

网管员最喜爱的产品推介方法

以上产品统一参加评选，主办者将对所有参选产品进行统一编号和统一推介。
其内容主要分为以下几部分：

- **产品推荐**

产品的简要介绍（600 字左右）和产品图片一张（图片为 Tiff 格式，分辨率不小于 800*600）。

- **应用案例**

案例文字在 1200 字左右，案例拓扑图一张（图片 Tiff 格式，分辨率不小于 800*600）；

- **技术特写**

技术特写文字在 1200 字左右，如需图片，每张图片减 200 字左右。

为用户提供快速、安全和自动化的远程维护方案

VNN4.7 远程维护产品

一键连天涯，维护无极限！

一、产品推荐：

1.关于美国维恩网络和 VNN 产品：

- ◇ 美国维恩网络公司成立于 2006 年，总部位于加州硅谷，属于创新技术产品公司，专注于构建虚拟专网和数据快速传输技术的发展；
- ◇ 拥有世界一流的技术研发团队，为国内最大的远程安全通讯运营服务提供商；
- ◇ 公司研发中心和国内总部设在北京，在华中设有办事处，核心研发和管理成员来自赛门铁克、Netscreen 和天融信等安全厂家；
- ◇ 公司 CEO 为前 Sygate 创始人之一，投资方为种子基金等风险创投公司；
- ◇ VNN 产品主要包括多 VPN 网络系统，远程技术支持维护平台、快速文件传输平台、软件 VPN 服务和云计算的虚拟桌面。

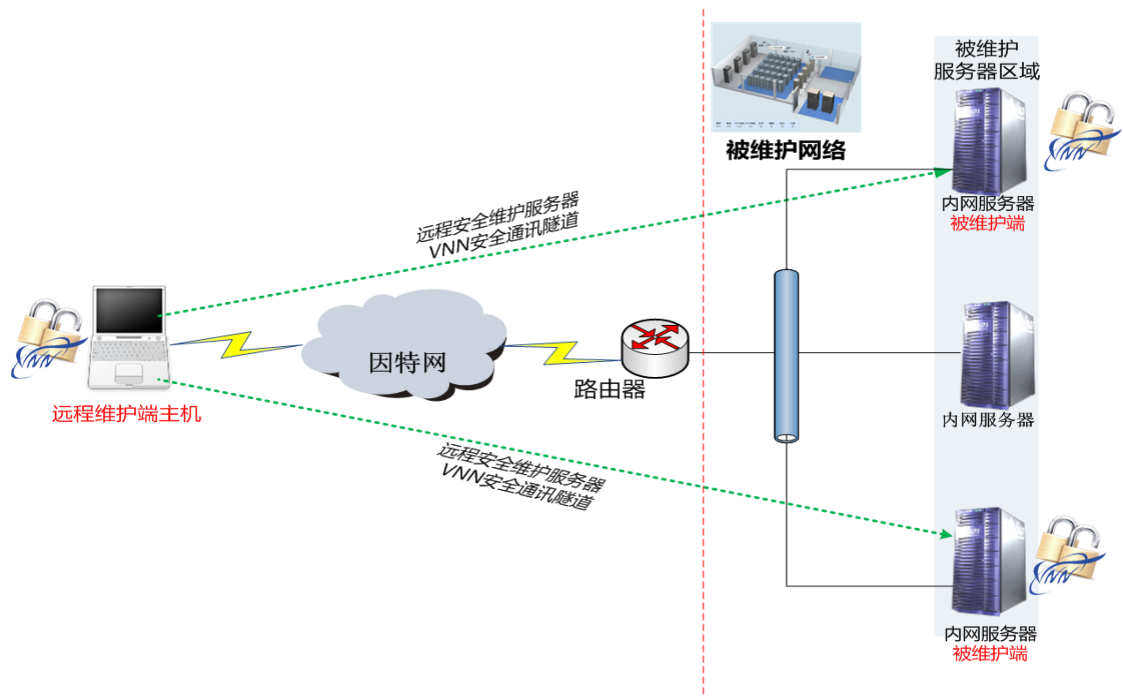
2.VNN 远程维护产品介绍：

针对用户 IT 远程维护需求所专门开发研制的安全通讯产品，内置了多个特色功能：一键维护、应用发布、文件快递、统一管理和安全保护等，具有使用简单、安全、快速和集中控制的特色，同时融合了多种 VPN、远程维护产品的优点。

