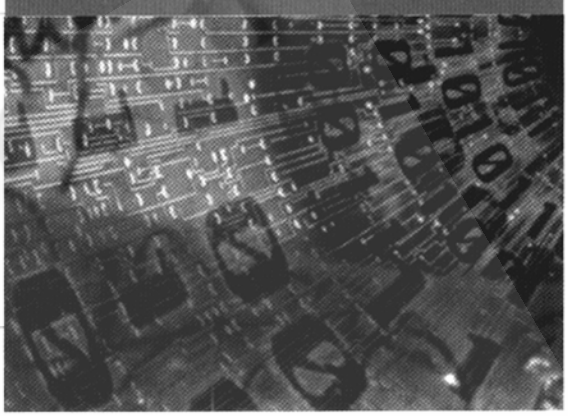
利用ISA和SNMP协议构建的防黑客攻击的自动报警系统

单迎春 (上海市教科院职业技术教育研究所)
(中科院软件所上海时佑信息系统有限公司)



摘要：随着Internet的迅速普及，计算机随时随地会遭到黑客的攻击，网络安全越来越多地受到了人们的重视。ISA是Microsoft推出的代理服务器和防火墙产品，它在网络安全上的功能独树一帜。本文提出了一个自动报警系统的体系结构，它基于SNMP协议，当ISA检测到网络攻击时能产生相应的Trap并最终发出Alert。

关键词：ISA SNMP XML Alert

1 引言

Microsoft Internet Security and Acceleration(ISA) Server是一个可扩展的企业防火墙和Web缓存服务器，可与Windows 2000集成，以便为联网实现基于策略的安全、加速和管理。它可提供两个紧密集成的模式：多层防火墙和高性能Web缓存服务器。防火墙不但提供在数据包、电路和应用程序电台的筛选(packet-,circuit-, and application-level traffic filtering)，还提供状态检查(stateful packet inspection)(用以检查跨越防火墙的数据)、控制访问策略以及通信的路由。缓存可通过存储时常请求的Web内容，改善网络性能和用户的经验。ISA Server构建在Windows 2000安全、上当、虚拟专用网络(VPN)和带宽控制基础之上。不论是作为一组单独的防火墙和缓存服务器部署，还是以集成的模式部署，ISA Server均可增强网络安全性，实施一致的Internet使用策略，加速Internet访问，并最大限度地提高各种规模公司的员工办公效率。ISA与Windows 2000's Active Directory (AD)或者NT的SAM的无缝结合是其他防火墙软件望尘莫及的，因为它可以做到用户和组一级的安全设置，而其他防火墙软件只能根据IP地址或者使用另一个单独的用户认证数据库来解决问题。

ISA自身提供了一套Alert机制，但使用的直观性、灵活性和可扩展性等都有相当的欠缺。微软意识到这一点，为了便于ISV进一步开发的需要，提供了相应的接口程序。本文构建的系统就是在此接口基础上设计并实现了支持SNMP协议、建立在WEB数据库上的自动报警系统。系统采用B/S结构，为客户端设置了良好的用户界面。

2 自动报警系统的设计和实现

本系统的主要设计原则是提供友好的界面和灵活的机制，并遵循各种已知的协议标准。系统的环境如图1所示：

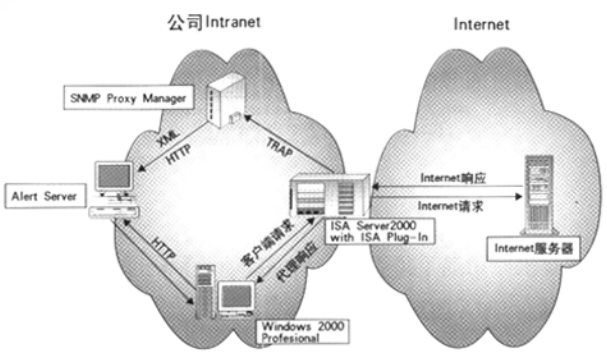


图 1 自动报警系统拓扑示意图

安装ISA Server的前提条件是安装好Win2000和

Active Diretory，然后安装SPI for Win2000，如果机器上曾经安装过Proxy Server 2.0，需要将各个服务器从其基于Proxy Server 2.0的阵列中移走；从每台服务器上卸载Proxy Server 2.0 。(请注意，应在没有对升级的可用支持时)；从每台服务器中卸载Internet Information Server(IIS) 5.0 ；将包含URL缓存的逻辑驱动器格式化。卸载IIS的原因是，Internet Information Services和ISA Server争用端口80，这是Internet Information Services的默认值，同时也是ISA Server使用的HTTP标准。因为ISA Server功能不以任何方式依赖IIS，所以没有理由在将要部署ISA Server的服务器上保留该软件。下面分析系统的整个机制：

