趋势科技

Deep Security 深度包过滤配置指南

Andrea_Xi
2013-08

目录

一、 定义和分配 DPI 规则

1. 确认受保护目标计算机类型

服务器

工作站

1.1 服务器信息收集

- 操作系统版本
- 主要应用
- 对外开放的端口号

1.2 执行“推荐扫描”获取系统漏洞信息

步骤：

a) 登录到 Deep Security Manager 8.0 管理控制台

b) 在控制台双击打开需要“深度数据包”检查的计算机配置界面 c

c) 点击“扫描建议”按钮，等待 Deep Security Agent 自动生成对受保护计算机生成推荐规则列表

二、 配置和部署 DPI 规则

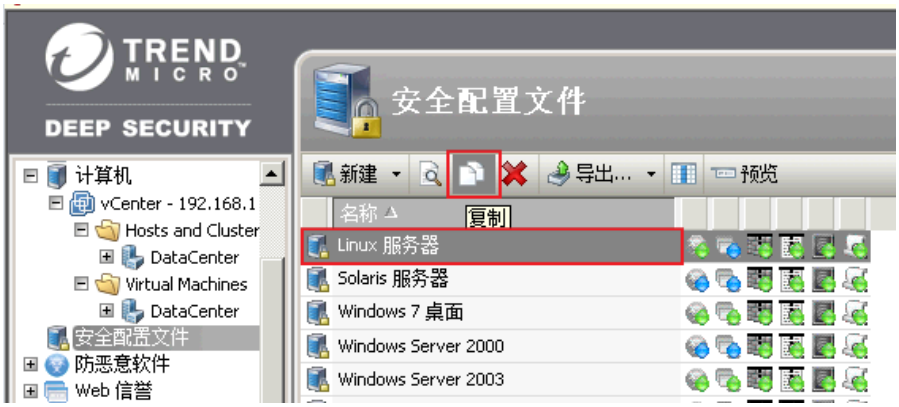
1. 通过安全概要文件部署 DPI 规则

对于保护的受保护的虚拟机或物理机不建议直接分配对应 DPI 规则，建议通过安全配置文件来部署 DPI 策略。由于默认安全配置文件已经包含有默认规则，实际操作时建议根据**扫描建议**结果去除不推荐的规则。

操作步骤：

a. 点击进入**安全配置文件**页面，根据操作系统类型选中需要分配的安全配置规则。例如，受保护 GUEST OS 为 linux 则选中“Linux 服务器”安全概要文件

b. 选中规则复制准备分配的**安全配置文件**，如图所示：



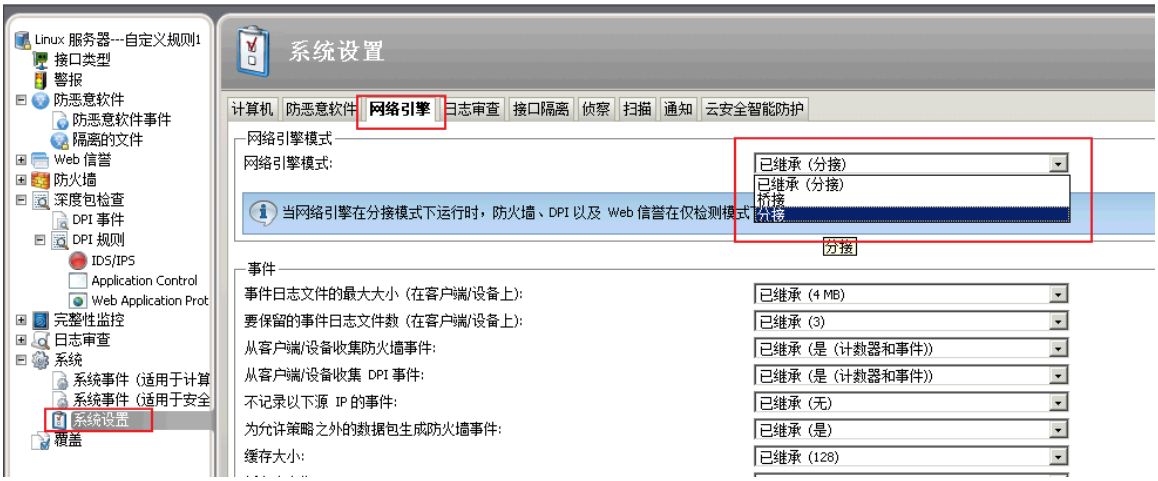
系统会自动生成复制的规则并自动命名为“Linux 服务器（2）”

