IWSA 系列安装指南

本安装指南适用于 IWSA1500, IWSA3000, IWSA5000, IWSA6000 和 IWSA10000。但有些步骤因平台不同会有些差异，请注意文档中的这个标记：“***差异步骤**”。遇到标记时，请根据平台选择对应的步骤。

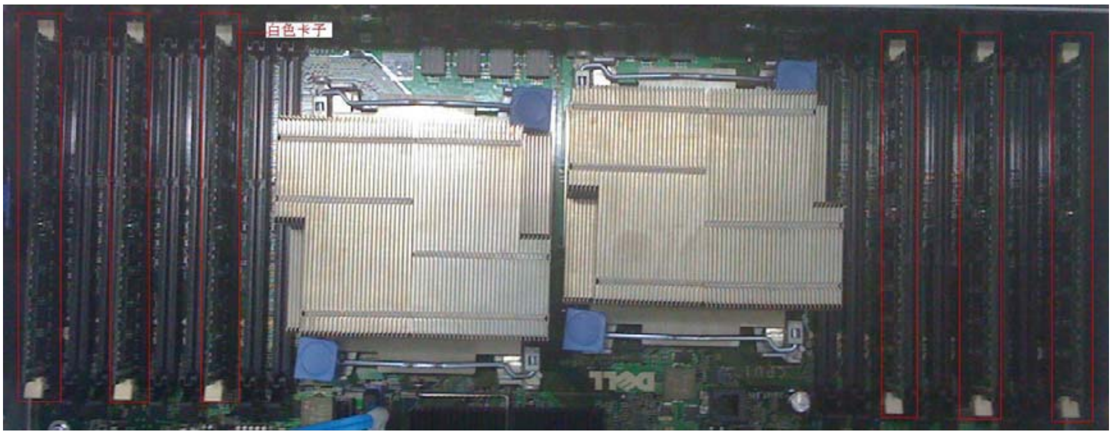
如果你拿到的是我们正式发货的 IWSA 设备，请从第二章开始配置，因为第一章在出厂时已配置完成。

如果你从第一章开始配置，你必须准备一个 USB 接口键盘和一台显示器。如果从第二章开始配置，你只需要一根串口线就可以。

一　安装步骤

1. 开机前内存检查（不适用于IWSA5000）

为了让内存的性能达到最优，开机前需要检查内存条的插法。以 12GB 内存为例，如单条内存是 2GB，那么一共是 6 根内存，每个 CPU 一侧各插 3 根。在这些内存插槽中，其中六个两端的卡子是白色的，需要把内存分别插在这 6 个插槽处。如下图所示：



如果只上一颗 CPU，请把内存插在靠 CPU 侧的插槽。并且按照插槽序号，先插 A1,再插 A2，依次类推。

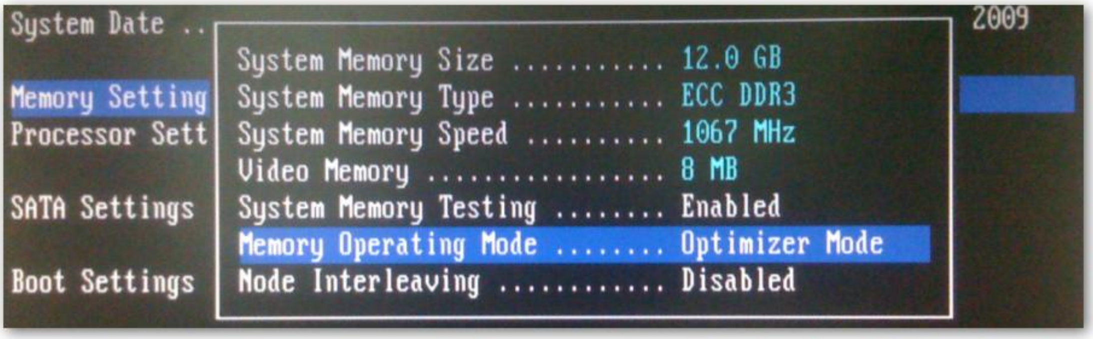
注：如果内存插法不对，又按照“2.1 选择 Memory Settings”进行了设置，系统启动的 BIOS 自检时会提示错误。

2. 开机BIOS设置

按 F2 进入 BIOS 设置：

1、选择 Memory Settings

设置 Memory Operating Mode 为 Optimizer Mode

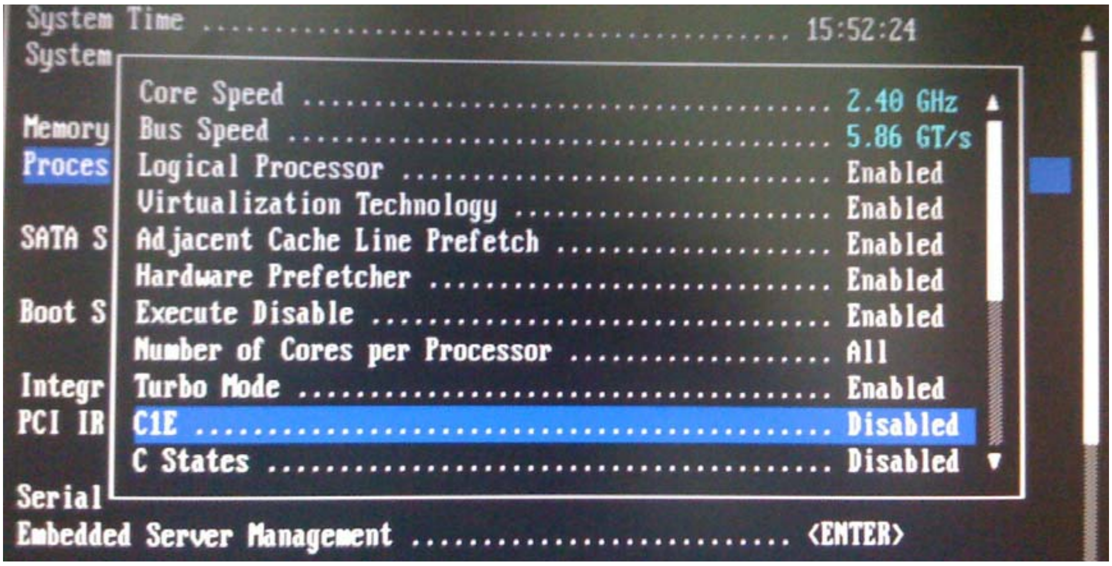


```
System Date ..                                                    2009

Memory Setting   System Memory Size ........... 12.0 GB
Processor Sett   System Memory Type ........... ECC DDR3
                 System Memory Speed .......... 1067 MHz
                 Video Memory ................. 8 MB
SATA Settings    System Memory Testing ........ Enabled
                 Memory Operating Mode ........ Optimizer Mode
Boot Settings    Node Interleaving ............ Disabled
```

2、选择 Processor Settings

设置 “C1E”和“C States” 为 Disabled

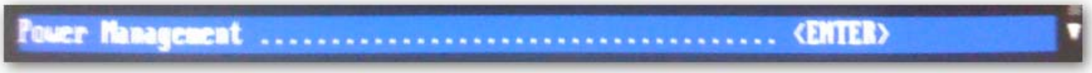
设置“Virtualization Technology”为 Enabled



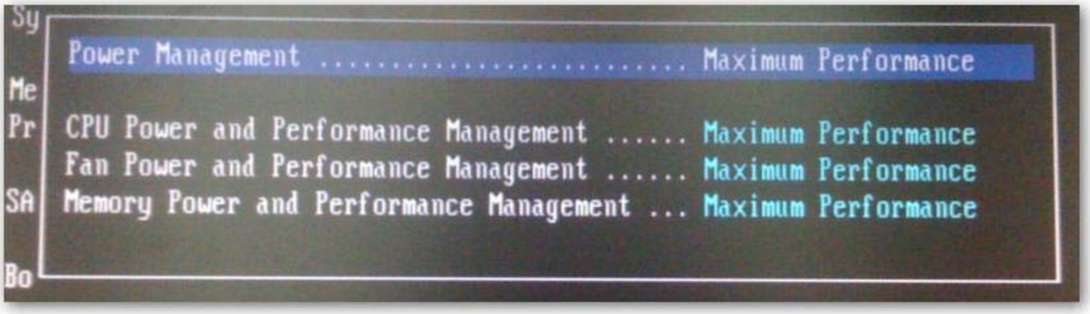
```
System Time ....................................... 15:52:24
System
        Core Speed ................................ 2.40 GHz
Memory  Bus Speed ................................. 5.86 GT/s
Proces  Logical Processor ......................... Enabled
        Virtualization Technology ................. Enabled
SATA S  Adjacent Cache Line Prefetch .............. Enabled
        Hardware Prefetcher ....................... Enabled
Boot S  Execute Disable ........................... Enabled
        Number of Cores per Processor ............. All
Integr  Turbo Mode ................................ Enabled
PCI IR  C1E ....................................... Disabled
        C States .................................. Disabled
Serial
Embedded Server Management .......................... <ENTER>
```

3、选择 Power Management

设置 Power Management 为 Maximum Performance



```
Power Management .................................. <ENTER>
```



```
Power Management ......................... Maximum Performance

CPU Power and Performance Management ...... Maximum Performance
Fan Power and Performance Management ...... Maximum Performance
Memory Power and Performance Management ... Maximum Performance
```

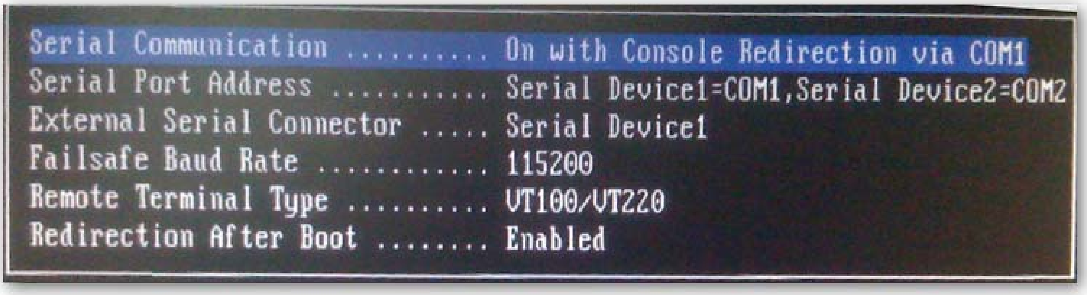
4、选择 Boot Sequence

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”



```
Serial Communication .......... On with Console Redirection via COM1
Serial Port Address ........... Serial Device1=COM1,Serial Device2=COM2
External Serial Connector ..... Serial Device1
Failsafe Baud Rate ............ 115200
Remote Terminal Type .......... VT100/VT220
Redirection After Boot ........ Enabled
```

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

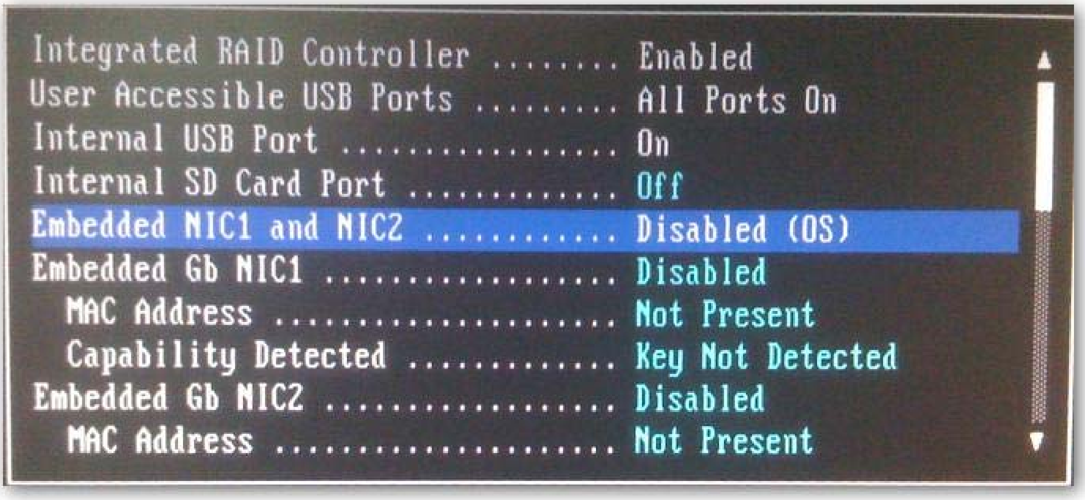
IWSA 5000

Embedded Gb NIC1:Disabled

Embedded Gb NIC 2: Enabled （只需要启用这一个，即主板集成的右边的那个网口）

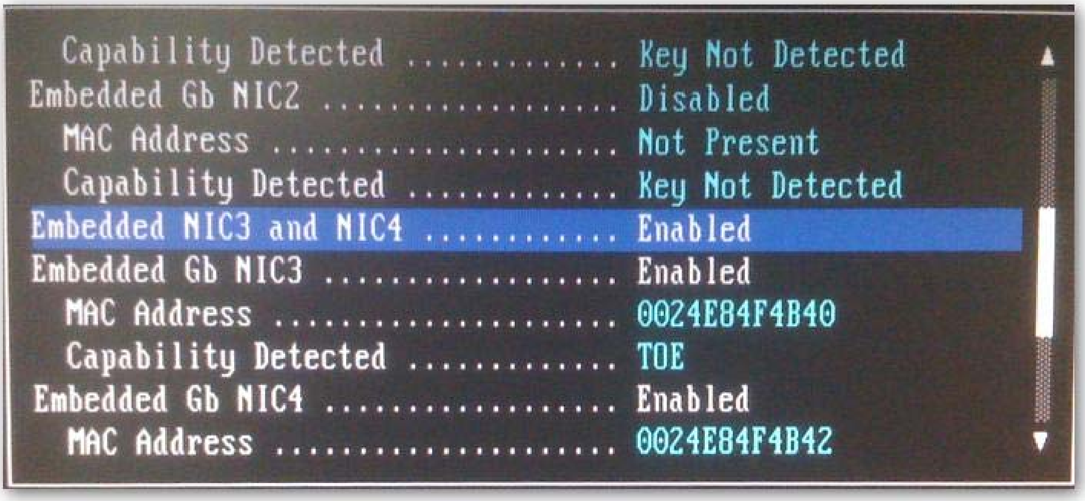
IWSA 3000, IWSA 6000 和 IWSA 10000

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



```
Integrated RAID Controller ........ Enabled
User Accessible USB Ports ......... All Ports On
Internal USB Port ................. On
Internal SD Card Port ............. Off
Embedded NIC1 and NIC2 ............ Disabled (OS)
Embedded Gb NIC1 .................. Disabled
  MAC Address ..................... Not Present
  Capability Detected ............. Key Not Detected
Embedded Gb NIC2 .................. Disabled
  MAC Address ..................... Not Present
```