2.1 Alert ISA Plug-In

它的功能主要在于提供ISA配置和转发Trap。

ISA可以从IP数据包和应用程序层检测到来自黑客的攻击。ISA Server支持入站和出站的IP数据包筛选。ISA Server的数据包筛选还可以阻止碎片，并可检测针对防火墙的数据包层的攻击。ISA Server防火墙提供的最完善通信检查层是应用程序层安全。“智能”应用程序筛选器可以分析某个应用程序的数据流，并在数据通过防火墙时提供应用程序特定的处理，包括检查、屏蔽或阻止、改向，甚至修改数据。这种机制可防止某些已知的漏洞，如不安全的SMTP命令，或针对内部域名系统(DNS)服务器的攻击。用于内容屏蔽的第三方工具，包括病毒检测、词法分析和站点分类，还使用应用程序筛选器和Web筛选器进一步扩展防火墙。

当ISA服务器检测到端口扫描、Windows out-of-band (如WinNuke)、Ping of Death、Land attacks和UDP bombs之类的常见网络攻击时，它将触发Alert ISA Plug-In. Alert ISA Plug-In 是用Visual Basic开发的一个ISA接口程序，它提供了相应的界面为用户配置当发生某些事件时需要转换为SNMP Trap，并向指定的机器(根据机器名或IP地址)发送Trap，可以选用SNMP v1和SNMP v2两种方式。下面以SNMP v1为例，Generic Code为6(Enterprise Defined Trap)，配置如图2所示。

用户按OK键后执行下面的Visual Basic代码，将发生事件后所要执行命令行写入ISA配置文件：

```
Set Fpc=CreateObject("FPC.Root")
Set Alerts=Fpc.Arrays(1).Alerts
'Construct command line to be executed after the related events happend
CmdLine=App.Path+"/SendTrap.exe"+Chr(34)
+txtCommunity+"&."+txtEnterprise+"&"+GenericValue+"&"
+txtSpecific+"&"+txtPortNumber+"&"+txtDestination+"&"+tx
tTimeStamp+"&"+AlertNumber+"&"+AlertType+"&"+AlertSeverity
+"&"+"ISA:"+AlertDescription+Chr(34)
Alert.Actions.Unset (fpcAlertActionCommand)
Alert.Actions.Refresh
Alert.Actions.SetCommand "SNMP Alert",CmdLine
Alert.Actions.Save
```

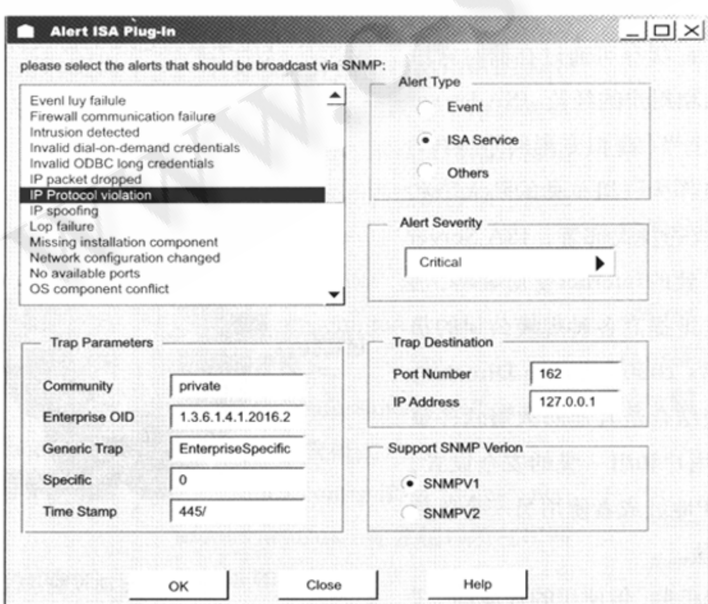


图 2　配置ISA Plug-In

命令行程序 SendTrap.exe 负责将发生的事件转化为 Trap：(程序代码略)

