完毕。

三．角色映射和功能模块

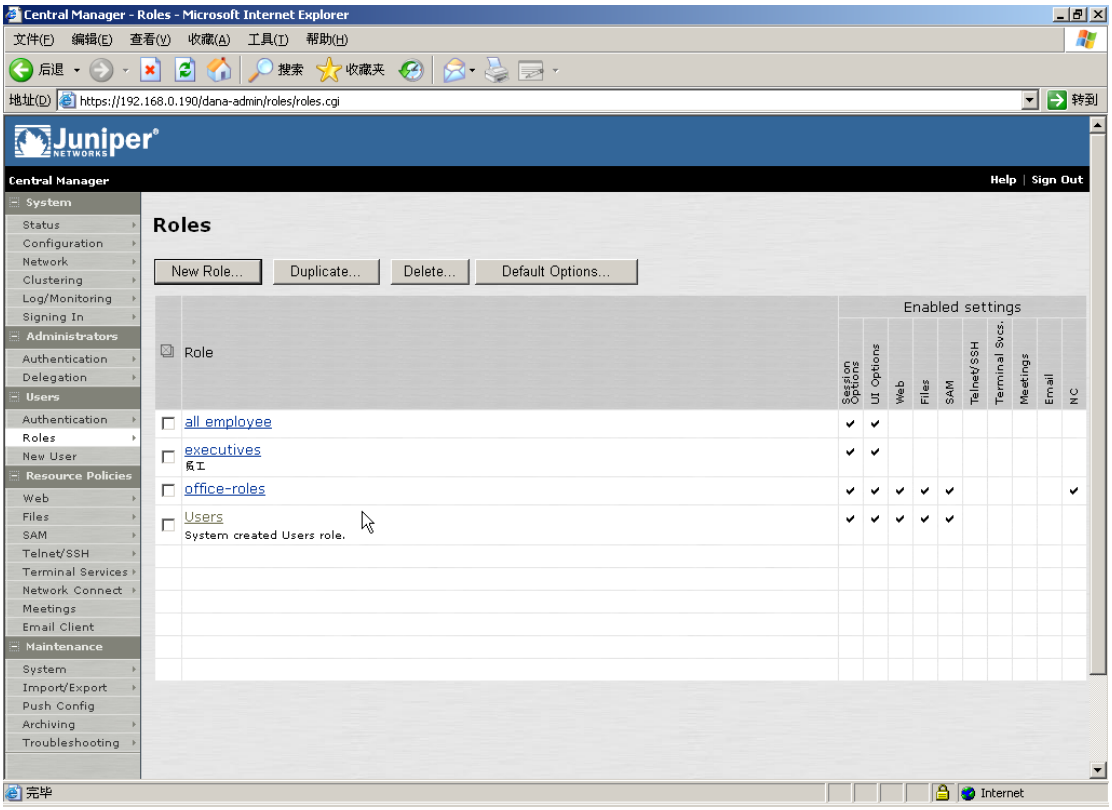
3.1、添加角色

在用户通过 SSL VPN 的身份认验证之后，需要给用户分配角色，这个角色是在 SSL VPN 中设置的，并且这个角色决定了用户能够在企业内网中享有什么样的权限和能访问什么样的资源。

