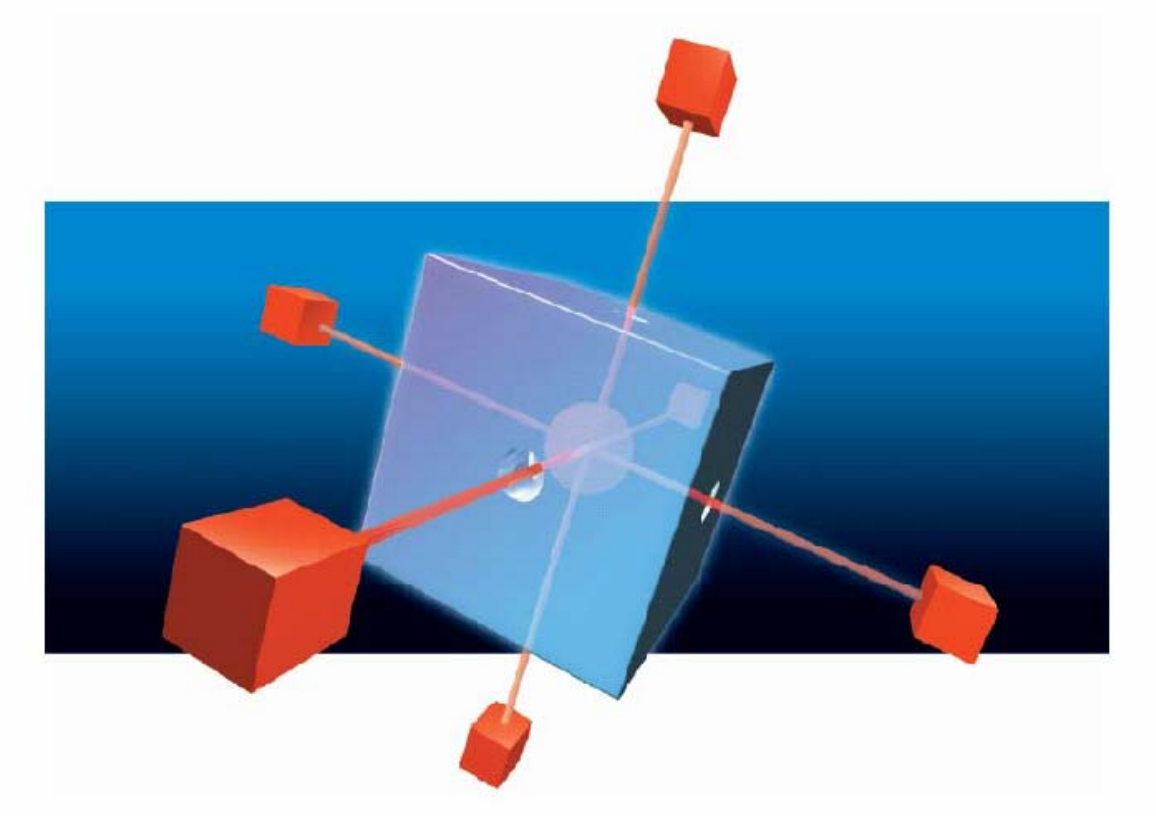
趋势科技

产品安装标准程序

Internet Web Security Application 2500



TREND MICRO™

趋势科技

2006-4-10

目录

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。

趋势科技防毒墙—Web 安全硬件版(简称 IWSA)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 216Mbps 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。

主要功能：

- 集成多种防护功能于一身，极高的性价比
- 灵活的部署方式，减少客户部署的难度
- 与损害清除服务器互动，将间谍软件赶尽杀绝
- 优化的内核，提供更高的稳定性及性能

1. 认识 IWSA

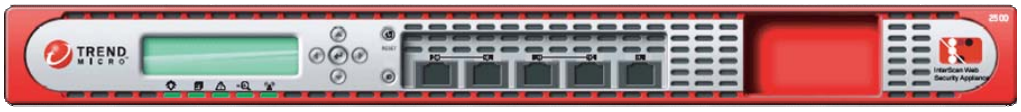
1.1 IWSA 硬件规格

IWSA 产品包装

第一次打开 IWSA 包装时，IWSA 的产品包装盒内带有以下组件：

- IWSA 硬件
- 一根直连线、一根交叉线和一个电源线
- 一个使用手册
- 序列号清单
- 安全架卡
- 包含核心镜像文件管理员手册的 CD

IWSA 硬件规格

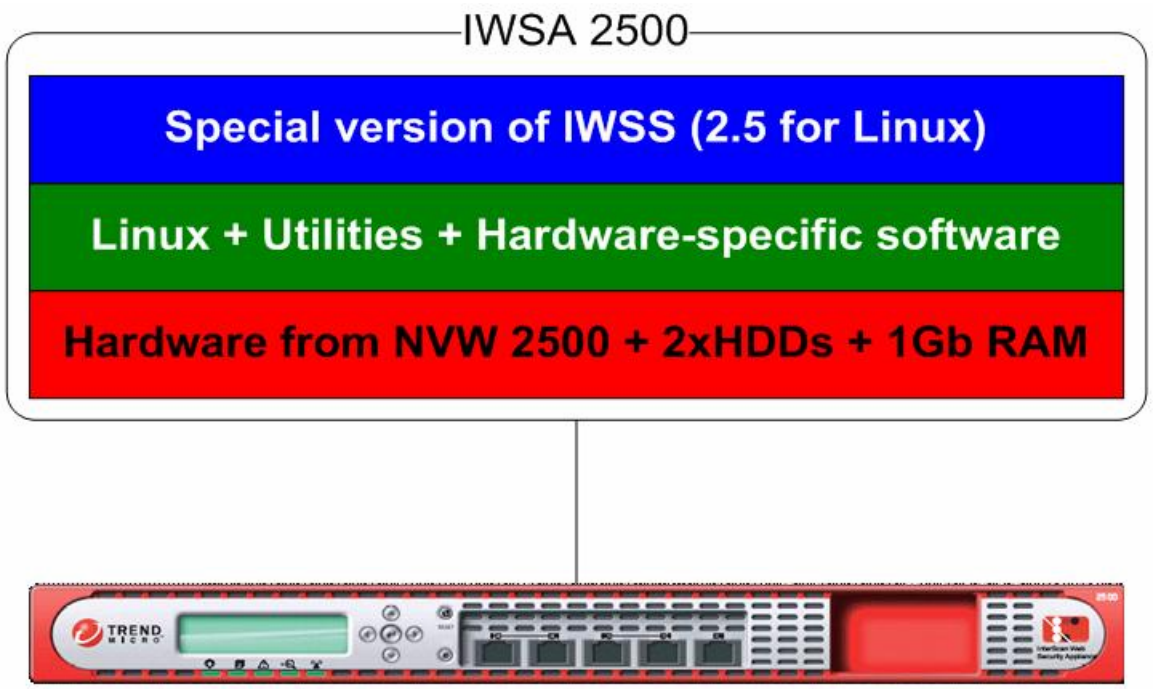


- 1 U 机架
- CPU = 2 CPU Xeon 2.8 Ghz
- DOM = 256 MB -- 磁盘存储器
- RAM = 2 Gbytes
- Hard disks = 2 x 40 Gbytes STA. Raid 0. Software mirror. Disk space = 40 Gbytes
- 界面:
    - 2 x 10/100/1000 接口(端口 1 and 端口 2)
    - 端口 5 用来升级应用操作系统
    - 端口 3 & 4 没有使用

- 无光纤接口

- 单一电源
- 系统风扇（双发动机）x 5，不能进行调整

1.2 IWSA 的组成



由上图可以看到，IWSA 有以下几个部分组成：

- IWSS 2.5 for Linux（特殊版本）；
- 内核：精简版本的 Linux；
- NVW 升级版硬件（2 个硬盘+1G 内存）

2. IWSA 的部署计划

IWSA 拥有 3 种部署方式，可满足不同用户环境的需求。

IWSA 的三种部署模式分别是：

- 与 Proxy 联动；
- 透明桥模式；
- 与 ICAP 联动模式。

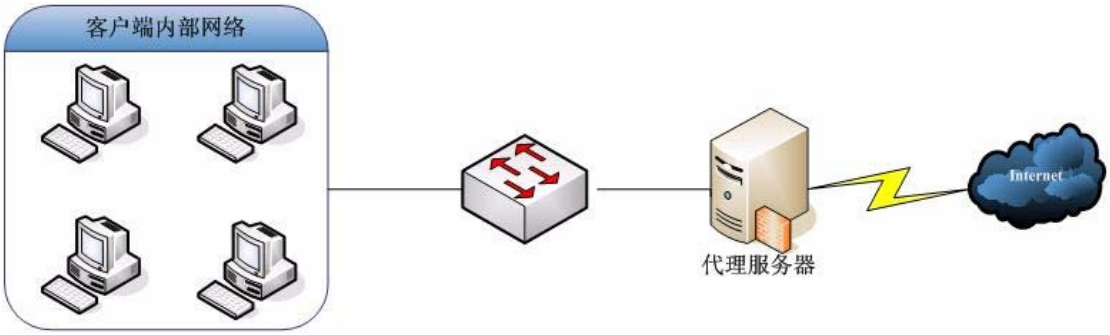
因此，必须首先了解清楚客户的具体环境需求

2.1 与 proxy 联动模式

2.1.1 目标客户群：

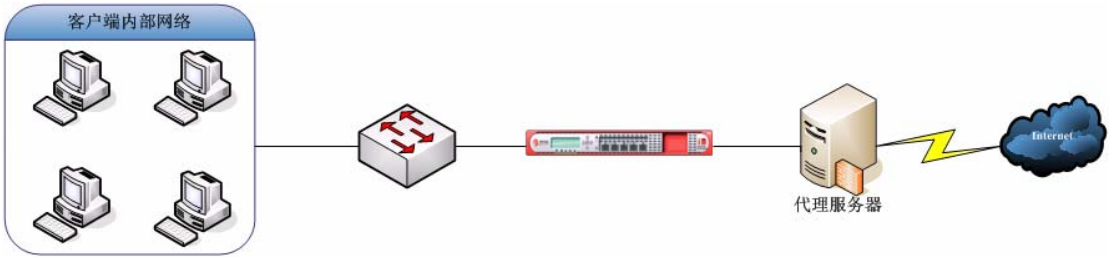
- 客户拥有代理服务器（如 ISA、Proxy2.0 等）
- 客户目前有间谍软件、钓鱼的困扰
- 客户环境中大部分人通过 Web 方式收取邮件

客户环境：

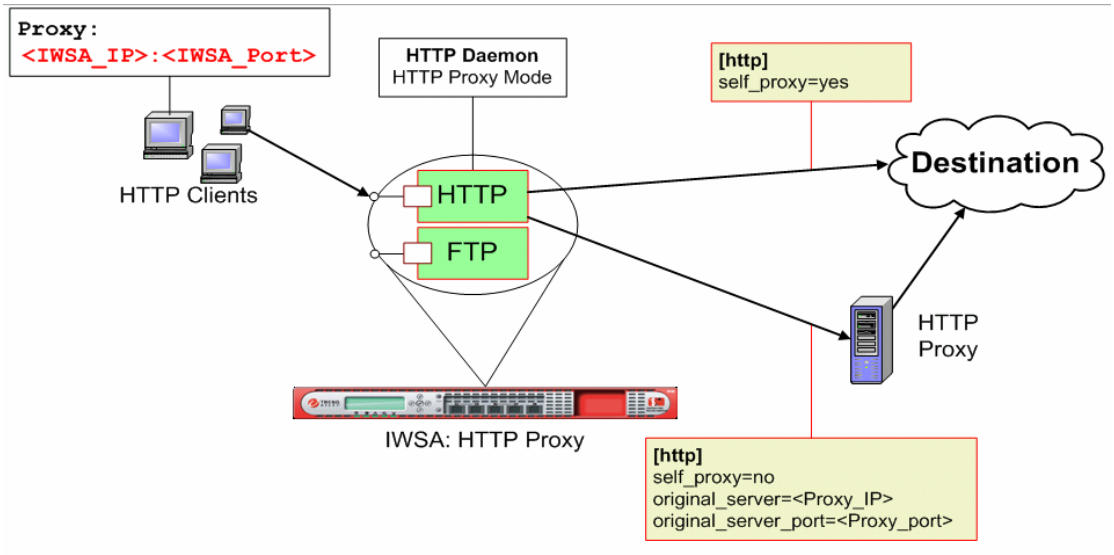


2.1.2 IWSA 部署方式

- IWSA 部署结构图：



端口扫描原理：



- 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。

2.1.3 优势所在：

- 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；

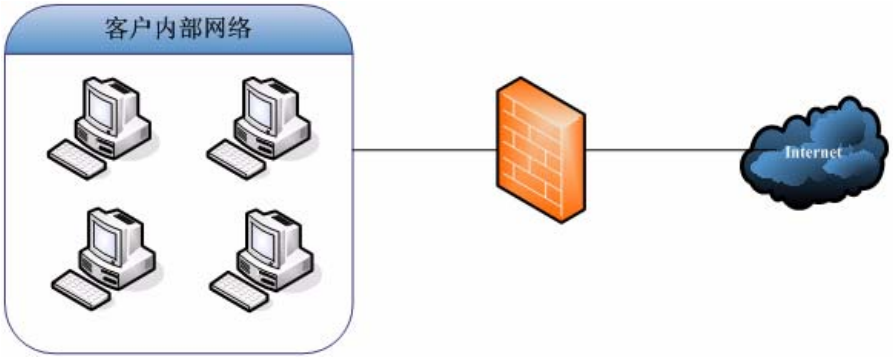
- 注意事项：管理员需要更改所有客户机的代理设置。

2.2 透明桥模式

2.2.1 目标客户群：

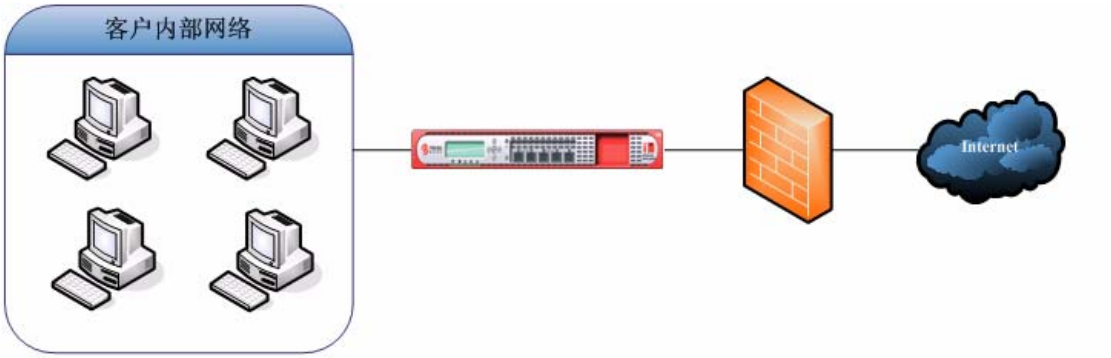
- 客户为透明网关上网方式，没有代理、ICAP
- 客户目前有间谍软件、钓鱼的困扰
- 客户环境中大部分人通过 Web 方式收取邮件
- 客户希望厂家能够提供 Web 安全网关解决方案
- 因为客户端数量众多，客户不希望因为 Web 安全网关更改客户端代理设置

客户场景：

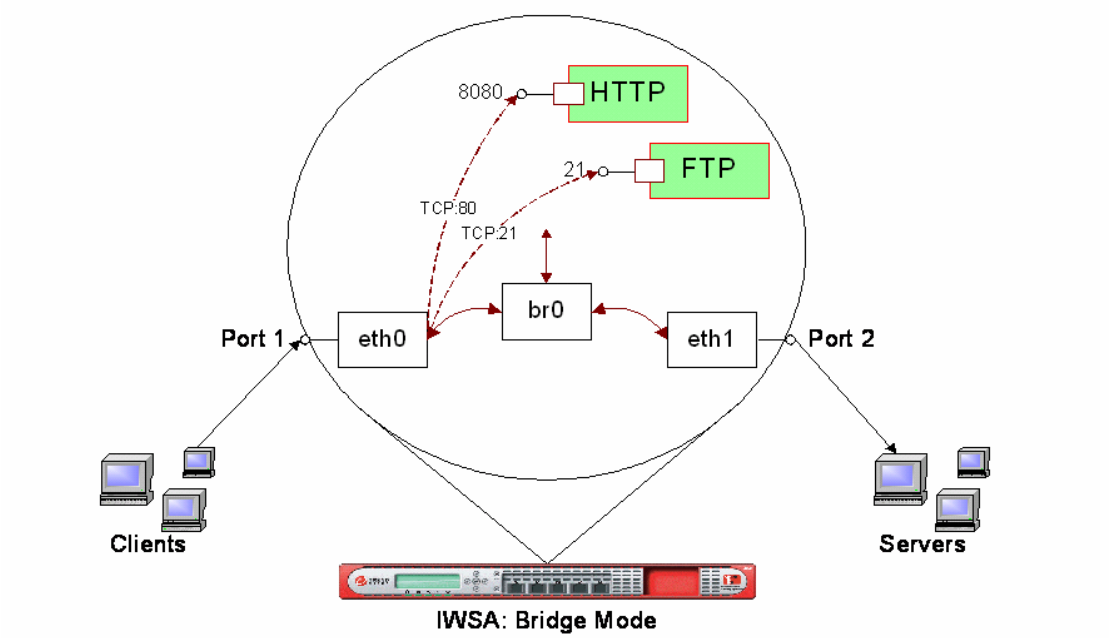


2.2.2 IWSA 部署结构图：

透明桥模式：



端口工作原理：



- 部署方式：把 IWSA 部署在客户端与 Web 服务器之间（如果需要保护企业 Internet 访问安全，则直接放在企业的 Internet 出口处），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。

2.2.3 优势所在：

- 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；

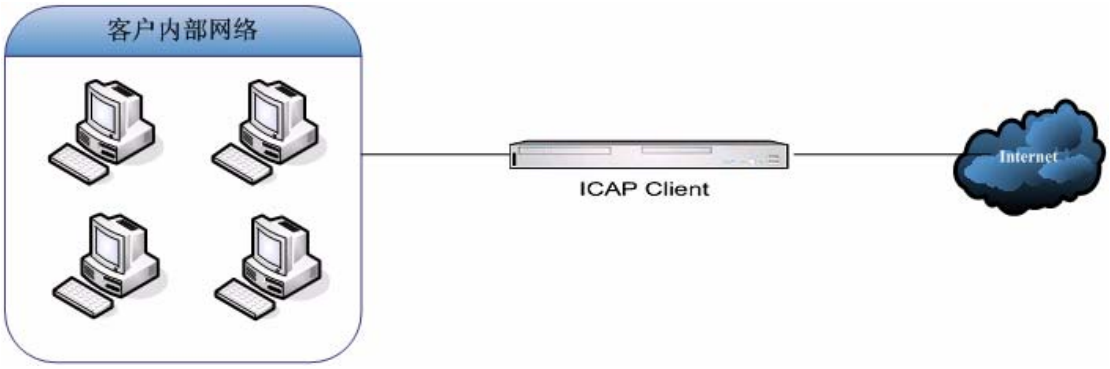
- 需要注意的地方：
  - 只能够检查 80（HTTP）及 21（FTP）两个端口，其它端口无法检测；