VNN 远程维护的三种模式：

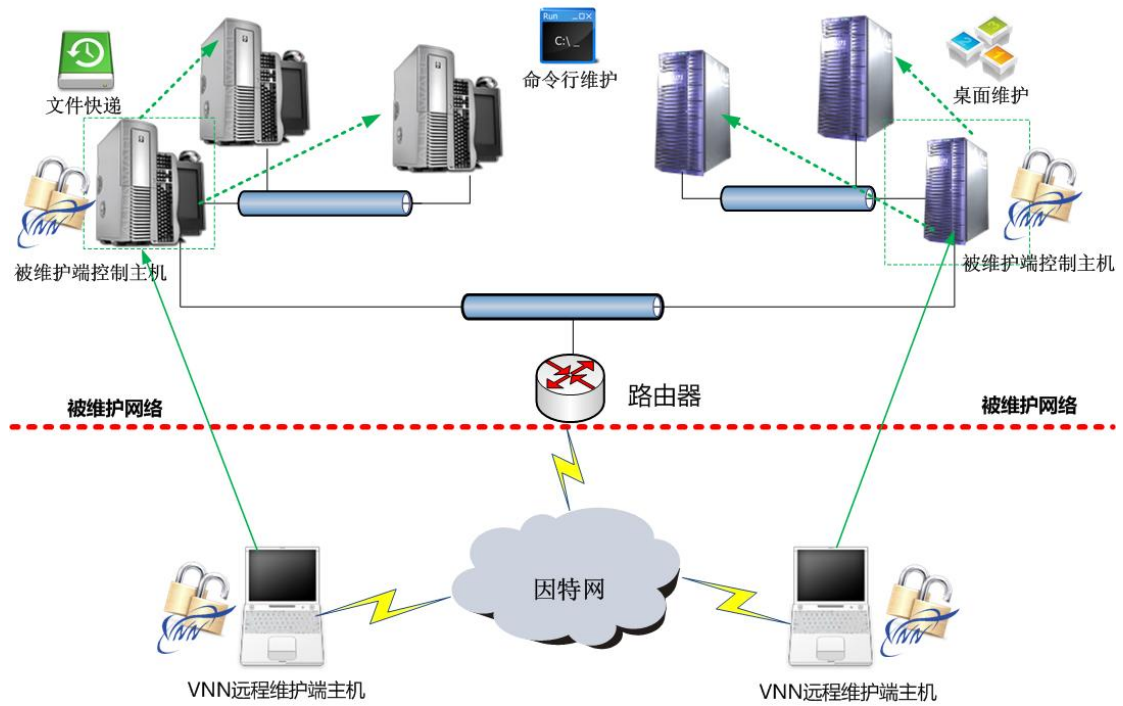
VNN 主动维护模式 A（适合维护端主动进行直接维护操作）

在需要被维护服务器上安装 VNN 安全通讯软件----此服务器为被控端，在远程维护 PC 上安装 VNN 安全通讯软件----此主机为维护端，被维护端和维护端使用各自 VNN 帐号登陆后处于同一虚拟局域网内即可进行远程维护工作。实施网络拓扑如下图所示：



VNN 主动维护模式 B（适于维护端主动维护多台服务器）：

在用户被维护端某台联网主机上安装 VNN 安全通讯软件----此主机统称为被维护端控制主机，在远程维护 PC 上安装 VNN 安全通讯软件----此主机统称为维护端，在被维护端控制主机上对内部其他需要被维护的服务器或网络设备进行应用发布设置后即可让远程维护端用户主动对 IDC 多台服务器或设备进行快速远程维护工作，部署网络拓扑图如下：