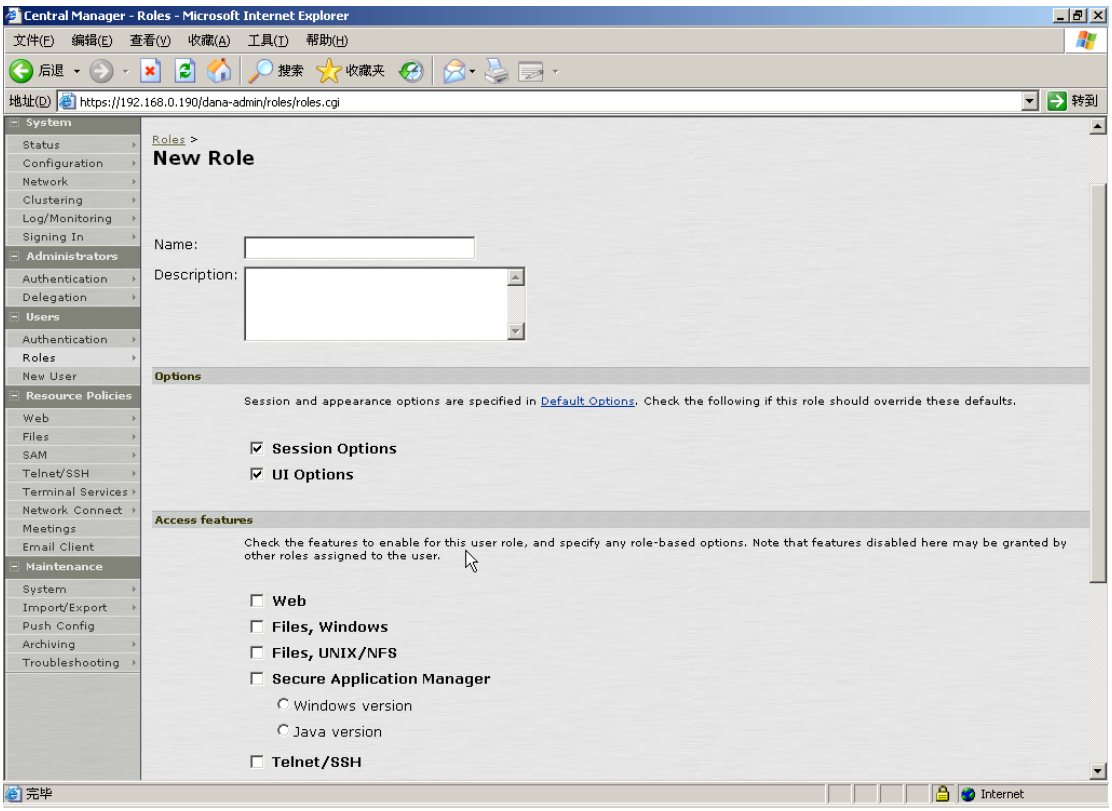
点击，SSL VPN 管理界面左栏的 **Roles**，如下图：



得到下图：



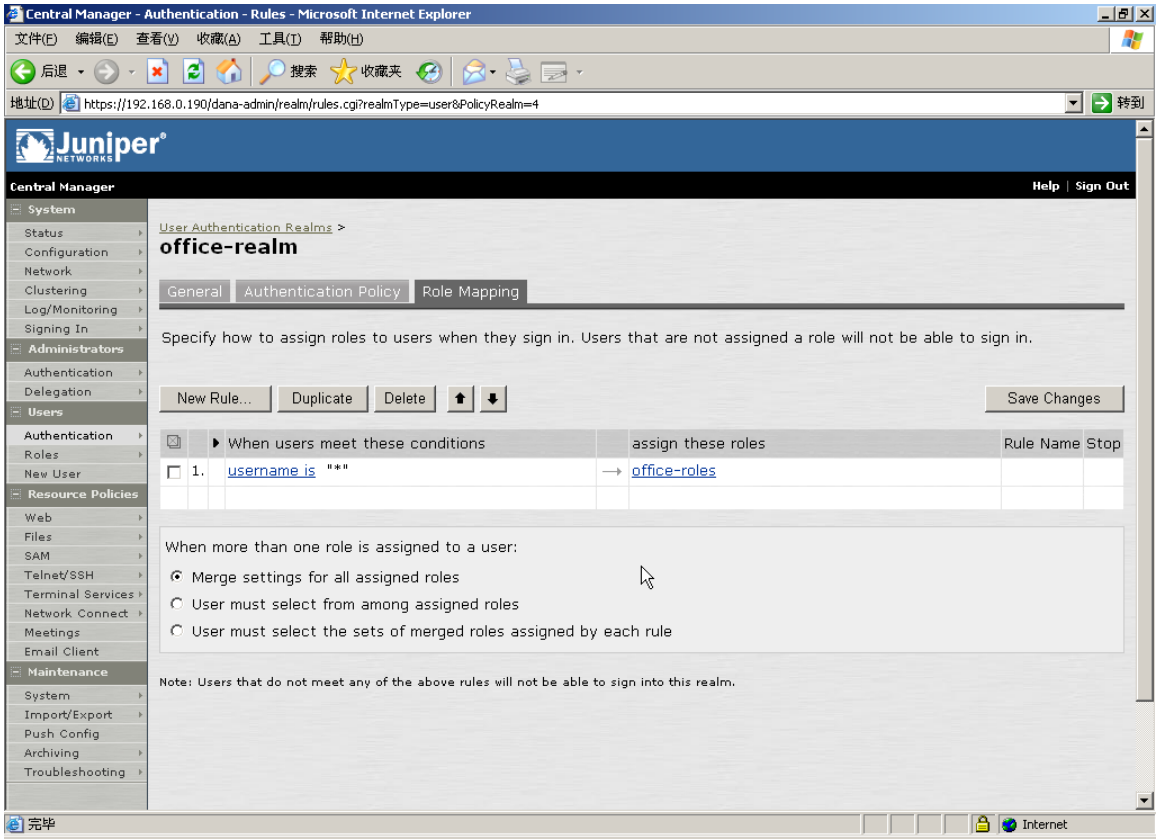
点击 **New Role** 添加一个角色：



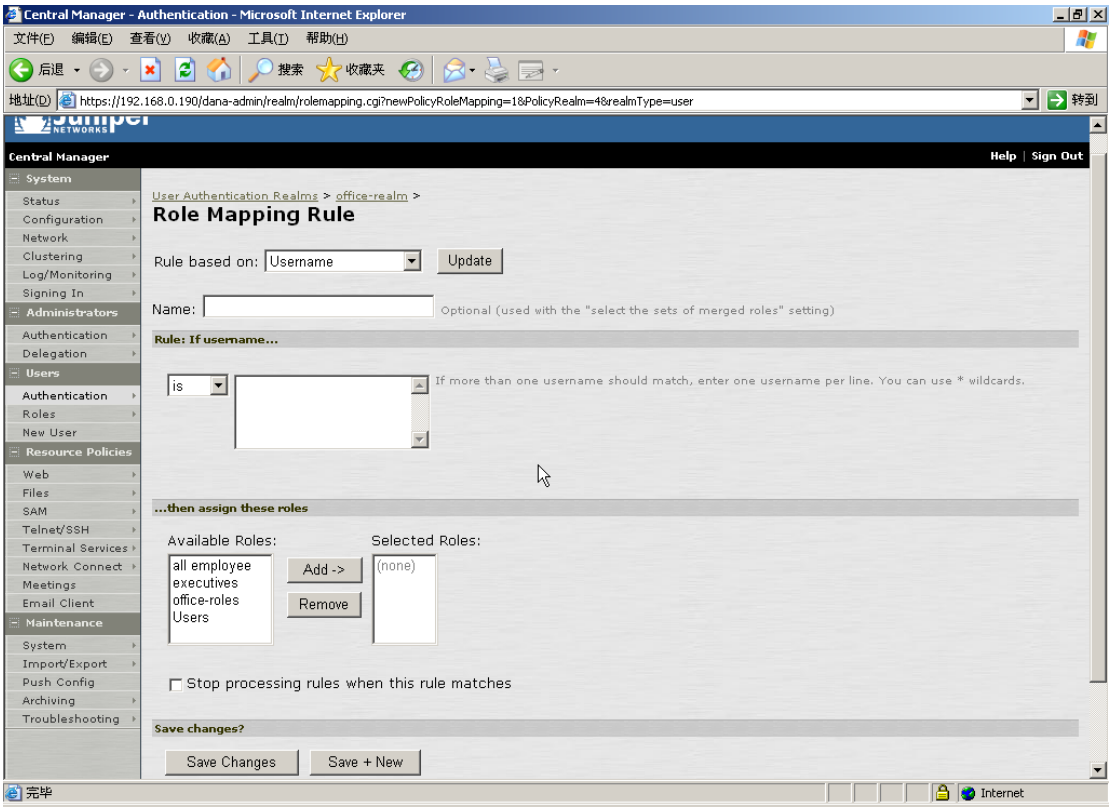
3.2、角色映射

在添加完角色后，就需要进行角色映射的工作，因为任何一个用户在身份认证之后，必须要把他映射成为 SSL VPN 中的一个角色，这样他才能拥有这个角色所能使用 SSL VPN 的功能模块和这个角色所能访问企业内网资源的权利。

以 Office-Realm 中的用户为例，点击 **Authentication-→Office-Realm-→Role Mapping**，得到下图:



选择 **New Rule…**



在**“is”**的下拉菜单右边文本框中填入相应的用户名字，可以是某一具体的用户名，也可以用通配符表示用户名，例如：**“*”**表示人任何用户。在**“Available Roles：”**下的文本框中，选择相应的角色，分配给这个用户。

例如如果我要把所有用户都分配给 **Users** 这个角色，则需要在**”IS”**下拉菜单右边的文本框中填入**“*”**，在**“Available Roles”**中选择**“Users”**加入到**“Selected Roles”**中即可。

这样一个用户的角色映射就完成啦。

3.3、功能模块

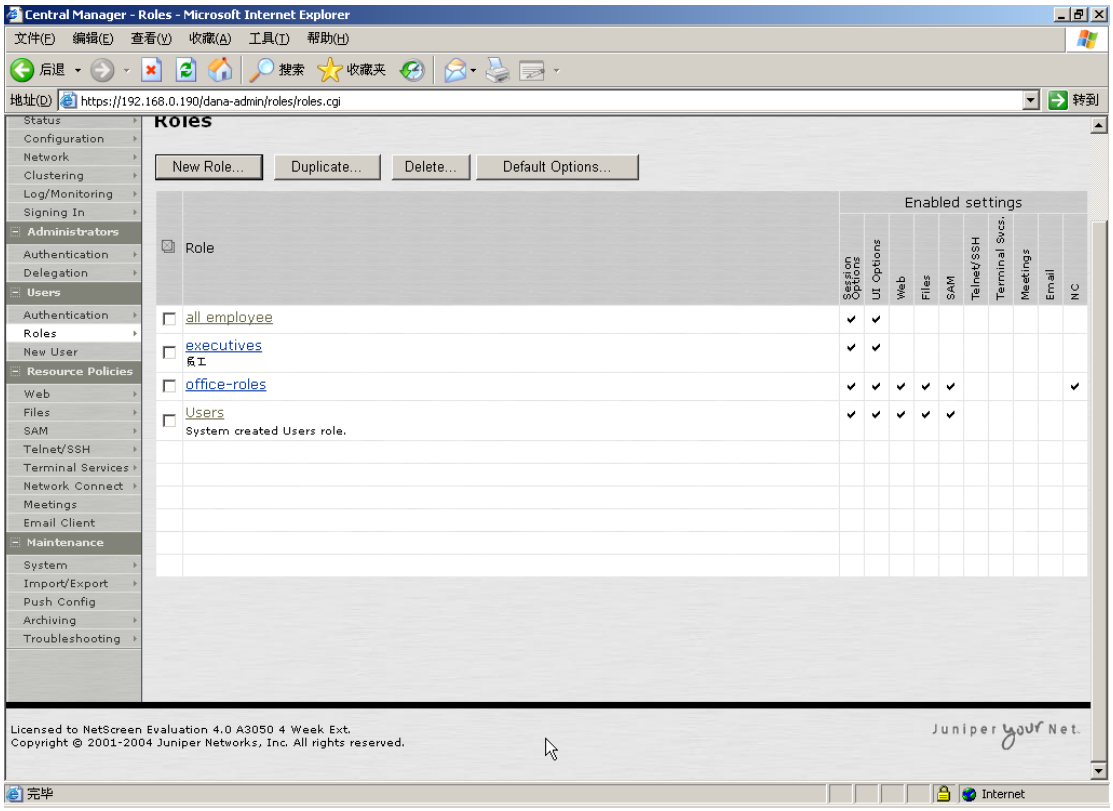
Juniper SSL VPN 上有三个功能模块，一个是基于 Web 功能和文件共享的 Core 模块，一个是保证 C/S 结构应用（例如：Lotus,Exchange,ERP 等）SAM 模块和最后一个全三层网络连接的 NC 模块。

根据设备的 License，每一台设备所具有的功能模块是不一样的，对于 SSL VPN 1000，3000 和 5000 系列，其中的 Core 功能模块是标配的，其他功能模块是单独购买的，而对于 SSL VPN RA－500 系列它只具有 NC 的功能模块，其

他功能模块需要单独购买。

即便是一台设备具有了上述全部的功能模块，但是对于不同的角色，他能够使用 SSL VPN 的功能模块是不一样的。

如下图，在我们建立一个角色时，可以选择他能够使用什么样的功能模块，比如说有的角色只能使用 Web 和 Files 共享，有的角色还可以使用 Secure Application Manager 的功能。



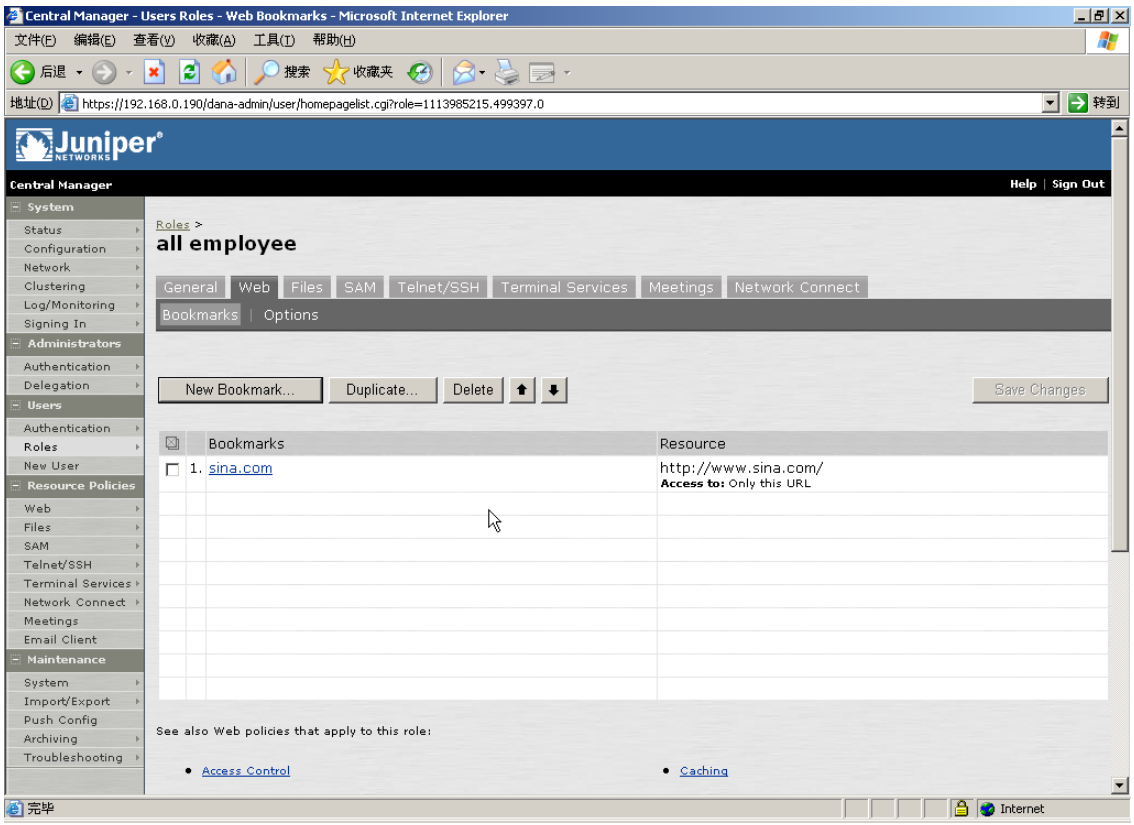
在图中一共有四个 SSL VPN 建立的角色，All Emplyees，Excutives，Office-roles，和 Users，但是从图中看出，每个角色所有拥有的 SSL VPN 功能模块是不一样的，比如 Users 角色只有 Core 和 SAM 的功能模块，而 Office-Roles 却有全部 Core，SAM 和 NC 的功能模块。这样大大的增强了角色的灵活性和安全性。