2.3 与 ICAP 联动

2.3.1 目标客户群：

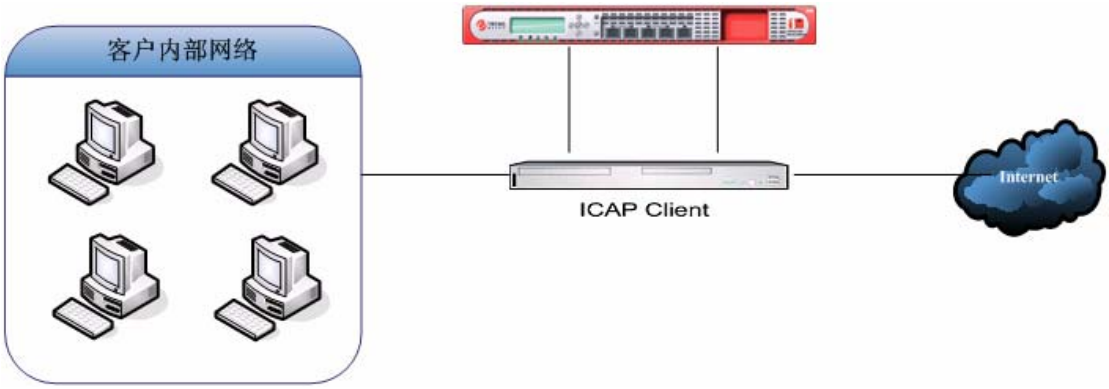
- 客户拥有自身的缓存服务器（如 NetApp、Blue coat 等）
- 客户目前有间谍软件、钓鱼的困扰
- 客户环境中大部分人通过 Web 方式收取邮件
- 客户希望厂家能够提供与 Catch 服务器联动的 Web 安全网关解决方案

客户场景：



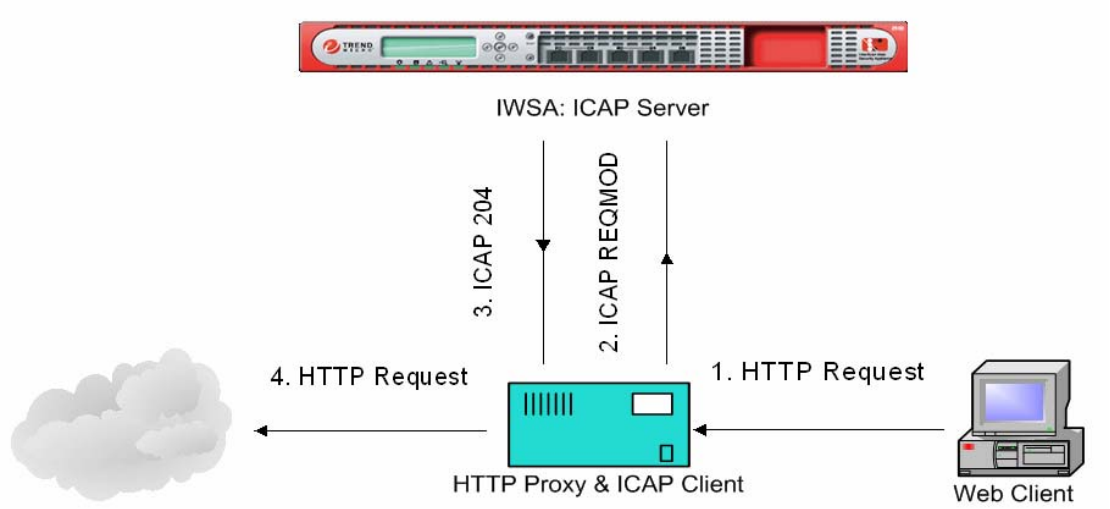
2.3.2 IWSA 部署结构图：

ICAP 联动模式：

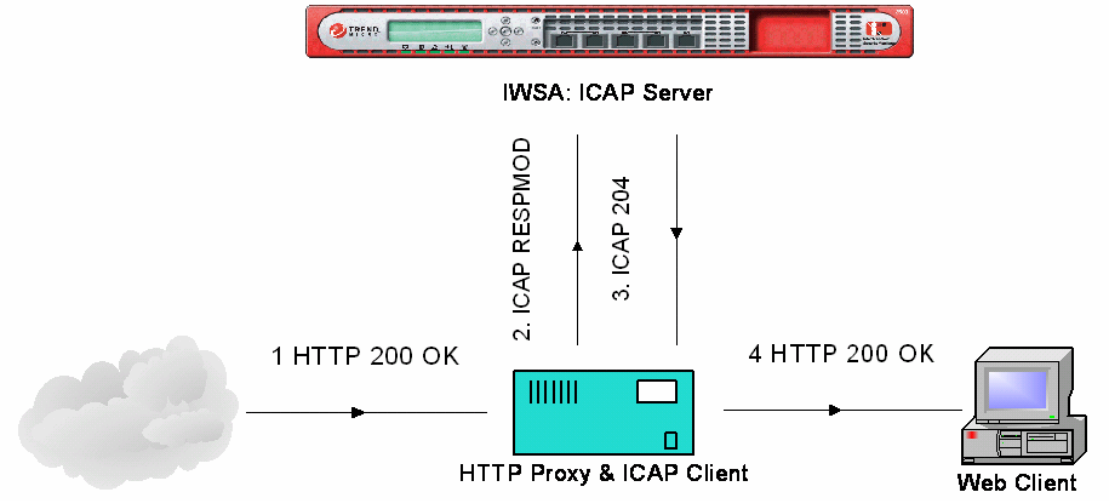


端口扫描原理：

- Request Modification Mode：客户端访问 Internet 或上传文件时，向 ICAP 提出 Request 请求，通过 IWSA 进行扫描后发送至 Internet，起到对上传文件扫描及 URL 过滤的功能；



- Response Modification Mode：客户端下载文件时进行内容安全检察；



2.3.3 优势所在：

- 通过 ICAP 的缓存功能，提供更高的 Web 安全处理性能；
- 对客户透明，客户机无需作任何改动（如果客户原来部署了 ICAP）；

- 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；

需要注意的地方：需要额外的硬件设备（ICAP 服务器）。

2.4 需要注意的地方

在进行 IWSA 部署的时候，需要对客户环境进行深入的分析，包括：

- 上网用户数量。紧记不能超过指定的 5000U，而且还要根据用户行为特征及部署方式作调整；
- 用户上网行为特征。如果大部分用户的上网行为不受管控（如学生宿舍区等），单台 IWSA 所能承受的用户数量需要特殊考虑；
- 以网桥模式部署 IWSA 的情况下，IWSA 部署的位置应该尽远离客户端，减少企业内部应用因经过 IWSA 而发生的影响；
- 请对客户环境有关 HTTP、FTP 的应用作调查，在部署或测试过程中可以检查这些应用会不会被 IWSA 所影响；

  建议在部署 IWSA 之前，首先对客户环境进行调研，研究一下客户的上网应用是否存在一些特殊的应用，以免在部署后遇到一些意外的情况。

  下面是针对客户环境的调研表：

客户环境调查问卷
--IWSA 部署

1、IWSA 在客户环境中以什么方式部署？

☐ 网桥模式；

☐ Proxy 模式；

☐ ICAP 模式；

2、客户环境是否使用 80 端口（如果是 Proxy 模式，则需要查看 IWSA 侦听端口，如 8080）的即时通讯软件应用？如果有，请给出相关应用：_____

☐ QQ ☐ MSN ☐ ICQ ☐ Yahoo Message

如果还有其他 IM 应用，请列出：_____

3、客户环境是否使用基于 80 端口的下载应用软件？如果有，请给出相关应用：_____（如 SUS、防病毒更新、数据同步软件等）

4、客户是否拥有面向内部员工的 Web 应用？如果有，请把该 Web 应用的连接地址列出来，如果应用包含控件下载，请注明。

如：Http://OA_ip

_____

_____

_____

5、客户是否需要访问合作伙伴的Web网站，或是经常访问其他第三方的Web网站，请把这些网站列出来。如果这些网站需要下载控件，请注明。如：Http://www.microsoft.com。

_____

_____

_____

3. IWSA 的安装步骤

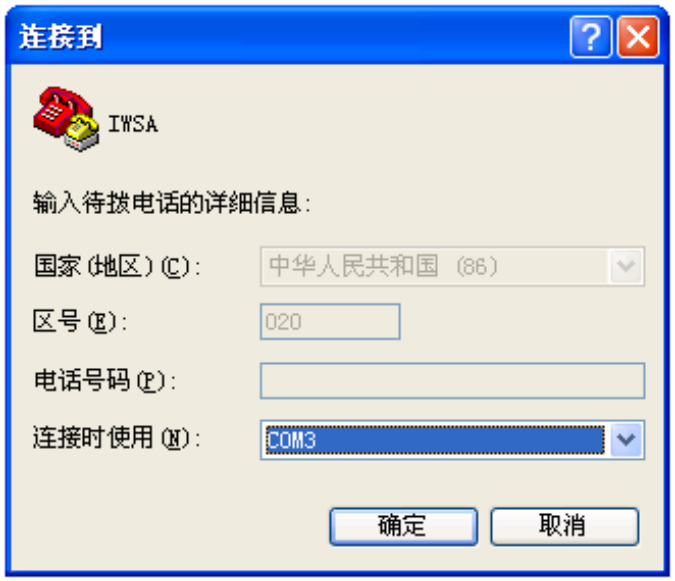
IWSA 的部署可以按照以下几个步骤进行：

1. 按照上一章所述：计划 IWSA 的部署(分析客户环境，决定 IWSA 以哪种方式部署)；
2. 按照部署计划所设计的工作模式，把 IWSA 接入网络；
3. 通过超级终端连接 IWSA，对 IWSA 进行初始的配置；
4. 通过 Web 控制台，对 IWSA 进行配置。

3.1 通过超级终端对 IWSA 进行初始配置

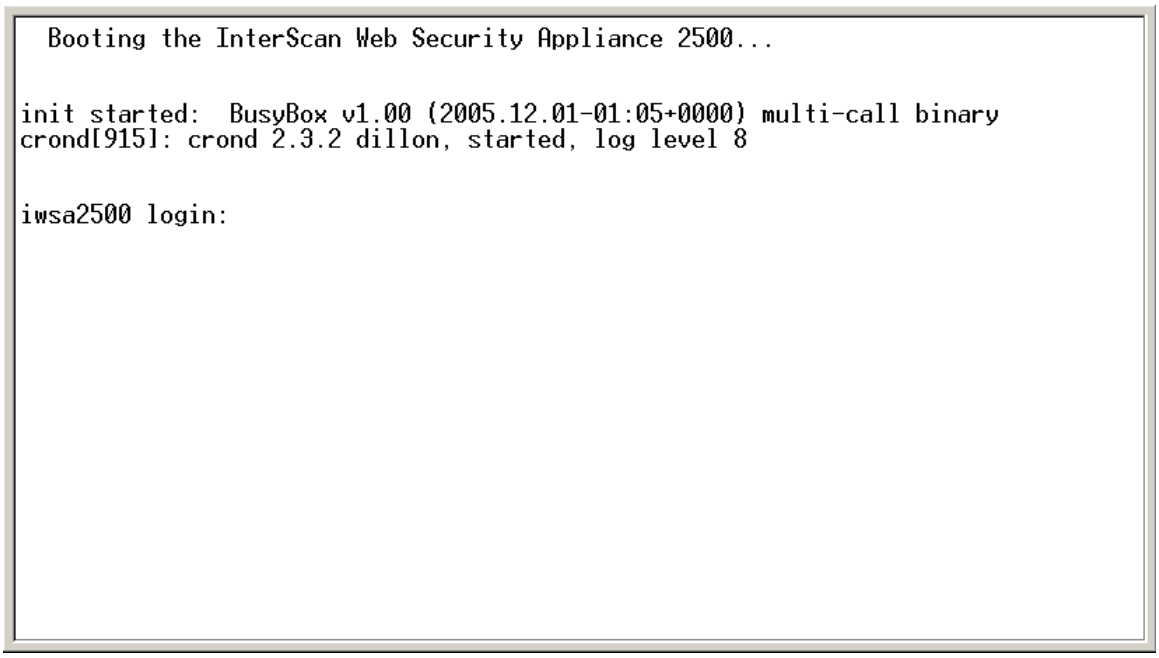
- 使用串口线将 IWSA 和配置机器的串口相连。
- 在配置机器上打开超级终端。
  1. 开始菜单→程序→附件→通讯→超级终端；
  2. 新建一个连接：任意给一个名字，如 IWSA，点击“确定”

- 连接时使用“COM1”

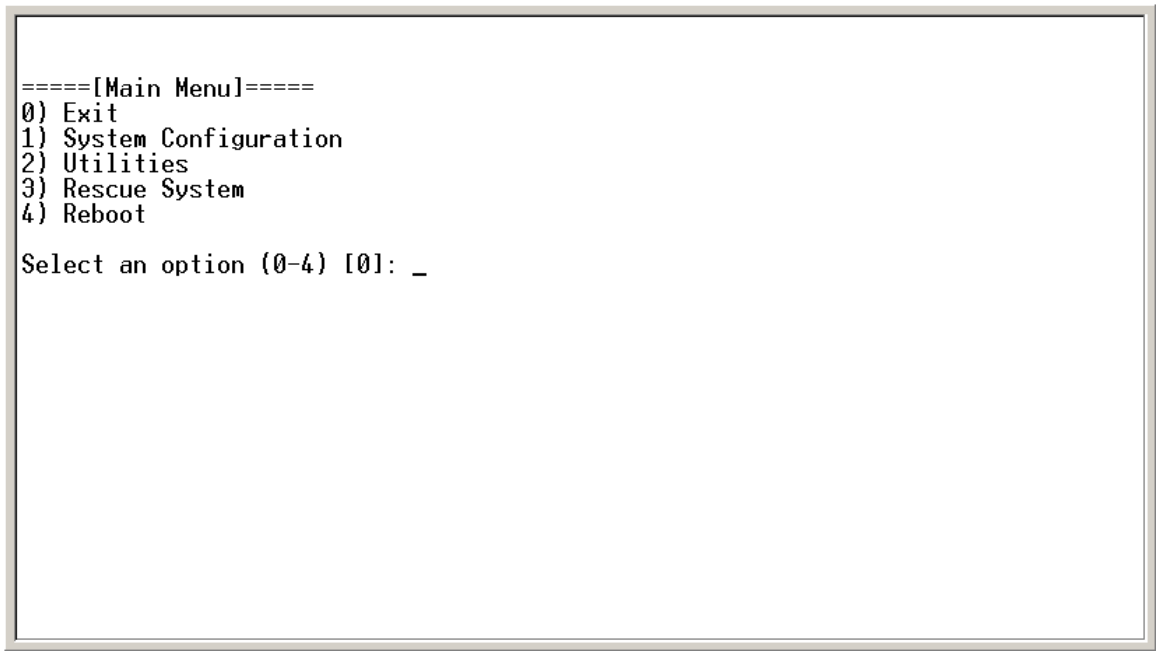


■ 在 COM 属性中设置比特率为“115200”，其他默认

启动 IWSA，就可以看到如下界面：



- 按<Enter>，弹出输入用户名与密码的页面。默认帐号与密码是：
  - 用户名：root
  - 密码：iwsa
- 输入确认后，进入 IWSA 的主菜单；



- 输入 1，进入系统配置子菜单；

```
=====[System Configuration Menu]=====
0) Back To Top
1) Change Management Port
2) Configure Device Settings
3) Configure Control Manager
4) Configure SNMP
5) Set Network Ports
6) Set Administrative UI Password
7) Set "root" Password
8) Set "remoteadmin" Password

Select an option (0-8) [0]: _
```

■ 输入 2，进入设备配置的子菜单，设定 IWSA 网络配置，

```
=====[Device Settings]=====
Device Settings Summary
    Host name: iwsa2500

Network Settings
    IP setting: Static
    IP address: 10.28.135.221
    Netmask: 255.255.255.0
    Default gateway: 10.28.135.1
    Primary DNS server: 10.28.128.8
    Secondary DNS server: 10.28.144.54
    WINS server: 10.28.128.8

0) Back To Top
1) Change Device Host Name
2) Change Device Network Settings
3) Change Route Settings

Select an option: (0-3) [0]: _
```

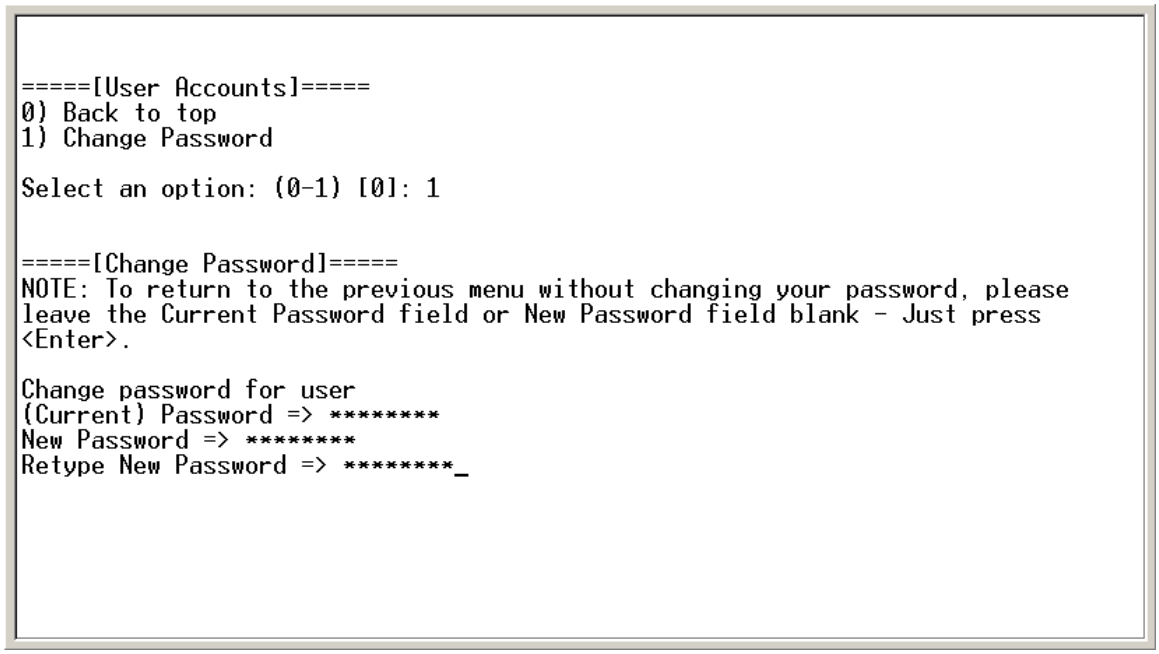
■ 输入 2，设定 IWSA 的管理 IP；设定 IWSA 的 IP 是通过 Web 管理 IWSA 的最低设定要求，只要你设定了 IWSA 的 IP 地址，你就可以通过浏览器对 IWSA 进行几乎所有的配置。

```
Network Settings
    IP setting: Static
    IP address: 10.28.135.221
    Netmask: 255.255.255.0
    Default gateway: 10.28.135.1
    Primary DNS server: 10.28.128.8
    Secondary DNS server: 10.28.144.54
    WINS server: 10.28.128.8

0) Back To Top
1) Change Device Host Name
2) Change Device Network Settings
3) Change Route Settings

Select an option: (0-3) [0]: 2


=====[Change Device Network Settings]=====
Static IP address => 10.28.135.221
Netmask => 255.255.255.0
Default gateway => 10.28.135.1
Primary DNS Server => 10.28.128.8
Secondary DNS Server => 10.28.144.54
WINS Server => 10.28.128.8_
```