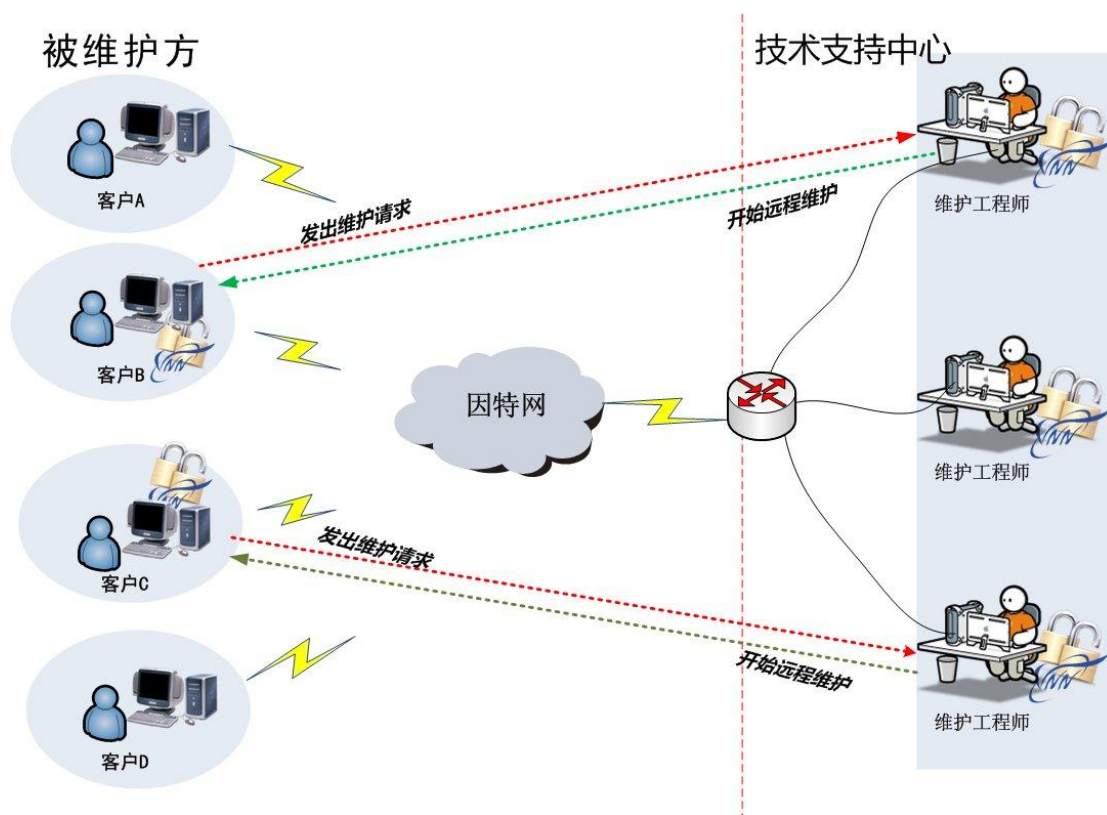
集成维护应用的界面截图如下：



VNN 按需维护模式：（适于被维护端主动发出维护请求，维护端接受请求后开始维护工作-----常见使用场景为硬件厂商为自己的用户提供远程技术支持服务）

在用户需要被维护的主机上安装 VNN 安全通讯软件（VNN 可与第三方应用软件集成作为其远程维护模块）----此主机统称为被维护端主机，在远程的厂商技术支持中心主机上安装 VNN 安全通讯软件-----此主机统称为维护端主机，当用户发起维护请求后，厂商技术支持中心工程师将通过 VNN 搭建的安全通讯隧道开始相应的维护操作，被维护端主机上将显示工程师维护操作过程。

