# Juniper SSL VPN

配置手册

ᅼ.	初始化设置	.3
	1.1、通过 Console 连接 SSL VPN	.3
	1.2、填写初始化信息	.3
	1.3、使用浏览器连接 SSL VPN	.5
二.	SSL VPN 基本设置	.6
	2.1、网络接口设置	.6
	2.2、设置 SSL VPN 的 License	.6
	2.3、添加用户认证服务器	.7
	2.4、添加认证用户	.9
	2.5、添加 SSL VPN 的认证域1	1
Ξ.	角色映射和功能模块1	13
	3.1、添加角色1	13
	3.2、角色映射1	5
	3.3、功能模块1	6
四.	使用 SSL VPN 的各个功能模块1	8
	4.1、使用 Core 功能模块1	8
	4.2、使用 SAM 功能模块1	9
	4.3、使用 Network Connect 模块2	23
五.	资源访问控制	26
	5.1、Core 和 SAM 的资源访问控制	26
	5.2、SAM 和 NC 的资源访问控制2	27
六.	设备管理2	28
	6.1、系统概览	28
	6.2、日志系统	29
	6.3、系统升级	30

# 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:

🗿 Secure Access 55L VPN - Microsoft Internet Explorer	
文件(E) 编辑(E) 查看(Y) 收藏(A) 工具(I) 帮助(H)	A.
Ġ 后退 • 🕤 - 💌 😰 🏠 🔎 搜索 🧙 收藏夹 🍪 😥 • 🌺 🔜 •	
地址(D) 🝘 https://192.168.0.190/dana-na/auth/url_admin/welcome.cgi	▼ 🔁 转到
	A
Welcome to the	
Secure Access SSL VPN	
Username Please sign in to begin your secure session.	
Password	
Sim In	
Note: This is the Administrator Sign-In Page.	
If you don't want to sign in as	
an Administrator, return to the standard Sign-In Page.	
	<b>_</b>
e) 完毕	🔒 🥶 Internet

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:

🎒 Central Manager - 1	Internal Port - Microsoft Internet Explore	er		_ 8 ×	
文件(E) 編録(E) 査看(Y) 收歳(A) 工具(I) 帮助(H)					
🕒 后退 🔹 🕥 🗸	🗙 💈 🟠 🔎 搜索 🤺 收藏夹	🥝 🙈 - 🌭 🔜 -			
地址(D) @ https://192	.168.0.190/dapa-admin/petwork/petwork-port.	coi?name=internal%cmbClusterSelector=	localbost2&name=external		
		cgi nano-incornatorino ciasco soloccor-			
	r			_	
Central Manager				Help   Sign Out	
- System					
Status >	Network				
Configuration >					
Network >					
Log/Monitoring	Overview Internal Port Exte	ernal Port 🛛 Hosts 🔹 Network 🤇	Connect		
Signing In	Settings   Virtual Ports   Stat	ic Routes   ARP Cache			
- Administrators	Enter the network settings and a	click the Save Changes butter	and the bettern of the page		
Authentication >	Enter the network settings and t	click the save changes buttor	r at the bottom of the page.		
Delegation >	Port Information				
- Users					
Authentication >	IP Address:	192.168.0.190			
Roles >	Netmask:	255.255.255.0			
New User					
Resource Policies	Default Gateway:	192.168.0.254			
Web >	Link Speed:	Auto 💌			
SAM >	Note: If you need to specify	static routes, you can do so on the	e <u>Static Routes</u> page.		
Telnet/SSH →					
Terminal Services +	Advanced Settings				
Network Connect →					
Meetings	ARP Ping Timeout:	5 seconds	3 to 300 seconds		
Email Client	MTU:	1500 bytes	Maximum Transmission Unit (576 to 1500)		
Import/Export	Save changes?	N			
Push Config		4			
Archiving +	Save Changes				
Troubleshooting >					
				-	
(2) 完毕				🕑 Internet	
	🖸 🕼 🕶 🔍 🔿 🚳 🛛 🙆 Office M		R) Defense	« 🖂 🖪 🖓 🔧 Ø., 18:21	
<u> </u>					

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:

	▼ ♪ 转到
Network       Licensing       Licensing       Security       Certificates       NCP       Client Types         Note that entering your license key signifies that you have read and agree to the terms described in the license agree to the terms described in the lic	▼ ➡ 转到
Network       Licensing       Security       Certificates       NCP       Client Types         Clustering       Signing in       Note that entering your license key signifies that you have read and agree to the terms described in the license and agree to the terms described in the license and agree to the terms described in the license and agree to the terms described in the license and agree to the terms described in the license and agree to the terms described in the license and agree to the terms described in the license and agree to the terms described in the license and agree to the terms described in the license and terms described in terms described in the license and terms described in terms described in the license and terms described in terms descr	areement.
Network         Licensing         Security         Certificates         NCP         Client Types           Clustering         Log/Monitoring         Note that entering your license key signifies that you have read and agree to the terms described in the license are	areement.
Log/Monitoring > Signing In >> Note that entering your license key signifies that you have read and agree to the terms described in the license ag	preement.
Signing In Note that entering your license key signifies that you have read and agree to the terms described in the license at	areement.
200 A desire in the second	
Kommersators     Company Name:	
Religion + NetScrap Evaluation 4 0 43050 4 V	
Authentication , LUCIISE REV(S).	
Roles >	
New User	
Web >>	
Files	
SAM >	
Terminal Saviest	
Network Connect >	
Meetings Product Summary	
Email Client Model: NetScreen-SA-3050 Advanced - 1000 Simultaneous Users	
Key: star era panorama windfall world currency operation	
System     Company: NetScreen Evaluation 4.0 A3050 4 Week Ext.     Imod Left: Dire	
Push Config Max Concurrent Users: 1000	
Archiving >	
Troubleshooting Upgrade License	
UPG-M10 - 10 Simultaneous Users - 5 Simultaneous Meetings	iours 🗙 –
Key: vista tomotrow surface toy wrench plasma sarah	
Central Manager for Secure Access - 1 Device License will expire in 26 days and 22 h	iours 🗙
Key: star far rye ranger radar jacket saffron	
UPG-NC Network Connect License will expire in 26 days and 22	iours 🗙
I Kevi oak script sapphire windfall quartz welcome lookout	Internet
	1 4 1 2 0 10.00

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

🦉 Central Manager - Signing In - Microsoft Internet Explorer	
文件(E) 编辑(E) 查看(Y) 收藏(A) 工具(I) 帮助(H)	🥂 🖉
😋 后退 • 🕥 - 💌 📓 🏠 🔎 搜索 🤺 收藏夹 🧐 🔗 - چ 🔜 -	
地址(D) 🕘 https://192.168.0.190/dana-admin/auth/listServers.cgi	▼ 🗦 转到
Central Manager	Help   Sign Out
- System	
Status Signing In	
Configuration >	
Network > Sign-in Policies Sign-in Pages Servers	
Clustering >	
Log/Monitoring >	
Administrators	
Authoritation	
Delegation , Authentication/Authorization Servers	Туре
Administrators	IVE Authentication
Authentication	IVE Authentication
Roles >	TUE Authentienties
New User	IVE Authentication
Resource Policies	
Web >	
Files >	
SAIM P	
Terminal Services >	
Network Connect >	
Meetings	
Email Client	
Aintenance	
System >	
Import/Export >	
Push Config	
Indules noting *	
	<u> </u>
	🔒 😫 Internet
🏂 开始 📔 🕑 🧿 🙆 🛐 👅 🍺 🕥 😻 📙 🖸 Office 🛛 🖉 Centr 📴 Produ 🦉 Defen	🔟 IVE 4 🗐 Junipe 🗀 SSL VPN 📗 🛐 🦿 < 💰 🏂 🧶 18:57

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: lveLocal)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:

🚰 Central Manager - Servers - Microsoft Internet Explorer	
	N
🚱 后退 🔹 🛞 🖌 🔎 搜索 🤺 收藏夹 🚱 🔗 😓 🗸	
地址(D) @ https://192.168.0.190/dana-admin/user/find.cgi?selauthserver=1&authname=ivelocal&authtype=Local	▼ 🗦 转到
Central Manager	Help   Sign Out
E System Status Configuration Intervention	
Clustering Settings Users Admin Users	
Signing In	rs Undate
Delegation	
Users New Delete	
Roles  Ver Username	Name
E Resource Policies	ceo
Web iack	Upspecified Name
Files I lui	Unsnerified Name
Telnet/SSH >	
Terminal Services >	user
Network Connect >	
Email Client	
🗏 Maintenance	
System >	
Import/Export >	
Push Config Archiving	
Troubleshooting >	
	<b>•</b>
· · · · · · · · · · · · · · · · · · ·	
🍠 开始 📔 🕑 🥑 🔕 🛐 🕞 🌖 🎒 🚺 Office Mail - M 🤌 IT 售前论坛! 🖗 Central Ma	ana 🗀 Working Files 🛛 🗟 Juniper SSL V 🛛 🛗 😨 ኛ ĸ 💋 🏂 16:47

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 lveLocal)

中添加一个用户,如下图:

- System	
Status 🔸	Servers > ivelocal >
Configuration +	New Local User
Network 🕨	
Clustering +	Username:
Log/Monitoring >	
Signing In 🔶 🔸	Full Name:
- Administrators	Authenticate using: ivelocal
Authentication +	
Delegation +	
- Users	Password:
Authentication >	Confirm Password:
Roles >	
New User	
- Resource Policies	Require user to change password at next sign in
Web →	Save Changes
Files >	

添加用户名和密码后,认证服务器 lvelocal 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:

🖉 Central Manager - I	Authentication - Microsoft Internet Explo	rer	_ 8 ×
文件(E) 编辑(E) 查	著(⊻) 收藏( <u>A</u> ) 工具(T) 帮助(H)		
Ġ 后退 🔹 💮 🕤	💌 💈 🏠 🔎 搜索 🥎 收藏夹	🥴 🔗 🦫 🗸	
地址(D) 🍯 https://192	.168.0.190/dana-admin/realm/listRealms.cgi		▼ → 转到
Status >	New Authentication R	ealm	
Configuration >			
Network >			
Log/Monitoring	Name:		Label to reference this realm
Signing In	Description:		
Administrators	Description.	A	
Authentication >		-	
Delegation >			
- Users			
Authentication →		When editing, start on the Role Mapping	page
Roles >			
New User	Servers		
Resource Policies			
Web >	Specify the servers to use for authenti-	cation and authorization. To create or manage servers	, see the <u>Servers</u> page.
Files >			
SAM →	Authentication:	ivelocal 🔹	Specify the server to use for authenticating users.
Terminal Services b	Directory/Attribute:	None -	Specify the server to use for authorization.
Network Connect +	Accounting	Nana	Constitution and the uses for Diadius association
Meetings	Accounting.	INOTE	specify the server to use for Kadius accounting.
Email Client			
Maintenance	Additional authentication serv	/er	
System >			
Import/Export >	Sign-in page (the labels for these input	ation server for single sign-on (SSQU purposes. The a ts are specified by the sign-in page), or they can be p	dditional credentials can be specified by the user on the re-defined below, in which case the user will not be
Push Config	prompted for the credential.		
Troublesheating			
modbleshooding /	Authentication #2:	None	
	Username is:	<ul> <li>specified by user on sign-in page</li> </ul>	
		C predefined as:	
	Password is:	<ul> <li>specified by user on sign-in page</li> </ul>	
<b>⑧</b> 完毕			🛛 🔤 🚔 💓 Internet

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 lvelocal 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:

🚰 Central Manager - Roles - Microsoft Internet Explorer								_ 8
文件(E) 編編(E) 查看(Y) 收藏(A) 工具(I) 帮助(H) 🧤								
🚱 后退 • 🕥 - 🗾 💈 🏠 🔎 搜索 🧙 收藏夹 🤣 忌 • چ 🕞 •								
地址(D) 🕘 https://192.168.0.190/dana-admin/roles/roles.cgi							•	▶ 转
Central Manager						Hel	o ∣ Si	gn Out
E System								-
Status , Roles								
Configuration >								
Network > New Pole Dunlicate Delete Default Ontions								
Clustering								
Log/Monitoring >			En	able	d set	tting	s	
Signing In						ő		
Role		S			н	No.	w	
Delegation >	58	ptio			et/s	euic	Buij	-
Elegadon /	ptic	0 1	éb.	AM SAM	ele	ern	Aeet	E O
	00		~ 1	L 0.	-	F	~	w 2
Roles >	•	•						
New User executives	~	~						
Resource Policies								
web , office-roles	Ý	~	<b>~</b> '	· ·				~
Files Vusers	~	~	•					
SAM > System created Users role.								
Teinet/SSH >								
Network Connect >								
Meetings								
Email Client								
🔚 Maintenance								
System >								
Import/Export >								
Push Config								
Archiving >								
Troubleshooting >								
2 完毕					1	Intern	et	

# 点击 New Role 添加一个角色:

🔄 Central Manager - Roles - Microsoft Internet Explorer 📃 🗗 🗙					
文件(E) 編編(E) 查看(Y) 收藏(A) 工具(I) 帮助(H) 7					
③ 后退 • ③ ▼ 区 3 1 → 搜索 ☆ 收藏夹 ④ ② • 曇 □ ▼					
推址DD 🕘 https://192.168.0.190/dana-admin/roles/roles.cgi 🗾 🖻 转到					
🖻 System					
Status , Roles >					
Configuration New Role					
Network >					
Custering ,					
- Administrators					
Authentication  Description:					
Delegation >					
🖻 Users					
Authentication >					
Roles >					
Nev User Options Options					
Resource Policies     Session and appearance options are specified in <u>Default Options</u> . Check the following if this role should override these defaults.					
Web >					
SAM Session Options					
Telnet/SSH > VI Options					
Terminal Services >					
Network Connect > Access features					
Meetings Check the features to enable for this user role, and specify any role-based options. Note that features disabled here may be granted by					
Email Clent other roles assigned to the user.					
Import/sport Web					
Push Config Files, Windows					
Archiving Files UNIX /NES					
Troubleshooting					
C Windows version					
C Java version					
Telnet/SSH					

### 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:

🚰 Central Manager - i	Authentication - Rules - Microsoft Internet Explorer							
文件(E) 编辑(E) 查	Ē看(⊻) 收藏(A) 工具(I) 帮助(H)							
😋 后退 • 🕘 - 🛃 😰 🏠 🔎 搜索 👷 收藏夹 🚱 🔗 • 🍃 🖂 -								
地址(D) 🍯 https://192	.168.0.190/dana-admin/realm/rules.cgi?realmType=user&PolicyRealm=4		▼ 🗲 转到					
	r°							
Central Manager			Help   Sign Out					
System Status Configuration Network	User Authentication Realms > office-realm							
Clustering → Log/Monitoring →	General Authentication Policy Role Mapping							
Signing In → - Administrators	Specify how to assign roles to users when they sign in. U	sers that are not assigned a role wil	not be able to sign in.					
Authentication → Delegation → Users	New Rule Duplicate Delete 🕇 🖶		Save Changes					
Authentication   Roles	When users meet these conditions	assign these roles	Rule Name Stop					
New User	1. <u>username is</u> "*"	→ office-roles						
Resource Policies								
Web → Files → SAM →	When more than one role is assigned to a user:							
Telnet/SSH →	• Merge settings for all assigned roles	$\mathbb{R}$						
Network Connect >	C User must select from among assigned roles							
Meetings Email Client	Meetings C User must select the sets of merged roles assigned by each rule Email Clent							
Maintenance     Note: Users that do not meet any of the above rules will not be able to sign into this realm.								
Import/Export >								
Push Contig Archiving								
Troubleshooting >								
宗毕								

选择 New Rule...

