# Vantage Report

## Support Notes

Version 3.0

Oct. 2006

ZyXEL

Unleash Networking Power

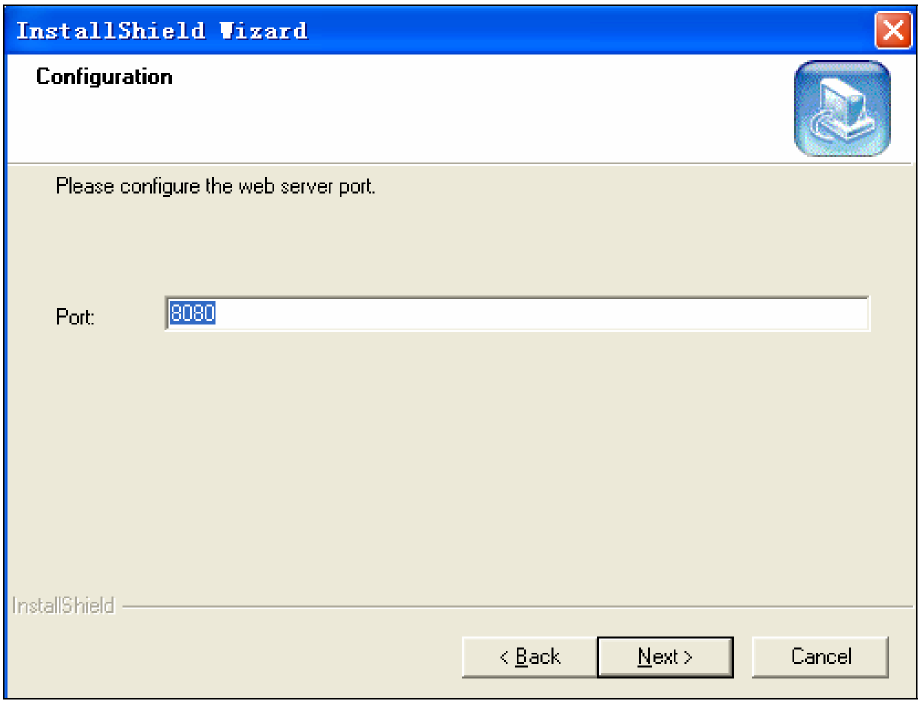
## INDEX

# Application Notes

## General Application Notes

### How to enable customized Web Server port VRPT?

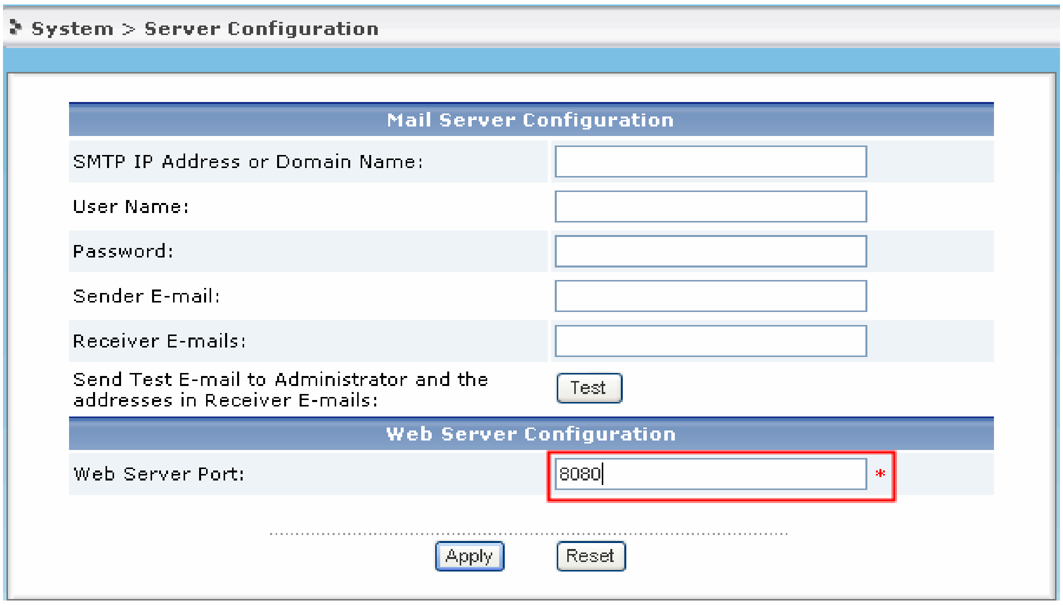
User could change the default TCP port 8080 to customized one when installing VRPT. Please do such change in Configuration step.



Please configure the web server port.

Port: 8080

After finishes installation, you can still change the customized server port under **System**>>**Server Configuration.**



System > Server Configuration

Mail Server Configuration

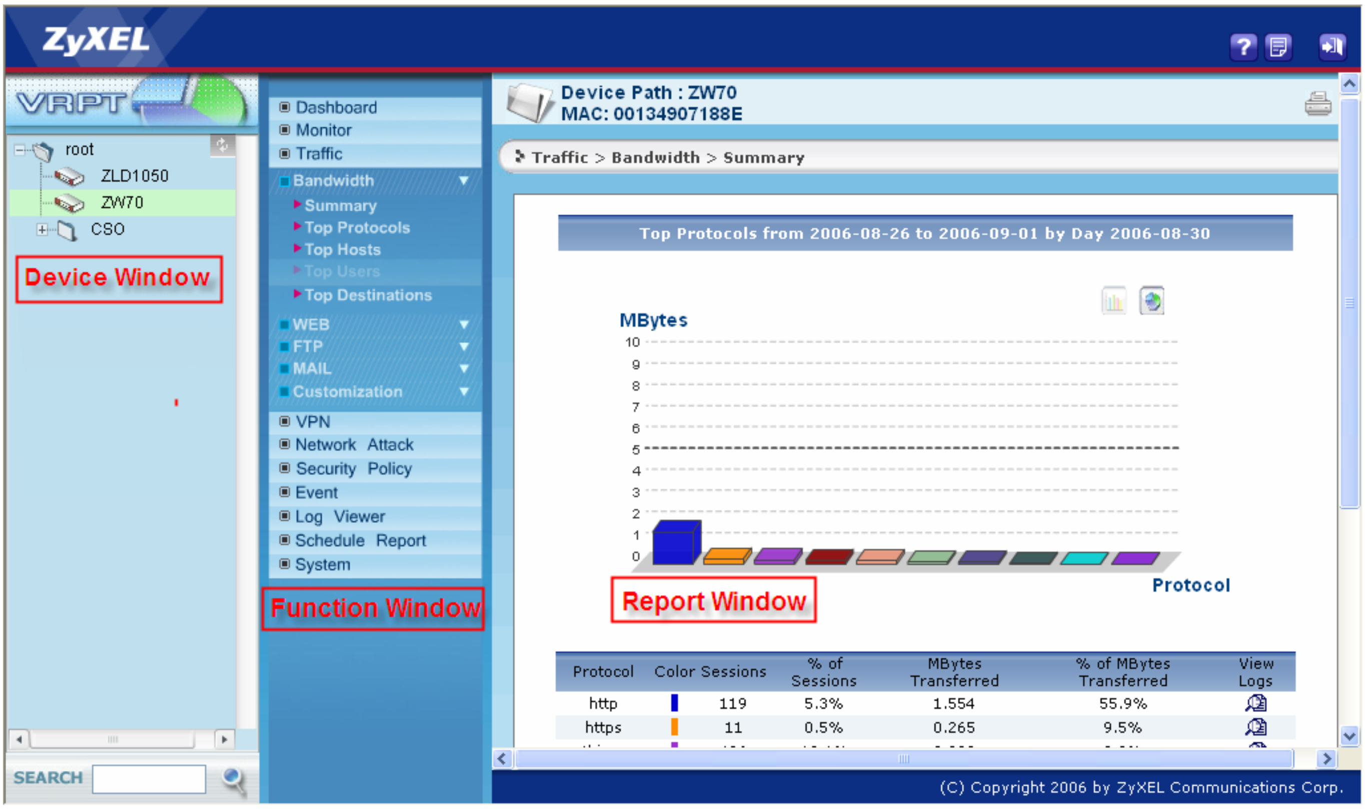
| | |
|---|---|
| SMTP IP Address or Domain Name: | |
| User Name: | |
| Password: | |
| Sender E-mail: | |
| Receiver E-mails: | |
| Send Test E-mail to Administrator and the addresses in Receiver E-mails: | |

Web Server Configuration

| | |
|---|---|
| Web Server Port: | 8080 * |

## Adding Device to Device Tree of VRPT

VRPT 3.0 supports multiple devices. Logs from these devices will be analyzed and imported to VRPT database. And then user could query reports for every individual device. But first of all the device should be added to **Device Tree** which is on the left Device window of VRPT. Below picture shows VRPT interface layout. Please go to **Add ZyWALL 1050 Device to VRPT Server** for details about ZyWALL 1050.



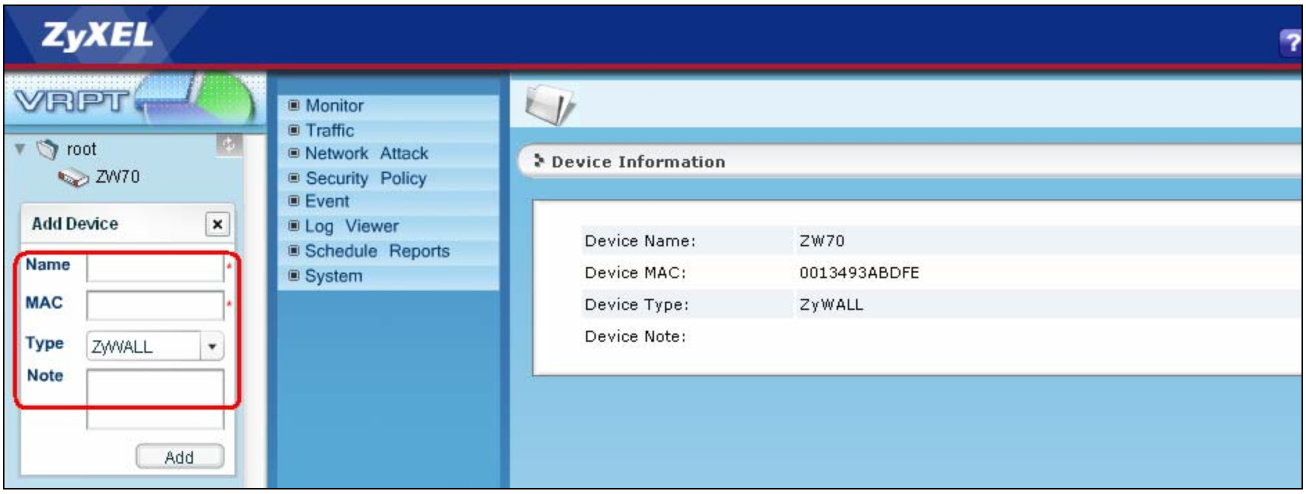
Device Path : ZW70
MAC: 00134907188E

Traffic > Bandwidth > Summary

Top Protocols from 2006-08-26 to 2006-09-01 by Day 2006-08-30

| Protocol | Color | Sessions | % of Sessions | MBytes Transferred | % of MBytes Transferred | View Logs |
|---|---|---|---|---|---|---|
| http | 🟦 | 119 | 5.3% | 1.554 | 55.9% | 🔍 |
| https | 🟧 | 11 | 0.5% | 0.265 | 9.5% | 🔍 |

You should move mouse to root folder then click right. After the "Add Device" windows appears, correct **Name**, **MAC** address and **Type** are needed if user wants to add a device for management.



Name:
MAC:
Type: ZyWALL
Note:

Device Information

| | |
|---|---|
| Device Name: | ZW70 |
| Device MAC: | 0013493ABDFE |
| Device Type: | ZyWALL |
| Device Note: | |

**NOTE:** If the device doesn't exist in this dev tree, its log will be discarded by VRPT. And also please make sure the **MAC** address is LAN MAC address of the device.

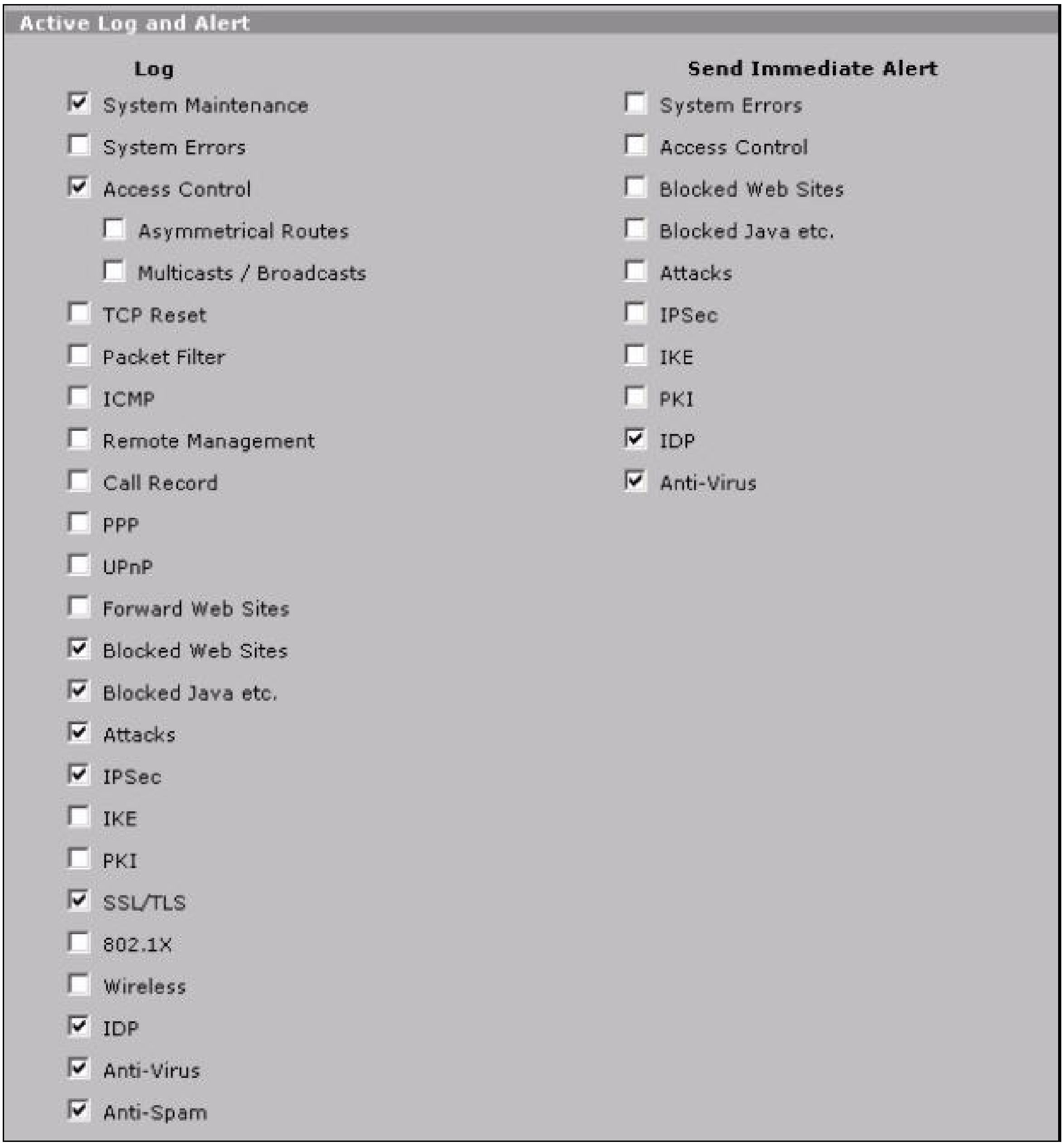
If user once removes a device from **Device Tree**, all the historical info about it will be removed by VRPT. And the process will take a period of time.

### How to forward device log to VRPT for analysis and report?

VRPT analyzes the logs based on the Syslogs from devices. Therefore, each device should take VRPT server as its **Syslog Server** at the first step then VRPT will collect Syslogs as the raw data. You could implement it either on WEB GUI or SMT menu on the device. For ZyWALL 1050, please go to Log Settings on ZyWALL 1050 for VRPT for details.

1. Configure From GUI (eWC)

For ZyWALL and xDSL, enter **LOGS**>>**Log Settings** to enable the Syslog logging and key in the server name or the IP address of VRPT server. It is recommended you to select following items.



Active Log and Alert

Log

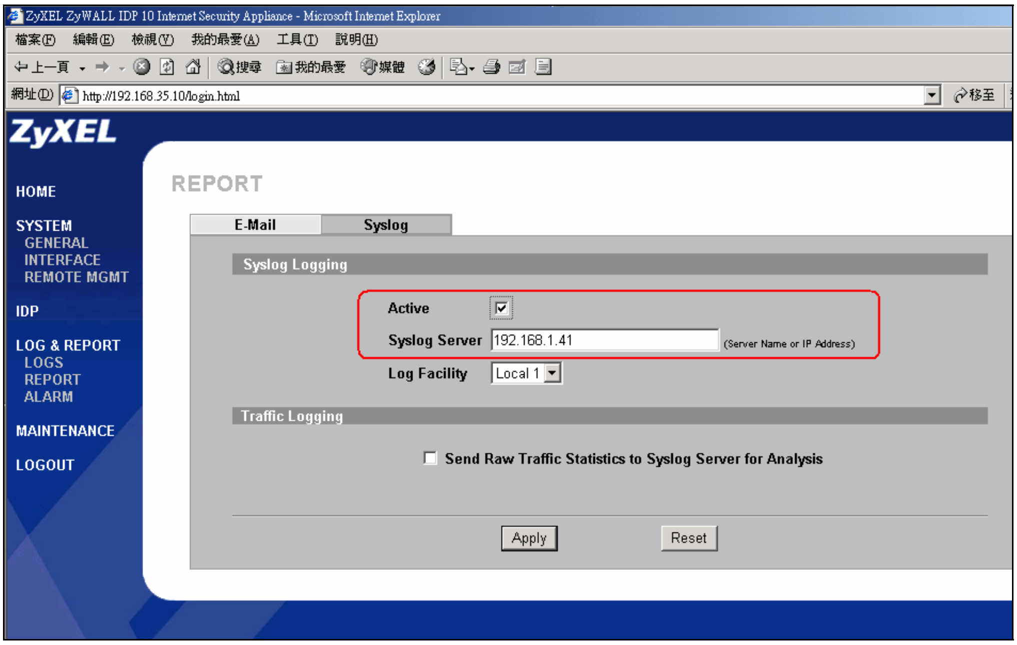
- ☑ System Maintenance
- □ System Errors
- ☑ Access Control
  - □ Asymmetrical Routes
  - □ Multicasts / Broadcasts
- □ TCP Reset
- □ Packet Filter
- □ ICMP
- □ Remote Management
- □ Call Record
- □ PPP
- □ UPnP
- □ Forward Web Sites
- ☑ Blocked Web Sites
- ☑ Blocked Java etc.
- ☑ Attacks
- ☑ IPSec
- □ IKE
- □ PKI
- ☑ SSL/TLS
- □ 802.1X
- □ Wireless
- ☑ IDP
- ☑ Anti-Virus
- ☑ Anti-Spam

Send Immediate Alert

- □ System Errors
- □ Access Control
- □ Blocked Web Sites
- □ Blocked Java etc.
- □ Attacks
- □ IPSec
- □ IKE
- □ PKI
- ☑ IDP
- ☑ Anti-Virus

Fig.5 Configure Syslog Server for ZyWALL series

The setting of **Log Facility** doesn't have matter for VRPT report.
For IDP10, enter **REPORT**>>**Syslog** and key in the server name or the IP address of VRPT server.



http://192.168.35.10/login.html

REPORT

Syslog Logging

Active ☑

Syslog Server 192.168.1.41 (Server Name or IP Address)

Log Facility Local 1

Traffic Logging

☐ Send Raw Traffic Statistics to Syslog Server for Analysis

Fig.6 Configure Syslog Server for IDP

2 Configure From SMT (Telnet/Console) menu24.3.2 (except IDP10)

Menu 24.3.2 - System Maintenance - Syslog Logging
Syslog:
Active= Yes
Syslog Server IP Address= 172.25.21.77
Log Facility= Local 1

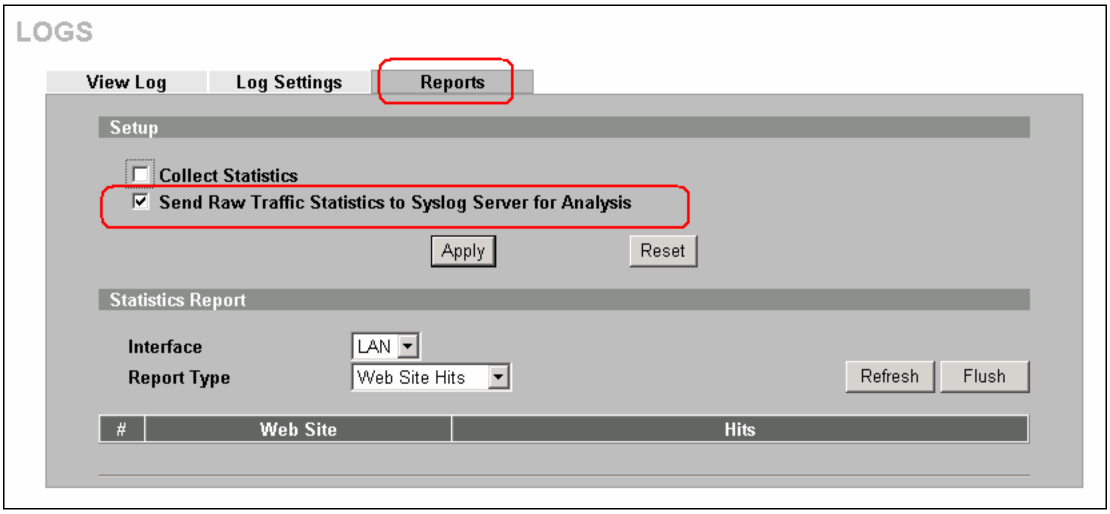
After activing the Syslog Server you should select the log types you want to send that are listed under the left side of **Active Log and Alert** (for ZyWALL,IDP) or under **Log** (for xDSL) column on this web page.

### How to enable traffic log feature on ZyWALL?

Note that traffic log is only available for ZyWALL 5/35/70 with firmware 3.63 and later. For ZyWALL 1050 traffic log issue please go to **How to enable traffic log feature ZyWALL 1050** for details. Two approaches can enable the traffic logs feature.

1. Enable Traffic Log From GUI (eWC)

Enter **Logs**>>**Reports** and select “Send Raw Traffic Statistics to Syslog Server for Analysis”.