四．使用 SSL VPN 的各个功能模块

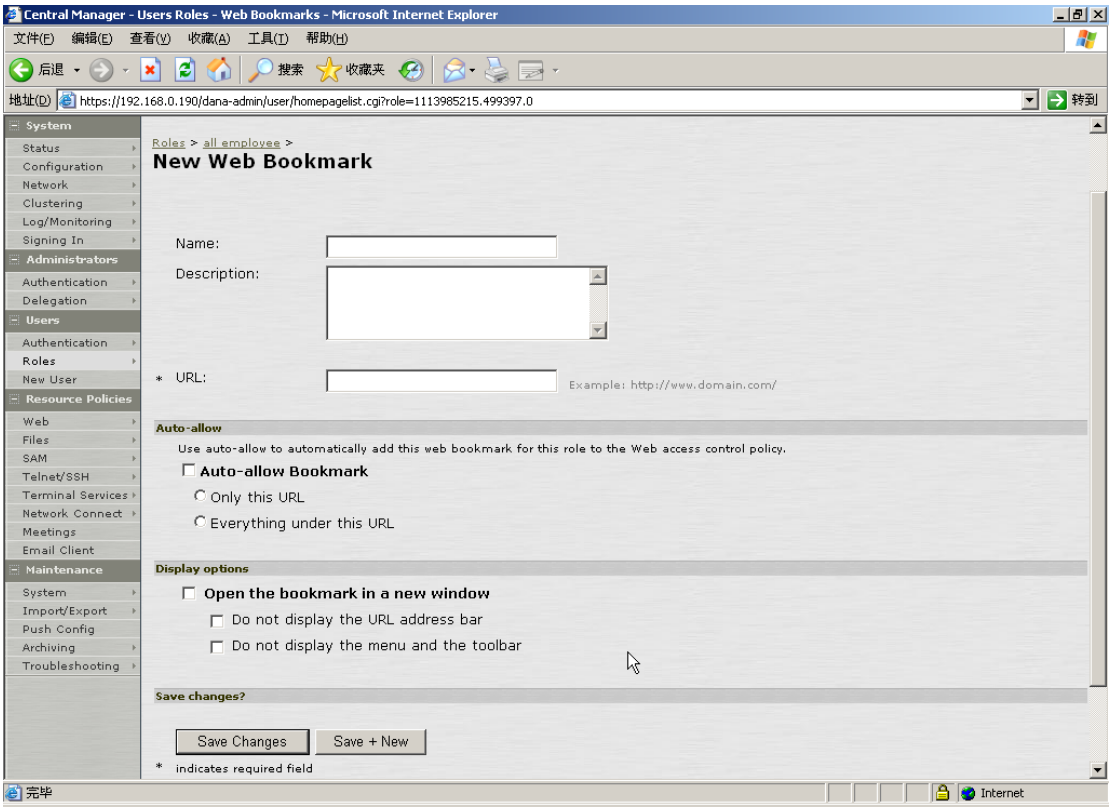
所有 SSL VPN 用户在访问内网资源时，例如：内部 Web 服务器，内部 Web Mail，内部的 Loutes 系统或是内部的 ERP 系统及一些网管系统，都是通过 SSL VPN 的三个功能模块来实现的。

4.1、使用 Core 功能模块

点击 SSL VPN 管理界面左部的 **Roles→All Employees-→Web**，得到下图:



点击 **New BookMark**，得到下图：



在”**Name”**中填入自己想要的名字，如果说是公司内部网站，可以写”**Corp Web”**登，在”**Description”**中填入相关的描述，在”**URL”**中填入公司网站的 IP 地址或是主机域名。

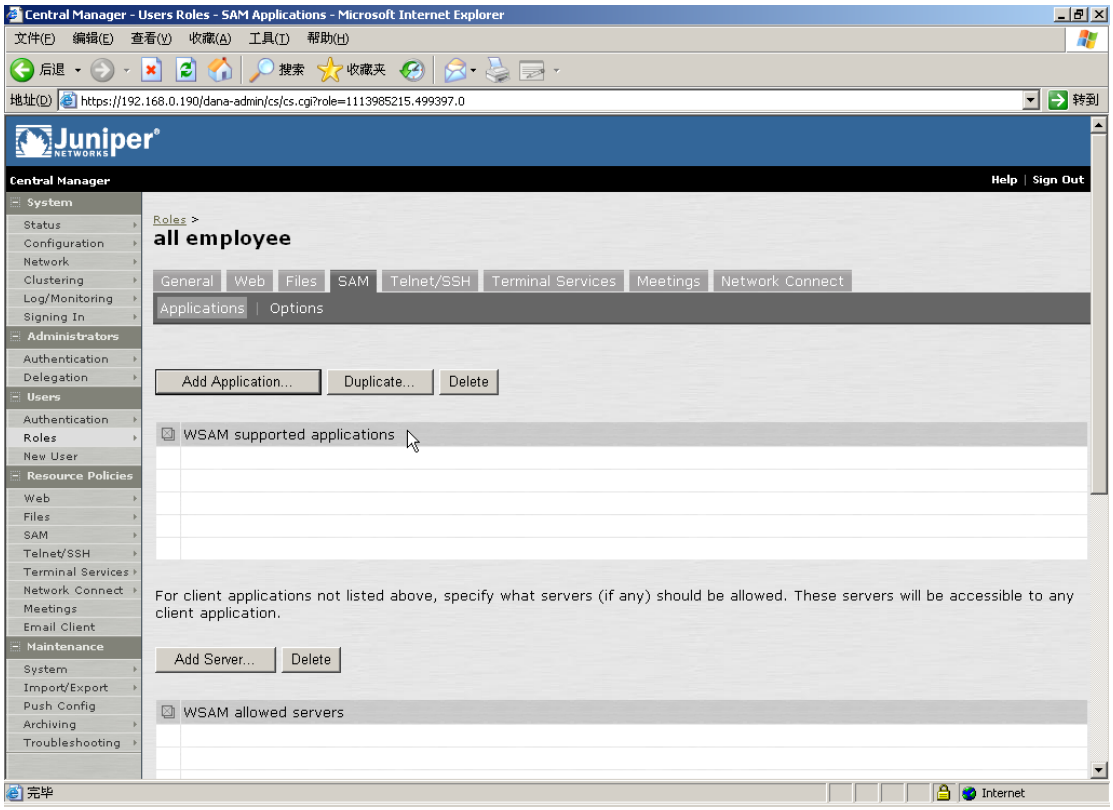
点选”**Auto-allow Bookmark”**和”**Everything under this Url”,**点击 **Save Changes** 这样就添加了一个内部资源的访问条目。

对于 Core 模块的另一个 Files 共享功能的实现原理基本和添加 Web BookMark 一样，请参考上述 Web 功能的设置步骤。

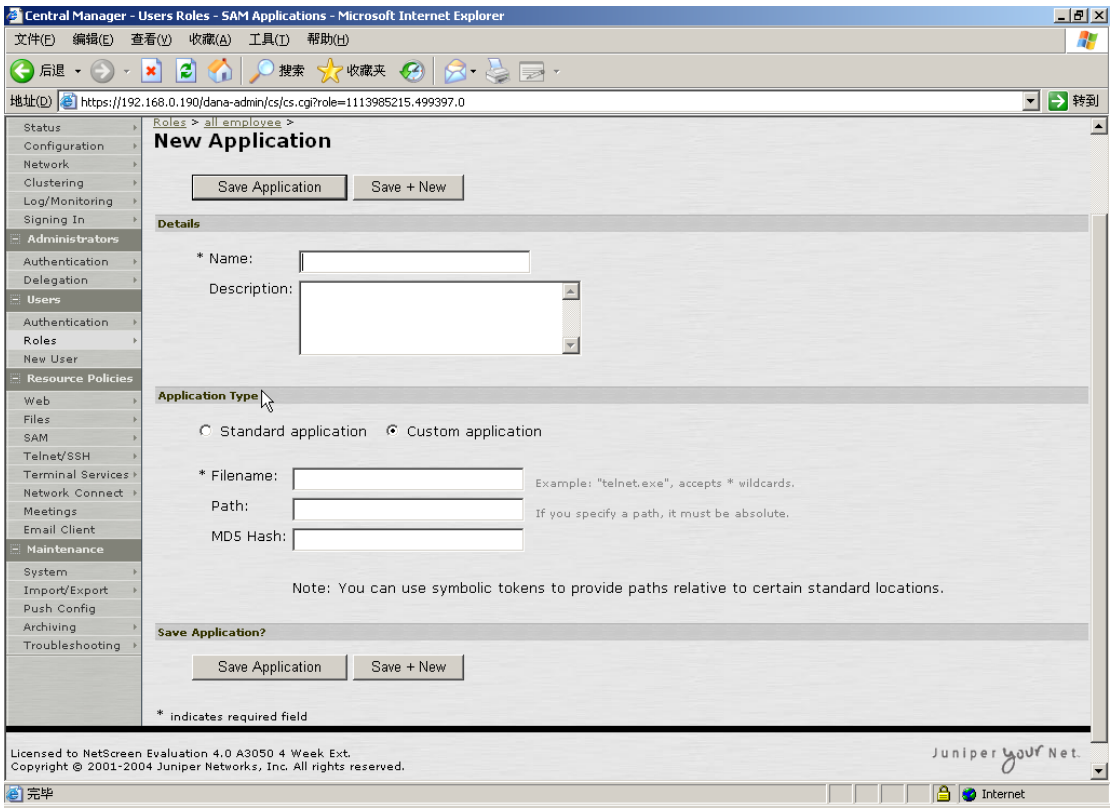
4.2、使用 SAM 功能模块

对于拥有自己开发的基于 C/S 结构的应用如 ERP 系统或是 Lotus 的客户来说，如果希望通过 SSL VPN 来访问后端的 C/S 应用，则需要使用到 SAM 功能模块。SAM 模块有 2 种，一种是适用于 Windows 版本的 SAM 模块，一种是适用于 Unix 系统的 SAM 模块。