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

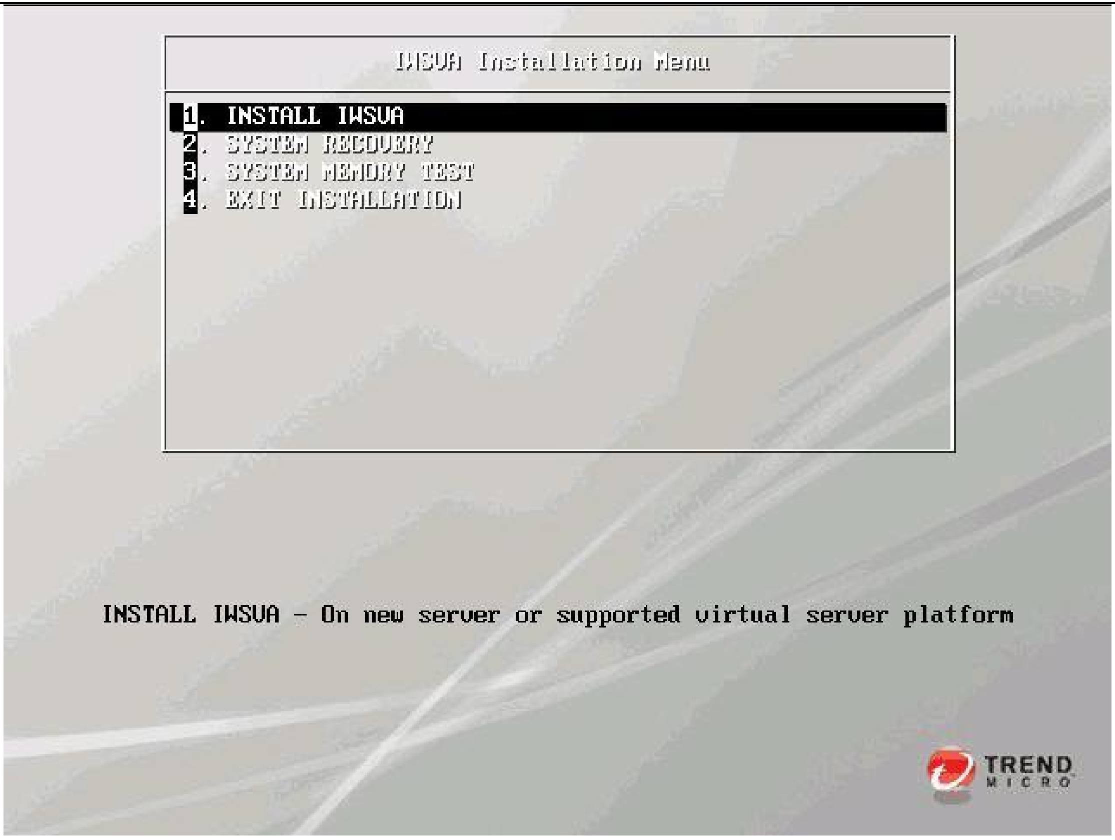


```
  Capability Detected ............. Key Not Detected
Embedded Gb NIC2 .................. Disabled
  MAC Address ..................... Not Present
  Capability Detected ............. Key Not Detected
Embedded NIC3 and NIC4 ............ Enabled
Embedded Gb NIC3 .................. Enabled
  MAC Address ..................... 0024E84F4B40
  Capability Detected ............. TOE
Embedded Gb NIC4 .................. Enabled
  MAC Address ..................... 0024E84F4B42
```

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.

3. 从CD-Rom引导

将光盘放入光驱后重启系统，看到如下界面：



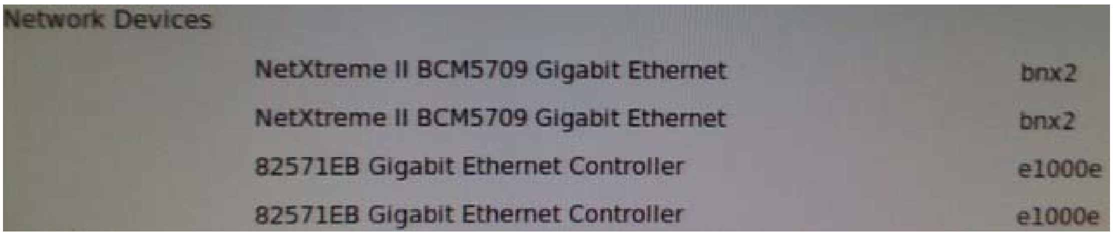
IWSVA Installation Menu

1. INSTALL IWSVA
2. SYSTEM RECOVERY
3. SYSTEM MEMORY TEST
4. EXIT INSTALLATION

INSTALL IWSVA - On new server or supported virtual server platform

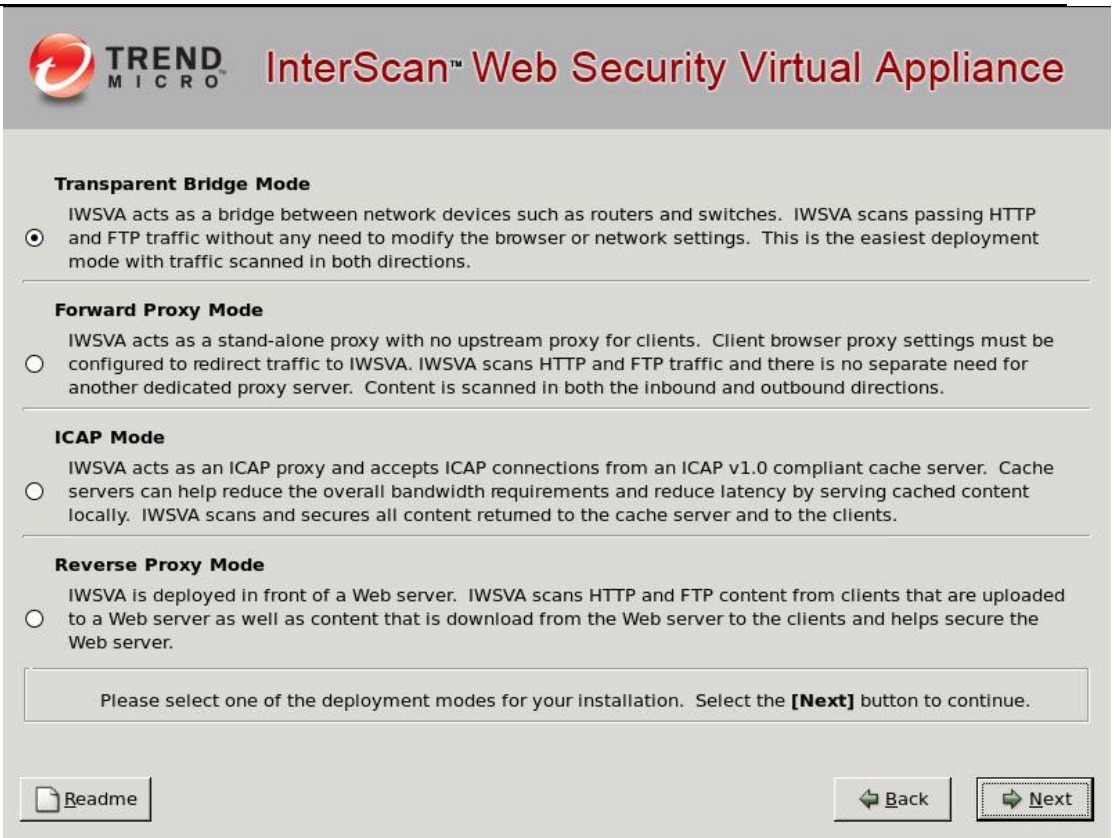
4. 准备安装

1） 从上图的菜单中选择 “1. INSTALL IWSVA”
2） 光驱会自动引导 IWSVA 安装进程
3） 在 License Agreement 界面上点击 “Accept”
4） Select your keyboard
5） Select which hard disk partition to install，取默认值点击“Next”；
6） 随后的出现的页面上会显示 IWSVA 安装程序检测到的硬件信息



```
Network Devices
          NetXtreme II BCM5709 Gigabit Ethernet          bnx2
          NetXtreme II BCM5709 Gigabit Ethernet          bnx2
          82571EB Gigabit Ethernet Controller            e1000e
          82571EB Gigabit Ethernet Controller            e1000e
```

7） Choose “Transparent Bridge Mode” from the mode deployment page then click Next button



TREND MICRO InterScan™ Web Security Virtual Appliance

Transparent Bridge Mode

● IWSVA acts as a bridge between network devices such as routers and switches. IWSVA scans passing HTTP and FTP traffic without any need to modify the browser or network settings. This is the easiest deployment mode with traffic scanned in both directions.

Forward Proxy Mode

○ IWSVA acts as a stand-alone proxy with no upstream proxy for clients. Client browser proxy settings must be configured to redirect traffic to IWSVA. IWSVA scans HTTP and FTP traffic and there is no separate need for another dedicated proxy server. Content is scanned in both the inbound and outbound directions.

ICAP Mode

○ IWSVA acts as an ICAP proxy and accepts ICAP connections from an ICAP v1.0 compliant cache server. Cache servers can help reduce the overall bandwidth requirements and reduce latency by serving cached content locally. IWSVA scans and secures all content retumed to the cache server and to the clients.

Reverse Proxy Mode

○ IWSVA is deployed in front of a Web server. IWSVA scans HTTP and FTP content from clients that are uploaded to a Web server as well as content that is download from the Web server to the clients and helps secure the Web server.

Please select one of the deployment modes for your installation. Select the **[Next]** button to continue.

8) Management Interface 参数配置

在硬件检测页面上点击 “Next” 后，界面上会显示网络参数配置信息

A. 选择 IWSVA 的 IP 地址的获取模式

B. 手工设置静态 IP 地址：

C. IP 192.168.252.1 Netmask 255.255.255.0

D. 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。

E. 如果选择手工配置网络参数，请务必配置一下参数：

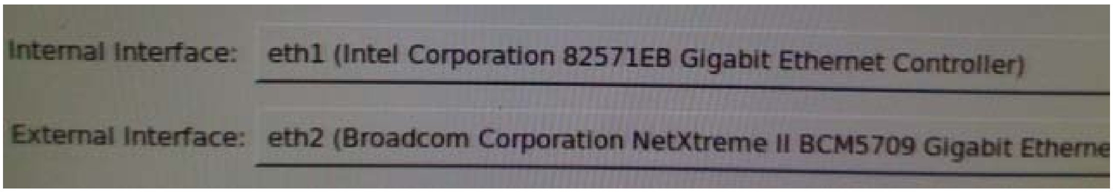
  a. 网关：192.168.252.254

  b. Primary DNS : 168.95.1.1

  c. Secondary DNS：

F. Internal Interface : eth1（请必须选择 eth1，不管界面显示的是哪个网卡）

G. External Interface : eth2（请必须选择 eth2，不管界面显示的是哪个网卡）



Internal Interface: eth1 (Intel Corporation 82571EB Gigabit Ethernet Controller)

External Interface: eth2 (Broadcom Corporation NetXtreme II BCM5709 Gigabit Etherne

5. 时区设置

1） 在网络参数配置页面点击“Next”就会随即显示时区配置页面
2） 为 IWSA 系统选择正确的时区 ： Asia/Chongqing

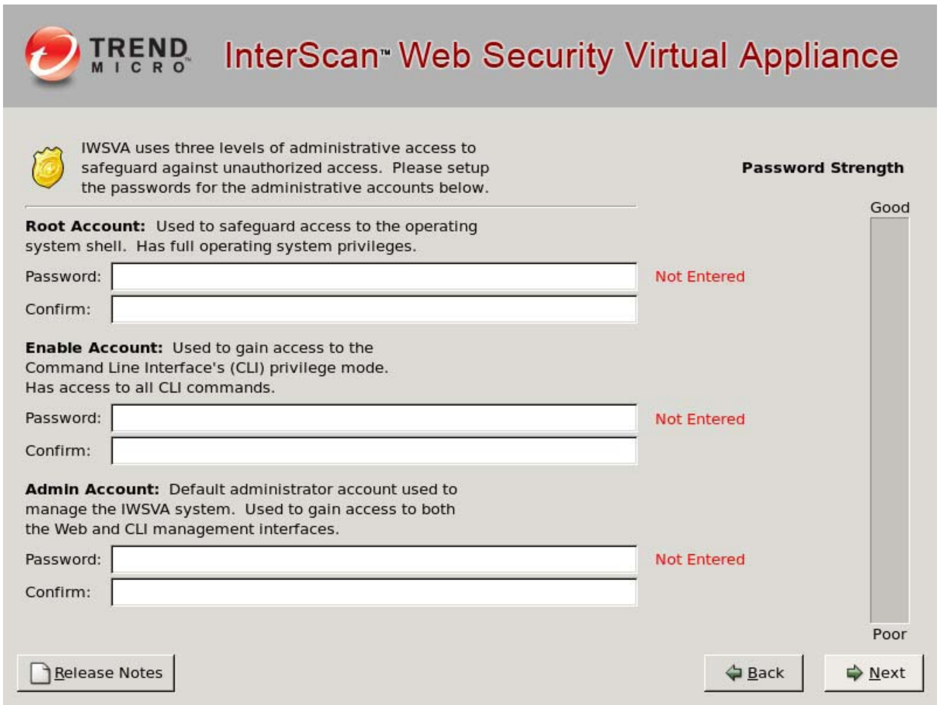
6. 设置口令

请配置成如下默认密码：

Root Account 密码： evita0

Enable Account 密码： evita0

Admin Account 密码： adminIWSS85


TREND MICRO InterScan™ Web Security Virtual Appliance

IWSVA uses three levels of administrative access to safeguard against unauthorized access. Please setup the passwords for the administrative accounts below.

Root Account: Used to safeguard access to the operating system shell. Has full operating system privileges.

Password: Not Entered

Confirm:

Enable Account: Used to gain access to the Command Line Interface's (CLI) privilege mode. Has access to all CLI commands.

Password: Not Entered

Confirm:

Admin Account: Default administrator account used to manage the IWSVA system. Used to gain access to both the Web and CLI management interfaces.