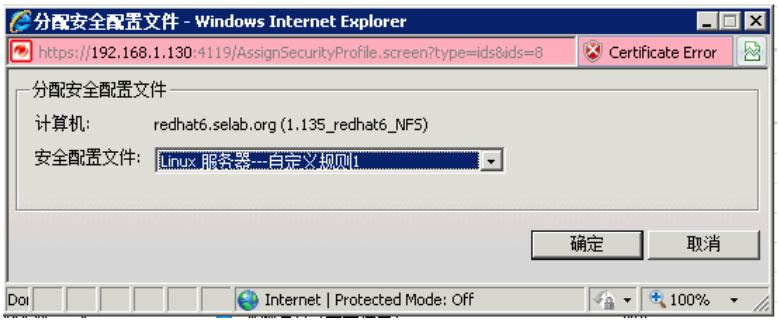
c. 双击进入复制规则的编辑页面，对规则进行自定义编辑

1） 修改规则名称，如 “linux 服务器---自定义规则 1”，点击“保存”使规则名称更改生效

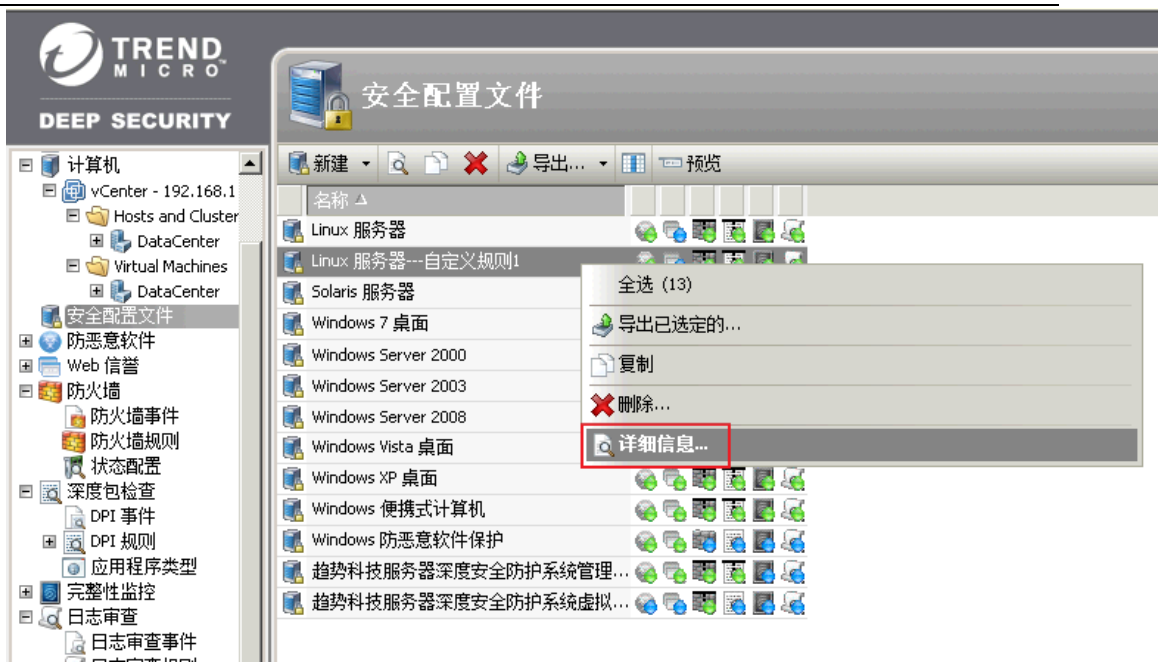
2) 点击进入 系统设置 ---> 网络引擎 ，修改网络引擎模式为 “分接”，点击“保存”使配置生效