□ Collect Statistics
☑ Send Raw Traffic Statistics to Syslog Server for Analysis

Interface: LAN
Report Type: Web Site Hits

Fig.7 Enable Traffic Log on ZyWALL

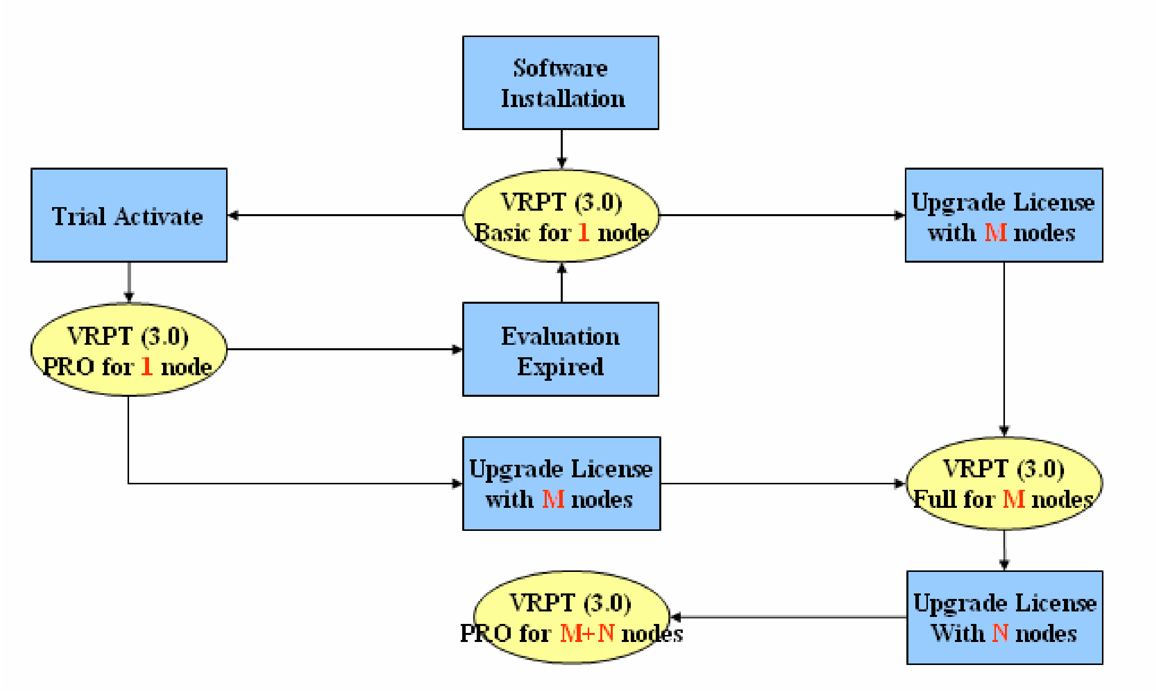
2. Enable Traffic Logs from SMT (Telnet/Console) menu 24.3.2

Enter its SMT Menu24.8 and type:

```
RAS>sys log load
RAS> sys log cat traffic 1
RAS> sys log save
```

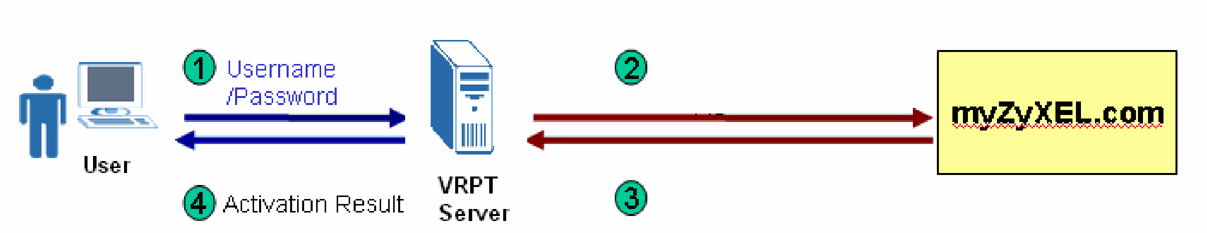
### VRPT Registration & Activation with myZyXEL.com

Below is a brief flow that describes the evolvement from Basic version to Full version.

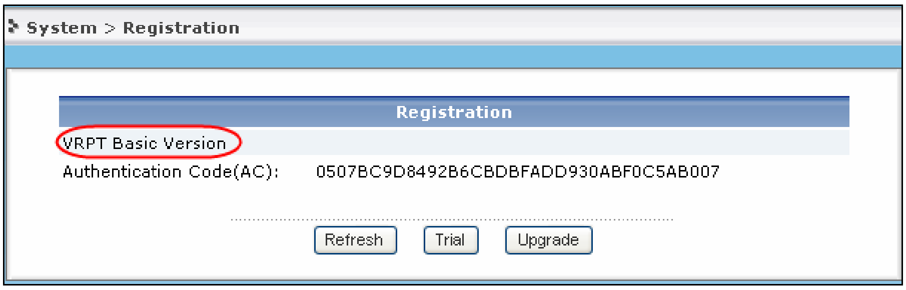

Software Installation
VRPT (3.0) Basic for 1 node
Trial Activate
Upgrade License with M nodes
VRPT (3.0) PRO for 1 node
Evaluation Expired
Upgrade License with M nodes
VRPT (3.0) Full for M nodes
VRPT (3.0) PRO for M+N nodes
Upgrade License With N nodes

When user installs VRPT 3.0, VRPT will show as Basic version. There's two way to upgrade Basic version to Full version. One is to achieve it by trial activation. But this kind of Full version has time restriction (30 days). Also in this Trial version, user only can manage one node (device). The other is to upgrade to Full version by inputting legal license user ever bought.
There are other two kinds of license. One kind supports 5 nodes, that user could manage 5 devices at most if he/she buy it. The other kind supports 25 nodes. Please notice the most devices that VRPT 3.0 can managed is 100.

- **VRPT Service Activation- Install Upgrade to Trial Version**



1. Go to **System**>> **Registration,** then click **Trial.**

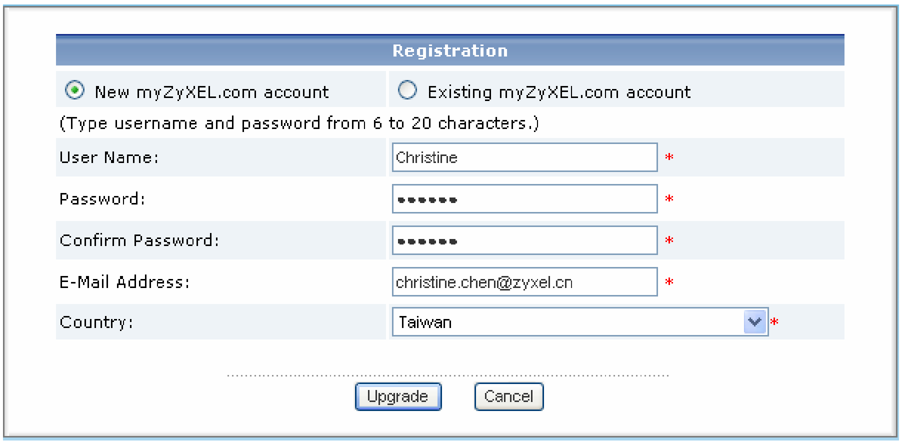


Registration

VRPT Basic Version

Authentication Code(AC): 0507BC9D8492B6CBDBFADD930ABF0C5AB007

2. Input **User Name**, **Password**, **E-mail Address** and **Country.**



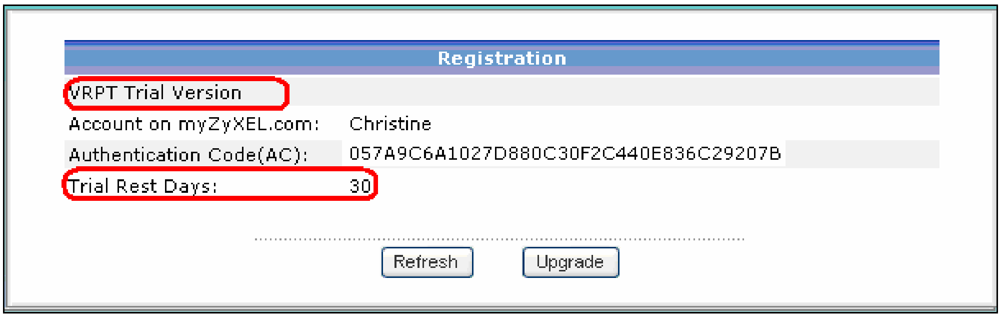
Registration

● New myZyXEL.com account ○ Existing myZyXEL.com account

(Type username and password from 6 to 20 characters.)

| | |
|---|---|
| User Name: | Christine * |
| Password: | •••••• * |
| Confirm Password: | •••••• * |
| E-Mail Address: | christine.chen@zyxel.cn * |
| Country: | Taiwan * |

3. VRPT 3.0 will send the **User Name, Password,** Trial License key and other information to myZyxel.com.

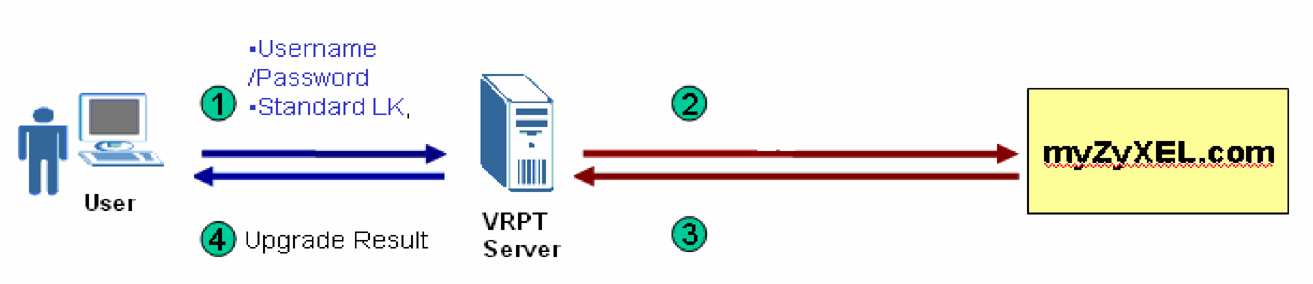


Registration

VRPT Trial Version

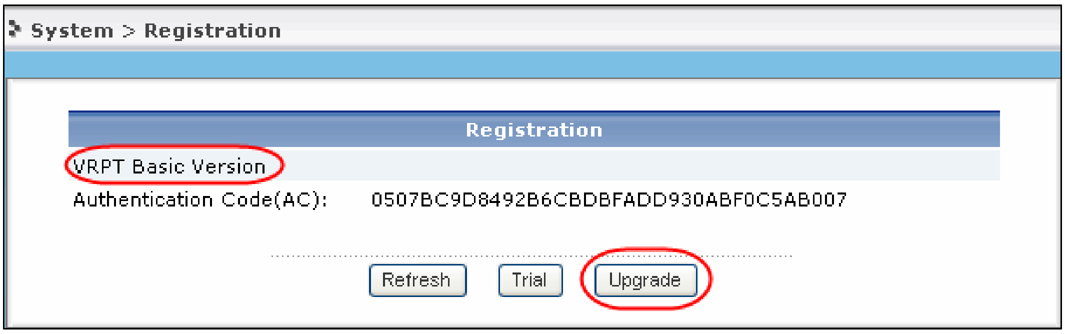
| | |
|---|---|
| Account on myZyXEL.com: | Christine |
| Authentication Code(AC): | 057A9C6A1027D880C30F2C440E836C29207B |
| Trial Rest Days: | 30 |

- **VRPT Service Activation-Install to Full Version**



If user has already installed VRPT service and wants to skip trial version to extend management node directly, he/she could follow such steps to do so.

1. Go to **System**>>**Registration**



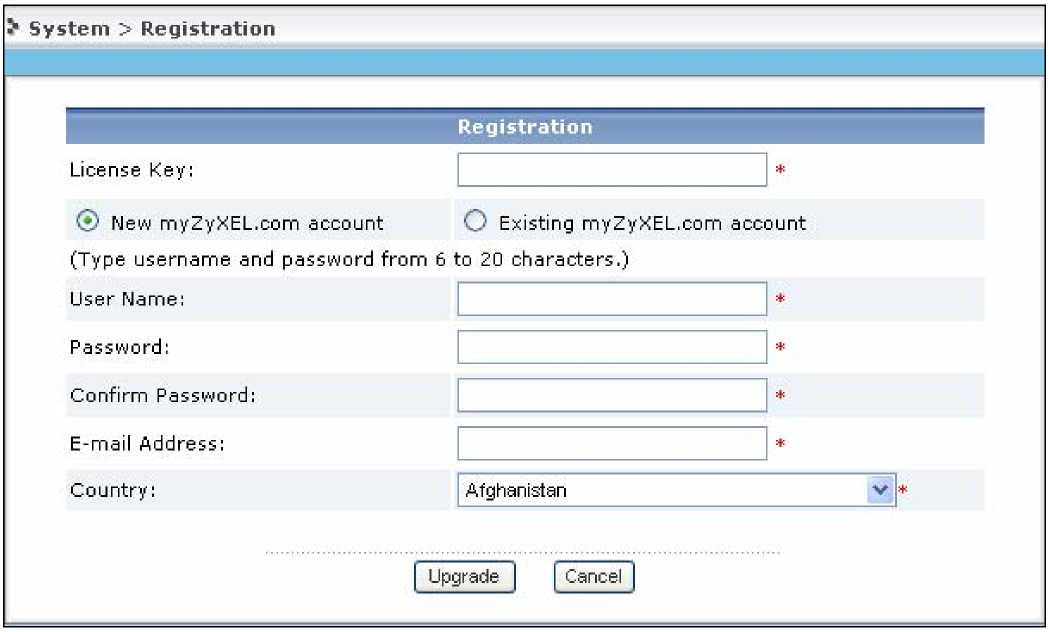
System > Registration

Registration

VRPT Basic Version

Authentication Code(AC): 0507BC9D8492B6CBDBFADD930ABF0C5AB007

2. Input **User Name**, **Password**, **License Key** and other information.



System > Registration

Registration

License Key: *

● New myZyXEL.com account ○ Existing myZyXEL.com account

(Type username and password from 6 to 20 characters.)

User Name: *

Password: *

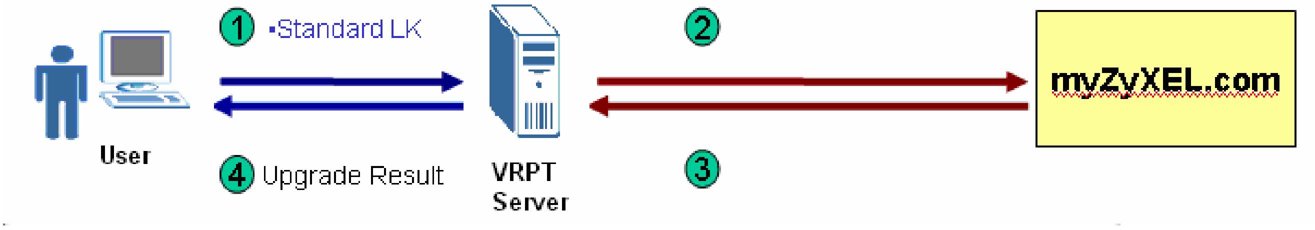
Confirm Password: *

E-mail Address: *

Country: Afghanistan *

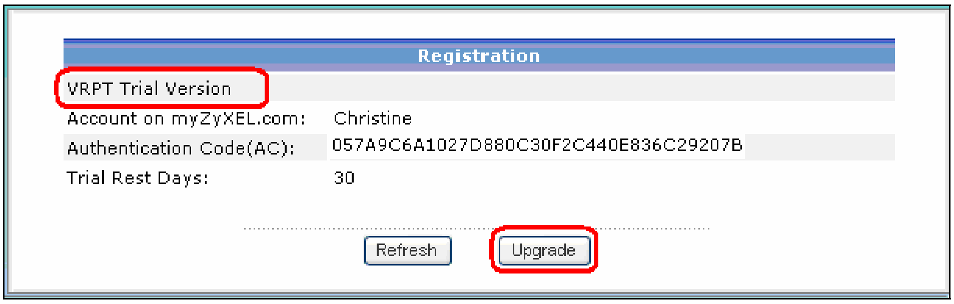
3. VRPT will send such items and other information to myZyXEL.com and complete authentication.

- **VRPT Service Activation-Trial version Upgrade to Full version**



If user has already activated VRPT trial service and wants to upgrade to Full status, please just follow such steps.

1. Click **Upgrade** button.


Registration

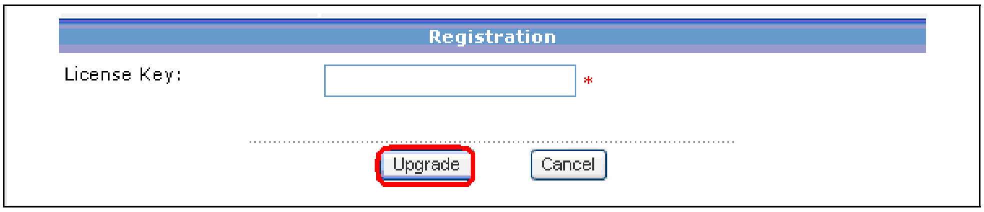
VRPT Trial Version

Account on myZyXEL.com: Christine

Authentication Code(AC): 057A9C6A1027D880C30F2C440E836C29207B

Trial Rest Days: 30

2. Input **License.**

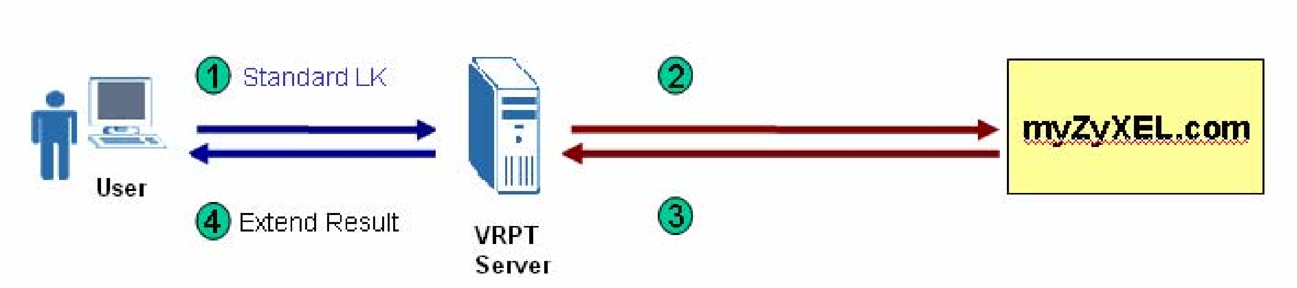

Registration

License Key: *

3. VRPT will send **License Key** and other information to myZyXEL.com and complete authentication.

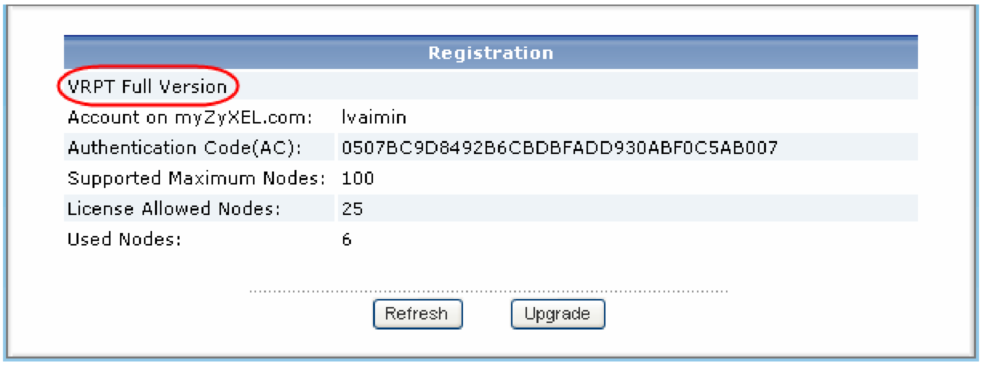
**NOTE**: If user reinstalls VRPT at same machine with OS untouched and it was full version already, VRPT will remain as full status.

- **VRPT Service Extend–Basic to Full version**



If user has installed VRPT service and VRPT is already in full status, user could extend management node by purchasing more license key and do upgrade for extension.

1. Go to **System**>>**Registration** and press **Upgrade**.

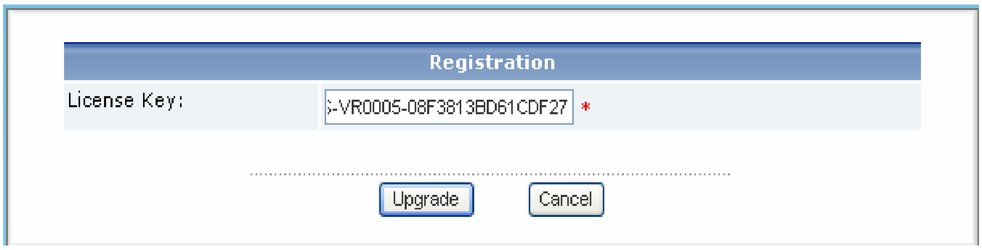


Registration

VRPT Full Version

| | |
|---|---|
| Account on myZyXEL.com: | lvaimin |
| Authentication Code(AC): | 0507BC9D8492B6CBDBFADD930ABF0C5AB007 |
| Supported Maximum Nodes: | 100 |
| License Allowed Nodes: | 25 |
| Used Nodes: | 6 |

2. Input **License Key**



Registration

License Key: -VR0005-08F3813BD61CDF27 *

3. VRPT will send License Key and other information to myZyXEL.com for authentication. And after such operation, the allowed nodes will increase to the legal number. One license key support 5 node at most.

