**清华永新统一安全网关 TN-SG5000 V5.0**

**交付和运行v1.0**

**江苏清华永新安全科技有限公司**

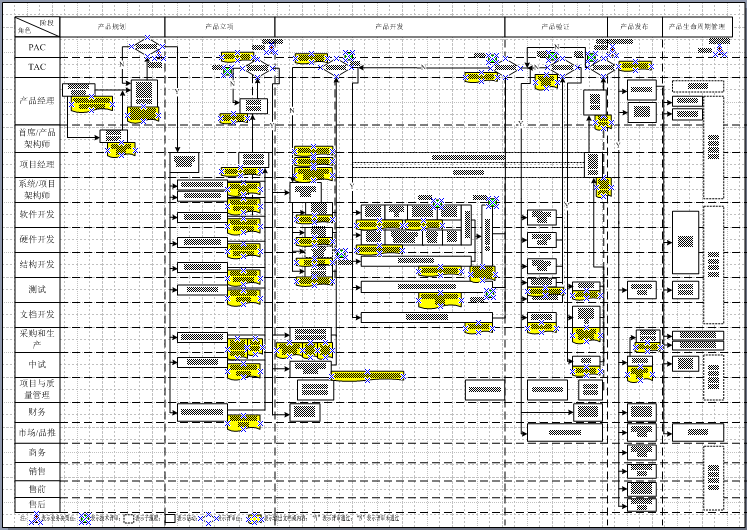
序言

本产品交付流程，规定了清华永新网络防火墙产品从开发、中试、生产到交付用户的流程和必备的交付件，从而保证产品产品交付过程中的完整性、一致性和可追溯性。

**一、交付**

1. 交付过程

交付过程涉及到从产品经理、开发者、测试人员、中试工程化人员、生产人员、客服人员、用户的交付全过程， 其中各个过程都需要严格按照相关规定提交交付件， 在每个过程中都需要严格按照相关子流程进行。



项目立项时，产品经理向研发、测试人员提交《产品需求规格》。

在开发者开发完成防火墙产品后，需要将防火墙软件版本和硬件整机交付测试人员，交付过程需要严格按照《产品测试申请单》进行，并提交《研发测试报告》。

在测试人员按照《产品需求规格》对产品进行严格的测试，测试完成并通过公司TR3评审后，需要更新《清华永新防火墙产品上线实施作业指导》、《清华永新网络项目实施管理规范》。

之后由产品经理将产品提交中试，提交过程需要提交《清华永新防火墙通用软件、光盘、生产文件提交单》、《产品随机光盘母盘》。同时由产品经理提交客户服务部门《清华永新防火墙产品上线实施作业指导》、《清华永新网络项目实施管理规范》。

中试人员按照《新品选型及中试流程》对产品进行中试和试生产，在完成中试确认无问题后将进行小批量试生产，同时测试人员完成产品BETA测试后，公司组织产品发布评审。之后中试人员将向硬件供应商提交《防火墙生产指导书》。

