趋势科技

InterScan Web Security Appliance EE 5.1

产品安装标准程序(SOP)

趋势科技技术支持部
陈卓君
2011 年 1 月

目 录

1. 认识 IWSA EE 5.1

企业的Web 网络流量日渐增加，所以同时兼顾企业的HTTP 和FTP 病毒防护，并且维持网络畅通，是决定企业安全解决方案成功与否的关键。尽管以往的病毒大部分通过邮件进入企业，但新形态的病毒威胁越来越倾向于采用Web 作为入侵的渠道。然而，不合理地扫描HTTP 和FTP 传输会造成网络配置的沉重负担，并影响客户端的使用效能，因此使得企业往往在HTTP和FTP 网关部署防毒措施上有所迟疑，造成整体安全防护的漏洞。

趋势科技防 InterScan Web Security Appliance EE 5.1（简称 IWSA EE 5.1）提供了基于网关的，对 HTTP 及 FTP 数据传输进行安全扫描的完善功能，并且具备可应用于各种规模企业的高性能、可自动更新升级特性。考虑到 Web 用户的实际应用要求，IWSA 重点解决了网关病毒扫描所造成的性能瓶颈问题，最大可达到 1.5Gbps 的处理速度，从而在保证安全扫描的前提下，大大提高了用户访问 Web 的速度。

为企业网络提供灵活的安全防御策略。IWSA基于支持多种配置与运行模式，支持多种未来新的应用系统的设计架构，再与趋势科技业界领先的企业安全防护策略(EPS)相结合，扩展了趋势科技关于Web安全的病毒爆发生命周期管理理念，从而获取最大的投资回报率。IWSA内嵌为PhishTrap的反钓鱼技术、Applets & ActiveX扫描技术、反间谍软件技术及URL过滤技术等。IWSA又同时和趋势科技的云安全做整合，可以使用Web信誉技术来对用户访问的URL网页进行评分，从而屏蔽那些含有间谍软件和病毒恶意代码的网页访问。

2. IWSA EE 5.1 系列硬件规格及参数

IWSA EE 5.1安装在实体Dell服务器上。本章节将介绍IWSA EE 5.1安装在实体机-Dell服务器上的硬件规格和参数。IWSA的型号表如下：

1-1-1表、IWSA EE 5.1的型号对照

IWSA的型号	对应的实体机型号
IWSA 1500	DELL R410
IWSA 3000	DELL R610
IWSA 5000	DELL 2950
IWSA 6000	DELL R710
IWSA 10000	DELL R710

IWSA系列的硬件参数表如下：

1-1-2表、IWSA系列产品的硬件参数表

系列	IWSA 1500	IWSA 3000	IWSA 6000	IWSA 10000	备注
接口类型	千兆	千兆	千兆	万兆	
平台	Dell OEM	Dell OEM	Dell OEM	Dell OEM	从 Dell OEM 出厂设备为 IWSA 产品完整包装，软件和硬件部分为特别定制，并按照定制化流程生产。
尺寸	1u	1u	2u	2u	
CPU	1x5500 系列	2x5500 系列	2x5500 系列	2x5500 系列	
内存	3G	6G	12G	24G	
HD	160Gx2	160Gx2	160Gx2	250Gx2	
软件版本	VA3.1	VA3.1	VA3.1	VA3.1	除 2500 外，其他型号软件版本相同
类型	EE	EE	EE	EE	
型号	TX	TX/FX	TX/FX	TX/FX	
多链路型号	是	是	是	是	1）支持 Multi-link, Port group, Link-loss forward 几种场景。 2）多链路型号需要厂商或代理商定制安装，包括硬件安装和补丁安装两个步骤。 3）定购多链路型号需要提前（申请特价时）说明。

最大可扩充故障直通端口数	4	8	16	16	不包含非故障直通端口数。

因此IWSA EE 5.1可以安装在IWSA 1500/3000/5000/6000/10000等产品上。由于Dell机型的不同，所以同一软件安装在IWSA上面所体现的性能也不同。

3. IWSA EE 5.1 的新功能

IWSA EE 5.1是基于IWSA/IWSS等系列产品改进而来。因此IWSA EE 5.1在继承了之前版本的功能之上，同时在性能、扫描等各方面做了较大的改进以更适应用户的网络环境和需求。

3.1 IWSA EE 5.1的性能

IWSA EE 5.1性能上更稳定，可以更好地处理网络流。即使网络流量出现了异常，IWSA EE 也可以确保您的Web访问不受影响。遇到相同的并发连接数和吞吐量时，IWSA EE 5.1比之前的版本可以占用较少的内存。

3.2 部署向导

在安装完毕之后，第一次登录Web控制台时，IWSA EE 的部署向导会自动弹出并协助用户进行初始设置。

3.3 故障转移和LAN Bypass

故障转移/LAN Bypass功能卡可以使用CLI命令模式来配置而不用登录到Shell模式下面去运行script脚本程序。

3.4 通知消息的改进

通知内容的格式废除了之前的文本模式，而是丰富多样化，从而帮助管理员或者最终用户来更方便理解通知的内容。

3.5 URL过滤警告模式

URL过滤现在提供了一种警告模式。在用户访问了一个不允许的站点时，消息会提前通知用户。

3.6 LDAP集成策略的改进

LDAP透明认证的改进集成了域控查询和Windows客户端查询。它可以协助我们减少终端用户的认证弹出对话框。

IWSA EE 5.1也支持2008AD域。

3.7 HTTPS的扫描

在透明模式下支持HTTPS的扫描。新的驱动加入了对SSL硬件加速卡的支持从而完成对HTTPS的计算。

3.8 X-Forwarded For Header

IWSA EE 现在可以解析“X-Forwarded-For”头来获得原始客户端的IP地址，并加入了针对上游代理的“X-Forwarded-For”头

3.9 病毒扫描技术的改进

增加了来自最新的vSAPI9.0的扫描技术，包含了被阻止文件类型的增强

4. IWSA EE 5.1 的部署方式

本章节将向您介绍如何部署IWSA EE 5.1。

4.1 IWSA EE 的网络架构

在部署IWSA EE 之前，首先要对您的企业网络架构有个全面的了解，同时需要考虑如何正确合适地把IWSA EE 放置在网络中。

通常现在大部分企业的基本架构如下：

一个DMZ区域和两个防火墙；

一个防火墙，不含DMZ区域。

小知识：什么是DMZ区域？

DMZ区域——DMZ区域是位于内部防火墙和外部防火墙之间。在DMZ区域内的主机可以接收来自对外服务器的连接。配置外部防火墙以允许来自外部计算机的数据包达到DMZ内的服务器。

因此需要您根据不同的网络架构来放置IWSA EE 和确定IWSA EE 的部署模式。

小知识：什么是公司局域网？

公司局域网——这些网络是位于内部防火墙的后面。配置内部分防火墙可以让数据包到达公司局域网内的机器，但是必须注意：这些数据流必须来源于DMZ区域。

网络架构一、一个DMZ区域和两个防火墙

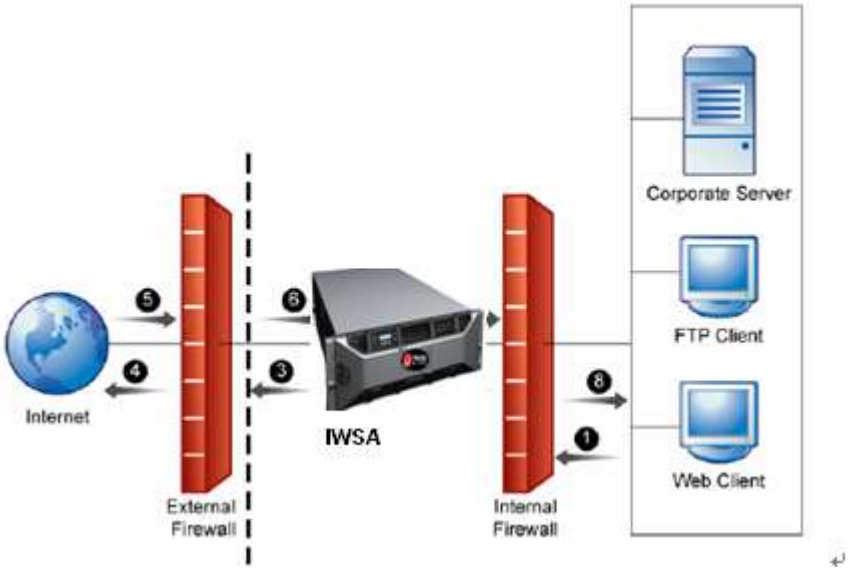


图4-1-1、双防火墙+DMZ

如图4-1-1，此架构是将DMZ区域放置在内部防火墙和外部防火墙之间，同时将IWSA EE 安装在DMZ区域内。该拓扑结构需要将所有来自外部服务器的数据先经过DMZ里面的IWSA EE ，然后达到局域网内的客户端。如果客户端要访问外网，必须先经过DMZ里面的IWSA EE ，才能通过外部防火墙出去访问Internet。

网络架构二、单防火墙（不含DMZ区域）

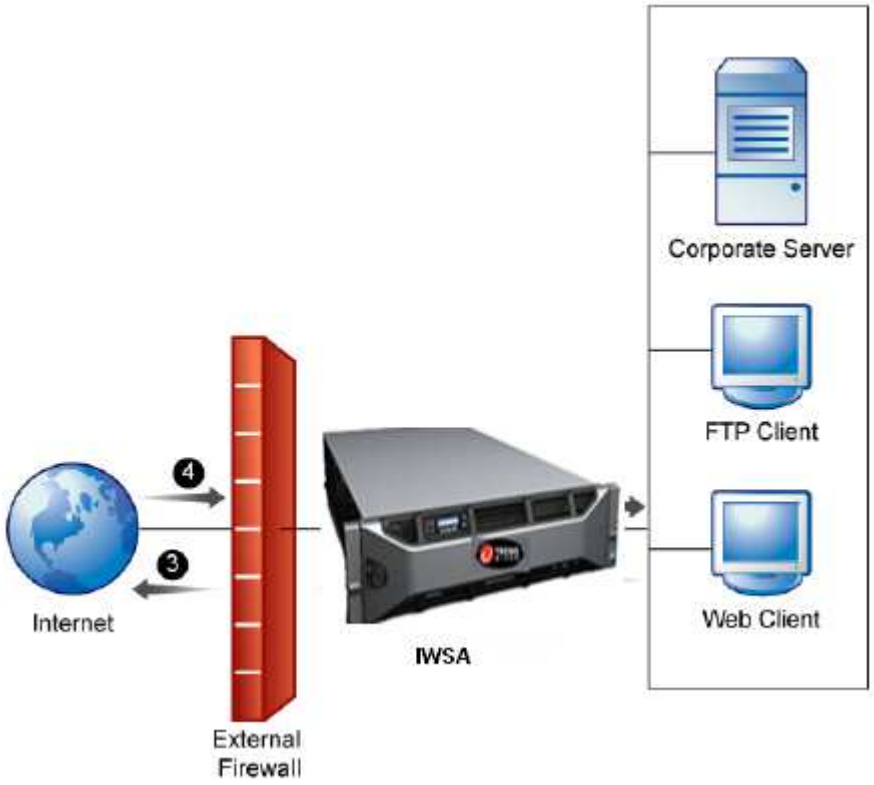


图4-1-2、单防火墙

防火墙配置允许链路达到内部的客户机。因此出于安全原因，防火墙必须限制达到内部机器的数据类型。例如防火墙只允许HTTP的数据经过IWSA EE 。

IWSA EE 的部署模式：

透明桥模式

HTTP代理模式

ICAP模式

WCCP模式

反向打理模式

用户可以根据不同的模式来部署IWSA EE ，下面章节将介绍IWSA EE 的部署模式。

4.2 透明桥模式

小知识：什么是透明桥模式？

透明桥模式——使用透明桥模式之后，用户不需要手动配置IWSA EE 为代理服务器就能够直接连接到Internet。IWSA EE 将以串接的模式接在网络中，让内部客户端通过IWSA EE 访问Internet。

当IWSA EE 被部署为桥接模式的时候，IWSA EE 通常被放置在两个网络设备中进行透明地扫描HTTP(S)和FTP流量。由于不需要用户去更改网络路由器、交换机等设置，部署桥模式的IWSA EE 是非常方便。

其网络结构图下：

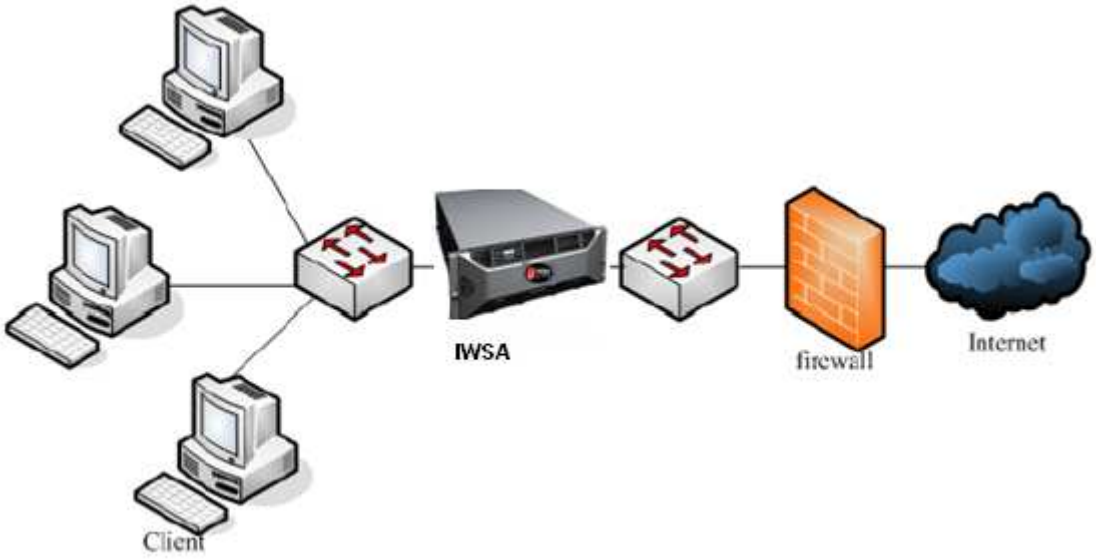


图4-2-1、IWSA EE 透明桥模式

IWSA EE 的桥模式工作方式：

1、客户端发送请求给Web服务器

2、IWSA EE 收到客户端的连接并发送请求给Web服务器

3、IWSA EE 与客户端建立连接

4、IWSA EE 与服务器建立连接，并从Web 服务器获得数据

5、如果数据不含病毒，那么IWSA EE 会把数据发送给Web客户端

6、如果数据包含病毒，那么IWSA EE 会阻止网页给Web客户端

该模式优势如下：

- 即插即用，部署简单，客户无需拥有代理服务器也可以部署，无需改动客户的网络环境；
- 客户端无需作任何的改动，只需要客户端的HTTP/FTP数据流经过IWSA，IWSA即可对此进行病毒的查杀；
- 可以在一款产品里同时对HTTP/FTP、间谍软件、钓鱼网站、Javaapplet进行防护，最大程度减少用户投资；
- 与DCS联动，协助管理员有效抵御间谍软件对企业网络的攻击；

4.3 Proxy模式

Proxy模式称之为代理模式，即IWSA EE 会作为代理服务器，当客户端需要上网的时候，需要通过IWSA EE 作为代理才能上网。因此从类别上来区分代理模式的话，可以把IWSA EE 划分为透明代理模式和非透明代理模式。

透明模式即用户不需要在各自的IE浏览器上配置IWSA EE 为代理服务器，因此在此种模式下，需要把IWSA EE 和4层交换机等合作，需要交换机把数据流指向IWSA EE 。

