Network VirusWall Enforce 2500 FAQ

问题：应用层中的病毒与网络层中的病毒相比之下有什么不同？

答：当数据通过网络从一个计算机传送到另一个计算机时，这些数据被分割成一个个小的部分，或者被分成一个个数据包，为了更加有效的传输，会在这些数据包中加入标签以及地址信息例如MAC 以及目标计算机的IP。最初的应用层数据可能被分割为许多数据包并通过网络传输。此外，那些运行在应用层的软件是不能觉察到网络层的数据包。因此，传统的病毒解决方案就是扫描传输的数据。这需要等到所有的数据包全部到达目标计算机并重新组成一个完整的物理文件。但是网络病毒诸如蠕虫病毒可以嵌入到单个数据包，在所有数据包还没有组成一个完整的文件前，感染目标机器。

问题：NVWE 扫描哪些协议？

答：NVW 扫描所有通过网络的 TCP、UDP 和 ICMP 协议。

问题：NVWE 听起来和入侵检测系统非常相似，它是入侵检测系统吗？

答：不是，尽管 NVW 和入侵检测系统都侦测网络层的通讯，并且很多入侵检测系统和 NVW 一样使用签名文件，但是在总体解决方案上还是有区别的。NVW 的设计是为了防止利用现有网络中的漏洞进行传播扩散的网络病毒。入侵检测系统首先设计是为了防止骇客和未授权用户利用网络漏洞或其他途径进行入侵。作为入侵检测的一部分，入侵检测系统要求多种启发式的程序植入到企图防止一系列已知的、能够获得未授权入侵的技术的解决方案中去。然而这些启发式的方案通常很难奏效或是有大量的负面影响。

问题：如果我在网络中已经安装了使用病毒码文件的入侵检测系统，那我还需要网络病毒防护吗?

答：还是需要的。尽管入侵检测系统可以使用病毒码文件，但是很多公司并没有专业人员来及时制作病毒码文件。因此在得到一个病毒码文件之前，客户的业务和网络很可能已经遭受了重大损失。与此相对应的是，Network VirusWall 可以获得趋势科技专家的支持，而趋势科技被商业周刊评为发布新病毒码文件速度最快的供应商之一。此外，当前很多入侵检测系统无法隔离或清理受到感染的网段。因此即使这些入侵检测系统获得了网络病毒码文件，它们也只能够封堵流经它的已知网络病毒，却无法对网络中已受感染的系统进行清理。

问题：NVWE 可以脱离 TMCM 独立操作吗？

答：可以，NVWE 注册到 TMCM 是可选操作。但 NVWE 的 OPP 必须通过 TMCM 来部署启用。

问题：什么是OPS?

答：当病毒爆发时 Network VirusWall Enforce 可以从 TMCM 接收爆发预警，通过 OPP 的设置，Network VirusWall 可以封闭以下选项：

1、IP 地址：单个目的 IP 或者一组 IP 地址
2、协议：TCP,UDP,ICMP
3、端口：单个目的端口或者一组端口
4、即时通讯：AOL,ICQ,MSN and Yahoo Messenger
5、文件传输：通过 FTP 或者 Http 传输的文件，网络文件的共享
6、网站：单个或者多个网站

问：NVWE 支持病毒发作防御策略（OPP）吗?

答：支持。在病毒发作期间，管理员可能需要从TMCM来发布OPP来封堵各种网络行为。此外，NVWE 的OPP还可以提供较大程度和细化的控制，因为它们在网络层操作的。使用 NVWE，管理员就可以根据端口、协议、IM特定数据类型、Windows文件共享数据类型以及文件名称和扩展名来实施封堵。但是，就像Network VirusWall只能够扫描网络数据包一样，NVWE OPP 不能够根据特定内容来进行封堵。内容封堵工作最好留给OfficeScan、IMSS以及IWSS等传统的防病毒解决方案来做。

问题：NVWE 的 OPPs 和其他产品的 OPPs 有什么不同？

答：两者之间最直接的不同点是，其他产品执行的 OPPs 封锁了应用层，NVW是通过网络传输将 OPPs 部署到目标。NVWE 的 OPPs 可以封锁指定端口的传输，例如文件传输、即时通讯。应用层的 OPPs 在则可以封锁邮件（基于标题、内容、附件的封锁），这两种 OPPs 互相完善，仅仅在封锁传输的功能有所相似。目前趋势的产品除了 NVWE 外，其它软件产品都是运行在应用层。

问题：NVWE能够检测和配置所有来自其他供应商的防病毒解决方案吗?