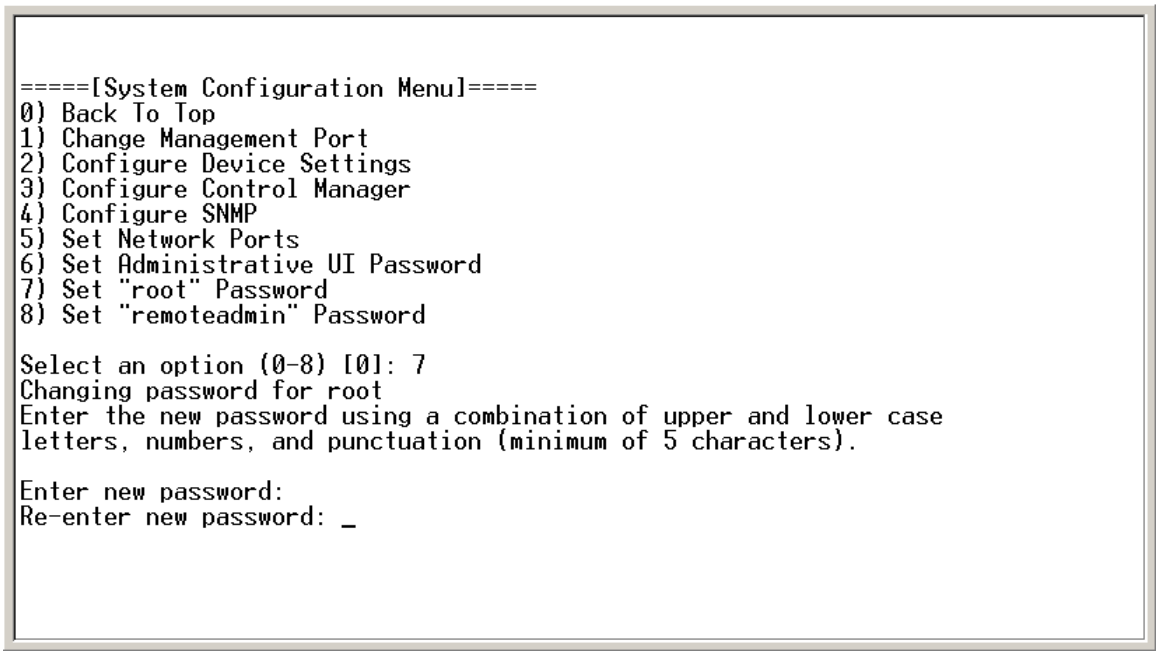
- 输入 0 进入上级菜单，在输入 3 进入设置 Control Manager 的菜单（可选），按照提示输入 TMCM 的 IP 信息与管理帐号；

```


=====[Control Manager Settings]=====
    IP or host name:
    Root account:
    CM Server listening port: 80
    E2E public key: Obtain from CM server
    NAT IP:
    CM registration status: Unregistered

0) Back To Top
1) Change Control Manager Server Settings

Select an option: (0-1) [0]: _
```

- 设置 Web 控制台密码，以便通过浏览器管理 IWSA；在 System Configuration 的 Set Administrative UI Password，输入 1 进入密码设置窗口：

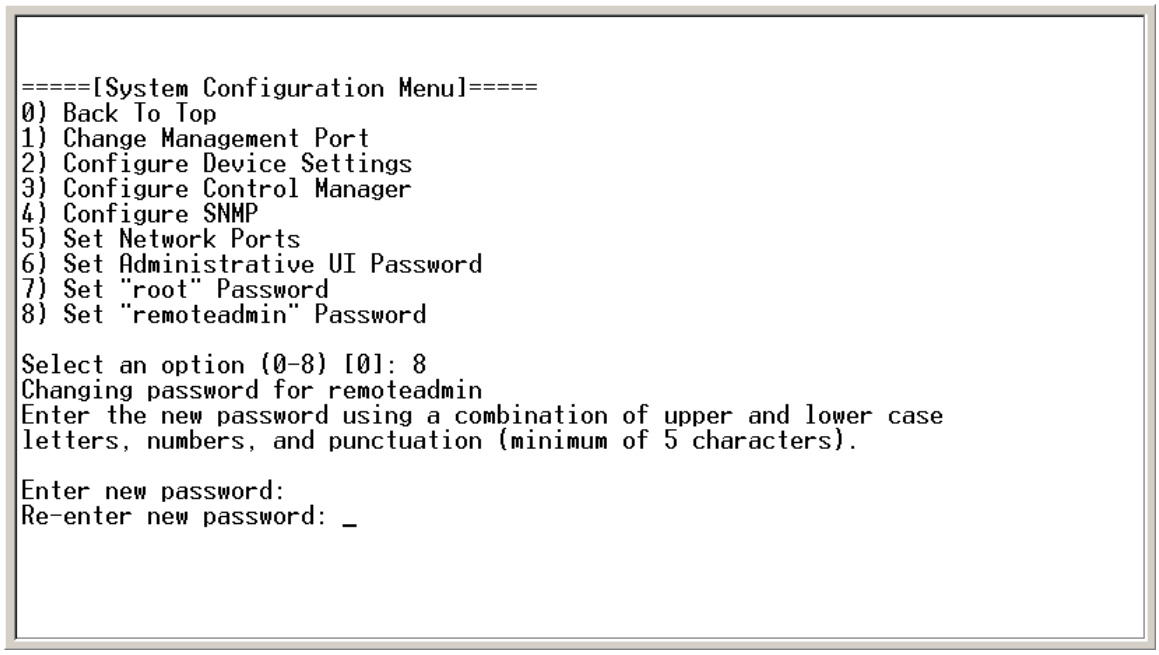


- 设置 root 管理员账号密码。在 System Configuration 的 Set root Password，输入 1，进入密码设定窗口：

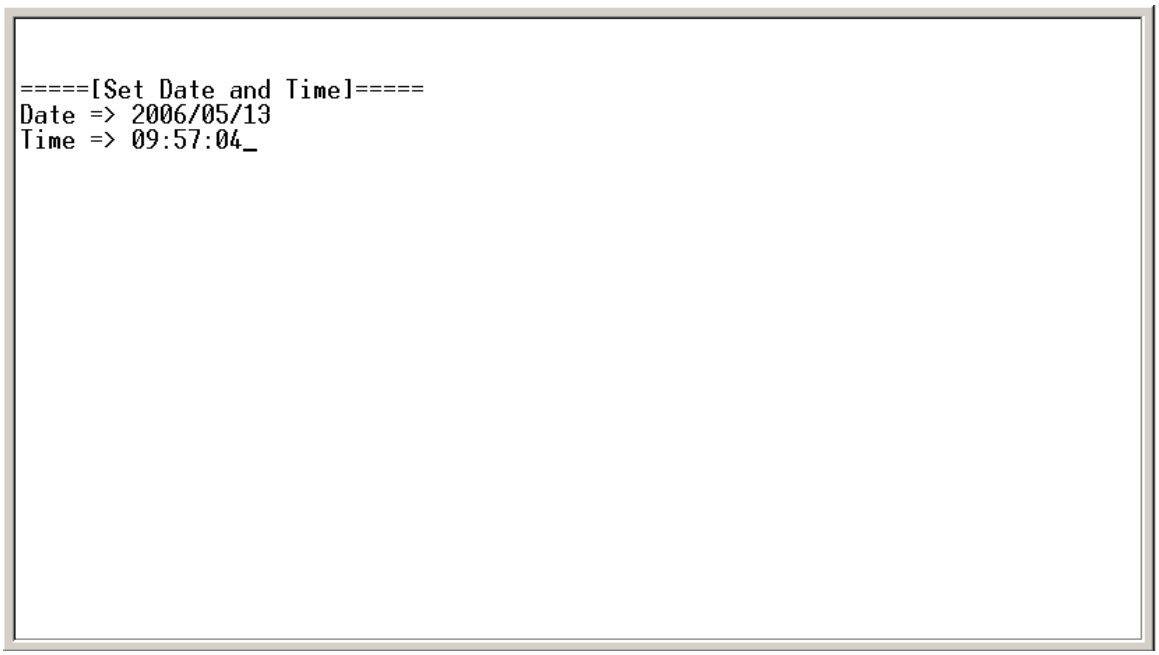


- 设置“remote admin”密码。如果管理员通过 SSH 方式登录 IWSA 进行管理，必须在这里设定“remote admin”的密码才能开通（默认不打开）。在 System Configuration 的 Set “remote admin” Password 修改该密码。修改后通过 SSH 登录，会有如下窗口出现（请注意，通过远程登录还需要输入 root 的密码

才能进行管理）：



- 设置 IWSA 时区。默认情况下，IWSA 的时区是美国时区，因此会出现时区不符的情况。在 System Utilities 的 Set Time Zone 选择正确的时区；
- 设置 IWSA 时间。如果 IWSA 系统时间有误，将会直接导致所检测的所有事件时间有误。原因是所有的日志均已 IWSA 的系统日志为参考。在 System Utilities 的 Set Date and Time 中设置正确的时间：



3.2 通过 Web 登录 IWSA

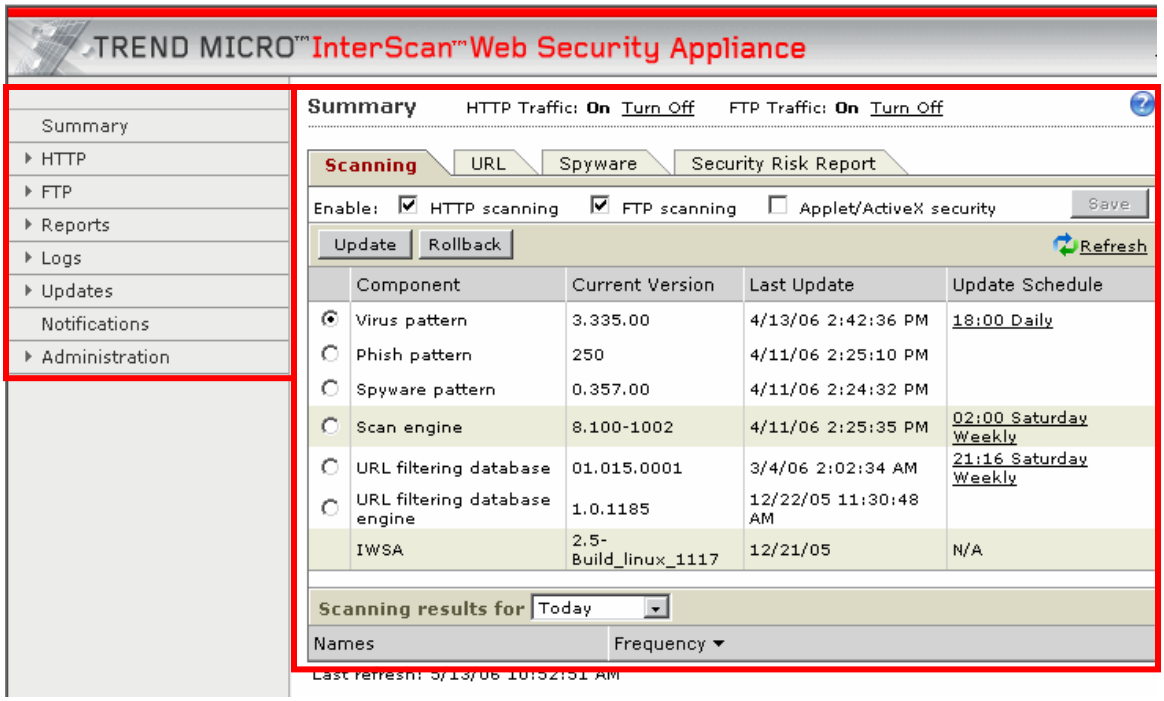
通过上面的基本配置，大家就可以通过浏览器访问 IWSA 并进行配置了。

管理员可以通过两种方式登录 IWSA 的 Web 控制台进行管理，分别是：

- HTTP方式：Http://IWSA_IP:1812;
- HTTPS方式：Https://IWSA_IP:8443;

注:IWSA_IP 是我们上一章设定的 IWSA 管理 IP,密码是我们设定的 Web 管理密码(默认是 adminIWSS85)

- IWSA 管理页面。IWSA 的管理页面由两部分构成。左方的导航菜单，涵盖了所有 IWSA 的功能配置；右方是每个子菜单具体的配置信息页面。



3.3 设置 IWSA 工作模式

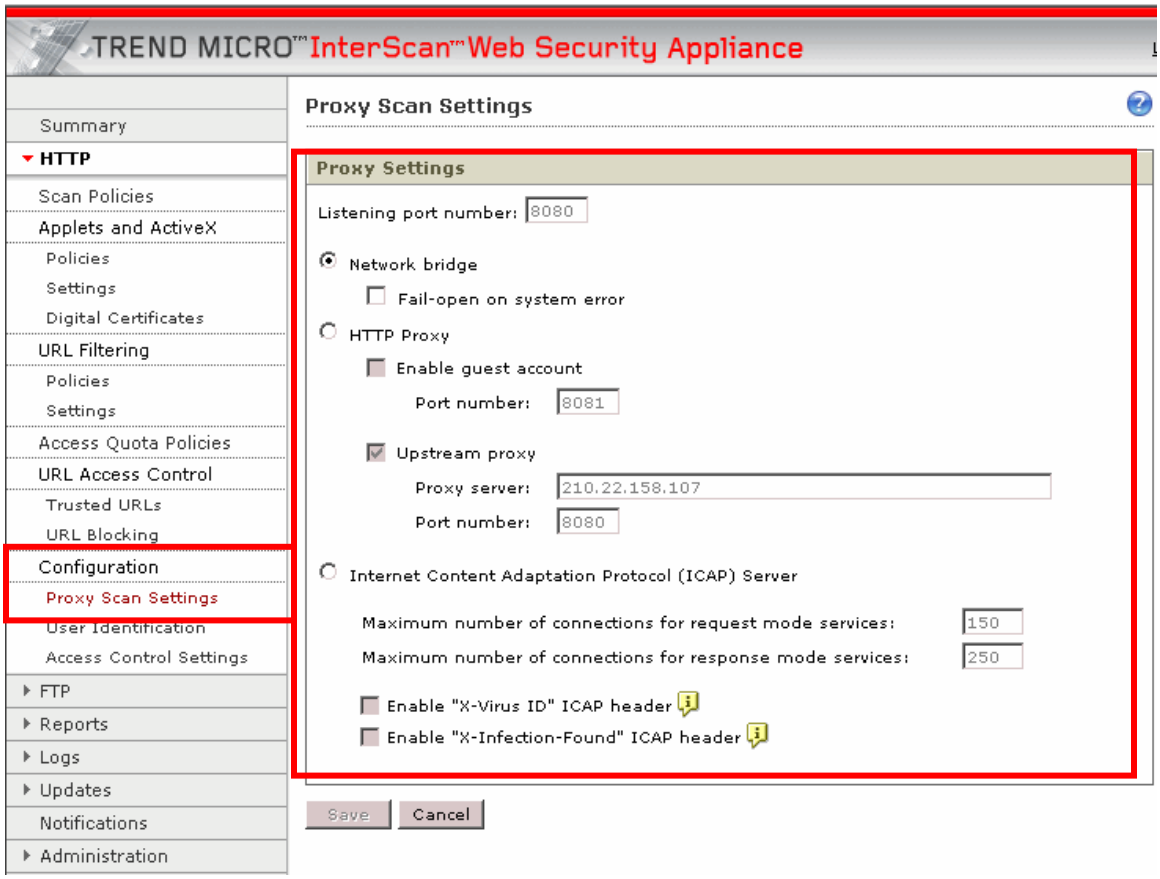
从上面的讨论可以知道，管理员只需在初始配置时设定 IWSA 的管理 IP，即可通过浏览器配置 IWSA：

➢ **设置 IWSA 的工作模式**

在第二章我们讨论过 IWSA 可以按照三种方式来部署，分别是：

- 网桥模式；
- Proxy 联动模式；
- ICAP 联动模式；

那在决定 IWSA 的工作模式后，我们就可以在 Configuration→Proxy Scan Setting 菜单进行设定：



- 如果需要工作在桥模式：
  - ✓ 点选 Network bridge 选项。此时，需要使用 IWSA 两个端口，端口 1 为

内网端口（被保护网络），端口 2 为外网口。

- ✓ HTTP 只监听 80 端口，FTP 只监听 21 端口。
- ✓ 点选 Fail Open on System error 后，当 IWSA 系统出现故障，自动切换至 Fail Open 状态。

■ 如果需要工作在 Proxy 模式

- ✓ 点选 HTTP Proxy 单选框。
- ✓ 如果以 Stand along 的模式运行，请设定侦听端口，默认为 8080；
- ✓ 如果需要与其他代理服务器联动，请设定 upstream proxy 的 IP 地址及代理端口；
- ✓ 如果还需要针对一些特殊用户进行处理，可以设定 Enable Guest Account，并设定监听端口，默认为 8081。
- ✓ 此时，IWSA 使用端口 1 作为侦听客户数据的端口。

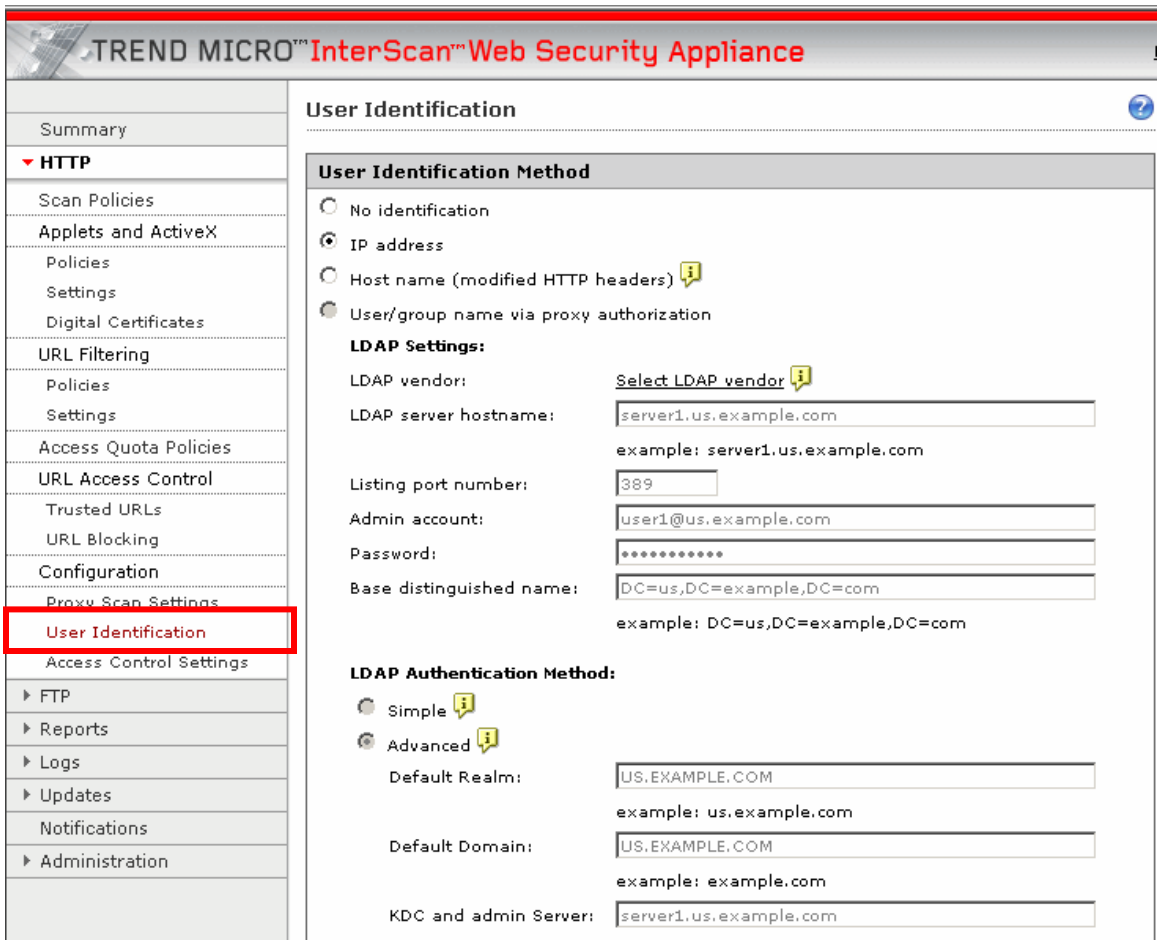
■ 如果需要工作在 ICAP 联动模式

- ✓ 如果需要，设定 Request mode 和 Response mode 服务的连接限制，默认是：250 150；

注：所有配置后必须电击下方的 Save 按钮才能保存策略。

➢ 配置 User Identification

用户可以通过这个功能设定 IWSA 是如何辨认一个“用户”，这个设置是有助于 IWSA 如何去强制用户执行安全策略，如：URL filtering 和 access Quota。



默认情况下，IWSA 是使用 IP 地址识别用户的。对于使用静态 IP 及 IP 管理比较严格的环境，这种方式会比较适合。如果是其他的情况，可以使用不同的选项来满足。

配置方法：

1、决定使用哪种机制识别用户；

2、点击 **HTTP** > **Configuration** > **User Identification**.