非透明模式即用户需要在各自的IE浏览器设置代理服务器指向IWSA EE 。

因此，从部署模式上来划分IWSA EE ，即：

1、独立模式——当ICAP设备不使用IWSA EE 时，IWSA EE 可以直接连接到Internet。

2、非独立模式——虽然不使用ICAP设备，但是IWSA EE 无法直接连到Internet，必须通过其他的HTTP代理。

3、透明代理模式——当使用L4交换机时，可以使用这种模式。

4、WCCP模式——IWSA EE 使用WCCP协议，并和有WCCP功能的设备联合。

下图为IWSA EE 非透明代理部署模式图：

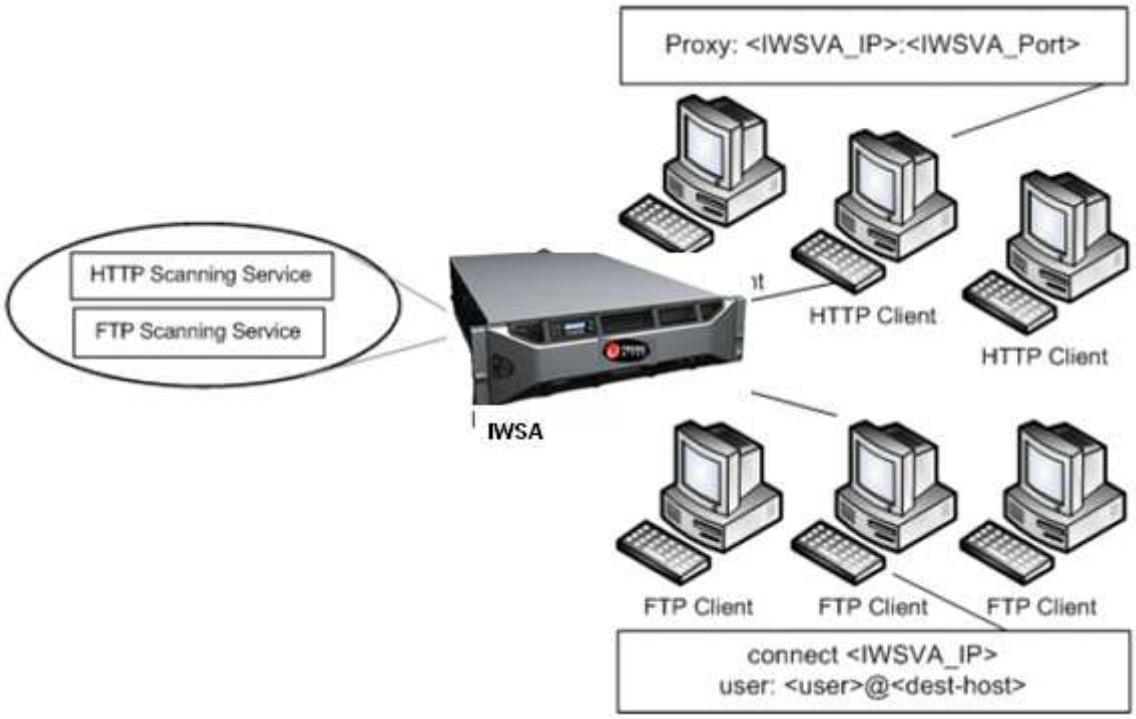


图4-3-1、IWSA EE 代理模式

部署方式：把IWSA部署在原来的代理服务器之前，客户端的IE代理设置指向IWSA的IP及侦听端口，IWSA接受客户端HTTP请求后再把相关请求重定向至原有的Proxy服务器。通过这样的部署，所有客户端发起的HTTP请求及Internet返回的HTTP数据流都必须经过IWSA的扫描，从而保证了企业内部的HTTP访问安全。

优势如下：

- 保护投资，原有的Proxy服务器可以继续使用，并且无需额外购买服务器，增加硬件投资；
- 可以根据管理员的需求定义HTTP的代理端口；
- 可以在一款产品里同时对HTTP/FTP、间谍软件、钓鱼网站、Javaapplet进行防护，最大程度减少用户投资；
- 与DCS联动，协助管理员有效抵御间谍软件对企业网络的攻击；

4.4 其他代理模式

除了基本的上述两种部署模式外，IWSA EE 还可以部署为反向代理模式和ICAP模式。本章节将简单描述这两种部署方式，具体详情可以查看我们的安装指南和管理员手册。

4.4.1 反向代理模式

虽然我们通常部署IWSA EE 是为了保护内网的客户端，但是我们也可以反过来部署IWSA EE 来保护内网的服务器，在这种模式下，其实已将IWSA EE 作为反向代理。因此对于外网的用户来说，要访问内网的服务器，需要先经过IWSA EE ，然后经过

扫描之后再将数据流重定向到内网的服务器。

其网络架构图如下：

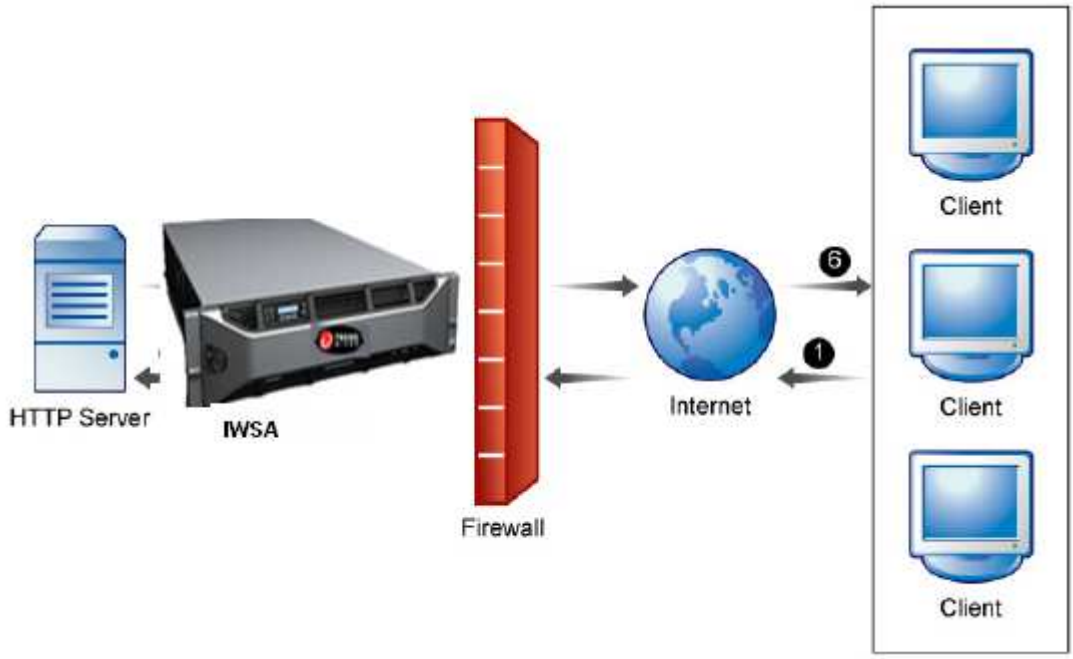


图4-4-1、反向代理模式

其客户端的访问流程如下：

1、客户端发起Web请求。

2、IWSA EE 收到请求。

3、IWSA EE 扫描网页内容，并将数据包转给实际的Web服务器。

4、Web服务器将请求的网页发给IWSA EE 。

5、IWSA EE 重写了页面头。

6、将修改的页面发送给请求的客户端。

4.4.2 ICAP部署模式

ICAP协议是用来将HTTP的请求/响应重定向到第三方处理设备，并从他们那里获取结果。发起ICAP请求的组件称之为ICAP客户端，处理请求的组件称之为ICAP服务器。

当IWSA EE 配置成ICAP模式，它可以处理来自各种ICAP客户端的请求。目前我们支持ICAP1.0版本：NetCache, Blue Coat, Cisco Content Engines (CE), and Squid。

其部署架构图如下：

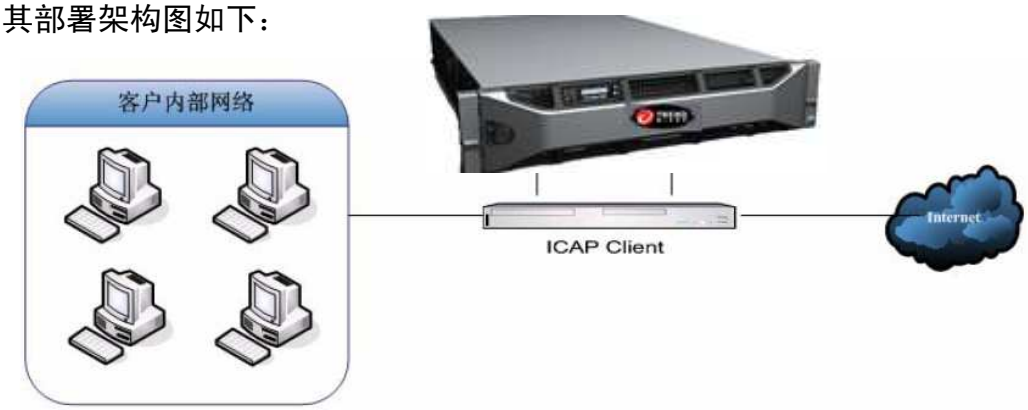


图4-4-2、ICAP模式

1、HTTP客户端请求外网的一个URL，然后发送请求给ICAP缓存代理设备

2、ICAP设备根据其配置来决定请求是否发送到IWSA EE 服务器

3、IWSA EE 检查URL的有效性

4、如果URL是有效的，ICAP服务器向Internet网发送URL请求

5、Internet把请求的网页返回给ICAP

6、如果网页有返回，ICAP返回给IWSA EE ，让其扫描

7、IWSA EE 扫描完毕之后，把反馈结果给ICAP

8、如果数据不含病毒等，ICAP设备把数据传给客户端，有问题的话，ICAP设备则返回错误信息给客户端

5. 安装 IWSA EE 5.1

5.1 安装前的准备

1、必须准备一个USB接口键盘和一台显示器和一个优盘。

2、注意：安装默认配置是除DELL正常配置外加一块两口Silicom Lanbypass卡。

以下为IWSA 1500的接口图：

位于左边的红框为板载Broadcom网卡，位于右边的红框为需要加入的Silicom网卡。

以下为IWSA 3000的接口图：

以下为IWSA 6000/1w的接口图：

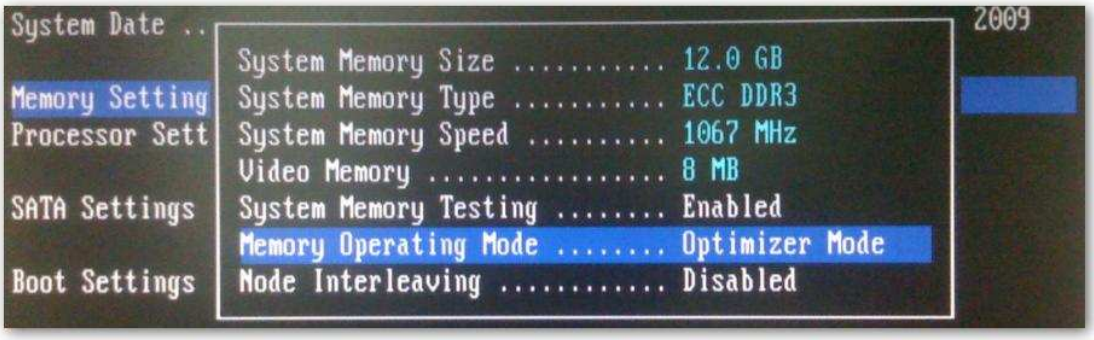
5.2 开机BIOS设置

按F2 进入BIOS设置：

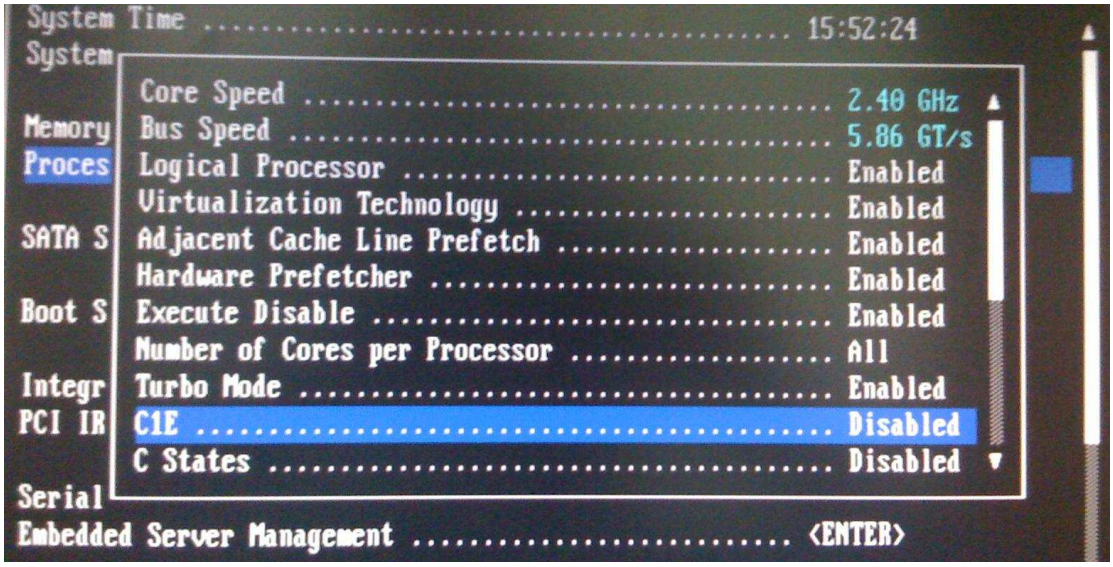
注意：进入BIOS可能存在需要输入密码。官方密码为qZTSpdum。

1、选择Memory Settings

设置 Memory Operating Mode 为 Optimizer Mode



2、选择Processor Settings
设置 “C1E”和“C States” 为 Disabled
设置“Virtualization Technology”为Enabled



3、选择Power Management
设置 Power Management 为 Maximum Performance

4、选择Boot Sequence
Embedded NIC 1 MBA disable(取消勾选)

5、选择Serial Communication，配置如下：

Serial Communication on with console redirection via com1

External Serial Connector : COM1 Choose “Serial Device1” if “Serial Device1=COM1”

Failsafe Baud Rate :115200

Remote Terminal Type: VT100/VT220

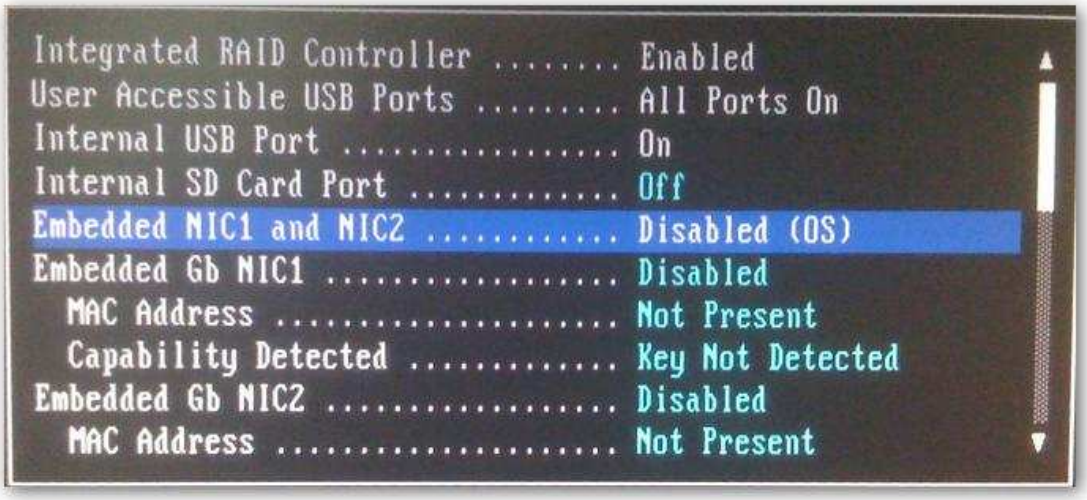
Redirection After Boot : Enabled

6. Integrated Devices（*差异步骤）

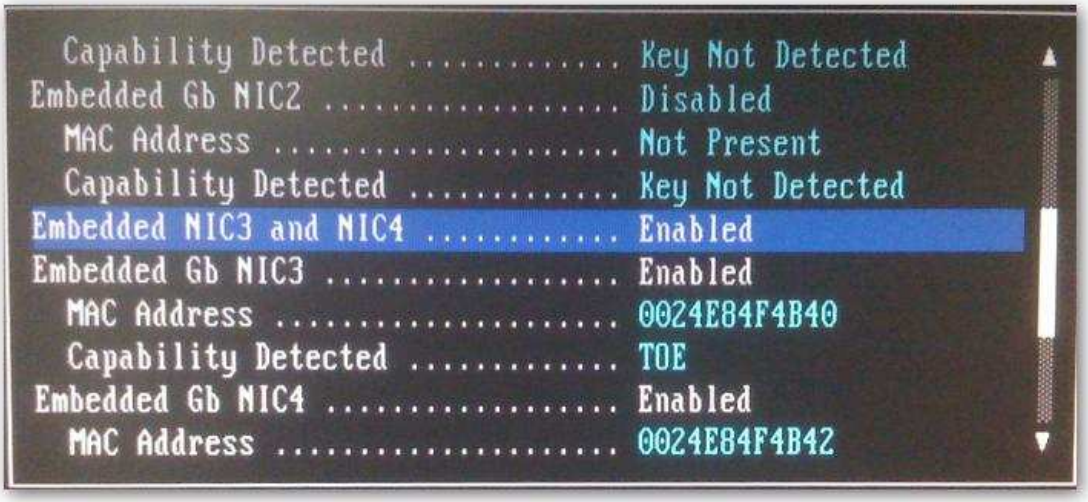
IWSA 1500 不需要修改

IWSA 3000, IWSA 6000, IWSA 10000 需要修改如下：

Disable “Embedded NIC1 and NIC2”（左边的两个网口）



Enable “Embedded NIC3 and NIC4”（右边的两个网口）



注:bypass网卡的两个口分别为eth1和eth2,主板集成的网卡左边两个(Gb1,GB2)被禁用，右边Gb3 为eth0.

