

IT SOLUTIONS & SERVICES



东软 NetEye 集成安全网关快速向导



本向导描述以下内容:

- 1. 安装硬件设备和系统
- 2. 连接设备和管理 PC
- 3. 部署 NetEye 到网络
- 4. 使用向导进行初始化配置
- 5. 使用 WebUI 进行初始化配置
- 6. 使用 CLI 进行初始化配置
- 7. 验证初始化配置
- 8. 常见问题

1. 安装硬件设备和系统

关于硬件安装的详细信息,请参见*东软 NetEye 集成安全网关安装向导*。 NISG 出厂时已经安装好系统,用户无需自己安装。 不同的硬件型号配备的接口不同,接口的编号方式也有所不同,包括:

- MGT 口: 该接口为管理接口,只能转发管理流量,不转发业务流量。
- ETH x: 表示板载接口, x 表示接口编号。
- ETH-sxpx:表示接口卡接口。sxpx表示接口板上的接口编号,sx表示接口所在接口板编号,px表示接口编号。

MGT 口为一个物理接口,专门转发管理流量。板载接口和接口卡接口都可在 WebUI 上 设置为逻辑上的管理接口。

本文以含有 MGT 口和 ETH-sxpx 接口为例进行阐述。

2. 连接设备和管理 PC



- 2.1 连接以太网接口
- 2.2 连接 Console □

2.1 连接以太网接口

1. 使用 RJ-45 网线连接管理 PC 至 NISG 的管理接口,或直接连接 NISG 的管理接口到 LAN。

如下图所示,使用一根 5 类、超 5 类或 6 类的非屏蔽双绞线或屏蔽双绞线连接设备, 两端均使用 RJ-45 接头。其中一端连接 NISG 设备的以太网接口,另一端连接局域网 HUB 或交换机设备的以太网接口。



2. 在管理 PC 上添加 IP 地址 192.168.1.200, 掩码设为 255.255.255.0。 用于管理 NISG 的管理 PC 上至少安装有以下一种浏览器:

- Microsoft Internet Explorer (7.0 或更高版本)
- Mozilla Firefox (10.0 或更高版本)
- Google Chrome (9.0 或更高版本)
- Opera (11.x 或更高版本)
- Safari (5.0 或更高版本)

2.2 连接 Console □

Console 访问默认是允许的,管理员可以通过 Console 口管理 NISG。 将 Console 线带有 RJ-45 连接头的一端连接到 Console 口,带有 DB-9 连接头的一端连接 到管理终端的串口。



选用任何兼容标准 VT100 并带有 RS-232 接口 (标准 DTE 接口)的终端或模拟终端, 并进行如下配置:

- 波特率: 9600
- 数据位:8
- 奇偶校验位:无
- 停止位:1

3. 部署 NISG 到网络

选择一种工作模式,并将 NISG 部署到网络中:

- 3.1 透明模式
- 3.2 路由模式
- 3.3 旁路模式

3.1 透明模式

NISG 可部署在私有网络的现有网关后面,无缝集成到现有网络中。透明模式下, NISG 主要用于数据的二层转发。当客户需要在不改变网络拓扑的情况下提供安全保护时,可使用此工作模式。



3.2 路由模式

NISG 可部署在公网和私网之间,作为局域网内主机的默认网关。路由模式下,NISG 可以让工作在不同网段之间的主机以三层路由的方式进行通信。



后续小节都按照此处两种模式的拓扑描述如何对 NISG 进行配置。

3.3 旁路模式

NISG 可旁路模式部署与网络中,对网络进行监控。流量经外部设备镜像至 NISG, NISG 对其进行监控检测。



提示:后续小节都按照此处三种模式的拓扑描述如何对 NISG 进行配置。

4. 使用向导进行初始化配置

NISG 提供一个 WebUI 向导用于完成初始化。本节介绍以下内容:

- 4.1 登录
- 4.2 设置系统语言 / 主机名 / 系统时间
- 4.3 配置透明模式
- 4.4 配置路由模式
- 4.5 配置旁路模式

提示: 旁路模式受 License 控制,如系统未被上载 License,或上载的 License 不包含旁路模式特性,则在配置向导中不会出现有关旁路模式的显示。

4.1 登录

在产品出厂、系统重置或重装后,当管理员首次通过 WebUI 登录 NISG 时,配置向导会自动弹出。管理员也可以点击 WebUI 界面右上角的、按钮,随时开启向导功能。本文中以产品出厂后管理员首次登录为例进行阐述。

- **1.** 启动 NISG 设备。
- 2. 在管理主机上打开浏览器,输入 https://192.168.1.100。出现一个证书错误提示页面。 点击"继续浏览此网站(不推荐)"选择信任 NISG 证书。

🏉 证书错误:	导航已阻止 - Windows Internet Explorer
	🙋 https://192.168.1.100/
×	此网站的安全证书有问题。
	建议关闭此网页 ,并且不要继续浏览该网站。
	单击此处关闭该网页。
	😵 继续浏览此网站(不推荐)。
	● 更多信息

3. 出现登录页面,在文本框中输入缺省用户名 admin,密码 neteye 以及验证码,点击登 录按钮。

Neusoft			\rightarrow \rightarrow
	该系统仅供推	受权使用	
用户名	admin		
密码	•••••		
验证码	599a	599a	8
		汞登录	

提示:如果连续输入密码错误达到5次,账号将被锁定20分钟。

4.2 设置系统语言 / 主机名 / 系统时间

4.	登录后系	统弹出欢迎负	面。そ	至下拉框。	中选 排	举相应	的语言	訂, 点日	告后一页。
				初始化					×
	欢迎	系统配置	模式	网络	Lice	ense	安全	完成	Neusoft
	欢迎使用	NISG配置向	导						
						系统	流信息		
				켚号		5000			
				软件名称		东软NetEy	e集成安全网	网关	
				软件版本		4.2 BUILD	700200		
				释放时间		2015-08-2	4 14:34:22		
				序列号		000C2947A	452		
			-	内存		4096 MB			
				系统运行时间		1 天 2 小	时 27 分		
				语言		简体	\$ 中文		-
						3	兆过		后一页

提示: 在首次登录且不愿使用配置向导进行初始化时,您可以点击**跳过**按钮,跳过配置向导, 采用其他方式配置系统。

5. 修改管理员密码,点击后一页。

			初	J始化				×
	欢迎	系统配置	模式	网络	License	安全	完成	Neusoft
修	改密码							
i IB	密码		•••••	*				
新	密码		•••••	*				
确	认新密码		•••••	*				
	取消				跳	过 f	前一页	后一页

提示:您也可选择点击**跳过**按钮,跳过密码设置步骤,使用缺省密码。但是,为了安全考虑, 我们建议您不要使用初始缺省密码。

		初始化				×
欢迎 系统配置	模式	网络	License	安全	完成	Name
•						Neuson
主机名和系统时间						
主机名 系统时间	NetEye					
时区	(GMT+08:00) ¢	中国/上海(北京)	•		
日期	2014-10-28		💽 (YYYY-MM-D)	D)		
时间	15:15:48		(HH:MM:SS)			
□与互联网上的时间服务器同步(N	TP)					
NTP服务器						
取消					前一页	后一页

6. 根据需要配置主机名、系统时间和 NTP 服务器地址等内容,点击后一页。

- 7. 选择一种部署模式
 - 4.3 配置透明模式
 - 4.4 配置路由模式
 - 4.5 配置旁路模式

4.3 配置透明模式

- 4.3.1 网络和安全设置
- 4.3.2 通过 WebUI 确认初始化配置
- 4.3.1 网络和安全设置
- 1. 选择透明模式,点击后一页。



2. 配置设备端口分配,点击后一页。

设备端口分配有两种方案可供选择,默认 WAN/LAN 和 WAN/LAN/OPT。如果选择 WAN/LAN,则第一个带编号的端口为 WAN 域,剩下的所有端口为 LAN 域;如果 选择 WAN/LAN/OPT,则带编号的端口中第一个端口划分为 WAN 域,最后一个端口 划分为 OPT 域,中间所有端口划分为 LAN 域。

				初始化				×
m	欢迎	系统配置	模式	网络	License	安全	完成	Neusoft
ż	医明模式							
Ì								
	◙ 默认WA	N/LAN						
	🔘 WAN/LA	N/OPT						
	WAN	LAN						
	取消						前一页	后一页

3. 配置网络设置,点击后一页。

	初始化 🗙											
	欢迎	系統配置	模式	网络	License	安全	完成	Noucoft				
				•				Neuson				
v	T AN语号											
	and the lat											
	IP地址/ 掩码	192.168.1.32	/ 24	*								
	网关	192.168.1.1										
	首选DNS											
	备选DNS											
	Vlan服务	🗹 SSH 📃 Telnet	🔽 Ping	Veb								
đ	带外管理接口配置											
I	P地址/ 掩码 1	10. 10. 1. 10	/ 24	*								
(🗸 SSH 📃 Telnet	✔ Ping 🛛 ✔ Web										
	取消						前一页	后一页				