🎒 Central Manager - A	Authentication - Microsoft Internet Explorer
文件(E) 编辑(E) 查:	看(火) 收藏(A) 工具(1) 帮助(出) 7
🔇 后退 🔹 💮 🖌	🞽 😰 🏠 🔎 搜索 👷 收藏夹 🚱 😥 - 🌭 📄 -
地址(D) 🕘 https://192.	168.0.190/dana-admin/realm/rolemapping.cgi?newPolicyRoleMapping=1&PolicyRealm=4&realmType=user 🔽 🎅 转到
E ZNETWORKS	• • • • • • • • • • • • • • • • • • •
Central Manager	Help   Sian Out 📹
- System	
Status	User Authentication Realms > office-realm >
Configuration >	Role Mapping Rule
Network >	
Clustering >	Pule based on: Lisemane
Log/Monitoring →	
Signing In →	
- Administrators	Name: Optional (used with the "select the sets of merged roles" setting)
Authentication >	Rule: If username
Delegation >	
- Users	in The If more than one username should match, enter one username per line. You can use * wildcards.
Authentication >	
Roles >	
New User	·
Resource Policies	
Web →	
Files >	then assign these value
SAM →	uten assign utese roles
Terminal Services >	Available Roles: Selected Roles:
Network Connect >	all employee Add > (none)
Meetings	executives
Email Client	office-roles Remove
- Maintenance	Users
System >	
Import/Export >	
Push Config	□ Stop processing rules when this rule matches
Archiving >	
Troubleshooting →	Save changes?
	Save Changes Save + New
, (4) 完毕	

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。

🗿 Central Manager - Roles - Microsoft Internet Explorer								_ 8
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(I) 帮助(H)								
③ 后退 ▼ ③ ▼ ≥  2 授索 ☆ 收藏夹 ↔ 2 小								
地址(D)   https://192.168.0.190/dana-admin/roles/roles.cgi							•	🔁 转到
Status KOIES								
Configuration +								
Network New Role Duplicate Delete Default Options								
Clustering								
Log/monitoring ,			Enal	bled	set	ting	s	
						Ś		
Role		ž			H	ŝ		
Authentication	52	otio			¢S;	in a	ŝ	
Delegation	otio	<u>о</u> 4	ŝ	¥.	e_	Ę	e et i	
Users	őő	5 3	Ē	ŝ	₽	Ĕ	žι	μž
Authentication	¥	~						
Roles								
New User	•	*						
Resource Policies     Office-roles	~	•	~	~				~
Files Users	Ŷ	v .	~	~				
SAM > System created Users role.								
Telnet/SSH >								
Terminal Services >								
Network Connect >								
Meetings								
Email Client								
- Maintenance								
System >								
Import/Export >								
Push Config								
Archiving >								
Troubleshooting >								
			-					-
Linear die Neternas Euclustics 4.0 420E0 4 Wash Euc				Lue	inc	- 1-	auto	Not
Copyright © 2001-2004 Juniper Networks, Inc. All rights reserved.				Jun	ipe	0	001	Net.
						-		
			_			_		
				Ö,	🙂 Ir	ntern	et	

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:

🏄 Central Manager - l	Jsers Roles - Web Bookmarks - Microsoft Internet Explorer	
文件(E) 编辑(E) 查	看(⊻) 收藏(A) 工具(T) 帮助(H)	A
🚱 后退 🔹 💮 👻	🞽 🛃 🏠 🔎 搜索 🥎 收藏夹 🚱 🔗 - چ 🖂 -	
地址(D) 🕘 https://192	168.0.190/dana-admin/user/homepagelist.cgi?role=1113985215.499397.0	💌 ラ 转到
	r°	<u> </u>
Central Manager		Help   Sign Out
- System		
Status >	Roles >	
Configuration >	all employee	
Network >		
Clustering >	General Web Files SAM Telnet/SSH Terminal Services	Meetings Network Connect
Log/Monitoring →	Bookmarks   Ontions	
Signing In →		
- Administrators		
Authentication >		
Delegation →	New Bookmark Duplicate Delete 1 🗣	Save Changes
- Users		
Authentication >	D Declarada	
Roles >	Bookmarks	Resource
New User	1. <u>sina.com</u>	http://www.sina.com/
Resource Policies		Access to: Only this DRL
Web >		
Files >	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	
SAM >		
Teinet/SSH >		
Network Copped		
Meetings		
Email Client		
- Maintenance		
Sustem >		
Import/Export >		
Push Config		
Archiving >	See also Web policies that apply to this role:	
Troubleshooting →		
	Access Control	<u>Caching</u>
一日本		A Distance
10 76°F		j j j j 🗾 🐨 miternet

点击 New BookMark,得到下图:

🚰 Central Manager - I	Users Roles - Web Bookmarks - Microsoft Internet Explorer	_ 8 ×
文件(E) 编辑(E) 查	E看(У) 收藏(A) 工具(I) 帮助(H)	n
( ) 后退 • ( ) •	😰 🛃 💭 搜索 🐈 收藏夹 🚱 😞 - 🤽 🥽 -	
thtth(D) Abtros://192	168.0 190/dana-admin/user/homenanelist.cni?role=1113985215.499397.0	▼ ➡ 转到
- System	In the transmit water premispagement grin the Interstation in State Provider	
Status	Roles > all employee >	
Configuration >	New Web Bookmark	
Network >		
Clustering >		
Log/Monitoring →		
Signing In →	Name:	
Administrators		
Authentication >		
Delegation >		
- Users	*	
Authentication >	1	
Roles >		
New User	* URL: Example: http://www.domain.com/	
Resource Policies		
Web >	Auto-allow	
Files >	Use auto-allow to automatically add this web bookmark for this role to the Web access control policy.	
Telpet/SSH	🗆 Auto-allow Bookmark	
Terminal Services >	C only this LIRI	
Network Connect →		
Meetings	C Everything under this URL	
Email Client		
Maintenance	Display options	
System →	Open the bookmark in a new window	
Import/Export >	Do not display the URL address har	
Push Config		
Archiving >	Do not display the menu and the toolbar	
I roubleshooting >		
	Save changes?	
	Save Changes Save + New	
	indicates required field	·
😂 完毕		📋 😼 Internet

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,

🗟 Central Manager – Users Roles - SAM Applications - Microsoft Internet Explorer	_ 8 ×
文件(E) 編辑(E) 查看(V) 收藏(A) I具(I) 帮助(H)	
③ 局退 • ⊙ - Ⅰ 2 公 /> 搜索 ☆ 收藏夹 经 ⊗ - ≥ □ -	
H811C0 🛃 https://192.168.0.190/dana-admin/cs/cs.cg?role=1113985215.499397.0	🔻 ラ 转到
	-
Central Manager Help	Sign Out
System	
Status , Roles > Configuration , all employee	
Network >	
Log/mintering - General web riles SAW Tellieu/San Terminal Services Meetings Network Connect	
Signing In Applications Options	
E Administrators	
Authentication +	
Delegation  Add Application Duplicate Delete	
- Users	
Authentication >	
in Resource Policies	
Web >	
Files >	
SAM >	
Telnet/SSH >	
Terminal Services >	
Network Connect + For client applications not listed above, specify what servers (if any) should be allowed. These servers will be accessible	to any
Final Client application.	
· Maintenance	
System , Add Server Delete	
Import/Export >	
Push Config Standard servers	
Archiving >	
Troubleshooting >	
資产毕	

# 点击 Add Application,得到下图,

🎒 Central Manager -	Users Roles - SAM Applications - Microsoft Internet Explorer	_ 8 ×
文件(E) 编辑(E) 査	を看(v) 收藏(A) 工具(I) 帮助(H)	
😪 后退 🔹 💮 🕤	🖹 🛃 🏠 🔎 搜索 🧙 收藏夹 🥝 🔗 - 😓 🖂 -	
地址(D) 🍯 https://192	.168.0.190/dana-admin/cs/cs.cgi?role=1113985215.499397.0	💌 🄁 转到
Status → Configuration →	Roles > all employee > New Application	
Network → Clustering →	Save Application Save + New	
Signing In		
Administrators	Details	
Authentication +	* Name:	
Delegation +		
- Users		
Authentication +		
Roles +	· · · · · · · · · · · · · · · · · · ·	
New User		
<ul> <li>Resource Policies</li> </ul>	Analyzation Tuno N	
Web >	Application Type 2	
Files >	C Standard application 🕜 Custom application	
Telnet/SSH >		
Terminal Services +	* Filename:	
Network Connect >	Example: "telnet.exe", accepts * wildcards.	
Meetings	Path: If you specify a path, it must be absolute.	
Email Client	MD5 Hash:	
- Maintenance		
System +		
Import/Export >	Note: You can use symbolic tokens to provide paths relative to certain standard locations.	
Push Config		
Troublesheating	Save Application?	
	Save Application Save + New	
	Save Thew	
	* to detail to see the detail	
	indicates required nero	
Licensed to NetScreer	r Evaluation 4.0 A3050 4 Week Ext. Junipe	wour Net.
Copyright © 2001-20	04 Juniper Networks, Inc. All rights reserved.	0
会 完毕		ternet

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:

🎒 Central Manager - I	Users Roles - SAM Applications - Microsoft Internet Explorer	_ 8 ×
文件(E) 编辑(E) 查	至看(⊻) 收藏(A) 工具(T) 帮助(H)	1
🕞 后退 🔹 💮 🗸	🖹 🗟 🏠 🔎 搜索 🧙 收藏夹 🚱 🔗 • 🌽 🖂 -	
地址(D) 🙆 https://192	2.168.0.190/dana-admin/cs/cs.cgi?role=1113985215.499397.0	▼ ラ 转到
Status >	Roles > all employee >	•
Configuration >	New Application	
Network →		
Clustering →	Save Application Save + New	
Log/Monitoring →		
Signing In →	Details	
🗄 Administrators		
Authentication >	* Name:	
Delegation >	Description:	
- Users		
Authentication >		
Roles →	·	
New User		
Resource Policies		
Web →	Application Type	
Files >	C [Standard and in this ] C Custom and institut	
SAM →		
Telnet/SSH >		
Terminal Services →	* Application: Citrix NFuse	
Network Connect >	Lotus Notes	
Freedings	Notes Soft Outlook/Exchange	
Maintenance	Net Dios nie blowsnig	
System >		
Push Coofig	Save Application?	
Archiving >	Save Annlication Save + New	
Troubleshooting >		
	* indicates required field	
Licensed to NetScreen	n Evaluation 4.0 A3050 4 Week Ext. 04 Juniper Networks, Inc. All rights reserved.	Juniper Gour Net.
		-
		A at the set
10元半		📄 🚽 Internet

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,

🗿 Central Manager - Users Roles - SAM Applications - Microsoft Internet Explorer	_ 12  ×
文件(E) 編録(E) 查看(Y) 收藏(A) 工具(I) 帮助(H)	
🔇 后退 • 🕘 - 💌 😰 🏠 🔎 捜索 🧙 收藏夹 🤣 🝰 • 🍃 🖂 •	
地址(D) @ https://192.168.0.190/dana-admin/cs/cs.cgi?role=1113985215.499397.0 🝷	🔁 转到
Central Manager Help   Si	gn Out
E System	
Status Roles > all employee	
Network >	
Clustering General Web Files SAM Telnet/SSH Terminal Services Meetings Network Connect	
Signing In Applications   Options	
- Administrators	
Authentication >	
Delegation > Add Application Duplicate Delete	
Authentication >	
Roles WSAM supported applications	
New User	
WeD >	
SAM >	
Telnet/SSH >	
Terminal Services >	
Network Connect > For client applications not listed above, specify what servers (if any) should be allowed. These servers will be accessible to	any
Meetings client application.	
Add Server Delete	
Upper/Export >>	
Push Config D WCAM allowed servers	
Archiving	
Troubleshooting	
资完毕	

### 点击 Add Server...,得到下图,

🚈 Central Manager - Users Roles - SAM Applications - Microsoft Internet Explorer	_ 8 ×
文件(E) 编辑(E) 查看(V) 收藏(A) 工具(I) 帮助(H)	A
😋 后退 • 🕑 - 💌 💈 🏠 🔎 搜索 🤺 收藏夹 🤣 🔗 • چ 🕞 -	
地址(D) 🕘 https://192.168.0.190/dana-admin/cs/cs.cgi?role=1113985215.499397.0	💌 🇲 转到
Central Manager	Help   Sign Out
- System Status Configuration Netvork	
Clustering > Name:	
Log/Monitoring > Description:	
I Administrators	
Authentication >	
Delegation >	
🗄 Users	
Authentication   * Server: Name or IP address You can use * or ? wildcard	s. You can also specify with a netmask or prefix-length
Roles > (10.10.10.20/255.255.255	0 or 10.10.10.20/8).
New User Port(s): You can specify multiple po	rts as comma-delimited lists (1,2,3,4) or ranges (1-4).
Files Save Changes Save + New	
SAM >	
Telnet/SSH > * indicates required field	
Terminal Services >	
Network Connect >	
Email Client	
🗏 Maintenance	
System >	
Import/Export >	
Push Config	
Archiving >	
Troubleshooding 7	
	📄 📄 💕 Internet

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:

🎒 Central Manager - N	Network Connect Connection Profiles - Microsoft Internet Explorer			_ 8 ×
文件(E) 编辑(E) 查	活(⊻) 收藏(A) 工具(I) 帮助(H)			
🕞 后退 🔹 🕥 🗸	🞽 🛃 🏠 🔎 搜索 🥎 收藏夹 🚱 😒 - 🌺 🔜 -			
地址(D) 🕘 https://192	.168.0.190/dana-admin/policies/policy.cgi?policy_type=nc-pools			💌 ラ 转到
	r°			-
Central Manager			Help	Sign Out
- System				
Status >	Network Connect Connection Profiles			
Configuration >				
Network >	Access NC Connection Profiles Split Tunneling Networks			
Clustering >				
Log/Monitoring →	Show profiles that apply to: All roles 🔽 Update			
Signing In				
Administrators	View/Modify NC Server side configuration			
Authentication >	view/mouny ne beiver side configuration			
- lisers				
Authoptication	New Profile Duplicate Delete		Save C	nanges
Roles >				Applies
New User	Profiles	IP Addresses	DNS Settings	to role
- Resource Policies	1. office-in-pool	192.168.0.12-22	No proxy server	office-
Web >			Default Sourch client DNS convers first	roles
Files >			search client Diro servers hist	
SAM →				
Telnet/SSH →				
Terminal Services →	Kaubaavd abartarta			
Network Connect →	Use "<" and ">" keys to move selected items up and down (remember to cli	k Save Changes after rea	rranging the list). Use Ctrl+Plus and Ctr	H+Minus to
Email Client	expand and collapse all items.			
– Maintenance				
System				
Import/Export >				
Push Config				
Archiving >				
Troubleshooting >				
				-
② 完毕			🔒 🙆 Interna	et