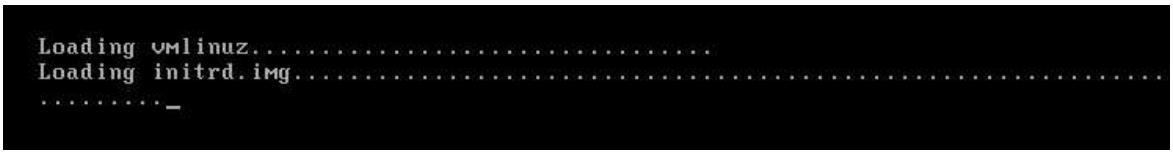
5.3 从CD-Rom引导

将光盘放入光驱后重启系统，看到如下界面：

5.4 准备安装

从上图的菜单中选择 “1. INSTALL IWSA EE ”

光驱会自动引导IWSA EE 安装进程

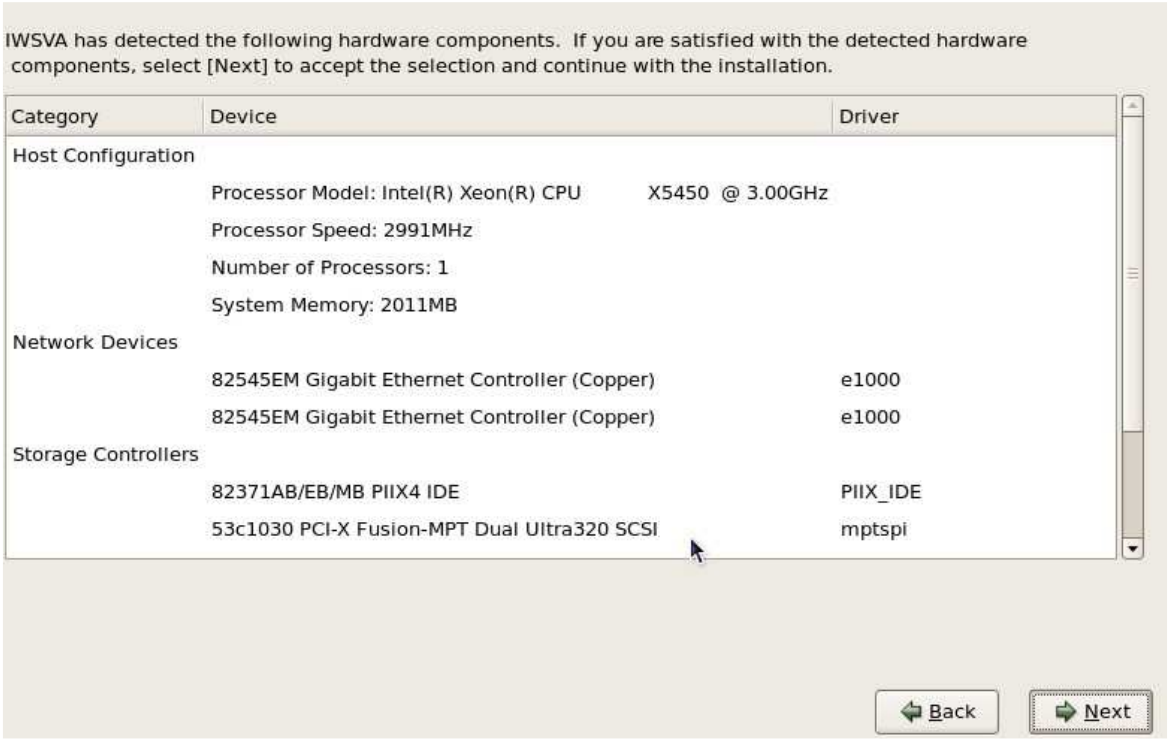


在License Agreement界面上点击 “Accept”

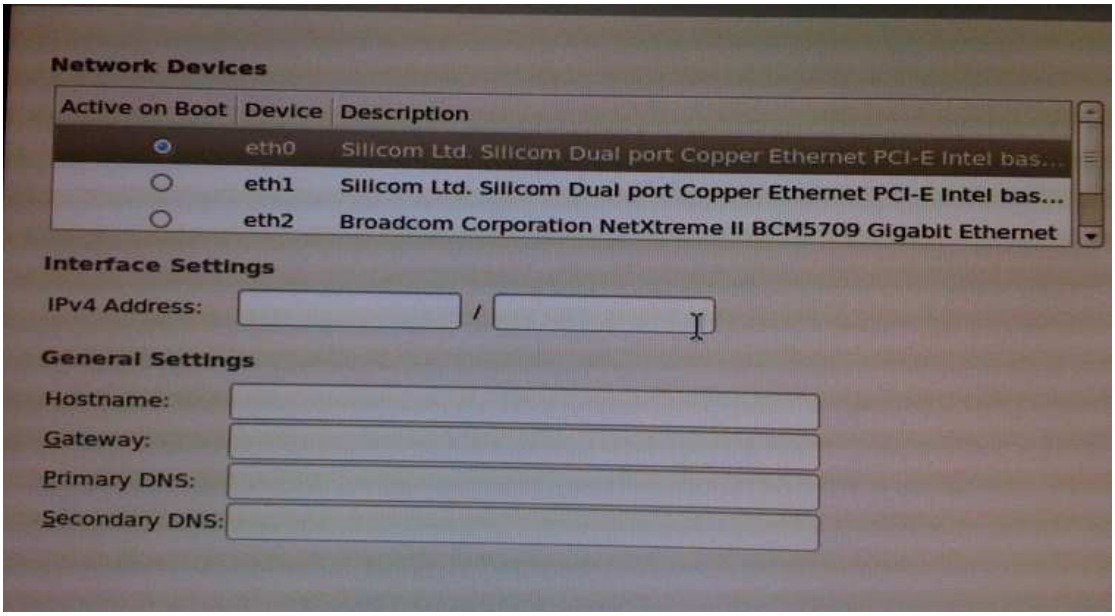
选择键盘

选择硬盘，取默认值点击“Next”;

随后的出现的页面上会显示IWSA EE 安装程序检测到的硬件信息



进入proxy设置界面(注意IWSA EE 5.1在安装的时候只能以proxy模式部署，如果要以transparent模式请参考后面步骤。)



A. 无论如何请选择eth0；

B. 配置IP

C. 配置主机名 （*差异步骤）

根据平台配置合适的主机名，如IWSA3000, IWSA6000等。

D. 配置网络参数:

网关: 192.168.252.254

Primary DNS : 168.95.1.1

Secondary DNS：

注意：以上设置是将来给DELL OEM的缺省设置，如果是自己手工安装，可以设置自己网络环境可用的网络环境参数，这样在后面就可以不必用COM口来连接IWSA进行配置。

5.5 时区设置

在网络参数配置页面点击“Next”就会随即显示时区配置页面

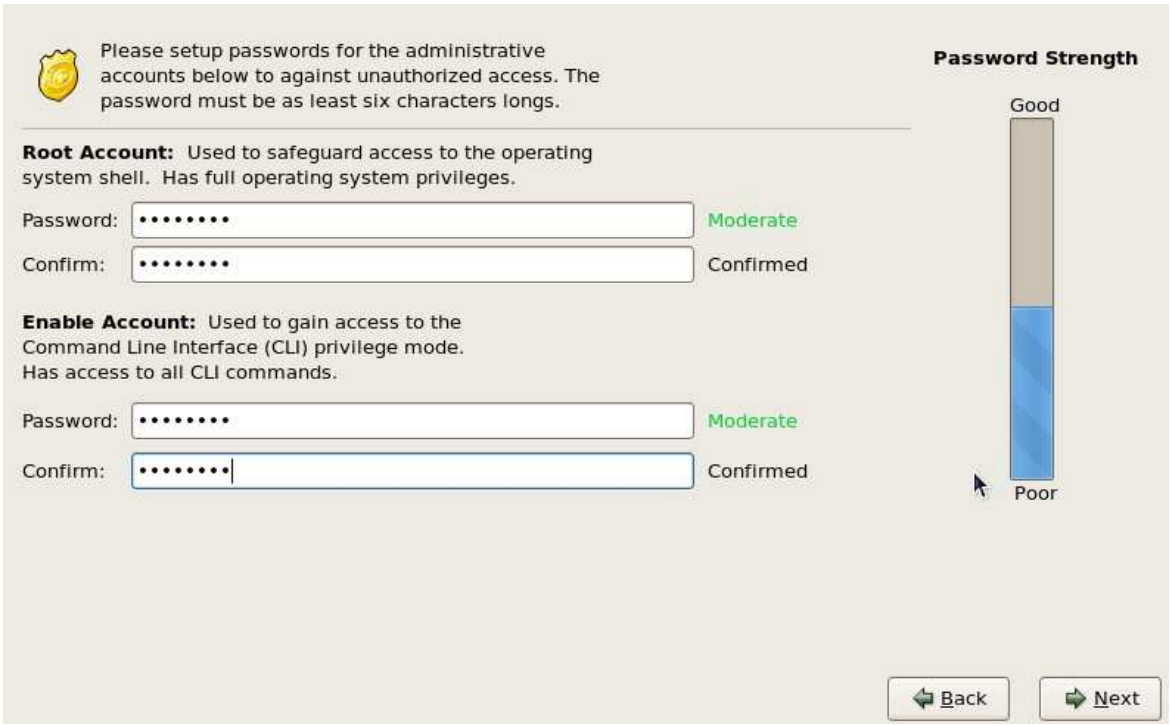
为 IWSA 系统选择正确的时区 : Asia/Shanghai

5.6 设置口令

请配置成如下默认密码：

Root Account密码：evita0

Enable Account密码：evita0



5.7 确认配置并开始安装

5.8 安装完毕要求重启计算机

5.9 拷贝系统补丁及性能优化程序

1. 登录Shell

登录帐号：root ， 密码:evita0

2. 用U盘将setup_iwsva51.tar.gz文件copy到IWSA的 /var 目录下

setup_iwsva51.tar.gz

fdisk -l （查看你的U盘 ， 它应该是/dev/sdb1 或 /dev/sdb2 或 /dev/sdc1）

mount /dev/sdb1 /mnt （mount 上你的U盘，/mnt前有空格）

cp /mnt/setup_iwsva51.tar.gz /var （注：/var前面是空格）

cd /var

tar xzvf setup_iwsva51.tar.gz

3. MAC地址绑定并更新OS补丁

cd /var/setup_iwsva51/

./setup_1.sh

reboot （setup_1.sh 会自动重启，如果没有，请手动重启并登陆后再进行后面操作）

系统在重新启动后，会完成MAC地址更新及绑定。重新登录系统，检查/etc/iftab是否存在，如果存在，表明该步骤完成。

4. 更新系统补丁及系统优化程序

cd /var/setup_iwsva51/

./setup_2.sh

系统后有提示，等待操作完成后，更新工作完成。
至此系统补丁及性能优化程序文件准备完成。

注意：当安装完第一章后，IWSA的网卡MAC地址已经绑定(与以前IWSA EE 3.1设置lanbypas卡的两个网口分别为eth1和eth2，而eth0为随机自带的位于右边的Gb3网口，作为管理口)，其他的overload bypass参数也已经设定，China BU的缺省设置也已经导入，但是此时IWSA还是proxy状态，还需要后续配置进行更改。)

6. IWSA EE 升级问题

目前IWSA EE 5.1不支持目前的IWSA EE 3.1的升级。

7. IWSA EE 5.1 的基本配置

7.1 网络的基本配置

安装完IWSA EE 之后需要重启机器，当机器重启完毕之后，就可以打开控制台根据IWSA EE 提供的配置向导来进行配置。当然如果您是拿到我们出厂的机器，即您拿到的机器已经安装了操作系统，因此首先您需要进行网络配置。可以通过COM口进行连接，配置参数与IWSA2500相同：

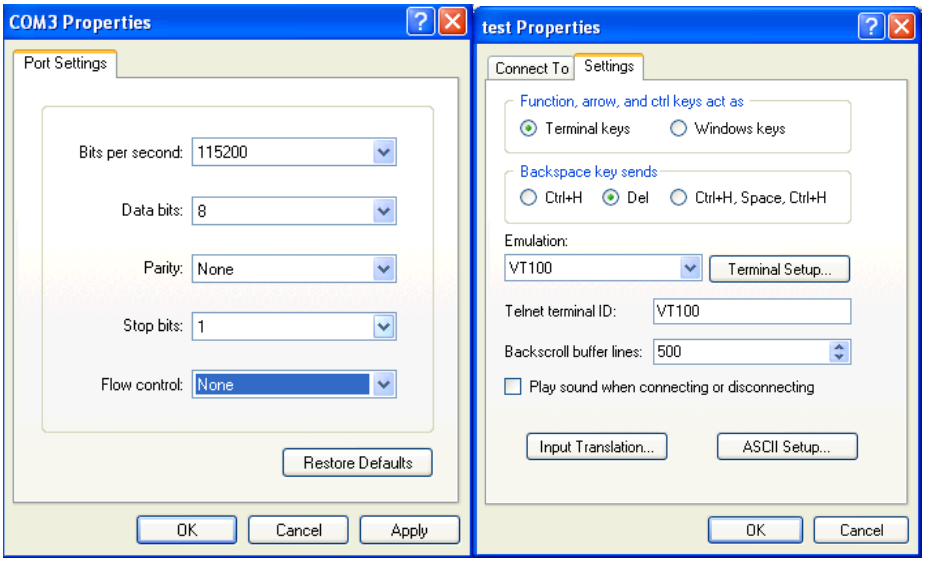


图7-1-1、COM设置

由于IWSA EE 5.1可以通过键盘和显示器来操作，因此不一定需要像IWSA2500一样，通过Com口来设置。

用root帐号登录执行“clish”命令，进入配置页面，再键入“enable”命令后(变成了enable帐户的身份)，就可进行系统设置，如下图：

```
[root@IWSVA56 ~]# clish
****************************************
*                 IWSVA                *
*                                      *
*      WARNING: Authorized Access Only *
****************************************
Welcome root it is Thu Sep 16 19:38:54 PDT 2010

> enable
Entering privileged mode...

enable#
enable#

configure   Configure system settings
exit        Turn off privileged commands
ftpput      Upload file through FTP protocol
help        Display an overview of the CLI syntax
history     Display the current session's command line history
ping        Ping
reboot      Reboot this computer immediately or after the specified delay.
resolve     Resolve a Web address either IP or FQDN on the network
restart     Restart a services
show        Show commands
shutdown    Shut down this computer immediately or after the specified delay.
start       Start a service, process or task
stop        Stop a s service, process
traceroute  TraceRoute
wget        Download file through HTTP/FTP protocols

enable#
```

图7-1-2、登录shell模式的clish模式

其中configure network命令可以设置很多网络相关的设置，如下图所示

```
enable# configure network
bridge    dns       hostname  interface lanbypass mgmt      portgroup proxy
route
```

图 7-1-3、配置网络设置

设置IWSA EE 的工作端口地址：

在图7-1-3中，使用configure network interface static eth0 <IP of IWSA EE > <netmask>（中间用空格）修改地址。

设置IWSA EE 的网关：

在上图中，使用configure network route default <IP of gateway>修改默认网关。

设置IWSA EE 的DNS：

使用configure network dns x.x.x.x可修改DNS（中间用空格）

当然更多的clish命令如图7-1-3所示。由于IWSA EE 的默认设置是正向代理模式，因此一个网卡是处于down的状态，如图7-1-4所示，我们用show network interfaces来查看状态。

```
Interface: eth0
        description: Intel Corporation 82545EM Gigabit Ethernet Controller (Copp
er) (rev 01)
        status: up
        type: PROXY
        driver: e1000
        businfo: 0000:00:11.0
        hardware addr: 00:0C:29:B5:DD:35

Interface: eth1
        description: Intel Corporation 82545EM Gigabit Ethernet Controller (Copp
er) (rev 01)
        status: down
        type: NONE
        driver: e1000
        businfo: 0000:00:12.0
        hardware addr: 00:0C:29:B5:DD:3F
```

图7-1-4、网口状态

7.2 使用配置向导来配置IWSA EE 5.1的透明桥模式

首先根据上节进行必要的网络配置，配置完后进行IWSA EE 的设置。由于IWSA默认安装好后管理口的IP地址配置在eth0上即板载的第一个网卡口上，因此需要登录IWSA EE来进行透明桥的配置。将笔记本的网口配置成和IWSA在同一网段，然后用直通线和IWSA的eth0相连。在笔记本的IE中输入http://<IWSA EE IP>:1812，用户名：admin 密码：adminIWSS85，如图：