### Version Type of VRPT 3.0 and Their Supported Feature

There are two main version types: Basic version and Full version. The table below shows the features they support. Trial status has the same features as Full version.

| Feature | Basic version | Full version | Note |
|---|---|---|---|
| Bandwidth Report by Direction | ALL | Incoming<br>Outgoing<br>ALL<br>LAN-WAN<br>LAN-DMZ<br>LAN-LAN<br>WAN-WAN<br>WAN-DMZ<br>WAN-LAN<br>DMZ-WAN<br>DMZ-DMZ<br>DMZ-LAN | |
| Traffic -> Bandwdith | Yes | Yes | Bandwidth monitor is available for Basic version. |
| Traffic -> WEB | Yes | Yes | |
| Traffic -> FTP | Yes | Yes | |
| Traffic -> MAIL | Yes | Yes | |
| Traffic -> Customization | Yes | Yes | |
| VPN->Site to Site -> Top Peer Gateways | Yes | Yes | |

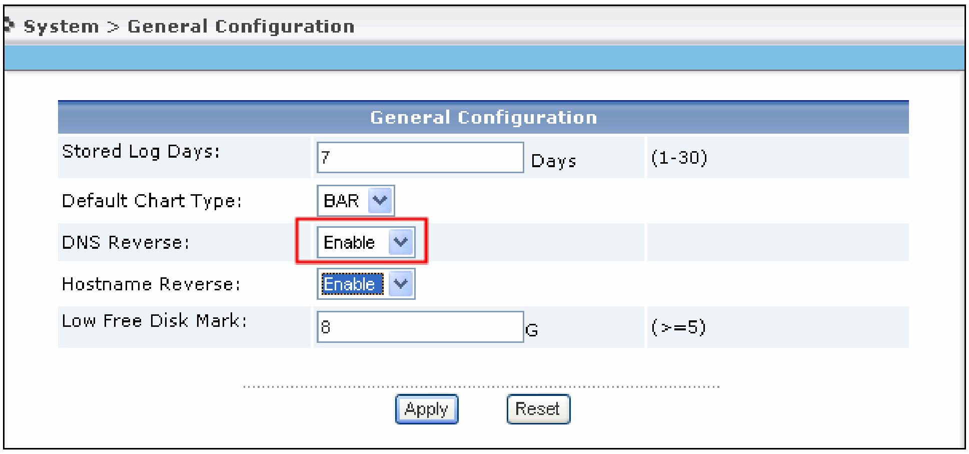
| | | | |
|---|---|---|---|
| VPN->Site to Site -> Top Hosts | Yes | Yes | |
| VPN others | No | Yes | |
| Network Attack ->Attack | Yes | Yes | |
| Network Attack -> Intrusion (Report for IDP10) | Yes | Yes | Available for 2.00(XA0) and later |
| Network Attack -> Intrusion (Report for ZLD) | No | Yes | Available for 4.00 and later if ZyWALL series.<br>Available for 1.01 and later if ZLD. |
| Network Attack ->AntiVirus | No | Yes | Available for 4.00 and later |
| Network Attack ->AntiSpam | No | Yes | Available for 4.00 and later |
| Security Policy ->Firewall Access Control | No | Yes | |
| Security Policy -> Application Access Control | No | Yes | |
| Security Policy -> WEB Blocked -> By Category | No | Yes | |
| Security Policy -> WEB Blocked others | Yes | Yes | |
| Security Policy -> WEB Allowed Report | Yes | Yes | |
| Event -> Login | Yes | Yes | |

| | | | |
|---|---|---|---|
| Event -> Session Per Host | No | Yes | |

| Feature | Basic version | Full version | Note |
|---|---|---|---|
| All reports for ZyWALL 1050 | No | Yes | Log Viewer is available for ZyWALL 1050. |
| Dashboard | No | Yes | |
| Template of Schedule report | No | Yes | On Basic version, user can define and apply template to Basic version. |
| Number of Scheduled Report | 20 | 20/device | |
| Number of supported node | 1 | The number is according to the license type<br>The maximum number it can support is 100 | |
| Schedule Report Format | PDF only | PDF & HTML | |
| Drill-down Report | 1 layer | 2 layers | |
| Reverse DNS Lookup | No | Yes | |
| Reverse Hostname | No | Yes | |

## the Way to Use DNS Reverse Function

VRPT 3.0 supplies DNS Reverse function to give convenience to user when checking the report. Instead of obscure IP address of web site, VRPT could let you check both the domain name and the IP address of it. It is like a good guider that pulls you out of the sea of the IP address. Please go to **System**>>**General Configuration** to enable the **DNS Reverse** function.

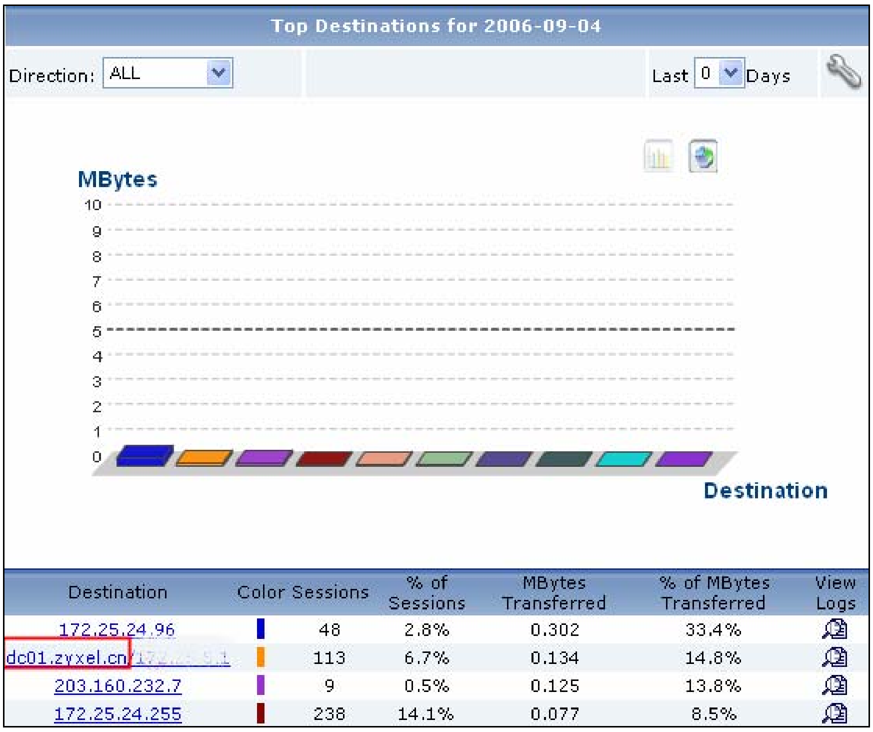


System > General Configuration

General Configuration

| | | | |
|---|---|---|---|
| Stored Log Days: | 7 | Days | (1-30) |
| Default Chart Type: | BAR | | |
| DNS Reverse: | Enable | | |
| Hostname Reverse: | Enable | | |
| Low Free Disk Mark: | 8 | G | (>=5) |

Please see the sample as following.



Top Destinations for 2006-09-04

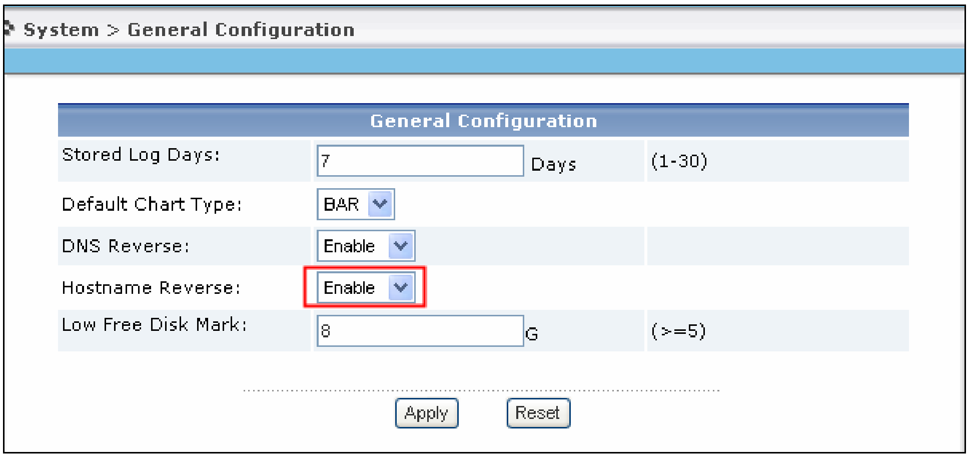
Direction: ALL

Last 0 Days

| Destination | Color | Sessions | % of Sessions | MBytes Transferred | % of MBytes Transferred | View Logs |
|---|---|---|---|---|---|---|
| 172.25.24.96 | 🟦 | 48 | 2.8% | 0.302 | 33.4% | |
| dc01.zyxel.cn/172.[illegible].9.1 | 🟧 | 113 | 6.7% | 0.134 | 14.8% | |
| 203.160.232.7 | 🟪 | 9 | 0.5% | 0.125 | 13.8% | |
| 172.25.24.255 | 🟥 | 238 | 14.1% | 0.077 | 8.5% | |

## the Way to Use Hostname Reverse Function

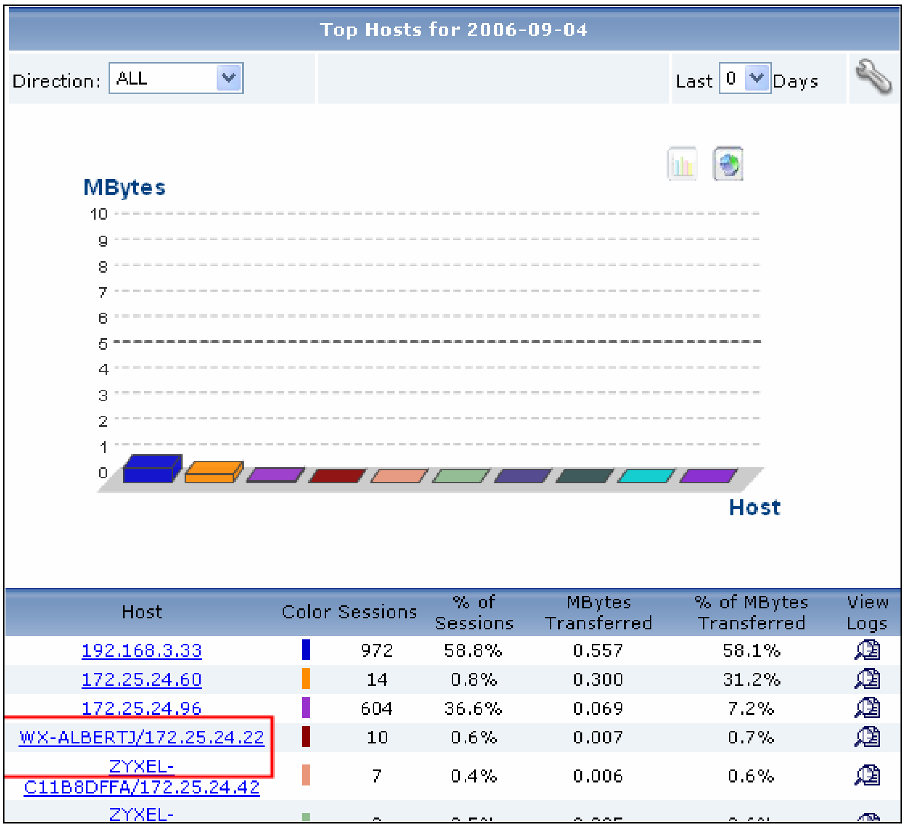
VRPT 3.0 supplies Hostname Reverse function to give convenience to user when checking the report. It is a useful tool for you to trace the operations of each PC.



System > General Configuration

General Configuration

| | | |
|---|---|---|
| Stored Log Days: | 7 Days | (1-30) |
| Default Chart Type: | BAR | |
| DNS Reverse: | Enable | |
| Hostname Reverse: | Enable | |
| Low Free Disk Mark: | 8 G | (>=5) |



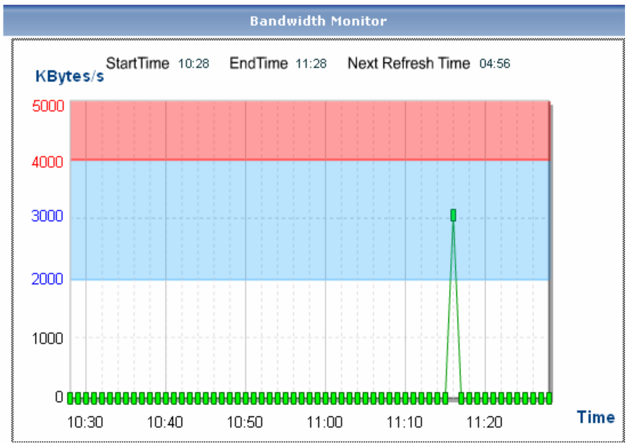
Top Hosts for 2006-09-04

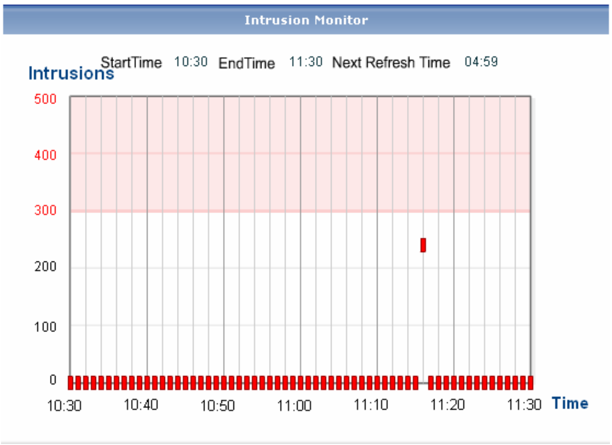
Direction: ALL    Last 0 Days

| Host | Color | Sessions | % of Sessions | MBytes Transferred | % of MBytes Transferred | View Logs |
|---|---|---|---|---|---|---|
| 192.168.3.33 | 🟦 | 972 | 58.8% | 0.557 | 58.1% | 🔍 |
| 172.25.24.60 | 🟧 | 14 | 0.8% | 0.300 | 31.2% | 🔍 |
| 172.25.24.96 | 🟪 | 604 | 36.6% | 0.069 | 7.2% | 🔍 |
| WX-ALBERTJ/172.25.24.22 | 🟥 | 10 | 0.6% | 0.007 | 0.7% | 🔍 |
| ZYXEL-C11B8DFFA/172.25.24.42 | 🟧 | 7 | 0.4% | 0.006 | 0.6% | 🔍 |
| ZYXEL- | | | | | | |

## Monitor Function for Live Check

There is a special menu in VRPT 3.0 for live monitor. That is **Monitor.** VRPT gives live monitor report according to the logs received during the last 60 minutes. Live monitor report for **Bandwidth** and **Service** will be shown as continuous curves for they are generated by traffic logs. While live report for **Attack**, **Intrusion**, **AntiVirus** and **AntiSpam** will expose to you as discrete picture for it monitors event logs. The x axes of each report shows the lease time. The unit for it is minute. Please see the below sample report for the service monitor (left) and attack monitor (right). Please check the below tables for coordinate information of the report.





Bandwidth /Service Monitor Report

| **Coordinate** | **Meaning** | **Unit** |
|---|---|---|
| Xaxis | Lease time | Minute |
| Yaxis | speed | Kbytes/s |

Attack/Intrusion/AntiVirus/AntiSpam Monitor Report

| **Coordinate** | **Meaning** | **Unit** |
|---|---|---|
| Xaxis | Lease time | Minute |
| Yaxis | Number of the events | |

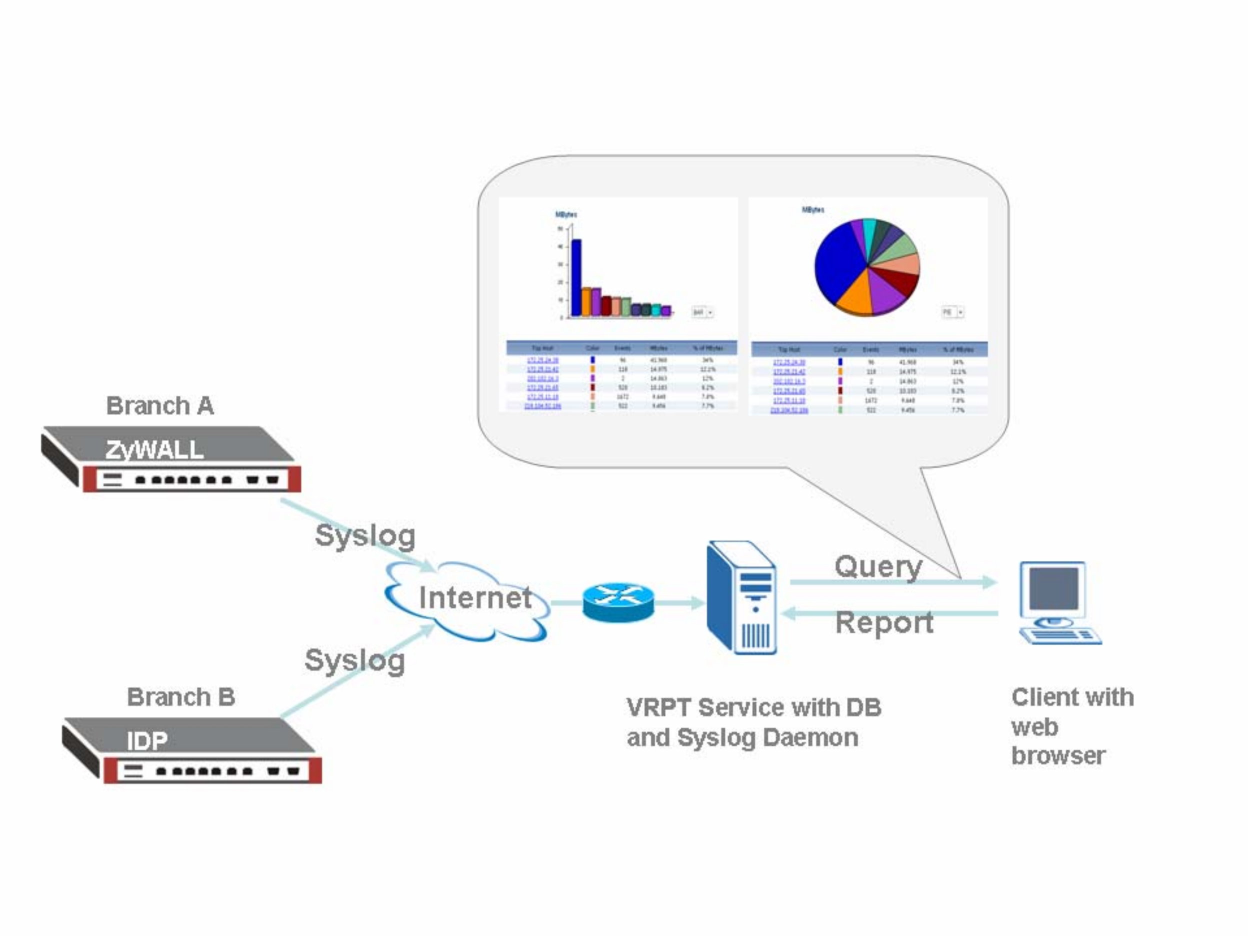
**NOTE:** You should select a device from **Device Tree** before querying a report from VRPT.

## Brief Data Flow for VRPT Server to Generate Report

To setup VRPT could be very easy. VRPT will take such steps to get reports.

1. System administrator configures ZyWALL/IDP10/xDSL to send Syslog to VRPT. Please see **How to forward device log to VRPT for analysis and report?**
2. System administrator starts up VRPT and then do some service registration and activation. Please see **VRPT Registration and Activation with myZyXEL .com.** After that he/she adds devices in VRPT. Please see **Adding Device to Device Tree of VRPT.**
3. Syslogs are received and stored in VRPT DB.
4. User queries for report when he/she access VRPT by browser.
5. VRPT server generates the report accordingly.
6. User gets the final report.

Below picture shows the brief data flow for VRPT and device.

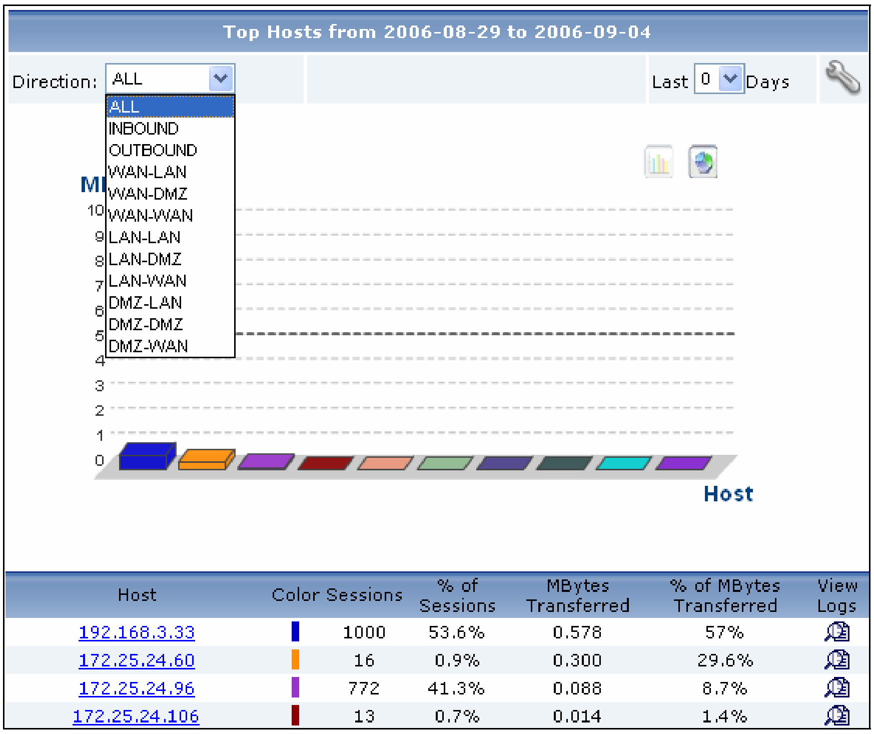


**NOTE**: If device is not added in VRPT, VRPT will ignore the Syslogs from that device.

Please make sure the gateway before VRPT server opens UDP port 514 and TCP port 8080. If user changes the Web Server port as customized port, she/he should forward such customized port instead of 8080.

Please select a device from the **Device Tree** by clicking before querying a report.

### Direction for Bandwidth Usage



Top Hosts from 2006-08-29 to 2006-09-04

Direction: ALL

Last 0 Days

| Host | Color | Sessions | % of Sessions | MBytes Transferred | % of MBytes Transferred | View Logs |
|---|---|---|---|---|---|---|
| 192.168.3.33 | 🟦 | 1000 | 53.6% | 0.578 | 57% | |
| 172.25.24.60 | 🟧 | 16 | 0.9% | 0.300 | 29.6% | |
| 172.25.24.96 | 🟪 | 772 | 41.3% | 0.088 | 8.7% | |
| 172.25.24.106 | 🟥 | 13 | 0.7% | 0.014 | 1.4% | |

User could choose different direction for their Bandwidth usage report. The meaning of the previous ten directions is as their names.

**INBOUND**, includes LAN-to-WAN-receive, DMZ-to-WAN-receive, WAN-to-WAN-receive, WAN-to-LAN-send, WAN-to-DMZ-send

**OUTBOUND** includes LAN-to-WAN-send, DMZ-to-WAN-send, WAN-to-WAN-send, WAN-to-LAN-receive, WAN-to-DMZ-receive

**NOTE:** The direction is very useful for administrator to add firewall or other rules to control the network condition for a single IP address is not enough.

Also, user could choose directions for Bandwidth report in scheduled report.

### How to migrate device list from VRPT 2.3 to VRPT 3.0?

As we know it is a little bit fussy for user to add device to VRPT especially when the amount of device is not small. You should go to input MAC address of LAN one by one, choose device type …etc. Now if you want VRPT 3.0 to manage the devices that are in the charge of VRPT 2.3, the job will be done well and fast by following steps and you can also check *Upgrade Note*.

**NOTE**:

1. If you currently use Vantage Report (VRPT) 2.3.1 (2.3.05.61.01), this document describes how to upgrade from Vantage Report 2.3.1 to Vantage Report 3.0 (3.0.00.61.00). To check the detailed version, please go to **System** > **About**.