Password: Not Entered

Confirm:

7. 开始安装

点击 “Next” 开始安装进程

8. 安装完成

1. 安装结束后，系统会自动显示一个安装结束的页面.
    a. 界面上只有一个“Reboot”按钮
    b. 请打开光驱取出光盘
2. 点击“Reboot”按钮，系统将自动重启，

9. 安装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.tgz 文件 copy 到 IWSA 的 /var 目录下

setup.tgz 的下载目录
http://support.trendmicro.com.cn/TM-Product/Product/IWSA/3.1/1500_3000_5000_6000_10000/setup.tgz

```
# 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.tgz  /var     （注：/var 前面是空格）
# cd /var
# tar xzvf setup.tgz
```

3. MAC 地址绑定并更新 OS 补丁

```
# cd /var/setup/
# ./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/
# ./setup_2.sh
```

系统后有提示，等待操作完成后，更新工作完成。

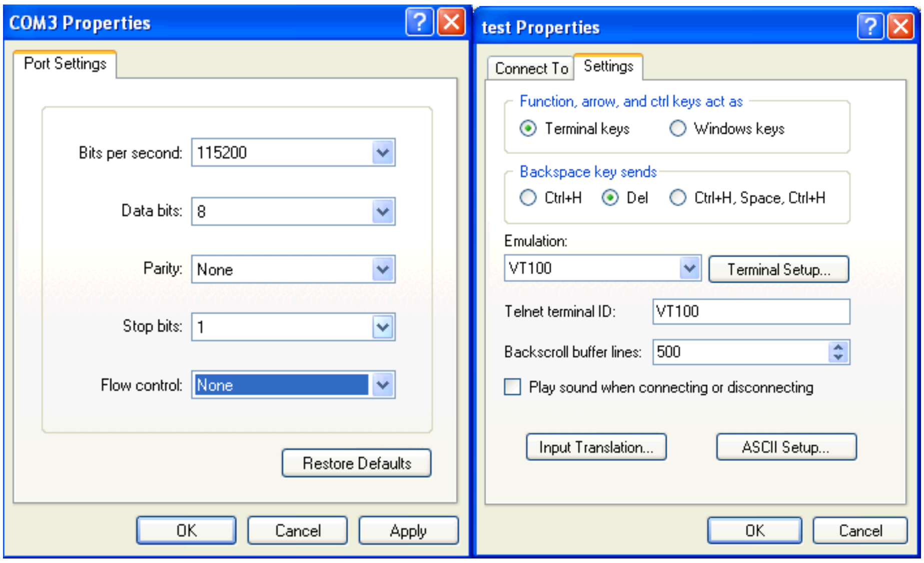
至此系统补丁及性能优化程序文件准备完成，可以 Ghost 系统盘了。

(注：IWSA 在流水线生产时就做这里，还需要按照“出厂检验步骤”完成后续工作。)

二　网络信息配置

1. 基本配置

1)　当你拿到一台新机器时，请先通过 COM 口进行连接，配置参数与 IWSA2500 相同：



COM3 Properties

Port Settings

Bits per second: 115200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

test Properties

Connect To | Settings

Function, arrow, and ctrl keys act as: ● Terminal keys ○ Windows keys

Backspace key sends: ○ Ctrl+H ● Del ○ Ctrl+H, Space, Ctrl+H

Emulation: VT100

Telnet terminal ID: VT100

Backscroll buffer lines: 500

□ Play sound when connecting or disconnecting

2)　默认机器是按透明网桥方式配置的，这时你需要确定你要采用哪种方式部署（透明、代理、ICAP、WCCP）。如果不采用透明方式部署，请执行如下步骤：

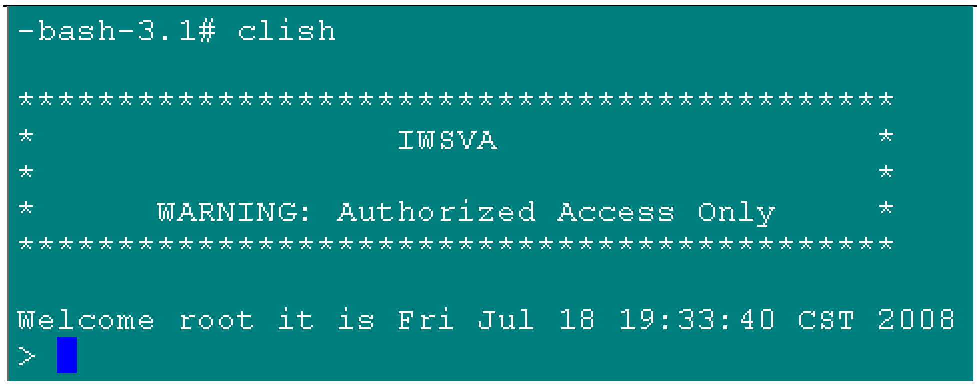
- ✧ #vi /etc/lanbypass.conf
- ✧ 将第二行的 BYPASS_MODE=AUTO 修改为 BYPASS_MODE=off，用:wq!保存退出
- ✧ #./etc/init.d/lanbypass start

然后访问Web界面（出厂地址为http://192.168.252.1:1812）进行模式更改，在非透明模式下，工作端口为扩展网卡的左边端口。

如果从非透明模式改成透明模式，则请将 BYPASS_MODE=off 修改为 BYPASS_MODE=AUTO，执行./etc/init.d/lanbypass start 后，再从 Web 界面上改。

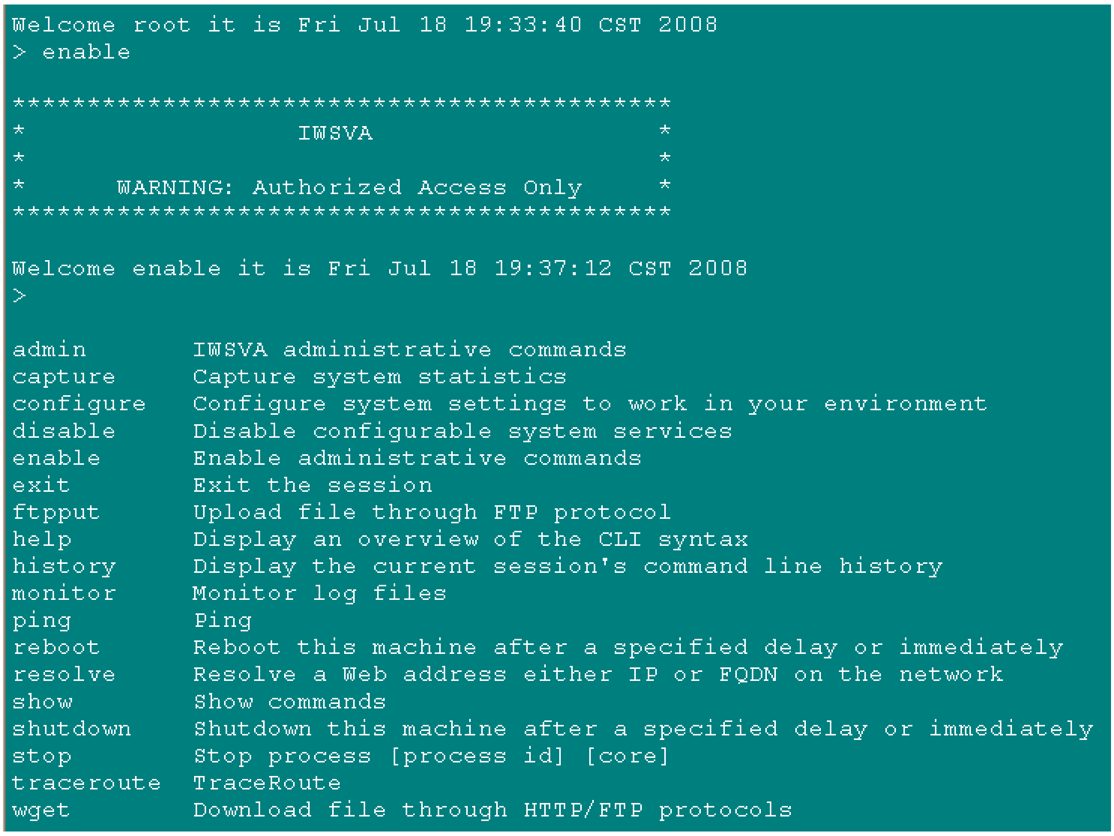
3)　部署模式配置好后，接下来就是配置网络地址等信息，基本步骤如下：

用 root 帐号登录执行“clish”命令，进入配置页面，如下图



```
-bash-3.1# clish

*******************************************
*                  IWSVA                  *
*                                         *
*      WARNING: Authorized Access Only    *
*******************************************

Welcome root it is Fri Jul 18 19:33:40 CST 2008
>
```

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



```
Welcome root it is Fri Jul 18 19:33:40 CST 2008
> enable

*******************************************
*                  IWSVA                  *
*                                         *
*      WARNING: Authorized Access Only    *
*******************************************

Welcome enable it is Fri Jul 18 19:37:12 CST 2008
>

admin        IWSVA administrative commands
capture      Capture system statistics
configure    Configure system settings to work in your environment
disable      Disable configurable system services
enable       Enable administrative commands
exit         Exit the session
ftpput       Upload file through FTP protocol
help         Display an overview of the CLI syntax
history      Display the current session's command line history
monitor      Monitor log files
ping         Ping
reboot       Reboot this machine after a specified delay or immediately
resolve      Resolve a Web address either IP or FQDN on the network
show         Show commands
shutdown     Shutdown this machine after a specified delay or immediately
stop         Stop process [process id] [core]
traceroute   TraceRoute
wget         Download file through HTTP/FTP protocols
```

其中configure命令支持如下参数：bridge date dns ethernet hostname ip ldap ntp password proxy redirect timezone

2. 修改工作端口地址（拿到机器后必做动作）

在上图中，使用 configure ip static x.x.x.x 掩码 网关 （中间用空格）可修改地址。

3. 修改DNS（拿到机器后必做动作）

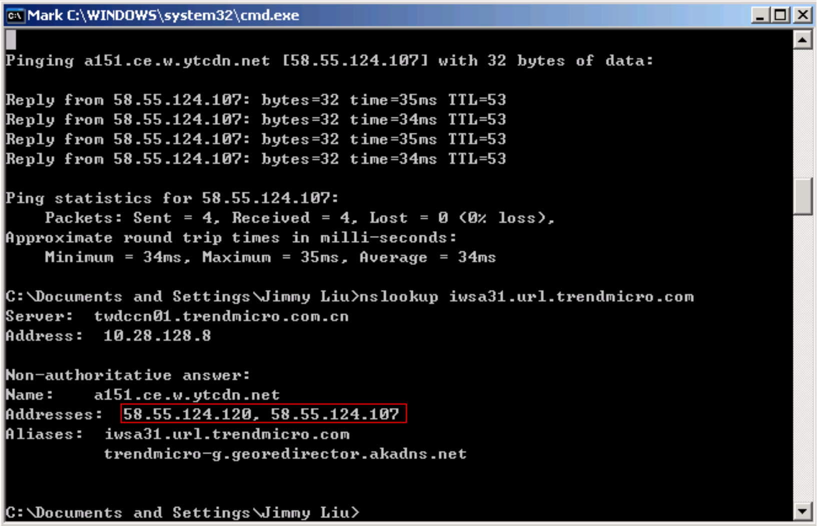
在上图中，使用 configure DNS x.x.x.x 可修改 DNS（中间用空格）

如果启用了 WRS/URLFilter, 请检查 DNS 是否可以解析域名

iwsa31.url.trendmicro.com

如果无法解析，请安装下面步骤在/etc/hosts 中添加域名的到 IP 的解析，

1. 在客户环境中的机器上运行 nslookup iwsa31.url.trendmicro.com

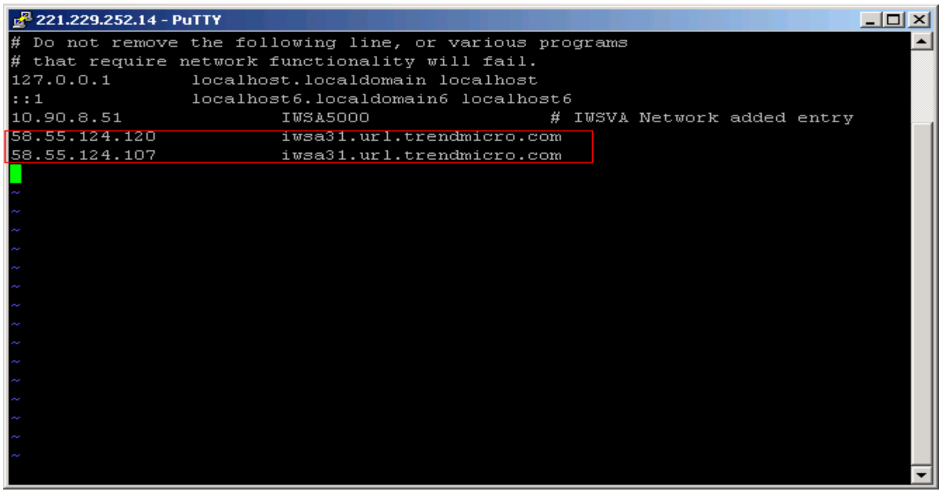


```
Pinging a151.ce.w.ytcdn.net [58.55.124.107] with 32 bytes of data:

Reply from 58.55.124.107: bytes=32 time=35ms TTL=53
Reply from 58.55.124.107: bytes=32 time=34ms TTL=53
Reply from 58.55.124.107: bytes=32 time=35ms TTL=53
Reply from 58.55.124.107: bytes=32 time=34ms TTL=53

Ping statistics for 58.55.124.107:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 34ms, Maximum = 35ms, Average = 34ms

C:\Documents and Settings\Jimmy Liu>nslookup iwsa31.url.trendmicro.com
Server:  twdccn01.trendmicro.com.cn
Address:  10.28.128.8

Non-authoritative answer:
Name:    a151.ce.w.ytcdn.net
Addresses:  58.55.124.120, 58.55.124.107
Aliases:  iwsa31.url.trendmicro.com
          trendmicro-g.georedirector.akadns.net


C:\Documents and Settings\Jimmy Liu>
```

查看解析到的 ip 地址，例如上图的 58.55.124.120 和 58.55.124.107

2. 在 IWSA 的 Linux shell 中运行：vi /etc/hosts，添加如下两行：

```
58.55.124.120          iwsa31.url.trendmicro.com
58.55.124.107          iwsa31.url.trendmicro.com
```



```
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1       localhost.localdomain localhost
::1             localhost6.localdomain6 localhost6
10.90.8.51              IWSA5000                # IWSVA Network added entry
58.55.124.120           iwsa31.url.trendmicro.com
58.55.124.107           iwsa31.url.trendmicro.com

~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
```

4. 启用ping（默认开启）

用 vi 编辑 /etc/iscan/network.ini
将 enable_ping=no 改成 enable_ping=yes
然后执行#/etc/init.d/network restart

5. 修改工作端口（可选）

IWSA 默认支持 80 和 8080,修改可通过在 clish 中执行 configure http_redirect port 来实现。

6. IWSA抓包（可选）

✧ 抓所有流量：

```
tcpdump -i br0 tcp and port 80 -s 1512 -w /var/iwss/UserDumps/aaa.pcap
```

✧ 开两个 SSH 终端，在 bridge 的两个网口分别抓包：

```
tcpdump -i eth1 tcp and port 80 -s 1512 -w /var/iwss/UserDumps/eth1.pcap
tcpdump -i eth2 tcp and port 80 -s 1512 -w /var/iwss/UserDumps/eth2.pcap
```

✧ 抓特定客户机流量：

```
tcpdump -i br0 tcp and port 80 host x.x.x.x  -s 1512 -w /var/iwss/UserDumps/aaa.pcap
```

注：host 后面的 x.x.x.x 为客户机的 IP，请替换为真实 IP

启用以上命令后，用客户机浏览网站，浏览一段时间后，然后用 Ctrl+c 终止抓包进程，然后从 Web 界面上的 support 页面上将 aaa.pcap 文件下载到本地进行分析。

三　正常透明模式配置步骤（在第一章中的安装脚本setup.tgz已经自动完成该步骤）

1. 登录Shell

可以使用 SSH 或串口连接 IWSA 的 IP 地址.