图7-2-1、登录界面图

登录之后由于第一次使用，因此会提示您修改密码，如图7-2-2。

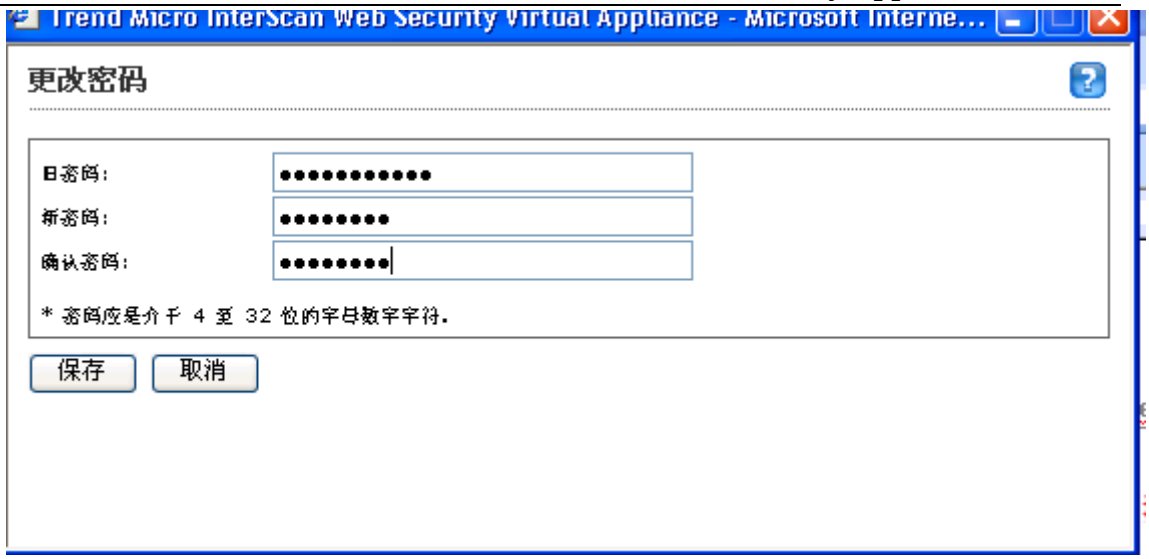


图7-2-2、修改密码

下面的步骤是配置透明模式，IWSA EE 可以提供部署向导来给用户设置。如图7-2-3。

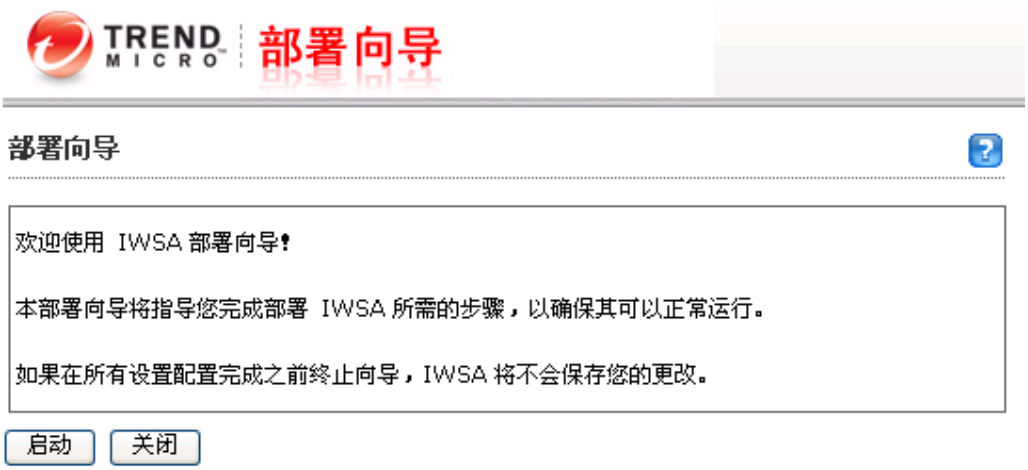


图7-2-3、部署向导

点击“启动”，选用需要部署的模式，提供的部署方式如图7-2-4。

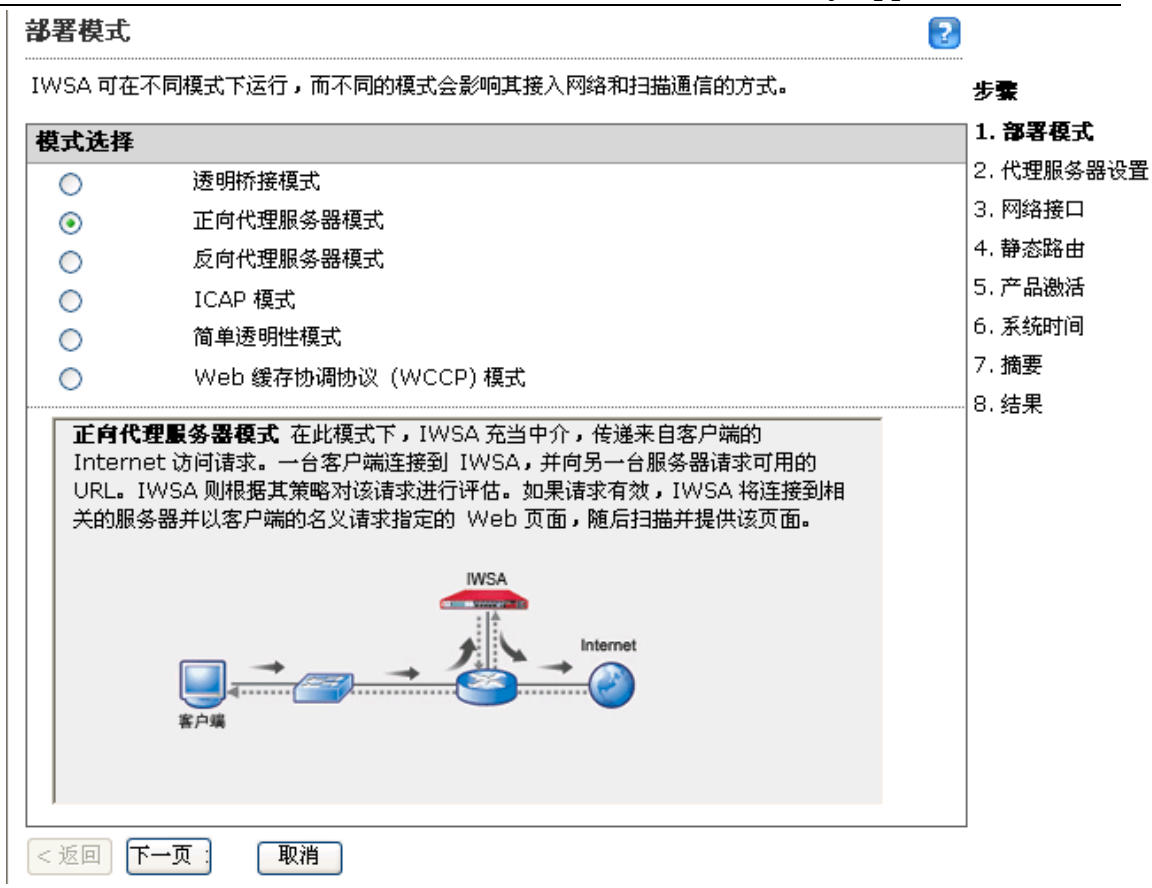


图7-2-4、模式选择

1） 我们选择透明桥模式，点击“下一页”。由于使用透明模式，也就是把 IWSA EE 串接在网络中，因此务必选择 eth1 和 eth2 口作为数据口。如果有单独的管理网段的话，勾选“单独管理口”，选择 eth0 口作为管理网段接口，然后设置管理 IP 地址，这样数据口的 IP 地址可以设任意与管理 IP 不在同一网段的 IP 地址，然后点“下一页”按钮，如下图 7-2-5 所示

图7-2-5、网络设置

在图7-2-5中左侧图片是没有设置管理口，由于IWSA真正使用的数据口进行扫描的是加载的Silicom网卡，因此需要调整为内部为eth1即IWSA的Silicom 1号口，外部为eth2，即Silicom的2号口。

右侧图为启用了管理口，IWSA的数据口仍然是加载的网卡，但是IWSA的管理口需要设置，您可以选择板载口Broadcom卡上的任一网口，如本例选用了BroadCom的1号口eth0。需要注意的是，启用了管理口之后，需要给管理口一个有效IP和有效网关，让用户可以通过IE登录IWSA以及让IWSA到外网去更新组件。但IWSA的桥接口bridge的IP可以设置为一个虚拟的无效IP，保证与IWSA的管理口IP尽量不在同一网段。

在5.1的版本中，通过控制台来启用管理口，无需到/var/iwss/network.ini中去修改配置文件。

勿忘记：如果IWSA启用了管理口，用笔记本直连配置的时候，需要将笔记本网口和IWSA的管理口相连；如果IWSA不用管理口的话，需要将笔记本与IWSA的加载网卡口相连。

如果有需要设置静态路由，如图7-2-6所示设置。

图7-2-6、设置网段、掩码和下一跳的路由IP

输入IWSA EE 的激活码，如图7-2-7。

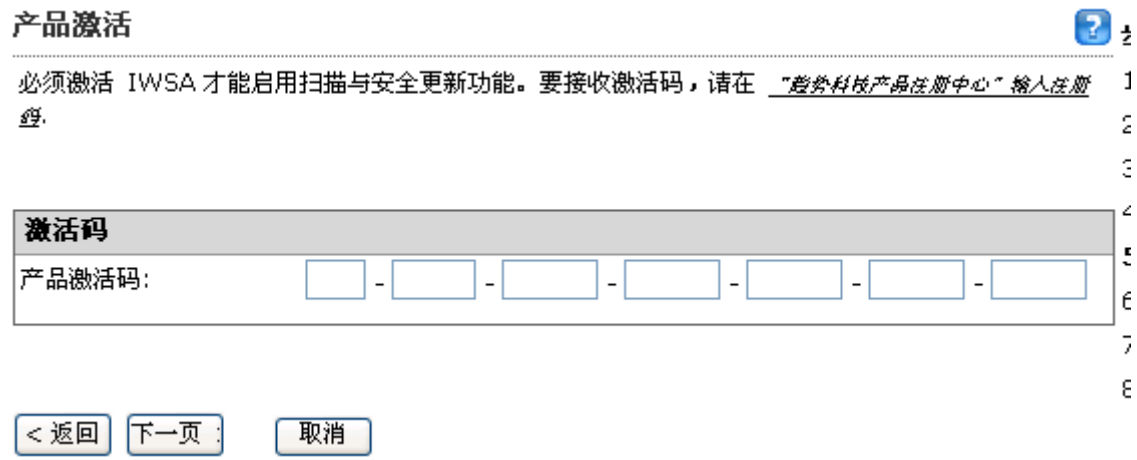


图7-2-7、激活码

设置IWSA EE 的系统时间，如图7-2-8。

图7-2-8、系统时间

点击“下一页”，显示配置的摘要，点击“提交”完成。

图7-2-9、配置摘要

显示配置进程。同时IWSA EE 将重启。

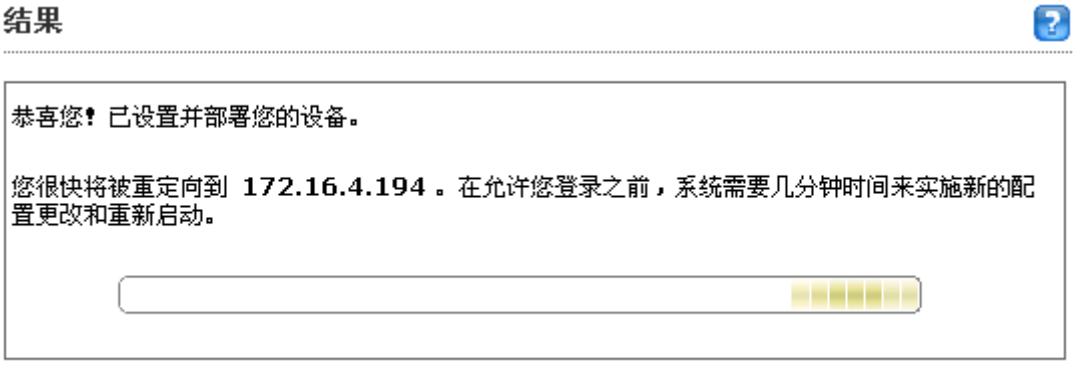


图7-2-10、配置进程

配置完成后，重新登录IWSA EE ，首页如图7-2-11。

图7-2-11、摘要界面

由于配置成了透明桥模式，因此我们再使用show network interfaces命令来查看，发现两个网口都启用了，如图7-2-12。

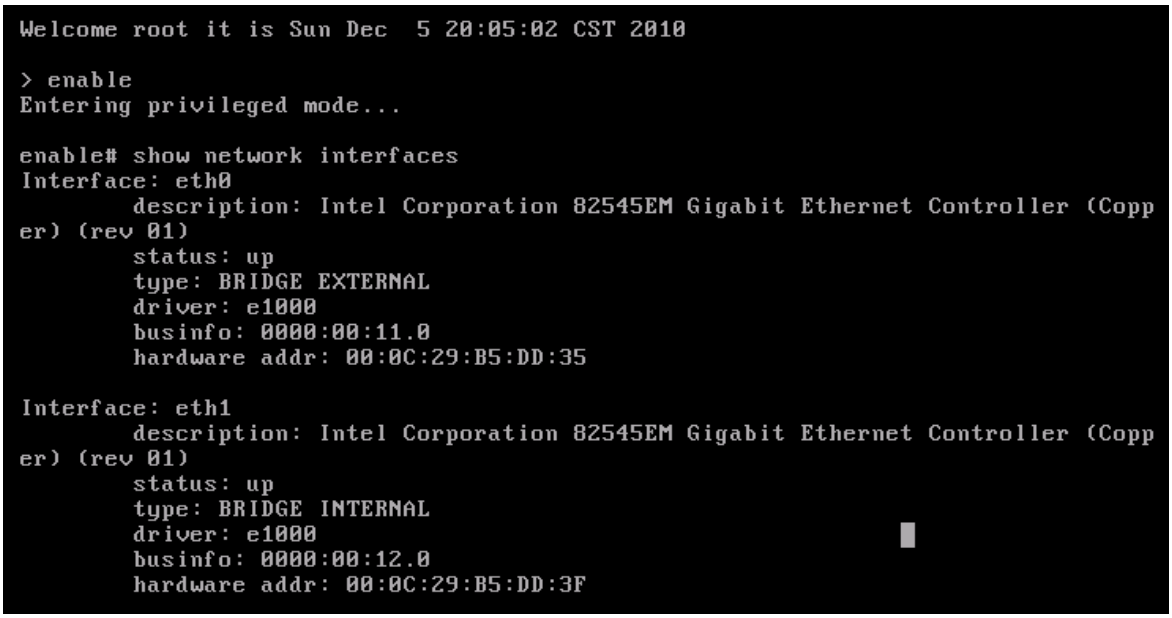


图7-2-12、网卡状态

7.3 IWSA EE 的基本设置

本章节将介绍部署完IWSA EE 之后需要操作的基本HTTP的配置和检查。

7.3.1 IWSA EE 的基本检查和管理设置

在配置HTTP的策略之前，需要检查IWSA EE 的HTTP和FTP扫描服务是否正常。即在摘要界面中的最上方“HTTP(s)通信”和“FTP通信”是否开启，正常状态如下图所示：

图7-3-1、服务状态

下面检查IWSA EE 的产品使用授权是否正确，点击“管理”-“产品使用授权”，如图所示：

图7-3-2、产品使用授权

如果发现产品没有激活或者激活码所显示的维护时间不准确，请点击“在线检查状态”或者点击“输入新激活码”连接，输入新的激活码，如图7-3-3所示：

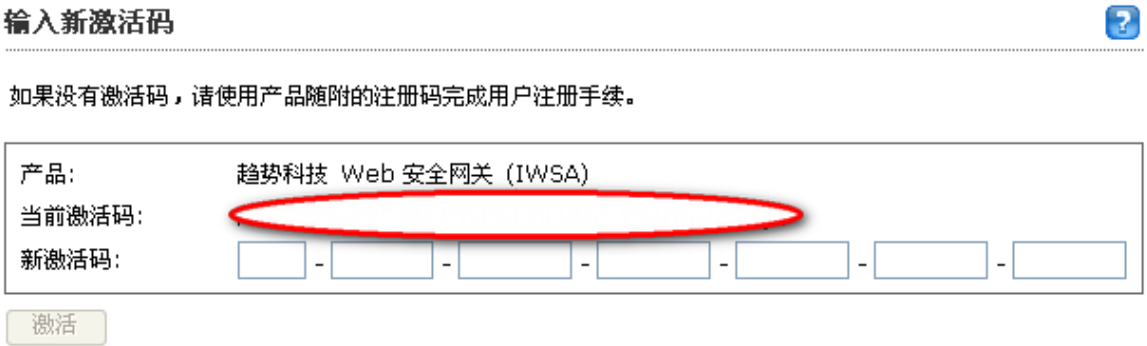


图7-3-3、激活码

7.3.2 IWSA EE 的开机和关机

除了通过机器上的power键来开关机，同时也可以使用IWSA EE 5.1的界面上来开

关机，如图7-3-4所示，当我们选择“关机”-“继续”，则IWSA EE 将自动关机。如果我们选择“重新启动”，可以选择“IWSA服务重新启动”或者“系统重新启动”。