2. If you currently use Vantage Report (VRPT) 2.3.0 (2.3.05.61.00), please get VRPT 2.3.1 installation package to upgrade your VRPT to 2.3.1 first.

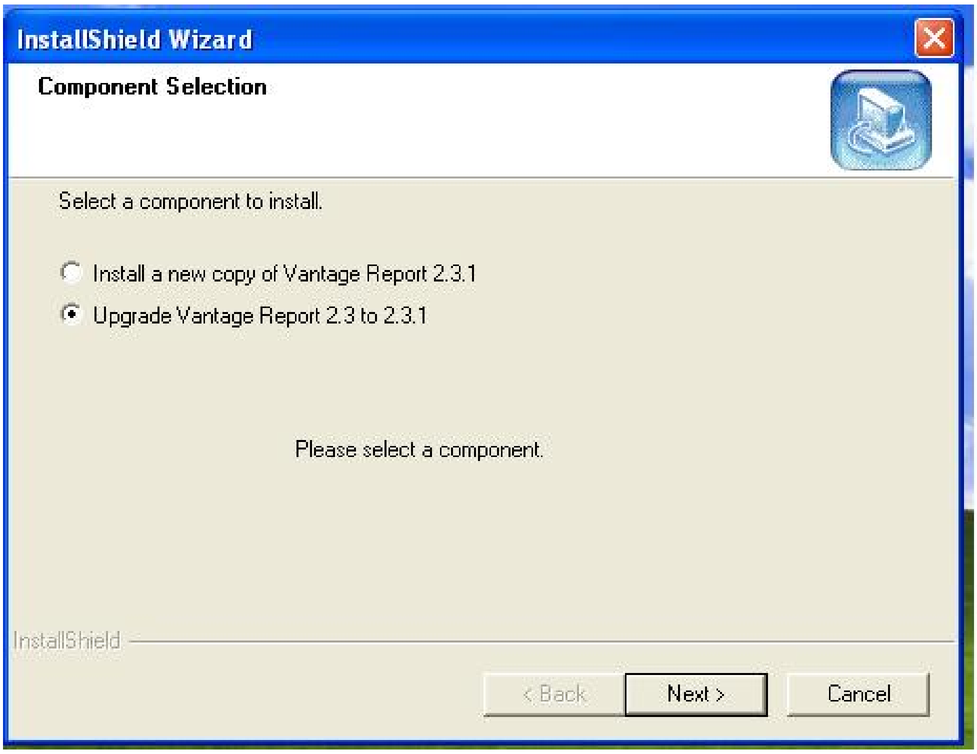
3. The upgrade package doesn't backup the data in database. In order not to loss all the data, please backup the content in <vrpt_home> folder in case of failure upgrade, or just go to backup the configuration file and device list.

After you login VRPT 2.3.1, go to **System** >>**Data Maintenance** >> **Configuration Backup** & **Restore** page, click **Backup** button to backup the configuration.

Go to **System** >> **Data Maintenance** >> **Device List Import** & **Export page**, click **Export** button to export the device list. Once the upgrade fails, you can restore the configuration and device list.

- **The following steps detail the procedure to upgrade VRPT 2.3 to 2.3.1.**

1. Prepare Vantage Report 2.3.1 installation package.
2. Execute the installation program. If VRPT 2.3 has been installed in your system, VRPT 2.3.1 installer will detect it. Please select **Upgrade Vantage Report 2.3 to 2.3.1** and click **Next** button if you want to upgrade your Vantage Report from 2.3 to 2.3.1.



InstallShield Wizard

Component Selection

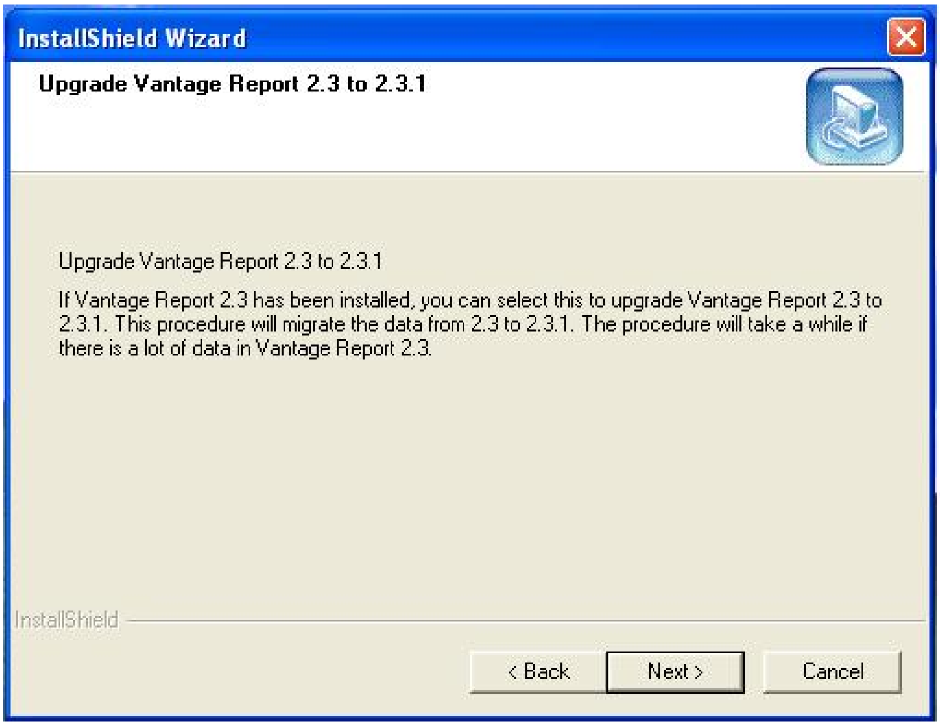
Select a component to install.

○ Install a new copy of Vantage Report 2.3.1

● Upgrade Vantage Report 2.3 to 2.3.1

Please select a component.

3. Press **Next** button to continue installation.



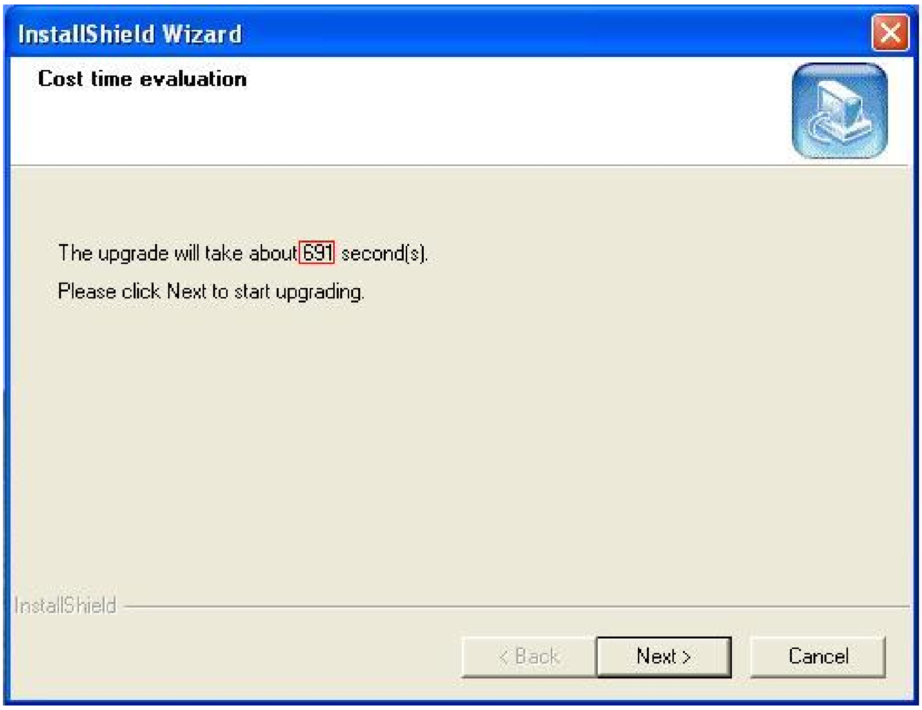
InstallShield Wizard

Upgrade Vantage Report 2.3 to 2.3.1

Upgrade Vantage Report 2.3 to 2.3.1

If Vantage Report 2.3 has been installed, you can select this to upgrade Vantage Report 2.3 to 2.3.1. This procedure will migrate the data from 2.3 to 2.3.1. The procedure will take a while if there is a lot of data in Vantage Report 2.3.

3. Please click **Next** button to continue installation. The displays about ‘691 seconds’ is the estimated time for this upgrade process.



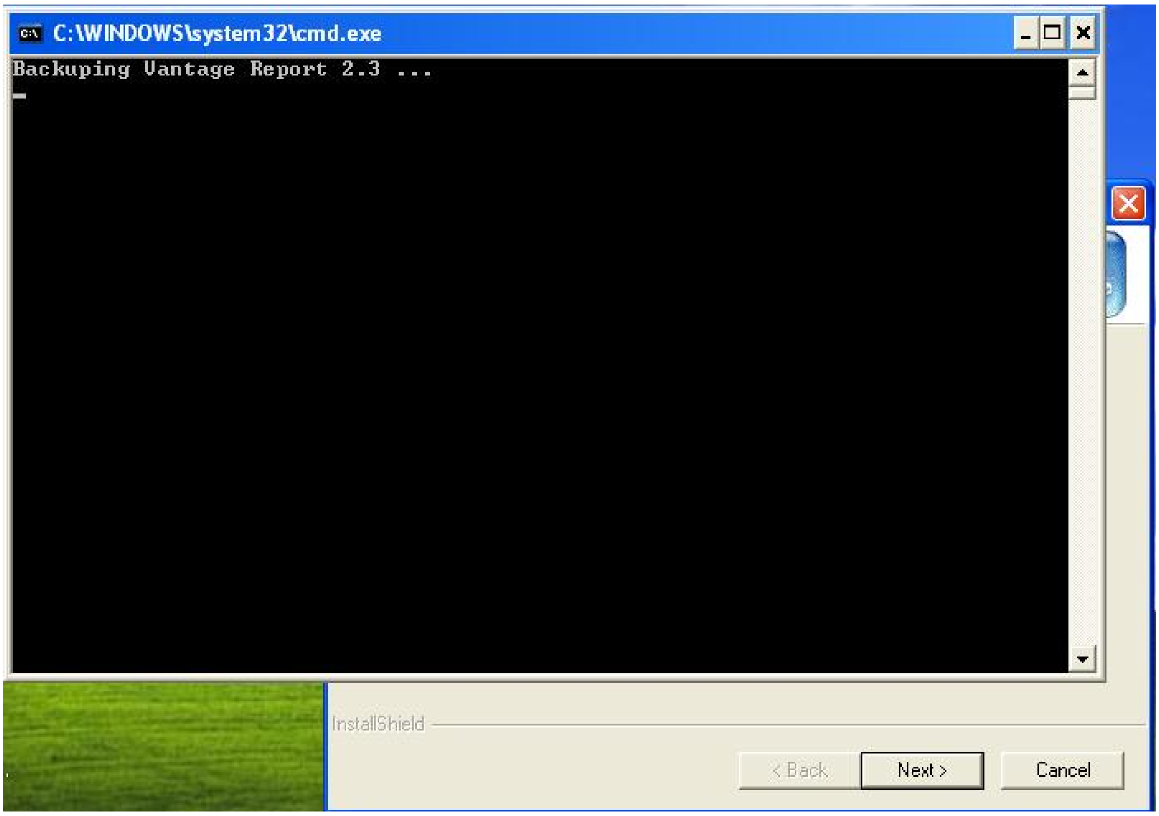
InstallShield Wizard

Cost time evaluation

The upgrade will take about 691 second(s).

Please click Next to start upgrading.

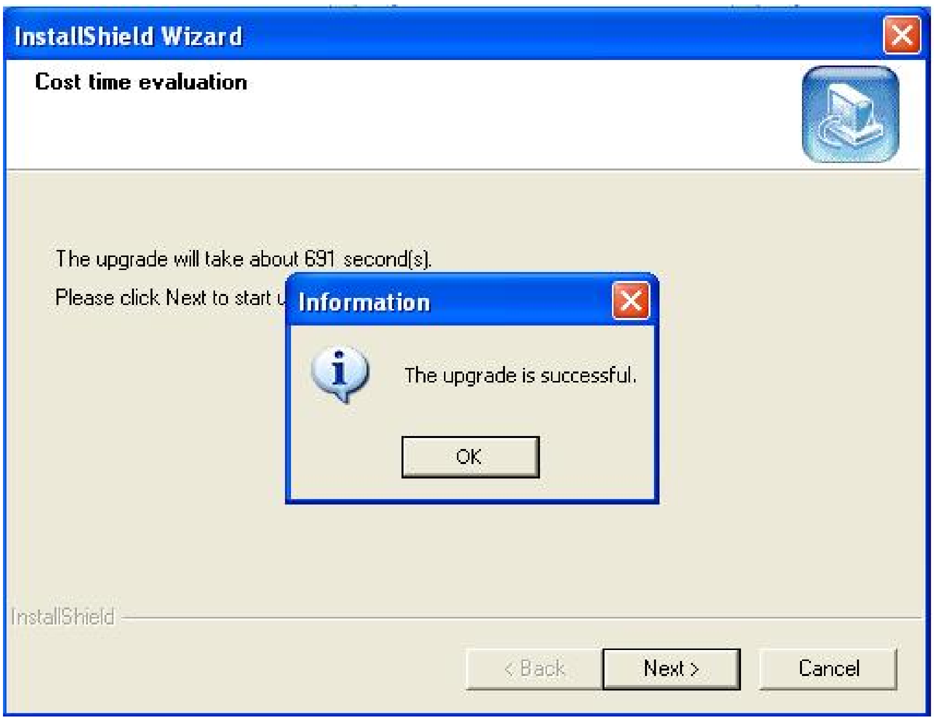
4. If upgrade is failed, the installer will restore VRPT 2.3. If the upgrade is successful, the backup will be deleted.



C:\WINDOWS\system32\cmd.exe

```
Backuping Vantage Report 2.3 ...
_
```

5. Click **OK** and **Next** button to continue the installation.



InstallShield Wizard

Cost time evaluation

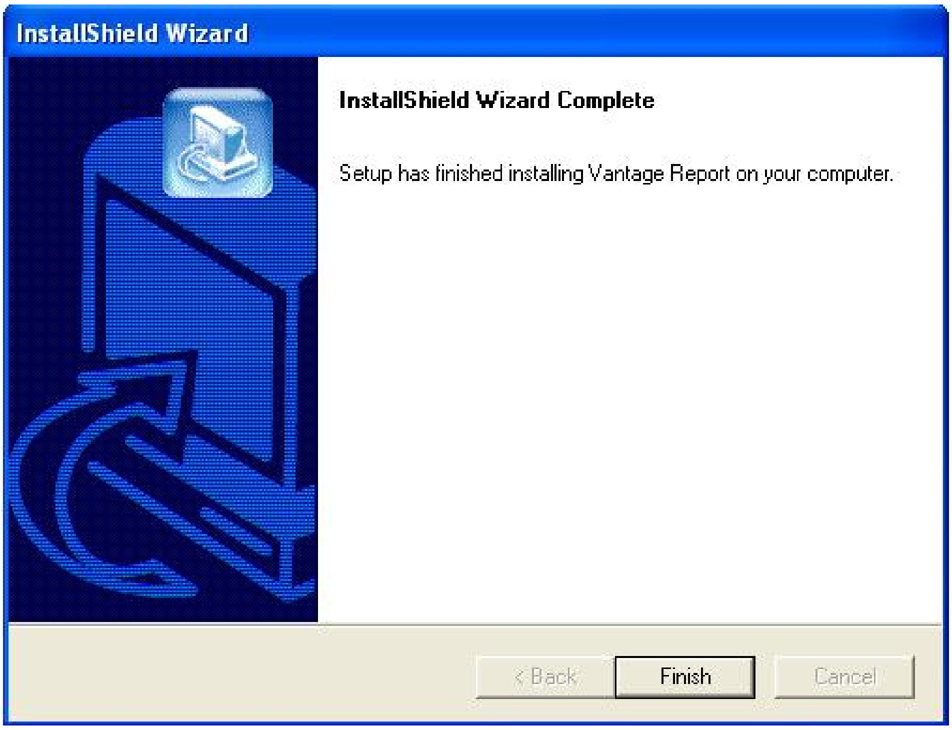
The upgrade will take about 691 second(s).

Please click Next to start u

Information

The upgrade is successful.

6. Click **Finish** button to finish the installation.



InstallShield Wizard

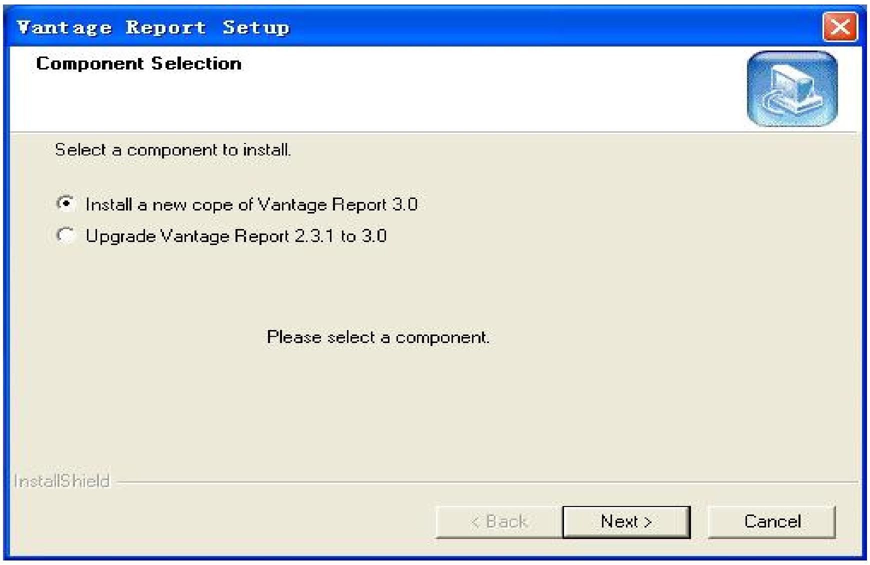
InstallShield Wizard Complete

Setup has finished installing Vantage Report on your computer.

7. Please go to start up Vantage Report and open http://<vrpt host>:<port>/ to login VRPT 2.3.1. If the login interface is still for Vantage Report 2.3, please go to clear the cached files in browser.
   After clearing the cached files, please refresh the browser.

- **The following steps detail the procedure to upgrade VRPT 2.3.1 to VRPT 3.0.**

1. Shutdown your VRPT 2.3.1 first and get Vantage Report 3.0 installation package.
2. Run the installation program. If VRPT 2.3.1 has been installed in your system, VRPT 3.0 installer will detect it automatically.


Vantage Report Setup

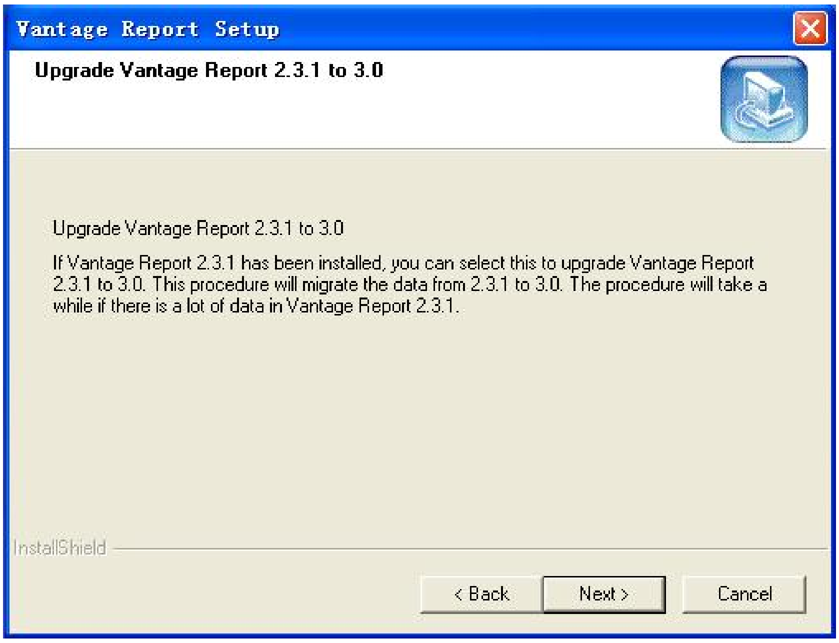
Component Selection

Select a component to install.

● Install a new cope of Vantage Report 3.0
○ Upgrade Vantage Report 2.3.1 to 3.0

Please select a component.

3. Please select **Upgrade Vantage Report 2.3.1 to 3.0** and click **Next** button if you want to upgrade your Vantage Report 2.3.1 to 3.0.