答：可以。NEW 现在可以通过在客户端部署代理程序（PEAgent）来检测市场上常见的杀毒软件。并且随着 NVWE 程序组件的更新，支持的杀毒软件的版本也在增加。

问题：NVWE 的防病毒策略实施机制是否需要使用代理?

答：需如果NVWE的Policy Enforcement(强制策略)只检测趋势科技的杀毒软件，并且没有进行其他强制策略，则可以不需要安装PEAgent。对于其他情况，客户端必须安装PEAgent来进行强制策略。

问题：安装了 NVWE，是否客户端就不用安装防毒客户端了？

答：NVW 不能扫描/检测特殊病毒(例如:邮件附件中病毒，文件病毒)，那是因为NVW 扫描数据包.它扫描每个数据包是基于以下规则：

1、依照不同类型扫描不同数据
2、源 IP 地址,源端口号
3、目标 IP 地址,目标端口号
4、Regular expression
扫描数据包(不包括包头)

如果网络病毒包含简单的攻击系统漏洞的命令,那么,NVWE能够通过包扫描监测到这类病毒.传统的文件病毒是不同的,除非我们合并所有的数据包

并且扫描整个文件,否则被感染的文件将不能被监测到.但是这样做,会降低NVWE的性能.因此我们建议对于文件病毒采用趋势科技其他产品(例如:OSCE, SPNT等等)

问题：NVWE 现在支持哪些杀毒软件：

答：请参考以下截图（2043 版本）。对于这些杀毒软件的具体支持版本，请联系趋势科技技术支持。

Product	Vendor
Trend Micro OfficeScan	Trend Micro, Inc.
Trend Micro PC-cillin	Trend Micro, Inc.
Trend Micro Server Protect	Trend Micro, Inc.
Symantec AntiVirus	Symantec Corp.
Norton AntiVirus Corporate Edition	Symantec Corp.
Symantec Scan Engine	Symantec Corp.
Norton AntiVirus	Symantec Corp.
Symantec Client Security	Symantec Corp.
Symantec Internet Security	Symantec Corp.
Symantec SystemWorks	Symantec Corp.
McAfee VirusScan	McAfee, Inc.
McAfee Internet Security	McAfee, Inc.
McAfee Managed VirusScan	McAfee, Inc.
eTrust Antivirus	Computer Associates International, Inc.
eTrust EZ Armor	Computer Associates International, Inc.
SOFTWIN BitDefender	SOFTWIN
Panda Antivirus	Panda Software
Panda Internet Security	Panda Software
Panda TruPrevent	Panda Software
Sophos Anti-Virus	Sophos Plc.
Kaspersky Anti-Virus	Kaspersky Labs
Authentium Command AntiVirus	Authentium, Inc.
F-Secure Anti-Virus	F-Secure Corp.
F-Secure Internet Security	F-Secure Corp.
Grisoft AVG Anti-Virus	Grisoft, Inc.
ZoneAlarm Anti-Virus	Zone Labs LLC
ZoneAlarm Anti-Virus	Check Point, Inc
Frisk F-Prot	Frisk Software International
SalD Dr.Web	SalD Ltd.
Eset NOD32 Antivirus	Eset Software
H+BEDV Datentechnik GmbH AntiVir	H+BEDV Datentechnik GmbH
Clam Win Antivirus	ClamWin
SBC Yahoo! Anti-Virus	Yahoo!, Inc.