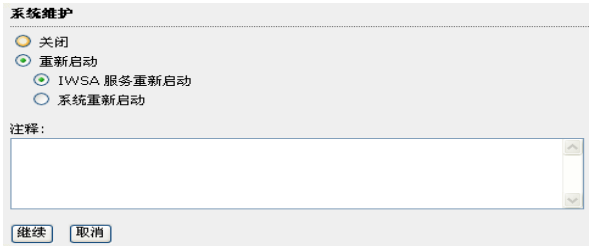


图7-3-4、开关机

注意在执行该操作的时候，需要在“注释”的文本框中添加开关机的原因即可成功执行。在IWSA EE 重启服务或者系统之前会有如下图的提醒：

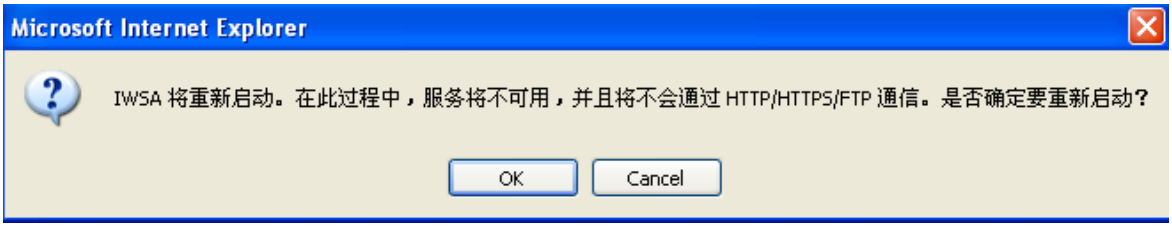


图7-3-5、开关机提醒

7.3.3 IWSA EE 的更新组件

当部署和配置好IWSA EE 之后，首先要做的事情是确保IWSA EE 可以更新组件并获得最新的组件。IWSA EE 的更新组件的方式主要分为两种：手动更新组件和自动更新组件。

手动更新组件，即用户人工点击IWSA EE 上面的更新按钮让IWSA EE 获得最新的病毒码版本。我们建议您在第一次部署完IWSA EE 之后运行一次手动更新组件。由于某些用户的环境里面需要设置代理服务器才能让IWSA EE 到外网去获得更新，因此需要添加代理设置。

添加代理设置的方法：点击“更新”-“连接设置”-“代理服务器设置”，如图7-3-6所示。

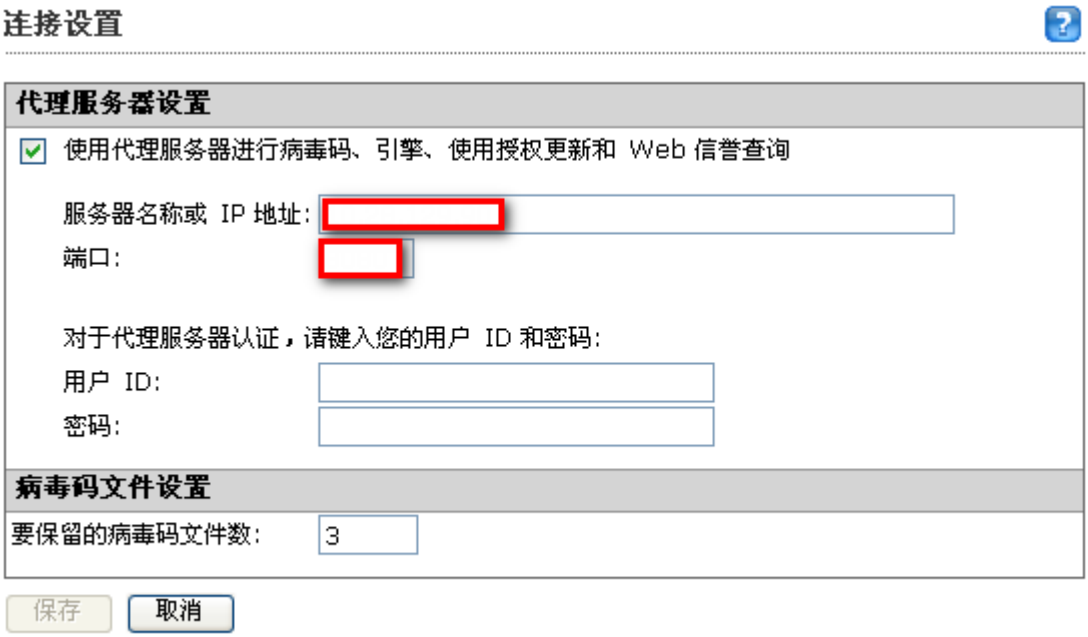


图7-3-6、代理设置

设置完代理模式之后，就可以进行手动更新，更新方法如下：

1、点击“更新”菜单、

2、选择“手动”

3、选择要更新的组件，点击“更新”，如图7-3-7所示。

用户也可以根据自己的实际情况来设置预设更新的时间，设置方法如下：

1、点击“更新”菜单

2、选择“时间表”

3、选择好病毒码、扫描引擎和URL Filtering扫描引擎的更新时间。这三类组件的更新是独立开来的。如图7-3-8所示。

图7-3-7、手动更新组件

图7-3-8、预设更新

7.3.4 配置HTTPS的解密

IWSA EE 5.1支持对加密的URL进行解密并扫描，一旦加密的URL被解密之后，HTTP的内容会被IWSA EE 的HTTP扫描策略和URL过滤策略给扫描。您可以根据您的需求来设置对特定网站进行解密扫描。

1、HTTPS的解密设置

我们可以点击“HTTPS解密”-“设置”，如图7-3-9所示。

图7-3-9、HTTPS解密设置-服务器证书验证

点击了启用证书验证之后，可以对客户端需要访问站点的SSL证书进行效验，如果证书过期或者有问题，IWSA EE 会拒绝客户端的访问。

我们可以点击“客户端证书处理”的时候，表示当服务器需要请求客户端证书时，IWSA EE 给予的处理操作。如图7-3-10所示。

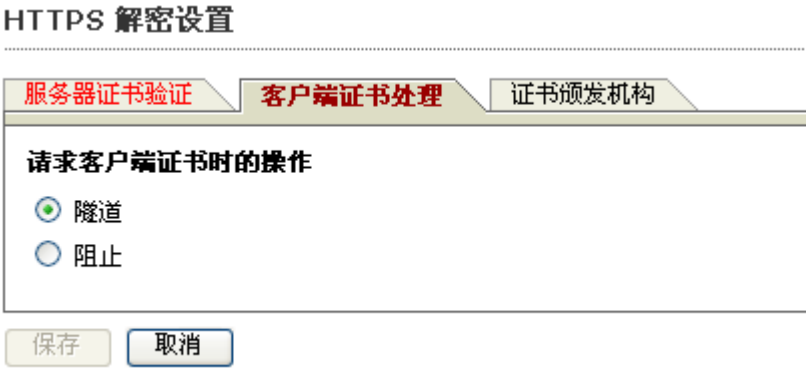


图7-3-10、客户端证书处理

IWSA EE 给予的操作：隧道和阻止。虽然一些安全性比较高的企业和银行需要请求客户端的证书，但是IWSA EE 目前还不支持对客户端证书的解密和扫描。因此IWSA EE 只提供了这两种操作。隧道的意思就是对请求客户端证书时直接放行。或者阻止请求客户端证书。

IWSA EE 默认会自动创建随机的证书给客户端，由于此CA证书没有被Internet CA机构认证，因此客户端的IE会显示证书警告。如果用户想不提示证书警告，需要设置CA证书。设置方法如下：

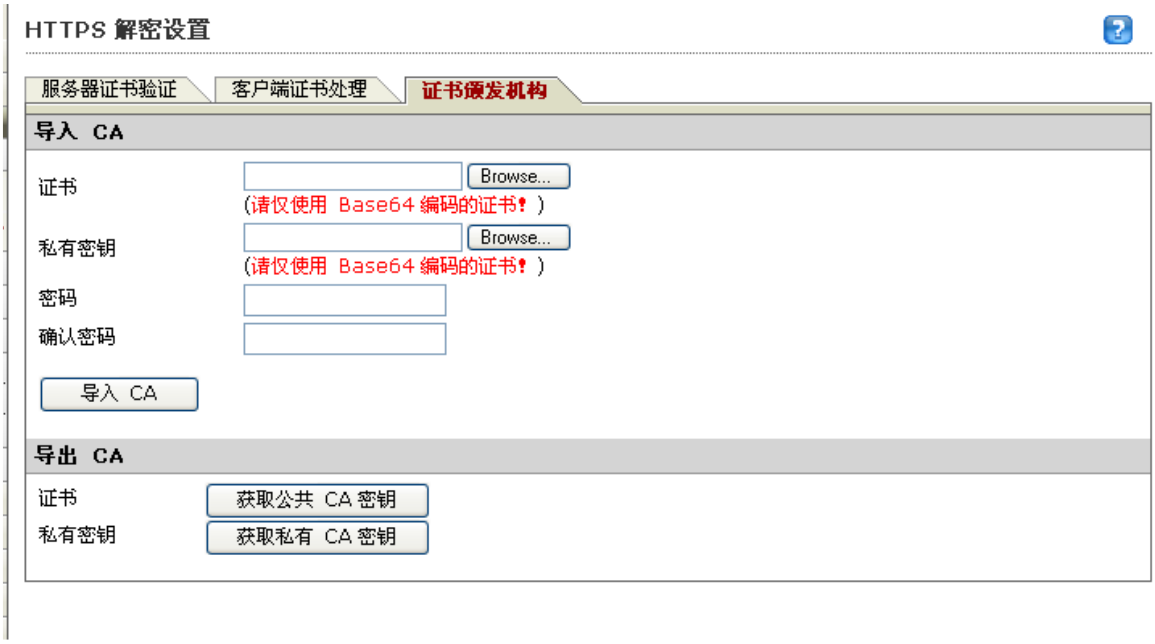


图7-3-11、CA设置

如图7-3-11所示，点击“Browse”导入公钥和私钥设置密码，并点击“导入CA”。需要公钥和私钥时，只要点击“获取公共CA密钥”即可。

2、设置IWSA EE 的HTTPS解密策略

点击“HTTPS解密”，选择“策略”。如图7-3-12所示。

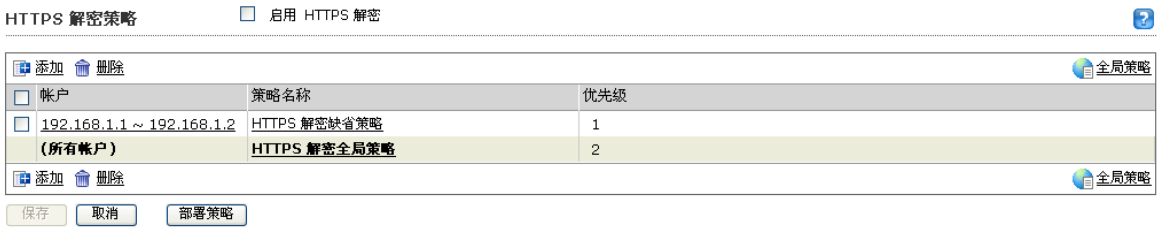


图7-3-12、解密策略

默认IWSA EE 没有启用HTTPS解密，因此需要点击该页最上方的“启用HTTPS解密”。启用之后，默认的策略为“HTTPS解密全局策略”，点击该链接进入下图7-3-13所示。

用户可以更改HTTPS解密策略的规则，点击“规则”项，可以发现列表为URL类别列表，其中可以根据类别依次展开内容，选择需要解密和扫描的HTTPS内容。修改过后，需要点击“保存”按钮，并在图7-3-12所示中，点击“部署策略”，让该规则生效。

点击图7-3-13的“例外”项，则可以设置允许的HTTPS的URL，如图7-3-14所示。其中可以选择允许列表。关于允许列表的定义，我们将在以后的章节中做介绍。

图7-3-13、HTTPS解密策略规则

图7-3-14、HTTPS解密例外

7.3.5 配置HTTP扫描

1、HTTP扫描设置

点击“HTTP”-“HTTP扫描”-“设置”，出现如下图7-3-15所示。此章节将介绍HTTP的扫描策略如何配置并使用。

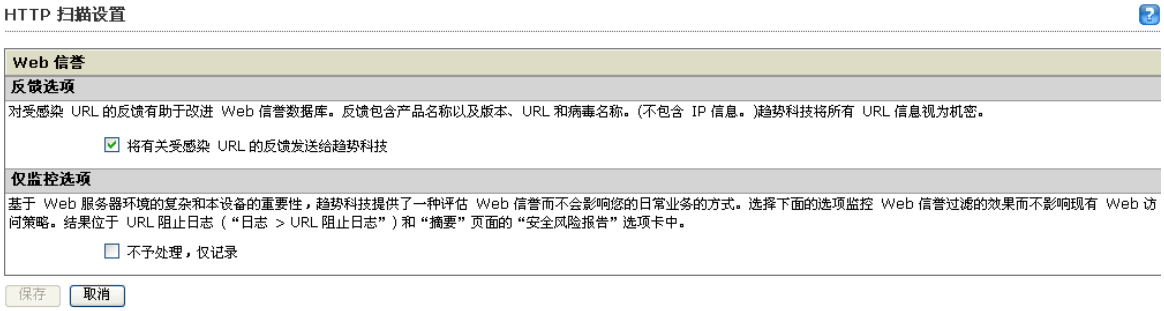


图7-3-15、HTTP扫描设置

此扫描设置主要分为“反馈选项”和“仅监控选项”。

“反馈选项”即将有感染的URL的反馈发送给趋势科技，以便我们改善URL过滤的准确度。

“仅监控选项”表示对于WEB信誉过低的URL，我们只是做一个记录，并不干涉。

2、HTTP的扫描策略

点击“HTTP”-“HTTP扫描”-“策略”，出现如下图7-3-16所示。我们可以配置HTTP的扫描策略。用户要真正使用IWSA EE 的扫描功能，需要开启“启用病毒扫描”，需要使用Web信誉功能，需要勾选这个选项。Web信誉功能是对用户访问的网页进行打分，如果分数低于设置的阀值，则IWSA EE 会阻止网页的访问。

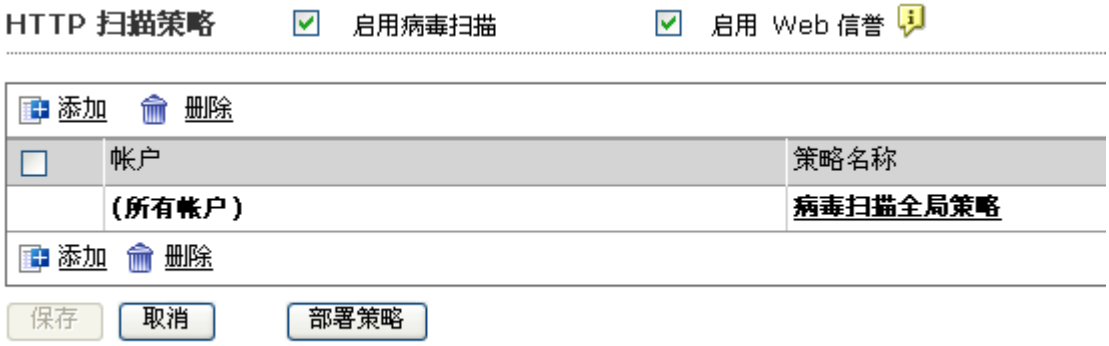


图7-3-16、HTTP扫描策略

默认只有“病毒扫描全局策略”，用户可以修改其默认的策略，点击“病毒扫描全局策略”。会出现如图7-3-17所示的页面。主要分为Web信誉规则、病毒扫描规则、间谍软件/灰色软件扫描规则、例外和处理措施。