3、选择相应的识别方式并保存。

4. IWSA 基本配置

4.1 全局配置

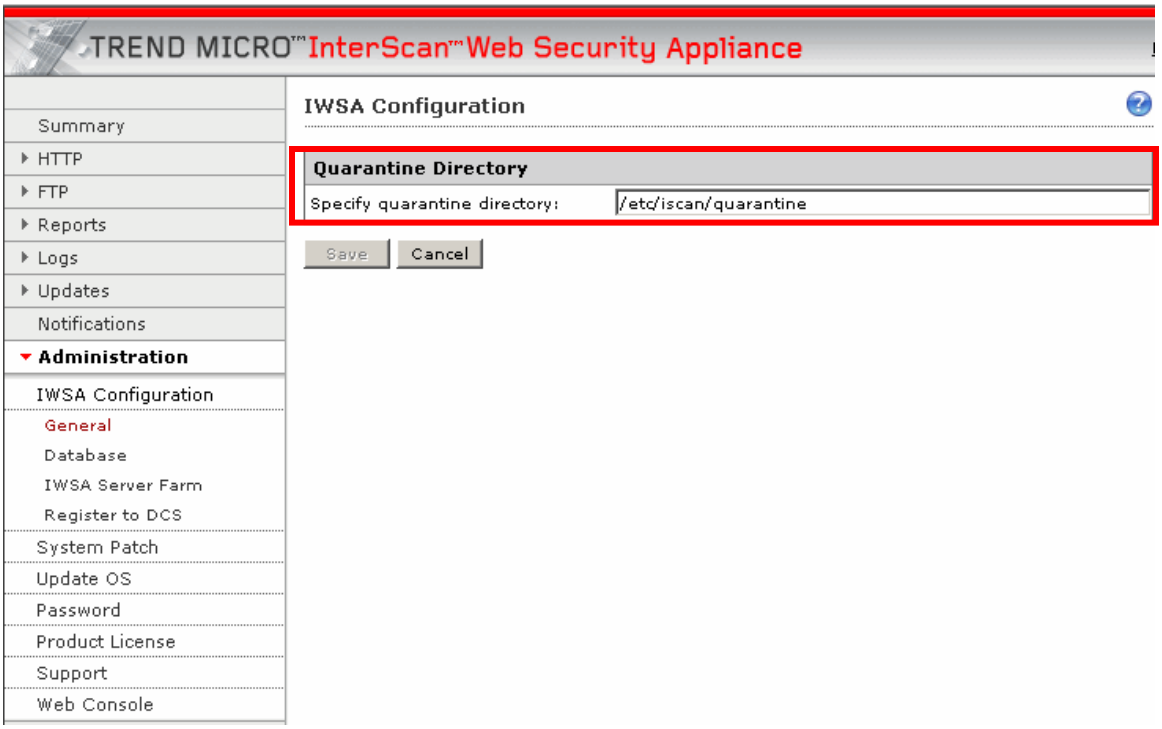
IWSA 有 3 个全局参数需要配置，分别是：

- 隔离目录；
- 注册 DCS 服务器；
- 产品激活码；

配置 IWSA 隔离目录

IWSA 隔离目录存放所有被 IWSA 隔离的文件，管理员可以通过 Web 控制台设定该路径，方便查找。但是 Web 控制台不提供隔离文件的访问手段，管理员必须通过超级终端或 SSH 等方式处理被隔离文件。

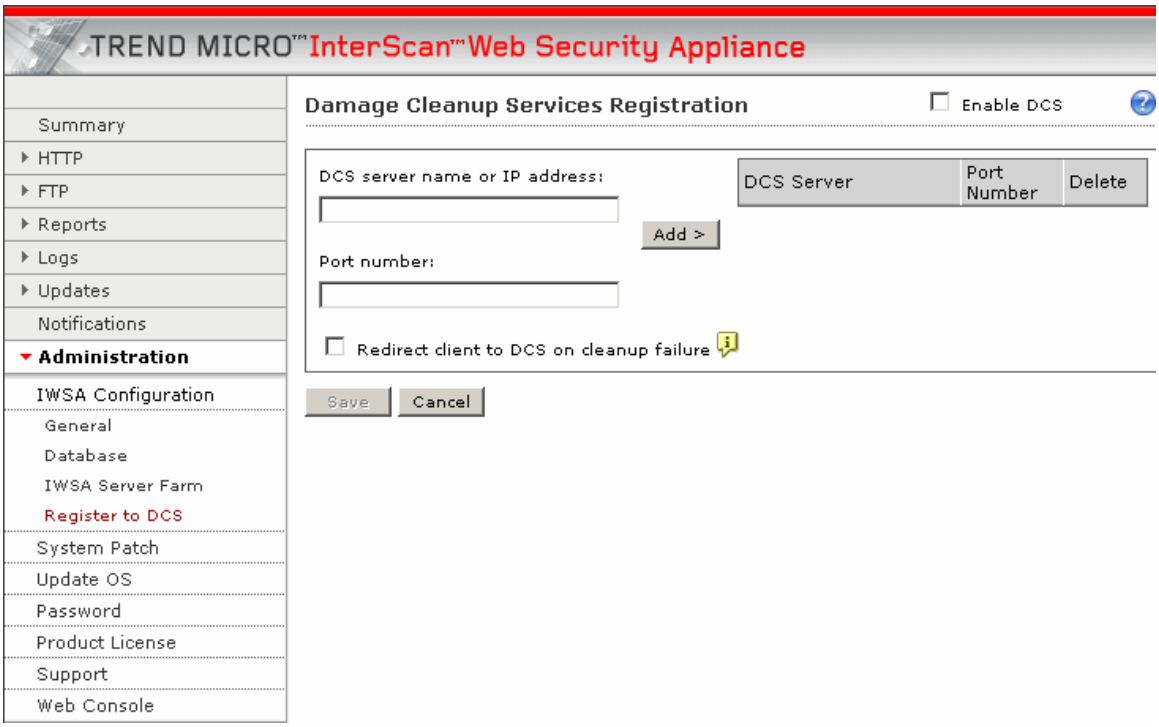
■ 在 Administration→IWSA Configuration→General：



注册 DCS 服务器

如果需要 IWSA 与 DCS 进行联动，对间谍软件进行清杀，可以在 IWSA 控制台加入 DCS 的服务器 IP（DCS 必须能够被 IWSA 搜索得到）。注册后你就可以在 IWSA 发现间谍软件的时候自动调用 DCS 对客户端进行清毒。

■ 在 Administration→IWSA Configuration→Register to DCS：

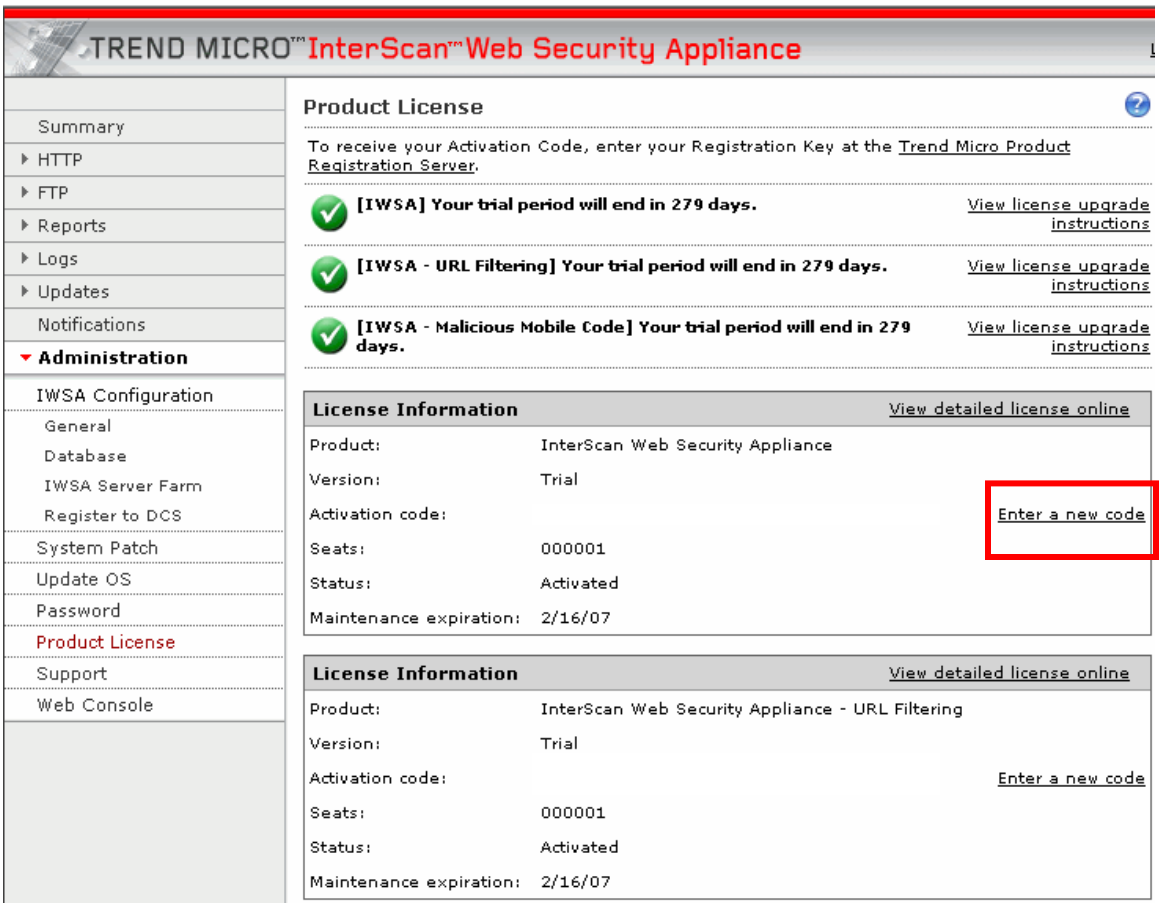


输入产品激活码

IWSA 有 3 个组件需要激活，包括：

- IWSA 主程序（必须）；
- URL 过滤；（可选）
- Applet and ActiveX Scanning 模块。（可选）

在 Administration→Product License 中输入产品的激活码：

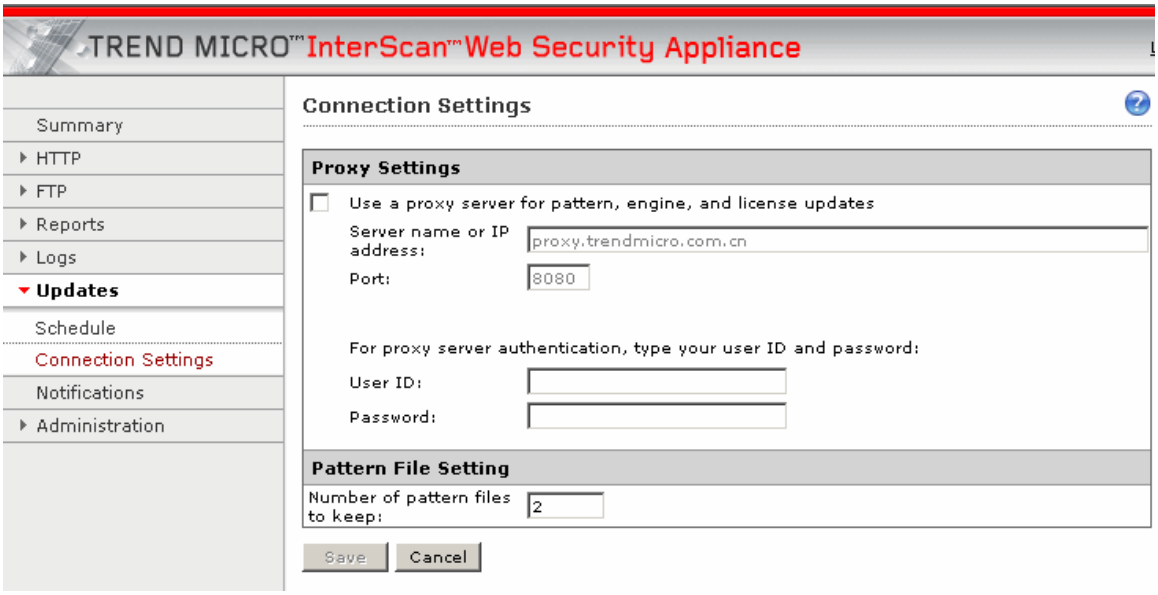

TREND MICRO™ InterScan™ Web Security Appliance
Summary
HTTP
FTP
Reports
Logs
Updates
Notifications
Administration
IWSA Configuration
General
Database
IWSA Server Farm
Register to DCS
System Patch
Update OS
Password
Product License
Support
Web Console
Product License
To receive your Activation Code, enter your Registration Key at the Trend Micro Product Registration Server.
[IWSA] Your trial period will end in 279 days.
View license upgrade instructions
[IWSA - URL Filtering] Your trial period will end in 279 days.
View license upgrade instructions
[IWSA - Malicious Mobile Code] Your trial period will end in 279 days.
View license upgrade instructions
License Information
View detailed license online
Product: InterScan Web Security Appliance
Version: Trial
Activation code:
Enter a new code
Seats: 000001
Status: Activated
Maintenance expiration: 2/16/07
License Information
View detailed license online
Product: InterScan Web Security Appliance - URL Filtering
Version: Trial
Activation code:
Enter a new code
Seats: 000001
Status: Activated
Maintenance expiration: 2/16/07

4.2 配置 IWSA 更新

IWSA 包含两种更新方式，分别是预设更新与手动更新；

配置预设更新

■ 更新代理设置

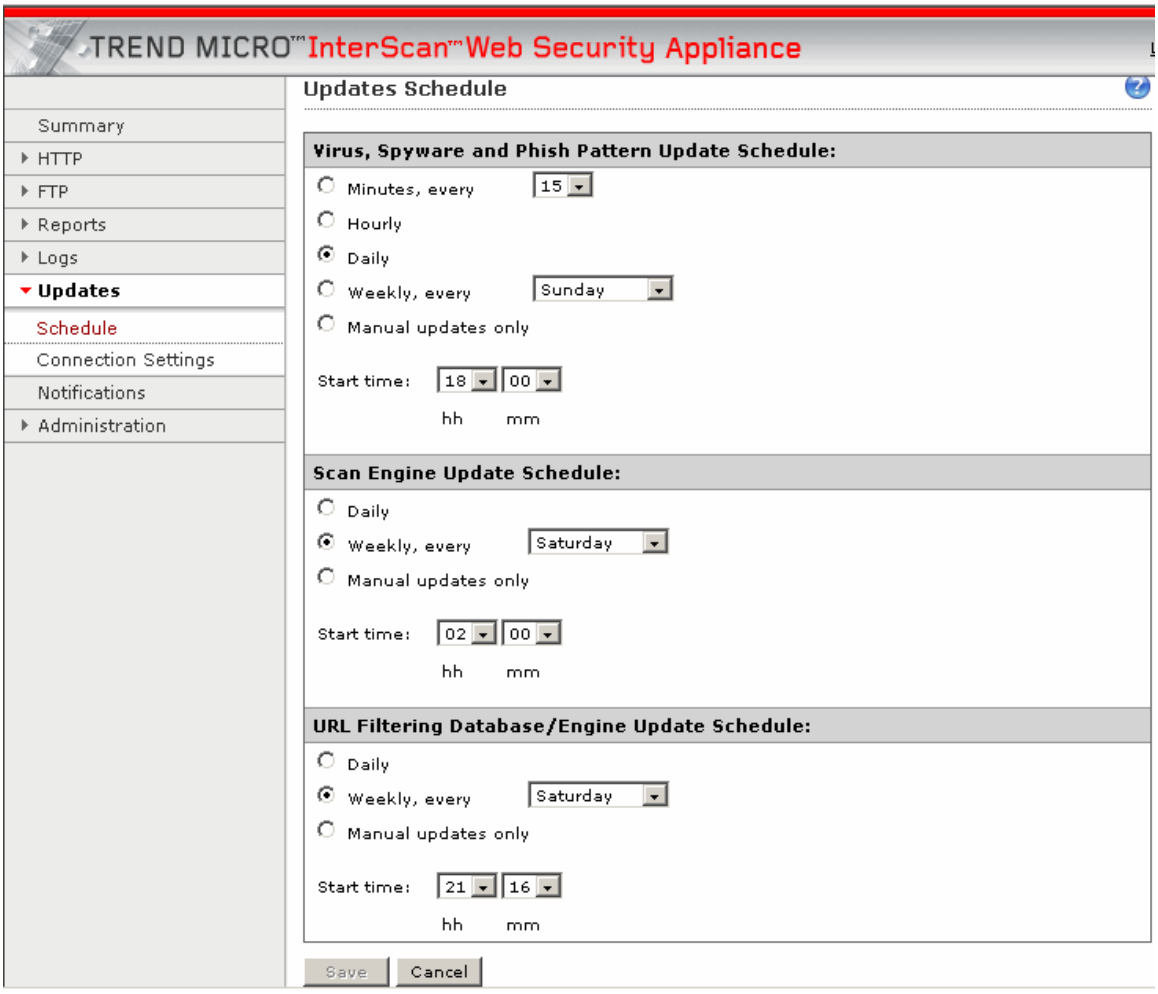


如果 IWSA 需要通过代理才能连接趋势科技在互联网的更新服务器，那么需要在这里填写相应的代理服务器信息。包括代理服务器 IP 及端口，如果需要身份认证，也需要在这里输入一个长期有效的账号。

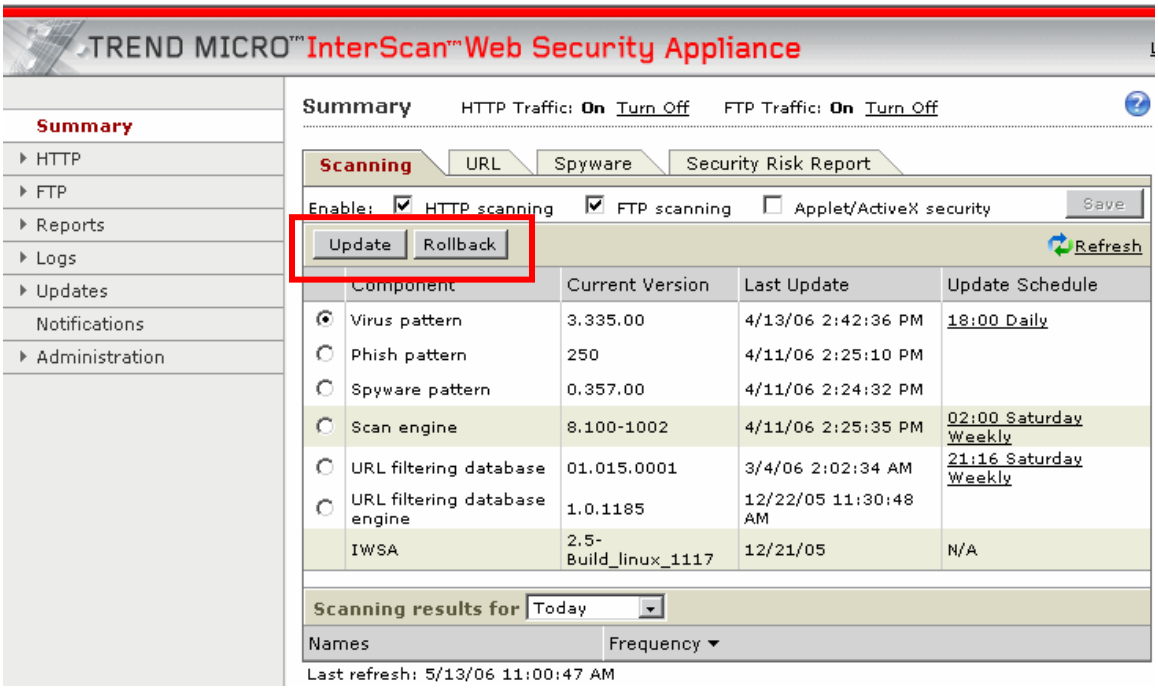
IWSA 支持病毒码 roll-back 功能。为了能够支持 roll-back 功能，IWSA 会保留一定数量的旧版本的病毒码。在这里可以设置保留的数量（0-65535），默认是 3。