点击“**Roles→All Employees-→SAM”，**得到下图，



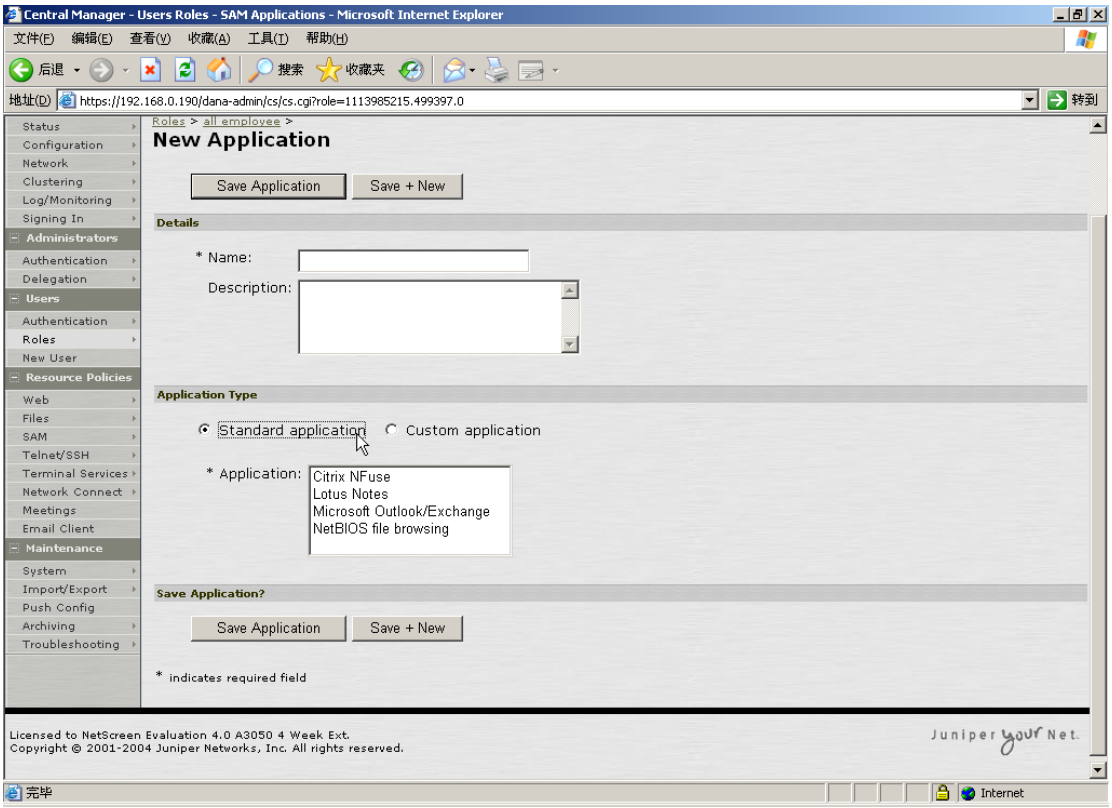
点击 **Add Application**，得到下图，



在 **Name** 中，填写应用程序的名字，如：Lotus 等，如果需要有描述的话在

Description 中加入描述。如果客户的应用程序是自己开发的选择 Custom application ,在 Filename 中填入客户端执行程序的名字，如果有必要，在 **Path** 后加入路径，点击 **Save application**,即完成了一个 Sam 条目的配置。

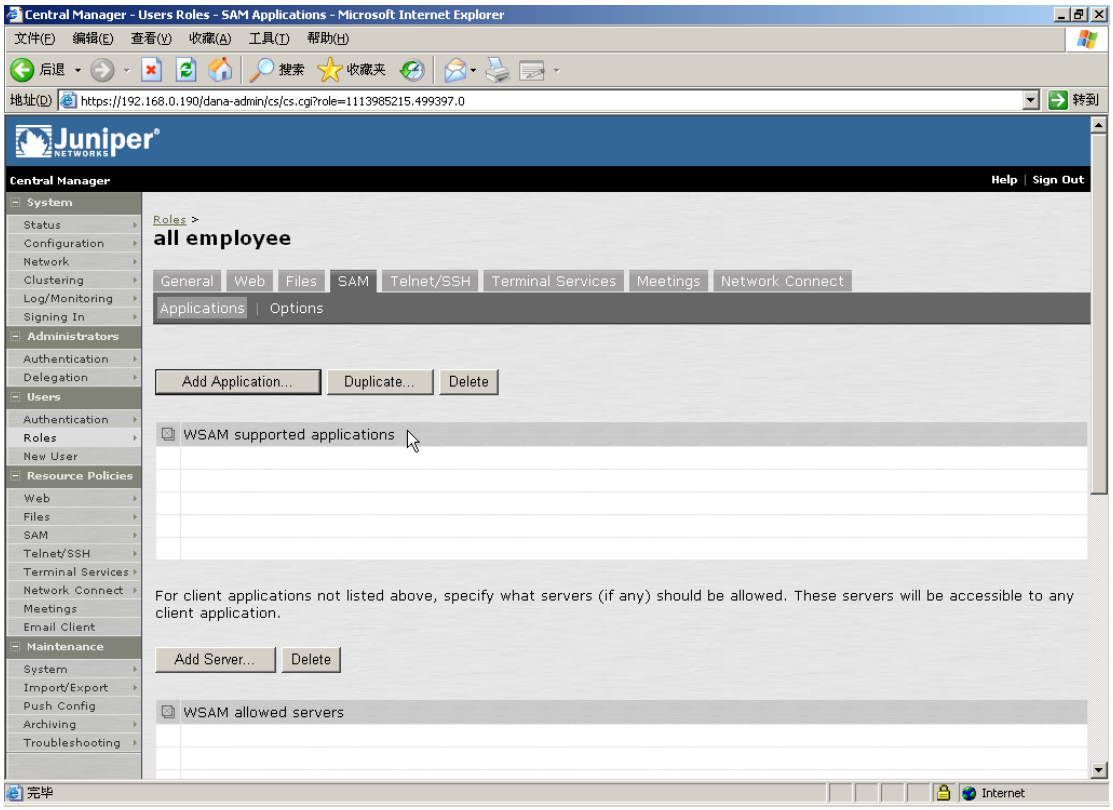
如果客户的应用程序是标准的商业软件，如 Lotus 等，请选择 **Standard application**，如下图：



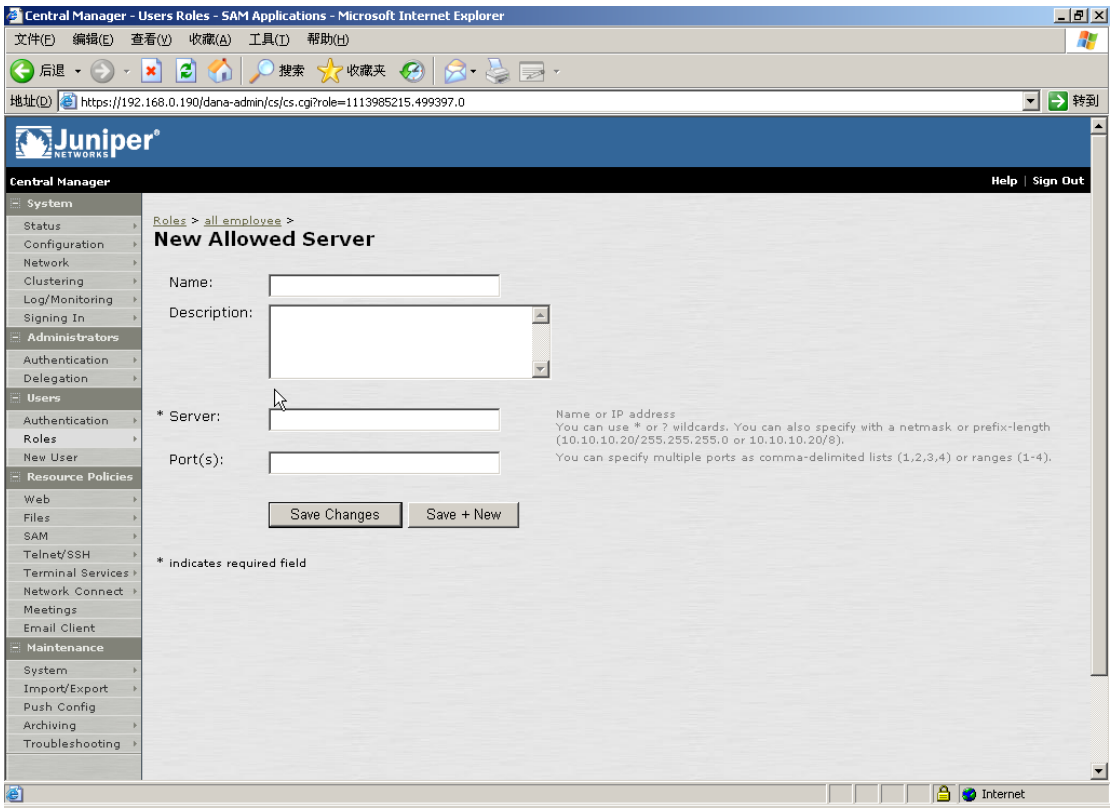
在 **Application** 框中选择，标准的程序后，点击 **Save Application** 即可。

如果公司内网的某台服务上有多个 C/S 应用在运行，为了方便管理员，SSL VPN 允许添加一个 Application Server，所有去往这个 Server 的请求都将被 SSL VPN 截获并处理，而不用在 SAM 中建立太多的客户端应用程序的条目（Application）。