登录帐号：root ， 密码:evita0

2. 绑定Br0 的两个端口（bypass网卡）

进入 Linux Shell 后，然后按照如下步骤进行：

```
#cd /var/setup/abc
#./gen_iftab.sh        （注：命令前面有个点）
```

用#cat /etc/iftab 命令查看 iftab 的内容，应该可以看到 MAC 地址和网卡描述，里面至少要有 eth1 和 eth2

```
#reboot         ----重启机器
```

3. 激活工作端口Bypass功能

```
> chkconfig --add lanbypass
> chkconfig lanbypass on
> /etc/init.d/lanbypass start
```

以上 3 个命令请完全照以上所写执行，执行命令是因为新网卡加电后，并不具备 bypass 功能，需要用以上命令激活后才可以在异常时自动 bypass，执行完后不需要重启设备。
非透明应用模式不需要启用此项功能。

四　配置单独管理口步骤（通常不用）

仅在前面配置的网桥地址不能上网或用户要求必须具备管理端口与管理网相连的时候才需配置。

1. 编辑/etc/iscan/network.ini

vi /etc/iscan/network.ini

ifname_mgt=eth0　（去掉这句前面的注释符号，启用本句命令，它对应的网口为服务器自带的右边的那个端口）

mgt_ip=192.168.252.1　（修改为用户提供的管理 IP）

mgt_netmask=255.255.255.0（修改为用户提供的管理网掩码）

#mgt_gw=192.168.252.254　（修改为用户提供的管理网网关）**改动要慎重！**

特别提醒 1：如果你将前面的注释符去掉，将更改工作端口网络配置的网关，所以如果你之前配置的工作端口可以上网，请保持前面的注释符#，如果你之前配置的工作端口的IP是随便写的，并不能上网，这个地方请去掉注释符，配成管理网的网关。

特别提醒 2：如果你启用这个网关配置后又注释掉了它，你必须用前面clish命令进入命令行，采用 “configure ip static x.x.x.x 掩码 网关”来配置正确的网关。

2. 为管理端口配置静态路由

vi /etc/sysconfig/network-scripts/eth0.route

增加如下图所示格式：

ADDRESS0=10.1.119.0　（远程的某个网段）

NETMASK0=255.255.255.0

GATEWAY0=192.168.252.254　（IWSA 管理端口网关）

```
ADDRESS1=10.2.202.0     （远程的另一个网段）
NETMASK1=255.255.255.0
GATEWAY1=192.168.252.254    （IWSA 管理端口网关）
```

加完所有网段后用:wq!命令保存退出。

```
/etc/init.d/network restart       （执行后立即生效）
```

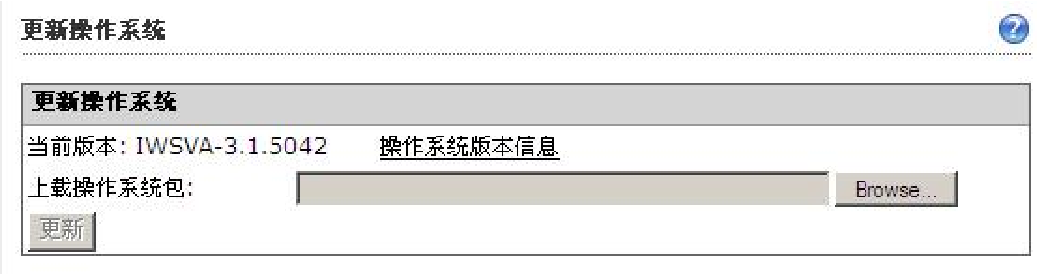
如果再次需要修改管理口 IP，请重复上面两个步骤修改即可。

IWSA测试配置建议

◆ 测试前的准备：

- ✧ 如果采用的是测试机，建议对测试机系统进行重新灌装；

- ✧ 通过 Web 界面，升级最新的 OS 和 AP 补丁：

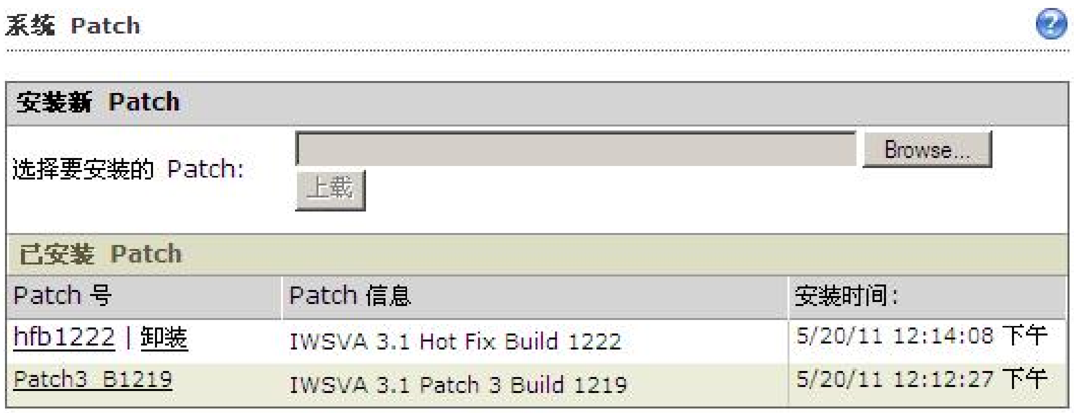


更新操作系统

更新操作系统

当前版本：IWSVA-3.1.5042　　操作系统版本信息

上载操作系统包：



系统 Patch

安装新 Patch

选择要安装的 Patch：

已安装 Patch

Patch 号	Patch 信息	安装时间：
hfb1222 | 卸载	IWSVA 3.1 Hot Fix Build 1222	5/20/11 12:14:08 下午
Patch3_B1219	IWSVA 3.1 Patch 3 Build 1219	5/20/11 12:12:27 下午

◆ 测试流程说明：

1. 在用户初次测试时，我们先启用HTTP/FTP Scanning、URL Blocking功能，其它如Web Reputation、Applets/ActiveX Security、URL Filtering功能暂不启用，待运行平稳一段时间后，再根据用户要求决定是否启用；

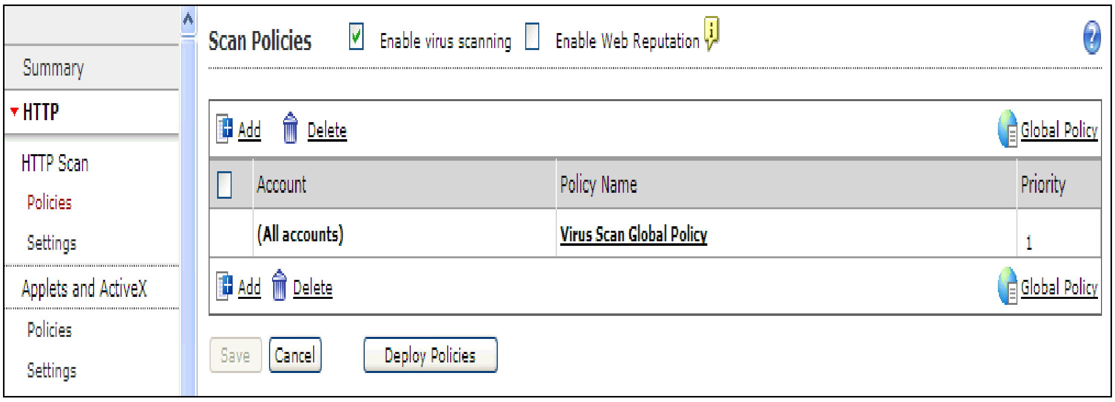
2. 在正式上线前，建议先在用户网络环境中做小范围测试，尽可能根据用户的网络特点来做测试；

3. 在正式上线时，建议将IWSA所有扫描功能关闭(<u>在Policy中关闭，但不能关闭Summary页面的HTTP Traffic/FTP Traffic，关闭则会阻断网络</u>)，接入网络后，待确认网络通讯正常，此时再逐项启用功能(此时启用

HTTP/FTP Scanning、URL Blocking功能，其它功能暂不启用）。

◆ 初步测试配置建议：

1. 测试初期配置启用HTTP virus scanning，暂不启用Web Reputation：

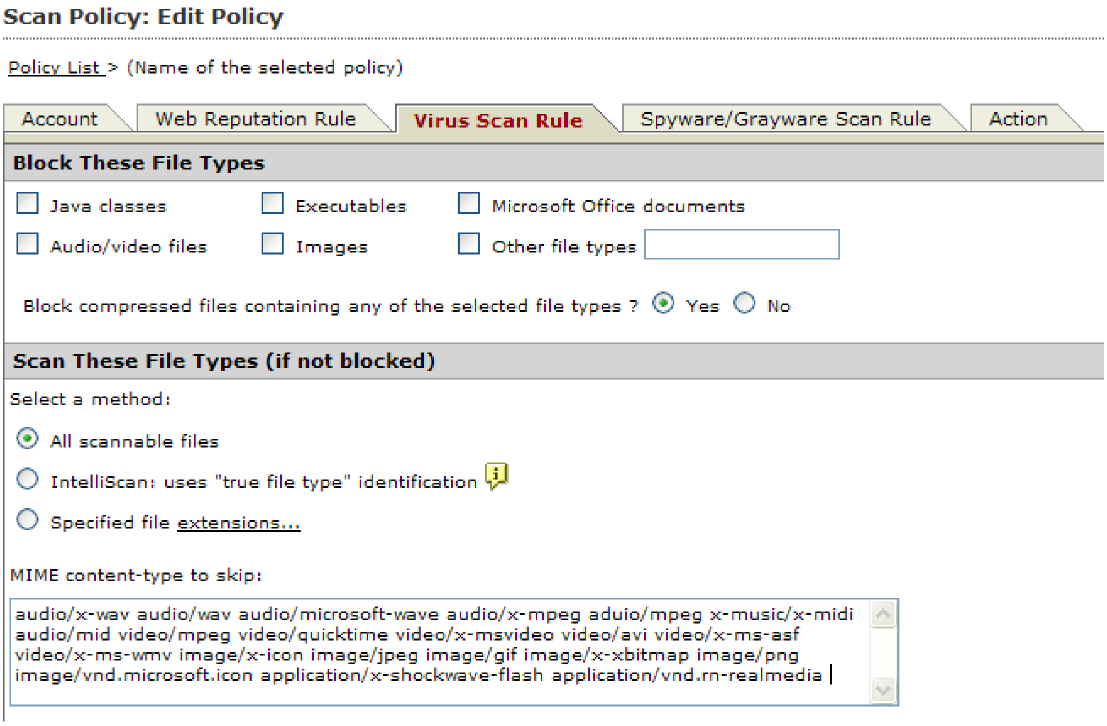


Scan Policies ☑ Enable virus scanning □ Enable Web Reputation

□	Account	Policy Name	Priority
	(All accounts)	Virus Scan Global Policy	1

2. 配置HTTP扫描所有文件，但配置HTTP SKIP 以下MIME类型：

audio/x-wav audio/wav audio/microsoft-wave audio/x-mpeg audio/mpeg x-music/x-midi audio/mid video/mpeg video/quicktime video/x-msvideo video/avi video/x-ms-asf video/x-ms-wmv image/x-icon image/jpeg image/gif image/x-xbitmap image/png image/vnd.microsoft.icon application/x-shockwave-flash application/vnd.rn-realmedia



Scan Policy: Edit Policy

Policy List > (Name of the selected policy)

Block These File Types

□ Java classes □ Executables □ Microsoft Office documents

□ Audio/video files □ Images □ Other file types

Block compressed files containing any of the selected file types ? ● Yes ○ No

Scan These File Types (if not blocked)

Select a method:

● All scannable files

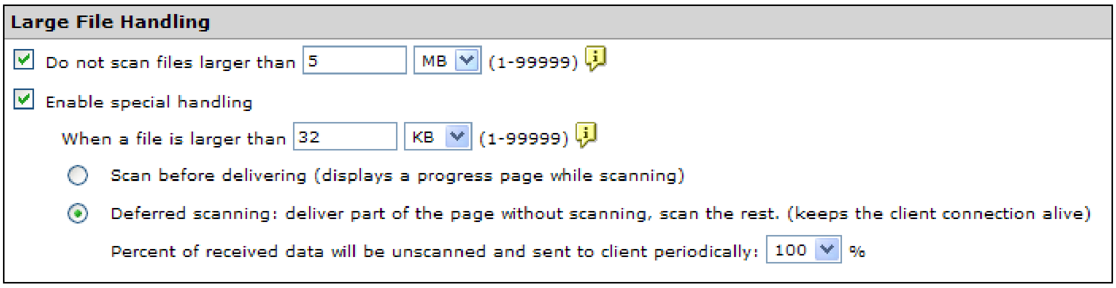
○ IntelliScan: uses "true file type" identification

○ Specified file extensions...

MIME content-type to skip:

audio/x-wav audio/wav audio/microsoft-wave audio/x-mpeg aduio/mpeg x-music/x-midi audio/mid video/mpeg video/quicktime video/x-msvideo video/avi video/x-ms-asf video/x-ms-wmv image/x-icon image/jpeg image/gif image/x-xbitmap image/png image/vnd.microsoft.icon application/x-shockwave-flash application/vnd.rn-realmedia

3. 配置HTTP不扫描超过5M的文件、配置HTTP对超过32KB的文件采用Deferred scanning，转发率为100%，配置如下图所示；



Large File Handling

☑ Do not scan files larger than 5 MB (1-99999)

☑ Enable special handling

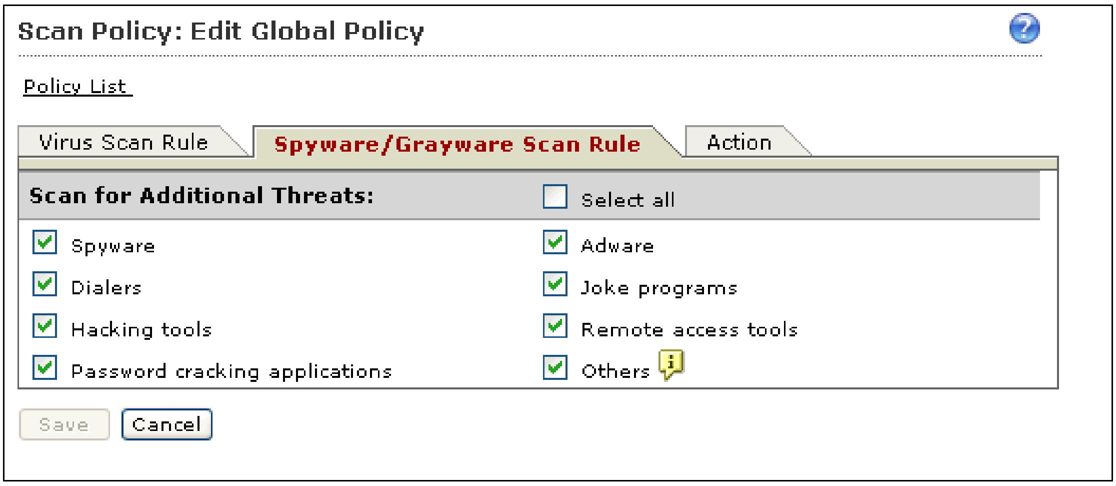
When a file is larger than 32 KB (1-99999)

○ Scan before delivering (displays a progress page while scanning)

● Deferred scanning: deliver part of the page without scanning, scan the rest. (keeps the client connection alive)

Percent of received data will be unscanned and sent to client periodically: 100 %