远程维护示意图如下所示：



三、应用案例

VNN 远程维护典型案例：

三信时代信息公司

----北京西部最大的 IDC 中心，向客户提供主机托管、宽带接入和虚拟主机等服务。

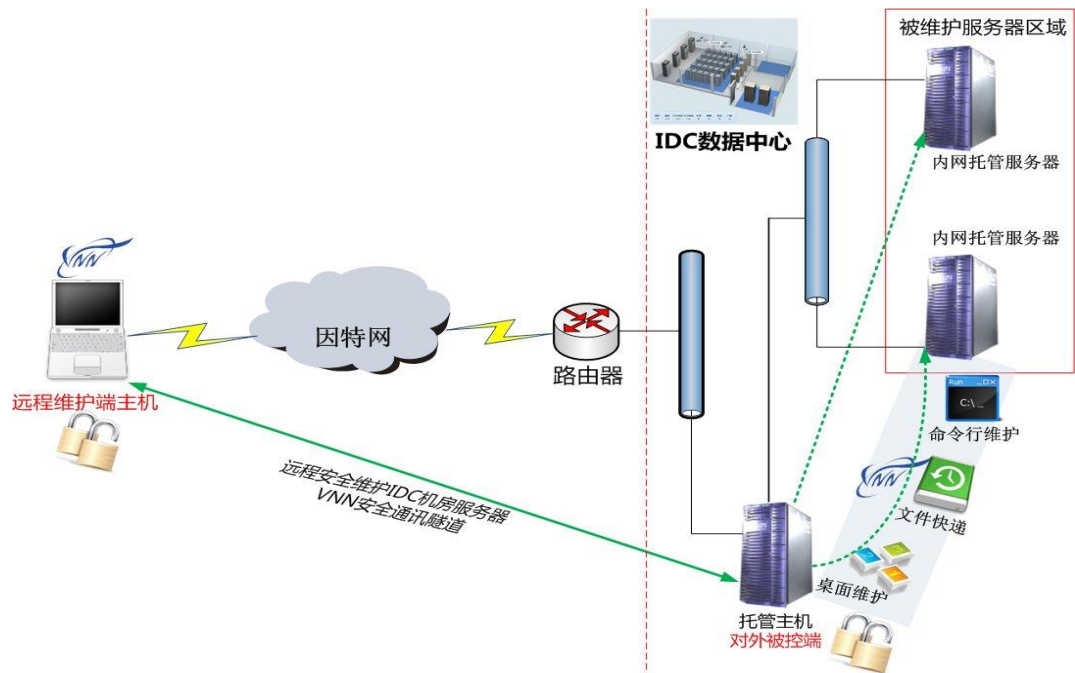
用户需求：

很多用户需要从远程对托管在 IDC 中心的服务器进行维护（例如网站公司的运维人员、大型企业公司的网管还有 IDC 中心的运维工程师等），维护工作主要包括：监视服务器和网络设备运行状况、查看网站用户访问日志、更新网站内容和升级服务器重启服务器等等。

VNN 提供的解决方案：

由三信时代向其用户提供 VNN 远程维护工具，分别在被维护端主机和维护端管理主机上安装。两端主机通过 VNN 构建的虚拟本地网络安全通讯隧道进行快速安全访问。

IDC 数据中心远程维护 VNN 实施拓扑图



VNN 远程维护方案在此 IDC 远程维护项目中具有的特色功能:

- a) 不需要在托管服务器上面开启额外的 TCP 监听端口, 维护数据在安全隧道内部传输, 减少远程维护被攻击的风险。
- b) 不需要额外部署设备占用用户托管机位, 在能够连接外网的一台托管主机上安装 VNN 远程维护软件即可维护内部多台服务器和 IP 设备。
- c) 不论托管的服务器是否有公网 IP, 都可以快速直接访问维护。
- d) 内置文件传输系统, 可以批量、自动在多台不同的服务器和电脑之间进行数据传输, 方便自动下载日志等。

VNN 远程维护用户列表:

三信时代	IDC 服务商, 使用 VNN 为用户提供远程维护增值服务
ICD Security (联科电子)	以色列智能安防厂商, 使用 VNN 对用户安防系统软件进行远程升级维护操作;
上海中智计算机服务公司	IT 外包服务商, 使用 VNN 给自己的医院用户进行 HIS 等服务器维护及 PC 桌面支持
北京华仪软件	酒店管理软件厂商, 使用 VNN 对部署在客户服务器上的酒店管理软件进行远程维护和升级操作
BTA (桥盟创联)	终端节点安全软件厂商, 使用 VNN 为自己的终端用户提供远程技术支持服务
东莞润赢电力	使用 VNN 远程维护部署在各配电站的数据采集设备
沸蓝网吧	华东网吧运营服务商, 使用 VNN 进行网吧服务器远程维护
中国通讯建设集团	中国最大的涉外通讯工程承建商, 通过 VNN 远程维护各地服务器

三、技术特写:

1. 远程维护的需求场景:

- a) 出差或者异地办公的企业网管, 远程维护本企业的远程电脑或者网络设备;
- b) 软硬件厂商的工程师给自己的用户提供远程网络技术支持;
- c) 以远程维护作为服务的公司 (IT 维护外包): 远程维护客户网络中的服务器和 PC;
- d) 对 IDC 中心的托管服务器进行远程维护及升级操作, 网站服务器内容更新。

- e) 远程使用家里或单位的计算机、远程为亲朋好友解决计算机或网络问题。

2. 远程维护的功能要求：

- ◇ 远程维护产品的部署不会改变现有网络架构；
- ◇ 远程维护产品的自身安全性，不会成为骇客攻击进入的跳板；
- ◇ 支持自动化操作，可以无人值守维护；
- ◇ 支持客户发起维护请求，提醒维护端工程师进行维护；
- ◇ 维护工具操作简单，具备集中维护应用界面，使用方便灵活；
- ◇ 能对各种网络设备和系统主机进行集成维护；
- ◇ 具备严格的访问控制和中央管理功能。

3. 目前常见远程维护通讯工具的难题：

- a) 通过硬件设备构建的专用网络：
 - 将改变现有网络架构
 - 网络访问范围过大
 - 设置安全网络隧道参数和访问策略配置复杂
 - 集中维护和管理不方便
- b) 使用专业的远程访问软件：
 - 被维护端需要具有公网 IP，易成为固定目标被攻击
 - 使用跳转多点维护时操作复杂并难以做访问控制
- c) 使用即时通讯软件提供的远程协助功能：
 - 不支持无人值守自动化维护操作
 - 无法避免大众通用软件容易引起的攻击和漏洞
 - 非企业商用软件产品，很多公司禁止使用