点击 **“Roles→All Employees-→SAM”**，得到下图，



点击 **Add Server...**，得到下图，



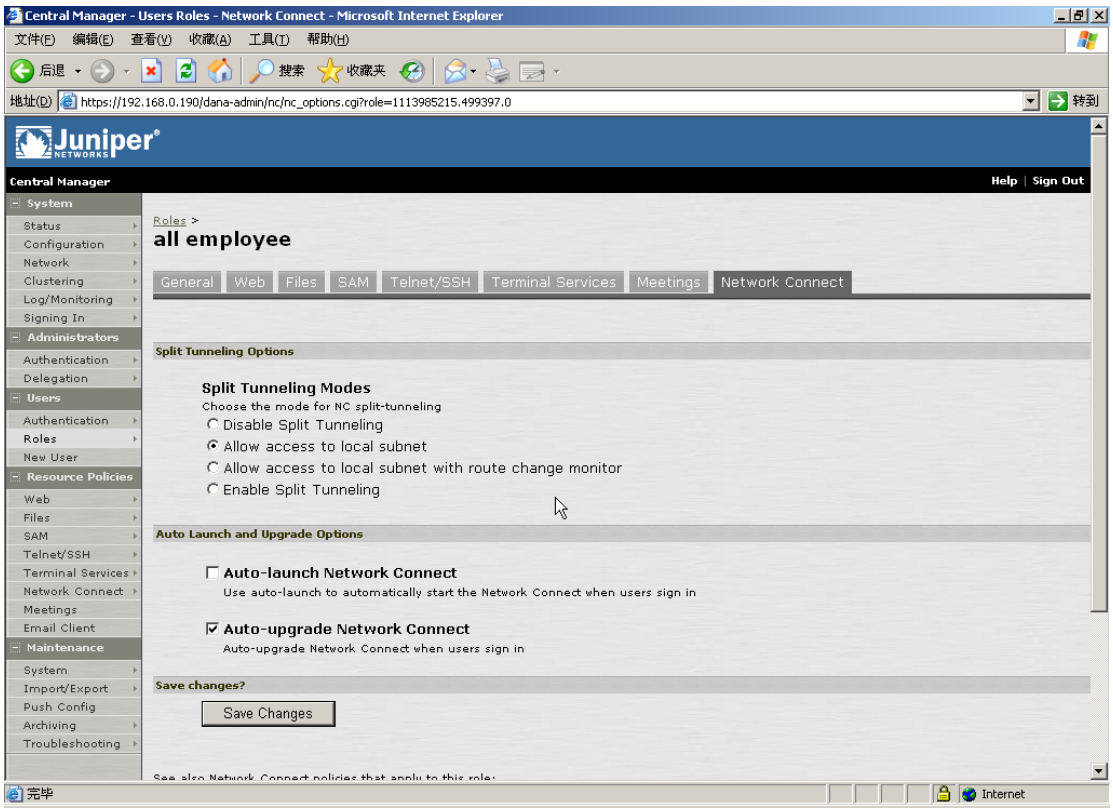
在 **Name** 中填入服务器的名字，在 **Server** 中填入 IP 地址或是域名。点击

Save Changes 完成配置。

4.3、使用 Network Connect 模块

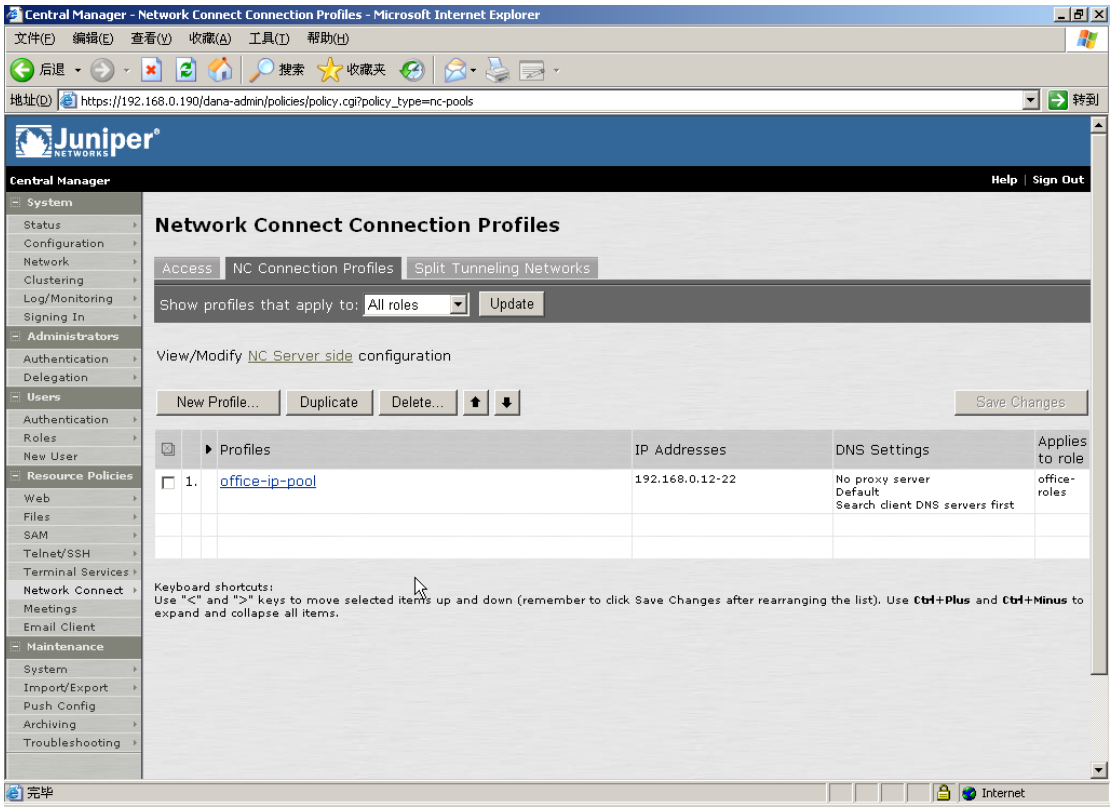
对于一些专业的技术人员，如果要使用 UDP 的协议，如 SNMP 等或是需要用到 Server Initialization Protocol 的应用时，这时候就需要 SSL VPN 的 NC 模块了。

点击“**Roles→All Employees-→Network Connect”**，得到下图：

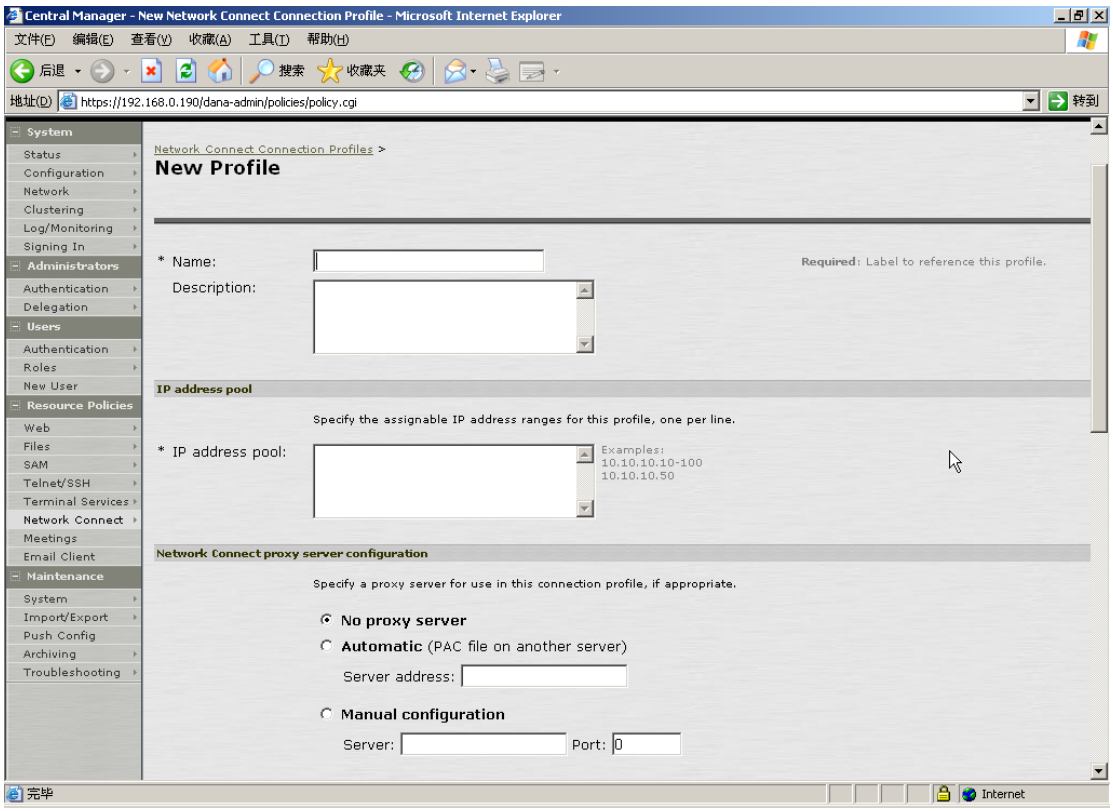


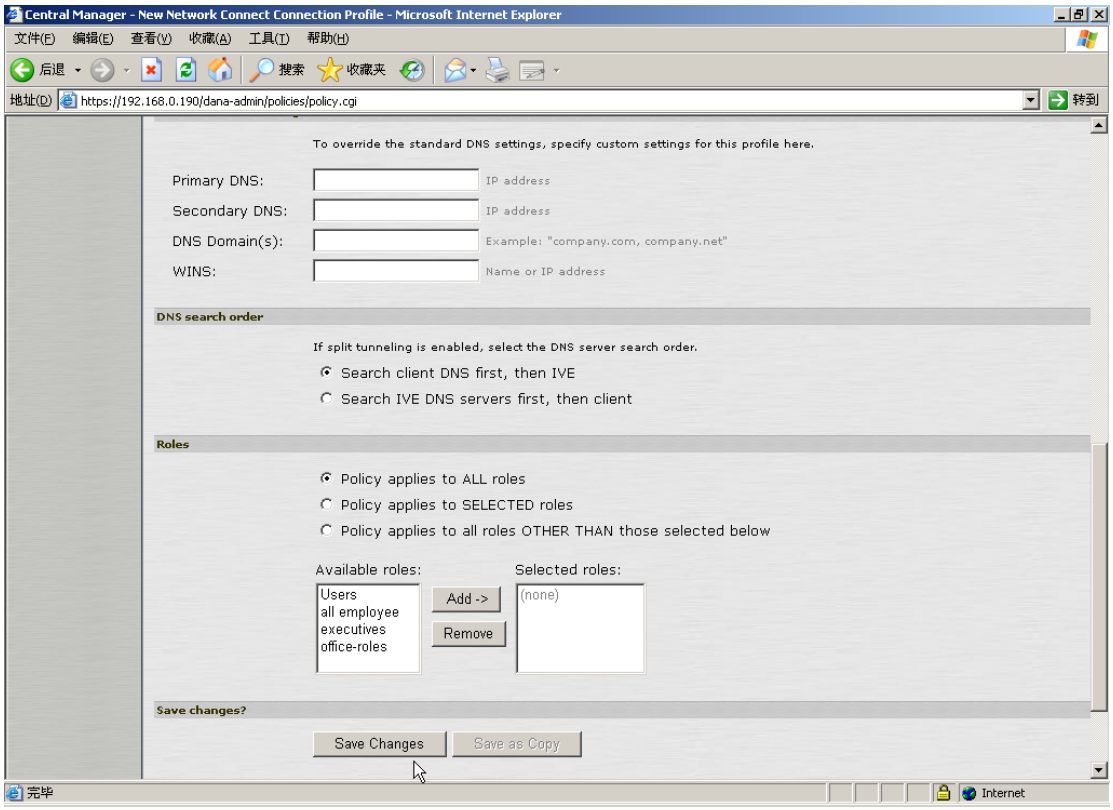
当希望客户在通过 SSL VPN 的 NC 模块登陆企业内网后，还能够让用户继续访问 Internet，请选择 **Enable Split Tunneling**。