■ 设置预设设定

IWSA 的组件升级分为三部分：病毒码（病毒、间谍软件及钓鱼）、扫描引擎、URL 过滤器的数据库及引擎。



执行手动更新及回滚



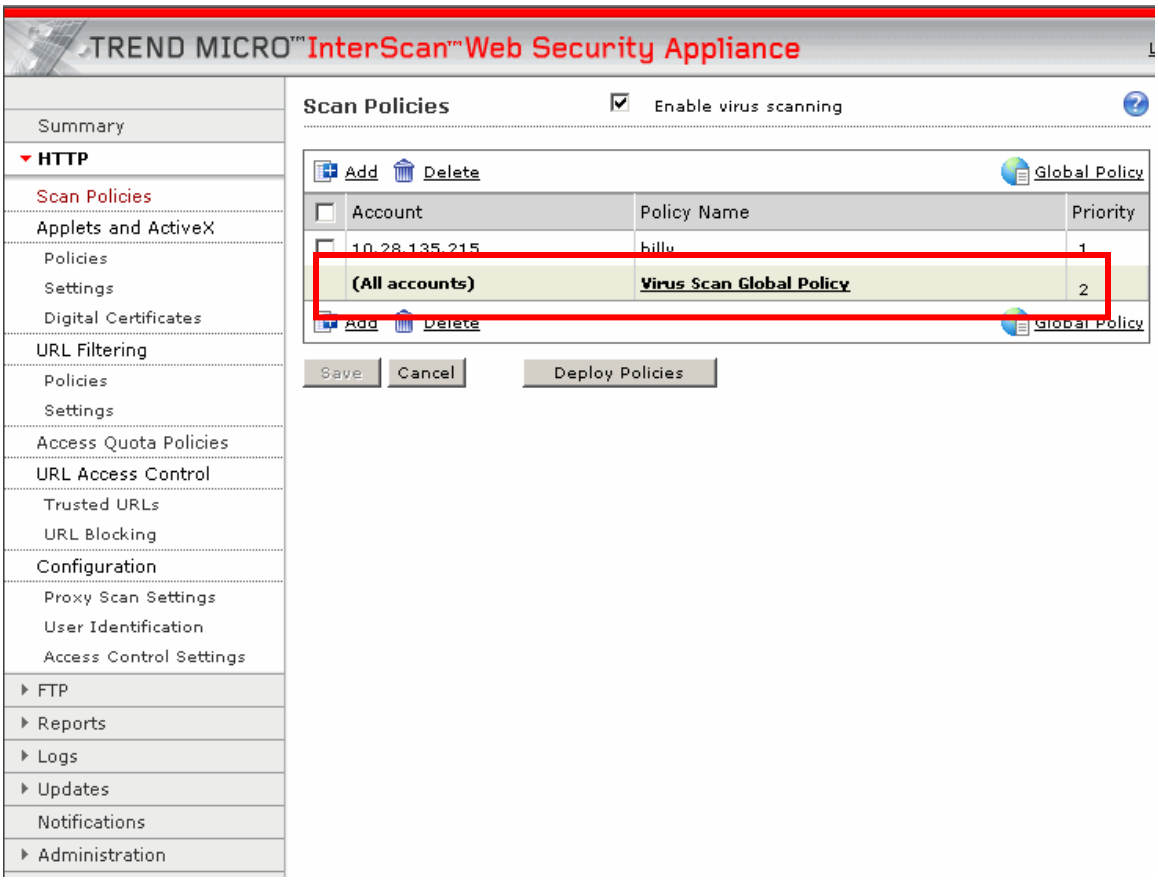
在 Summary→Scanning，点选 update 或 Rollback 进行手动更新或是回滚的操作。

4.3 HTTP 扫描选项配置

HTTP 扫描选项包含所有 IWSA 针对 HTTP 斜体提供的过滤功能，管理员可以通过这个菜单设置以下功能：

- Scan Policies – 管理员可以在此设置针对 HTTP 流中包含恶意代码的扫描及处理动作。这里所指的恶意代码包括病毒及间谍软件。
- Applet and ActiveX – 管理员可以在此设置 IWSA 针对 Java Applet 和 ActiveX 的控制。
- URL Filtering Policies – 管理员可以通过这个功能净化企业内部员工的上网内容，提高上网效率。
- URL Quota Policies – 管理员可以通过这个功能限制终端用户的上网流量。
- URL Access Control – 管理员可以通过这个功能设置针对网站的黑、白名单。
- Configuration – HTTP 自身相关的配置。如：工作模式等（在 3.3 已经讨论过）

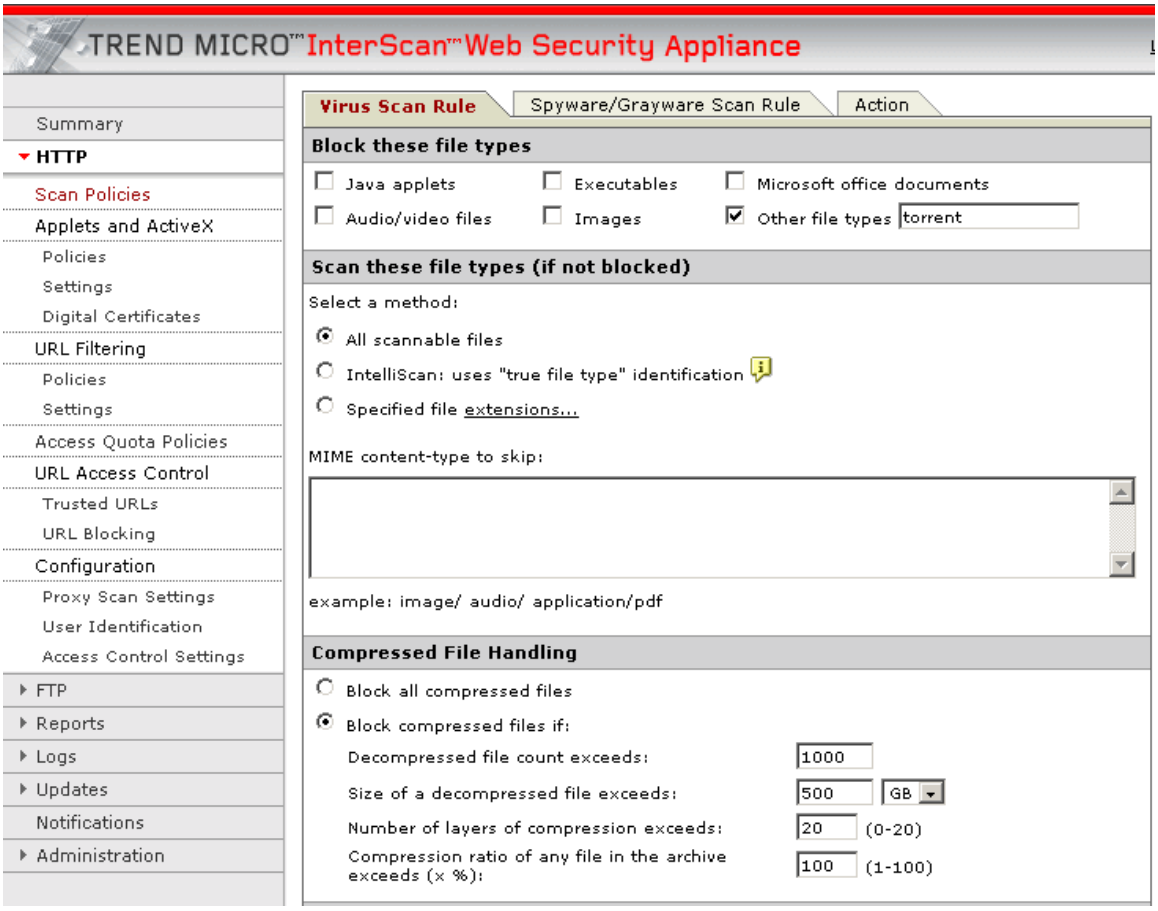
所有的 HTTP 配置项见下图：



4.3.1 配置 Scan Policies

IWSA 病毒扫描由策略构成，每条策略包含三部分：病毒扫描规则、间谍软件扫描规则、处理动作。管理员可以根据需要而针对每个部分进行微调。

- **病毒扫描规则**



在此，管理员可以针对以下几个方面进行配置：

- Block these file type – 这里可以允许管理员设置 IWSA 对特定类型的文件进行拦截。
- Scan these file type (If not block) – 这里允许管理员设置 IWSA 扫描那些文件。包括：
  - ✓ All file types – 所有文件类型；
  - ✓ Use IntelliScan – 真实文件类型扫描；
  - ✓ Specified file extensions – 特定扩展名文件扫描。
- Compressed file handling – 管理员可以通过这里配置对压缩文件的处理措施。选项包括：
  - ✓ Number of files – 解压后文件数的大小，超过这个数字，将会被拦截；
  - ✓ Decompressed percent – 解压后文件增大的比例的限制；

- ✓ Decompressed size – 解压后文件增大的值的限制；
- ✓ Decompressed layer – 压缩层数的限制；

■ **Large file handling** – 管理员可以在此设置 IWSA 对大文件的处理方式；

- ✓ Do not scan file large than – 当文件大小超过限值后 IWSA 不做扫描；
- ✓ Enable special file handling – 管理员可以在此设置 IWSA 对超过大小限制的文档的处理方式，一旦选择这种方式，管理员配置其下子选项中其中一个：
  - ◆ Deferred scan – 大文件下载过程中，客户会看到一个下载进程窗口。一旦过程中发现病毒，连接会被中段。（建议使用）
  - ◆ Scan after delivering – 与 deferred scan 类似，但下载大文件过程中如果发现病毒不会断开当前连接,只会断开后来发起的连接。这种情况风险较大。

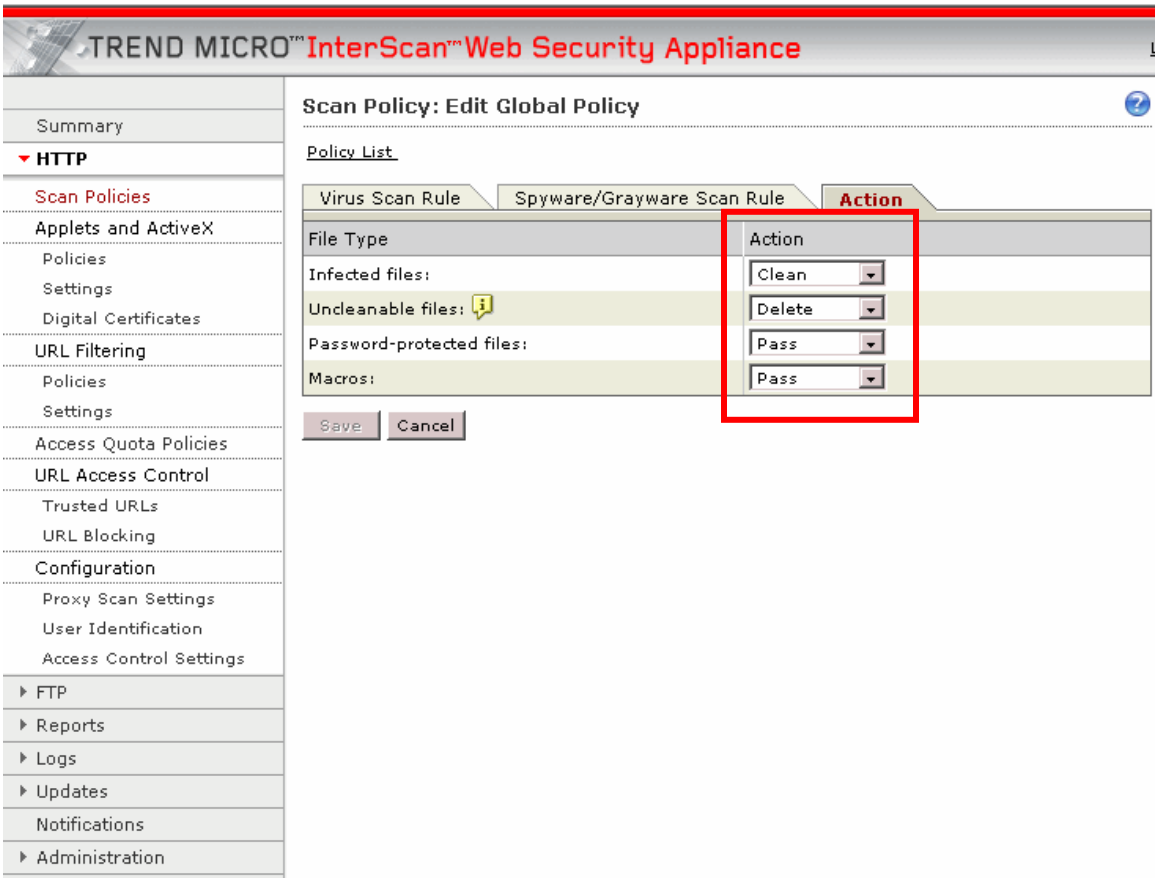
■ **Quarantined files handling** – 隔离文件处理措施。