- VLAN 设置:
 - IP 地址 / 掩码: 创建 VLAN, 并为 VLAN 配置 IP 地址和掩码。创建 VLAN 后所有带编号的接口都处于 VLAN 中。
 - 网关: VLAN 的网关。
 - DNS 服务器:用于解析 NISG 到 Internet 的域名请求。
 - VLAN 服务: 启用或禁用可连接 NISG 的服务。勾选表示启用。
- 带外管理接口配置 (如为没有 MGT 口的机型, 在配置向导处不会显示此项):
 - IP 地址 / 掩码: 配置带外管理口的 IP 地址和掩码。
 - 服务配置: 启用或禁用可连接 NISG 的服务。勾选表示启用。
- **4.** 点击**是**,然后点击**结束**,提交所做的基本配置并继续进行安全配置;或者点击**否**,然后点击**结束**,提交所做的基本配置并退出向导。

				初始化				×
	欢迎	系统配置	模式	网络	License	安全	完成	Noucoft
I				0				Neuson
				概述				
	语言			简体中	文 文			
	主机名			NetEye				
	时区			(GMT+C	18:00)中国/上¾	專(北京)		
	日期时间			2014-1	0-28 17:04:19			
	类型			透明模	式−所有接口在一	个VLAN中		
	已完成基本酉	祝罢。是否要继续进行安全配罢 ? 退出向导)						
	TE IN						× T	11.00
	取消						前一页	结束

提示:点击结束后,将无法点击前一页返回基本配置页面进行修改。

- 5. (可选)如果系统中不存在 License,向导将跳转到 License 激活页面。您必须在激活 License 后才可做后续安全配置。License 激活支持自动和手动两种方式:
 - 自动:选择自动获取 License,点击激活按钮。点击按钮前,请确保 NISG 可以访问互联网。
 - 手动:选择手动输入 License,输入 License 字符串,然后点击激活按钮。

				初始化				×
	欢迎	系統配置	模式	网络	License	安全	完成	Neusoft
		₩ 提示:	必须在进行妄	≂全配置前激 [;]	fLicense∘			
0)自动获取License							
C)手动输入License				~			
	取消							激活

				初始化				×
	欢迎	系统配置	模式	网络	License	安全	完成	Neusoft
12	۵							
	±	Internet			从LAN到WAN		④ 允许	◎ 阻断
					☑ 启用防病毒			
	WAI	N 💼 📕 🕴			☑ 启用IPS			
		342	JAN		☑ 启用反垃圾	邮件		
					☑ 阻断P2P应月	ŧ		
					☑ 阻断IM应用			
		P IP 🔷 <			🗹 阻断文件共	享类应用		
					✔ 阻断社交网	络类应用		
					☑ 阻断游戏类	应用		
					从WAN到LAN		◎ 允许	◎ 阻断
	取消							后一页

6 设置访问安全控制动作 自田或埜田安全功能 占去后一面

提示:如果设备已有可用 License,向导会跳过此步,请直接执行步骤 6。

提示:具体可配置安全功能由 License 控制,上图显示所有安全功能。

关闭

			初始化				×			
欢迎	系統電置	模式	网络	License	安全	完成	Neusoft			
					•					
			概述							
从LAN管IWAN			允许							
防病毒			启用							
IPS			启用							
反垃圾邮件			启用							
			P2P							
			IM							
阻断应用			文件共享							
			社交网络							
			游戏							
M WANEJLAN			阻断							
取消						前一页	结束			
初始化成	戊功后,点击 乡	长闭 按钮:	退出向导	0						
			初始化				3			
欢迎	系统配置	模式	网络	License	安全	完成				
							Neusof			
恭喜!										
		设名	公初始化	成功。						

7. 检查详细配置信息,点击结束。

提示:如果在向导中执行了激活 License 操作,系统将出现重启提示,请根据提示重启 系统。否则, License 将不会生效。重启过程将持续三分钟左右,请三分钟后再进行登录。

4.3.2 通过 WebUI 确认初始化配置

要确认初始化配置是否生效,请执行以下操作:

- 1. 输入缺省用户名和密码进行登录。
- 2. 查看主页上方的主机名和系统时间,可以看到新的主机名和系统时间已生效。

🎯 FW1 🤮 admin 2015-08-28 02:28:46

3. 选择网络 > 接口查看接口配置。可以看到新建 VLAN 接口 vlan1 包含 eth-s1p1 和 eth-s1p2。

► P	网络 ▶ 接口									
新建 ▼ 删除 接口列表										
	接口	链路状态	接口状态	模式	MAC地址	属于	IP地址	引用		
	eth-s1p1		~	Layer2 (Access)	00:0C:29:AE:9C:48	vlani			ø	
	eth-s1p2	C	× .	Layer2 (Access)	00:0C:29:AE:9C:52	vlani			ø	
	mgt		~	Layer3	00:0C:29:AE:9C:69		10.10.1.10/24(静态)		ø	
	vlani	C	× .	Layer3	00:0C:29:DB:69:11		192.168.1.32/24(静态)		/ x	

4. 选择网络>安全域查看安全域配置。可以看到新建二层安全域LAN和WAN,WAN包含 eth-s1p1, LAN 包含 eth-s1p2。安全域被缺省访问策略引用。

• 🖻	网络▶安	全域				
	新建	刪除	安全	È域列表(总数:2)		
		名称	类型	接口	引用	
		WAN	基于二层接口(vlan1)	eth-s1p1	^	ø
		LAN	基于二层接口(vlan1)	eth-s1p2		ø

5. 选择网络 > 路由 > 缺省路由查看默认网关是否已经修改。下面是缺省配置。

▶ 网络	▶路由▶	缺省路由			
新建	t m	除 缺省	路由表(总数:1)		
	ID	目的	出口接口/网关	Metric	
	1	任意	192.168.1.1	1	🖉 🗙

6. 选择防火墙 > 访问策略。可以看到系统已经添加两条缺省访问策略,允许 LAN 到 WAN 的访问,同时拒绝 WAN 到 LAN 的访问。

▶ 防火	(墙▶访)	可策略										
ł	提示: 其他個	点击列表中 言息。如需修	■策略名称的超 ₿改策略的更多	链接可じ 信息,译	从编辑策略的描 青点击编辑图标	述信息; 点击其 ;。	他参数对	拉的超错	涟接可以	编辑	鍜	略的
新	建 8	刪除	明 禁用		λ 导出	访	可策略列	表(总詞	赦:2)			
	的房号	🏨 名称	盟 源安全域	盟源IP	🛄 目的安全域	🛍 目的IP/域名	的服务	盟动作	的自用			
	1	<u>def lw</u>	LAN	<u>任意</u>	WAN	<u>任意</u>	<u>任意</u>	允许	 Image: A second s	Ø	2	×
	2	<u>def wl</u>	WAN	<u>任意</u>	LAN	<u>任意</u>	<u>任意</u>	拒绝	× .	Ø	2	×

	以且 旦徂瓜;	方)	正百 山 似 归 用 !	以示用。		
▶ 系统 ▶ 服务配置 ▶ 访问设置		W	eb			
Telnet			允许Ψeb访问	◎否 ◎♬	Ē	
允许Telnet访问 💿 否 💿 是			SSL端口号	443	*(默认值:	443)
Telnet端口号 23 *(默认值:23)		访问控制列表	長(总数:2)	添加	10
访问控制列表(总数:0)	添加	•	IP地:	址	入口安全	:域
IP地址 入口	口安全域		0.0.0.0-255.2	55.255.255	mgt-inter	face
空列表			0.0.0.0-255.2	55.255.255	LAN	
SSH		Pi	ng			
		π	许Ping访问	◎ 否	◎ 是	
			访问控制列表	(总数:2)	添	加 🕨
SSH端口亏 22	*(默认倡:22)		IP地址		入口安全地	щ
访问控制列表(总数:2)	添加	▶ 0	.0.0.0-255.255	.255.255	mgt-interf	ace
IP地址 入口	口安全域	0	.0.0.0-255.255	. 255. 255	LAN	
0.0.0.0-255.255.255.255 mgt-:	interface	rc	oot用户访问控制			
0.0.0.0-255.255.255.255	LAN		允许root用户	远程登录	◎否	◎ 是
			/GH1000H/	也性艺术		U TE

进**迟至结、肥久配罢、法词边罢**本手肥久且不可逆户田式林田

提示:访问服务允许的 IP 地址范围默认为 0.0.0.0-255.255.255.255, 管理员应根据实际 情况修改允许访问的 IP 地址范围。

4.4 配置路由模式

- 4.4.1 网络和安全配置
- 4.4.2 通过 WebUI 确认初始化配置

4.4.1 网络和安全配置

1. 选择路由模式。选择以下任意一种 WAN 接口获取 IP 地址的方式。点击后一页。





■ 为 ISP 客户端认证软件使用 PPPoE。



2. 配置设备端口分配,点击后一页。

设备端口分配有两种方案可供选择,默认 WAN/LAN 和 WAN/LAN/OPT。如果选择 WAN/LAN,则第一个带编号的端口为 WAN 域,剩下的所有端口为 LAN 域;如果 选择 WAN/LAN/OPT,则带编号的端口中第一个端口划分为 WAN 域,最后一个端口 划分为 OPT 域,中间所有端口划分为 LAN 域。