点击“**Resources Police→Network Connect-→NC Connection Profile”,** 得到下图：



点击 **New Profile….**,得到下图：





在 **Name** 中填入，NC 分配的**地址池名称**，在 **IP Address Pool** 中填入 NC 使用的 **IP 地址池**，选择是否给使用 NC 的用户设置**代理服务器**，是否为这些用户**设置内部 DNS**，以及调整这些用户的 **DNS 查询次序**，选择这条 Policy 适用那个**角色**。

点击 **Save Changes**，完成 NC 的设置

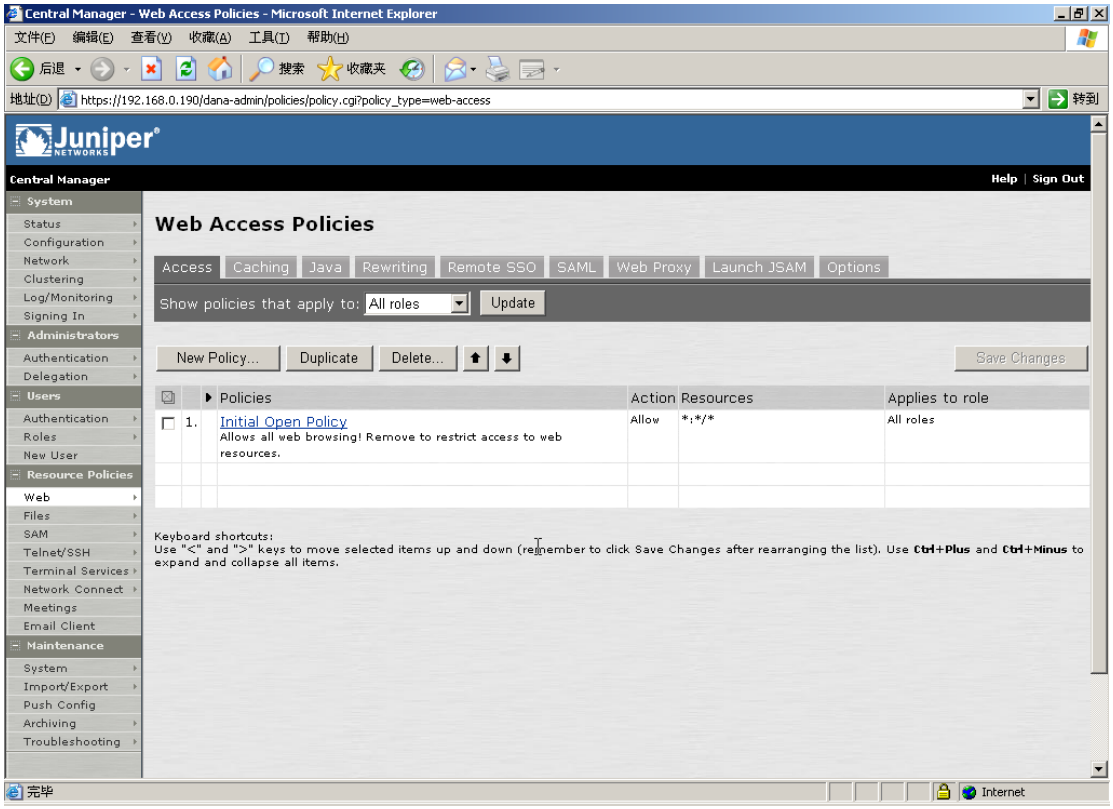
注意：如果一个角色既有 Core，SAM 的功能模块，又有 NC 的功能模块，这几个的功能模块的执行优先次序是 Core>SAM>NC,也就是说如果有一个用户登入 SSL VPN 后使用了 NC 模块，但是他发现自己访问内网的 Web 服务器时，依旧使用的是 Core 模块，这不用觉得奇怪。

五．资源访问控制

SSL VPN 和传统的 IPSec VPN 最大的区别之一，就是 SSL VPN 拥有应用层的资源访问控制，也就是说当一个用户登入 SSL VPN 之后，他不能象 IPSec VPN 用户那样自由的访问内网的所有资源，而必须接受 SSL VPN 的限制，有限制的访问内网资源。这样更提高了 VPN 网络的安全性和稳定性。

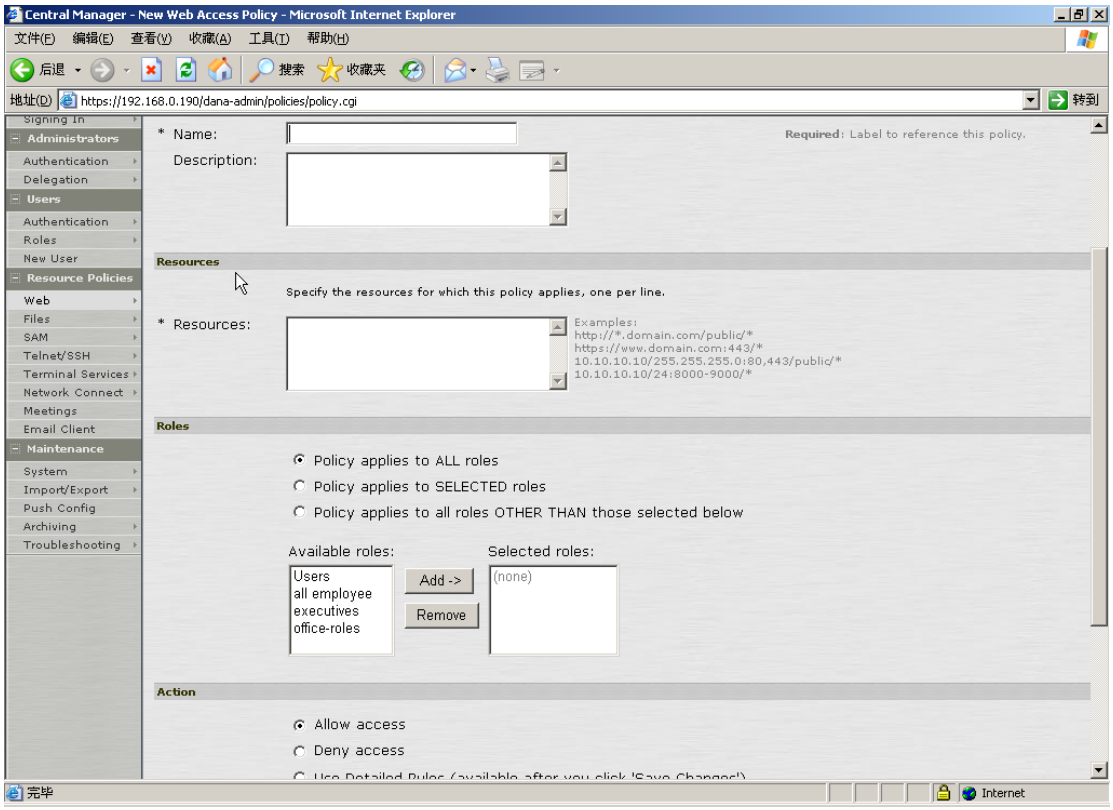
5.1、Core 和 SAM 的资源访问控制

点击“**Resources Police→Web-→Access Control”**，得到下图：



SSL VPN 会在此添加一个缺省的 Web Access 策略，允许用户访问所有 Web 资源。

点击 **New Policy…**,得到下图，来建立新的 Web Access 策略。



在“**Name**”中填入 Web 资源的名称，在“**Resources**”中加入需要控制的资源，可以根据 Http，Https 协议，URL，或是某段地址池来定义控制的资源，在**“Roles”**中，选择这个资源是针对于哪个角色的，在**“Action”**中选择定义的资源对于选定的角色是否运行其访问。