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **流程名称** | 新品选型及中试流程 | | | | | **流程负责人** | **硬件研发、产品中试** | |
| **流程起点：** 新品需求 | | | **流程目的：**提高产品化效率、提升产品质量、 | | | **流程终点：**新品试生产下线 | | |
| **步骤编号** | **步骤** | | **描述** | | | | | **参与部门** |
| **1** | 新品需求 | | * 由产品经理**发起会议**，对新品提出功能、性能、成本、进度安排等要求，并填写《新品立项需求表》 | | | | | 产品经理（召集人） 供应链、硬件研发、中试、软件研发 |
| **2** | 新品选型 | | * 由硬件研发、中试根据产品经理提出需求，对新品进行海选。   主要考虑几点：   * 1. 产品应该从合格供应商厂家选择   2. 产品应该符合要求的功能   3. 产品应该符合要求的性能   4. 产品应该符合要求的成本   5. 产品能够按照要求的供货周期供货 * 完成选型后填写《新品硬件平台参数详表》 | | | | | 硬件研发（召集人）  产品经理、供应链、  中试 |
| **2.1** | 筛选 | | * 对于满足性能、价格需求的硬件平台，进入评测阶段 * 供应链对供应商初步谈判输出《供应商评审表》 * 由产品测试输出《性能测试报告》 * 由中试部输出《硬件平台测试报告》 | | | | | 供应链（召集人）  中试（召集人）  产品测试 |
| **3** | 选型会 | | * 由硬件研发**发起评审会** * 根据《新品立项需求表》、《硬件平台评测报告》、《性能测试报告》《供应商评审表》等数据 * 最终输出《选型会签表》 * 供应链开始正式商务谈判，并签订相关供货合同 * **启动软件研发** | | | | | 硬件研发（召集人）  供应链、产品经理、  中试、软件研发 |
| **4** | 样机确认 | | * 由中试整理《BOM表》，通知供应链、产品经理，并安排厂家制作样机。 * 由硬件研发、中试确认样机合格后进入产品中试阶段 | | | | | 产品经理（召集人）  中试、硬件研发、供应链 |
| 5 | 产品中试 | | * **启动产品中试** * 由中试小组安排整个中试计划：  1. 测试周期为7日（工作日，如遇2款同时增加3个工作日） 2. **产品经理在中试期间提交**《软件交接单》、《光盘内容提交单》、《硬件信息文件交接单》、《手册内容》、产品经理安排测试更新生产服务器、提供LICENSE文件等产品信息，由中试验证。 3. 中试按照中试流程分别对产品做内部结构、外部结构、散热、电性能、稳定性、一致性、可维护性、可生产性、可量产性、相关器件辅料品质、软件生产等方面测试。 4. 工程化人员**启动工程化工作，**准确编写《BOM表》，整理《工程注意事项》。  * 中试测试完毕后，中试填写《中试报告》 * 中试合格后转入第４步骤，工程化传递生产线BOM及EN * 不合格回转第２步重新进行新品选型工作。 | | | | | 中试（召集人）、  产品经理、硬件研发 |
| 6 | 产品定型 | | * 新品中试结束， **召集中试评审会** * 中试通知产品经理、供应链、硬件研发，通过**《会签中试报告》**，来判断是否发布此新品。 | | | | | 中试(召集人)  产品经理、硬件研发、供应链 |
| 7 | 产品发布 | | * 由产品经理通过总裁审批发布，召集**新品发布会**，确认供货政策、周期、开始供货时间。 | | | | | 产品经理（召集人）、中试  供应链 |
| 8 | 新品试生产（小批量） | | * 新品试生产工程化人员需要产线指导，生产工程师及产线工人一起测试，并按要求提供测试数据 * 中试人员整理**《新品试生产记录表》** | | | | | 供应链（召集人）、中试 |
| 9 | 新品试生产下线 | | * **召开量产会**，核对生产的所需文件，完成批量生产前的交接。 | | | | | 供应链 （召集人）、中试、产品经理 |
|  | | | | | | | | |
| **流程输入** | **步骤编号** | **输入部门** | | **输入内容** | **输入标准** | | | **载体名称** |
|  |  | |  |  | | |  |
| **流程输出** |  |  | |  |  | | |  |
|  |  | |  |  | | |  |

产品经理将中试最后确认的软件生产文件存放在FTP服务器上供硬件供应商通过专用账号下载，同时附带该文件的MD5校验码文件，用于生产文件进行一致性校验。硬件供应由硬件供应商按照《防火墙生产指导书》进行产品的生产、检验、老化测试、包装，按照《产品随机光盘母盘》生产产品的随机光盘。并将产品发给用户，同时提交《产品装箱单》、《保修卡及服务承诺》。并将客户信息、产品信息提交给客户服务人员。

客户服务人员，根据客户产品信息、保修卡服务承诺，向用户提供售后服务，包括：上线实施、后续问题响应。过程需要严格按照《清华永新防火墙产品上线实施作业指导》、《清华永新网络项目实施管理规范》进行。