Sereniti The River Home Network Security Suite	Sereniti, Inc.
Sereniti Antivirus	Sereniti, Inc.
ALWIL avast! Antivirus	ALWIL Software
AhnLab V3 Pro	AhnLab, Inc.
AhnLab Security Pack	AhnLab, Inc.
Rising Antivirus	Beijing Rising Technology Corp. Ltd.
Microsoft	Microsoft Corp.
EarthLink Protection Control Center AntiVirus	EarthLink, Inc.
America Online AntiVirus	America Online, Inc.
eTrust Internet Security Suite AntiVirus	Computer Associates International, Inc.
Panda WebAdmin Client Antivirus	Panda Software
eTrustITM Agent	Computer Associates International, Inc.
Kingsoft AntiVirus	Kingsoft Corp.
Symantec series	Symantec Corp.
McAfee series	McAfee, Inc.
CA series	Computer Associates International, Inc.
Sophos series	Sophos Plc.
Trend Micro HouseCall	Trend Micro, Inc.
Jiangmin AntiVirus	Jiangmin, Inc.
Grisoft series	Grisoft, Inc.
Norman Virus Control	Norman ASA
Norman ASA series	Norman ASA
MicroWorld eScan	MicroWorld
GData AntiVirusKit 2006	GData Software AG
Aluria Security Center AntiVirus	EarthLink, Inc.
Avira AntiVir	Avira GmbH
Defender Pro	Defender Pro
RadialPoint	RadialPoint Inc.
Verizon	Verizon
BellSouth	BellSouth
HAURI	HAURI, Inc.
AEC	AEC, spol. s r.o.
Proventia	Internet Security Systems, Inc.
VCOM System Suite	VCOM
BullGuard	BullGuard Ltd.
K7 Computing	K7 Computing Pvt. Ltd.

问题：为什么我们需要使用特殊的扫描引擎来检测网络病毒，而不是用传统的扫描引擎来检测网络病毒？

答：传统的防病毒软件需要通过完全组合才能知道文件的内容以及主题，所以他们不能处理被感染的网络层数据包,由于以上原因,特别在网络层上监测恶

性代码时,需要独立的扫描引擎以及特殊的病毒代码.

问题：NVWE 可以防护哪些病毒？

答：请参考以下文件中的列表。

http://www.trendmicro.com/ftp/products/nvwpattern/nvp-new.txt

问题：NVWE与Cisco的安全策略实施方案有何不同?

答: Cisco要求防病毒软件供应商（趋势科技、NAI 和 Symantec）在桌面客户端解决方案中实施一项代理服务来与Cisco的策略服务器进行通信。发送信息和作出决定是二元化的。在大多数情况下，其目的仅在于判断是否存在三家防病毒公司的防病毒产品。如果存在，就会命令路由器允许计算机访问网络。否则，访问就会被拒绝。如果实施的是RADIUS服务器，则就可以根据扫描引擎和病毒码文件的版本编号进行策略实施。但是，NVWE要灵活得多，因为它无需在客户端内嵌入代理，也不需要Cisco路由器、Cisco策略服务器或RADIUS服务器，就可以实施防病毒策略。此外，NVWE还可以提供范围广泛的Cisco无法提供的其它安全措施，比如漏洞评估和隔离、网络分段以及网络病毒检测和清除。

问题：我可以拷贝NVWE镜像并将它安装到其它计算机来运行吗?

答：不可以。Network VirusWall具有防拷贝机制，可以防止 NVWE 代码在非 NVWE 的硬件平台上执行。

问题：NVWE检查漏洞时，是否需要用TMVA进行扫描？

答： NVWE进行漏洞检查时，不再与NVW 1.8版本一样，通过TMCM的TMVA功能去检查客户端，而是通过客户端安装的代理软件PEAgent来完成。

NVWE 2500 是否支持千兆接口的速度？

答：是的，Network VirusWall Enforcer 2500 有五个 (5) 用户可配置的铜千兆 LAN 端口和多达 4 个的光纤端口。

此发行版是否支持基于光纤的网络？

是的， Network VirusWall Enforcer 2500 支持基于光纤的网络。本设备随附以下两个物理配置之一： 安装有一个双工多模光纤卡，或者没有安装光纤卡。更多关于受支持的光纤媒体卡的信息，请参考《Network VirusWall Enforcer 2500 入门指南》> 为基于光纤的网络选择光纤媒体连接器一节。

Network VirusWall Enforcer 2500 的日志存储在哪里？我怎样才能访问这些日志？

答:Network VirusWall Enforcer 2500 仅使用 256MB 的 IDE 模块磁盘 (DOM) 闪存盘进行存储。因此，没有可用的内存空间来存储日志文件。Network VirusWall Enforcer 2500 将其常规日志发送到控制管理中心服务器。或者， Network VirusWall Enforcer 2500 也可将系统日志（也包含调试信息）发送到网络中的任何计算机上。有关详细信息，请参考第 2-20 页的配置设备和系统设置 和 第 4-3 页的了解日志。