1)、Web信誉规则

我们可以在图7-3-17页面中设置在此策略中是否使用Web信誉规则并设置阀值，默认为中级。同时还可以勾选是否检查有域名欺骗和钓鱼网络的存在。

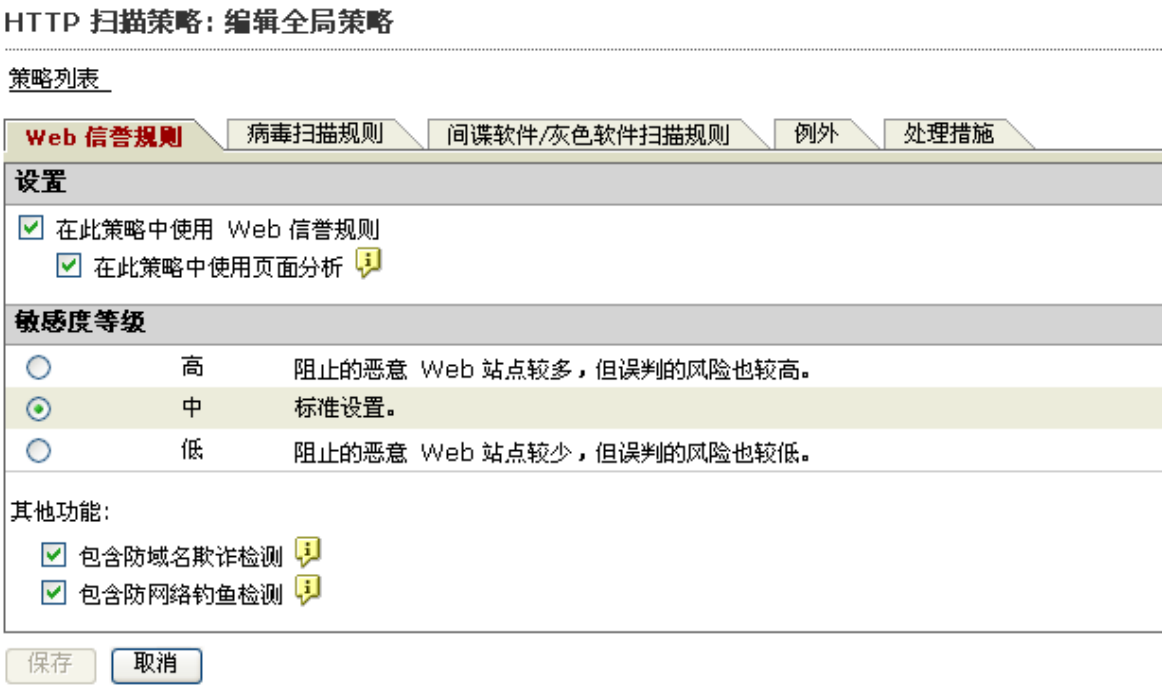


图7-3-17、Web信誉规则

2)、配置病毒扫描规则

点击“病毒扫描规则”选项，可以对HTTP页面做如下操作：

阻止以下文件类型

如图7-13-18所示：

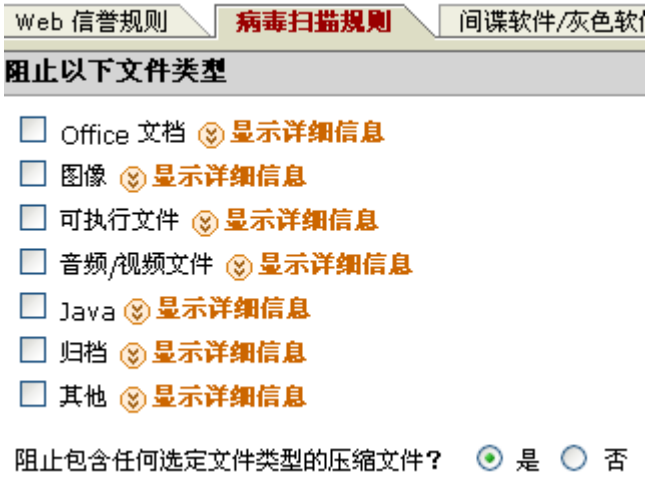


图7-3-18、阻止文件类型

在此类别中勾选需要阻止的文件类型。

扫描以下文件类型

设置需要扫描的文件类型，如图7-3-19所示。设置是否扫描“所有可扫描文件”、“IntelliScan”（判断文件的真实类型）和“特定文件”（只扫描某些特定的文件）。也可以例外某些MIME文件。

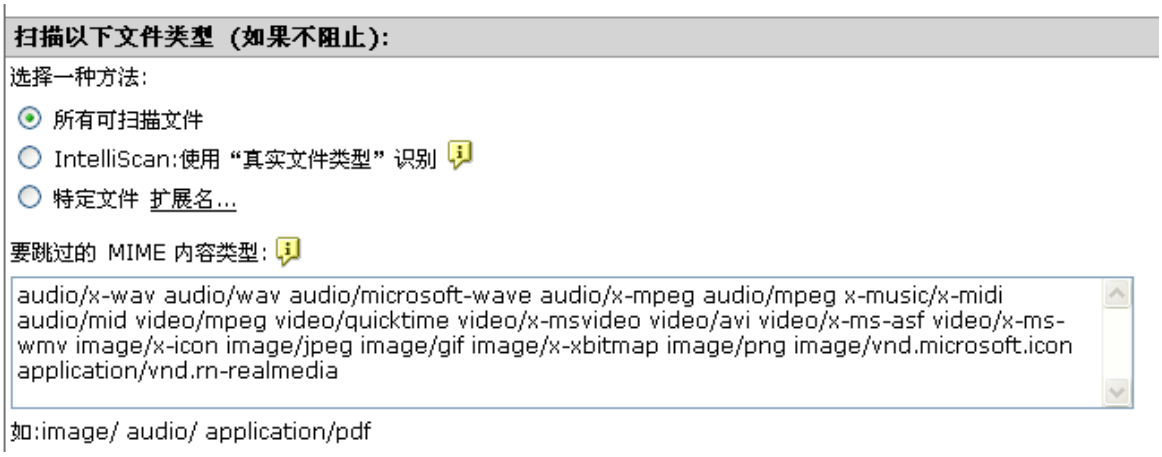


图7-3-19、扫描文件类型

IntelliTrap

启用此选项可以对潜在恶意的压缩文件（通常由病毒生成）进行启发式检测。

压缩文件处理

IWSA EE 可以对网页中包含的压缩文件进行扫描，并允许用户来设置压缩文件的处理规则。如图7-3-20所示。用户可以设置是否阻止或者放行压缩文件，并应用到相应的压缩文件（如文件数目，解压大小，层数设置等。）

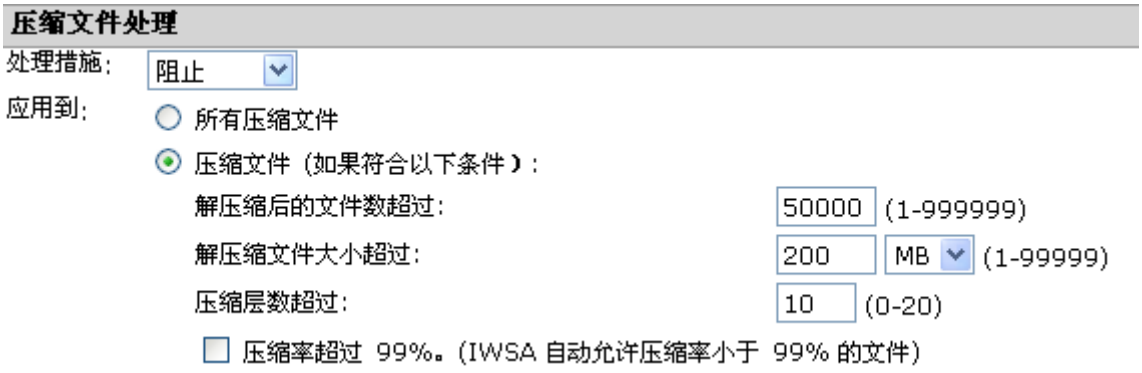


图7-3-20、压缩文件处理

大文件处理

遇到较大文件时，可以设置相对应的措施。

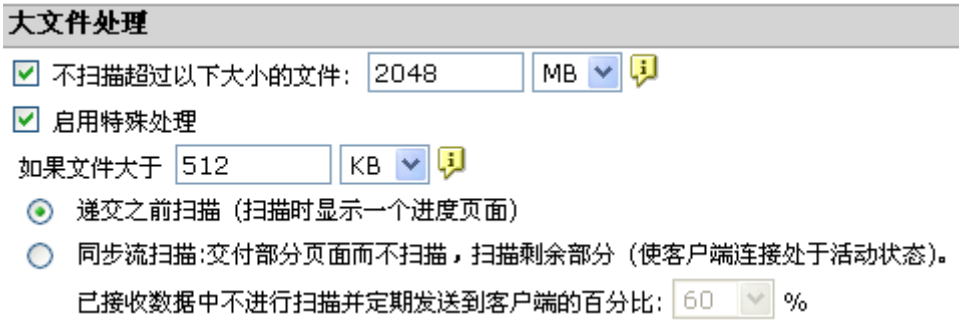


图7-3-21、大文件处理

如果用户经常访问比较大的文件时，可以勾选“同步流扫描”，这样可以使用户同时扫描，同时可以访问网页。

隔离文件的处理

可以选择是否对已隔离文件进行加密

3)、配置间谍软件

默认IWSA EE 不扫描间谍软件和灰色软件，用户可以出于安全考虑选择相应的类

型进行扫描。如图7-3-22所示。

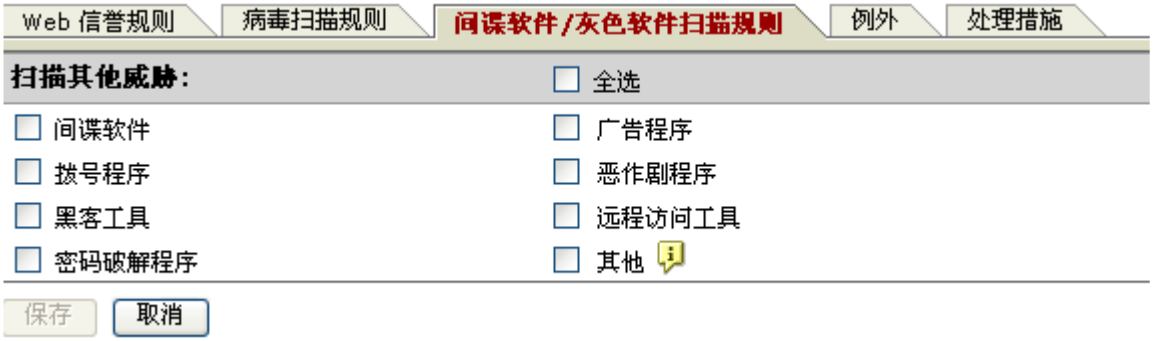


图7-3-22、间谍软件设置

4)、设置例外

设置例外列表可以允许IWSA EE 不扫描特定的URL以放行IWSA EE 可能误判的网页。从IWSA EE 5.1开始，为了方便用户统一管理例外列表，不再使用之前的trusted URL列表，而全部改用例外列表。如图7-3-23所示。

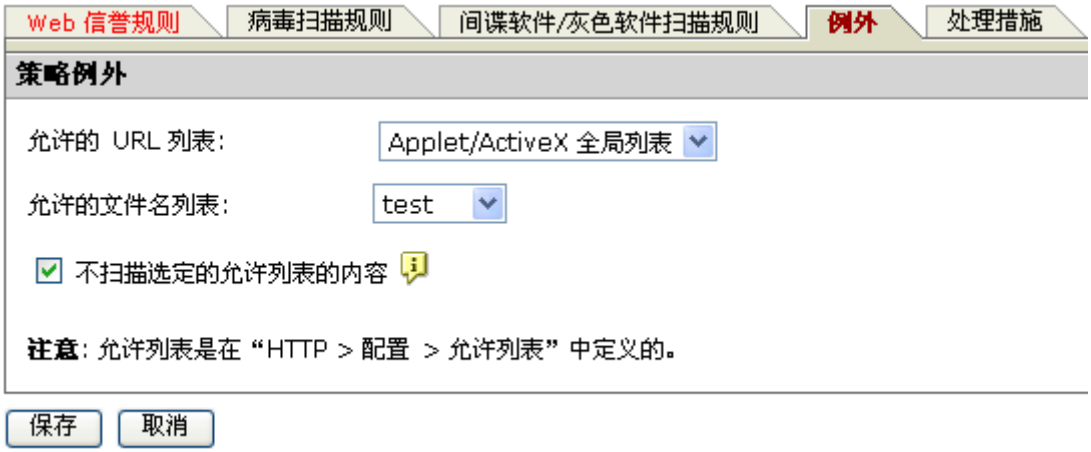


图7-3-23、例外列表

在“允许的URL列表”中选择需要过滤的URL表格，在“允许的文件名列表”下拉框中选择文件列表名，同时勾选“不扫描特定的允许列表的内容”，并点击“保存”。关于允许列表的设置将在后面的章节中进行介绍。

5)、配置处理措施

用户可以配置IWSA EE 对检测到的URL和文件的处理措施。如图7-3-24所示。基本的处理措施为：删除、隔离、清除和不予处理。

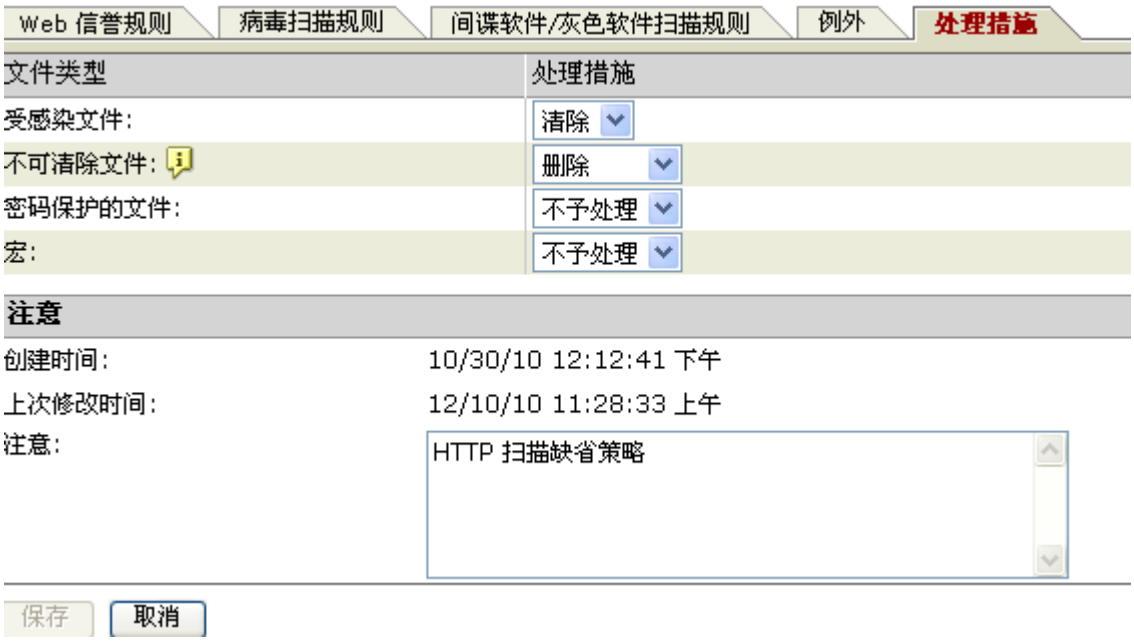


图7-3-24、处理措施设置

7.3.6 配置URL过滤

IWSA EE 除了可以设置对URL的扫描，同时也可以设置URL的过滤，即可以保障内网的用户在工作的时间内不去访问外网的某些网页。

1、URL的设置

用户需要定义好访问网页的时间。点击“HTTP”-“URL过滤”-“设置”，如图7-3-25所示：

图7-3-25、URL过滤时间表

用户可以定义工作的时间段以及工作日，表示在这些时间段部分娱乐类的网页无

法被访问。

2、URL的过滤策略

定义了时间表之后，需要设置过滤策略。点击“HTTP”-“URL过滤”-“策略”，进入“URL过滤全局策略”。如图7-3-26所示：

图7-3-26、URL过滤规则

用户可以设置需要过滤的URL的分类。如果网站被拦截，可以点击进入我们的网页类别查询系统，地址如下：

http://www.trendmicro.com/submit-files/index.htm

7.3.7 设置URL列表的允许和阻止

在前面的章节中有介绍到需要设置允许的URL例外列表，因此本章节将介绍如何设置URL列表。URL的允许列表分为两类：全局允许和策略允许。全局允许即在IWSA EE的所有策略中生效，策略允许即在IWSA EE 里面的某条定义的策略中生效。一旦全局策略中将站点加入到阻止列表中后，即使策略中定义为扫描例外站点，该站点也会被阻止。同时全局允许列表的优先级高于全局阻止列表，即在全局允许列表中加入站点之后，即使在全局阻止中加入该站点，此站点还是被允许访问。

1、添加全局允许列表。登录控制台，点击菜单“HTTP”，展开“URL访问控制”，点击“全局可信URL”，如图7-3-27所示，加入站点。

图7-3-27、设置可信URL

在“匹配”的文本框中输入站点路径，点击“信任”，会在“不扫描以下URL”中出现您添加的站点，点击“保存”即可。

注意：由于允许可信任的URL，默认是不启用，因此请打钩页面上方的“启用可信URL”。

2、添加阻止的URL列表

登录控制台，点击菜单“HTTP”，展开“URL访问控制”，点击“全局URL阻止”，如图7-3-28所示，加入站点。

图7-3-28、全局URL阻止

在“匹配”的文本框中输入站点路径，点击“阻止”，会在“阻止列表”中出现您添加的站点，点击“保存”即可。

3、允许列表的制作

1)、URL列表

如果要设置策略中的允许列表，请如下操作，点击菜单“HTTP”，展开“配置”-“允许列表”，默认IWSA EE 已设置了策略“Applet/ActiveX 全局列表”，用户可以自定义相关的允许列表。如图7-3-29所示，点击“添加”。

图7-3-29、允许URL列表

图7-3-30、添加URL

在“列表名称”中输入列表的名称，在“匹配”的文本框中输入相应的URL，点击“添加”，在“允许的URL”框中会显示允许的URL，点击“保存”。如果需要删除此URL的允许，需要选择好URL，点击“移除”。