备注：当网络引擎工作在分接模式时 firewall 规则和 DPI 规则都不会对实际数据包造成影响，因此可以避免由于错误规则导致网络中断的风险





3) 重新进入自定义规则配置页面 --->深度包检查 ---> DPI 规则


TREND MICRO
DEEP SECURITY
安全配置文件
新建
导出...
预览
名称
Linux 服务器
Linux 服务器---自定义规则1
Solaris 服务器
Windows 7 桌面
Windows Server 2000
Windows Server 2003
Windows Server 2008
Windows Vista 桌面
Windows XP 桌面
Windows 便携式计算机
Windows 防恶意软件保护
趋势科技服务器深度安全防护系统管理...
趋势科技服务器深度安全防护系统虚拟...
全选 (13)
导出已选定的...
复制
删除...
详细信息...
计算机
vCenter - 192.168.1
Hosts and Cluster
DataCenter
Virtual Machines
DataCenter
安全配置文件
防恶意软件
Web 信誉
防火墙
防火墙事件
防火墙规则
状态配置
深度包检查
DPI 事件
DPI 规则
应用程序类型
完整性监控
日志审查
日志审查事件

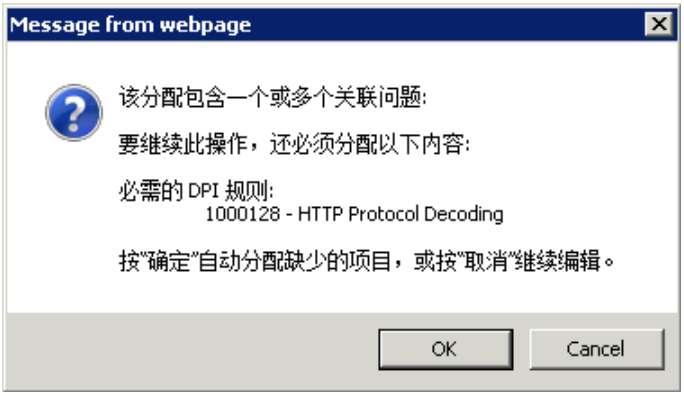

Linux 服务器---自定义规则1
接口类型
警报
防恶意软件
防恶意软件事件
隔离的文件
Web 信誉
防火墙
深度包检查
DPI 事件
DPI 规则
IDS/IPS
Application Control
Web Application Prot
完整性监控
日志审查
日志审查事件
日志审查规则
系统
系统事件 (适用于计算
系统事件 (适用于安全
系统设置
覆盖
DPI 规则 (按模式) (显示建议取消分配的项目)
新建
导出...
名称
应用程序类型
仅检测 (1)
1004951 - DNS Denial Of Service Vuln... DNS Client
阻止 (88)
1000128 - HTTP Protocol Decoding Web Server Common
1000630 - Apache htgrep Header Info... Web Server Apache
1001028 - Apache mod_cache Module... Web Server Apache
1001312 - MySQL yaSSL Pre-authenti... Database MySQL
1001332 - Web Server Apache 'mod_... Web Server Apache
1002376 - Multiple Vendor CUPS Admi... Unix CUPS
1002381 - Multiple Vendor CUPS GIF D... Unix CUPS
1002687 - Apache 'mod_proxy_ftp' Wi... Web Server Apache
1003536 - Apache mod_dav svn Rem... Web Server Apache
1003736 - Dnsmasq TFTP Service Rem... TFTP Server
1004273 - CUPS Web Interface Infor... Unix CUPS
1004369 - Apache CXF XML DTD Proc... Web Server Apache

4) 在 DPI 规则过滤条件中选择“显示建议取消分配的项目”