- 3. 配置 WAN 设置,点击后一页。
 - 如果在步骤1中选择使用静态 IP,请配置以下 WAN 页面。

				初始	化				×
	欢迎	系统配量	模式	网络	8	License	安全	完成	Neusoft
1				0					neusone
	WAN设置								
1									
	IP地址/ 掩码	202.1.1.1	1	24	*				
	WAN服务	SSH 🗌 Telnet	Ping	Web					
	网关	202.1.1.100							
	首诜DNS	202. 1. 1. 100							
	5 Hours								
	更近UN2	_							
	启用NAT								
	转换后IP地址								
	◙ ₩AN接口主I	P							
	◎ 指定IP地址								
	取消						[前一页	后一页

- IP地址/掩码 WAN接口的IP地址。此处的静态IP地址由上游网络管理员分配, 请向上游网络管理员索取,请不要私自配置 IP 地址。
- WAN 服务: WAN 服务表示在外网可使用的能够管理系统的服务,缺省情况下,不允许外网终端管理系统。
- 网关: WAN 接口的网关。
- DNS: DNS 服务器 IP 地址。
- 启用NAT:如果此处选择启用NAT,系统将自动生成一条名为def_lw的SNAT规则,将数据包的源 IP 地址转换为指定的转换后 IP 地址。该指定 IP 地址不能为 192.168.255.254。
- 如果在步骤1中选择使用 DHCP 动态分配的 IP 地址,请配置以下 WAN 页面。

			初始化				×
欢迎	系统配置	模式	网络	License	安全	完成	Neusoft
			0				incuboit
WAN设置							
获取IP地址	使用DHCP	动态分配的IP地	!址				
启用DNS代理							
WAN服务	SSH	📃 Telnet	: Ping	Web			
启用NAT	\checkmark						
转换后IP地址							
◙ ₩AN接口主IP							
◎ 指定IP地址							
取消						前一页	后一页

- 启用 DNS 代理: NISG 设备代理 DNS 服务器。
- WAN 服务: WAN 服务表示在外网可使用的能够管理系统的服务,缺省情况下,不允许外网终端管理系统。

- 启用NAT:如果此处选择启用NAT,系统将自动生成一条名为def_lw的SNAT规则,将数据包的源 IP 地址转换为指定的转换后 IP 地址。该指定 IP 地址不能为 192.168.255.254。
- 如果在步骤1中选择为 ISP 客户端认证软件使用 PPPoE,请配置以下 WAN 页面。

				1	明始化				×
	欢迎	系统配量		模式	网络	License	安全	完成	Neusoft
-					•				neuson
WA	N 没 世								
PF	PoE设置								
	用户名		test						
	密码		••••	••					
	启用DNS代理		~						
W2	N服务		SSH 🗌	🗌 Telnet	Ping	Web			
肩	用NAT		~						
	转换后IP地址								
	◙ ₩AN接口主IF	2							
	◎ 指定IP地址								
	_								
	取消							前一页	后一页

- 用户名、密码: PPPoE 登录时需要的用户名和密码。
- 启用 DNS 代理: NISG 设备代理 DNS 服务器。
- WAN 服务: WAN 服务表示在外网可使用的能够管理系统的服务,缺省情况下,不允许外网终端管理系统。
- 启用NAT:如果此处选择启用NAT,系统将自动生成一条名为def_lw的SNAT规则,将数据包的源 IP 地址转换为指定的转换后 IP 地址。该指定 IP 地址不能为 192.168.255.254。
- 4. 配置 LAN 设置,点击后一页。

如果管理员选择在 LAN 上启用 DHCP 服务器角色为内网 DHCP 客户端分配 IP 地址,需要设置 DHCP IP 地址池的起始和终止 IP 地址。还可以设置为 DHCP 客户端分配的网关地址和 DNS 服务器地址。

						1.11/1	
			初始化				×
欢迎	系统配量	模式	网络	License	安全	完成	Neusoft
			0				
LAN设置							
IP地址/ 撞码 LAN服务 启用DHCP服务器 起始IP地址 终止IP地址 网关 DNS	192.168.1.100	/	24 V Web				
带外管理接口配置							
IP地址/ 摘码 ▼ SSH □ Telnet 取消	10.10.1.10 : VPing V	/ 24 Web	4 ,			前一页	后一页

起始和终止 IP 地址必须和配置的 LAN 的 IP 地址在同一网段上。

提示:如设备没有 MGT 口,在配置向导处不会显示带外管理接口配置相关内容。

5. 点击是,然后点击结束,提交所做的基本配置并继续进行安全配置;或者点击否, 然后点击结束,提交所做的基本配置并退出向导。

				初始化				×
	欢迎	系统配置	模式	网络	License	安全	完成	Neusoft
				概述				
	语言			简体中的	х			
	主机名			NetEye				
	时区			(GMT+O	8:00)中国	1/上海(北京)		
	日期时间			2014-1	0−28 17 : 04	1:19		
	类型			路由模	式-PPPoE	显示因选择模式	不同而不同	
i	2完成基本配置	5。是否要继续进行安全配置 ?						
	◎ 否(退出	出向导)						
	◙ 是							
	取消						前一页	结束

提示:点击结束后,将无法点击前一页返回基本配置页面进行修改。

- 6. (可选)如果系统中不存在 License,向导将跳转到 License 激活页面。您必须在激活 License 后才可做后续安全配置。License 激活支持自动和手动两种方式:
 - 自动:选择自动获取 License,点击激活按钮。点击按钮前,请确保 NISG 可以访问互联网。
 - 手动:选择手动输入 License,输入 License 字符串,然后点击激活按钮。

				初始化				×
=	欢迎	系統配置	模式	网络	License	安全	完成	Neusoft
		😲 提示:	必须在进行安	₹全配置前激泪	License •			
۲	自动获取License							
0	手动输入License				A 			
	取消							激活

				初始化	///////////////////////////////////////	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		
	欢迎	系统配置	模式	网络	License	安全	完成	Neusoft
1								
安	全							
		Internet			从LAN到WAN		◙ 允许	◎ 阻断
	WAN				✓ 后用防病等			
		E F	_		✓ 启用1P5	La dil		
			LAN			田\$1千 		
					☑ 阻断P2P应用	B		
					🗹 阻断IM应用			
		P (P 💎 🔍			☑ 阻断文件共:	享类应用		
					🗹 阻断社交网	络类应用		
					☑ 阻断游戏类	应用		
					从WAN到LAN		◎ 允许	◎ 阻断
	取消							后一页

7. 设置访问安全控制动作, 启田或禁田安全功能, 占击后一页。

提示:如果设备已有可用 License,向导会跳过此步,请直接执行步骤 7。

提示:具体可配置安全功能由 License 控制,上图显示所有安全功能。

			初始化				3
欢迎	系统配置	模式	网络	License	安全	完成	Neusof
			Jaco Salt		•		
从LAN⊉IVAN			☆				
防病毒			启用				
IPS			启用				
反垃圾邮件			启用				
			P2P TM				
阻断应用			文件共享				
			社交网络				
U an an Tala a sa			游戏				
MWAN JILAN			阻断				
取消						前一页	结束

8. 检查详细配置信息,点击结束。

9. 初始化成功后,点击关闭按钮退出向导。



提示:如果执行了激活 License 操作,系统将出现重启提示,请根据提示重启系统。否则, License 将不会生效。重启过程将持续三分钟左右,请三分钟后再进行登录。

4.4.2 通过 WebUI 确认初始化配置

要确认初始化配置是否生效,请执行以下操作:

- 1. 输入缺省用户名和密码进行登录。
- 2. 查看主页上方的主机名和系统时间,可以看到新的主机名和系统时间已生效。

œ	FW1	👗 admin

2015-08-28 02:28:46

3. 选择网络>接口查看接口配置。

■ 如果选择**使用静态 IP**,显示如下:

▶ 网络	网络~接口											
新建	▼ 删除			_	接口列表	_	_	-				
	接口	链路状态	接口状态	模式	MAC地址	属于	卫地址	引用				
	eth-s1p1	69	~	Layer3	00:0C:29:25:00:01		202.1.1.1/24(Static)		ø			
	eth-s1p2	E	×	Layer2 (Access)	00:0C:29:25:01:01	vlan1			ø			
	eth-s1p3		×	Layer2 (Access)	00:0C:29:25:02:01	vlan1			ø			
	eth-s1p4	C	×	Layer2 (Access)	00:0C:29:25:03:01	vlan1			ø			
	mgt		~	Layer3	00:0C:29:25:4C:01		10.1.3.127/21(Static)		Ø			
	vlan1	C	1	Layer3	00:0C:29:25:4C:22		192.168.1.100/24(Static)		🥒 🗶			

■ 如果选择**使用 DHCP 动态分配的 IP 地址**,显示如下:

▶ 网络	接口								
新建 ▼									
	接口	链路状态	接口状态	模式	MAC地址	属于	卫地址	引用	
	eth-s1p1	-	-	Layer3	00:0C:29:25:00:01		202.1.1.1/24(DHCP)	•	ø
	eth-s1p2	C	×	Layer2 (Access)	00:0C:29:25:01:01	vlan1			ø
	eth-s1p3	-	×	Layer2 (Access)	00:0C:29:25:02:01	vlani			ø
	eth-s1p4	-	× -	Layer2 (Access)	00:0C:29:25:03:01	vlan1			ø
	mgt		1	Layer3	00:0C:29:25:4C:01		10.1.3.127/21(Static)		P
	vlan1	-	×	Layer3	00:0C:29:25:4C:22		192.168.1.100/24(Static)		🥜 🗙