4. 配置HTTP扫描Spyware/Grayware；



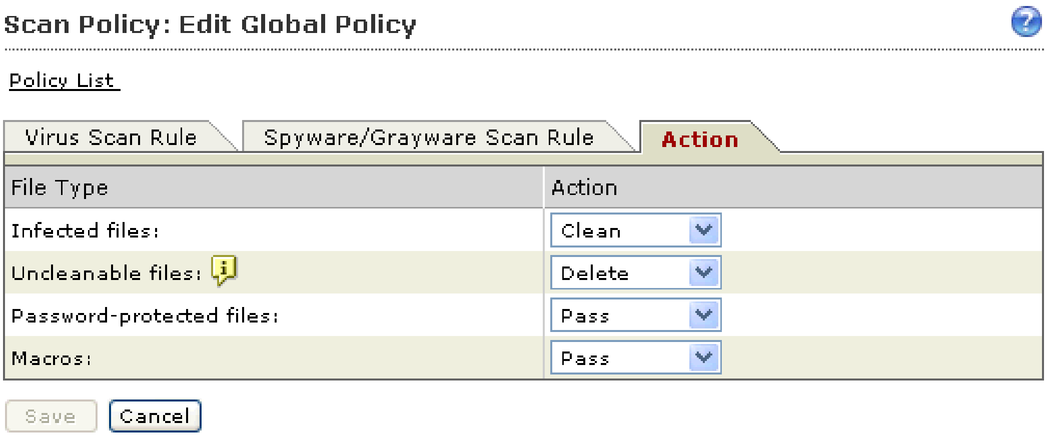
Scan Policy: Edit Global Policy

Policy List

Virus Scan Rule | **Spyware/Grayware Scan Rule** | Action

Scan for Additional Threats: □ Select all

☑ Spyware	☑ Adware
☑ Dialers	☑ Joke programs
☑ Hacking tools	☑ Remote access tools
☑ Password cracking applications	☑ Others



Scan Policy: Edit Global Policy

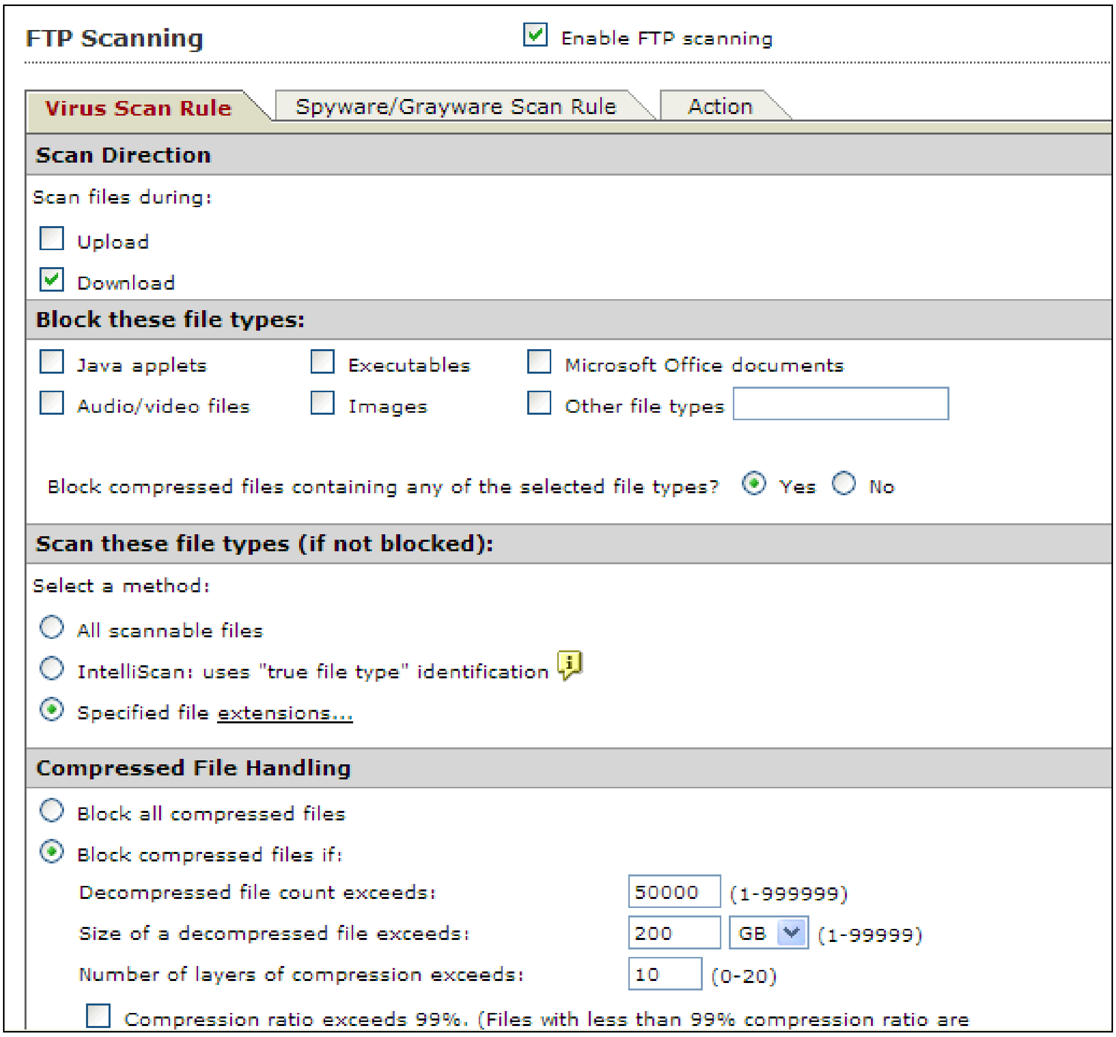
Policy List

Virus Scan Rule | Spyware/Grayware Scan Rule | **Action**

File Type	Action
Infected files:	Clean
Uncleanable files:	Delete
Password-protected files:	Pass
Macros:	Pass

注：配置完成后，请在Scan Policies界面中点击“Deploy Policies”，以使得新配置马上应用。

5. 配置FTP只扫描下载文件、配置扫描特定类型文件、超过5MB不扫描，转发率为100%(与HTTP配置相同)，配置扫描Spyware、配置采用默认处理动作；



FTP Scanning ☑ Enable FTP scanning

Scan Direction

Scan files during:

☐ Upload

☑ Download

Block these file types:

☐ Java applets ☐ Executables ☐ Microsoft Office documents

☐ Audio/video files ☐ Images ☐ Other file types

Block compressed files containing any of the selected file types? ● Yes ○ No

Scan these file types (if not blocked):

Select a method:

○ All scannable files

○ IntelliScan: uses "true file type" identification

● Specified file extensions...

Compressed File Handling

○ Block all compressed files

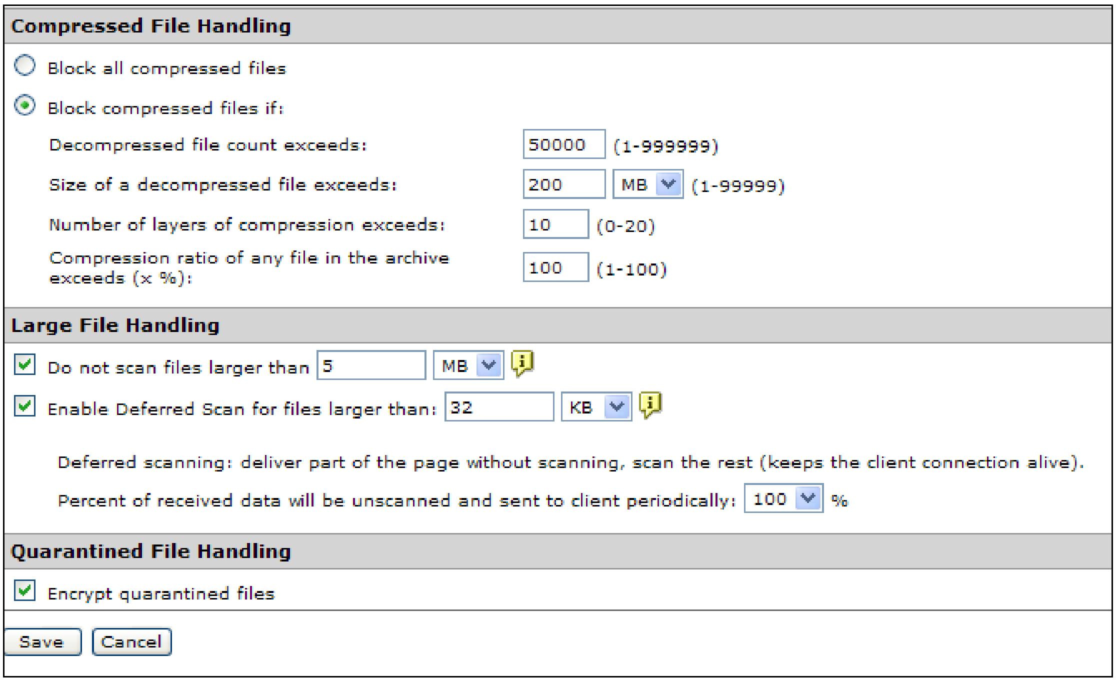
● Block compressed files if:

Decompressed file count exceeds: 50000 (1-999999)

Size of a decompressed file exceeds: 200 GB (1-99999)

Number of layers of compression exceeds: 10 (0-20)

☐ Compression ratio exceeds 99%. (Files with less than 99% compression ratio are



Compressed File Handling

○ Block all compressed files

● Block compressed files if:

Decompressed file count exceeds: 50000 (1-999999)

Size of a decompressed file exceeds: 200 MB (1-99999)

Number of layers of compression exceeds: 10 (0-20)

Compression ratio of any file in the archive exceeds (x %): 100 (1-100)

Large File Handling

☑ Do not scan files larger than 5 MB

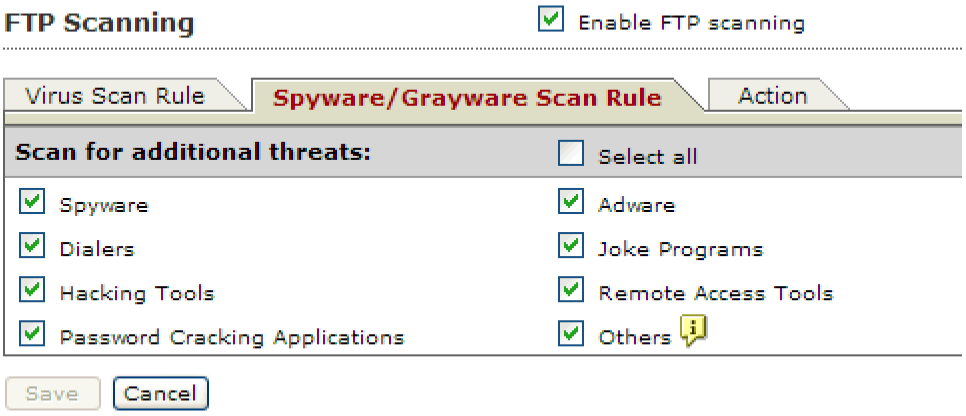
☑ Enable Deferred Scan for files larger than: 32 KB

Deferred scanning: deliver part of the page without scanning, scan the rest (keeps the client connection alive).

Percent of received data will be unscanned and sent to client periodically: 100 %

Quarantined File Handling

☑ Encrypt quarantined files



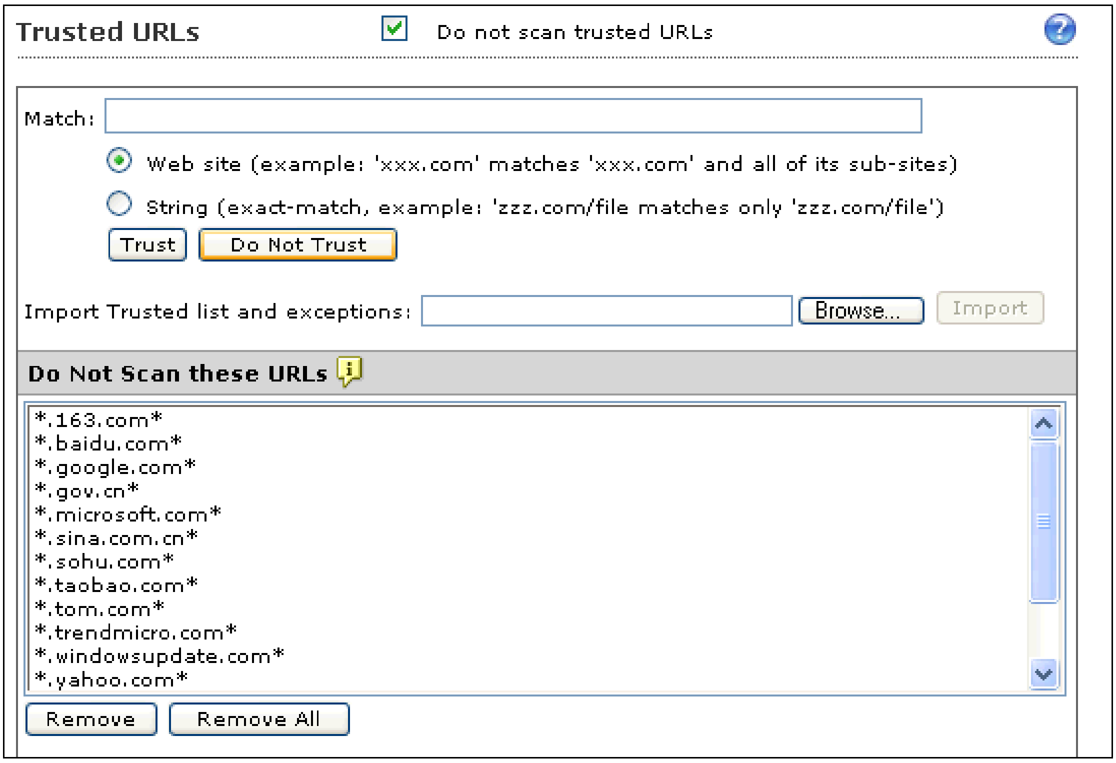
FTP Scanning ☑ Enable FTP scanning

Virus Scan Rule | Spyware/Grayware Scan Rule | Action

Scan for additional threats: □ Select all

☑ Spyware ☑ Adware
☑ Dialers ☑ Joke Programs
☑ Hacking Tools ☑ Remote Access Tools
☑ Password Cracking Applications ☑ Others

6. URL Blocking建议将常用的网址加在白名单中，同时启用Pattern File对URL进行Blocking，配置建议如下：



Trusted URLs ☑ Do not scan trusted URLs

Match:

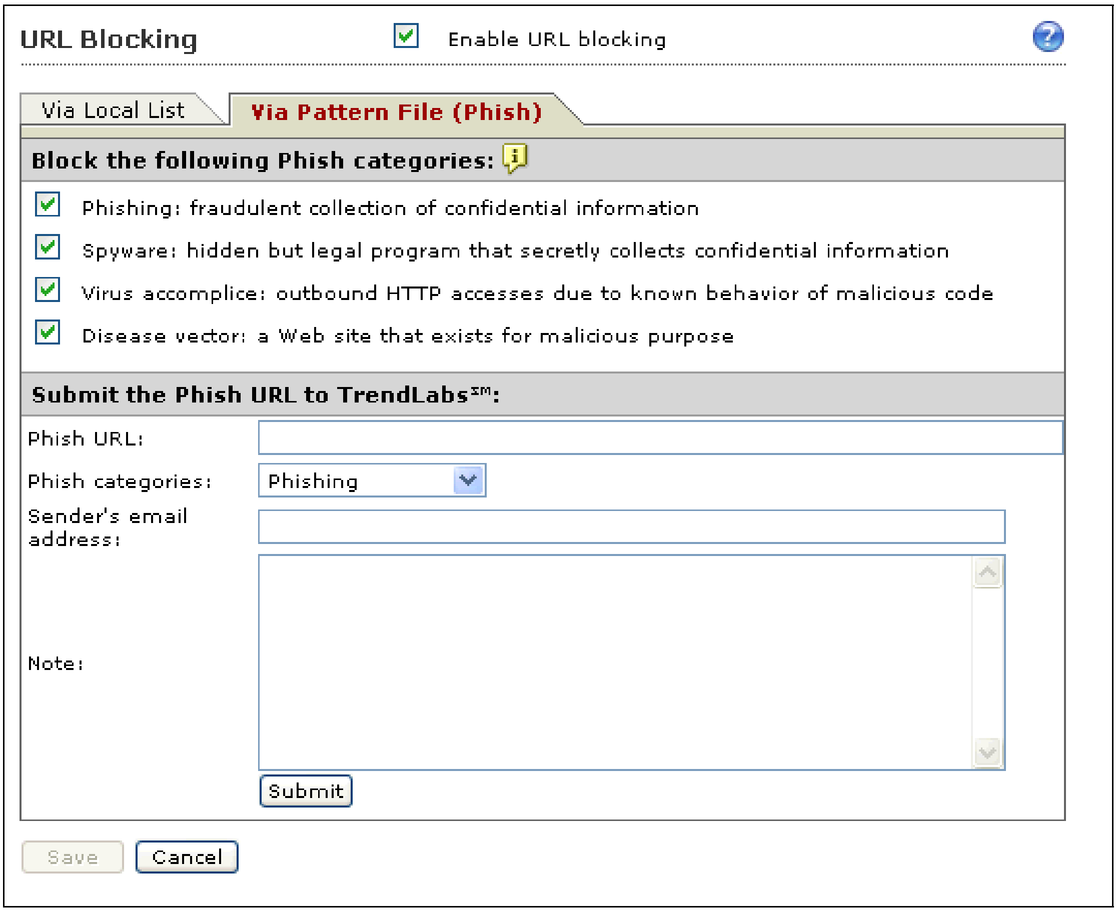
● Web site (example: 'xxx.com' matches 'xxx.com' and all of its sub-sites)