这样就建立了一条 Web Access 方面资源访问控制。

5.2、SAM 和 NC 的资源访问控制

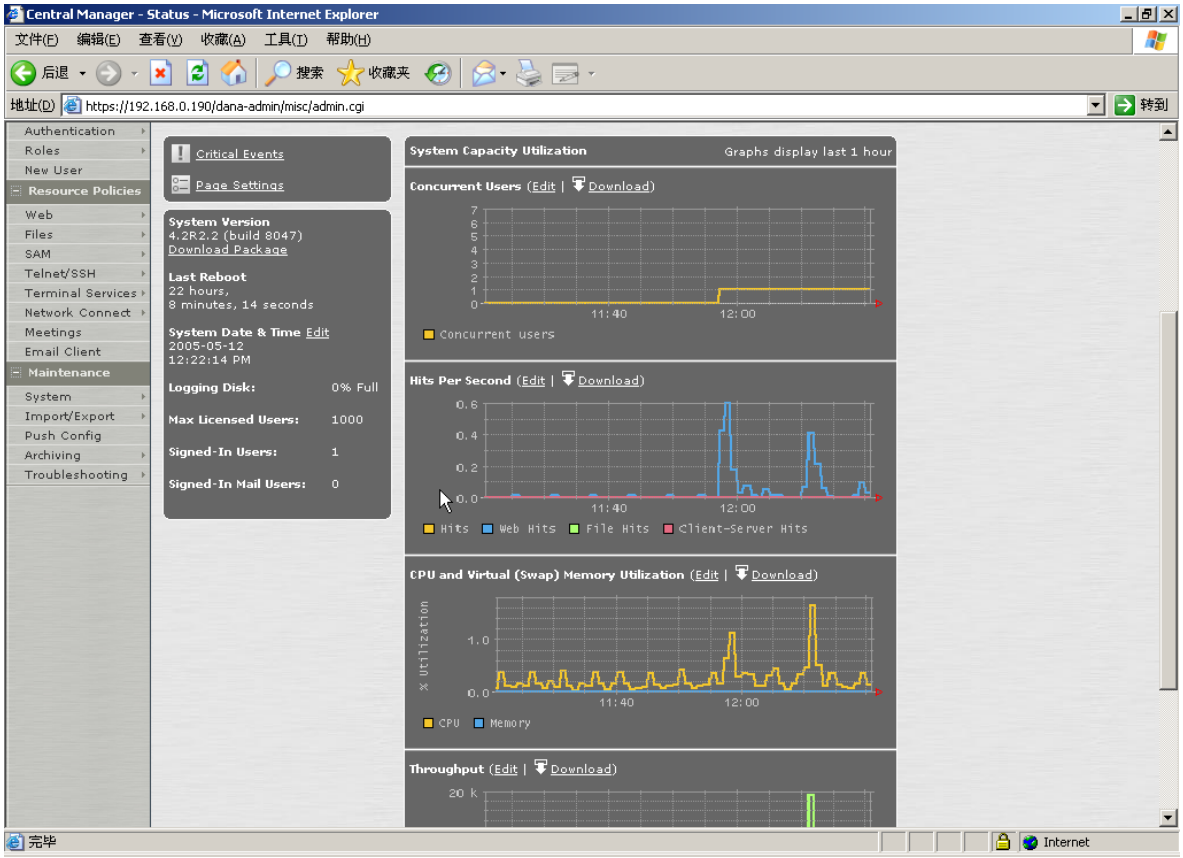
分别点击“**Resources Police→ SAM-→ Access Control”和“Resources Police→ Network Connect-→ Network ConnectAccess Control”**，就可以 SAM 和 NC 两个模块的资源访问控制界面。

它们的配置方法基本和 Web Access 的控制是一样的，只是在 SAM 中更侧重在 TCP 端口和 IP 的资源控制，而在 NC 中则更侧重在对不同协议如，IP，TCP，ICMP，UDP 等方面的 ACL 控制。

六．设备管理

6.1、系统概览

Juniper 的 SSL VPN 自身的设备管理和监控方式非常简便但也很全面，第一次进入 SSL VPN 管理员界面时，SSL VPN 会展示给管理员一个整个产品的概况图，如下：

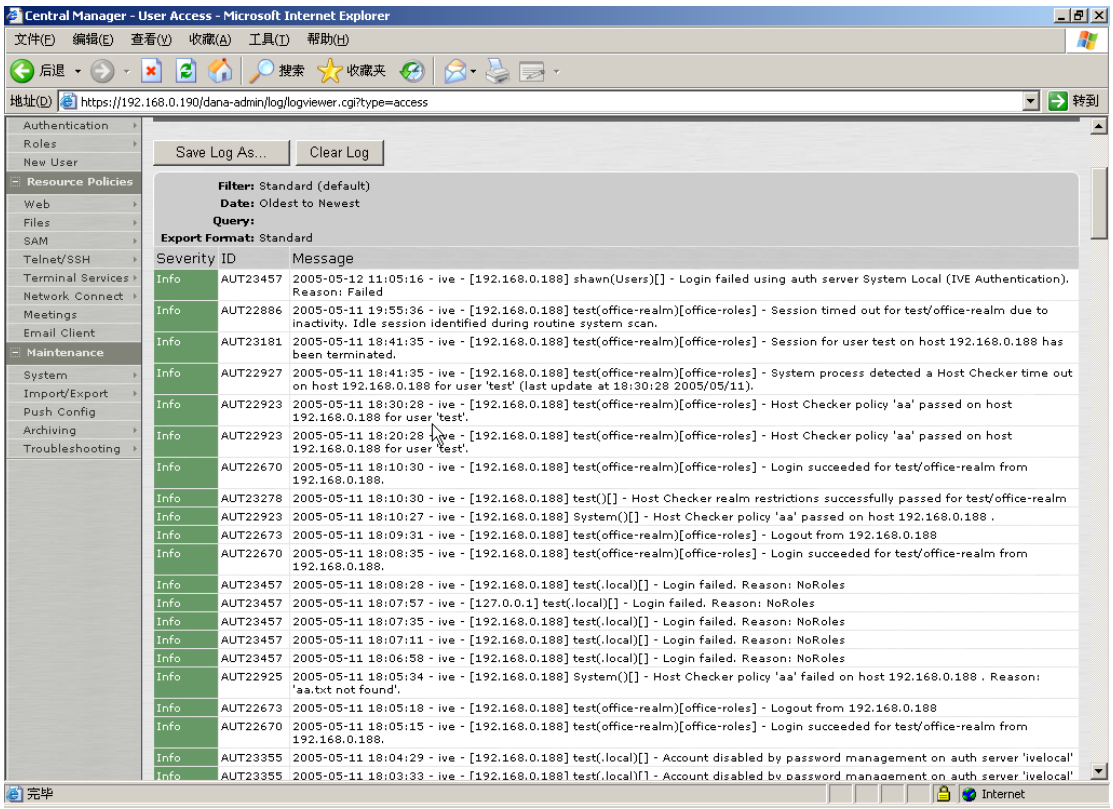


在这副图中，我们可以看到给设备目前的并发用户数，每秒的点击率，CPU 及内存的使用率，吞吐量以及系统软件版本和运行持续时间等信息，对于网管人员来讲能够非常方面的一目了然 SSL VPN 的状态，这个功能是 Juniper SSL VPN 独有的，许多同类厂商的产品不具备这样的功能。

6.2、日志系统

Juniper SSL VPN 的日志系统非常全面，主要分三个方面记录日志，分别是用户日志，管理员日志和系统日志，每部分日志都有非常详尽的记录，包括用户的登陆时间，登陆结果和访问资源的等许多信息，管理员可以自建 Filter 来查看自己感兴趣的日志信息。

点击“**Log/Monitoring-→User Access Log--→log”**，就可以得到用户访问日志。

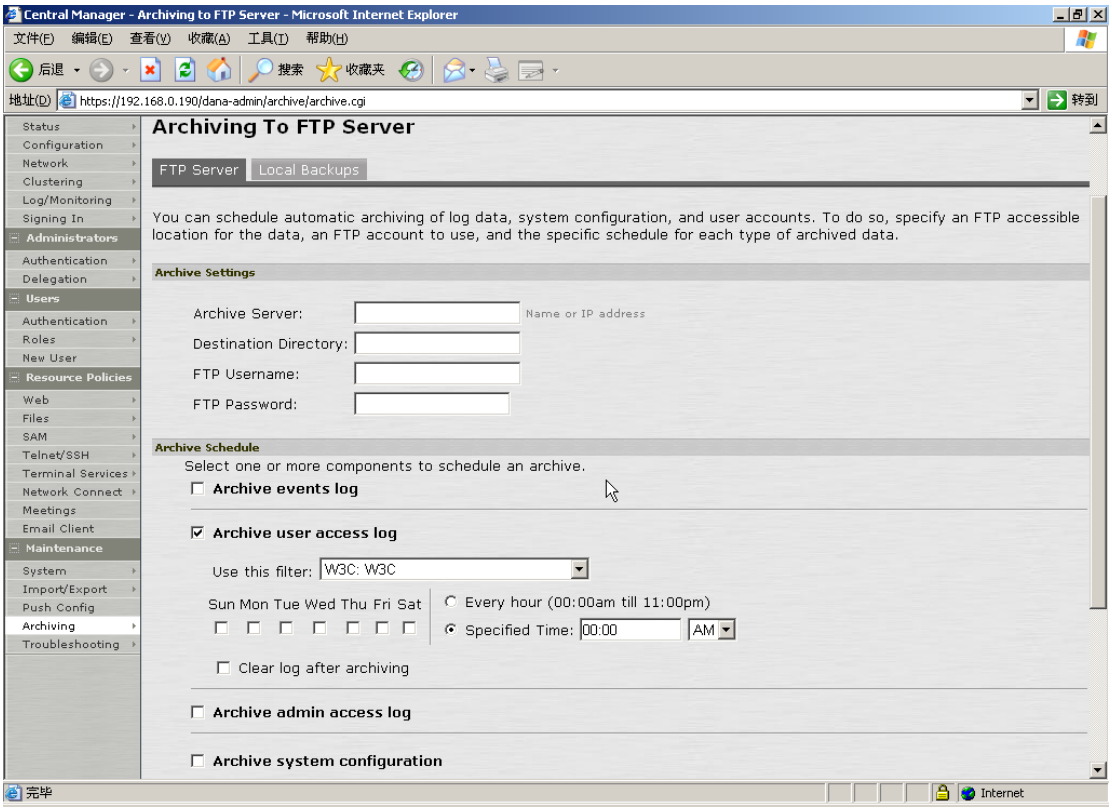


如果想看系统日志和管理员日志，点击：

“ Log/Monitoring-→Event Log--→log ” 和 **“ Log/Monitoring-→Admin Access Log --→log”** 即可。