■ 如果选择为 ISP 客户端认证软件使用 PPPoE,显示如下:

▶ 网络	▶接口							
新建	【▼ 删除				接口列表			
	接口	链路状态	接口状态	模式	MAC地 址	属于	卫地址	引用
	eth-s1p1		1	Layer2 (Access)	00:0C:29:25:00:01			^
	eth-s1p2	C	×	Layer2 (Access)	00:0C:29:25:01:01	vlan1		
	eth-s1p3		×	Layer2 (Access)	00:0C:29:25:02:01	vlan1		
	eth-s1p4		1	Layer2 (Access)	00:0C:29:25:03:01	vlan1		
	mgt	C	-	Layer3	00:0C:29:25:4C:01		10.1.3.127/21(Static)	
	vlan1	C	×	Layer3	00:0C:29:25:4C:22		192.168.1.100/24(Static)	
	ppp0	E	×	Layer3			202. 1. 1. 1	

4. 选择网络 > 安全域查看新建的三层安全域 LAN 和 WAN。

在选择使用静态 IP 和使用 DHCP 动态分配的 IP 地址,	显示如下:
 5 . 5 . 1 . 9	

▶ 网络 ▶ 🕏	全域				
新建	刪除		安全域列表(总裁	(: 2)	
	名称	类型	接口	引用	
	WAN	基于三层接口	eth-s1p1		ø
	LAN	基于三层接口	vlan1		ø

■ 在选择为 ISP 客户端认证软件使用 PPPoE,显示如下:

▶ 网络 ▶	安全域				
新建	刪除		安全域列表(总	.数:2)	
	名称	类型	接口	引用	
	WAN	基于三层接口	ppp0	Ŷ	Ø
	LAN	基于三层接口	vlan1	_	Ø

5. 选择**网络 > 地址转换 > 源地址转换**,查看系统是否已按初始化配置创建了一条 SNAT 规则。

■ 如果选择使用静态 IP 和使用 DHCP 动态分配的 IP 地址,显示如下:

► 🖂 🖇	络▶地址	止转换▶∶	源地址转换	:								
亲	健 📗	删除	启用	禁用	导入	导出	源地	址转换((总数:1)			
	序号	名称		源IP		转换质	旨₽/接口	入口接口	出口接口保留时间	(秒)	NAPT	启用
	1	def_lw	192.168.	1.101-192	2.168.1. <mark>19</mark>	9 et.	h−s1p1	vlani	eth-s1p1		 Image: A second s	 Image: A second s

■ 如果选择为 ISP 客户端认证软件使用 PPPoE,显示如下:

▶网络▶∶	地址转换▶〗	原地址转换										
新建	删除	启用	禁用	导入	导出			源地址	转换	(总数	k : 1)
🗌 序号	名称	源:	IP		转换后IP/接口	入口接口	出口接口	保留时间	(秒)	NAP T	启用	
1	def_1w 192.	168.1.101-	192.168	. 1. <mark>19</mark> 9	pppO	Any	Any			×	1	🥒 🗙

6. 选择网络 > 路由 > 缺省路由, 查看缺省路由是否已按初始化配置修改。

M3	各▶路由▶	缺省路由			
亲	f建 HH	<mark> 除</mark> 缺省器	各由表(总数:1)		
	ID	目的	出口接口/网关	Metric	
	1	任意	202.1.1.100	1	🥖 🗙

7. 选择防火墙 > 访问策略, 查看系统是否已创建了两条访问策略, 允许 LAN 到 WAN 的 访问, 同时拒绝 WAN 到 LAN 的访问。

▶ 防火	と墙▶访	可策略										
-	提示:点击列表中策略名称的超链接可以编辑策略的描述信息;点击其他参数对应的超链接可以编辑策略的 其他信息。如需修改策略的更多信息,请点击编辑图标。											
新	建	删除	明 禁用		く 専出	访门	可策略列	表(总	数:2)			
	皇序号	🛄 名称	🏨 源安全域	触 源 IP	🏨 目的安全域	🔒 目的IP/域名	🏨 服务	出动作	的自用			
	1	<u>def lw</u>	LAN	<u>任意</u>	WAN	<u>任意</u>	<u>任意</u>	允许	 Image: A second s	<i>/</i>	<i>.</i>	×
	2	<u>def wl</u>	WAN	<u>任意</u>	LAN	<u>任意</u>	<u>任意</u>	拒绝	× .	<i>/</i>	₆ 27	×

8. 选择网络 > DHCP > DHCP 作用域,查看是否创建成功缺省的 DHCP 作用域。

▶ 网络	各▶DHCP▶DHCP作用域					
影	健刪除	1	DHCP作用域列表(总数	: 1)		
	名称	网络地址	IP地址池	保留IP地址	租期(分钟)	
	Default_DHCP_on_LAN	192.168.1.0/24	192.168.1.101- 192.168.1.199		1440	/ ×

	为内女王 ,且有	3 /1 H		-1/1/1/-//	11/11	
▶ 系统 ▶ 服务配置 ▶ 访问设置		W	ſeb			
Telnet			允许₩eb访问	◎否 ◎爿		
允许Telnet访问 💿 否 🏾	是		SSL端口号	443	*(默认值:443)	
Telnet端口号 23	*(默认值:23)		访问控制列表	長(总数:2)	添加	₽
访问控制列表(总数:0)	添加	▶	IP地	址	入口安全域	
IP地址	入口安全域		0.0.0.0-255.2	255.255.255	mgt-interface	
空列表			0.0.0.0-255.2	255.255.255	LAN	
SSH		Ρ:	ing			
允许SSH访问 💿 否	◎ 是	5	位许Ping访问	◎ 否	◉ 是	
ssu端口是 22	●		访问控制列表	(总数:2)	添加	₽
55IISMI 1 5	* (x0, 0/(<u>H</u> :22)		IP地址		入口安全域	
访问控制列表(总数:2)	添加	Þ	0.0.0.0-255.25	5.255.255	mgt-interface	
IP地址	入口安全域	(0.0.0.0-255.25	5.255.255	LAN	
0.0.0.0-255.255.255.255	mgt-interface	r	pot用户访问控制			
0.0.0.0-255.255.255.255	LAN		允许root用户	远程登录	◎ 否 ◎ 是	

9. 选择系统 > 服务配置 > 访问设置, 查看相关服务是否已经启用或禁用。

提示:访问服务允许的 IP 地址范围默认为 0.0.0.255.255.255.255, 管理员应根据实际 情况修改允许访问的 IP 地址范围。

4.5 配置旁路模式

- 4.5.1 网络设置
- 4.5.2 通过 WebUI 确认初始化配置。

4.5.1 网络设置

			初始化				x
欢迎	系统配置	模式	网络	License	安全	完成	Noucoft
		0					neuson
讲你描言							
A217176.04							
◉ 旁路 模式-监	控镜像接口						
● 透明模式设	备工作在二层						
● 路由模式设	备工作在三层						
WAN IP	使用静态IP			-			
	(
			2				
					1.14.1810		
				Mirror I	Port		
				Mirror	Port		
				Mirror	Port		
	-			Mirror	Port		
	-				Port		
	-			Mirror	Port		
		••			vort		
取消		44			Port	前一页	后一页
取消					Port	前一页	后一页
取消 设置网	络参数,点击	▲ ▲			Port	前一页	后一页
^{取消} 设置网	络参数,点击	↓ ↓	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		Port	前一页	后一页
取消 设置网: 欢迎	络参数,点击	▲ 后一页。 概	初始化 网络	License	Port	前一页	后一页
取消 设置网: 欢迎	络参数,点击 彩魂	▲ ▲ 活一页。 概	初始化 网络	License	Port	前一页 完成	后一页 Neuso
取消 设置网 欢迎	络参数,点击 <i>新</i>酒	人 后一页。 概	初始化 网络	License	Port	前一页 完成	后一页 Neuso
取消 设置网: 欢迎 <u><u></u>穷路模式</u>	络参数,点击 <i>新</i>和选	▲ ▲ 活后一页。 概	初始化网络	License	Port	前一页 完成	后一页 Neuso
取消 设置网 <u>欢迎</u> <u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u><u></u></u>	络参数,点击 <i>新</i>和选	▲ ▲ 活 一 页。 概	初始化网络	License	Port	前一页 完成	后一页 Neuse
取消 设置网: 次迎 筹縮模式 管理接口设置	<u>络参数,点击</u> <i>新</i>和置	读 。 活 一 页 。 概	初始化 网络	License	Port	前一页 完成	后一页 Neuso
取消 设置网: 次迎 第編模式 管理接口设置 IP地址/播码	<u>络参数,点击</u> <i>新</i>编置 。	↓ ↓ 示后一页。 板	初始化 网络	License	Port	前一页 完成	后一页 Neuso

 ■ SSH
 □ Telnet
 ■ Ping
 ● Web

 取消
 前一页
 后一页

 場示
 此か的 IP 抽屉:
 抽屉:
 ● 加季

提示:此处的 IP 地址缺省配置在现有的管理接口上,如需另外增加或改变管理接口,需 在初始化之后,在网络 > 接口处进行配置。

首选DNS 备选DNS 服务配置

初始化 × 欢迎 系統配置 模式 网络 License 安全 完成 Neusoft 概述 语言 简体中文 主机名 NetEye 时区 (GMT+08:00) 中国/上海(北京) 日期时间 2015-06-18 03:17:41 类型 旁路模式 取消 前一页 结束