# 点击 New Profile....,得到下图:

🚰 Central Manager - M	iew Network Connect Connection Profile - Microsoft Internet Explorer	
文件(E) 编辑(E) 查	者(⊻) 收羅(A) 工具(I) 帮助(H)	
승 后退 🔹 💮 🐇	🗙 😰 🏠 🔎 搜索 🤺 收藏夹 🚱 忌 - 🌭 🤜 -	
地址(D) 🕘 https://192	168.0.190/dana-admin/policies/policy.cgi	🗾 🏓 转到
System           Status         >           Configuration         >           Network         >           Clustering         >           Log/Monitoring         >           Signing In         >	Network Connect Connection Profiles > New Profile	
Administrators  Authentication Delegation Users  Authentication Roles	* Name: Description:	Required: Label to reference this profile.
New User	IP address pool	
Resource Policies      Web     Files     SAM     Telnet/SSH     Terminal Services     Network Connect	* IP address pool:       Examples: 10.10.10.10-100 10.10.10.50	L3
Email Client	Network Connect proxy server configuration	
Maintenance System	Specify a proxy server for use in this connection profile, if appropriate.	
Import/E×port → Push Config	• No proxy server • Automatic (PAC file on another server)	
Troubleshooting	Server address:	
	C Manual configuration	
	Server: Port: 0	
A 完毕		A Internet

Central Manager - New Network Con 文件(F) 編号(F) 本吾(y) 收確(A)	nect Connection Profile - Microsoft Internet Explorer
地址(D) @ https://192.168.0.190/dana-a	min/policies/policy.cgi 고 화회
	To override the standard DNS settings, specify custom settings for this profile here.
Primary DI	NS: IP address
Secondary	y DNS: IP address
DNS Doma	in(s): Example: "company.com, company.net"
WINS:	Name or IP address
DNS search or	der
	If split tunneling is enabled, select the DNS server search order.
	Search client DNS first, then IVE
	C Search IVE DNS servers first, then client
Roles	
	Policy applies to ALL roles
	C Policy applies to SELECTED roles
	C Policy applies to all roles OTHER THAN those selected below
	Available roles: Selected roles:
	Users all employee executives office-roles
Save changes	
	Save Changes Save as Copy
● 完毕	📄 💧 👔 Internet

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

🏄 Central Manager - W	Yeb Acce	ss Policies - Mic	rosoft Internet Explorer									
文件(E) 编辑(E) 查:	看(⊻) 屹	(藏( <u>A)</u> 工具( <u>T</u> )	帮助(出)			🥂						
😪 后退 🔹 💮 👻	× 2	🏠 🔎 捜	素 🥎 收藏夹 🚱 🔝 -									
地址(D) 🕘 https://192.3	168.0.190	I/dana-admin/polici	es/policy.cgi?policy_type=web-access			💌 🄁 转到						
	r°					<u>^</u>						
Central Manager						Help   Sign Out						
- System												
Status >	Web	Access	Policies									
Configuration >												
Network >	Access Caching Java Rewriting Remote SSO SAMI Web Proxy Launch ISAM Ontions											
Clustering +					,	and the second se						
Log/Monitoring →	Show	policies that	apply to: All roles 🔽 Update									
Signing In 🔸	_											
Administrators			n r . I n . I t t . I									
Authentication >	Nev	v Policy	Duplicate Delete 1			Save Changes						
Delegation >	-											
🖃 Users	M	Policies		Action	n Resources	Applies to role						
Authentication +	□ 1.	Initial Ope	n Policy	Allow	*;*/*	All roles						
Roles >		Allows all we	b browsing! Remove to restrict access to web									
- Resource Policies		(coodicco)										
Web Files												
SAM >	Kaubaa	rd chorteuter										
Telnet/SSH >	Use "<"	" and ">" keys t	o move selected items up and down (regnem	ber to click Save (	Changes after rearrang	ing the list). Use Ctrl+Plus and Ctrl+Minus to						
Terminal Services >	expand	l and collapse al	l items.									
Network Connect →												
Meetings												
Email Client												
- Maintenance												
System >												
Import/E×port →												
Push Config												
Archiving +												
Troubleshooting →												
三字 完毕						🔒 🥑 Internet						

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。

Central Manager - I	New Web Access Policy	- Microsoft Internet Explorer
又仟(E) 编辑(E) 鱼	皆者(⊻) 収臧(A) ⊥具(	
🤇 后退 🔹 💮 🐐	🞽 🛃 🏠 🔎	捜索 ☆ 收蔵来 🧐 🔕 🕏 🏷 🔜 -
地址(D) 🕘 https://192	2.168.0.190/dana-admin/po	Jicies/policy.cgi 🗾 🛃
Signing In	* Name:	Required: Label to reference this policy,
	Description:	
Delegation >	Description.	A
🖃 Users		
Authentication		
Roles >		
New User	Resources	
🗏 Resource Policies	R	Specify the recovered for which this policy applies and por line
Web →		speary the resources for which this policy applies, one per line.
Files >	* Resources:	Examples:
Telpet/SSH		https://www.domain.com/443/*
Terminal Services +		10.10.10.10/255.255.255.080,443/public/*
Network Connect →		
Meetings		
Email Client	Roles	
Maintenance	-	Policy applies to ALL roles
System >		C Policy applies to SELECTED roles
Push Config		
Archiving >		C Pulicy applies to all roles OTHER THAN those selected below
Troubleshooting >		Available roles: Selected roles:
		all employee
		executives Remove
		office-roles
	Action	
		Allow access
		C Denv access
		C Use Detailed Bulles (qualitable offer you aliab (Caus Changes))
② 完毕		- Internet