- **间谍软件扫描配置**

管理员可以在此配置对间谍软件/灰色软件的防御。

- **HTTP 病毒处理动作配置**

管理员在此处配置 IWSA 对各种病毒的处理动作。



4.3.2 配置 Applet and ActiveX

IWSA 可以对 Java Applet 与 ActiveX 进行扫描，主要配置项如下：

1、全局设定；

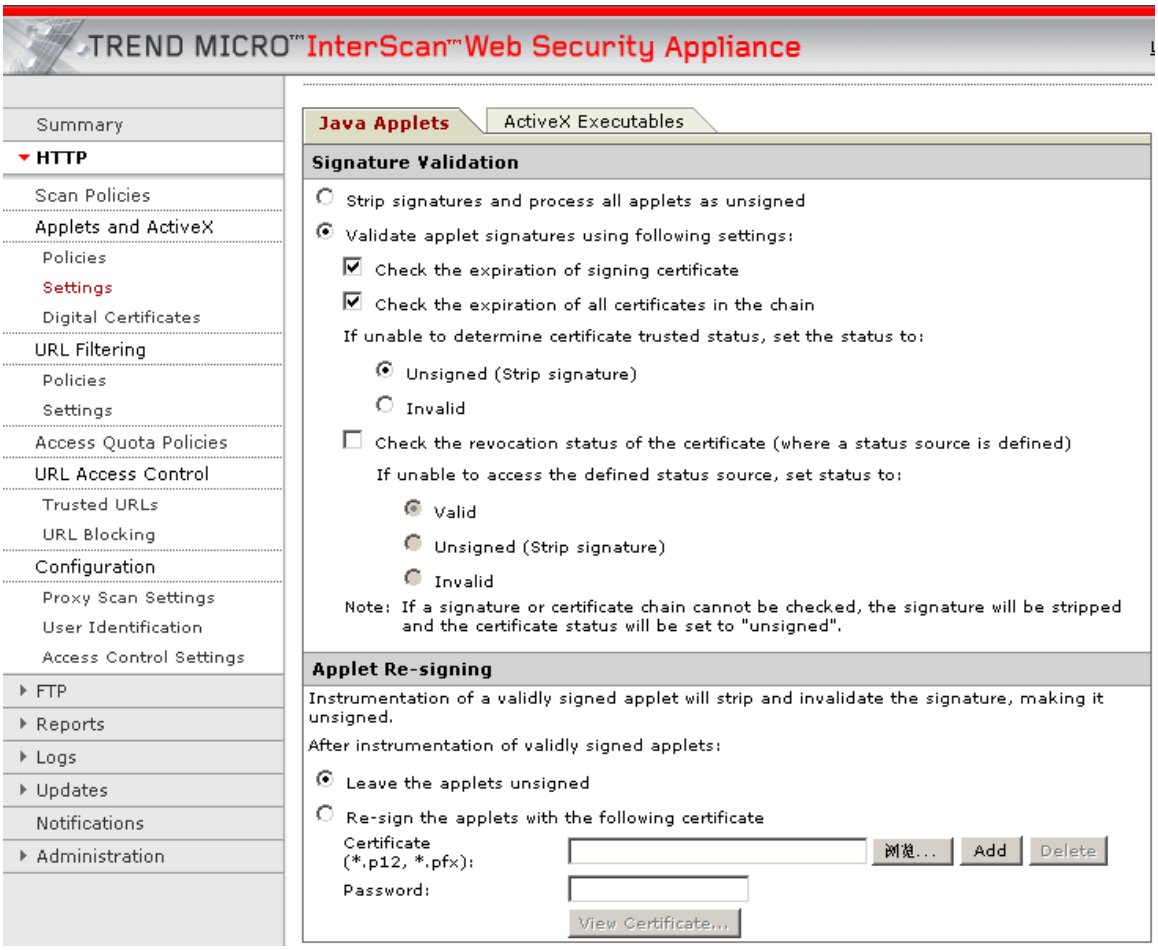
2、可信数字证书数据库；

3、扫描策略配置；

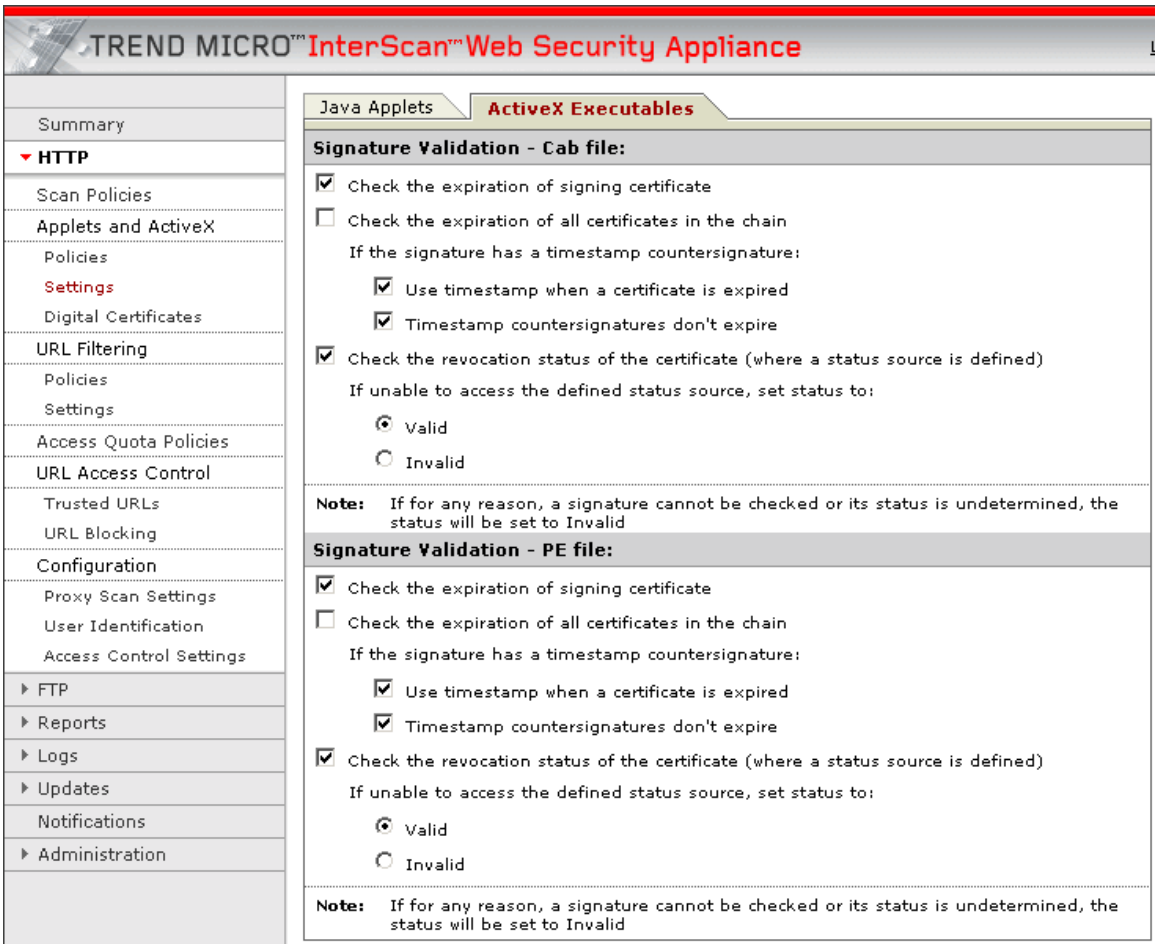
设定全局的配置：

设定 IWSA 对 Java Applet 与 ActiveX 的数字证书的合法性；

- 针对 Java Applet 的配置，HTTP→Applet and ActiveX→Setting



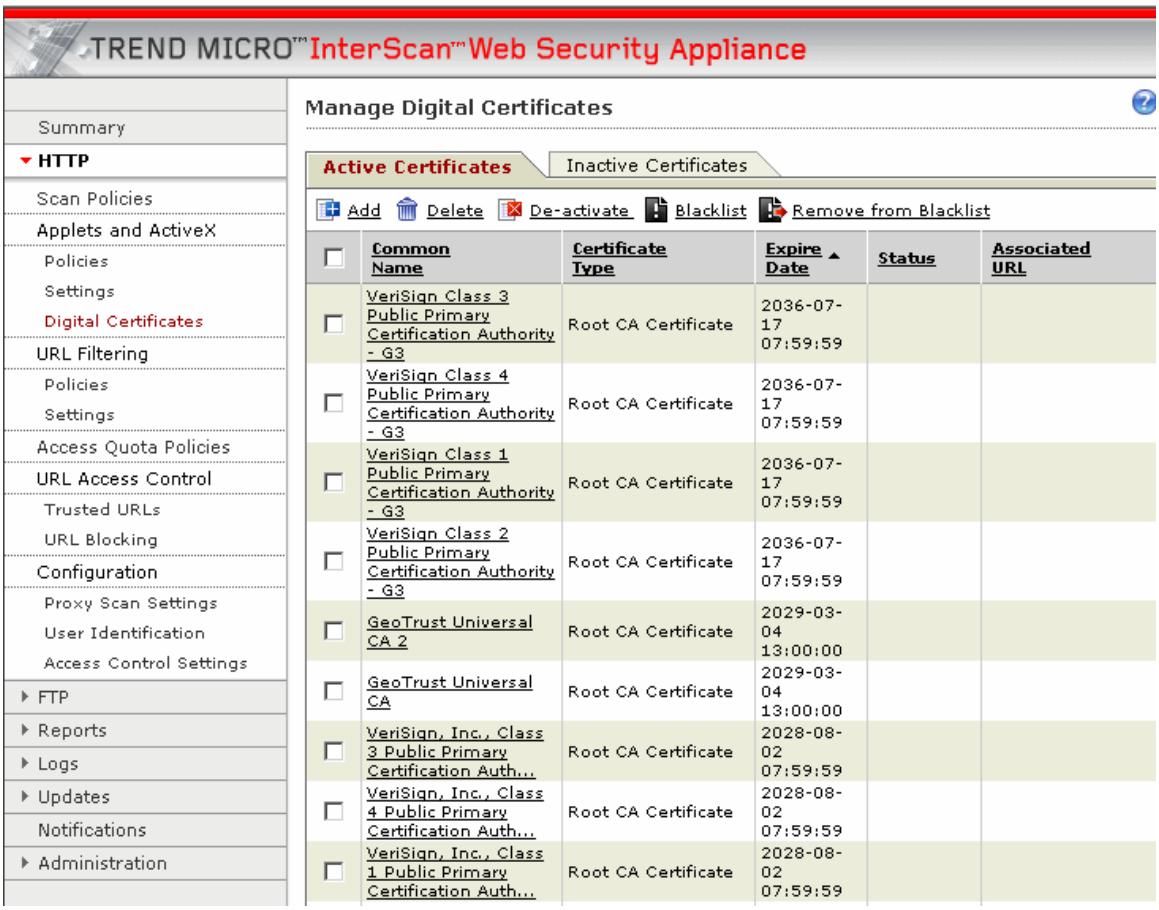
- 针对 ActiveX 的配置，HTTP→Applet and ActiveX→Setting



可信数字证书数据库

上一部分阐述了 IWSA 会检查 Java Applet 及 ActiveX 数字证书的检查，在这里就设定 IWSA 是以什么作为参考标准。管理员可以在这里进行增加、删除及黑名单等操作。

通过 HTTP→Applet and ActiveX→Digital Certificates 进入配置页面，根据用户的需求进行配置

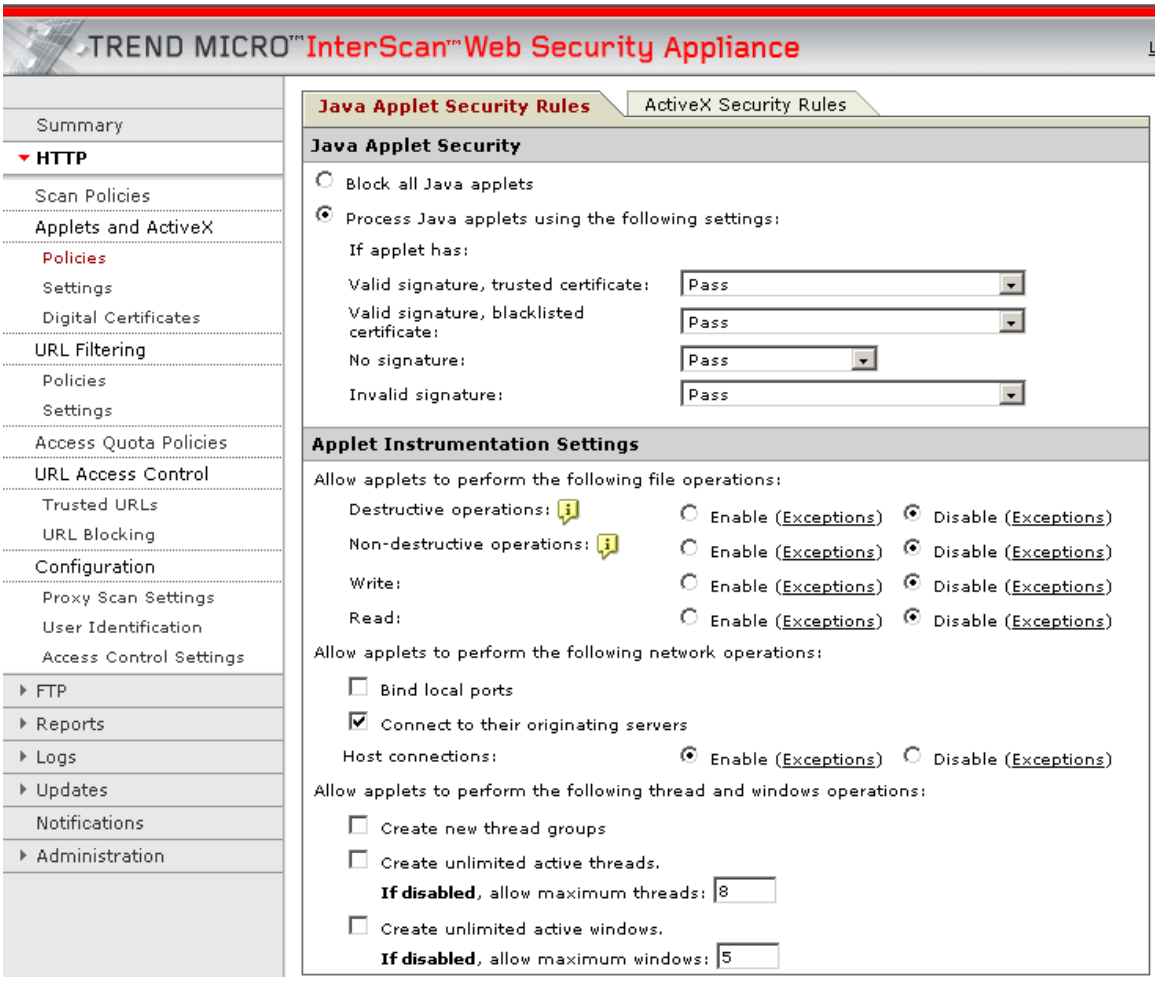


Applet and ActiveX 扫描策略配置

与 IWSA 其他的过滤器一样，Applet and ActiveX 扫描也是基于策略的，如果默认策略与企业自身不相符，管理员可以自定义一条新的策略。

通过 HTTP→Applet and ActiveX→Policies 登录扫描策略 Applet and ActiveX 扫描策略配置页面。这里也针对 Java Applet 与 ActiveX 分为不同的扫描设置。

- Java Applet



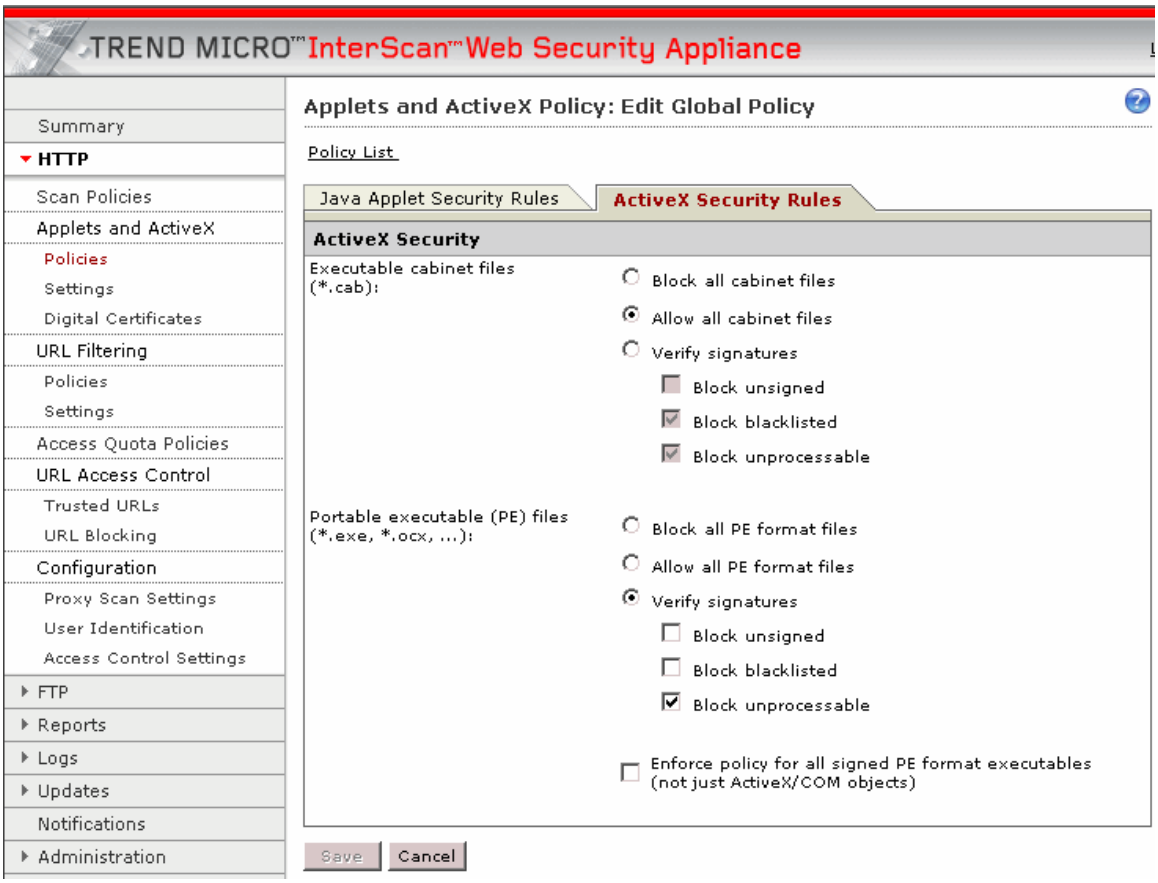
此页面有两个部分可以配置：

1、Java Applet Security – 用户设置哪种 Java Applet 需要处理，以及处理的动作；

2、Applet Instrumentation Settings – 允许 Applet 执行什么样的动作。

■ 针对 ActiveX 扫描设置

管理员可以根据自身的需要对 ActiveX 的扫描进行设置，通过 HTTP→Applet and ActiveX→Policies 进入配置页面：



在这里，管理员可以对以下两种类型的内容文件进行不同的处理：

1、Executable cabinet files（可执行的.cab 文件）- 对此类文件可以做不同的处理方式

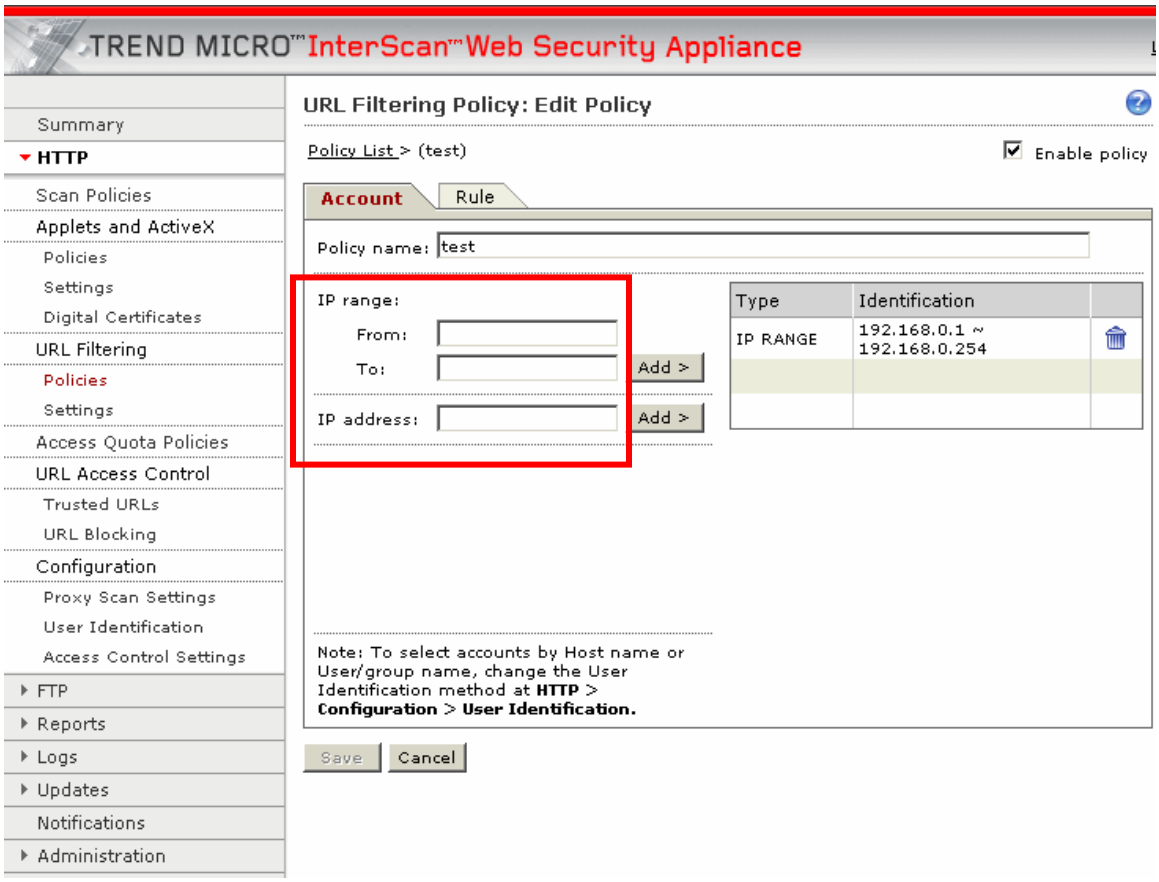
2、Portable Executable files -对此类文件可以做不同的处理方式

3、处理的方式包含：拦截、允许或扫描

4.3.3 配置 URL Filtering

IWSA 拥有强大的 URL 过滤功能，可以协助企业用户净化上网流量及增强员工工作效率。一般情况下，管理员只需要使用默认的 URL 过滤策略已经可以满足需求。创建一条 URL Filtering 的策略过程如下：