1. 交付件

|  |  |
| --- | --- |
| **交付件** | **说明** |
| 1. 《产品测试申请单》 | 产品在研发人员完成开发和集成测试后，提交产品测试人员的交付件，包括产品信息唯一性标识、获取方式、生产过程等 |
| 1. 《研发测试报告》 | 产品在研发人员完成开发和集成测试后，提交产品测试人员的交付件，包括：功能说明、预期结果、实际测试结果等 |
| 1. 《产品需求规格》 | 产品研发立项时对产品要实现功能、规格的详细描述 |
| 1. 《清华永新防火墙产品上线实施作业指导》 | 清华永新防火墙产品上线实施作业指导，是产品上线实施的指导性文件，其中包括了上线前的准备、上线步骤、故障排查等详细说明 |
| 1. 《清华永新防火墙通用软件、光盘、生产文件提交单》 | 是由产品经理发布给中试、工程化负责人的产品相关唯一性标识，包括产品内容、产品说明文档、产品生产方式等 |
| 1. 《产品随机光盘》 | 是由产品经理发布给中试、工程化负责人的产品使用说明文档光盘 |
| 1. 《产品装箱单》 |  |
| 1. 《保修卡及服务承诺》 |  |
|  |  |

1. **安装、生成和启动程序**

# 客户服务与技术支持

通过运行Internet浏览器的任何计算机使用HTTP或一个安全的HTTPS连接，您便能够配置并管理清华永新TN-SG5000设备。建议管理计算机显示器使用的分别率为1280X1024。基于web的管理器支持多种语言。配置清华永新UTM设备使其接受来自任何清华永新TN-SG5000设备接口的HTTP与HTTPS管理访问。

清华永新TN-SG5000技术支持帮助用户快速安装，配置简便，操作方便。

# 硬件安装

本章节讲述如何将清华永新TN-SG5000设备安装到机房，环境要求，和如何上机架。

本章涵盖以下部分：

* 环境要求
* 注意事项
* 安装清华永新TN-SG5000
* 关闭清华永新TN-SG5000

**环境要求**

首先，需要确定机房的环境是否能够满足清华永新TN-SG5000使用的要求

* 工作温度 0 to 40°C

如果是将设备安装与机架，则要注意的是，在机架上的温度有可能高于室温，所以说设备工作周围温度一定要匹配设备安装要求。

* 保存温度-25 to 70°C
* 湿度: 5 to 90%非凝结
* 气流- 机架安装时要考虑到是否有足够的气流以保证系统的安全。
* 独立安装时，需要确定设备周边有3.75cm的距离，以确保足够的空气流动空间和冷却所需。

该设备符合part FCC Class A or Class B, Part 15, UL/CUL, C Tick, CE和VCCI的要求。

**注意事项**

首先，需要确定机房的环境是否能够满足清华永新TN-SG5000的要求

接地

* 确保接地状态正确。
* 尽可能采用屏蔽双绞线，而非非屏蔽双绞线。
* 当设备开机时，请勿接线和断线，防止给设备带来危害。

机房内的地板可采用高架地板。对较大的计算机系统采用高架地板有下述优点：

* 避免信号电缆与电源线交错，有碍观瞻，且电缆线穿梭于地板下，铺设不受限制。
* 保护电源、电缆线及接头。
* 未来扩充设备时机器易于重新摆置。
* 计算机机房外观美观。
* 避免工作人员绊倒。
* 机器的重量分散在整个地板结构上。
* 地板强度
* 当机房铺设高架地板时，必须考虑地板是否能支撑机房所有设备的重量，在计算所需的地板强度时必须考虑：
* 计算机主机及所有外围设备的重量
* 辅助设备的重量，如桌、椅、储柜、打字机等
* 工作人员的重量
* 高架地板的重量(约每平方英尺10磅或每平方米48.8斤)
* 电缆线重量(约每平方英尺0.85磅)
* 高架地板
* 高架地板应具有下列性质：
* 高架地板高度在20～30公分(8～13英寸)
* 高架地板尺寸，长×宽不大于60公分×60公分(2英尺×2英尺)
* 点荷重(Point Load)：454公斤
* 高架地板有接地处理，即支架与金属地板应与建筑物接地以导线连接
* 地板绝缘电阻大于150K欧姆,小于20,000M欧姆
* 地板面使用有乙烯基或其他防静电材料