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

🚰 Central Manager - A	rchiving to FTP Server - Microsoft Internet Explorer									
文件(E) 编辑(E) 查	看(V) 收藏(A) 工具(I) 帮助(H)									
🔇 后退 🔹 💮 🗸	🗙 😰 🏠 🔎 搜索 ☆ 收藏夹 🥝 🔗 - 🤮 🥽 -									
地址(D) 🕘 https://192.:	168.0.190/dana-admin/archive/archive.cgi									
Status >	Archiving To FTP Server									
Configuration +										
Network →	FTP Server Local Backups									
Log/Monitoring >										
Signing In →	You can schedule automatic archiving of log data, system configuration, and user accounts. To do so, specify an FTP accessible									
🖃 Administrators	location for the data, an FTP account to use, and the specific schedule for each type of archived data.									
Authentication >	Archive Settings									
Elisers										
Authentication >	Archive Server: Name or IP address									
Roles >	Destination Directory:									
New User	ETRUSonamo									
Resource Policies										
Files	FTP Password:									
SAM >										
Telnet/SSH →	Archive Schedule Select one or more commonents to schedule an archive.									
Terminal Services →	Archive events log									
Meetings										
Email Client	✓ Archive user access log									
Maintenance										
System →	Use this filter: I wat: wat									
Push Config	Sun Mon Tue Wed Thu Fri Sat C Every hour (00:00am till 11:00pm)									
Archiving >	AM •									
Troubleshooting →										
	L Clear log atter archiving									
	C Archive admin access log									
	C Archive system configuration									
。 ② 完毕										

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:

Centr	al Manage	er - Tr	oubleshooting	1														_ 8 ×
文件(E)	编辑(E)	查看	昏(⊻) 收藏( <u>A</u> )	工具(I)	帮助( <u>H</u> )													
合品	. • 🕥	-	1 🗈 🏠	▶○ 搜索	🤋 🥎 收藏夹	0	<b>@-</b> 🎍											
地址( <u>D</u> )	🍯 https:/,	/192.1	.68.0.190/dana-	admin/diag/d	iag.cgi?a=td													💌 🄁 转到
<b>(</b> )	Junir	per	,0															
Central	Manager																Help	Sign Out
- Syste	em																	
Statu:	5	Þ	Trouble	shoot	ina													
Confi	guration	Þ																
Netwo	rk	Þ	User Sessi	ons Se	ssion Recordin		/stem Sr	napshot	ТСР	Dump	Comma	nds Re	mote D	Debua	aina	Debuo	a Log	
Cluste	ering	Þ	This allows	you to se	oiff the nacke	t head	ars on th	ne networ	k an	d save	them in	a dumo fi	ilo	_				
Log/M	lonitoring	Þ	THIS allows	you to si	пп пе раске	t neau	ers on u	ie networ		u save	chem m	a uump n	ne.					
Signin	ig In		TOP	<b>O</b> 1-1	Otomo d				-									
- Author	inis tra tors		TCP Dump	Status:	Stopped													
Deleg	ation		Interface:		Internal F	Port C	Externa	al Port										
- User	dion					~~												
Autho	ntication		Promiscuou	is mode:	• on 0 01	TT												
Roles	nacación	•	Filter:															
New L	lser				1													
🗏 Reso	urce Polici	ies																
Web		-			Start Sniffin	g												
Files		Þ				-												
SAM		•																
Telne	t/SSH	Þ			N													
Termi	nal Service	es⊧			42													
Meeti	rk Connec nas	π ,																
Email	Client																	
- Maint	tenance																	
Syste	m	•																
Impo	rt/Export	F																
Push	Config																	
Archiv	ing	Þ																
Troub	leshooting	<b>j</b> →																
																		-
(2) 完毕																<u> </u>	🔮 Intern	et

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:

Central Manager - Troubleshooting	_ 8 ×
文件(F) 編唱(に) 香香(v) 収蔵(A) 工具(T) 帮助(H)	
##1/12 / // // /////////////////////////	> 转到
Help   Sign	Out
a System	
Status Troubleshooting	
Configuration >	
Network > User Sessions Session Recording System Spanshot TCP Dump Commands Remote Debugging Debug Log	
Clustering Osel Jession's Jession's Vestioning System Shapshok, TCP Dump Commands, Kemoke Debugging, Debug Log	
Log/Monitoring Command: Ping	
Signing In * Target server: Ping	
Administrators	
Authentication > NSLookup et	
a de se se contract :	
Authentication > Compart.	
New User	
en Resource Policies	
Web >	
Files >	
SAM ›	
Telnet/SSH >	
Terminal Services >	
Network Connect >	
Frail Clent	
Maintenance	
Sustem >	
Import/Export >	
Push Config	
Archiving >	
Troubleshooting	
	-
う 完 単	

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。