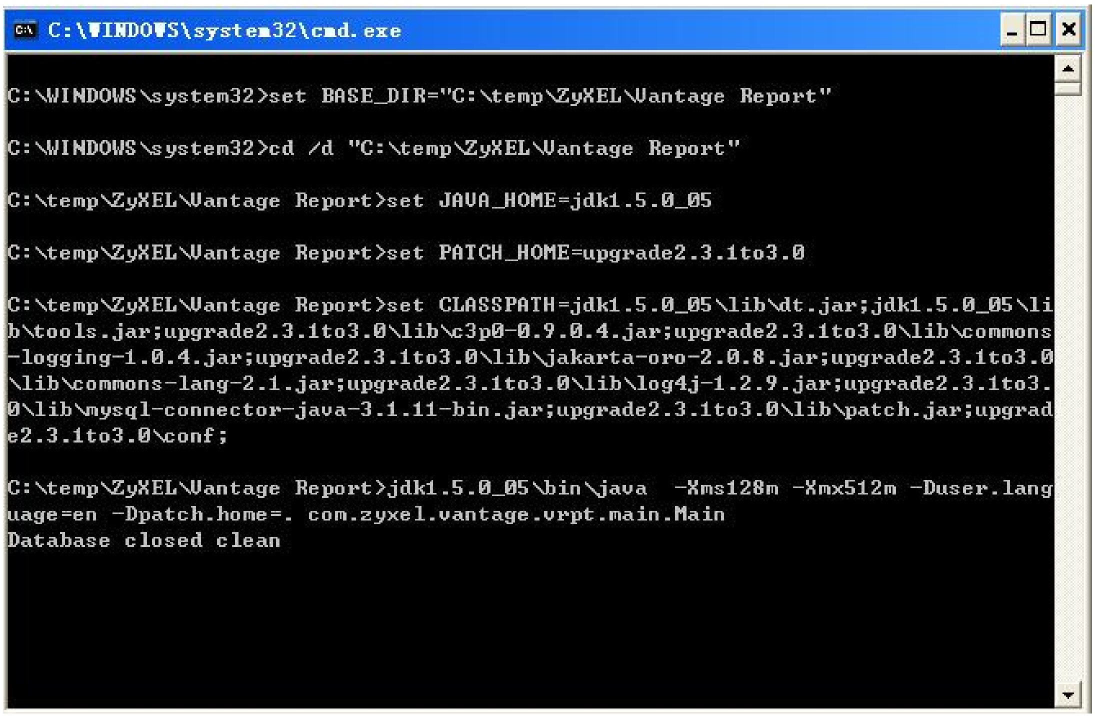


Upgrade Vantage Report 2.3.1 to 3.0

Upgrade Vantage Report 2.3.1 to 3.0

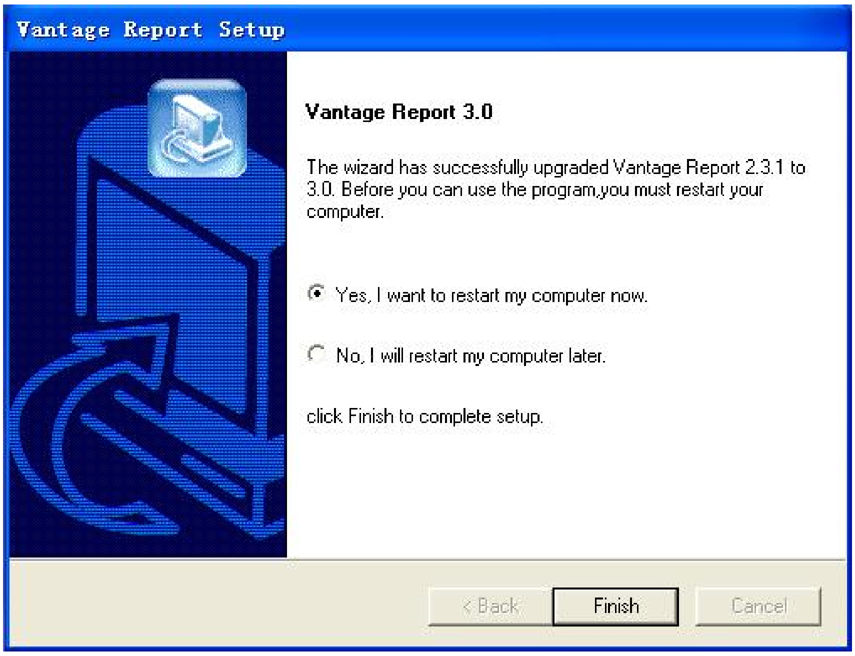
If Vantage Report 2.3.1 has been installed, you can select this to upgrade Vantage Report 2.3.1 to 3.0. This procedure will migrate the data from 2.3.1 to 3.0. The procedure will take a while if there is a lot of data in Vantage Report 2.3.1.

4. The installer will copy files to disk and start to upgrade.



```
C:\WINDOWS\system32>set BASE_DIR="C:\temp\ZyXEL\Vantage Report"

C:\WINDOWS\system32>cd /d "C:\temp\ZyXEL\Vantage Report"

C:\temp\ZyXEL\Vantage Report>set JAVA_HOME=jdk1.5.0_05

C:\temp\ZyXEL\Vantage Report>set PATCH_HOME=upgrade2.3.1to3.0

C:\temp\ZyXEL\Vantage Report>set CLASSPATH=jdk1.5.0_05\lib\dt.jar;jdk1.5.0_05\li
b\tools.jar;upgrade2.3.1to3.0\lib\c3p0-0.9.0.4.jar;upgrade2.3.1to3.0\lib\commons
-logging-1.0.4.jar;upgrade2.3.1to3.0\lib\jakarta-oro-2.0.8.jar;upgrade2.3.1to3.0
\lib\commons-lang-2.1.jar;upgrade2.3.1to3.0\lib\log4j-1.2.9.jar;upgrade2.3.1to3.
0\lib\mysql-connector-java-3.1.11-bin.jar;upgrade2.3.1to3.0\lib\patch.jar;upgrad
e2.3.1to3.0\conf;

C:\temp\ZyXEL\Vantage Report>jdk1.5.0_05\bin\java  -Xms128m -Xmx512m -Duser.lang
uage=en -Dpatch.home=. com.zyxel.vantage.vrpt.main.Main
Database closed clean
```

5. After finishing upgrade, the successful dialog will be shown.
6. Click OK button in pop-up window.



Vantage Report 3.0

The wizard has successfully upgraded Vantage Report 2.3.1 to 3.0. Before you can use the program,you must restart your computer.

● Yes, I want to restart my computer now.

○ No, I will restart my computer later.

click Finish to complete setup.

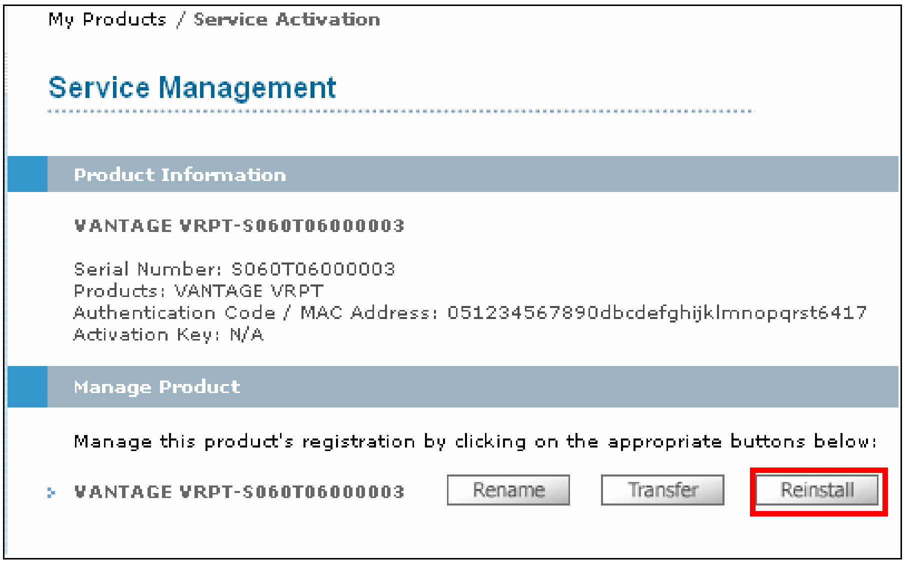
7. Click Finish button to finish this installation.
8. Please go to restart your system and open http://<vrpt host>:<port>/ to login VRPT 3.0. If login page is still for Vantage Report 2.3.1, please go to clear the cached files in browser.

### License Migration When Re-installing VRPT 3.0

Due to some reason that customer only needs to re-install VRPT on the same machine and remains other environment untouched, it is only needed to go to **System**>>**Registration** to press **Refresh** button to migrate license after finishing installing VRPT.

While if customer wants to run VRPT on a more powerful machine (OS upgrade or OS re-install on the same machine is also included) and still wants to keep previous license, he should go to myZyXEL.com to complete registration.

1. Please choose registered VRPT and press **Reinstall.**



My Products / Service Activation

Service Management

Product Information

VANTAGE VRPT-S060T06000003

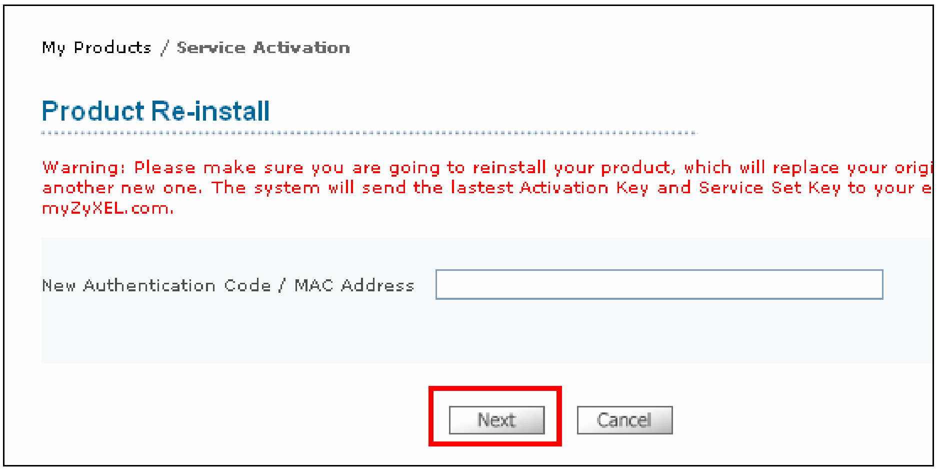
Serial Number: S060T06000003
Products: VANTAGE VRPT
Authentication Code / MAC Address: 051234567890dbcdefghijklmnopqrst6417
Activation Key: N/A

Manage Product

Manage this product's registration by clicking on the appropriate buttons below:

VANTAGE VRPT-S060T06000003

2. New Authentication Code is needed in this step. User could obtain it when installing VRPT trial version on new PC. Please go to **System**>>**Registration** to get it.



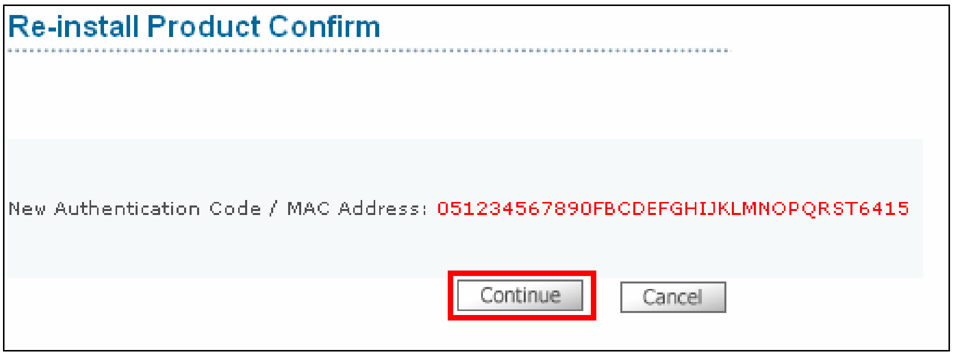
My Products / Service Activation

Product Re-install

Warning: Please make sure you are going to reinstall your product, which will replace your origi
another new one. The system will send the lastest Activation Key and Service Set Key to your e
myZyXEL.com.

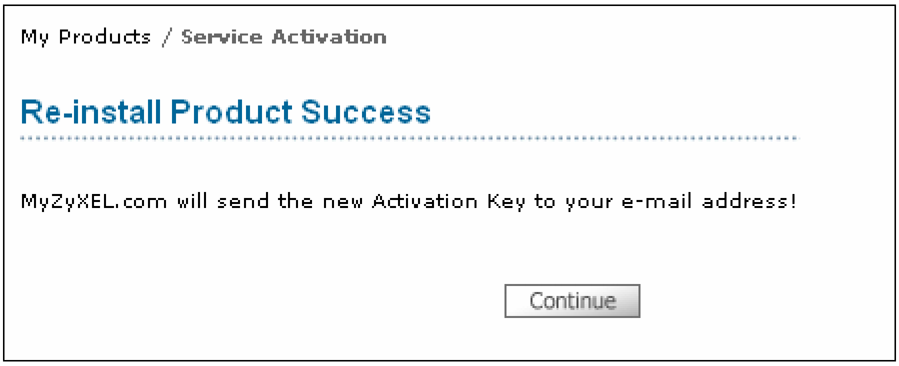
New Authentication Code / MAC Address

3. Press **Continue**, myZyXEL.com will fresh product Information to new one.



Re-install Product Confirm

New Authentication Code / MAC Address: 051234567890FBCDEFGHIJKLMNOPQRST6415



My Products / Service Activation

Re-install Product Success

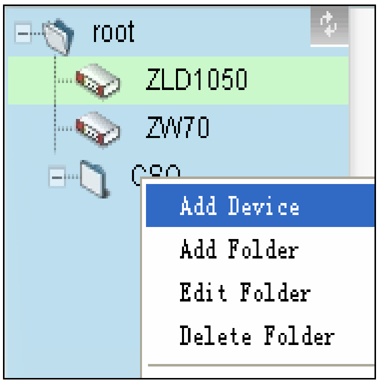
MyZyXEL.com will send the new Activation Key to your e-mail address!

### All Logs under View Logs

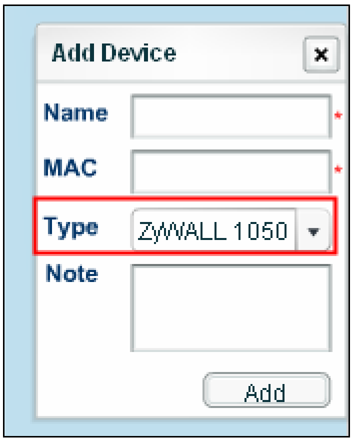
**Log**>>**Viewer** >>**All Logs** will show all the logs accepted by VRPT. It will need VRPT about 5 minutes to load these heavy data. Here 5 minutes means the interval between VRPT receives and shows such log under **Log**>>**Viewer**>>**All Logs.**

## Application Notes for ZyWALL 1050

### Add ZyWALL 1050 Device to VRPT Server



Move to the root or folder as you want and right click, and then input the **MAC** address and **Name** of ZyWALL 1050. Also make sure the Type is ZyWALL 1050. Here the **MAC** should be the smallest **MAC** address of ZyWALL 1050.



Add Device ×

Name *

MAC *

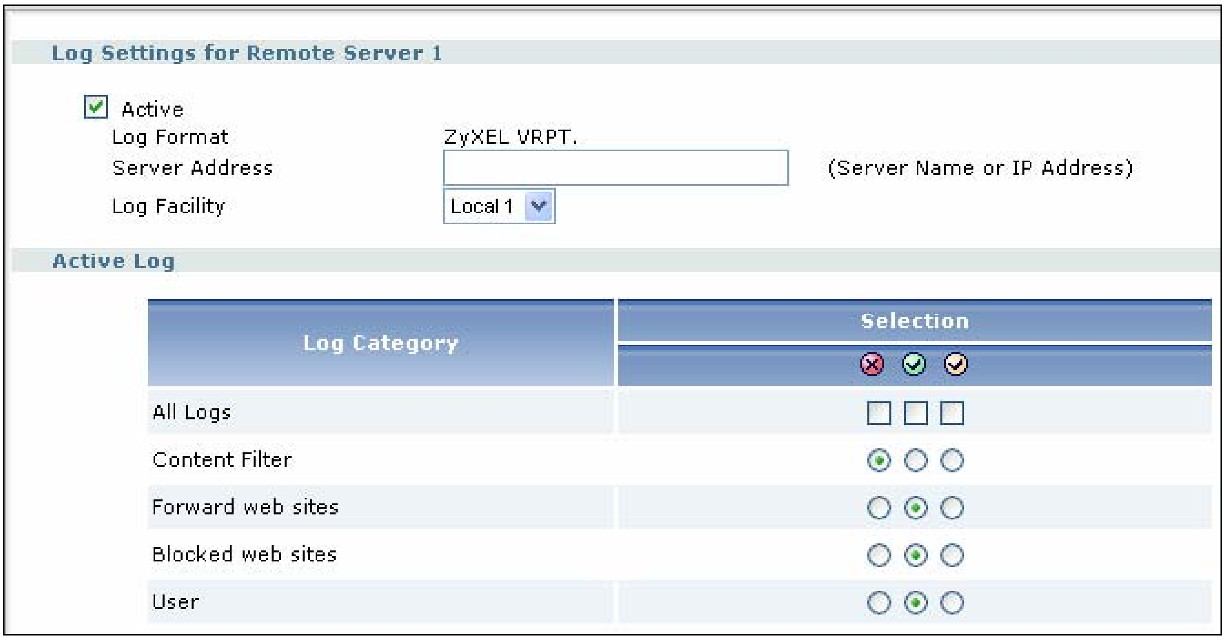
Type ZyWALL 1050 ▾

Note

Add

### Log Settings on ZyWALL 1050 for VRPT

Please go to **ZyWALL 1050**>>**Maintenance**>>**Logs**>>**Log Setting**>> **Remote Server** >>**Edit** to active log for VRPT server. Make sure the **Server Address** before VRPT server collects logs.



Log Settings for Remote Server 1

☑ Active

Log Format ZyXEL VRPT.

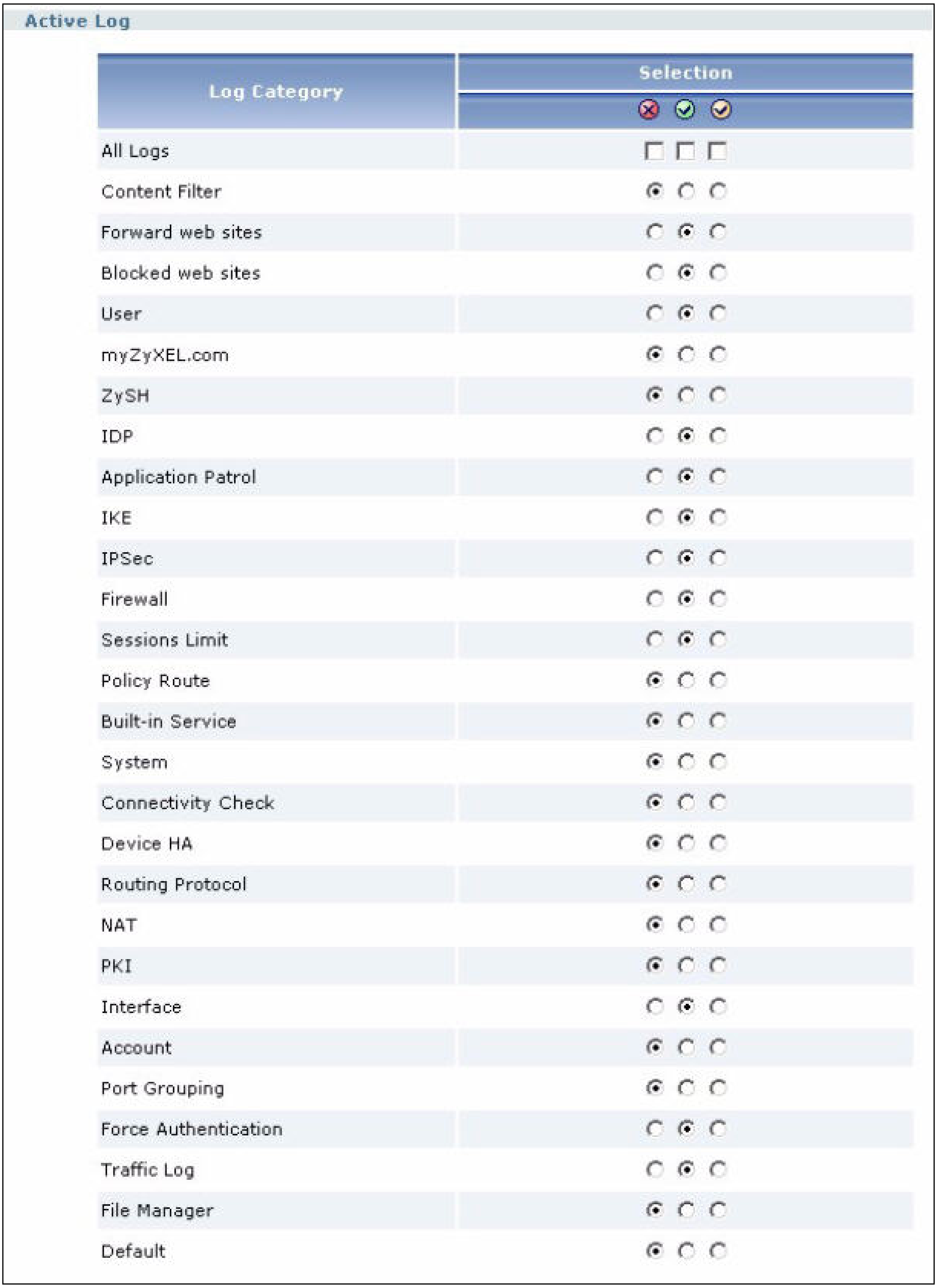
Server Address (Server Name or IP Address)

Log Facility Local 1 ▾

Active Log

| Log Category | Selection |
|---|---|
| | ☒ ✓ ✓ |
| All Logs | □ □ □ |
| Content Filter | ● ○ ○ |
| Forward web sites | ○ ● ○ |
| Blocked web sites | ○ ● ○ |
| User | ○ ● ○ |

It is recommended you to select following items

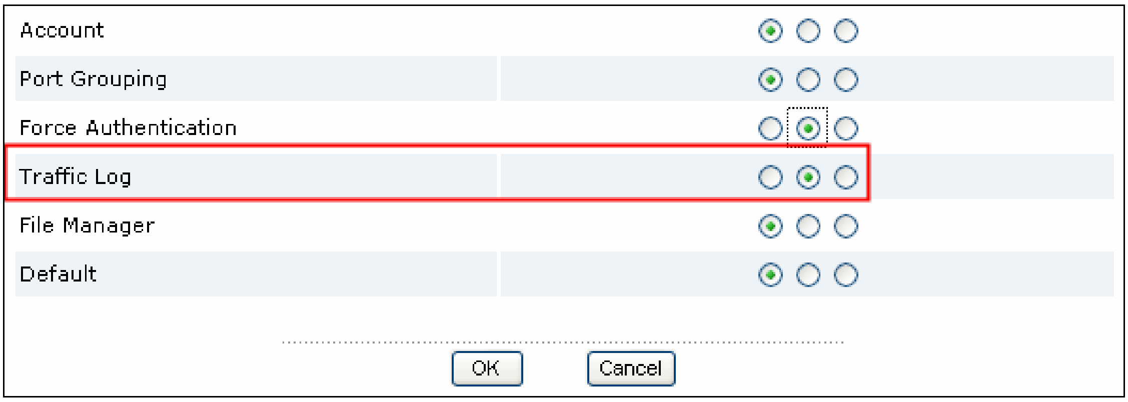


Active Log

| Log Category | Selection | | |
|---|---|---|---|
| | ⊗ | ✓ | ✓ |
| All Logs | □ | □ | □ |
| Content Filter | ● | ○ | ○ |
| Forward web sites | ○ | ● | ○ |
| Blocked web sites | ○ | ● | ○ |
| User | ○ | ● | ○ |
| myZyXEL.com | ● | ○ | ○ |
| ZySH | ● | ○ | ○ |
| IDP | ○ | ● | ○ |
| Application Patrol | ○ | ● | ○ |
| IKE | ○ | ● | ○ |
| IPSec | ○ | ● | ○ |
| Firewall | ○ | ● | ○ |
| Sessions Limit | ○ | ● | ○ |
| Policy Route | ● | ○ | ○ |
| Built-in Service | ● | ○ | ○ |
| System | ● | ○ | ○ |
| Connectivity Check | ● | ○ | ○ |
| Device HA | ● | ○ | ○ |
| Routing Protocol | ● | ○ | ○ |
| NAT | ● | ○ | ○ |
| PKI | ● | ○ | ○ |
| Interface | ○ | ● | ○ |
| Account | ● | ○ | ○ |
| Port Grouping | ● | ○ | ○ |
| Force Authentication | ○ | ● | ○ |
| Traffic Log | ○ | ● | ○ |
| File Manager | ● | ○ | ○ |
| Default | ● | ○ | ○ |