问题：我能否连接多个 Network VirusWall Enforcer 2500 设备，或者将它们堆叠在一起，以提高吞吐量？

答：是的，通过 Network VirusWall Enforcer 2500 平台，Network VirusWall Enforcer 2500 使用冗余设备实现高可用性 (HA)。请参考第 1-27 页的高可用性 以了解详细信息

Network VirusWall Enforcer 2500 是否支持生成树协议 (STP)？

答：否。Network VirusWall Enforcer 2500 被设计为网络中的透明 L2 设备，所以它将忽略那些数据包。

问题：忘记密码如何恢复？

答：可以通过重新刷 NVWE 的 firmware 来实现。方法：

1、从 http://www.trendmicro.com/download/product.asp?productid=53 下载 Network VirusWall Enforcer 2500 v2.0 Firmware Flash Utility，Program File 文件。其中，Rescue Unility 是用于上传的文件，Program File 需要解压缩。

2、用交叉线连接 NVWE 第五口

3、电脑 ip 设置为 192.168.252.*，(非 1 都可以)

4、然后重新启动 NVWE，进入 Resure 模式，运行 Network VirusWall Enforcer 2500 v2.0 Firmware Flash Utility，选择 Flash DOM，上传 image 文件，上传完成后，NVWE 会自动重新启动。

注意：上传过程中，切勿关闭 NVW 电源！

问题：升级 NVWE Program File 前，我怎样才能备份 Network VirusWall Enforcer 2500 的配置？

答：请使用“预配置 (Preconfiguration)”控制台系统任务 (System Tasks) > 导出配置文件 (Export Configuration File) 选项来备份 Network VirusWall Enforcer 2500 的配置。此外，“预配置 (Preconfiguration)”控制台系统任务 (System Tasks) > 导入配置文件 (Import Configuration File) 选项让您从相同的 Network VirusWall Enforcer 2500 设备导入设置。

您也可以在 Network VirusWall Enforcer 2500 Web 控制台从管理 (Administration) > 备份配置 (Backup Configuration) 执行此程序。

远程登录和 ActiveX 功能能否在 Windows 95、98 和 ME 中使用？

答： 对于 Windows 98 和 ME，此设备只支持 ActiveX，但不支持远程登录。对于 Windows 95，此设备不支持远程登录或 ActiveX。

远程登录和 ActiveX 功能是否支持在 NAT 后的端点中使用？

答：对于在 NAT 后面的端点， Network VirusWall Enforcer 2500 不支持远程登录和 ActiveX

HTTPS 流量为什么没有重定向到阻止页面？
答：此版本的设备不支持解密加密的 HTTPS 流量。

问题： 通过查看 NVWE 的 Endpoint History，发现对于一组不同的 IP 地址，反映出来 MAC 地址的值是一样的，这是怎么回事？
答： 这个现象是因为那些客户机与NVWE不在同一个子网中，通常这些客户机的数据都是从路由器传输过来的，所以NVW只能拿到路由器的MAC地址。

问题：NVWE是否可以防通过共享（比如IPC$）传播的病毒（worm_SDBOT.ZA, SDBOT.MK)? 阻止（TCP/UDP）的什么端口可以防止通过IPC$共享传播的病毒
答：鉴NVWE只能扫描特定的网络型病毒，请参考NVWE所支持的网络病毒列表。对于通过IPC$共享传播的病毒可以通过设置NVWE阻止TCP/UDP 的135~139端口。

问题：在NVWE中设置IP地址除了与TMCM进行通讯，其他还有何作用吗？
答：SNMP, System log 输出, webproxy (警告界面) ，远程安装PEAgent，ActiveX部署PEAgent，与PEAgent进行通讯，SSH。

问题：NVW当OS有问题时会变成纯粹switch的模式,请问会转换成switch的模式的临界判断点哪里?
答：当系统崩溃，OS无响应时。

问题：网络环境中有两台交换机作Trunk，将NVWE直接取代Trunk的那条网线，将两个交换机连在一起，请问NVWE支持这种方式么？
答：支持的。

问题：可以自己更换NVWE的硬件吗？（比如添加内存、更换CPU，这样是否就可以提升性能？）
答：不行。 因为这个在kernel 和硬件上都限死了。

问题：趋势科技如何获得安全补丁数据库和杀毒软件病毒码版本库？
答：趋势科技的TrendLab会维护补丁数据库和杀毒软件病毒码版本库。这2个数据库只是漏洞评估服务和病毒码检测使用的Pattern文件，并不是真正的补丁文件和病毒库文件。