1、点选 HTTP→URL Filtering Policies，点击 Add；

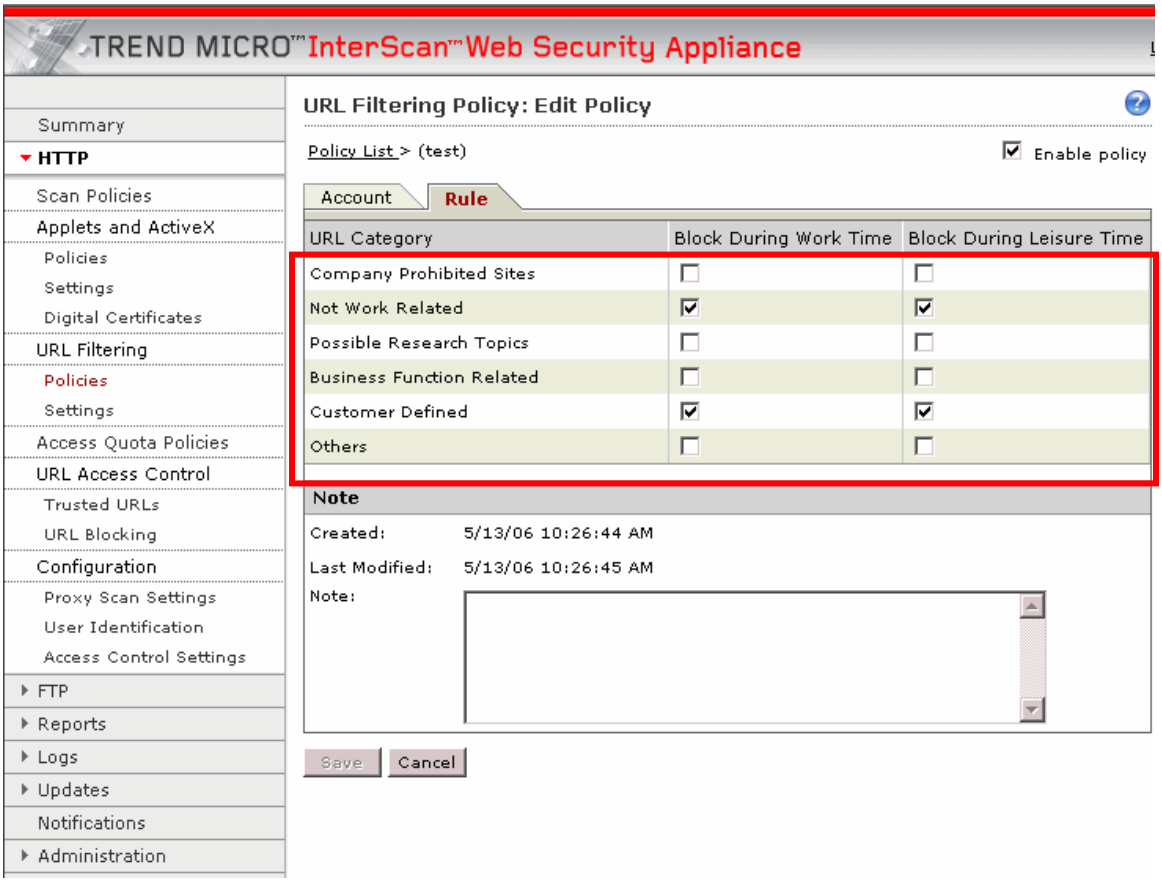


2、这时弹出一个如上图的窗口；

3、为新增的策略赋予一个唯一的名字；

4、接下来设定辨别用户身份的方式，包括通过 IP、主机名、LDAP User 等方式；

5、设定后，点击 Next 进入下一个页面，如下图：



6、选择用户不能浏览的 URL 分组；

7、点选 Enable policy。

8、点击 Save。

9、如果需要立刻生效，点击 Deploy Policies。

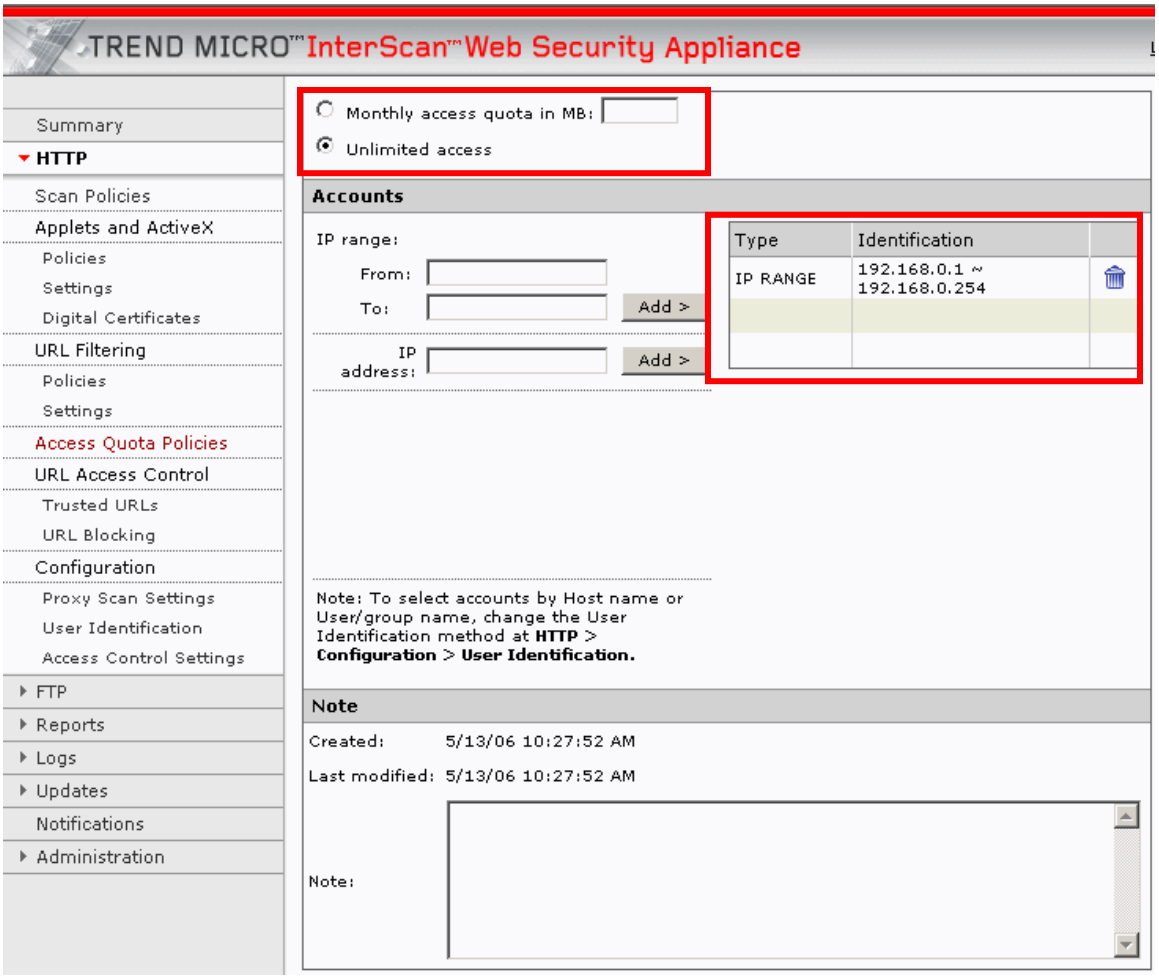
4.3.4 配置 Web Access Quota Policies

管理员可以在此设定某个用户（按 IP、主机名、LDAP User）在某个时间段内能够下载/上传的数据总数。如果这个用户在这个时间段内超过了这个限值，IWSA 会把这个用户的连接中断，直到这个时间内完结。

默认情况下，IWSA 不会对任何的用户设定该限值。

创建一条新的 Web Access Quota Policies，步骤如下：

1、点选 HTTP→Access Quota Policy，点击 Add，弹出以下窗口：



2、选择标识身份的方式，加入需要监控的客户，点击 Next；

3、选中 Enable Policy；

4、设定该用户的流量限制；

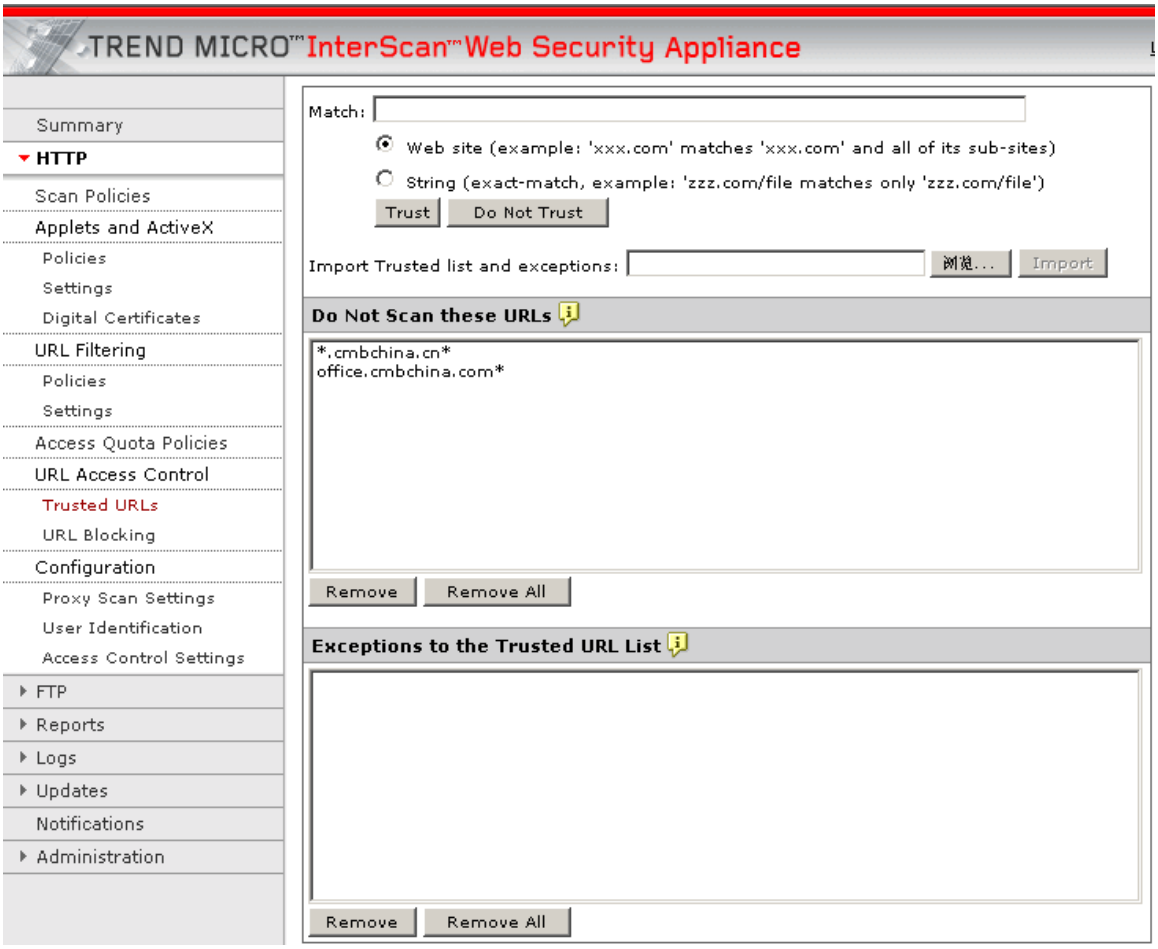
5、点击 Save；

6、如果想立刻生效，点击 Deploy Policies。

4.3.5 配置 URL Access Control

➢ URL 白名单配置

1、点选 HTTP→URL Access Control→Trusted URLs，弹出以下页面：



2、在 Match 的文本框中输入你信任的网站关键字，关键字可以是主机名、域名或是 IP 地址等；

3、选择匹配的方式；

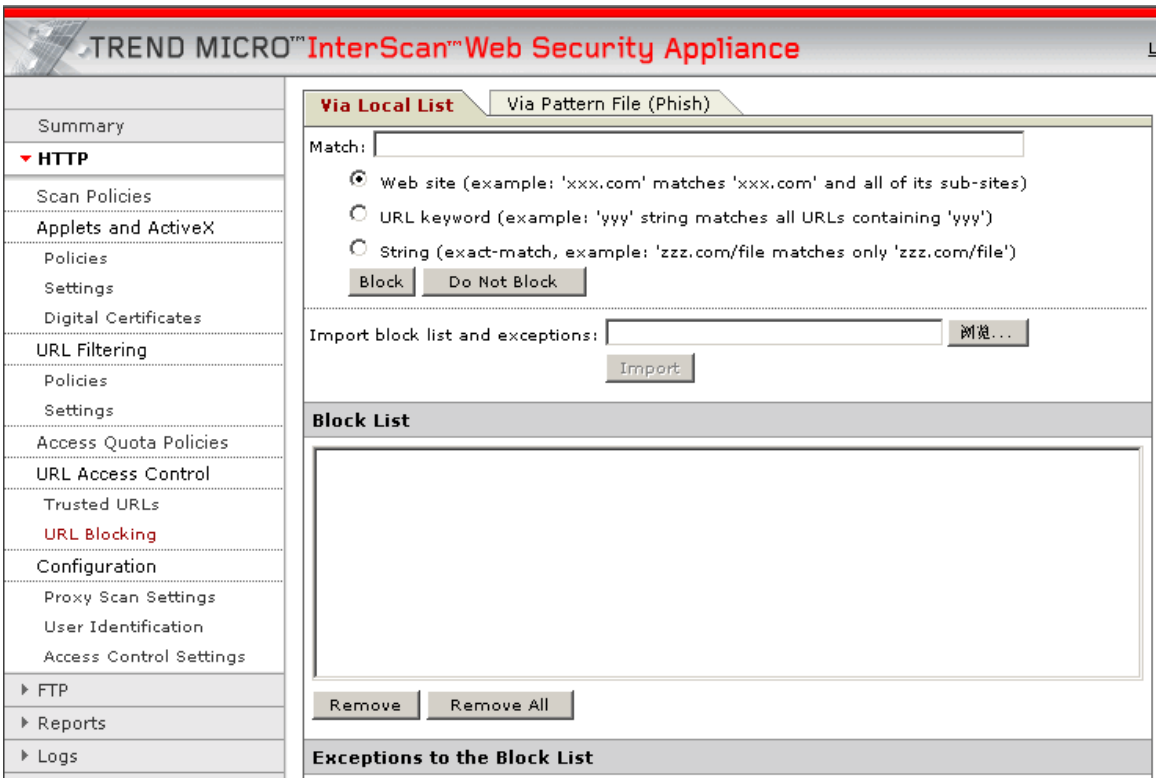
4、点选 Approve 把该网站加入可信任网站列表中，点选 Do not Approve 把该网站加入例外列表中；

5、点选 Save。

➢ URL Blockling

新增一个 URL blocking list，主要有以下步骤：

1、点选 HTTP→URL Blockking→Via Local List，弹出一个配置窗口，如下：



2、在 Match 的文本框中输入你想拦截的网站，

3、选择匹配的方式（Website、URL keyword、String）；

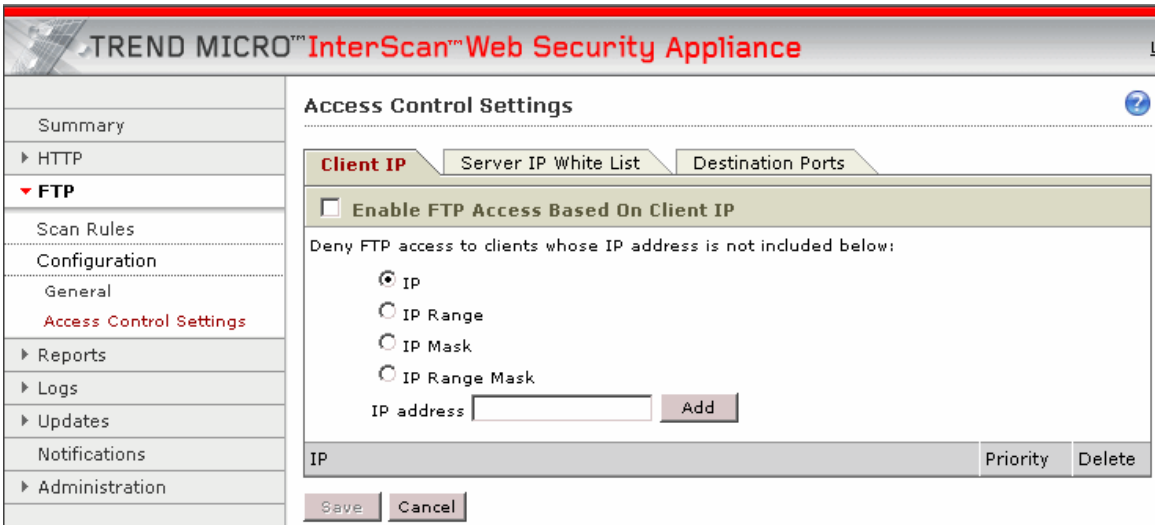
4、电选 Block，此网站会放入 Block list 中，点选 Do not Block，此网站会放入 Exception to Block List 中；

5、点选 Save。

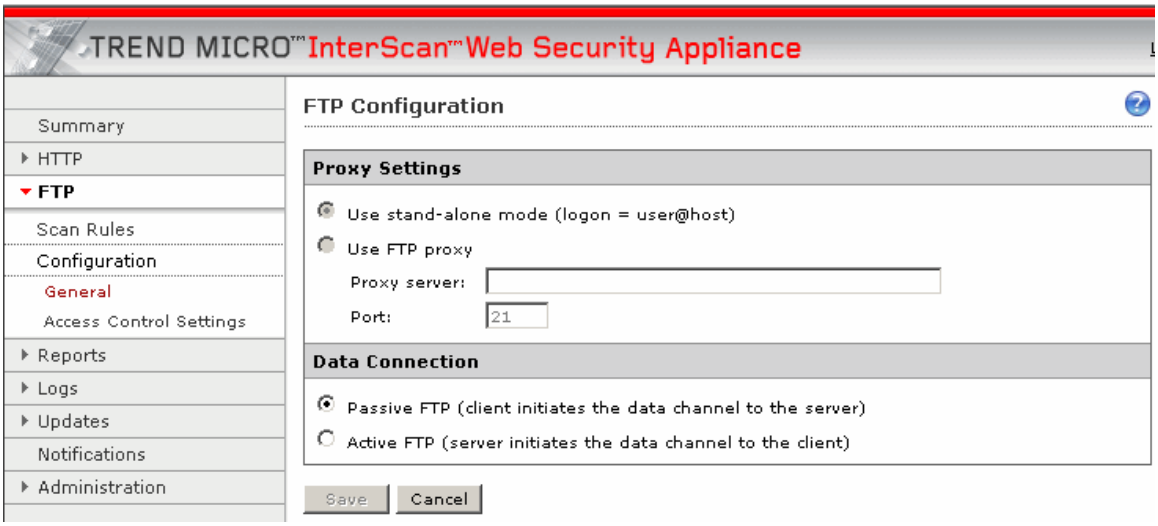
4.4 FTP 扫描选项配置

IWSA 可以针对 FTP 协议进行病毒及间谍软件的清查。FTP 扫描选项主要包含以下菜单：

- Scan Rules – 对病毒的处理措施设置；
- Configuration ：
  - ✓ General – 全局参数的设置；
  - ✓ Access Control Settings – 访问策略配置项。



配置全局参数



在这里主要配置 IWSA 的工作模式：

设定 IWSA 的工作模式：

- Stand-alone：自身作为企业的 FTP 代理服务器。
- Use FTP Proxy：自身无法直接联入 Internet，需要与原有的 FTP 代理作联动。

配置 FTP 扫描选项

在 FTP 扫描选项中增加了数据流方向的扫描，包括 upload 与 download 两个方向，用户可以根据保护的对象不同设定扫描的方向，增强 IWSA 的性能。

其余的选项与 HTTP 病毒扫描选项一致，详细可以参考 4.3.1。

4.5 IWSA 日志与报表

4.5.1 IWSA 日志

IWSA 对自身运行状况及病毒处理状况作了比较丰富的日志记录，主要有以下几种日志：

- ✓ 病毒日志；
- ✓ 间谍软件日志；
- ✓ URL 拦截日志；
- ✓ URL 访问日志；
- ✓ 性能日志；
- ✓ FTP Get 日志；
- ✓ FTP Put 日志；
- ✓ 清除日志

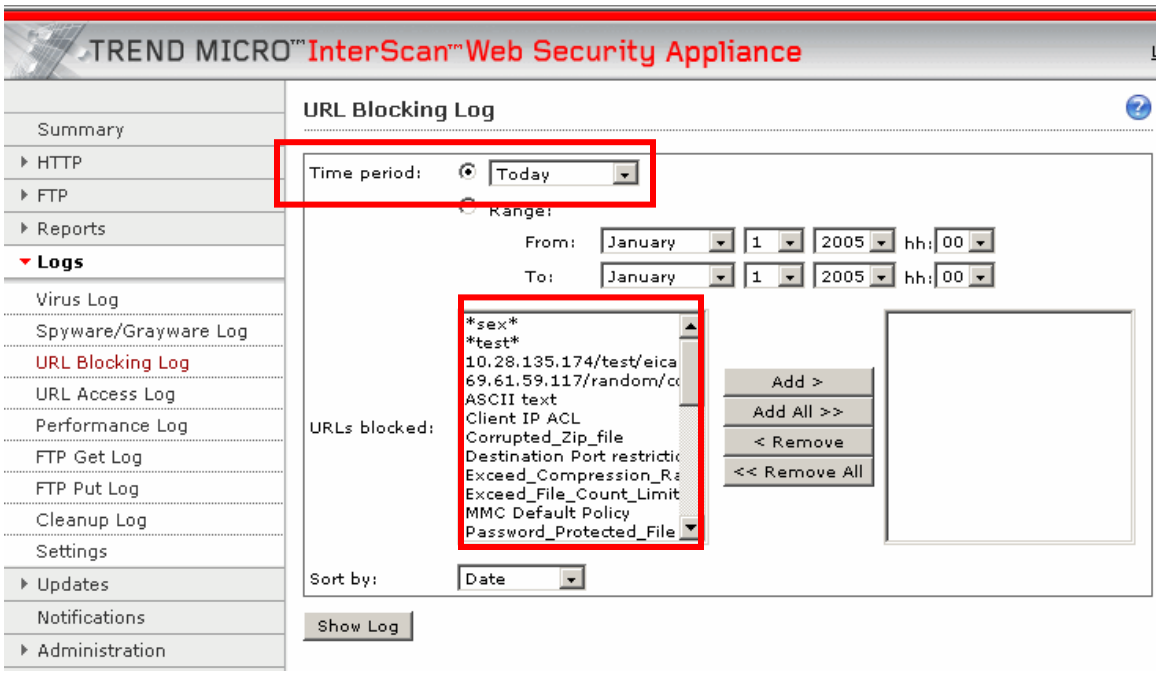
IWSA 的系统日志有：

- ✓ HTTP Scan Log；
- ✓ FTP Scan log；
- ✓ Mail Log；
- ✓ Admin Log；
- ✓ Update Log。