2)、文件名列表

在“允许列表”的页面中选择“文件名列表”选项卡，点击“添加”。输入相应的文件名称，点击“保存”，如图7-3-31所示。

图7-3-31、文件名称列表

允许列表的设置主要是运用在之前介绍过的HTTP策略中设置的列表，如图图7-3-23所示。

7.4 日志和报表的查询

7.4.1 测试IWSA EE

当配置完IWSA EE 的基本操作之后，我们可以尝试来检测IWSA EE 是否能阻止威胁的网站，并生成日志以便查询。

测试IWSA EE 是否可以正常抓到病毒，让测试病毒eicar网站经过IWSA EE 。Eicar网址如下：

http://www.eicar.org/anti_virus_test_file.htm

点击“Download area using the standard protocol http”中的“eicar.com”。

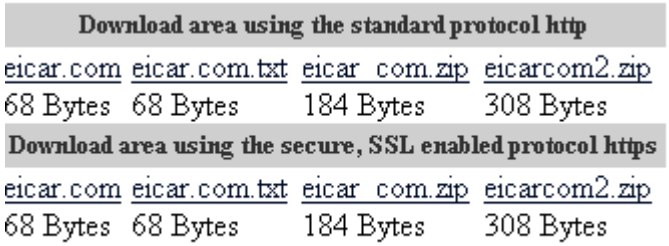


图7-4-1、eicar测试病毒

由于下载了eicar的测试病毒，因此IWSA EE 会检测出此病毒，并显示阻止该文件的下载，如图7-4-2所示。

图7-4-2、IWSA EE 成功拦截Eicar病毒

如果出现图7-4-2的页面，表示IWSA EE 工作正常，能够捕获到病毒，并列出病毒的名称。

7.4.2 IWSA EE 的日志查询

1)、URL的阻止日志

根据IWSA EE 抓到的病毒和阻止的页面，我们可以通过日志来查询。点击“日志”菜单，展开“日志查询”。点击“URL阻止日志”，会列出被阻止的URL的名称或者被阻止的URL的策略。如图7-4-3所示。

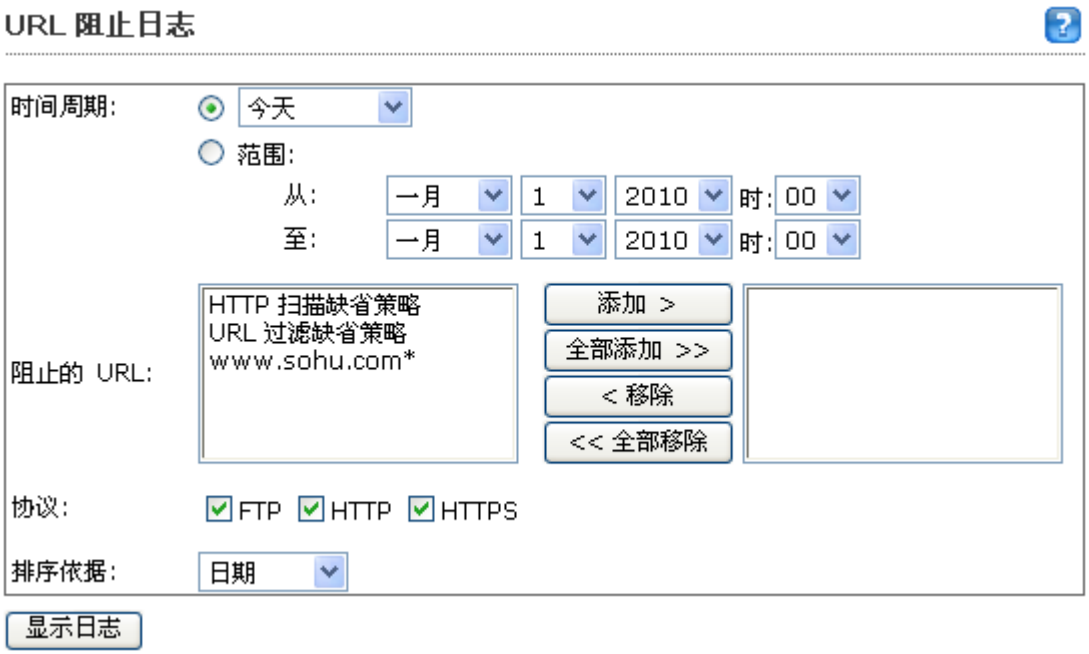


图7-4-3、URL阻止日志查询（一）

选择要查看的URL后，点击“添加”，然后选择相应的协议，点击“显示日志”，如图7-4-4所示我们前面访问的eicar网站的日志记录。

日期	类别	规则	用户 ID	扫描类型	OPP ID	URL	协议
12/13/10 11:05:42 上午	病毒	HTTP 扫描缺省策略	172.16.4.185	病毒扫描	0	http://www.eicar.org/download/eicar.com.txt	http

图7-4-4、URL阻止日志查询（二）

2)、审计日志

点击“日志”菜单，展开“日志查询”。点击“审计日志”，会列出登录IWSA EE 的账户所做过的操作。如图7-4-5所示，显示了admin账户所执行的操作，如修改配置文件，添加列表等。

用户	日期	执行的处理措施
admin	12/13/10 9:44:56 上午	changed /etc/iscan/intscan.ini: [URL-trusting] enable=yes(no)
admin	12/13/10 9:44:56 上午	Trusted URL list now contains: au.download.windowsupdate.com*
admin	12/13/10 9:44:56 上午	Trusted URL list now contains: www.update.microsoft.com*
admin	12/13/10 9:44:56 上午	Trusted URL list now contains: www.windowsupdate.com*

图7-4-5、审计日志查询

用户需要保存日志的话，可以点击“导出为CSV格式”，将日志导出。

3)、病毒日志

对于用户来说，病毒日志是比较重要的，通过病毒日志的查询可以知道目前被IWSA EE 查杀的病毒情况。点击“日志”菜单，展开“日志查询”。点击“病毒日志”，

选择查杀出来的病毒，点击“添加”，点击“显示日志”，如图7-4-6所示。

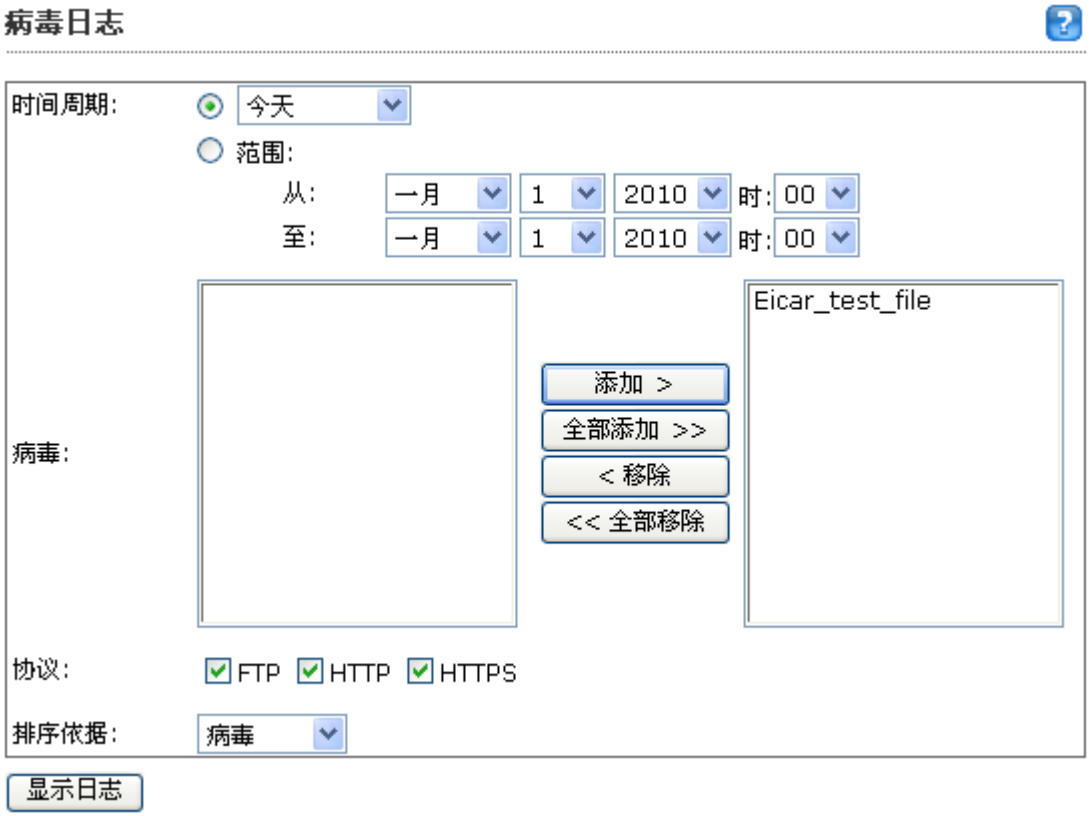


图7-4-6、病毒日志查询（一）

图7-4-7、病毒日志查询（二）

关于其他的日志分类查询请查阅我们的管理员手册以便详细了解各项分类如何查询。

7.4.3 报表查询

IWSA EE 不但可以提供详细的日志查询功能，而且还可以提供报表的制作。方便用户定期查看报告，了解当前网络的情况。

1)、实时报告

实时报告相当于一次性报告，根据选择的条件、时间和选项的内容来生成报告。如图7-4-8所示，制作当前的病毒报告。

图7-4-8、实时报告的设置

点击“生成报告”，如图7-4-9所示。用户可以把报告通过页面上的导出格式来保存，目前可以选择的格式为PDF和CSV。

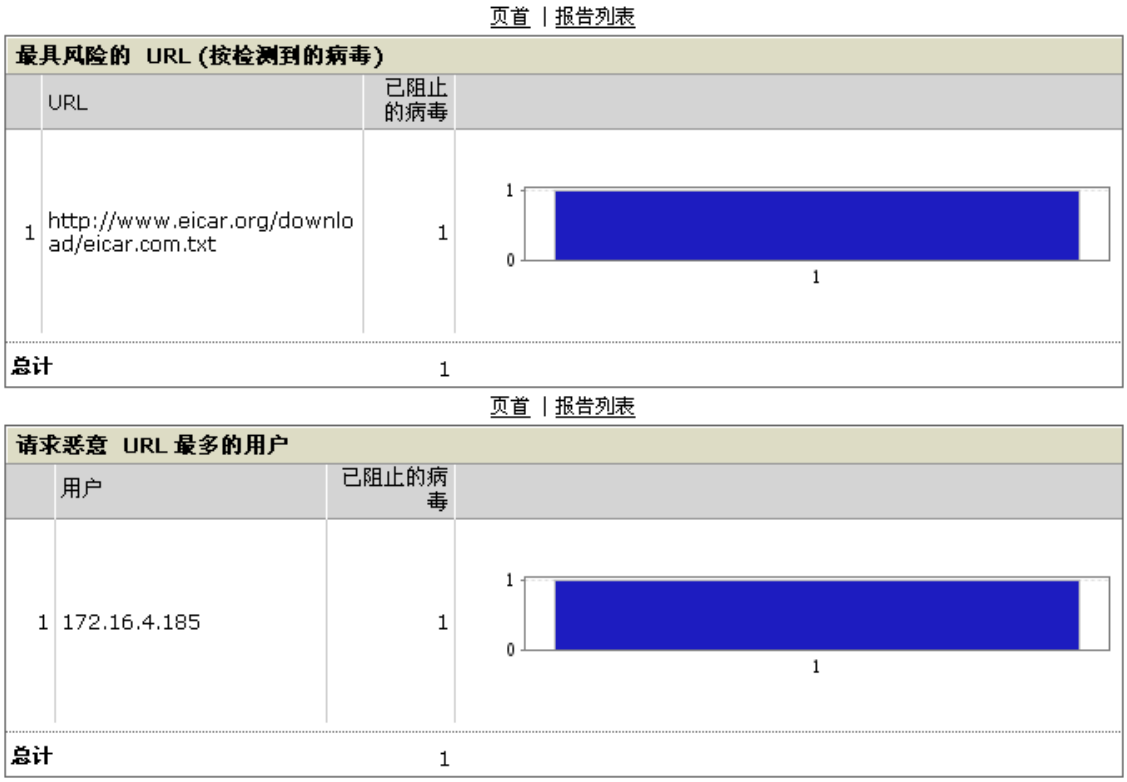


图7-4-9、实时日志报告

2)、报告模版的设置

由于用户比较关心的是定期生成报表，因此我们将在下面一章节介绍如何设置预设报表。制作预设报表之前，用户可以先配置报告模版。点击“报告”菜单，展开“报告模版”，输入模版名称，选择报告的协议、用户、报告类型和报告中使用的图形（如线状、柱状等），如图7-4-10所示。

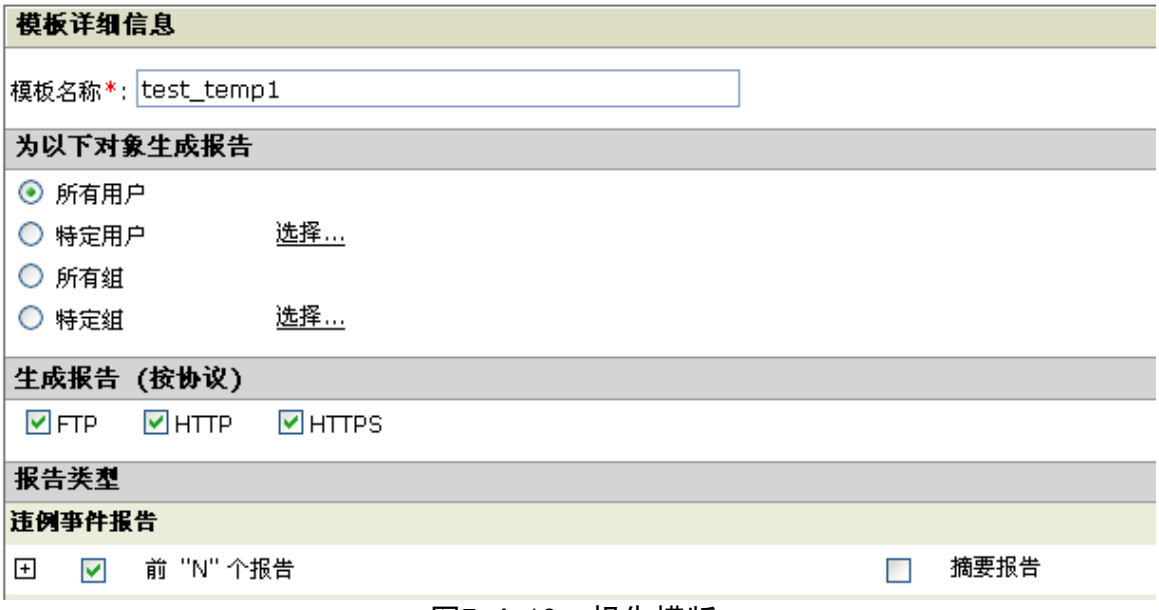


图7-4-10、报告模版

点击“保存”。报告模版就设置完毕。

3)、预设报告

让IWSA EE 自动生成报告，可以使用预设报告的功能。点击“报告”菜单，展开“预设报告”，选择预设报告的类型。目前预设报告分为三类：每日报告、每周报告、

每月报告。

以每日报告为例，点击“每日报告”，选择“预设每日报告”选项卡，单击“添加”。如图7-4-11所示。

图7-4-11、预设报告设置

勾选“启用报告”，输入报告名称、选择制作报告的开始时间、选择预设的报告模版，如果需要每日发送报告，勾选“使用电子邮件发送此报告”，选择报告的格式，以及填写收件人、发件人和邮件主题。点击“保存”。如图7-4-12所示，一个预设报告的设置已经完成。

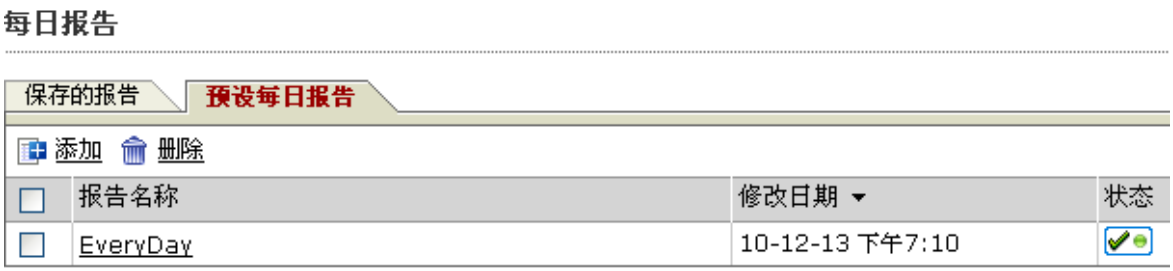


图7-4-12、预设每日报告

每月报告和每周报告的设置和每日报告的方式相同，只是设置的报告制作时间不同，具体用户可以参考管理员手册来设置。

7.5 配置通知

点击“通知”菜单，如图7-5-1所示，IWSA EE 针对哪些事件会发送通知。

图7-5-1、通知的类型

点击右上角的“将通知发送给...”，如图7-5-2所示：

图7-5-2、电子邮件设置

设置发件人地址、收件人地址、SMTP服务器地址、端口等。

用户需要自定义各项扫描通知邮件的内容的话，点击链接即可，如点击图7-5-1中“HTTP/HTTPS阻止文件类型”，出现图7-5-3。

图7-5-3、阻止文件类型通知设置

用户可以自定义邮件正文内容，定义好后，点击“保存”即可。当IWSA EE 遇到文件类型阻止事件之后，会发送消息给管理员，并在用户的Web页面上显示出消息内容。

7.6 IWSA EE 的维护

本章节将介绍如何来配置和维护IWSA EE 。IWSA EE 的维护主要为以下几个内容：

系统升级；

程序升级；

配置备份；

账户管理；

日志/报告维护

1)、更新操作系统

更新操作系统是对IWSA EE 里面本身自带的操作系统进行升级。由于每过一段时间，我司会推出新的系统补丁，因此为了解决操作系统中存在的各类问题，建议用户在安装完或者定期给IWSA EE 安装补丁。