问题：当有3层交换机位于NVWE保护网段内，有什么影响？
答：1、如果3层交换机设置了IP MASQUERADE，那么NVW将无法获得客户端的真实IP。
2、NVWE将无法获得客户端的MAC地址，因为所有客户端的MAC地址会被替换为交换机的MAC地址

问题：该用什么网线来连接NVWE（或者说什么时候使用交叉线连接NVWE）？

答：把NVWE看做是一台普通的PC机，如果你将PC机直接与NVWE连接，那么请使用交叉线（因为他们是同种设备），如果交换机与NVWE连接，那么使用直连线。

问题：NVWE上的网口我该如何连接？

答：把NVWE上的口不再区别INT和EXT。NVWE将会扫描从一个网口到另一网口的数据包。

问题：使用终端程序来设置NVWE时，BackSpace键不起作用？

答：在终端程序窗口点击文件菜单-->属性-->在属性窗口设置-->"Backspce键发送"为Del，点击确定回到空白窗口.

问题：我能否输入 DBCS URL 链接作为重定向 URL 或例外 URL？

答：此版本的设备不支持 DBCS URL 链接。

问题：Network VirusWall Enforcer 2500 是否会阻止 socks4 和 socks5 的活动？

答：此版本的设备不会阻止使用 socks4 和 socks5 的 IM 活动。

问题：用于端点安装的远程登录和 ActiveX 为什么不工作？

答：检查以下各项：

- 如果端点安装有 Windows 98、ME 或 XP Home，则不支持远程登录。
- 在 Windows XP Professional 中，端点用户需要通过在“选项 (Option)” > “视图 (View)”中取消选择“简单文件共享 (Simple files sharing)”以禁用简单文件共享。”
- 对于远程登录安装，必需禁用端点防火墙设置。
- 确保端点用户帐户具有管理员权限，并且可以下载 ActiveX 控件。

问题：HTTP、HTTPS 和 SSH 管理控制台可以有几个会话？

答：HTTP 和 HTTPS 分别能够具有 10 各并发会话， SSH 可具有 10 个以上的并发会话。

问题：设备是否阻止上传到 HTTP？

答：此版本的设备不支持此功能。

问题：为什么我会被从远程终端控制台上注销？

答：如果您更改当前窗口大小，设备会自动将您注销。

问题：为什么 MSN 被阻止了？

答：如果 HTTP 文件阻止设置符合 gateway.dll， MSN 也将被阻止。当指定要阻止的文件时，避免使用 *.dll。

问题：Network VirusWall Enforcer 是否支持 MSN 8.0 Beta 中共享文件夹的

文件阻止？

答：Network VirusWall Enforcer 不支持 MSN 8.0 Beta 中共享文件夹的文件阻止。

问题：为什么实时扫描(Real Time Scan)没有安装到具有 Windows 2003 和 Windows 2003 R2 操作系统的端点？

答：实时扫描(Real Time Scan)不支持 Windows 2003 和 Windows 2003 R2 操作系统

问题：我刚刚安装了 Network VirusWall Enforcer 2500，为什么无法访问 Web
控制台？

答：如果您使用的是 Windows 2003 Internet Explorer，该浏览器上的缺省设置需要您将 Network VirusWall Enforcer 2500 IP 地址添加到信任站点列表后才能访问

问题：从 Web 控制台禁用网络病毒扫描后，实时状态窗口上的当前连接项目是
否更新？

答：否。禁用网络病毒扫描后，不会清除会话计数。

问题：当我将 Network VirusWall Enforcer 2500 1.8 配置文件导入 Network VirusWall Enforcer 2500 2.0 时，例外主机将会怎样？

答：所有组都将转换为 Network VirusWall Enforcer 2500 中的网络区域(Network Zones) 以获得更大的灵活性。

问题：为什么显示内部错误消息，而非摘要窗口？

答：当 Network VirusWall Enforcer 同时阻止 1000 个以上的端点时，不会显示摘要(Summary) 窗口。

问题：Network VirusWall Enforcer2500 是否支持 Windows ™ Vista ™?