## How to enable traffic log feature ZyWALL 1050

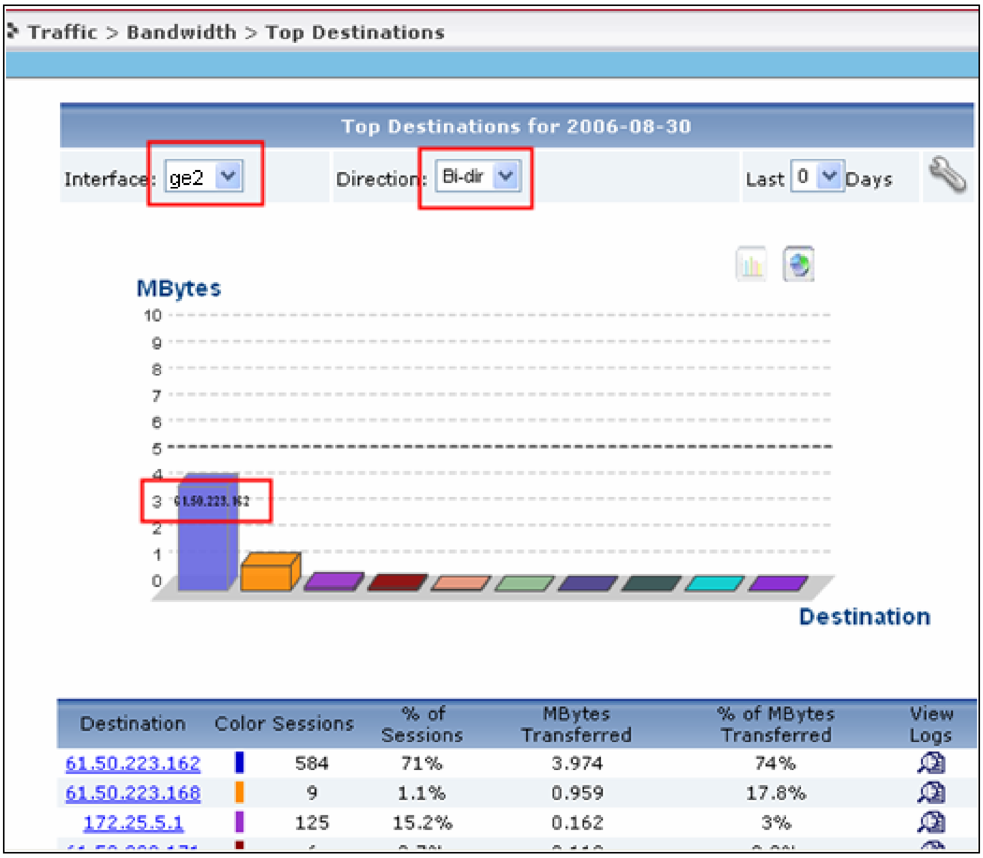
Please go to **ZyWALL 1050**>>**Maintenance**>>**Logs**>>**Log Setting**>> **Remote Server** >>**Edit** to Enable the traffic log.



| | |
|---|---|
| Account | ● ○ ○ |
| Port Grouping | ● ○ ○ |
| Force Authentication | ○ ● ○ |
| Traffic Log | ○ ● ○ |
| File Manager | ● ○ ○ |
| Default | ● ○ ○ |

## Checking Bandwidth Usage

It is almost daily job for MIS administrator to check the bandwidth usage of the company. VRPT 3.0 supplies special enhancement for ZyWALL 1050’s bandwidth usage report. Besides traffic direction, you can specify Interface for checking.



Top Destinations for 2006-08-30

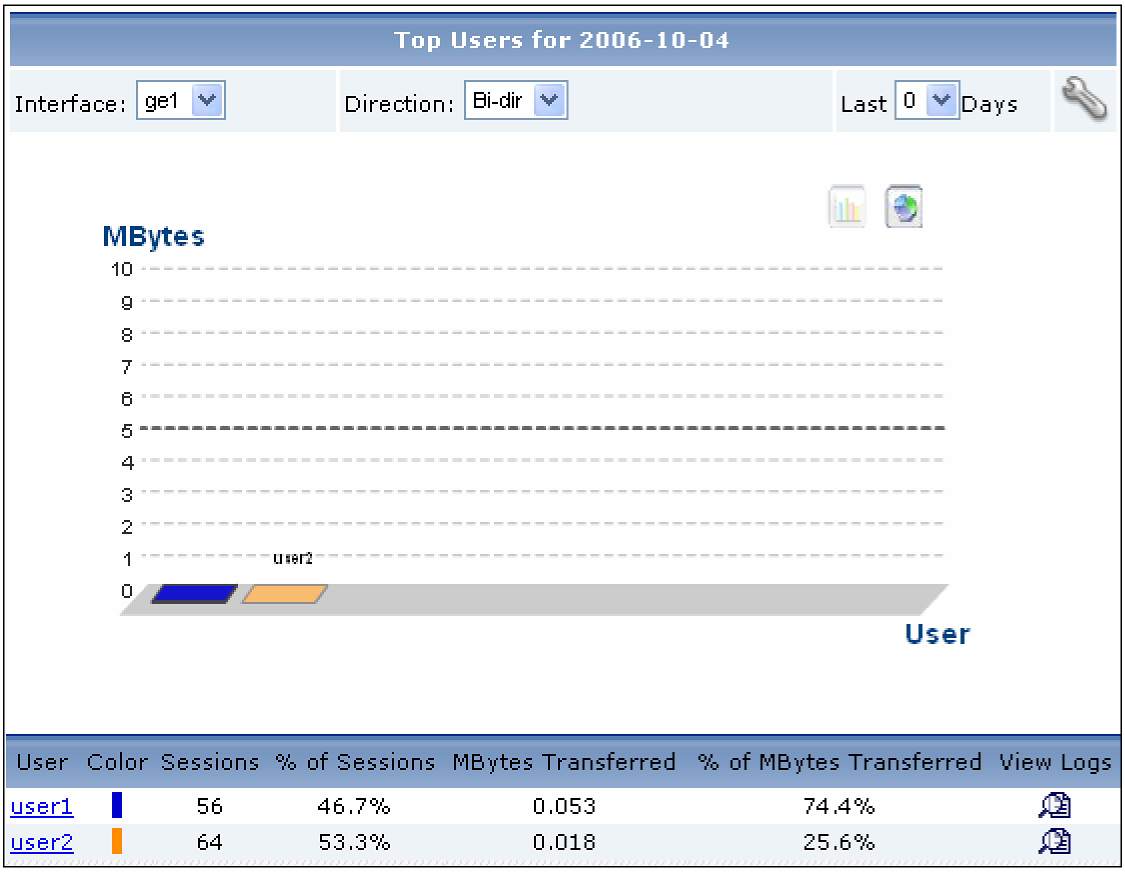
Interface: ge2 Direction: Bi-dir Last 0 Days

| Destination | Color | Sessions | % of Sessions | MBytes Transferred | % of MBytes Transferred | View Logs |
|---|---|---|---|---|---|---|
| 61.50.223.162 | 🟦 | 584 | 71% | 3.974 | 74% | 🔍 |
| 61.50.223.168 | 🟧 | 9 | 1.1% | 0.959 | 17.8% | 🔍 |
| 172.25.5.1 | 🟪 | 125 | 15.2% | 0.162 | 3% | 🔍 |

Especially, you can get what you can see by clicking the bar on the report.
For example, when you click the first bar in the sample report, you can easily find that 61.50.223.162 was the top destination that has been accessed.

### User Aware Application on Traffic Report

User aware is an import conception on ZyWALL 1050. Vantage Report supplies user aware report for administrator to manage the network. Let’s take bandwidth report as an example. Under **Bandwidth**>>**Top Users**, it is easily to look through the bandwidth usage for every user. Also you can just click the bar on the report to get brief information.
The sample displays shows the usage report for user1 and user2.



Top Users for 2006-10-04

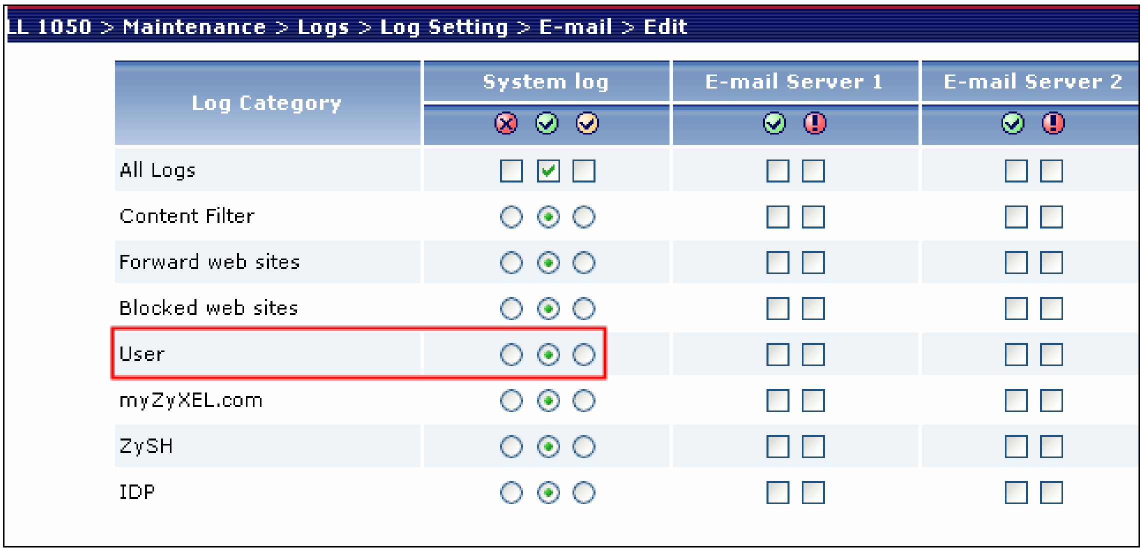
Interface: ge1 Direction: Bi-dir Last 0 Days

| User | Color | Sessions | % of Sessions | MBytes Transferred | % of MBytes Transferred | View Logs |
|---|---|---|---|---|---|---|
| user1 | 🟦 | 56 | 46.7% | 0.053 | 74.4% | 🔍 |
| user2 | 🟧 | 64 | 53.3% | 0.018 | 25.6% | 🔍 |

## User Aware Application on Login Record

That the login records on VRPT server are user aware is consistent with ZyWALL 1050. You can monitor and trace the login history of each user under menu **Event**>>**Login** only if you has enabled the centralized log on ZyWALL 1050.

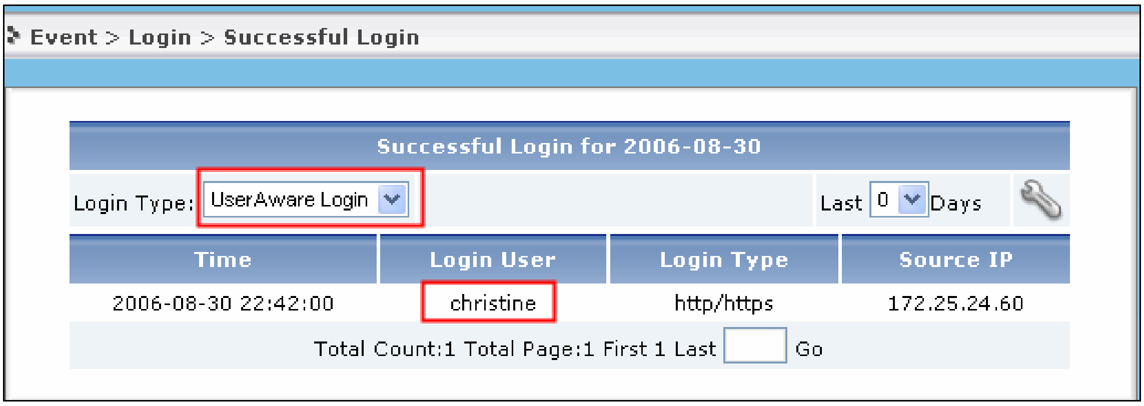
1. Enable the log on ZyWALL 1050 under menu **ZyWALL 1050**>> **Maintenance**>>**Logs**>> **Log Settings**>>**E-mail**>>**Edit.**



LL 1050 > Maintenance > Logs > Log Setting > E-mail > Edit

| Log Category | System log | | | E-mail Server 1 | | E-mail Server 2 | |
|---|---|---|---|---|---|---|---|
| | ☒ | ✓ | ✓ | ✓ | ! | ✓ | ! |
| All Logs | □ | ☑ | □ | □ | □ | □ | □ |
| Content Filter | ○ | ● | ○ | □ | □ | □ | □ |
| Forward web sites | ○ | ● | ○ | □ | □ | □ | □ |
| Blocked web sites | ○ | ● | ○ | □ | □ | □ | □ |
| User | ○ | ● | ○ | □ | □ | □ | □ |
| myZyXEL.com | ○ | ● | ○ | □ | □ | □ | □ |
| ZySH | ○ | ● | ○ | □ | □ | □ | □ |
| IDP | ○ | ● | ○ | □ | □ | □ | □ |

2. Check the login record for user.



Event > Login > Successful Login

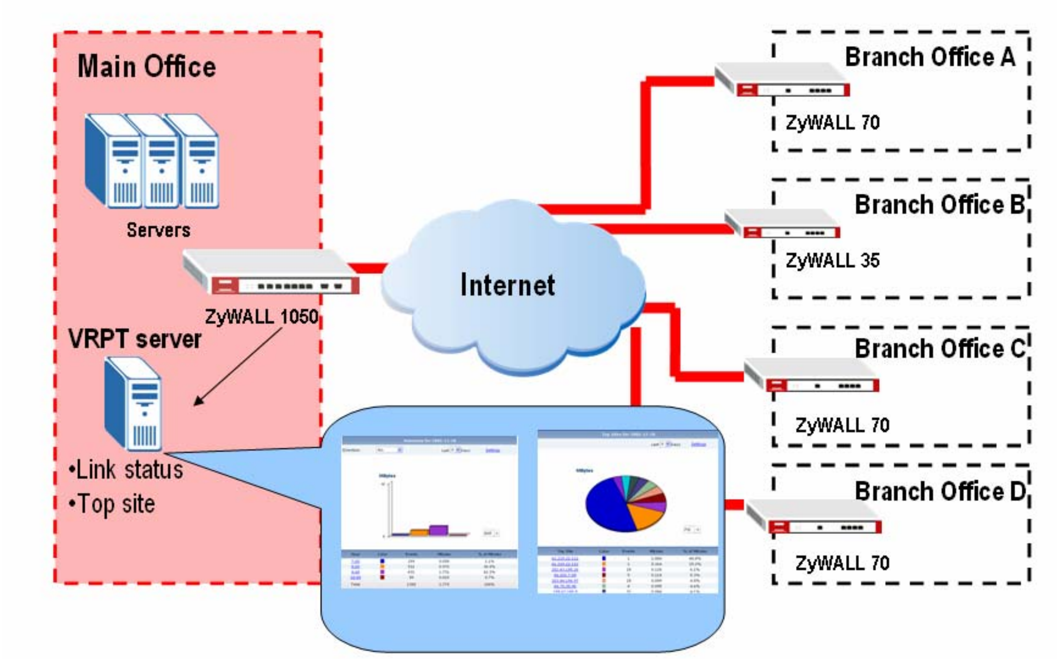
Successful Login for 2006-08-30

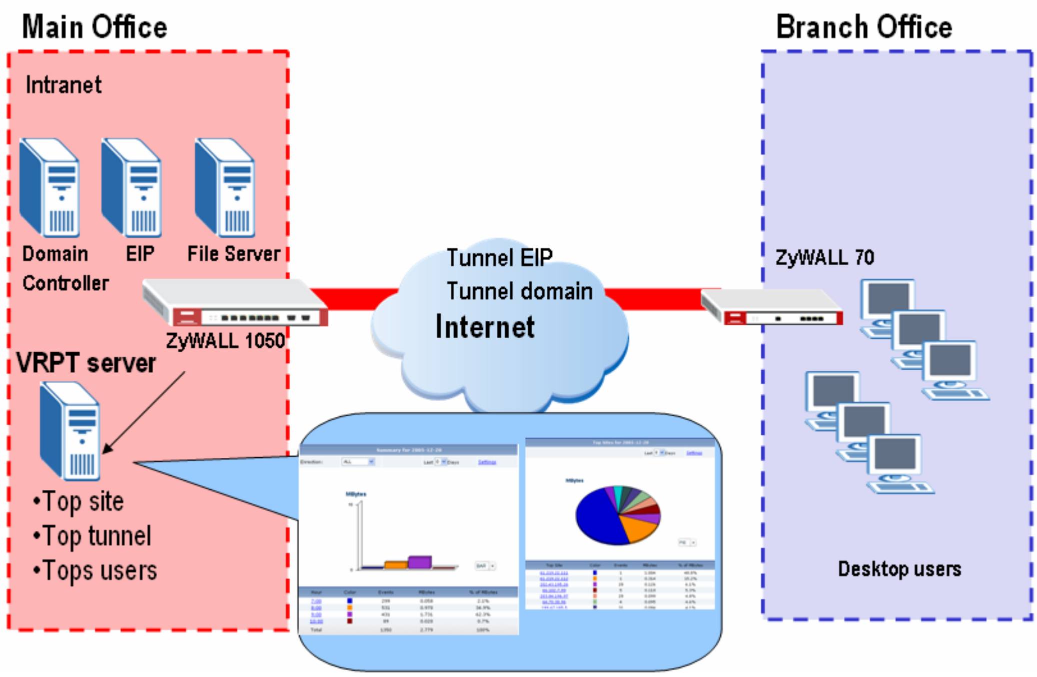
Login Type: UserAware Login    Last 0 Days

| Time | Login User | Login Type | Source IP |
|---|---|---|---|
| 2006-08-30 22:42:00 | christine | http/https | 172.25.24.60 |

Total Count:1 Total Page:1 First 1 Last Go

## ZyWALL 1050 VPN Site-to-Site Application



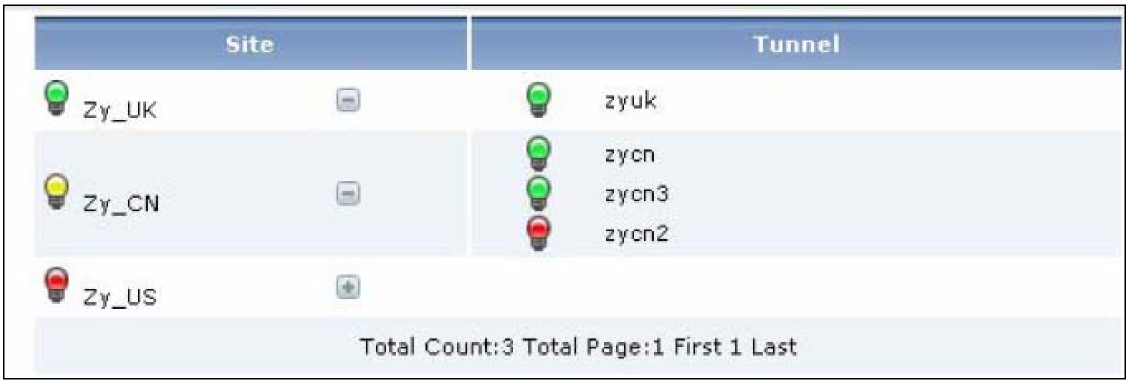


Let's suppose scenario between HQ and branch office.

Companies have geographically distributed operation offices, Branch A, Branch B, Branch C and Branch D. Each branch office (remote site) builds several IPsec VPN tunnels for different purpose. One is for EIP and the other is for Domain controller. Different users execute different application by different tunnel.

HQ MIS administrator can trace the usage of site to site VPN by VPN report.

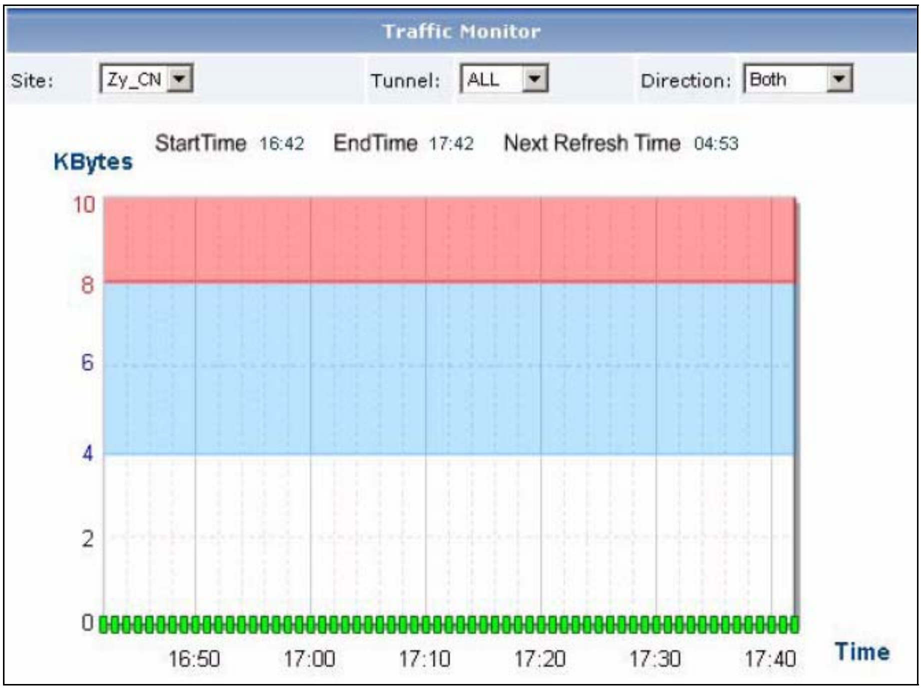
1. Administrator can check the link status by **Link Status** report under **VPN**>>**Site-to-Site**>>**Link Status**. Green status means tunnel is up and red means tunnel is down.



| Site | | Tunnel |
|---|---|---|
| 🟢 Zy_UK | ⊟ | 🟢 zyuk |
| 🟡 Zy_CN | ⊟ | 🟢 zycn<br>🟢 zycn3<br>🔴 zycn2 |
| 🔴 Zy_US | ⊞ | |

Total Count:3 Total Page:1 First 1 Last

2. **Traffic Monitor** report helps the administrator to monitor the total amount of traffic handled by a device's VPN tunnels.