➢ 如何察看 IWSA 日志

IWSA 所有的 Log 的查看方式基本一致，这里以 URL Blocking Log 为例：

1、点选 Logs→URL Blocking Log，弹出以下窗口：

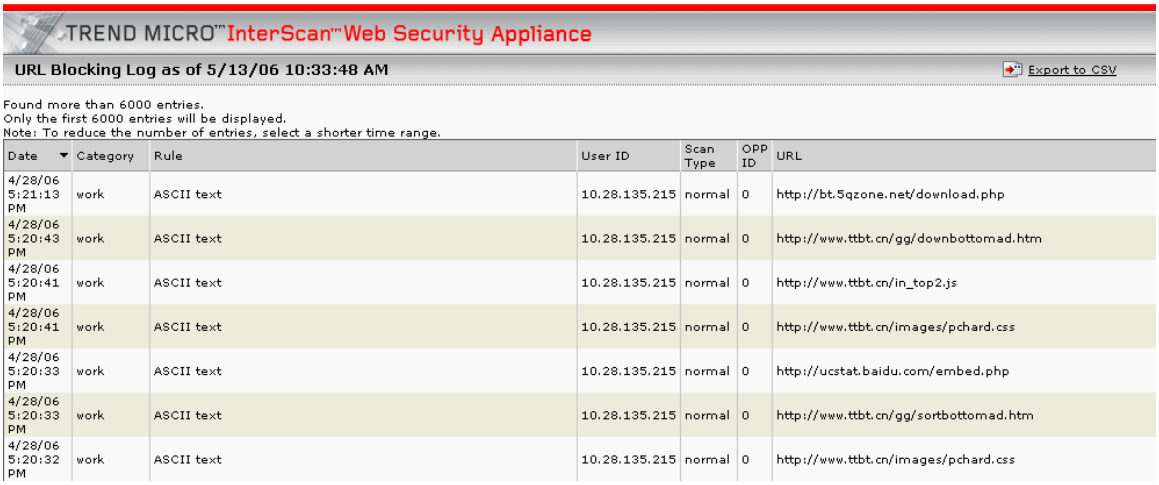


2、在右方的窗口选定你想查看的时间；

3、选择你想查看的被过滤的内容；

4、选择相应的排序；

5、点选 show log 就可以显示相关的日志。


TREND MICRO™ InterScan™ Web Security Appliance

URL Blocking Log as of 5/13/06 10:33:48 AM

Export to CSV

Found more than 6000 entries.
Only the first 6000 entries will be displayed.
Note: To reduce the number of entries, select a shorter time range.

Date	Category	Rule	User ID	Scan Type	OPP ID	URL
4/28/06 5:21:13 PM	work	ASCII text	10.28.135.215	normal	0	http://bt.5qzone.net/download.php
4/28/06 5:20:43 PM	work	ASCII text	10.28.135.215	normal	0	http://www.ttbt.cn/gg/downbottomad.htm
4/28/06 5:20:41 PM	work	ASCII text	10.28.135.215	normal	0	http://www.ttbt.cn/in_top2.js
4/28/06 5:20:41 PM	work	ASCII text	10.28.135.215	normal	0	http://www.ttbt.cn/images/pchard.css
4/28/06 5:20:33 PM	work	ASCII text	10.28.135.215	normal	0	http://ucstat.baidu.com/embed.php
4/28/06 5:20:33 PM	work	ASCII text	10.28.135.215	normal	0	http://www.ttbt.cn/gg/sortbottomad.htm
4/28/06 5:20:32 PM	work	ASCII text	10.28.135.215	normal	0	http://www.ttbt.cn/images/pchard.css

4.5.2 创建 debug Log

除了通过 Web 控制台来设定上述的日志以外，管理员还可以在 /etc/iscan/intscan.ini 上设置 IWSA 创建 Debug 信息。Debug log 对产品排错有极大的帮助，当 IWSA 产品发生故障时，售后人员会安排管理员协助打开 IWSA 的 Debug log 选项。

打开 IWSA debug log 的方法：

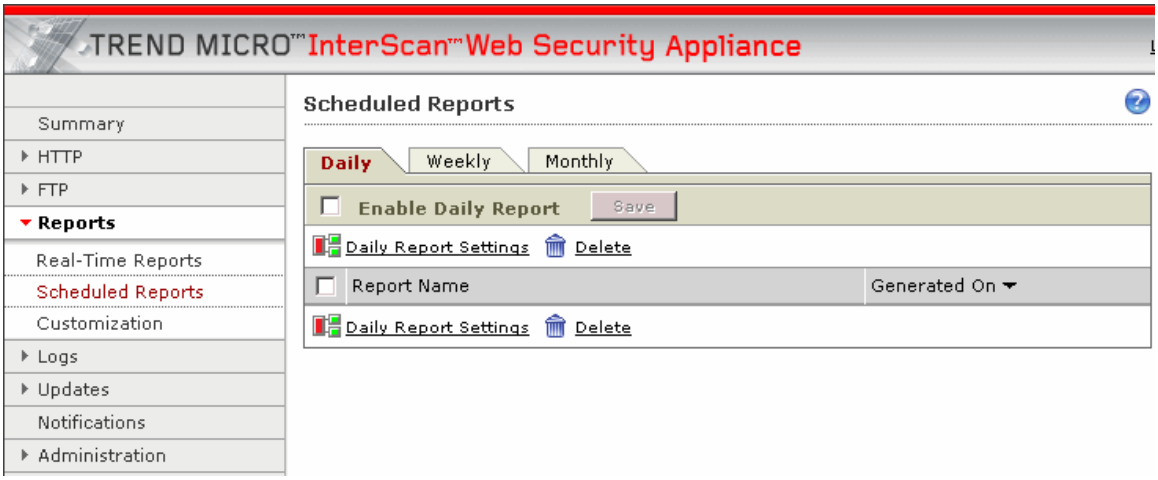
- 通过 shell 进入命令行；
- vi 打开/etc/iscan/intscan.ini；
- 针对 HTTP：

  [http]
  #switch for debug log
  # 1 -> turn on
  # 0 -> turn off
  verbose=1
- 针对 FTP：

  [ftp]
  #switch for debug log
  # 1 -> turn on
  # 0 -> turn off
  verbose=1
- 退出并保存；
- 重启动 IWSA 服务。输入：./S991Sproxy reload
- IWSA 会在 log 目录生成文件名为“http.log.yyyymmdd.000x”的 log；
- 通过“cp http.log.yyyymmdd.000x ../UserDumps”把 log 拷贝至 UserDumps 目录；
- 通过 Web 控制台 Administration->Support 可以找到该文件，下载至本地即可。

4.5.3 创建 IWSA 报表

管理员可以根据自身的需要，定制一个预设生成的报表，以供检查。



定制的方法如下：

1、点选 Report→Settings→Daily Report；

2、激活 Enable Daily Report 选项；

3、选择希望生成报表的时间，默认是 12AM；

4、定义一个邮箱地址，用于接收报表生成通知；

5、选择 Report 生成的范围（用户等）；

6、选择 Report 种类；

7、选择 Report 的格式；

8、选择 Save，保存设置。

4.6 恢复 IWSA2500 出厂设置

为了方便工程师重置 IWSA2500 的设置，我们提供以下方法恢复 IWSA2500 的出厂设置。你可以根据你的需求做以下的操作：

1. 保存当前的网络设置但恢复出厂时的软件设置；
   - Reset IWSA Software Binary files;
   - Reset All IWSA software configurations.
2. 恢复网络及软件的出厂设置。
   - Reset IWSA Network Configurations;
   - Reset IWSA Software Binary files;
   - Reset All IWSA software configurations.

4.6.1 Reset IWSA Network Configurations

1) 通过串口线接入 IWSA2500;

2) 访问 Shell;

1. 输入 root 帐号与密码（默认 iwsa);
2. 选择相关的菜单进入 shell: “Utilities” (2) → “Start Shell Interface” (1) → “y” [Enter] to continue
3. # /etc/resetconfig.sh - 恢复为默认配置（桥模式、没有管理 IP、没有注册至 TMCM)
4. 重启动 IWSA
   - 输入 exit [Enter]
   - “0” [Enter] - 上级菜单（主菜单)
   - “4” [Enter] - Reboot
5. 重新配置 IWSA2500 的 IP 地址与主机名
   - Access the shell interface (See step 2)

- System Configuration (1) → Configure Device Settings (2)

4.6.2 Reset IWSA Software Binary Files

1) 通过串口线接入 IWSA2500;

2) 访问 Shell;

- 输入 root 帐号与密码（默认 iwsa);
- 选择以下选项： “Restore IWSS to Factory-default installation” “Rescue System” (3) → “Restore IWSS to Factory-default installation” (2)

4.6.3 Reset All IWSA software configurations

通过以下步骤，IWSA2500 会丢失的原有信息，包括日至、配置及策略等，并且 IWSA2500 会恢复为原厂的所有配置。

1. # mount - Verify which partition is mounted (/dev/hda2 or /dev/hda3)
   Look for one of the following:
   /dev/hda2 on / type ext2 (ro)
   /dev/hda3 on / type ext2 (ro)
2. # mount -o remount /dev/hda2 / - Mount File system Read/Write (specify partition in previous step)
3. # cd /var/iwsa_image/1130 - Change present working directory to the location of the iwsa installtion files.
4. /var/iwsa_image/1130 # chmod 744 uninstall_appliance.sh - make uninstall
   script executable
5. /var/iwsa_image/1130 # ./uninstall_appliance.sh - Uninstall IWSA

Software

6. /var/iwsa_image/1130# ./install_appliance.sh - Reinstall IWSA Software

- Binary Package File? [Binary-2006mmdd.tar.gz] [Enter]
- Data Package File? [Data-2006mmdd.tar.gz] [Enter]
- Enter password for new user iwsa [Enter]
- Enter it again. iwsa [Enter]

5、如何检查部署是否成功

说明：关于病毒的测试统一使用EICAR 测试文件。请不要使用真正的病毒在您的系统上做测试。EICAR European Institute for Computer Antivirus Research)欧洲计算机抗病毒研究中心是由学院，商业协会，媒体政府机构等一起组成的一个团体，主要成员有网络安全专家，法律专家等。这个组织致力于控制计算机病毒和计算机资源的滥用。同时也是EICAR 测试文件的提供者。您可以在以下链接下载到该文件：http://www.eicar.org/anti_virus_test_file.htm

5.1 HTTP 防毒功能测试

- 把测试客户机的代理设置指向 IWSA(如果 IWSA 工作在桥模式则无需这样设置)；
- 通过浏览器打开 Eicar 测试网站，该文件会被 IWSA 所检测而无法下载。IWSA 会在客户段浏览器弹出警告窗口，告知该网页含有病毒。

5.2 FTP 防毒功能测试

这里以 IWSA 工作在桥模式之下的方式来测试。

目标FTP站点：ftp://download.trendmicro.com/products/eicar-file/eicar.com

通过 IE 直接打开该连接，会发现文件不能下载，该页面被检测为含有病毒的页面。

6、FAQ

Q：IWSA 用的是 NVW2500 的硬件，请问 IWSA 能否使用 5 个端口同时工作？

A：不可以。IWSA 最多只能使用 3 个端口。使用多少个端口根据 IWSA 的工作模式来决定。

Q：目前版本 IWSA 透明桥模式能否支持 Vlan?

A：不支持。目前版本暂时无法支持 Vlan。

Q：IWSA 最高支持的用户数有 5000，但为什么我的用户数只有 2000，就觉得很慢？

A：5000u 是指在用户行为比较规范时所能够运行的理想环境。如果用户行为比较复杂的时候（如：BT、下载电影等等），则需要另外考虑 IWSA 所能承受的用户数。

参考建议：

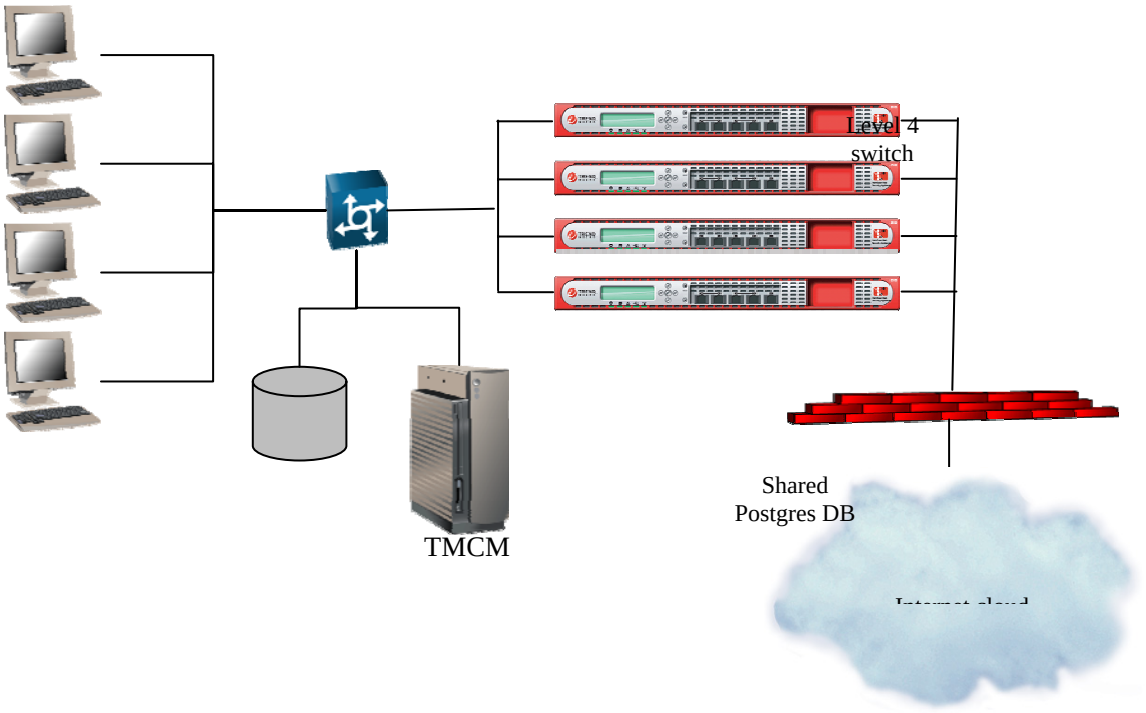
- 性能高低排序（由高至底）：ICAP 联动模式→Proxy 联动模式→桥模式；
- 启用 URL 过滤，性能下降 25%；
- 启用 MMC，性能下降 20%；
- 如果用户行为复杂，需要针对用户行为作微调，如（设定文件类型拦截、大文件处理方式、压缩文件处理方式等）

Q：如果我的客户超过 5000u，IWSA 还能否部署在客户环境中？如果能部署，部署多少台，性能如何？

A：可以部署。部署多少台需要根据用户环境来决定。理想情况下单台 IWSA 可以承受 5000u，以客户当前环境的用户总数/5000=IWSA 需要部署的台数。

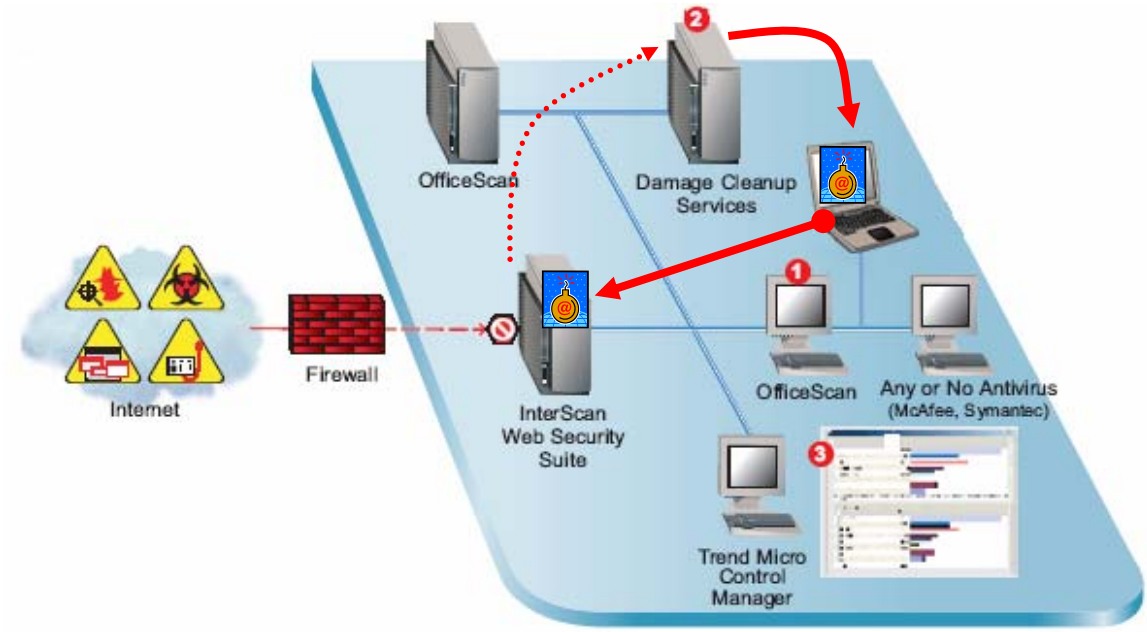
需要注意的是：多台的联动需要 4 层交换机来配合。

如下图：



Q：IWSA 检测到间谍软件后，如何与 DCS 联动？

A：当 IWSA 发现客户端发生间谍软件的“Phone-home”时，会调用已经注册并且能够连接到的 DCS 服务器，对客户端进行远程清除间谍软件的动作。如果清除不成功（没有客户机密码），IWSA 会把客户端重定向至 DCS 服务器的页面，进行清毒后才能上网。原理如下图：



Q：IWSA 是否支持 VLAN 环境？？

A：经过测试；IWSA 是可以支持 VLAN 的环境，通过超级终端，在 IWSA 的配置中必须加入对应的 VLAN routing IP 和 NAT IP。（前提：IWSA 的位置必需放在三层交换机之前）

Q：IWSA 是否断点续传的连接？对于断点续传的文件是否进行扫描？

A：经过测试；IWSA 可以支持断点续传的连接，而且在断点续传的同时进行病毒扫描。

Q：IWSA 是否支持中文的病毒警告？

A：经过测试；IWSA 的病毒警告信息是可以支持 Double byte；详细请见以下图示。

Q：IWSA 在透明模式下只支持 HTTP80 端口的扫描，其它的 HTTP 端口是否支持？

A：确实 IWSA 在透明模式下只支持 HTTP80、FTP21 的扫描；如果客户希望扫描其它端口，我们也有解决方案；在 IWSA command line 中修改，可是修改过程比较复杂。

7、厂家资源

- 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
  www.trendmicro.com
- 病毒查询
  www.trendmicro.com/vinfo/zh-cn/
- 中文版资料及软件下载
  ftp.trendmicro.com.cn
- 趋势科技英文产品下载网站
  www.trendmicro.com/download
- 试用版序列号申请：
  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
- 趋势科技金销报订阅网址
  www.trendmicro.com.cn/corporate/about/channel/news/subscribe.asp