答：否。此版本的 Network VirusWall Enforcer 2500 不支持 Windows Vista。

问题：为什么端点无法访问重定向 URL？

答：如果以大写字母配置重定向 URL，端点则无法访问该 URL。URL 扫描功能是区分大小写的， Internet Explorer 自动将 URL 转换为小写，所以端点无法访问重定向 URL。

问题：为什么无法将 PEAgent 部署到 Windows Server 2003 R2 端点？

答：缺省的 Internet Explorer 安全设置阻止了部署。请更改端点的 Internet Explorer 上的安全设置，启用 Java Script、Signed ActiveX 下载/ 执行。

问题：策略列表中为什么有多个相同策略的副本？

答：如果选择一个策略并多次单击复制 (Copy)，则会将该策略的多个副本添加

到列表。或者相同的 IP 地址出现在多条策略中。

问题：什么可能妨碍 PEAgent 的成功部署？

答：以下各项可能会妨碍 PEAgent 的成功部署：

- 如果 Network VirusWall Enforcer 2500 和端点不属于同一网络段。
- 端点的流量通过设备后直接进入路由器。

问题：Network VirusWall Enforcer 2500 执行端点评估后，为什么端点浏览器显示“页面未找到 (Page not found)”？

答：如果网络中使用代理脚本，在端点评估期间，Network VirusWall Enforcer 2500 可能阻止将代理脚本下载到端点。评估后，关闭端点浏览器然后重新打开以访问因特网。

要防止此问题，将代理脚本添加到网络区域例外列表。

注意： 如果将代理服务器添加到全局端点例外列表中， Network VirusWall Enforcer 2500 将不会评估使用该代理服务器的端点。

问题：在带有互联网协议语音 (VoIP) 的网络中，Network VirusWall Enforcer 2500 是否忽略 VoIP 数据包。

答：是的，Network VirusWall Enforcer 2500 实时扫描通过的每个数据包。但是，由于通过 VoIP 数据包传输的数据太小， Network VirusWall Enforcer 2500 将忽略这些数据包。

问题：Network VirusWall Enforcer 2500 设备能否被连接或堆叠成一体以提高吞吐量？

答：Network VirusWall Enforcer 设备被设计为并行连接而非串行连接。所以，无法将它们连接在一起以提高吞吐量。

问题：Network VirusWall Enforcer 2500 能否视为网络中的中继器？

答：Network VirusWall Enforcer 2500 并不会放大信号或数据包。

问题：使用安装程序安装 PEAgent 后，PEAgent 图标显示灰色

答：请执行以下操作：

1、点击开始->运行，输入 cmd，进行命令行模式。

2、输入 cd c:\windows\peagent 进入 PEAgent 的安装目录

3、运行以下命令：

PEAgent.exe /stop

PEAgent.exe /init persist NVWE_IP:5088

PEAgent.exe /stop

PEAgent.exe /start

备注：NVWE_IP 为 NVWE 的 ip 地址

问题：Network VirusWall Enforcer (NVWE) 2500 2.0 不能隔离受感染数据包

的客户机

答：为了解决这个问题，从 Policy Enforcement > Policies 中检查策略执行服务的配置。选择策略设置，隔离受感染数据包的客户机。

NVWE 隔离的最大数量客户机为 4096。如果客户机数量超过该数量，则 NVWE 会根据先进先出的策略删除记录。

问题：部署强制策略(Polciy Enforcement)后，客户端访问网页时提示该页无法显示

答：

环境：

NVWE 与客户机在同一个网段中，并且能够互相访问(telnet NVWE_IP 5088 也是通的) 。该客户机肯定违反了强制策略，强制策略的处理措施为 Block 该客户机。但当该客户机通过 NVWE 访问其他网络时，并没有出现部署 PEAgent 的页面或者是该客户机被 block 的页面，而是显示该页无法显示的提示内容。

原因：

出现该问题的原因是该客户机使用的 DNS 服务器为其他网络中的 ip 地址。即当该客户机访问网页时，该客户机需要解析域名，但该客户机由于被 Block 了，所以无法访问 DNS 服务器，这样就导致了该页无法显示的提示内容。

解决方法：

方法一：使用内部 DNS 服务器，并确认该服务器可以被客户机访问到。

方法二：将客户机使用的 DNS 服务器 ip 地址添加到 NVWE 的全局列外列表中

添加方法：

Web 控制台->Policy Enforcement->Global Endpoint Exceptions

将 DNS 服务器添加到列表中。

问题：在 VLAN 环境下该如何设置 NVWE（如何添加 Bridge IP）

答：

网络环境：

Route---L2 Switch---NVWE----L2 Switch---Client

VLAN 信息定义在 Route 上，2 层交换机上将一些端口设为了对应的 VLAN。

NVWE 接在 2 台 2 层设备的 Trunck 口上。

NVWE 的 IP 为：192.168.100.3(VLAN1)，管理地址。

Client 地址：192.168.3.0/24(VLAN6) 网关为 192.168.3.254.