3. 点击结束,提交所做的基本配置。

提示:点击结束后,配置生效,您需要激活 License 后才能正常使用。激活 License 具体步 骤请参见 5.8 导入 License。

4.5.2 通过 WebUI 确认初始化配置。

- 1. 检查系统时间等项是否正确。
- 2. 重新登录后,选择网络>工作模式,检验是否为旁路模式。

设备工作模式	○ 在线模式● 旁路模式		
		确定	取消

3. 选择网络>接口,检查管理接口的 IP 地址是否为所配置 IP 地址。

۲	网络▶接口											
	接口列表											
	接口	链路状态	接口状态	模式	MAC地址	IP地址	控制接口					
	eth-s1p1	-	×	管理	00:0C:29:E6:D6:41	192.168.1.100/24(Static)		ø				
	eth-s1p2	C	×	监听	00:0C:29:E6:D6:4B			ø				
	eth-s1p3		×	监听	00:0C:29:E6:D6:55			ø				
	eth-s1p4	C	×	监听	00:0C:29:E6:D6:5F			ø				

5. 使用 WebUI 进行初始化配置

- 5.1 登录
- 5.2 WebUI 概述
- 5.3 重置密码
- 5.4 设置系统语言 / 主机名 / 系统时间
- 选择配置以下任意一种工作模式:
- 5.5 配置透明模式
- 5.6 配置路由模式
- 5.7 配置旁路模式

要配置功能,需要导入有效的 License:

■ 5.8 导入 License

5.1 登录

- 1. 通过 WebUI 向导登录,步骤同 4.1 登录。
- 2. 在欢迎页面选择简体中文,点击跳过,弹出 WebUI 页面。

5.2 WebUI 概述

WebUI 操作按钮如下表所示。 表1 WebUI 操作按钮

衣 T N	WebUI操作按钮		
按钮	描述	按钮	描述
	配置锁 (同一时间只能有一个管理用户 拥有配置锁)	<u>@</u>	切换虚拟系统
10	保存		编辑系统日期时间
	在线帮助		被引用 (查看引用某条目的策略或防护配置)
G	退出 (系统)	6 2	移动策略以改变其优先级
2	刷新	C)	克隆
•	恢复(系统设置)	 Image: A second s	(条目) 启用状态
Q	查看	\times	(条目)禁用状态
•	下载	21	过滤条件被启用 (过滤条件用于设置要显示 的参数项)
-	导出	<u>en</u>	过滤条件被禁用
ø	修改密码	+	添加条目到列表框
P	编辑	+	从列表框删除条目
×	关闭窗口(或删除条目)	+	向上移动列表中的条目
1	调出配置向导	+	向下移动列表中的条目
N@ rad	调出 Webshell		

5.3 重置密码

要 1.	修改 选	(缺省登3 择 系统 >	_{录密码} , 认证 。	请抄	れ行り	人下操作	:	
► j	系统▶	认证▶管理用	1户					
要修改缺省登录密码,请执行以下操作: 1. 选择系统 > 认证。 *系统,认证,管理用户 新建 删除 留景类型 用户类型 admin 本地 Telnet,SSH,Web Administrator 2. 点击 修改密码。 修改密码 * 新密码 ●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●								
[名称	认证类	型	3	登录类型	用户类型	
		admin	大本	本地		et, SSH, Web	Administrator	I 2
2.	点	击 👂 修i	<u> </u>	。 修i	汝密码		×	
	当前密	e码	••••	••		*		
	新密码	3	••••	••••	••	*(6-128)		
	确认亲	所密码	••••	••••	••	*(6-128)		
			确	定		取消		
3.	点	击 确定 。	新密码	在下	次登	录时生效	汝。	

5.4 设置系统语言 / 主机名 / 系统时间

English 简体中文

開加

1. 选择 系统 > 横	既述。						
▶ 系统 ▶ 概述							
	系统信息						
主机名	NetEye	P					
语言	简体中文	P					
时区	(GMT+08:00) 中国/上海(北京)	P					
当前时间	当前时间 2015-08-28 02:34:42 🧳						
License	APPUP, SVPN, IPSUP, VPN, AV, ASOL, AS, IPS, AVUP, FW, UFOL, U	P					
SNMP	禁用						
上次更新时间							
	主机名 ¥						
主机名 F₩	*						
	确定取消						
- 3. 点击 确定 。 4. 点击 语言 对应	☑的✐按钮。						
	语言 🗙						
语言 简体	中文						

取消

- 5. 选择一种语言,点击**确定**。
- 6. 点击时区和当前时间对应的 **》**按钮。

		时区	:	×		当前时间	×
时区	(GMT+08:00)	中国/上海(北京)	•		日期 2014-03-18		* (YYYY-MM-DD)
	(GMT+08:00) (GMT+08:00)	马来西亚/ 吉隆坡 中国/上海(北京)	*		中に同 21・21・17		• (III. III. SS)
	(GMT+08:00)	马来西亚/古晋 新加坡			ын <u>ст.ст.т</u>		* (HH:MM:55)
	(GMT+08:00)	和//HAX 印度尼西亚/乌戎潘当,望加锡			确定		取消

7. 编辑系统时间,点击确定。点击 💾。

5.5 配置透明模式

1. 选择网络>接口。设置接口如下:

Do	网络 ▶ 接口												
新建 ▼ 删除													
	接口	链路状态	接口状态	模式	MAC地址	属于	IP地址	引用					
	eth-s1p1	-	× -	Layer2 (Access)	00:0C:29:AE:9C:48	vlani			ø				
	eth-s1p2	-	×	Layer2 (Access)	00:0C:29:AE:9C:52	vlani			Ø				
	vlan1	-	~	Layer3	00:0C:29:AE:9C:69		192.168.1.32/24(Static)		Ø×				

设置接口的具体方法:

- a. 点击新建 > VLAN, 创建 VLAN 接口 vlan1;
- **b.** 添加 eth-s1p1 和 eth-s1p2 接口到 vlan1。
- 2. 选择网络 > 安全域, 创建二层安全域 LAN 和 WAN。添加 eth-s1p1 到 WAN, 添加 eth-s1p2 到 LAN。

▶网络▶妾	R全域						
新建	刪除	安全词	安全域列表(总数:2)				
	名称	类型	接口	引用			
	LAN	基于二层接口(vlan1)	eth-s1p2		ø		
	WAN	基于二层接口(vlan1)	eth-s1p1		Ø		

3. 选择防火墙 > 访问策略, 创建如下访问策略:

▶ ₿決	j火墙▶ì	方问策略										
	提示:点击列表中策略名称的超链接可以编辑策略的描述信息;点击其他参数对应的超链接可以编辑策略的 其他信息。如需修改策略的更多信息,请点击编辑图标。											
	新建	删除	启用 禁門	目	引入 日本	រ	方问策略	列表(急数:2)		
	的 序号	🏨 名称	🏨 源安全域	的源IP	🛍 目的安全域	🛍 目的IP/域名	的服务	出动作	的启用			
	1	<u>LANtoWAN</u>	LAN	<u>任意</u>	WAN	<u>任意</u>	<u>任意</u>	允许	× .	<i>@</i>	1 2	×
	2	WANt oLAN	WAN	<u>任意</u>	LAN	<u>任意</u>	<u>任意</u>	拒绝	× .	Ø	1 22	×

4. 点击💾。

5.6 配置路由模式

此处 eth-s1p1 为连接内部的接口, eth-s1p2 为连接外部的接口。

- 5.6.1 以太网连接
- 5.6.2 PPPoE 连接
- 5.6.1 以太网连接

1. 选择网络>接口。设置接口如下:

	网络 ▶ 接口												
新	建 - [删除	接口列表										
	接口	链路状态	接口状态	模式	MAC地址	属于	IP地址	引用					
	eth-s1p1	-	1	Layer3	00:0C:29:AE:9C:48		192.168.1.100/24(Static)		P				
	eth-s1p2		1	Layer3	00:0C:29:AE:9C:52		202.1.1.1/24(Static)		ø				
	mgt	-	~	Layer3	00:0C:29:DB:68:F0		10.10.1.10/24(Static)		0				

2. 创建三层安全域 LAN 和 WAN。添加 eth-s1p1 到 LAN,添加 eth-s1p2 到 WAN。

▶网络▶	安全域						
新建 删除		安全域列表(总数:2)					
	名称	类型	接口	引用			
	LAN	基于三层接口	eth-s1p1		P		
	WAN	基于三层接口	eth-s1p2		Ø		

3. 修改缺省网关为 202.1.1.100。

▶ 网络	▶路由▶	缺省路由			
新建	t M	涂 缺省器	路由表(总数:1)		
	ID	目的	出口接口/网关	Metric	
	1	任意	eth-s1p2:202.1.1.100;	1	🥖 🗙

4. 创建 SNAT 规则,将 192.168.1.0/24 转换成 eth-s1p2 的 IP 地址:

► F	▶ 网络 ▶ 地址转换 ▶ 源地址转换												
	新建		删除	启用	禁用	- 导)	、 导	出	源地	址转	魚(总	数: 1	D
	序号	名称		源IP	转换后I	.P/接口	入口接口	出口接口	保留时间	(秒)	NAPT	启用	
	1	out	192.1	68.1.0/24	eth-s	s1p2	Any	Any			1	1	🥒 🗙
5.													
► F	防火墙	▶ 访问	策略										
	提示: 点击列表中策略名称的超链接可以编辑策略的描述信息; 点击其他参数对应的超链接可以编辑策略的 其他信息。如需修改策略的更多信息,请点击编辑图标。												
	新建	₩	除	启用	朝	导入	导出	រៀ	与问策略列	表(鳥	急数:2)	
	的原	;号 [自名称	盟 源安全地	或 🏨 源 IF	出目的	安全域 🛄 目	的IP/域名	的服务员	动作	🏨 启用		

WAN

LAN

<u>任意</u>

<u>任意</u>

<u>任意</u> 允许

拒绝

<u>任意</u>

6. 点击 💾。

LANt oWAN

<u>WANtoLAN</u>

LAN

WAN

<u>任意</u>

<u>任意</u>

1

2

🥒 🧀 🗙

5.6.2 PPPoE 连接

1. 选择网络>接口。设置接口如下:

▶ 网络 ▶ 接口							
新建 ▼ 删除		_	接口列表	_	_		
📃 接口 链路状态	接口状态	模式	MAC地址 属	子 IP地均	上 引用		
eth-s1p1 📟	🖌 L	ayer3 00:0	C:29:AE:9C:48	192.168.1.100/	(24(静态) 🥜		
eth-s1p2 📾	🖌 Layer:	? (Access) 00:0	C:29:AE:9C:52				
mgt 📾	✓ L	ayer3 00:0	C:29:AE:9C:69	10.10.1.10/2	4(静态)		
🗌 ppp0 📟	V L	ayer3		202.1.1	.1		
2. 创建三层安全	全域 LAN 利	WAN,添加	eth-s1p1到I	LAN,添加 pp	p0到WAN。		
▶ 网络 ▶ 安全域							
新建 删除		ŧ	全域列表(总额	数:2)			
2 名	称	类型	接口	引用			
W.A.	N	基于三层接口	pppO		🥒 🗙		
	N	基于三层接口	eth-s1p1		<i>⊘</i> ×		
3. 修改缺省网-	关为 202.1.1	.100。					
▶ 网络 ▶ 路由 ▶ 缺	省路由						
新建 删除	缺省	ì路由表(总数	: 1)				
ID ID	目的	出口接	口/网关	Metric			
1	任意	eth-s1p2:2	02.1.1.100;	1	🖉 🗙		
4. 创建 SNAT #	现则,将 19	2.168.1.0/24 年	专换为 ppp0 的	りIP 地址。			
▶网络▶地址转换▶	源地址转换						
新建 删除	启用	禁用 导入	导出	源地址转换(总数:1)		
□ 序号 名称	源IP	转换后IP/接口	入口接口 出口接	8日保留时间(秒)	NAPT 启用		
1 out 1	92.168.1.0/2	1 ppp0	Any Any	7	🗸 🖌 🍠 🗙		
5. 创建访问策略,允许 LAN 到 WAN 的访问,拒绝 WAN 到 LAN 的访问。							
▶ 防火墙 ▶ 访问策略							
提示:点击列表中策略名称的超链接可以编辑策略的描述信息;点击其他参数对应的超链接可以编辑策略的 其他信息。如需修改策略的更多信息,请点击编辑图标。							
新建 删除	启用 禁	用导入	导出	访问策略列表(总数:2)		
🔲 🏨 序号 🏨 名称	『 🏨 源安全域	的。 出源IP 出目的。	g全域的IP/比	或名 🏨 服务 🛄 动作	F 船 启用		
1 LANtow	AN LAN	<u>任意</u> WAI	「 <u>任意</u>	<u>任意</u> 允许	🖌 🖉 🥔 🗙		
	on won	任音 T 47	r 任音	任音 拒絕	🗸 🥒 🛷 🗙		

6. 点击💾。

5.7 配置旁路模式

1.	选择 网络 > 工作模式	,选择旁路模式。	
	○ 在线相 ② 在线相 ③ 旁路相 ● 旁路相	模式 模式	
		确定	取消
2.	系统弹出提示框,点	击 确定 。	
		确认	×
	系统将切换为旁路工作模式。 备份后进行:	当前工作模式下的安全配置将丢失。 该项操作。是否确认继续操作 ?	建议进行系统
	是	a E 否	
3.	选择 网络 > 接口 ,在	接口页面修改接口模式和	IP 地址。

5.8 导入 License

在进行以下步骤之前,请确认您已将有效 License 文件存放到本地 PC。

|--|

۶.	系统 ▶ 维护 ▶ License					
			系统License信		导入License	×
	功能	参数		◙ 导入Licer	use文件	
			空列表		浏览	
	수 유통창 편하게 한		τ· → ΛLα	◎ 输入Licen	确认	×
	目动获取License	、	License X H i		系统需重启。	
	License发行者 功能	名称	值		是否	
			空列表	L	确定 取消	i

提示:您也可以点击自动获取 License 按钮在线激活 License,但前提是您的 NISG 设备与 License 服务器之间是互通的。

2. 系统重启后自动跳转到登录页面,您可以登录后通过 WebUI 继续配置 NISG。

6. 使用 CLI 进行初始化配置

- 6.1 通过 Console 登录
- 6.2 CLI 基本信息
- 6.3 设置系统语言 / 主机名 / 系统时间
- 6.4 重置密码
- 6.5 配置透明模式
- 6.6 配置路由模式
- 6.7 导入 License
- 6.8 使用 SSH 登录
- 6.9 使用 Telnet 登录

6.1 通过 Console 登录

- 1. 在管理 PC 上选择开始 > 所有程序 > 附件 > 通讯 > 超级终端。
 - a. 输入区域码和连接名称,并在下面的对话框中依次点击确定。



Username:admin Password: NetEye@root> _

如果连续输入密码错误达到5次,账号将被锁定20分钟。

6.2 CLI 基本信息

首次登录 CLI 会出现如下提示符: NetEye@root>

在此提示符下可输入以下命令:

- show 命令:用于查看系统配置信息,如 show system info、 show interface brief、 show service 和 show route。
- 简单操作命令,如 clear、 halt、 debug 和 save config。
- configure mode override: 如果输入此命令,其他管理员将不能继续配置 NISG,除非他们重新抢占配置锁,不过他们已经提交的修改不会丢失。执行此命令后,系统提示如下提示符: NetEye@root-system]。您可以在此命令符下输入下表中的命令进入相应的配置模式。

命令	配置项	提示符
vlan vlan_id	VLAN 接口	NetEye@root-system-vlan1]
interface ethernet	以太网接口	NetEye@root-system-if-eth-s1p1]
interface_id		
channel channel_id	以太网通道接口	NetEye@root-system-if-ch1]
tunnel tunnel_id	VPN 隧道接口	NetEye@root-system-tunnel1]
<pre>rint rint_id</pre>	冗余接口	NetEye@root-system-rint1]
<pre>veth veth_id</pre>	虚拟接口	NetEye@root-system-veth1]
loopback lo_id	环回接口	NetEye@root-system-lo1]
pppoe pppoe_id	PPPoE 接口	NetEye@root-system-pppoe1]
cluster	集群	NetEye@root-system-cluster]
virtual router vrid	虚拟路由器	NetEye@root-system-vr1]
detection group group_id	虚拟路由器探测组	NetEye@root-system-dg1]
<pre>policy route policy_name</pre>	基于策略的路由	NetEye@root-system-routepolicy-test]
vpn	VPN	NetEye@root-system-vpn]
sslvpn	SSL VPN	NetEye@root-system-sslvpn]
vsys vsys_id	虚拟系统	NetEye@root-system-vsys1]
<pre>vnet vnet_id</pre>	虚拟网络	NetEye@root-system-vnet1]

输入以上任意一种命令,您可以对相应的配置项进行配置,如接口、集群/虚拟路由器、 VPN、 Vsys 等。在上面的例子中,你可以用 **ip** address 为接口配置 IP 地址。

- CLI 支持:
 - 在关键字或参数后输入"?",系统会提示该关键字或参数的帮助信息。
 - 在关键字或参数后面加空格,然后再输入"?",系统会提示下一个关键字或参数。
 - 可以通过按 Tab 键,补齐当前输入的关键字。如果有多个可选关键字,按 Tab 键则显示所有关键字。
 - 支持缩写。例如,可以将命令 configure mode 缩写为 con mo。

下面是如何使用 CLI 为 VLAN 接口配置 IP 地址的例子:

```
Username:admin
Password:
NetEye@root> configure mode override
NetEye@root-system] vlan 1
NetEye@root-system-vlan1] ip address 192.168.1.32 255.255.255.0
NetEye@root-system-vlan1] end
NetEye@root> save config
NetEye@root> _
```

6.3 设置系统语言 / 主机名 / 系统时间

1. 使用 show system info 命令查看系统信息。

-	2. 设置系统基本配置信息:
	🗞 FW1 - HyperTerminal
	NetEye@root> configure mode override NetEye@root-system] language Chinese NetEye@root-system] hostname FW1 FW1@root-system] time 2014-03-20 14:04:00 FW1@root-system] end FW1@root> save config FW1@root> _