如果管理员希望对这些日志能够做进一步的分析，例如利用第三方软件来处理这些日志信息的话，SSL VPN 也提供日志上传的功能，如下：

点击**“Archiving-→Ftp Archiving”**,得到下图

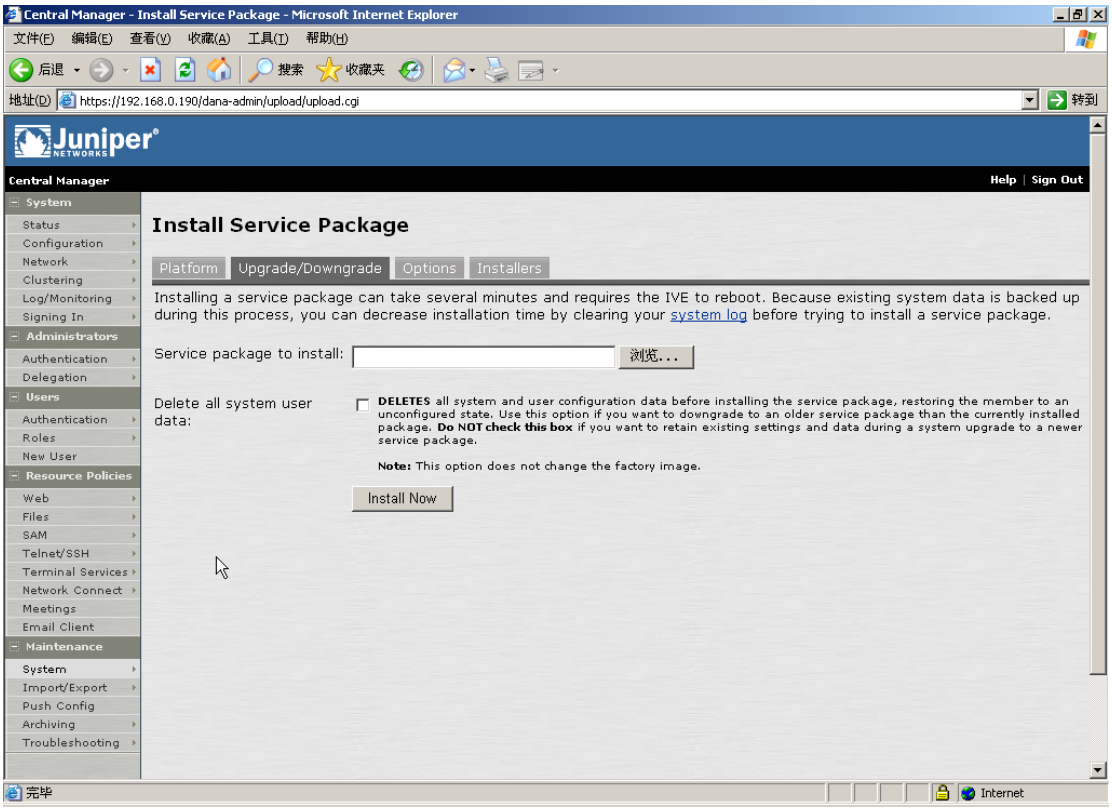


在“**Archives Setting**”中，填入 FTP 服务器的相关信息,再点击“**Archive User Access Log**”，选择记录日志的格式和设置上传的时间，即可完成上传用户日志的设置。

6.3、系统升级

SSL VPN 的系统升级，很简单。

只需要点击“System-→Upgrade/Downgrade”后，在下图中选择:

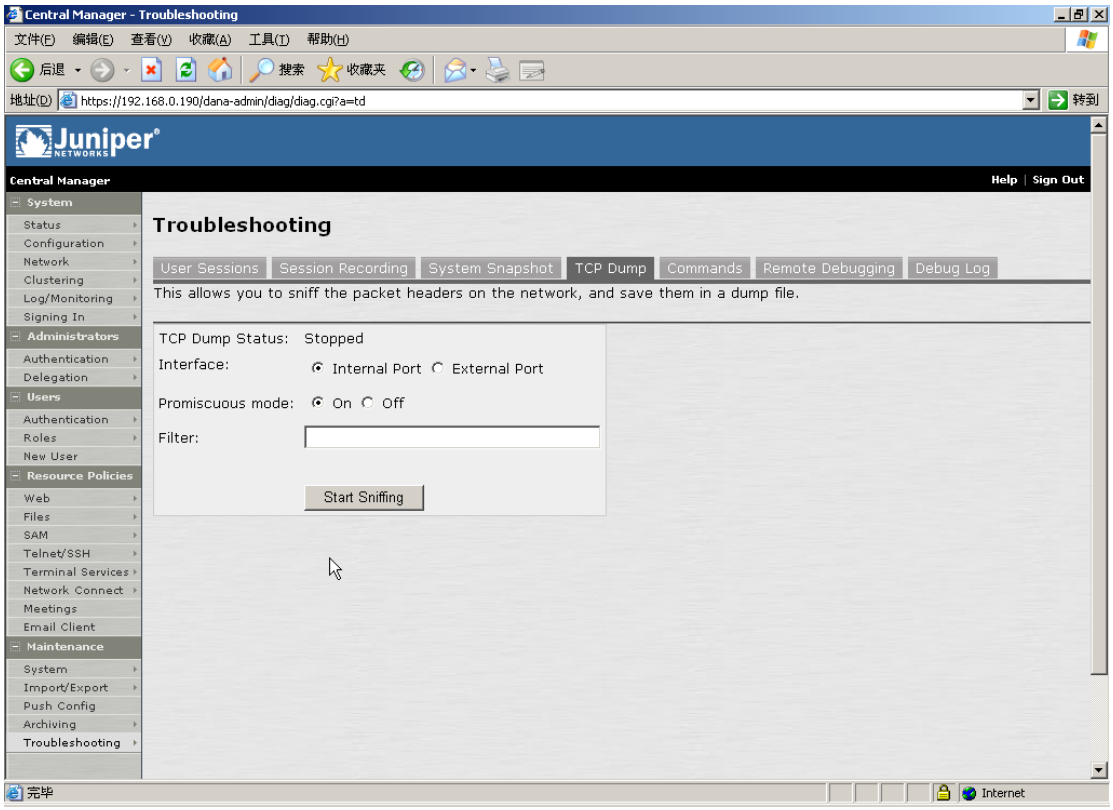


点击**浏览**，在自己的电脑中找到 SSL VPN 升级的软件，然后点击 **Install Now**，即可完成设备的系统升级。

6.4、设备排错

SSL VPN 内置了许多排除的工具，如 TCP DUMP，System Snapshot，Ping 和 Traceroute 等命令，帮助网管人员在发现问题时，能够有充分的工具和手段找出问题原因，解决问题故障并做好预防问题出现的措施。

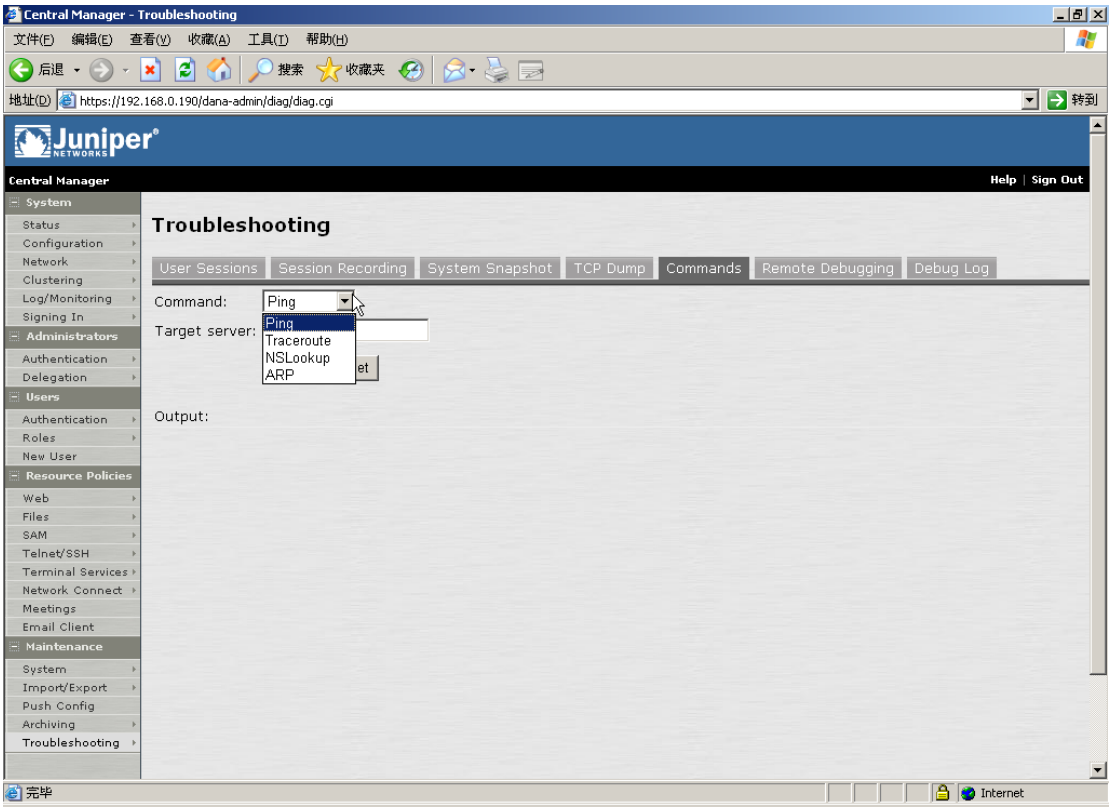
点击**“Troubleshooting--→Tcp Dump”**，得到下图：



在进行 Tcp Dump 时，选择在 SSL VPN 的内口或外口进行 Sniffer，然好点击**“Start Sniffing”** 就可以开始收集数据包啦。

收集一段时间后，点击**“Stop Sniffing”**，即可以停止收集，SSL VPN 会提示用户把收集后的数据文件存储在管理者的计算机上。这个文件可以用 Ethereal 软件打开。

点击**“Troubleshooting--→Commands”**，得到下图：



SSL VPN 支持利用 Ping，Traceroute，Nslookup 和 ARP 这四个命令进行网络层次的排除。

在“**Command**”中，选择相应的命令，在“**Target Server**”中填入目标 IP 地址或是域名，点击 OK，开始执行命令。

在“**Output**”中可以看到这个命令执行的结果。