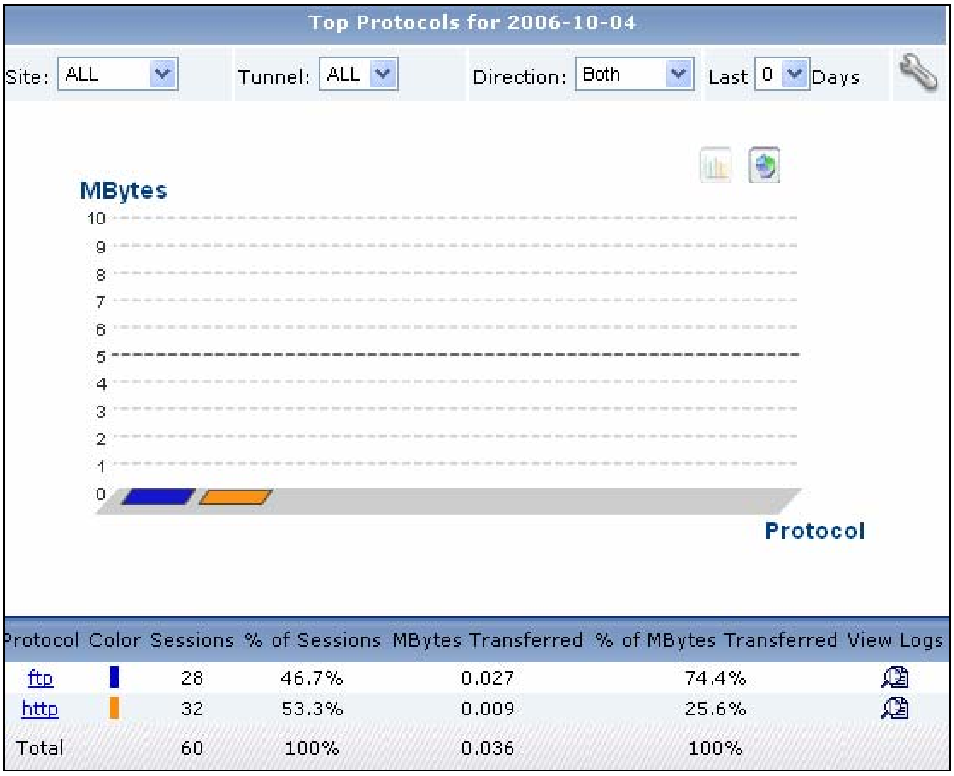


Traffic Monitor

Site: Zy_CN  Tunnel: ALL  Direction: Both

StartTime 16:42  EndTime 17:42  Next Refresh Time 04:53

3. **Top Protocol** report can tell which application consumes most bandwidth. If it illegal application appears, you can use firewall or policy rule to stop the waste of bandwidth.

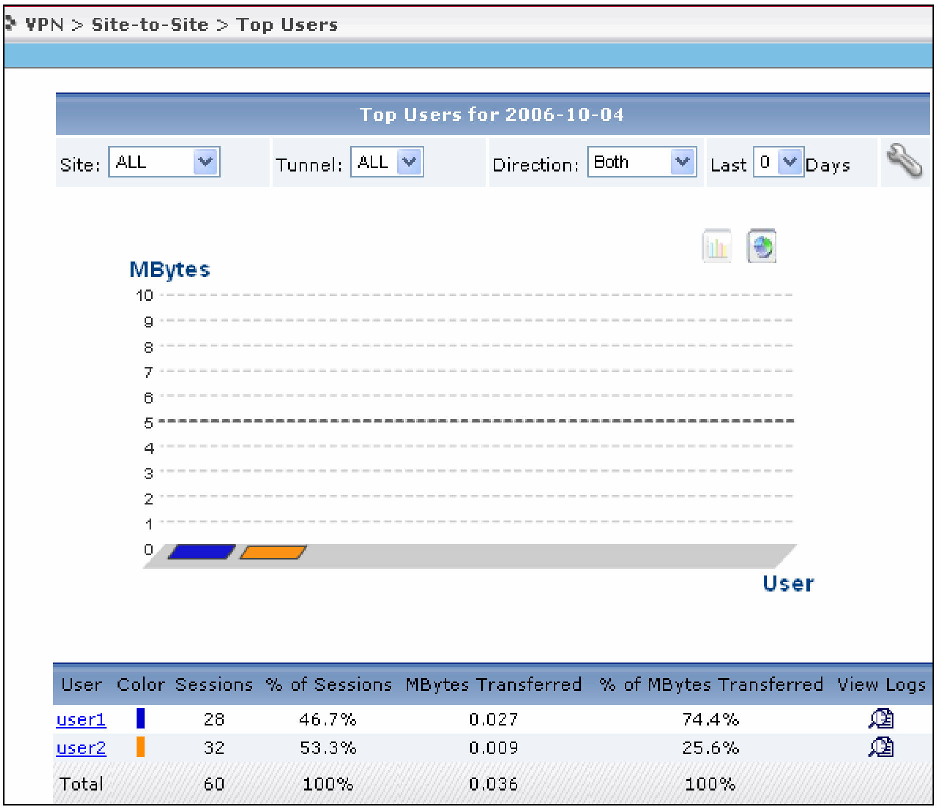


Top Protocols for 2006-10-04

Site: ALL Tunnel: ALL Direction: Both Last 0 Days

| Protocol | Color | Sessions | % of Sessions | MBytes Transferred | % of MBytes Transferred | View Logs |
|---|---|---|---|---|---|---|
| ftp | 🟦 | 28 | 46.7% | 0.027 | 74.4% | |
| http | 🟧 | 32 | 53.3% | 0.009 | 25.6% | |
| Total | | 60 | 100% | 0.036 | 100% | |

4. Also you can check which user or host consumes mostly bandwidth by **Top Users** report or **Top Hosts** report.



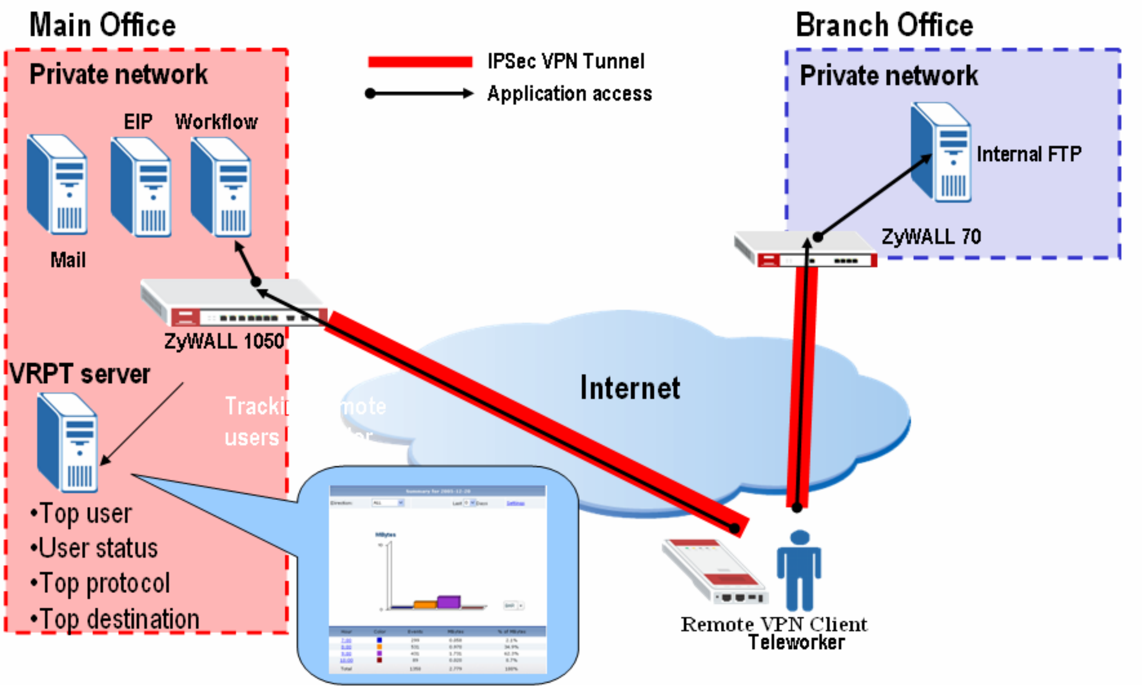
VPN > Site-to-Site > Top Users

Top Users for 2006-10-04

Site: ALL Tunnel: ALL Direction: Both Last 0 Days

| User | Color | Sessions | % of Sessions | MBytes Transferred | % of MBytes Transferred | View Logs |
|---|---|---|---|---|---|---|
| user1 | 🟦 | 28 | 46.7% | 0.027 | 74.4% | |
| user2 | 🟧 | 32 | 53.3% | 0.009 | 25.6% | |
| Total | | 60 | 100% | 0.036 | 100% | |

## ZyWALL 1050 VPN Remote Access Application

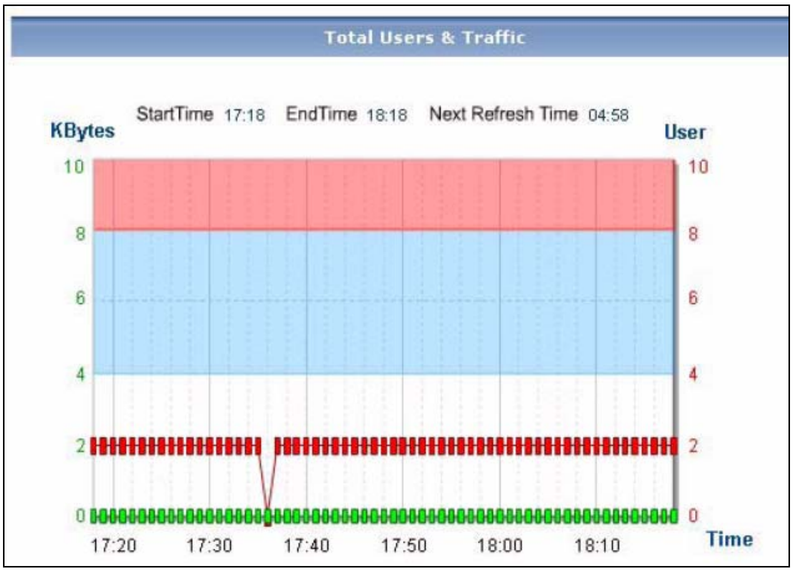


Suppose there's VPN mobile user is an employee on the road (a.k.a. teleworker). He wants to gain full network access simply by tapping into an Internet connection.

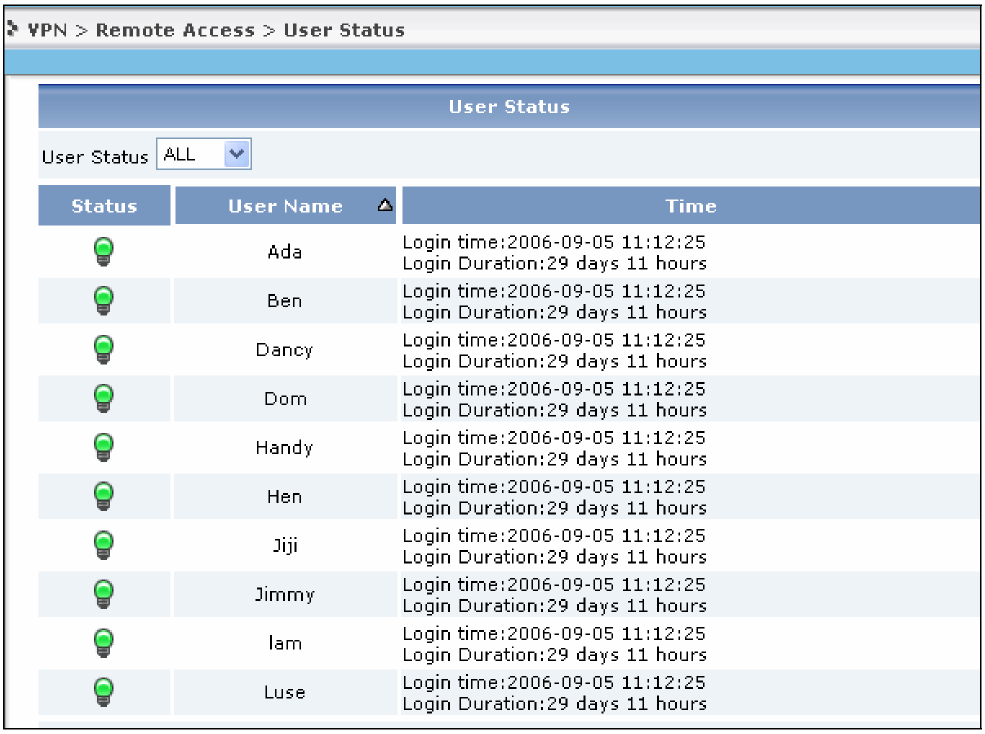
H can build IPSec VPN by remote VPN client, for example ZyWALLP1, to access HQ or branch off internal or remote resource (mail, EIP….).

HQ or branch MIS administrator can control the behavior of remote access by Remote Access report.

1. **Top User & Traffic** can monitor the total number of remote access users connected to the device and the amount of traffic the device handled for the dynamic VPN tunnels.



2. Administrator can check which user is on line by **User Status** report.



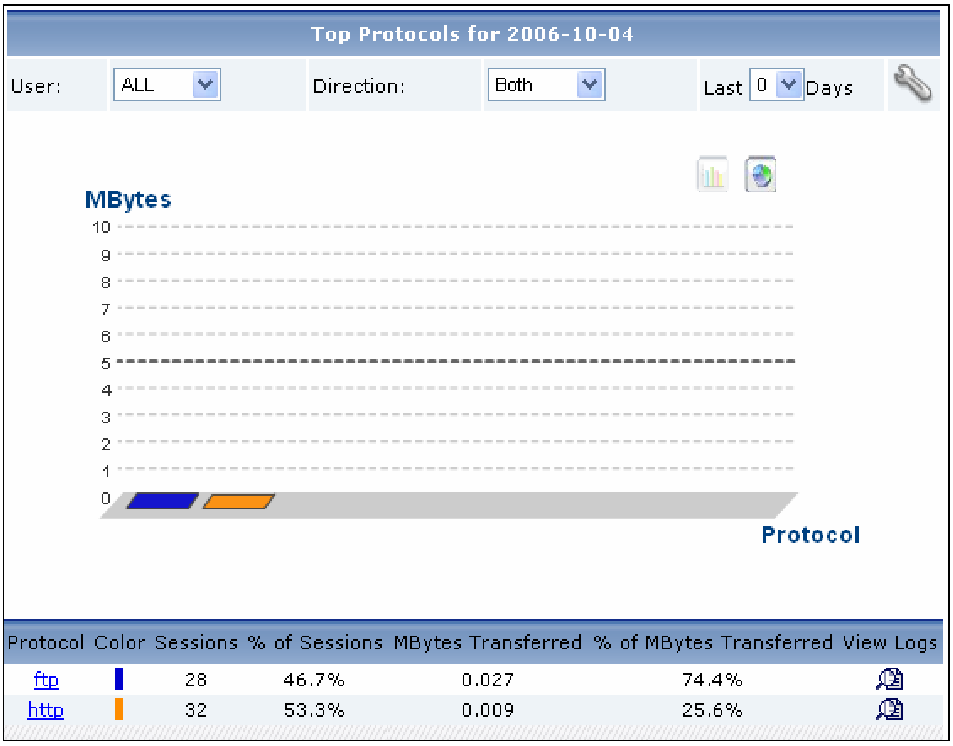
VPN > Remote Access > User Status

User Status

User Status: ALL

| Status | User Name | Time |
|---|---|---|
| ● | Ada | Login time:2006-09-05 11:12:25<br>Login Duration:29 days 11 hours |
| ● | Ben | Login time:2006-09-05 11:12:25<br>Login Duration:29 days 11 hours |
| ● | Dancy | Login time:2006-09-05 11:12:25<br>Login Duration:29 days 11 hours |
| ● | Dom | Login time:2006-09-05 11:12:25<br>Login Duration:29 days 11 hours |
| ● | Handy | Login time:2006-09-05 11:12:25<br>Login Duration:29 days 11 hours |
| ● | Hen | Login time:2006-09-05 11:12:25<br>Login Duration:29 days 11 hours |
| ● | Jiji | Login time:2006-09-05 11:12:25<br>Login Duration:29 days 11 hours |
| ● | Jimmy | Login time:2006-09-05 11:12:25<br>Login Duration:29 days 11 hours |
| ● | Iam | Login time:2006-09-05 11:12:25<br>Login Duration:29 days 11 hours |
| ● | Luse | Login time:2006-09-05 11:12:25<br>Login Duration:29 days 11 hours |

3. **Top Protocol** report can tell which application consumes most bandwidth.

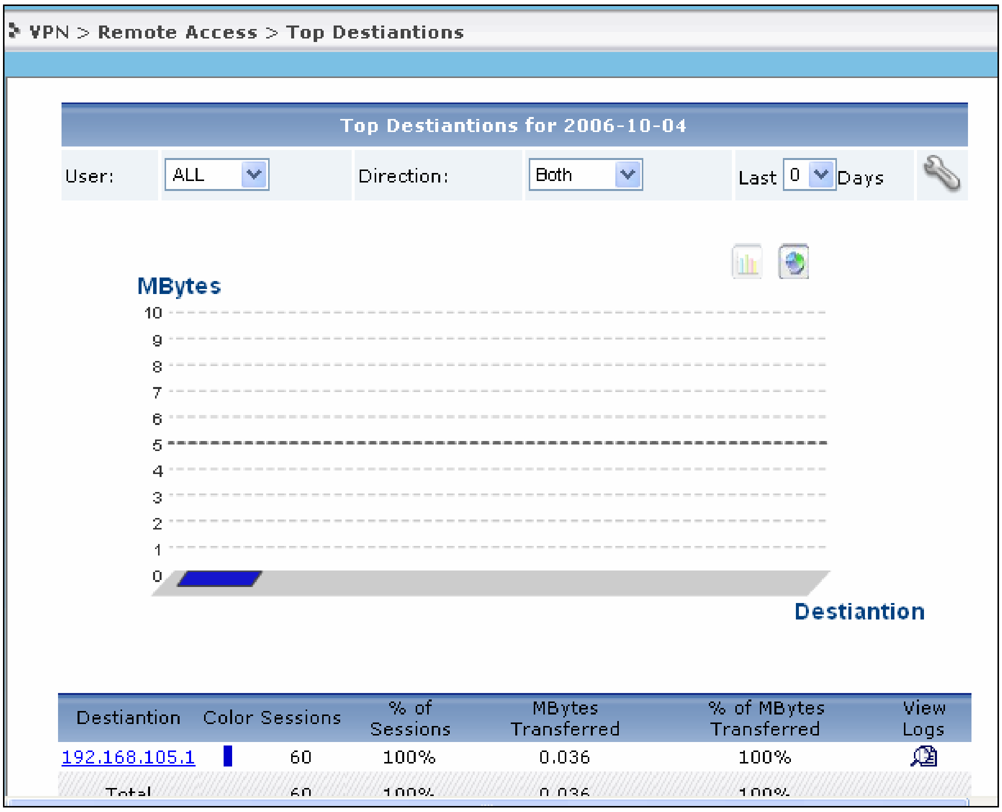


Top Protocols for 2006-10-04

User: ALL Direction: Both Last 0 Days

| Protocol | Color | Sessions | % of Sessions | MBytes Transferred | % of MBytes Transferred | View Logs |
|---|---|---|---|---|---|---|
| ftp | 🟦 | 28 | 46.7% | 0.027 | 74.4% | 🔍 |
| http | 🟧 | 32 | 53.3% | 0.009 | 25.6% | 🔍 |

4. **Top destination** report reflects which server most user access.



VPN > Remote Access > Top Destiantions

Top Destiantions for 2006-10-04

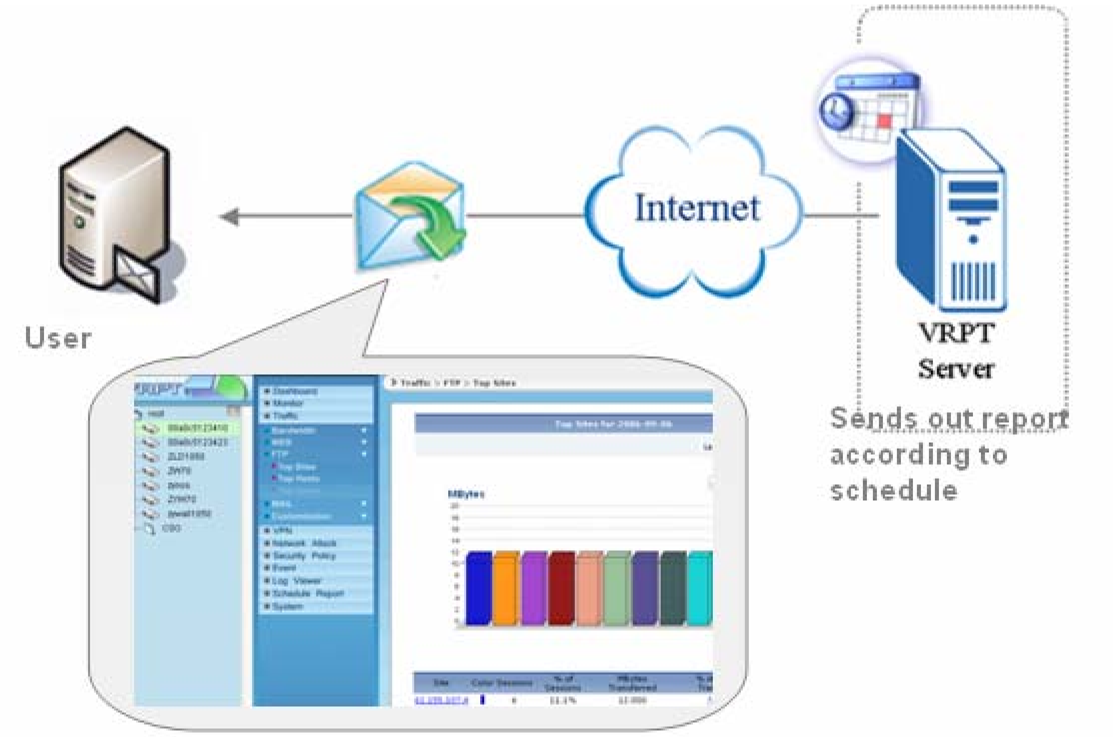
User: ALL Direction: Both Last 0 Days

| Destiantion | Color | Sessions | % of Sessions | MBytes Transferred | % of MBytes Transferred | View Logs |
|---|---|---|---|---|---|---|
| 192.168.105.1 | ▮ | 60 | 100% | 0.036 | 100% | 🔍 |
| Total | | 60 | 100% | 0.036 | 100% | |

## Advanced Application Notes

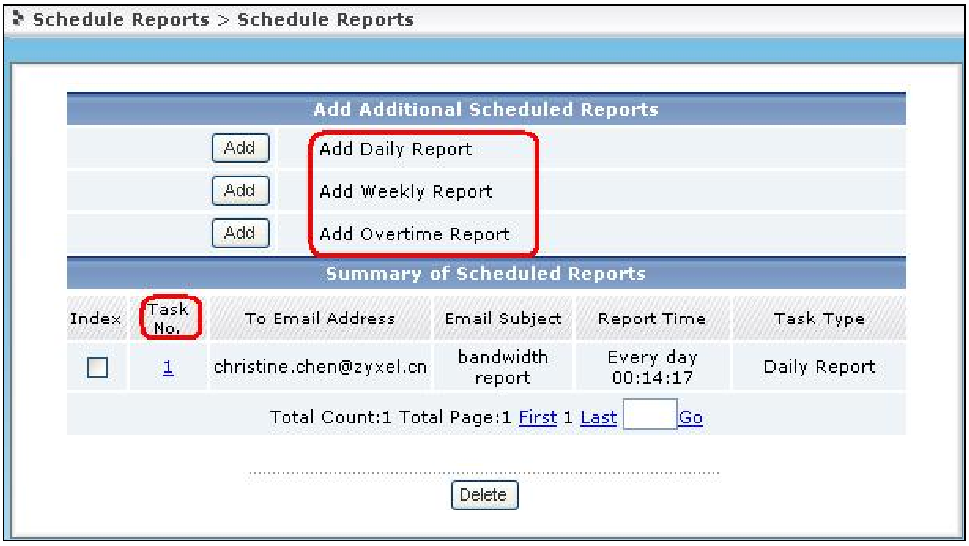
### Using Schedule Report

VRPT provides support for emailing and archiving daily, weekly and overtime reports. User could create such schedules for these reports (daily/weekly/overtime) for individual device. VRPT will generate the reports and send them to receiver as an email according to the schedule. And user could check them at their available time. Below figure shows the brief flow for scheduled report process.