○ String (exact-match, example: 'zzz.com/file matches only 'zzz.com/file')

Import Trusted list and exceptions:

Do Not Scan these URLs

```
*.163.com*
*.baidu.com*
*.google.com*
*.gov.cn*
*.microsoft.com*
*.sina.com.cn*
*.sohu.com*
*.taobao.com*
*.tom.com*
*.trendmicro.com*
*.windowsupdate.com*
*.yahoo.com*
```



URL Blocking ☑ Enable URL blocking

Block the following Phish categories:

☑ Phishing: fraudulent collection of confidential information

☑ Spyware: hidden but legal program that secretly collects confidential information

☑ Virus accomplice: outbound HTTP accesses due to known behavior of malicious code

☑ Disease vector: a Web site that exists for malicious purpose

Submit the Phish URL to TrendLabs℠:

Phish URL:

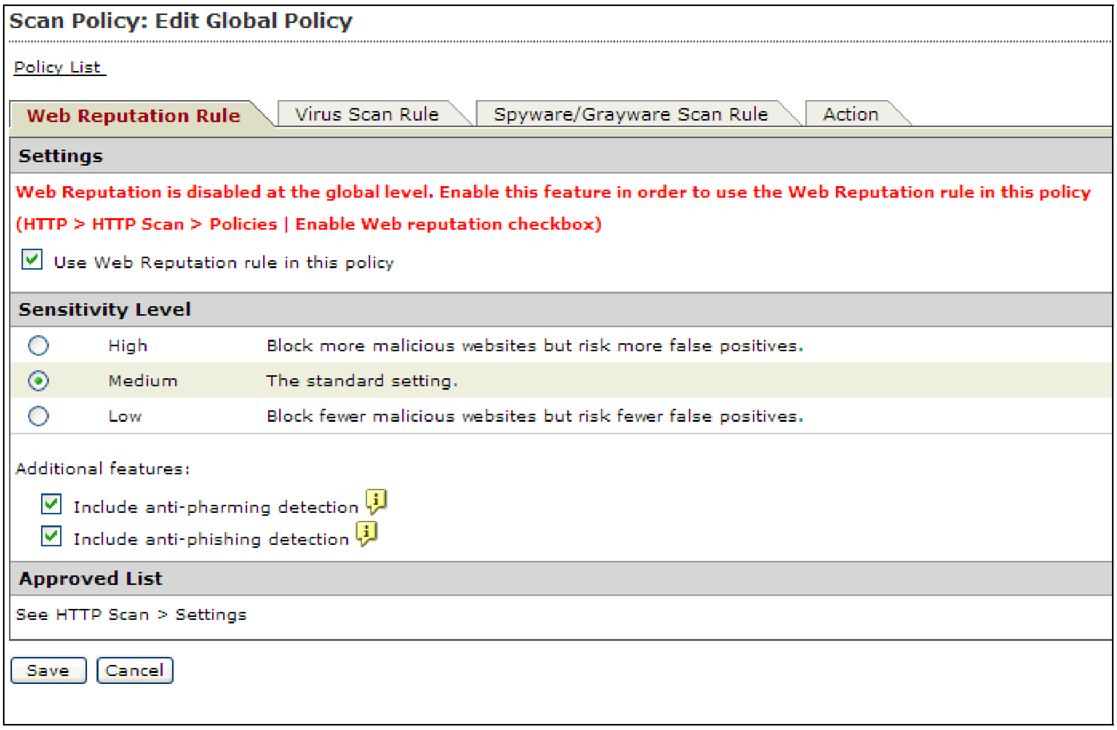
Phish categories: Phishing

Sender's email address:

Note:

◆ 深入测试配置建议：

7. 如果启用Web Reputation，请首先确认您配置的DNS服务器响应速度足够快，然后在Scan Policies右边选择Enable Web Reputation，在策略中配置如下：



Scan Policy: Edit Global Policy

Policy List

Settings

Web Reputation is disabled at the global level. Enable this feature in order to use the Web Reputation rule in this policy (HTTP > HTTP Scan > Policies | Enable Web reputation checkbox)

☑ Use Web Reputation rule in this policy

Sensitivity Level

○	High	Block more malicious websites but risk more false positives.
●	Medium	The standard setting.
○	Low	Block fewer malicious websites but risk fewer false positives.

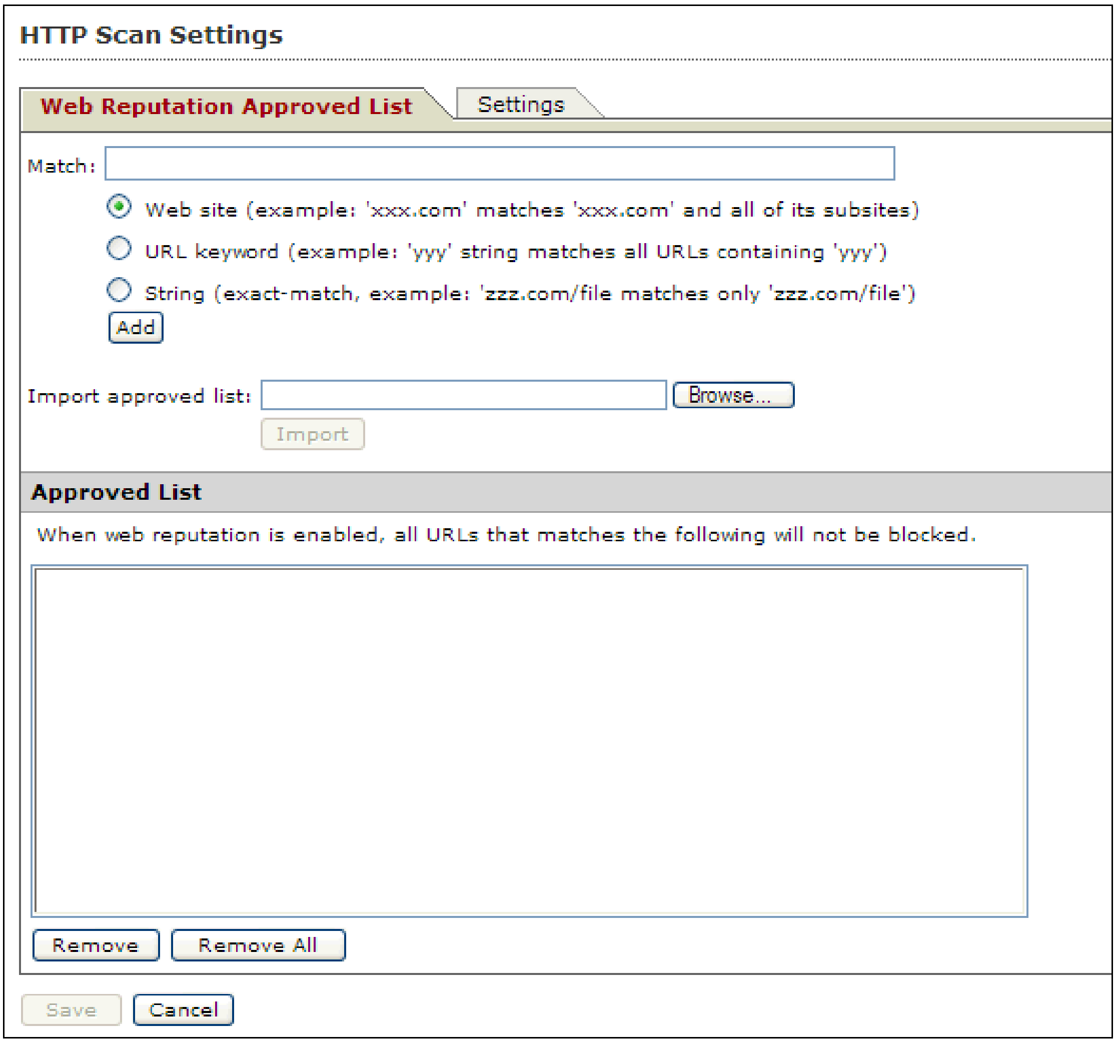
Additional features:

☑ Include anti-pharming detection

☑ Include anti-phishing detection

Approved List

See HTTP Scan > Settings



HTTP Scan Settings

Match:

● Web site (example: 'xxx.com' matches 'xxx.com' and all of its subsites)

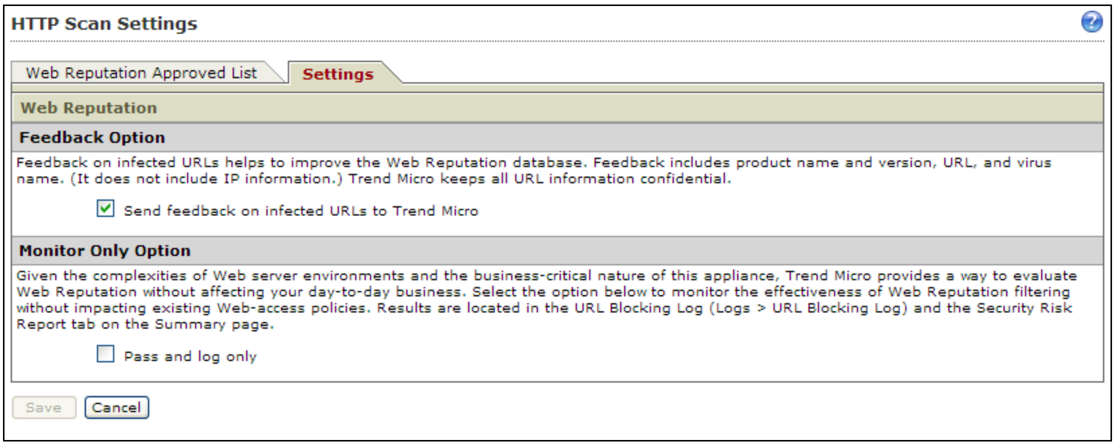
○ URL keyword (example: 'yyy' string matches all URLs containing 'yyy')

○ String (exact-match, example: 'zzz.com/file matches only 'zzz.com/file')

Import approved list:

Approved List

When web reputation is enabled, all URLs that matches the following will not be blocked.



HTTP Scan Settings

Web Reputation Approved List | **Settings**

Web Reputation

Feedback Option

Feedback on infected URLs helps to improve the Web Reputation database. Feedback includes product name and version, URL, and virus name. (It does not include IP information.) Trend Micro keeps all URL information confidential.

☑ Send feedback on infected URLs to Trend Micro

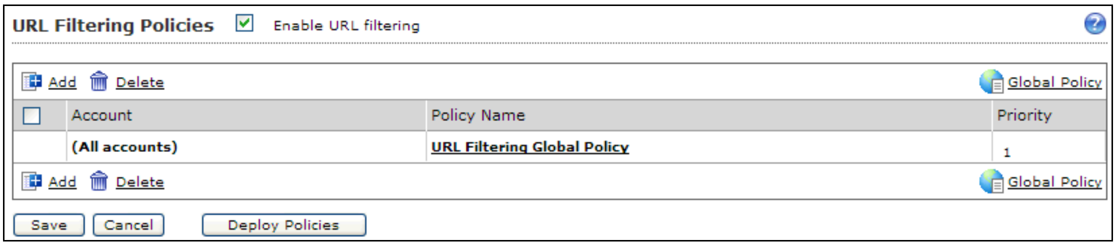
Monitor Only Option

Given the complexities of Web server environments and the business-critical nature of this appliance, Trend Micro provides a way to evaluate Web Reputation without affecting your day-to-day business. Select the option below to monitor the effectiveness of Web Reputation filtering without impacting existing Web-access policies. Results are located in the URL Blocking Log (Logs > URL Blocking Log) and the Security Risk Report tab on the Summary page.