6.4 重置密码

通过以下命令重置缺省登录密码:

1. 输入 configure mode override 命令,按 Enter 键。

- 2. 执行 password simple 命令。
- 3. 输入旧密码。
- 4. 输入新密码。
- 5. 重复新密码。



6.5 配置透明模式

1. 配置 NISG 工作在透明模式:

🗞 FW1 - HyperTerminal
FW1@root-system] interface ethernet mgt
FW1@root-system-if-mgt] ip address 10.10.1.10 255.255.255.0
FW1@root-system-if-mgt] exit
FW1@root-system] vlan 1
FW1@root-system-vlan1] hold ethernet eth-s1p1
FW1@root-system-vlan1] hold ethernet eth-s1p2
FW1@root-system-vlan1] ip address 192.168.1.32 255.255.255.0
FW1@root-system-vlan1] exit
FW1@root-system] zone LAN
FW1@root-system] zone WAN
FW1@root-system] zone LAN based-layer2 vlan 1 eth-s1p1
FW1@root-system] zone WAN based-layer2 vlan 1 eth-s1p2
FW1@root-system] policy access LANtoWAN LAN any WAN any any permit enable
FW1@root-system] policy access WANtoLAN WAN any LAN any any deny enable
FW1@root-system] end
FW1@root> save config
FW1@root> _

2. 查看接口配置信息:

🌯 FW1 - F	🗞 FW1 - HyperTerminal								
FW1@root>	show inter	face brief							
Nаме	Active	IP Addres	35		MAC	Held In			
terfaces	MTU U	Jsys							
мgt	on	10.10.1.1	LØ/24(Static)	00:0C:29:DB:68:F0				
-	1500 r	oot							
vlan1	on	192.168.1	L.32/24(Stat	ic)	00:0C:29:DB:69:11	eth-s1p			
1~	1500 r	oot							
Naмe	Active	Status	Speed	Duplex	Mode	Vlan Li			
st									
eth-s1p1	on	սք	1000Mb/s	Full	Layer2 Access	vlan1			
eth-s1p2	on	սք	1000Mb/s	Full	Layer2 Access	vlan1			
wet	<u></u>		1000Mb /o	F., 11	Laura 2				
ույւ	011	սբ	1000UD\2	ruil	Layers				

3. 查看安全域信息:

FW1@root≻ show	zone		
Name	Refcount	Policy	Descriptio
n			
LAN	2	Access Policies	
WAN	2	Access Policies	
FW1@root≻ _			

4. 查看访问策略:

FW1@root≻ show policy access							
Number Name	From To	Source ip	Destination ip				
Source users Services	Action State Tunnel						
1 LANtoWAN	LAN WAN	Any Ip	Any Ip				
any user any	permit enable						
2 WANtoLAN	WAN LAN	Any Ip	Any Ip				
any user any	deny enable						
/W1@root> _							

5. 查看服务设置:

FW1 - HyperTerminal	
FW1@root> show service	
Telnet service: Allow Access: No Access:	
Ssh service: Allow Access: Yes Access: allow any	0.0.0.0-255.255.255.255
Web service: Allow Access: Yes Access: allow any	0.0.0.0-255.255.255.255
Ping service: Allow Access: Yes Access: allow any	0.0.0.0-255.255.255.255
FW1@root>	

提示: 访问服务允许的 IP 地址范围默认为 0.0.0.255.255.255.255, 管理员应根据实际 情况修改允许访问的 IP 地址范围。

6.6 配置路由模式

此处 eth-s1p1 为连接内部的接口, eth-s1p2 为连接外部的接口。

- 6.6.1 以太网连接
- 6.6.2 PPPoE 连接
- 6.6.1 以太网连接

1. 设置 NISG 工作在路由模式并通过以太网接口访问 Internet:

🗞 FW1 - HyperTerminal
FW1@root-system] interface ethernet eth-s1p2
FW1@root-system-if-eth-s1p2] working-type layer3-interface
FW1@root-system-if-eth-s1p2] ip address 202.1.1.1 255.255.255.0
FW1@root-system-if-eth-s1p2] exit
FW1@root-system] zone LAN
FW1@root-system] zone WAN
FW1@root-system] interface ethernet eth-s1p1
FW1@root-system-if-eth-s1p11 working-type layer3-interface
FW1@root-system-if-eth-s1p1] exit
FW1@root-system] zone LAN based-layer3 eth-s1p1
FW1@root-system] zone WAN based-layer3 eth-s1p2
FW1@root-system] route default gateway 10.1.1.1 interface eth-s1p2
FW1@root-system] policy access LANtoWAN LAN any WAN any any permit enable
FW1@root-system] policy access WANtoLAN WAN any LAN any any deny enable
[FW1@root-system] policy snat out netmask 192.168.1.0 255.255.255.0 interface eth
-s1p2 napt enable
FW1@root-system] interface ethernet mgt
FW1@root-system-if-mgt] ip address 10.10.1.10 255.255.255.0
FW1@root-system-if-mgt] exit
FW1@root-system] interface ethernet eth-s1p1
FW1@root-system-if-eth-s1p11 ip address 192.168.1.100 255.255.255.0
FW1@root-system] end
FW1@root> save config

2. 查看接口信息:

FW1@root>	show interf	ace brief			HOP	11-14	T.u.
паме	HCTIVE	IP Haaress			MHC	нета	In
terfaces	MTU Vs	ys					
eth-s1p1	on	192.168.1.1	00/24(Static))	00:0C:29:DB:00:F0		
	1500 ro	ot					
eth-s1p2	on	202.1.1.1/2	4(Static)		00:0C:29:DB:01:F0		
× -	1500 ro	ot					
Mat	on	10.10.1.10	<pre>/24(Static)</pre>		00:0C:29:DB:68:F0		
	1500 ro	nt					
	1000 10						
Name	Active	Status	Speed	Duplex	Mode	Vlan	Li
st							
eth-s1p1	on	սթ	1000Mb/s	Full	Laver3		
-		1			,		
eth-s1n2	011	un	1000Mb/s	Fu 1 1	Lauer3		
oth orpz	011	чр	1000110, 3	1411	Luyers		
мgt	on	սք	1000Mb∕s	Full	Layer3		

3. 查看安全域信息:

FW1@root>	show zone		
Nаме	Refcount	Policy	Descriptio
n			
LAN	2	Access Policies	
WAN	2	Access Policies	
FW1@root≻	-		

4. 杳看访问策略:

FW1@root> show policy access						
From	То	Source ip	Destination ip			
Action	State Tunnel	-	_			
LAN	WAN	Any Ip	Any Ip			
perмit	enable					
- Wan	LAN	Any Ip	Any Ip			
deny	enable					
	s From Action LAN permit WAN deny	s From To Action State Tunnel LAN WAN permit enable WAN LAN deny enable	s From To Source ip Action State Tunnel LAN WAN Any Ip permit enable WAN LAN Any Ip deny enable			

5	. 查看:	SNAT	见则:					
F	7W1@root≻	show po	olicy sn	at				
1 1 1	Hum Poli rans L out	су-Nаме Napt True	State Enable	In-Interface Any	Out-Interface Any	Before-Trans 192.168.1.0/	24	After-T eth-s1p2
ł	/W1@root>	_						
6	. 查看月	B 务设置	- 1.:					
1	🌯 FW1 - H	lyperTer	minal					
	FW10root Telnet s Allow Access	> show s ervice: Access:	service No					
	Ssh serv Allow Access allo	ice: Access: :: w any	Yes	0.0.0.0-255.	255.255.255			
	Web serv Allow Access allo	ice: Access: : w any	Yes	0.0.0.0-255.	255.255.255			
	Ping ser Allow Access allo FW1@root	vice: Access: ;; w any	Yes	0.0.0.0-255.	255.255.255			

提示:访问服务允许的 IP 地址范围默认为 0.0.0.255.255.255.255, 管理员应根据实际 情况修改允许访问的 IP 地址范围。

6.6.2 PPPoE 连接

1. 设置 NISG 工作在路由模式并通过 PPPoE 接口访问 Internet:

🗞 FW1 - HyperTerminal
FW1@root-system] pppoe 0
FW1@root-system-pppoe0] hold ethernet eth-s1p2
FW1@root-system-pppoe0] username test password neteye
FW1@root-system-pppoe0] active on
FW1@root-system-pppoe0] exit
FW1@root-system] zone LAN
FW1@root-system] zone WAN
FW1@root-systeм] zone LAN based-layer3 eth-s1p1
FW1@root-system] zone WAN based-layer3 ppp0
FW1@root-system] route default gateway 202.1.1.100 interface ppp0
FW1@root-system] policy access LANtoWAN LAN any WAN any any any permit enable
FW1@root-system] policy access WANtoLAN WAN any LAN any any deny enable
FWI@root-systemJ policy snat out netmask 192.168.1.0 255.255.255.0 interface PPP0
FWI@root-systemJ end
rwieroot> save coniig
KMT@LOOt > _