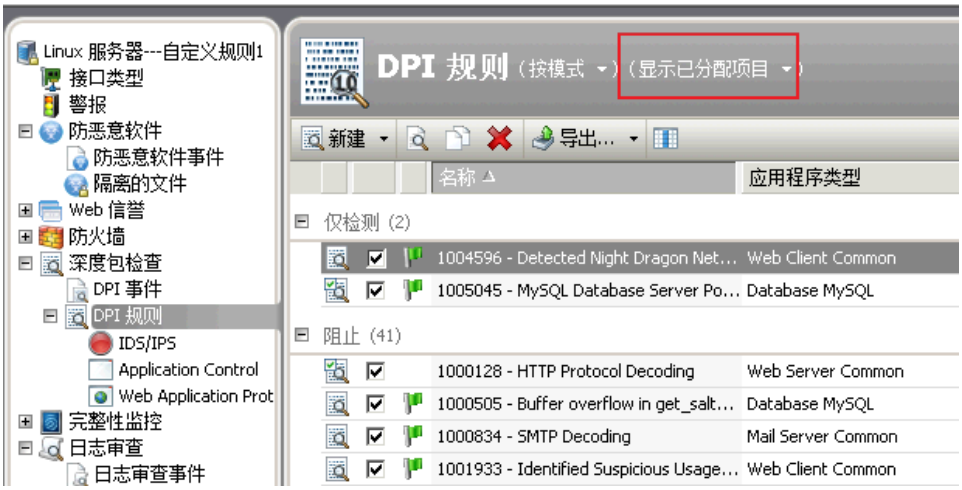
5) 全选建议取消分配的规则

6) 对选中的规则**取消分配规则，**点击保存使配置生效

如提示自动分配缺少的项目对话框，则直接按 OK 继续



7) 更改安全配置文件中的 DPI 规则筛选条件为 “显示已分配项目”



查看当前分配的规则前是否存在有感叹号⚠标记

DPI 规则图标：

常规 DPI 规则
根据时间表运行的 DPI 规则
具有配置选项的 DPI 规则
需要配置的 DPI 规则

8) 对提示“需要配置的 DPI 规则”进行配置
备注：*如对具体规则配置有任何疑问请联系趋势科技技术支持部门*

9) 对于未提示“需要配置的 DPI 规则”但显示“具有配置选项的 DPI 规则”  ，一般可以保持默认设定，或**联系趋势科技技术支持部门获取该 DPI 规则的配置建议。**

完成以上配置以后请检查受保护的计算机是否有关于深度包保护的告警提示出现，如显示绿色状态则表示当前 DPI 规则不存在规则依赖性冲突，或端口依赖性冲突等问题。如遇到以上问题，请参考 **“DPI 规则依赖性问题处理章节”**对应内容。

三、 DPI 规则分配最佳实践

Deep Security 深度包防护功能提供了基于主机的入侵阻止功能，但是趋势科技依然建议对于已知高危系统漏洞优先考虑**安装**对应的操作系统或应用程序补丁进行防护。Deep Security 深度包过滤功能并非用于完全替代系统或应用程序补丁程序修复软件存在的 bug，而是提供了一种快捷部署和防御高危漏洞的手段。精简保护计算机的 DPI 规则数量有助于提升受保护计算机的网络性能，降低受保护计算机的性能负载和资源消耗。

深度包过滤适合应用以下场合：

- 提供更为方便快捷的基于网络的安全漏洞的应对手段
- 对于在线生产服务器可以在不中断业务的情况下，部署漏洞防御规则来保护计算机免受攻击威胁
- 对于暂时无法大规模部署系统补丁的客户机提供临时的虚拟机补丁防护

最佳实践

- 对于生产服务器:
  一旦发现服务器操作系统或应用程序存在严重安全漏洞，可以在服务器不停机的情况下提供虚拟补丁防护。服务器在计划停机时间一旦正式部署对应操作系统或应用服务补丁修复程序以后建议取消对应 DPI 规则，以确保服务器可以获得最佳性能。
- 对于客户机：
  客户机一旦发现新的安全漏洞，通常部署对应系统补丁会产生较大工作量并且需要较长时间才能完成全部漏洞补丁部署，此时可以使用 Deep Security 深度包过滤提供漏洞保护。

趋势科技推荐定期对受保护计算机进行“建议扫描”以提供动态的最佳安全保护状态。

性能优化

趋势科技深度包过滤的“建议扫描”功能根据操作系统当前的系统版本和应用程序安装情况提供最大化的安全防护建议，实际实施中可以根据受保护计算机不同应用类型进行对应的规则优化，减少一些非必要的规则分配以提升受保护计算机的网络吞吐性能。

按应用程序类型优化

- 对于 Windows 服务器操作系统建议选择以下应用程序类型：

DPI 规则应用程序类型	**备注**
Windows Services RPC server	推荐
DNS Client	推荐
Remote Desktop Protocol Server	（可选）如启用远程桌面服务请开启对应分类的规则
Web Server IIS	（可选）如服务器启用 IIS 服务器则启用此规则
Web Server IIS HTTPS	（可选）如服务器启用 IIS 服务器则启用此规则
Windows Services RPC Client	推荐
Windows Services RPC Server	推荐
Windows Services RPC Server DCERPC	推荐
Web Server Common	（可选）对于 web server 服务器推荐启用此功能