4. VNN 远程维护通讯工具的相对优点：

- a) 旁路单点部署，即可维护多台服务器及设备，不改变网络拓扑；
- b) 具有维护应用资源发布和中央控制功能，可以方便地进行维护访问控制，可将需要被维护的后台主机及 IP 设备资源统一发布在界面上进行统一集中管理维护操作；
- c) 安全通讯隧道搭建简单自动化，无需用户进行复杂设置；
- d) VNN 内置的远程控制功能，具有无人值守即可访问到桌面、安全口令认证等特点；

- e) 企业重要的内部数据库、核心业务服务器或小型机在它们不允许访问外网的情况下也可以被维护。
- f) VNN 内置的 Web 文件共享功能，可以从被维护端主机上将文件快速下载到本地；
- g) VNN 内置的文件快递功能，可以将大批量文件（文件夹）按照自定义时间自动上传到指定服务器的指定文件夹中，或者将服务器上的文件快速进行异地备份和存储。
- h) 被维护端控制主机无需静态公网 IP，能联网即可，降低了固定 IP 目标被扫描和暴力攻击的可能。

此外，通过 VNN 结合第三方维护软件也可以方便地对远端服务器进行各种维护操作：

使用 SSH 命令行工具：Putty/SecureCRT 等。

使用专业维护工具：SolarWinds 等

使用远程桌面类工具：微软远程桌面/VNC/PC Anywhere 等。

5. VNN 远程维护产品具有如下特点：

a) 维护资源集成发布：

可以将所需维护的主机资源全部发布到一个界面上去，供远程工程师进行统一访问和使用，如下图所示：



b) 被维护端可无人值守自动化维护:

与某些通讯软件自带的远程协助功能不同，VNN 的远程维护功能支持无人值守自动维护，远程不需要用户配合，可以直接操作，包括重启服务器等。

c) 支持两种模式的运维:

可以工作在远程无人模式，也可以允许远程用户配合进行维护操作。

d) 多系统多设备支持:

既可以支持 Windows 的服务器和电脑，又可以维护非 Windows 的系统，包括网络设备、IP 摄像头和打印机等。

e) 安全性高:

不同于常见的 VPN 硬件，不会由于需要被远程维护，就暴露整个被维护的内部网络。VNN 点对点的通讯模式，仅允许访问被维护的服务器；内部的数据库、核心业务服务器或小型机可以在不允许访问外网的情况下被维护。

f) 防护级别高:

对远程维护人员做双因子认证，远程维护数据加密处理，非静态端口通讯，降低被攻击的可能。

g) 中央访问控制:

内置隧道防火墙，可对被维护服务器进行安全访问控制。

h) 跨运营商加速:

针对跨 ISP 访问慢的难题，具有广域网加速访问功能，可有效提高远距离跨 ISP 的访问维护速度。

i) 支持文件自动化快速传输:

内置快速文件共享分发功能，方便传送补丁包、升级文件等软件到被维护的主机，同时也适用于网站服务器的内容定时更新。

j) 支持详细日志:

包括登陆日志便于审计技术支持的工作，详细操作日志可以自动记录被操作的截屏。

k) **高性价比:**

可以按照维护工程师和并发被维护用户数来计费，有限的账号，维护无限的用户。

l) **灵活的收费模式:**

支持按年服务费的方式，也支持一次买断的方式，可以自己搭建远程维护平台。

附录:

VNN 远程安全通讯软件系统要求:

1. 支持 Windows 2000 以上所有的版本，包括 64 位系统。
2. 通过 Windows 系统，间接支持非 Windows 的系统，包括网络设备和 Linux 系统。
3. 每个用户，至少需要 2 个 VNN 账号进行远程维护工作。

名词释义:

****VNN 虚拟本地网**是一种 VPN 产品，它能够让处于不同物理位置的主机通过 VNN 搭建的虚拟专用隧道进行安全、稳定和快速的双向通讯。VNN 使用了智能探测和连接技术，在各端主机无静态公网 IP 并处于各自内部网络的情况下，可以把所有网络主机连成一个虚拟本地网络。

在此虚拟本地内的主机就如同在实际的局域网中，可以通过因特网网进行数据实时交互和访问各种应用，例如各种基于 C/S 或 B/S 架构的企业应用、远程桌面、远程演示、语音会议、文件共享、文件快递和即时通讯等等。

IDC----互联网数据中心 (Internet Data Center) 简称 IDC，是电信或者专业公司利用已有（或租用）的互联网通信线路、带宽资源，建立标准化的电信专业级机房环境，为企业、政府提供服务器托管、租用以及相关增值等方面的全方位服务。