2. 查看接	日信息:							
FW1@root>	FW1@root> show interface brief							
Naмe	Active	IP Address			MAC	Held In		
terfaces	MTU V	sys						
eth-s1p1	on	192.168.1.	100/24(Stat	ic)	00:0C:29:DB:00:F0			
-	1500 r	oot						
eth-s1p3	on	_			00:0C:29:DB:02:F0			
-	1500 r	oot						
мgt	on	10.10.1.10	/24(Static)		00:0C:29:DB:68:F0			
Ū	1500 r	oot						
Name	Active	IP Address			MAC	Held In		
terfaces	MTU V	sys						
ppp0	on	202.1.1.1			_	eth-s1p2		
	1454 r	oot						
Nаме	Active	Status	Speed	Duplex	Mode	Vlan Li		
st								
eth-s1p1	on	սք	1000Mb/s	Full	Layer3			
eth-s1p2	on	սք	1000Mb/s	Full	Layer2 Access			

;	3.	查看	Ī安	全域(官息 :	
Г	THE		4.5	1		

FW1@root≻	show zone		
Nаме	Refcount	Policy	Descriptio
n			
LAN	2	Access Policies	
WAN	2	Access Policies	
FW1@root≻			

4. 查看访问策略:

FW1@root> show policy acces	88			
Number Name	From	То	Source ip	Destination ip
Source users Services	Action	State Tunnel		-
1 LANtoWAN	LAN	WAN	Any Ip	Any Ip
any user any	perмit	enable		
2 WANtoLAN	LAN	LAN	Any Ip	Any Ip
any user any	deny	enable		
FW1@root> _	-			

ļ	5. 查看 SNAT 共	见则:				
Ī	FW1@root> show p	olicy sna	t			
	Num Policy-Nam rans Nap 1 out Tru	e t State e Enable	In-Interface Any	Out-Interface Any	Before-Trans 192.168.1.0/24	After-1 ppp0
L	FW1@root> _					
(6. 查看服务设置	置 :				
	🍣 FW1 - HyperTe	rminal				
	FW1@root> show Telnet service: Allow Access: Access:	service No				
	Ssh service: Allow Access: Access: allow any	Yes	0.0.0.0-255.2	255.255.255		
	Web service: Allow Access: Access: allow any	Yes	0.0.0.0-255.2	255.255.255		
	Ping service: Allow Access: Access: allow any	Yes	0.0.0.0-255.2	255.255.255		
	FW1@root>					

提示:访问服务允许的 IP 地址范围默认为 0.0.0.0-255.255.255.255, 管理员应根据实际 情况修改允许访问的 IP 地址范围。

6.7 导入 License

1. 在管理 PC 上搭建一个 TFTP 服务器,并将 License 文件放在下载路径。

2. 使用 license import 命令导入 License,根据提示输入 y 重启系统:
◆FW1 - HyperTerminal

FW1@root-system] license import from tftp 192.168.1.200 FW1.dat

License upload succeeded. System needs to reboot.

Continue? (v/n)v

如果重启系统前不保存配置,所有配置将在重启系统后丢失。

3. 重启后重新登录,并继续通过 CLI Console 配置 NISG。

6.8 使用 SSH 登录

1. 打开 SecureCRT, 点击 Quick Connect。在 Hostname 文本框中输入 NISG 的管理 IP 地址, 在 Username 文本框中输入缺省用户名。点击 Connect。

Quick Cor	nnect 🔀
Protocol:	SSH2
Hostname:	192.168.1.100
Port:	22 Firewall: None
Username:	admin
Authentication	
 ✓ Password ✓ PublicKey ✓ Keyboard In ✓ GSSAPI 	teractive
Show quick c	onnect on startup Dpen in a tab
	Connect Cancel
1. 输入密码	马,点击 OK。
Enter Sec	ure Shell Password 🛛 🔀
admin@192.168 Please enter a n	X1.100 requires a password.
Username: ad	min Cancel
Password: **	
Save passwo	ord
). 登录后酉	2置 NISG,配置方式同使用 CLI Console。
🖬 192.168.	1.100 - SecureCRT
192.168.1.100	
Neusoft NetEy NetEye@root>	/e (NetEye) (pts/0)
elnet 登	$\overline{\mathbf{x}}$
elnet 服务制	状认是天团的。
I. 使用 Iel	net 连接之间, 需要先通过 CLI Console 后用 Telnet 服务:
NetEye@root	-system] service telnet on
<u>mettye@root</u>)	-systemi service ternet arrow zone any 0.0.0 255.255.255.255.255. AC 上选择 开始、低方租底、附件、会众担子效 打工会众担子容白 通过Talmat
品 在官理P	C工选择开始>所有程序>附件>砷学旋小符,打开砷令旋小窗口,通过Telnet 星登录 NISG:
🔤 命令提示符	行
C:\Document	s and Settings\IDPC>cd\
C:∖>telnet	192.168.1.100
. 登录后酉	2置 NISG,配置方式同使用 CLI Console。
🚥 Telnet	192.168.1.100
Neusoft Net	Eye (NetEye) (pts/0)
Jsername:ad	min

6.9 使用

7. 验证初始化配置

初始化之后,执行以下步骤测试网络的连通性:

- **1.** Ping 管理接口。如果 Ping 失败:
 - a. 检查管理 IP。(缺省为 192.168.1.100/24。)
 - WebUI: 选择网络>接口。
 - CLI: 运行 show interface brief 命令。
 - **b.** 检查相关服务是否开启。运行 show service 和 show service port 命令查看服务和 端口配置。 Telnet 服务默认关闭,若使用 Telnet 登录,需要先开启 Telnet 服务。

FW1@root> show service Telnet service: Allow Access: No Hccess:	
Ssh service: Allow Access: Yes Access: allow any	0.0.0.0-255.255.255.255
Heb service: Allow Access: Yes Access: allow any	0.0.0.0-255.255.255.255
Ping service: Allow Access: Yes Access: allow any FW1@root>	0.0.0.0-255.255.255.255

FW1@root>	show	service	port					
Telnet por SSH por	rt: 23	3						
Web poi	rt: 44	43						
FW1@root> _								

- **c.** 检查是否存在 IP 冲突。 将 NISG 设备从网络中移除,从管理 PC 上 Ping NISG 的管理 IP 地址。如果收到 应答,表明存在 IP 冲突。
- d. 使用 HTTPS 而非 HTTP 访问 NISG WebUI (输入 "https://" 和管理 IP 地址)。
- e. 换一个浏览器或 PC 访问 NISG。
- f. 检查管理 PC 和 NISG 设备之间的网线连接。 应使用 RJ45 网线连接管理 PC 和 NISG 的接口。 检查接口是否是 Up 状态。
- g. 检查路由设置。 如果管理 PC 和 NISG 设备之间有路由设备,检查管理 PC、 NISG 和路由设备上 是否正确配置了路由信息。

在 NISG 上启用 Ping 服务,从管理 PC 上 Ping NISG 的管理 IP 地址。

FW1@root-system] service ping on FW1@root-system] service ping allow zone any 0.0.0.0 255.255.255.255

如果 Ping 失败,检查路由设置和网络拓扑。在 NISG 上执行 show route 命令查看 路由信息。

- 2. Ping 外网口 WAN 接口。如果 Ping 失败:
 - 透明模式下,检查 NISG 的安全域和访问策略配置。
 - 路由模式下,检查 NISG 的安全域、访问策略、路由、 NAT 规则配置,以及管理 PC 上的网关配置。
 访问策略按优先级从高到低进行匹配。一旦匹配到一条策略,其他策略不再进行 匹配。

- **3.** Ping NISG 的网关。如果 Ping 失败:
 - 检查 NISG 上的缺省路由。
 - 检查 NISG 和其网关之间的网线连接。
- **4.** 访问 Internet。如果访问失败:
 - 检查以上步骤。如果能 Ping 通 NISG 的网关, Traceroute 被访问网站来定位问题所 在。
 - 如果出现在重启系统后,检查重启系统前是否忘记保存配置。

提示:详细信息请参见前一小节相关步骤。

8. 常见问题

疑难1

初始化之后访问不了 NISG。

解决办法

- 检查管理接口或 IP 是否在初始化过程中被修改。
- 检查 NISG 网关是否在初始化过程中被修改。

疑难2

能登录,但访问的页面不正确。

解决办法

- 清空浏览器缓存再访问。
- 检查是否存在 IP 冲突。

疑难3

登录后不能配置 NISG 功能。

解决办法

- 没有配置锁。点击 WebUI 右上角的 de 按钮获取配置锁,或在 CLI 下执行 configure mode override 命令获取配置锁。
- 未上载相关功能的 License。要上载 License,请参见 5.8 导入 License。

疑难4

不能激活 License。

解决办法

- 检查 NISG 的 IP 是否同 License 服务器在同一子网。
- 为NISG 配置 DNS 服务器地址,用于解析 DNS 请求。
- 检查 NISG 和 Internet 之间的连通性。

疑难5

不能通过 WebUI 登录 NISG。 解决办法

- 检查 Web 服务是否开启。
- 如果您连续5次输入密码错误,登录账号将被锁定20分钟。
- 在CLI下执行df命令,确保有足够的存储空间。

疑难6

不能通过 PPPoE 接口访问 Internet。

解决办法

- 检查 NISG 上的 PPPoE 接口是否开启,所绑定的二层以太网接口是否连接正确。
- 检查 NISG 上为 PPPoE 接口配置的用户名和密码是否正确。
- 检查 PPPoE 接口和 Internet 之间的连通性。

沈阳浑南新区新秀街 2 号 客服热线: 400 655 6789 http://neteye.neusoft.com