安装补丁方法如下：

- 点击左边“管理”菜单，展开“更新操作系统”，出现如下图7-6-1所示的页面。
- 点击“浏览”，选择相应的更新文件。

- 点击“更新”
- IWSA EE 会要求重启机器就完成了更新操作系统。

图7-6-1、更新操作系统

2)、程序升级

用户在安装完IWSA EE 需要安装系统patch以解决应用程序中可能出现的问题。程序安装方法如下：

- 点击左边“管理”菜单，展开“系统 Patch”，出现如下图7-6-2所示的页面。
- 点击“浏览”，选择相应的更新文件。
- 点击“更新”
- IWSA EE 会要求重启机器就完成了系统Patch的更新。

图7-6-2、系统Patch

3)、系统备份/恢复

定期的备份IWSA EE 配置文件可以帮助用户保存之前的设置，比如URL的过滤设置、允许的URL访问列表等。当遇到IWSA EE 重装或者需要恢复之前的配置文件时，可以迅速恢复过来。备份方法如下：

- 点击左边“管理”菜单，展开“配置备份/恢复”，出现如下图7-6-3所示的页面。
- 点击“导出”，会出现图7-6-4所示的进度条。
- 点击“保存”，选择相应的位置来存放打包的配置文件，格式为tar，如图7-6-5所示。

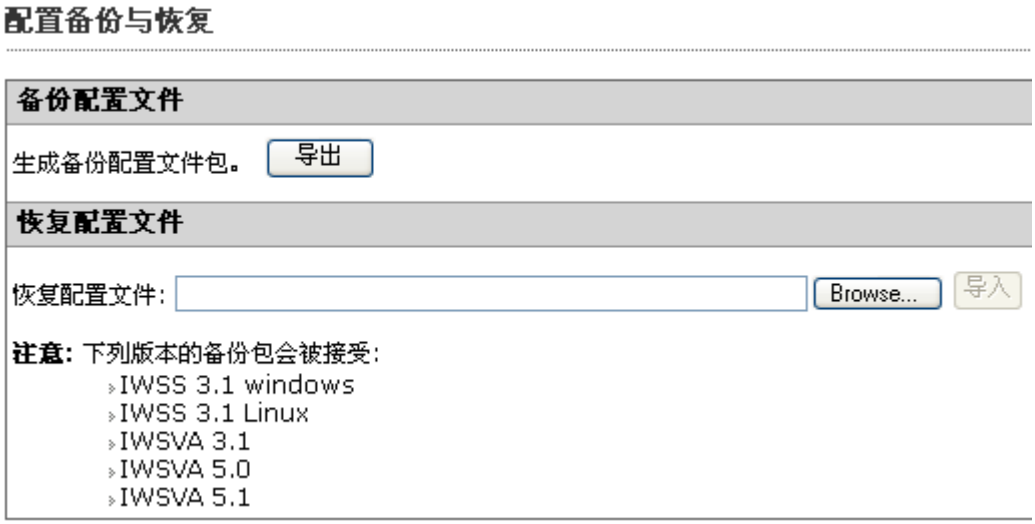


图7-6-3、备份/恢复配置

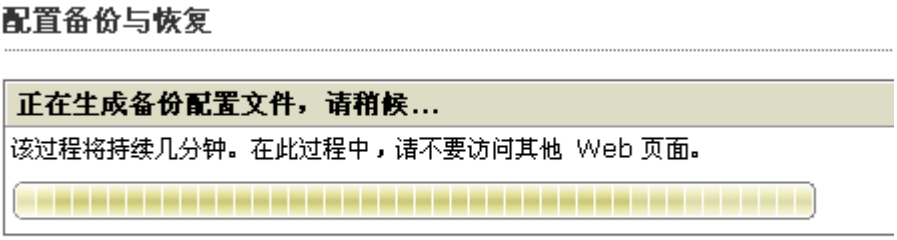


图7-6-4、生成备份文件

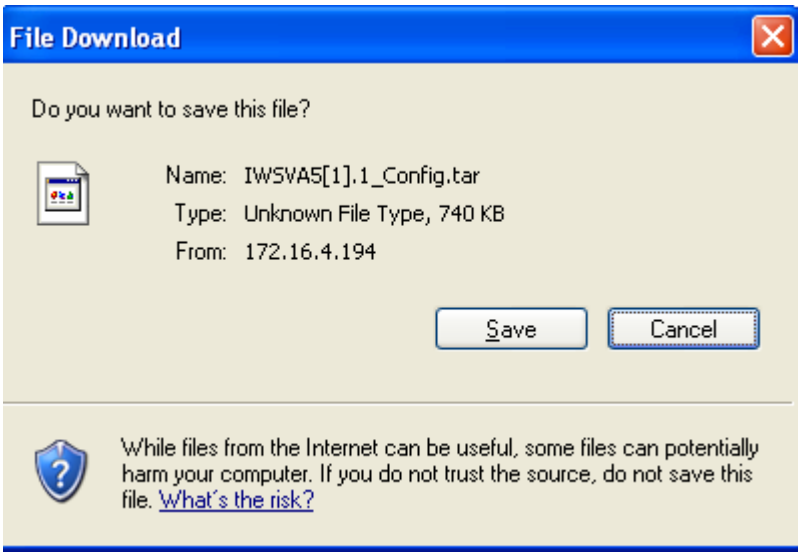


图7-6-5、保存配置

需要恢复配置文件的话，只需要点击图7-6-3里面的“恢复配置文件”项里面的“浏览”，然后选择之前备份的tar包，点击“导入”即可。

4)、账号管理

由于公司的策略关系，需要设置对IWSA EE 控制台的访问权限，并创建不同的账户。如图7-6-6所示，方法如下：

- 点击“管理”菜单；
- 展开“管理控制台”；

- 点击“账户管理”
- 点击“添加”
- 输入用户名、密码和描述
- 选择角色，即访问权限的设定

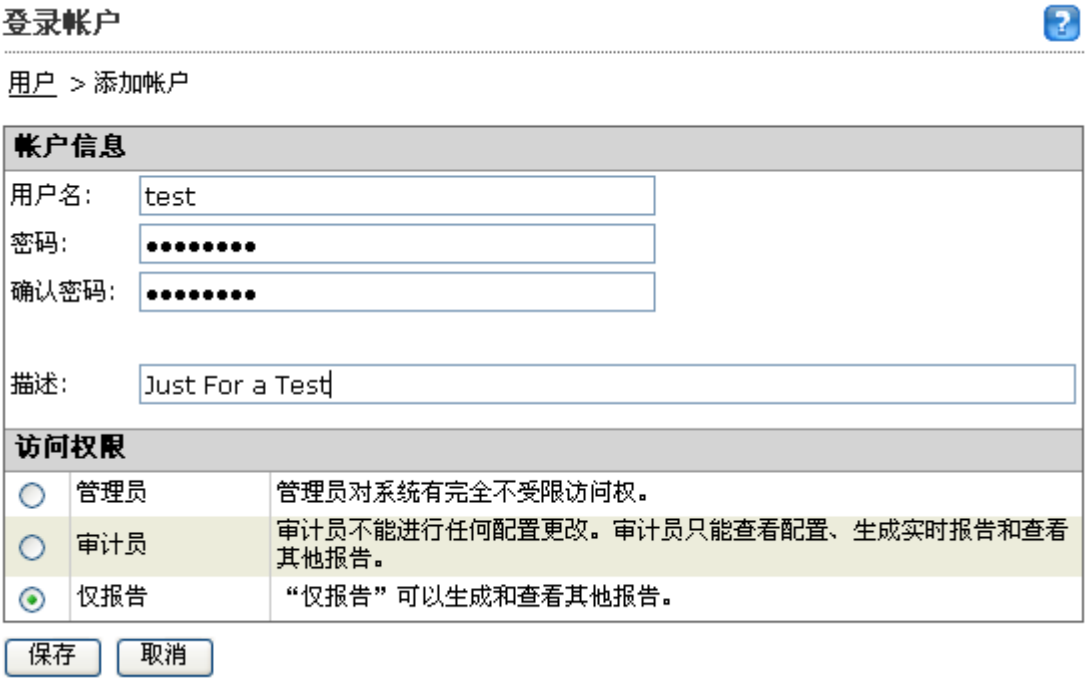


图7-6-6、创建账号

5)、日志/报告的维护

设置日志和报告的维护可以减轻IWSA EE 服务器的压力，并释放相应的空间，使其性能优化，删除过旧的日志和报告，并设置IWSA EE ，让其自动删除。具体操作如下：

- 点击“日志”菜单
- 选择“日志设置”
- 在“报告日志”中去除“记录 HTTP/HTTPS/FTP 访问事件”（除非用户有特别的需求，默认不开启，开启之后IWSA EE 会记录URL的访问记录，从而使日志变得非常庞大。）
- 设置合理的“存储日志的天数”，默认为30天
- 设置完毕后，点击“保存”

如图7-6-7所示。

图7-6-8显示了设置系统日志的方法，默认保留天数是5天，用户可以根据具体情况来增加或减少天数。

图7-6-7、报告日志的设置

图7-6-8、系统日志的设置

报告的保留数目也雷同。如图7-6-9所示，方法如下：

- 点击“报告”菜单

- 选择“配置”
- 在页面中设置各个类型的报表的保留数目

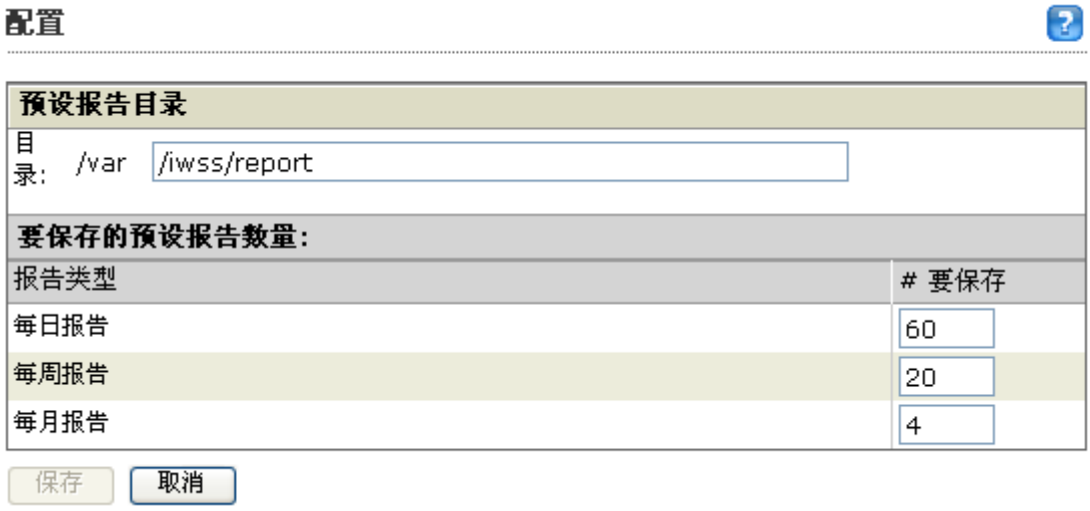


图7-6-9、预设报告的保留数量

7.7 IWSA EE 的Bypass设置

Bypass的目的在于当出现意外的情况下，为了保证网络不断掉，从而让IWSA暂时不处理应用流量。

7.7.1 IWSA的硬件bypass方案

此方案会让IWSA不处理任何流量，让网络流量暂时都通过。登录IWSA的Shell模式，执行如下命令：

查看IWSA是否为bypass状态： bpctl eth1 get_bypass

启用lanbypass： bpctl eth1 set_bypass on

禁用lanbypass： bpctl eth1 set_bypass off

7.7.2 IWSA的系统bypass方案

利用IWSA操作系统内核conntrack进行bypass，即通常所说的rpolicy bypass。应用系统bypass可以让IWSA针对某些IP来进行bypass，而不是完全bypass。

登录到IWSA的Shell模式，执行如下命令：

1、查看当前的策略（简单的策略）

```
# more /proc/conntrack/rpolicy
Redirect Policy Table ****************************************
[0] Redirect -dport 80
[1] Redirect -dport 8080
[2] Redirect -dport 21
```

注意：内核会把目标端口为80,8080（HTTP）和21（FTP）的流量导到上层的程序做扫描。

2、临时bypass部分源或目标IP

基本格式如下：

```
echo "ADD|DEL ftp_port_number" > ftp
echo "ADD [-i phys] [-p tcp|udp] [-sm srcmac] [-dm dstmac] [-v
[v1,v2...|v1-v2]] [-sport [p1,p2...|p1-p2]] [-dport [p1,p2...|[p1-p2]]
[-sip [srcip|iprange]] [-dip [dstip|iprange
]]" > redirect
echo "DEL rule_id" > redirect
```

注意：rpolicy来bypass的话，IWSA会根据规则从编号0开始依次检查，如果哪条规则触发的话，那么下面的规则就不执行。因此请调整您的规则顺序

举例：

不扫描到目的IP 65.45.60.1的流量

```
echo "ADD -dip 65.45.60.1 -action pass" > /proc/conntrack/redirect
```

清除编号为2的规则：

```
echo “DEL 2” > /proc/conntrack/redirect
```

案例：

实例分析：bypass飞信服务器IP地址，动态增加飞信服务器的IP地址到bypass的列表 65.45.60.1/24

先查看rpolicy中端口转发的规则编号(more /proc/conntrack/rpolicy)， 输出如下：

```
Redirect Policy Table ***************************************
[0] Redirect -sip 137.12.8.7-137.12.8.7 -action pass
[1] Redirect -sip 10.11.0.253-10.11.0.253 -action pass
[2] Redirect -dport 80
[3] Redirect -dport 8080
[4] Redirect -dport 21
```

再删除rpolicy中端口转发的规则

```
echo "DEL 4 " > /proc/conntrack/redirect
echo "DEL 3 " > /proc/conntrack/redirect
echo "DEL 2 " > /proc/conntrack/redirect
```

再添加bypass某些目的IP的规则

```
# echo "ADD -dip 65.45.60.1/24 -action pass" > /proc/conntrack/redirect
```

然后再添加端口转发规则

```
# echo "ADD -dport 80 " > /proc/conntrack/redirect
# echo "ADD -dport 8080 " > /proc/conntrack/redirect
# echo "ADD -dport 21 " > /proc/conntrack/redirect
```

再确认规则是否成功添加(more /proc/conntrack/rpolicy)， 输出如下

```
Redirect Policy Table ***************************************
[0] Redirect -sip 137.12.8.7-137.12.8.7 -action pass
[1] Redirect -sip 10.11.0.253-10.11.0.253 -action pass
[2] Redirect -dip 65.45.60.1-65.45.60.255 -action pass
[3] Redirect -dport 80
[4] Redirect -dport 8080
[5] Redirect -dport 21
```

3、永久bypass部分源或目标IP

修改/etc/iscan/network.ini

Bypass目标IP，在network.ini中添加或修改如下项:

bypass_dstIP=65.45.60.1/23;210.68.95.10;220.13.85.20;

使用分号分隔多个IP或IP段

Bypass源IP，在network.ini中添加如下项：

bypass_srcIP=192.168.0.1/24;10.64.44.210;

使用分号分隔多个IP或IP段

重启网络服务让修改生效（ service network restart ）

8. FAQ

8.1 IWSA EE 5.1是否支持TrendMicro Control Management（TMCM）5.0?

答：兼容TMCM5.0和5.5。由于TMCM3.5已经停止技术支持，因此建议升级到5.0或者5.5。

8.2 LDAP认证是否支持IWSA EE 5.1的桥模式？

答：IWSA EE 5.1的透明桥模式已经支持LDAP的认证。

8.3 IWSA EE 5.1支持把日志传送到别的服务器上否？

答：IWSA EE 5.1可以把日志存储到其他的Syslog服务器上，需要在控制台的界面中进行设置，具体可以参考管理员手册。

8.4 IWSA EE 5.1的反向代理模式支持HTTPS的扫描吗？

答：目前IWSA EE 5.1的版本反向代理的部署模式不支持HTTPs的扫描，因此需要在服务器上安装客户端防毒软件。

9. 厂商联系方式

- 800 免费售后热线

800-820-8839

- 售后电子邮件地址

service@trendmicro.com.cn

- 趋势科技中文网站

http://www.trendmicro.com.cn

- 病毒查询

http://www.trendmicro.com/vinfo/zh-cn/

- 中文版资料及软件下载

http://support.trendmicro.com.cn

- 趋势科技英文产品下载网站

http://www.trendmicro.com/download

- 试用版序列号申请：

http://www.trendmicro.com.cn/corporate/techsupport/online_registration/cd.asp

- 趋势科技病毒递交信箱

virus_doctor@trendmicro.com.cn