□ Pass and log only

Save | Cancel

8. URL Filtering按如下建议配置(第一次上线不启用)：



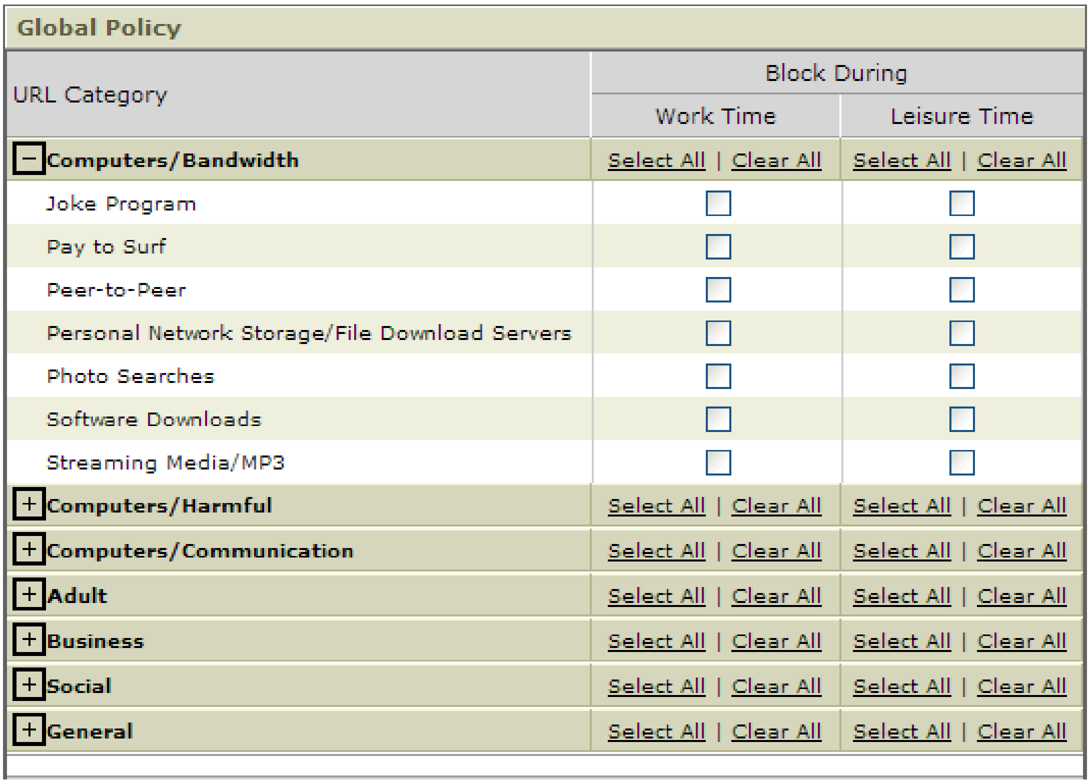
URL Filtering Policies ☑ Enable URL filtering

Add | Delete | Global Policy

□	Account	Policy Name	Priority
	(All accounts)	**URL Filtering Global Policy**	1

Add | Delete | Global Policy

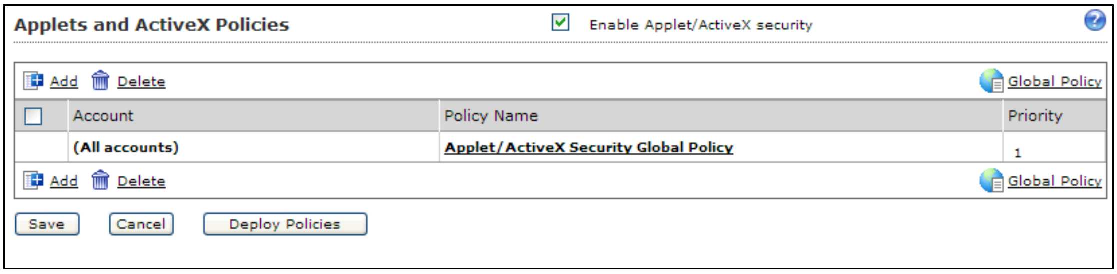
Save | Cancel | Deploy Policies



Global Policy

URL Category	Block During	
	Work Time	Leisure Time
− Computers/Bandwidth	Select All | Clear All	Select All | Clear All
Joke Program	□	□
Pay to Surf	□	□
Peer-to-Peer	□	□
Personal Network Storage/File Download Servers	□	□
Photo Searches	□	□
Software Downloads	□	□
Streaming Media/MP3	□	□
+ Computers/Harmful	Select All | Clear All	Select All | Clear All
+ Computers/Communication	Select All | Clear All	Select All | Clear All
+ Adult	Select All | Clear All	Select All | Clear All
+ Business	Select All | Clear All	Select All | Clear All
+ Social	Select All | Clear All	Select All | Clear All
+ General	Select All | Clear All	Select All | Clear All

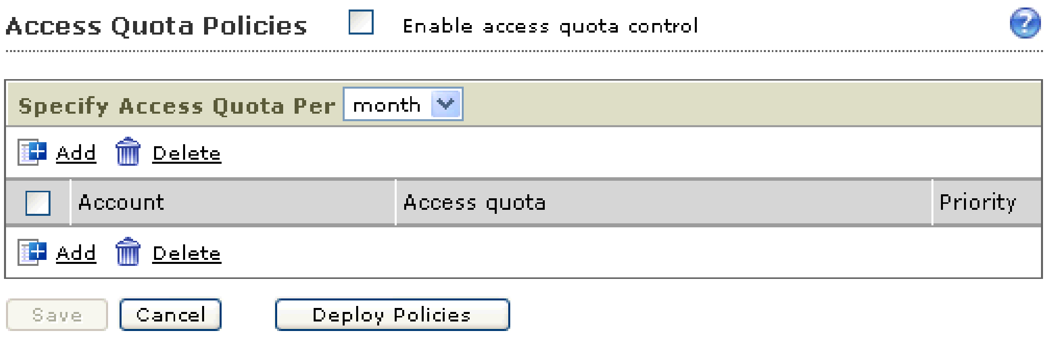
9. 如果启用Applets/ActiveX，其它配置取默认，下面界面配置建议如图所示(第一次上线不启用)：



Applets and ActiveX Policies ☑ Enable Applet/ActiveX security

□	Account	Policy Name	Priority
	(All accounts)	Applet/ActiveX Security Global Policy	1

10. Access Quota原则上在第一次测试时不启用；

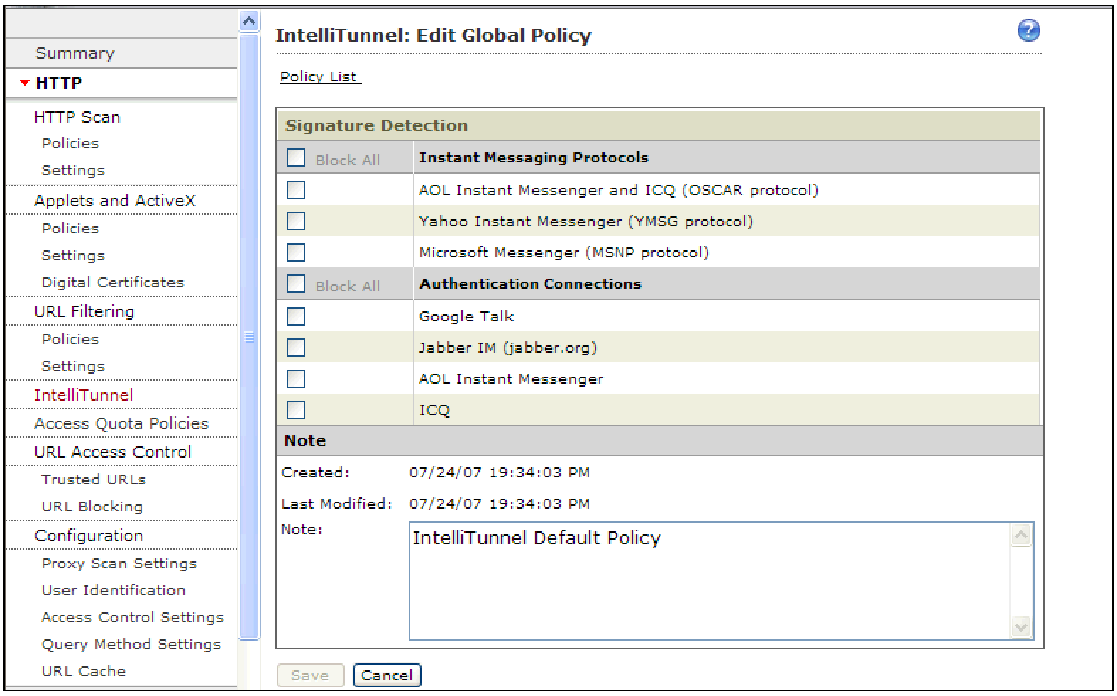


Access Quota Policies □ Enable access quota control

Specify Access Quota Per: month

□	Account	Access quota	Priority

11. 如果希望启用IntelliTunnel，请在界面中配置；



IntelliTunnel: Edit Global Policy

Policy List

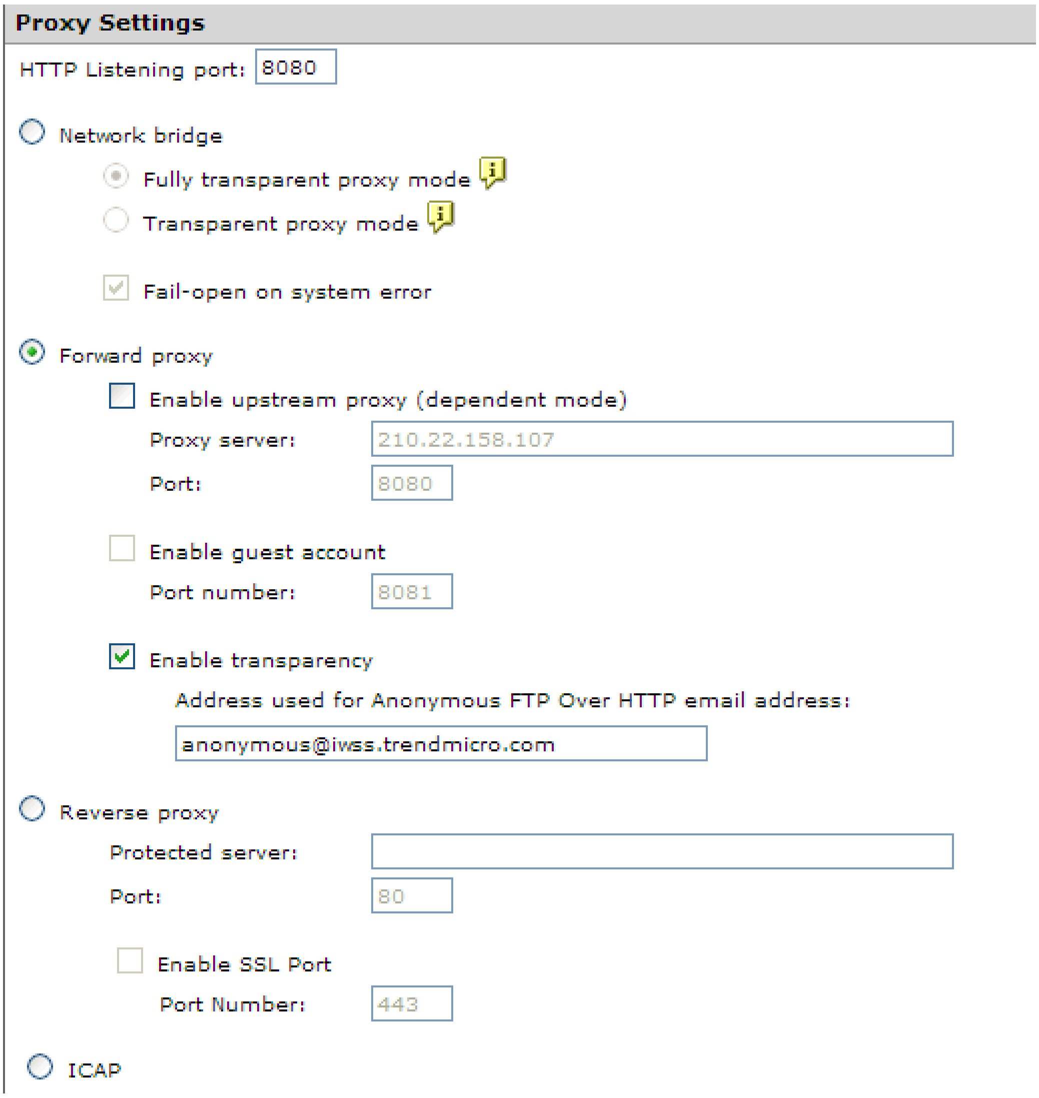
Signature Detection

□ Block All	**Instant Messaging Protocols**
□	AOL Instant Messenger and ICQ (OSCAR protocol)
□	Yahoo Instant Messenger (YMSG protocol)
□	Microsoft Messenger (MSNP protocol)
□ Block All	**Authentication Connections**
□	Google Talk
□	Jabber IM (jabber.org)
□	AOL Instant Messenger
□	ICQ

Note

Created:	07/24/07 19:34:03 PM
Last Modified:	07/24/07 19:34:03 PM
Note:	IntelliTunnel Default Policy

12. 工作模式根据情况选用，IWSA增加了reverse proxy，用来保护Web Server；



Proxy Settings

HTTP Listening port: 8080

○ Network bridge

○ Fully transparent proxy mode

○ Transparent proxy mode

☑ Fail-open on system error

● Forward proxy

□ Enable upstream proxy (dependent mode)

Proxy server: 210.22.158.107

Port: 8080

□ Enable guest account

Port number: 8081

☑ Enable transparency

Address used for Anonymous FTP Over HTTP email address:

anonymous@iwss.trendmicro.com

○ Reverse proxy

Protected server:

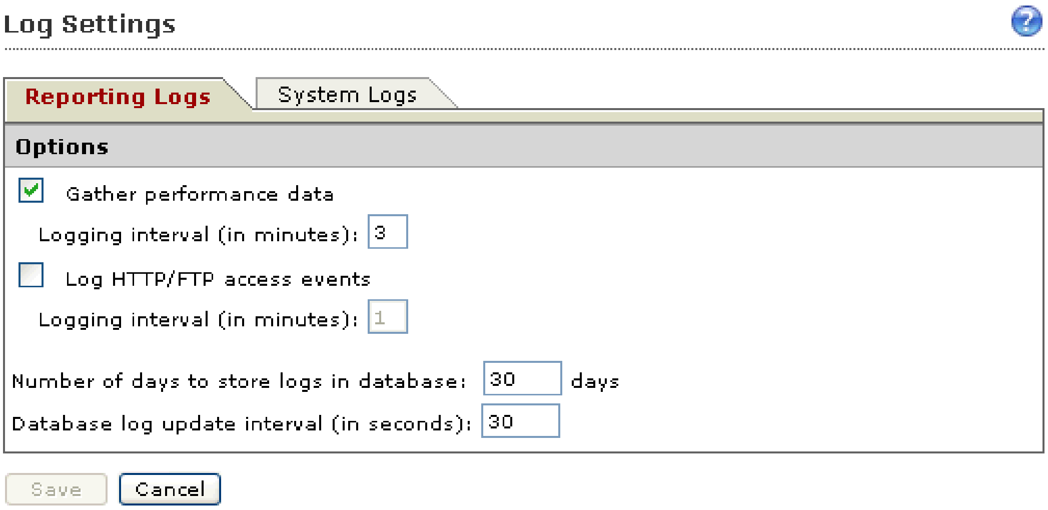
Port: 80

□ Enable SSL Port

Port Number: 443

○ ICAP

13. 在Log Settings中，请只启用Gather performance data（每3分钟1次）



Log Settings

Options

☑ Gather performance data

Logging interval (in minutes): 3

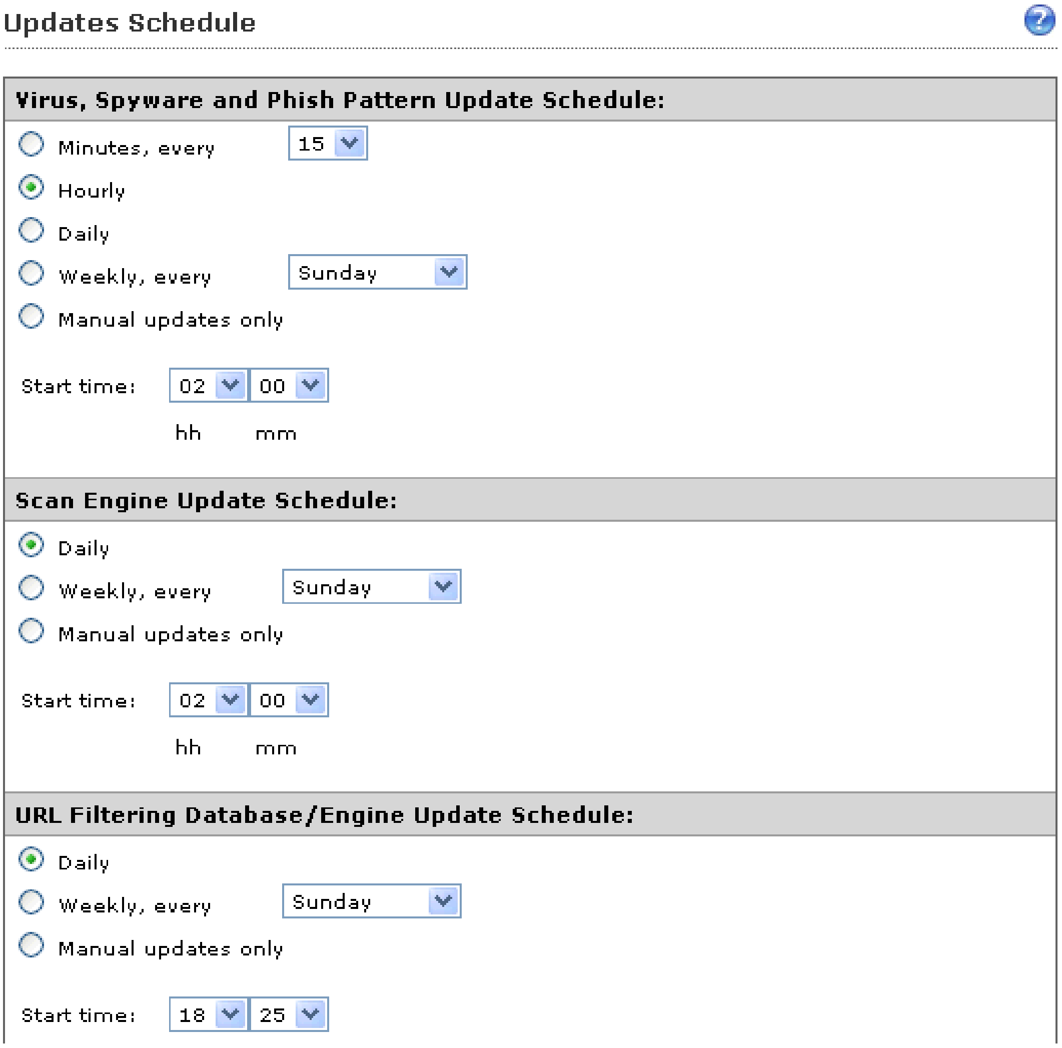
□ Log HTTP/FTP access events

Logging interval (in minutes): 1

Number of days to store logs in database: 30 days

Database log update interval (in seconds): 30

14. 配置代码库每小时更新一次，其它组件每天更新一次。



Updates Schedule

Virus, Spyware and Phish Pattern Update Schedule:

○ Minutes, every 15
● Hourly
○ Daily
○ Weekly, every Sunday
○ Manual updates only

Start time: 02 00
hh mm

Scan Engine Update Schedule:

● Daily
○ Weekly, every Sunday
○ Manual updates only

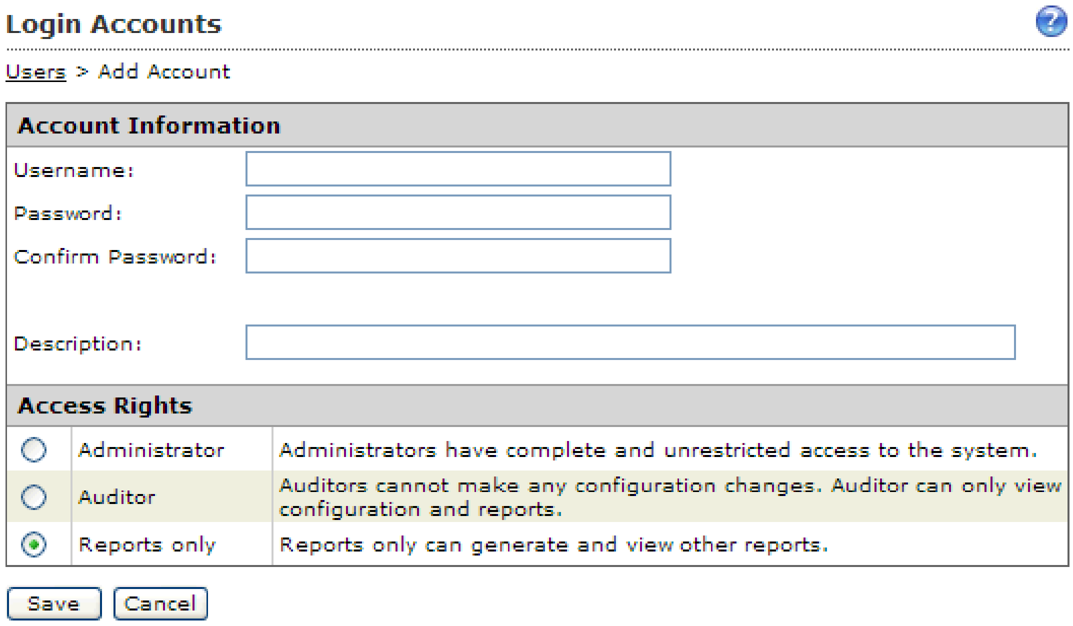
Start time: 02 00
hh mm

URL Filtering Database/Engine Update Schedule:

● Daily
○ Weekly, every Sunday
○ Manual updates only

Start time: 18 25

15. IWSA支持多管理员不同权限管理，可在如下界面中添加管理员：



Login Accounts

Users > Add Account

Account Information

Username:

Password:

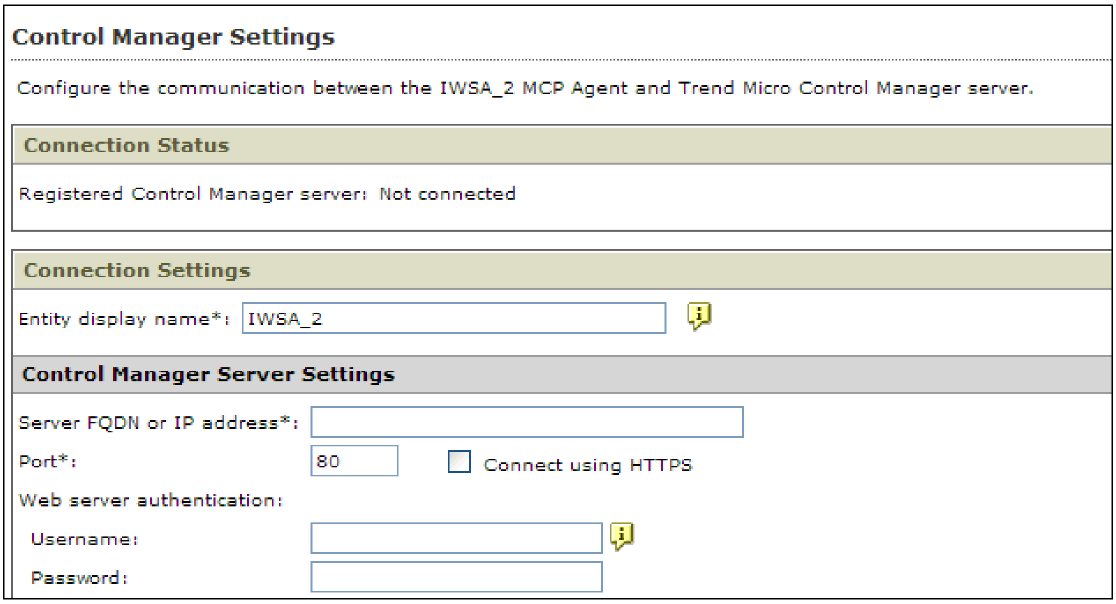
Confirm Password:

Description:

Access Rights

○	Administrator	Administrators have complete and unrestricted access to the system.
○	Auditor	Auditors cannot make any configuration changes. Auditor can only view configuration and reports.
●	Reports only	Reports only can generate and view other reports.

16. IWSA支持在Web界面配置向TMCM注册，界面如下：



Control Manager Settings

Configure the communication between the IWSA_2 MCP Agent and Trend Micro Control Manager server.

Connection Status

Registered Control Manager server: Not connected

Connection Settings

Entity display name*: IWSA_2

Control Manager Server Settings

Server FQDN or IP address*:

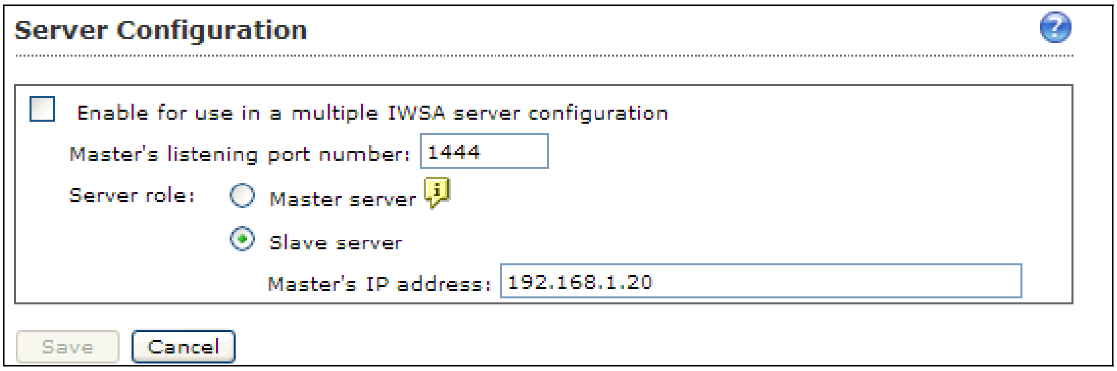
Port*: 80 □ Connect using HTTPS

Web server authentication:

Username:

Password:

17. IWSA支持在多台环境下，配置一台为主设备，其它为从设备，从设备从主设备上同步配置数据：



Server Configuration

□ Enable for use in a multiple IWSA server configuration

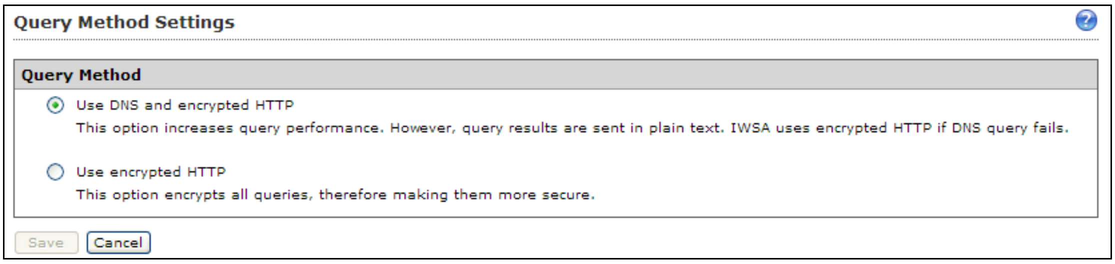
Master's listening port number: 1444

Server role: ○ Master server

● Slave server

Master's IP address: 192.168.1.20

18. Web Reputation查询支持两种查询方式，DNS查询速度更快些，建议采用如下配置，同时支持手动清除Url Cache功能：



Query Method Settings

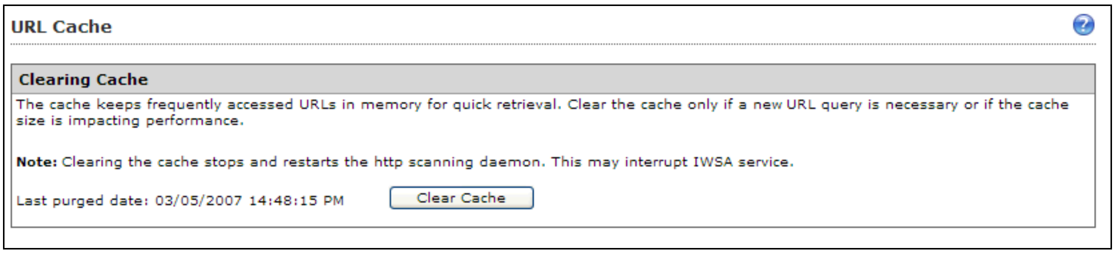
Query Method

● Use DNS and encrypted HTTP

This option increases query performance. However, query results are sent in plain text. IWSA uses encrypted HTTP if DNS query fails.

○ Use encrypted HTTP

This option encrypts all queries, therefore making them more secure.



URL Cache

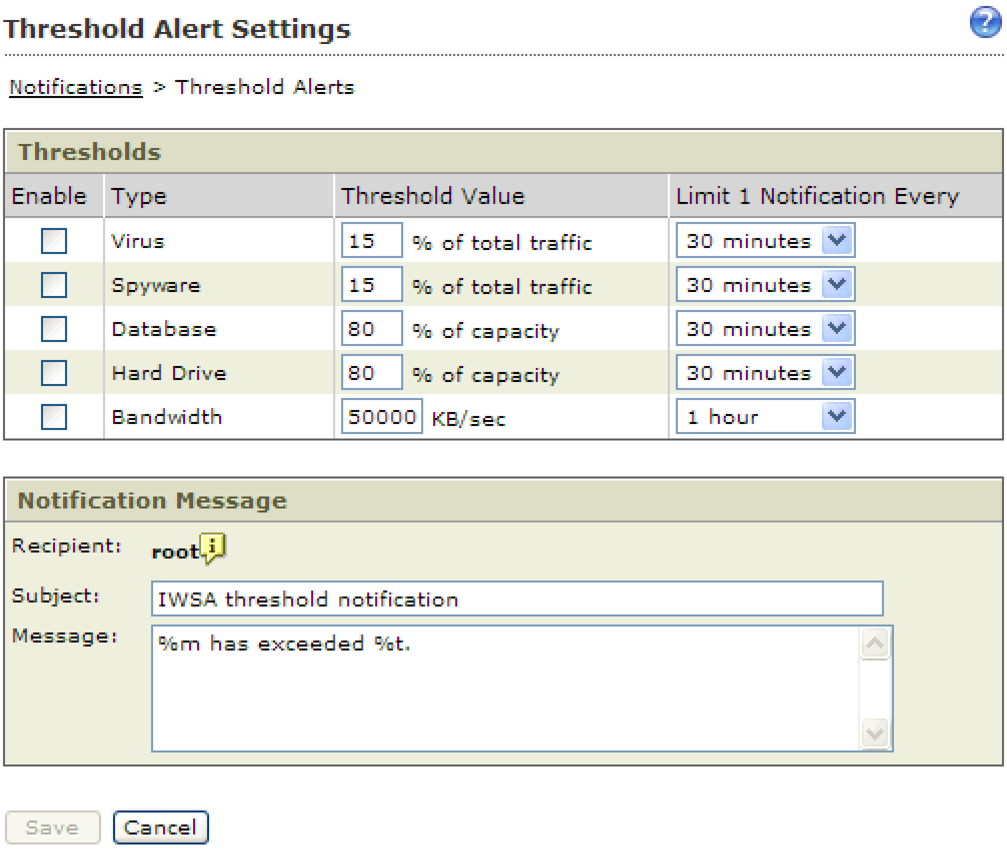
Clearing Cache

The cache keeps frequently accessed URLs in memory for quick retrieval. Clear the cache only if a new URL query is necessary or if the cache size is impacting performance.

Note: Clearing the cache stops and restarts the http scanning daemon. This may interrupt IWSA service.

Last purged date: 03/05/2007 14:48:15 PM

19. IWSA支持系统资源报警，配置如下：



Threshold Alert Settings

Notifications > Threshold Alerts

Thresholds

Enable	Type	Threshold Value	Limit 1 Notification Every
□	Virus	15 % of total traffic	30 minutes
□	Spyware	15 % of total traffic	30 minutes
□	Database	80 % of capacity	30 minutes
□	Hard Drive	80 % of capacity	30 minutes
□	Bandwidth	50000 KB/sec	1 hour

Notification Message

Recipient: **root**

Subject: IWSA threshold notification

Message: %m has exceeded %t.