**安装设备**

机房内振动度不得高于0.5g。机房内避免将产生震动的机器放置在一起，因颤动会使机器内的机械部分、接头、主机面板接触部分产生松动，造成机器工作不正常。

对于落地型设备，当体积较大、重量较大且易滑动或易倾倒，设备应具备抗震加固特性。

**关闭清华永新TN-SG5000**

关闭清华永新TN-SG5000建议采用以下步骤，避免可能的硬件问题：

1 进入管理界面，找到“系统>状态”

2 设备操作显示处，选择“关闭”。或者在命令行下输入

execute shutdown

3 拔掉电源线

**软件安装**

本章节讲述如何将清华永新TN-SG5000设备软件初始化和配置。

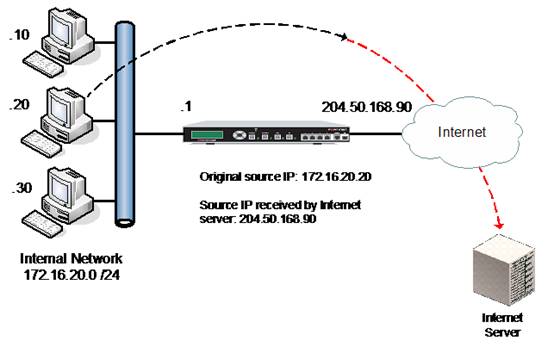
本章涵盖以下部分：

* 设置源地址转换
* 如何设置映射服务器
* 检查网络连通性

**设置源地址转换**

缺省情况下，端口地址翻译为外部接口IP地址，配置如下：

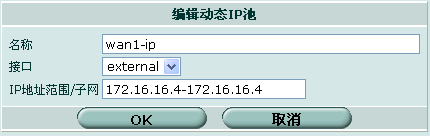




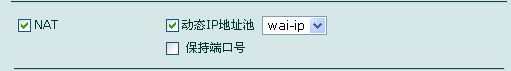
 多对一的源地址转换是通过转换源端口来实现的。理论上上，最多一个公网地址可以支持64500个会话。如果选择”保持端口号“，则无法实现多对一的地址映射。

**如何设置源地址转换——不使用接口地址**，而是将地址翻译成指定范围的IP地址：配置如下

1、进入防火墙>虚拟IP >IP池



1. 在防火墙对应策略里面引用上面配置的地址池，如下所示：



1. 如何来验证

可以登陆防火墙命令行下面执行命令抓包：diagnose sniffer packet any ‘icmp’

4、然后在内网机器：ping [www.sina.com.cn](http://www.sina.com.cn/)这时候可以在防火墙命令行下抓看到进出接口名称及源目的IP地址以确认转换成功。

**如何设置映射服务器**

1. **一对一映射**

进入防火墙---->虚拟IP 新建一个虚拟IP项目，如下图：

1. **端口映射，**

进入防火墙---->虚拟IP 新建一个虚拟IP项目，如下所示：



**3、设置服务器的负载均衡**

进入防火墙---->虚拟IP 新建一个虚拟IP项目，如下所示：



**4、添加允许访问服务器的策略**



**5、如何验证：**

将内部服务器10.0.X.1映射到192.168.11.10X，让旁人从external接口ping 192.168.11.10X，然后登陆到命令行下面用下面的命令抓包分析：diagnose sniffer packet any ‘icmp’ 4

**检查网络连通性方法**

**1、适用范围**

所有的运行在NAT或者TP模式下面的清华永新TN-SG5000设备。

**2、说明**

本文描述的是在清华永新TN-SG5000上面检查网络连通性的三个典型步骤，这三个步骤的输出信息同样对于清华永新TN-SG5000技术支持中心来说是非常有用的也是提交tcket必须的附件。

我们假设的网络环境如下显示：

**[ PC1 ] ===   portA [** TN-SG5000 **] portB ==== [ PC2]**

PC1和PC2分别直连在清华永新TN-SG5000的portA和portB口上或者是跨过路由器连到清华永新TN-SG5000的portA和portB口上，出现的问题是PC1不能连接到PC2。