请根据服务器实际用途启用对应应用程序的**深度数据包过滤防护规则**

对于非 windows server 如 linux 服务器通常工具 linux 服务器上的启用的服务，可以直接参考**扫描建议**的结果。

四、 DPI 策略风险规避

DPI 规则可能带来的风险：

- 性能过载
- 误报
- 应用程序兼容性
- 性能下降
- 其他问题

性能过载：

当 Deep Security 深度数据包过滤功能通过 DSVA 保护对 VMWARE vSphere 环境的虚拟机进行无代理安全防护时需要注意避免出现，ESXi heap memory 不足问题。需要通过命令来调整 ESXi 的 heap memory 参数，详情请参考以下知识库链接：
http://esupport.trendmicro.com/solution/zh-cn/1094274.aspx

误报

Deep Security 深度包过滤规则分为：漏洞，入侵，智能。三种类型的规则。三者关系分别为：

一个 DPI 漏洞规则可对应多个利用此漏洞进行入侵攻击的规则
一个 DPI 智能规则可以为一个或多个漏洞提供虚拟补丁保护
一个 DPI 入侵防护规则可以精确匹配并组织一种入侵方式

因此从效率上来讲，智能规则 > 漏洞规则 > 入侵规则
从精确性来讲，入侵规则 > 漏洞规则 > 智能规则 由于智能规则可以提供更宽泛的防护因此，智能策略可能需要通过一些自定义配置来防止误报。

对于重要的生产服务器，要避免出现误报问题，请尽量避免使用智能类型的 DPI 规则。

应用程序兼容性

DPI 规则由于对数据包进行深度过滤，因此对于某些应用 DPI 的规则可能会影响到部分网络应用的正常工作。要避免可能出现的兼容性问题带来的影响，建议在正式部署规则前执行以下测试来规避可能存在的潜在风险。

1. 将网络扫描引擎设置为“分接”模式
2. 在启用 DPI 规则后，查看 DPI 日志，查看是否有触发 DPI 规则的记录，并分析此问题是否有可能影响到实际网络业务。
3. 在经过“分接”模式测试后，请对重要业务在非工作时段切换到桥接模式，确认业务可以在 DPI 规则保护下正常工作。

性能下降

DPI 规则的数量对受保护客户机的网络性能有相应影响。 DPI 规则越多，受保护端损失的网络性能可能越大。对于一些有明确 SLA 要求的网络应用。可以在 DPI 规则提供桥接保护以后进行性能测试确保当前分配的 DPI 规则可以在有效保护目标主机的前提下，维持原有客户机可

接受的性能。

减少 DPI 规则数量可以提升受保护客户机的网络性能并且降低 DSVA 性能负载。要减少 DPI 规则负担。

其他问题：

对于其他不可预知的问题，要避免未知问题影响重要网络业务，建议在正式部署 DPI 规则以前先对相应规则进行模拟检测，确认对应规则不会对正常网络应用产生严重影响。

五、 DPI 规则应用程序端口冲突问题

每条 DPI 规则都有对应的应用程序类型，而每种应用程序类型又包含有此应用程序类型所包含的应用程序端口号等信息。当某 DPI 规则分配后，其规则所对应的应用程序类型没有包含此规则所保护的应用程序端口。 如遇到类似问题，请参考以下知识库：
http://esupport.trendmicro.com/solution/zh-cn/1093291.aspx

六、 DPI 规则故障诊断

当部署 DPI 规则后遇到疑难问题，请及时联系趋势科技技术支持部门获取帮助。 通常部署 DPI 规则后遇到产品网络不通等现象请先对问题进行隔离：

a. 问题初次出现的时间
b. 提供足够的时间请对方调研资料
c. 进一步对故障进行隔离，通过确认以下几个方面：
   - 确认关闭 DPI 规则后问题是否立即消失
   - 确认受影响的应用程序端口号
   - 在 DPI 规则中尽量关闭相关的应用程序规则，确认问题是否解决
   - 确认在分接模式下，对应问题是否有消失或改善
   - 收集 Deep Security 完整系统日志，以便可以提供给后端工程师参考。