现象：

在此环境中，如果不设置 Bridge Ip 地址，即使 PEAgent 运行正常，NVWE 也无法成功 Block 该客户机。问题原因请参考 NVWE 的管理员手册说明。

解决方法：

对于 VLAN6 添加一个 Bridge Ip 地址，NVWE 将用该 IP 地址和该 VLAN 的客户机进行通讯。

1、Web 控制台->Administration->IP Address Settings

2、添加 Bridge IP 地址：

切换到 Bridge IP Address(es)

添加如下信息：

IP address: 192.168.3.190

Subnet mask: 255.255.255.0
Port: Bridge
VLAN ID: 6
注意：NVWE 需要使用 192.168.3.190 与客户机通信，故该 IP 不能被其他设备使用
3、添加 Static Route：
切换到 Static Route 页面：
添加如下信息：
Network ID: 192.168.3.0
Netmask: 255.255.255.0
Router: 192.168.3.254
Port: Bridge.VLAN6
4、确定客户端可以访问到 5088 端口
在客户端上运行：telnet 192.168.3.190 5088
如果 telnet 通，会有乱码字符输出。
5、如果 PEAgent 已经安装，在客户端上运行以下命令：
cd %windir%\PEAgent
PEAgent.exe /init persist 192.168.3.190:5088
PEAgent.exe /stop
PEAgent.exe /start
6、以上操作后，再次查看策略是否生效。

问题：对客户机设置强制策略后，客户端并没有出现安装 PEAgent 的提示页面
答：请确认以下几种情况：
1、确认该客户机的 IP 地址没有在例外列表中
Policy Enforcement->Global Endpoint Exceptions
2.确认该客户机并没有在对应 Network Zone 的列外列表中
Policy Enforcement->Network Zones,选择该客户机应该匹配策略的所在的 Network Zone 之后，编辑该 Network Zone，检查其 Exception
3、请确认没有勾选"Disable endpoint assessment for unidentifiable operating systems"选项，该设置选项在策略的第一步 Specify Endpoint Settings 中进行设置。
3、确认该客户机匹配的策略的杀毒软件没有启用"Assess Trend Micro products only by using networking protocols"，该选项在设置策略的第三步 Specify Enforcement Policy 中进行选择。

问题：客户端评估未通过后，无法跳转到指定的页面
答：
问题描述: 当客户端在被评估后，其结果为违反策略。NVWE 定义了其网页跳转到某个页面，但该客户端一直停留在评估后的页面上。
解决方案: 解决方法：
1、进入 Policy Enforcement->URL List。
2、添加一个新的列表，并且添加可以并客户端访问的 URL 地址。
如果一个网站都需要被访问或者是其中部分路径文件被访问，请使用通配符*来

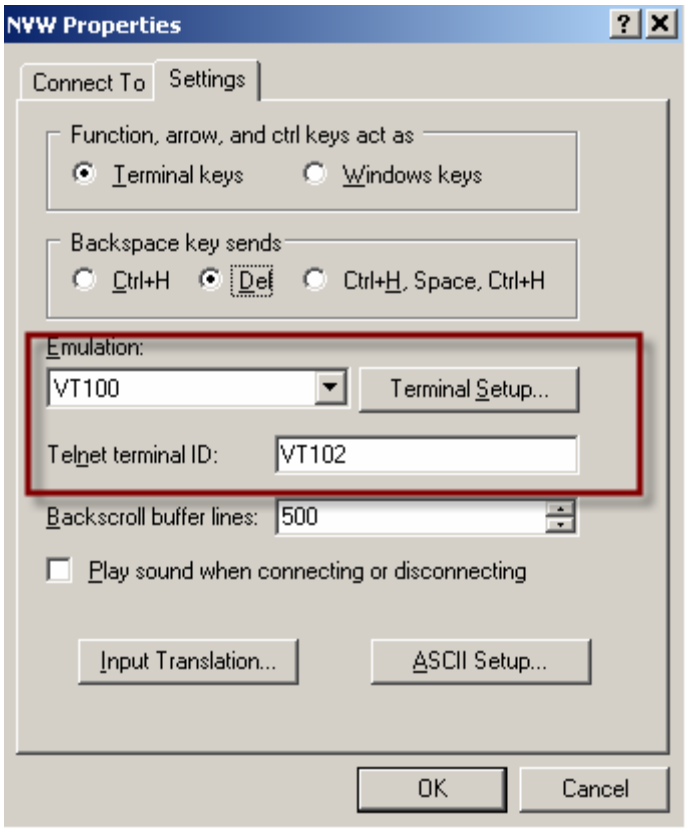
表示。
如 http://*abc.com/*
3、保存新建的 URL 列表。
4、进入设定好的策略，并修改该策略。
5、在修改策略的第 6 步 Policy URL Exceptions 中，将新建的 URL 列表添加到 Selected URL Lists 中。
6、保存该策略。