**3、解决方案**

大体上的故障排除过程如下：   
步骤一：sniffer  
步骤二：debug flow  
步骤三：session list

**步骤一 sniffer**

可以让PC1持续的ping着PC2然后确认如下几个问题结果：

1. Ping请求包是否从所期望的清华永新TN-SG5000网口收到；
2. 检查ARP请求是否正确的从目的接口发出去；
3. 检查ping请求包是否从期望的清华永新TN-SG5000几口发出去；
4. 检查ping响应是否从上面的出接口收到；
5. 检查ping响应是否正确的从清华永新TN-SG5000的portA口发向PC1。

具体命令如下：

**TN# diagnose sniffer packet any "host <PC1> or host <PC2>" 4**

或者

**TN# diagnose sniffer packet any "(host <PC1> or host <PC2>) and icmp" 4**

在sniffer过滤器里面可以同时增加ARP协议，这样有助于发现到PC2的ARP请求响应是否正确。 具体命令如下：

**TN# diagnose sniffer packet any "host <PC1> or host <PC2> or arp" 4**

敲“CTRL+C”可以中止sniffer

Sniffer命令参数‘4’可以显示出报文具体的进口和出口。

**步骤二，debug flow**

正确的ping包应该可以正常的穿过清华永新TN-SG5000，如果没有正常穿越，可以尝试用debug flow命令来查找问题：

**diag debug enable   
diag debug flow filter add <PC1>    或者    diag debug flow filter add <PC2>   
diag debug flow show console enable   
diag debug flow trace start 100    <== 这样可以查看到前100个报文   
diag debug enable**

要停止debug flow，可以使用命令 "diag debug flow trace stop"

1. 下面是debug flow具体的数据流由于没有匹配上了防火墙策略而被阻挡输出：

**id=20085 trace\_id=319 func=resolve\_ip\_tuple\_fast line=2825 msg="vd-root received a packet(proto=6, 192.168.129.136:2854->192.168.96.153:1863) from port3."**

**id=20085 trace\_id=319 func=resolve\_ip\_tuple line=2924 msg="allocate a new session-013004ac"**

**id=20085 trace\_id=319 func=vf\_ip4\_route\_input line=1597 msg="find a route: gw-192.168.150.129 via port1"   
id=20085 trace\_id=319 func=fw\_forward\_handler line=248 msg=" Denied by forward policy check"**

1. 下面是debug flow具体的数据流匹配上了防火墙基于策略IPSEC VPN策略ID＝2的输出：

**id=20085 trace\_id=1 msg="vd-root received a packet (proto=1, 10.72.55.240:1->10.71.55.10:8) from internal."  
  
id=20085 trace\_id=1 msg="allocate a new session-00001cd3"  
  
id=20085 trace\_id=1 msg="find a route: gw-192.168.56.230 via wan1"  
  
id=20085 trace\_id=1 msg="Allowed by Policy-2: encrypt"  
  
id=20085 trace\_id=1 msg="enter IPsec tunnel-RemotePhase1"  
  
id=20085 trace\_id=1 msg="encrypted, and send to 192.168.225.22 with source 192.168.56.226"  
  
id=20085 trace\_id=1 msg="send to 192.168.56.230 via intf-wan1“  
  
id=20085 trace\_id=2 msg="vd-root received a packet (proto=1, 10.72.55.240:1-10.71.55.10:8) from internal."  
  
id=20085 trace\_id=2 msg="Find an existing session, id-00001cd3, original direction"  
  
id=20085 trace\_id=2 msg="enter IPsec ="encrypted, and send to 192.168.225.22 with source 192.168.56.226“ tunnel-RemotePhase1"  
  
id=20085 trace\_id=2 msgid=20085 trace\_id=2 msg="send to 192.168.56.230 via intf-wan1"**

**步骤三，session list**

再进一步的故障分析可以检查防火墙的连接表，连接表查看支持过滤器设置，可以根据具体的源目的IP地址或端口等信息过虑需要查看的防火墙连接表信息，具体如下：

**diag sys session filter src PC1   
diag sys session list**   
或者

**diag sys session filter dst PC1   
diag sys session list**

清楚过虑器过虑出来的防火墙连接的命令如下：

**diag sys session filter dst PC1   
diag sys session clear**