2.2 SNMP Proxy Manager

SNMP Proxy Manager 的主要任务是管理各种支持 SNMP 协议的设备(SNMP Enabled Devices)。包括两方面内容(见图 3)：

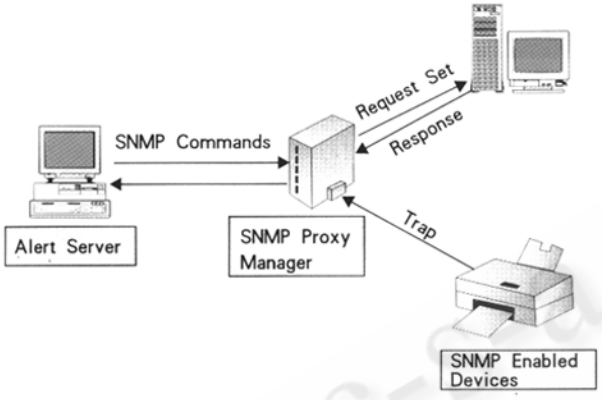


图 3 SNMP Proxy Manager 功能示意图

SNMP Proxy Manager 接到相应的 Trap 后，将它转化为如下的 XML 文件，发送给 Alert Server。

```
<SNMP version="1" community="private" command="trap"
requestedID="4" error_status="0"
error_index="0"><trap enterprise="1.3.6.1.4.1.2016.2"
agent_address="172.16.1.5" type="6"
specific_code="0" timestamps="0" active="TRUE">
<varbindinglist_trap OID_trap="1.3.6.1.2.1.1.3.0"
value_trap="4457"/>
<varbindinglist_trap OID_trap="1.3.6.1.6.3.1.1.4.1.0"
value_trap="1.3.6.1.4.1.2016.2.0.0"/>
<varbindinglist_trap OID_trap="1.3.6.1.4.1.2106.2.1.1"
value_trap="7B-46-46-46-46-38-45-39-39-2D-39-34"/>
<varbindinglist_trap OID_trap="1.3.6.1.4.1.2106.2.1.2"
value_trap="2"/>
<varbindinglist_trap OID_trap="1.3.6.1.4.1.2106.2.1.3"
value_trap="1"/>
<varbindinglist_trap OID_trap="1.3.6.1.4.1.2106.1.4"
value_trap="ISA:IP protocol violation."/>
<varbindinglist_trap OID_trap="1.3.6.1.4.1.2106.2.1.5"
value_trap="5/10/2001 5:51:50 PM"/>
<varbindinglist_trap OID_trap="1.3.6.1.4.1.2106.2.1.6"
value_trap="172.16.1.173"/>
<varbindinglist_trap OID_trap="1.3.6.1.6.3.1.1.4.3.0"
value_trap="1.3.6.1.4.1.2016.2"/>
</trap></SNMP>
```

2.3 Alert Server

Alert Server 是一个 WEB 应用程序，基于 IIS+SQL Server7.0 用 ASP，Java Applet,Java Script 开发，目前正在移植到 Linux 的 Apache 上。Alert Server 的主要功能包括：

(1) 提供用户针对不同 Trap 在任意时段内灵活配置 Alert 的方法；

(2) 自动搜索并树状显示网络内所有的机器及属性；

(3) 网络监控。

Alert Server 解析相应的 XML 文件，并把它记录到 Trap 数据库中，利用 Java applet 显示的 Trap 列表如下：下面是用浏览器可以观测到新生成的 Trap,如图 4 所示。

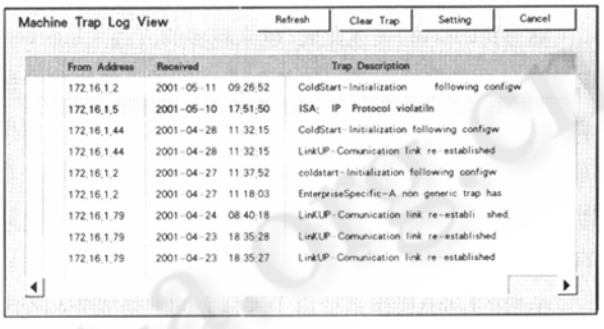


图 4 Java Applet 显示的 Trap 列表

如果事先定义了针对这种 Trap 的 Alert，如发送电子邮件或寻呼，发送广播(Broadcast)信息给管理员或某些特定的机器，那么响应的 Alert 就会被启动。

3 小结

本文提出的技术给ISA Server提供了能识别此类攻击的集成入侵检测机制，比 ISA 本身提供的 Alert 机制更加灵活，我们还编制了 Schedule 模块，这样可以配置在什么时间段(如星期一、三、五的上班时间)由谁处理相应的 Alert。我们已经在某一网管软件中做出了成功的试验，实践证明这种结构是有效和实用的。■