问题：当 NVW2500 2.0 的 BIOS 的界面中，当选择菜单时，出现 discard changes and exit 的信息

答：解决方法：
1、设置超级终端的模式为：File->Setting 页面中，将 emulation 设置为 AUTO
2、保存后，再按 Ctrl+R 组合键进行刷新。

问题：NVWe2500 2.0 通过 console 登陆后显示不正常

答：请将 Emulation 设置为 VT100 ，并将 Telnet terminal ID：设置为 VT102



并检查终端设置是否正确

- Bits per second: 115200
- Data Bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

问题：Network Viruswall Enforce 2500 无法检测到 OSCE 客户

答：

问题描述:　部署 NVWE 2.0 版本后，通过"Summary"信息，发现很多客户机都是 No AV Product.但查看客户机，发现客户机确实安装了 OSCE 7.3 英文版本。另外，客户设置 NVW 检测杀毒软件时，使用的检测方法是"Assess Trend Micro products only by using networking protocols". 使用 Assess Trend Micro products only by using networking protocols 方法检测时，NVW 会去检测 OSCE 客户端的通讯端口来确定客户机是否安装了 OSCE。

故出现这种情况的原因有 2 种：

1、在 NVW 上设置的 OSCE 端口不正确。

2、客户端防火墙导致 NVW 无法访问到该客户机的通讯端口。

解决方案：

1、检测 OSCE 通讯端口设置是否正确。

NVW web 控制台->Policy Enforcement->OfficeScan Settings

请确认其中填写的端口为 OSCE 客户端的通讯端口。该栏最多可以填写 10 个端口。

客户端通讯端口确认方法：

HKEY_LOCAL_MACHINE\SOFTWARE\TrendMicro\PC-cillinNTCorp\CurrentVersion\

LocalServerPort= 后的值就是客户端的通讯端口。

2、如果客户端有安装防火墙（XP 自带防火墙），或者 NVW 与客户端之间有防火墙，请确认该端口在防火墙上有设置允许访问。

问题：Network Viruswall Enforce 2500 与 PEAgent 通讯机制解释。

答：当客户机通过 NVWE 访问访问资源时，NVWE 首先会尝试访问客户端的 5091 端口，如果可以访问到 5091 端口（表示 PEAgent 在运行状态），则 NVWE 将与 PEAgent 进行通讯，并通知 PEAgent 执行对应操作，PEAgent 执行完成后，会将对应信息发送个 NVWE。如果 NVWE 无法访问到客户端的 5091 端口，则 NVWE 会认为该客户机没有安装 PEAgent，NVWE 会尝试通过 ActiveX 或者 remote login 方式去部署，如果成功操作，并且发现该客户机有安装 PEAgent，则部署进程会尝试启动 PEAgent，如果没有发现 PEAgent，则 NVWE 会进行 PEAgent 的安装操作并启动 PEAgent，PEAgent 成功启动后，其会执行对应操作，并将相关信息传输给 NVWE。

问题：Persist Agent 和 Agentless 的区别

答：Persist Agent 和 Agentless 表示 PEAgent 的运行方式。Persist Agent 表示 Agent 安装后，将一直驻留系统，并主动汇报信息给 NVWE，您同时可以在系统托盘中看到 PEAgent 的图标。Agentless 表示 PEAgent 安装后，只运行一次，收集完成信息并传输信息给 NVWE 后，PEAgent 将停止运行。但 PEAgent 服务已经在系统服务中生成。