1. Go to **Schedule Reports**>>**Schedule Reports** for adding schedule reports. There are three kinds of schedule reports (Daily & Weekly & Overtime) available.

**NOTE:** the schedule **Task** list will contain no more than 20 items. User could create 20 schedules for each device at most.



Schedule Reports > Schedule Reports

Add Additional Scheduled Reports

| | |
|---|---|
| Add | Add Daily Report |
| Add | Add Weekly Report |
| Add | Add Overtime Report |

Summary of Scheduled Reports

| Index | Task No. | To Email Address | Email Subject | Report Time | Task Type |
|---|---|---|---|---|---|
| □ | 1 | christine.chen@zyxel.cn | bandwidth report | Every day 00:14:17 | Daily Report |

Total Count:1 Total Page:1 First 1 Last Go

Delete

2. Design customized configuration for schedule report. Take **Overtime Report** for example.

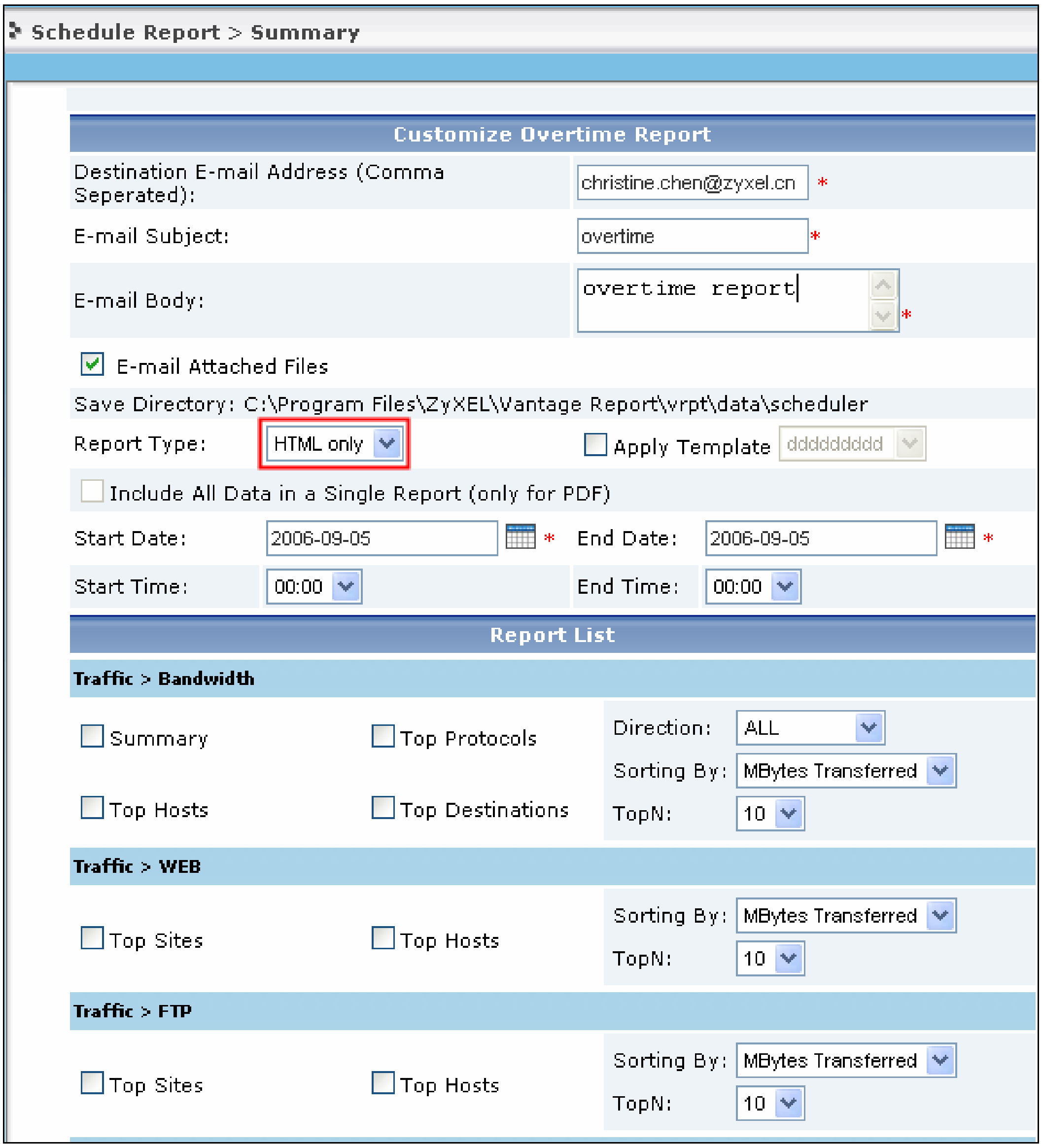
2.1. Go to **Add Overtime Report** scheduled report, **Destination E-mail address**, **Email-Subject and Email-Body** are needed to be filled in first to configure the email info for user.

2.2. Choose report type. There are two types of **Report Type** user could choose. One is **HTML** pattern and the other is **PDF** pattern. The HTML pattern looks just like the one you could check on VRPT. User could take it as offline VRPT report.

3.0. Choose the time duration. After doing that user should choose **Start Date** and **End Date** to give the time duration. For Daily Report configuration there's no such feature and for Weekly Report there's **Day to Submit** feature instead.

2.4. About **Include All Data in a Single Report** feature. Now **Include All Data in a Single Report** feature is only for PDF pattern report. If you enable this feature the scheduled report will contain all statistics in a single PDF file and it is easy to read. Otherwise, each item in report list will form a PDF file.

2.5. Finally user should choose the report he/she wants from **Report List**.



Schedule Report > Summary

Customize Overtime Report

| | |
|---|---|
| Destination E-mail Address (Comma Seperated): | christine.chen@zyxel.cn * |
| E-mail Subject: | overtime * |
| E-mail Body: | overtime report * |

☑ E-mail Attached Files

Save Directory: C:\Program Files\ZyXEL\Vantage Report\vrpt\data\scheduler

Report Type: HTML only ☐ Apply Template dddddddd

☐ Include All Data in a Single Report (only for PDF)

Start Date: 2006-09-05 * End Date: 2006-09-05 *

Start Time: 00:00 End Time: 00:00

Report List

**Traffic > Bandwidth**

☐ Summary ☐ Top Protocols Direction: ALL

Sorting By: MBytes Transferred

☐ Top Hosts ☐ Top Destinations TopN: 10

**Traffic > WEB**

☐ Top Sites ☐ Top Hosts Sorting By: MBytes Transferred TopN: 10

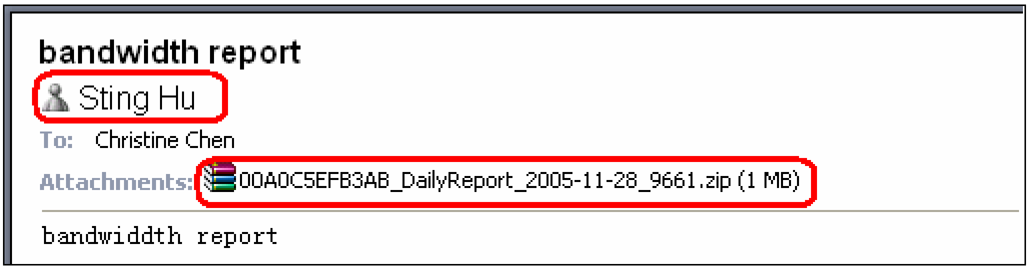
**Traffic > FTP**

☐ Top Sites ☐ Top Hosts Sorting By: MBytes Transferred TopN: 10

**NOTE:** If you want to add a daily report, do not set the value for log storing days as 1. Because the daily report only reports log statistics yesterday. That is to say the mail you get each time you've set will show nothing if you set "log store day=1". The date in the PDF /HTML file is the day before.

User could only set scheduled report for device individually.

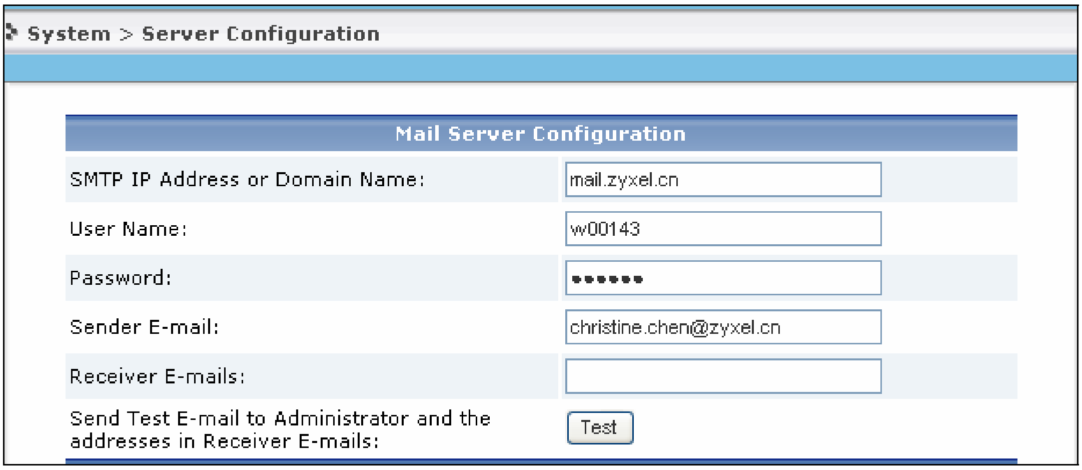
3. VRPT generates scheduled report.
Below picture shows Daily report sample received by user.



bandwidth report
Sting Hu
To: Christine Chen
Attachments: 00A0C5EFB3AB_DailyReport_2005-11-28_9661.zip (1 MB)

bandwiddth report

Here Sender 'Sting Hu' matches the **Sender Email** under **System**>>**Server Configuration**>>**Sender Email**.



System > Server Configuration

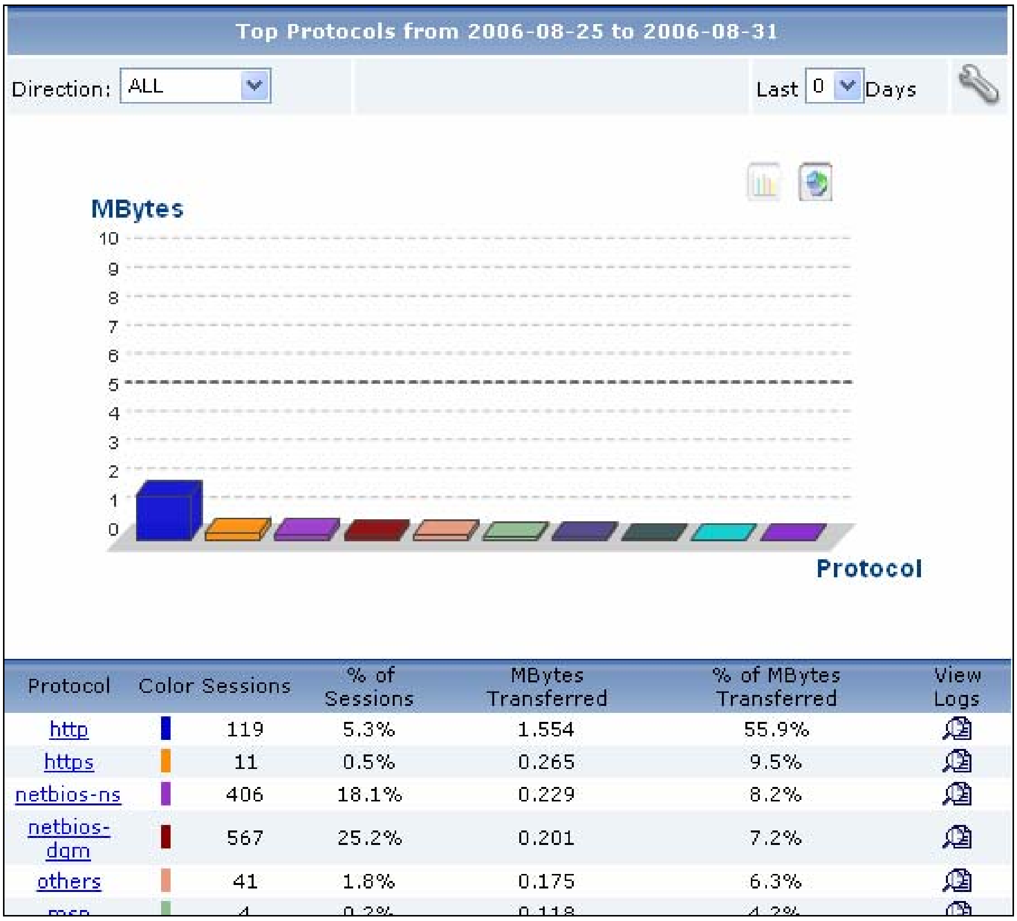
Mail Server Configuration

| | |
|---|---|
| SMTP IP Address or Domain Name: | mail.zyxel.cn |
| User Name: | w00143 |
| Password: | •••••• |
| Sender E-mail: | christine.chen@zyxel.cn |
| Receiver E-mails: | |
| Send Test E-mail to Administrator and the addresses in Receiver E-mails: | Test |

All the customized reports are included in the .zip file with the name '00A0C5EFB3AB_Daily Report_2005-11-28_9661'. And '00A0C5EFB3AB' denotes the MAC address of your device.

**NOTE**: In the .zip file, there's an index.html file. It is like the home page of the schedule report. User could check all the reports you have ever selected by accessing this file. Also the size of the attached file will always large than 2Mbytes.

### The Suggested Countermeasure for Protocol Report

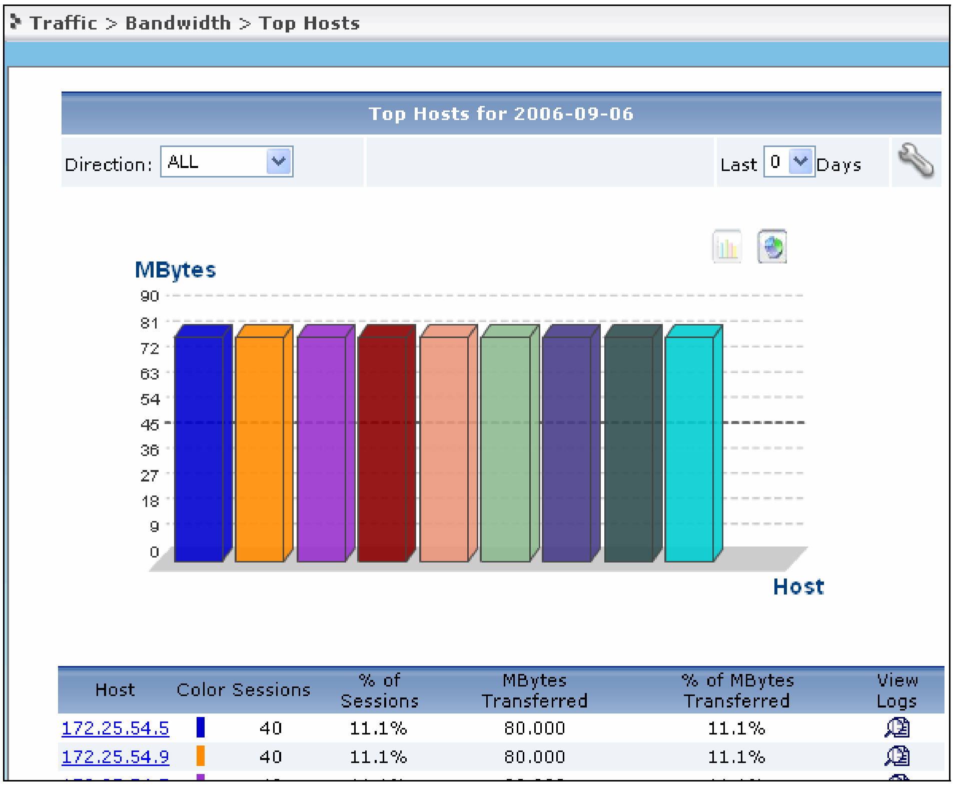


| Protocol | Color | Sessions | % of Sessions | MBytes Transferred | % of MBytes Transferred | View Logs |
|---|---|---|---|---|---|---|
| http | 🟦 | 119 | 5.3% | 1.554 | 55.9% | 🔍 |
| https | 🟧 | 11 | 0.5% | 0.265 | 9.5% | 🔍 |
| netbios-ns | 🟪 | 406 | 18.1% | 0.229 | 8.2% | 🔍 |
| netbios-dgm | 🟫 | 567 | 25.2% | 0.201 | 7.2% | 🔍 |
| others | 🟥 | 41 | 1.8% | 0.175 | 6.3% | 🔍 |
| msn | 🟩 | 4 | 0.2% | 0.118 | 4.2% | 🔍 |

Under **Traffic** >>**Bandwidth** menu, there is a **Top Protocol** report. It is designed for long time usage. User could estimate the bandwidth usage of each protocol after observing a period of time. Then user could add MBM rules on ZyWALL or other devices to guarantee such protocol usage when the bandwidth is insufficient.

### How to check bandwidth usage?

One day the employees complain the network of the company is so bad that they even can not send and receive the E-mail properly. All the traffic go through a ZyWALL 70.The administrator will go to this device and check the **Traffic**>>**Bandwidth>>Top Hosts**. He finds the below report.



Traffic > Bandwidth > Top Hosts

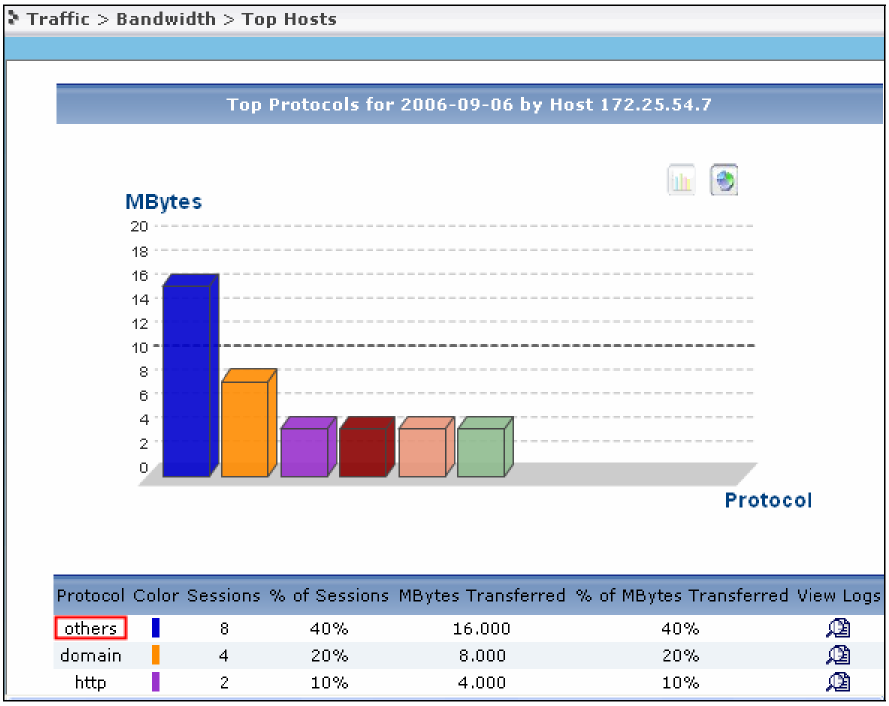
Top Hosts for 2006-09-06

Direction: ALL

Last 0 Days

| Host | Color | Sessions | % of Sessions | MBytes Transferred | % of MBytes Transferred | View Logs |
|---|---|---|---|---|---|---|
| 172.25.54.5 | 🟦 | 40 | 11.1% | 80.000 | 11.1% | |
| 172.25.54.9 | 🟧 | 40 | 11.1% | 80.000 | 11.1% | |

It shows the users with IP address 172.25.54.5 is on the top of the list. Administrator could enter the drill down menu of it to check further. See below.



Traffic > Bandwidth > Top Hosts

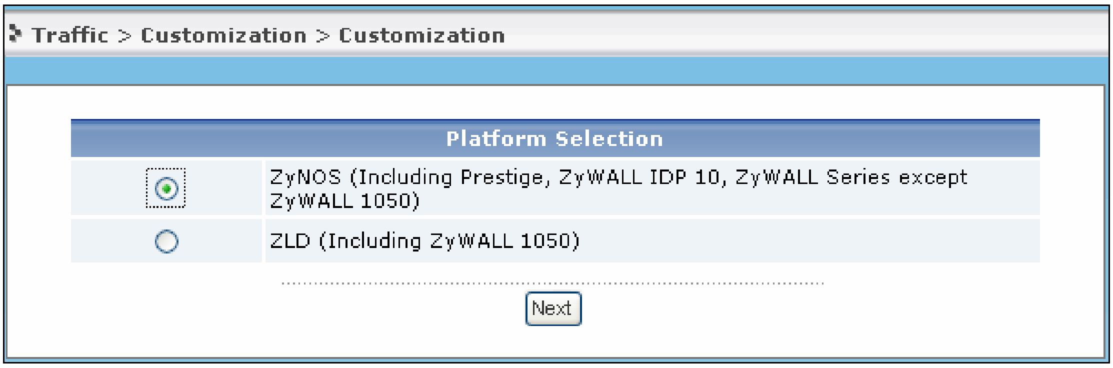
Top Protocols for 2006-09-06 by Host 172.25.54.7

| Protocol | Color | Sessions | % of Sessions | MBytes Transferred | % of MBytes Transferred | View Logs |
|---|---|---|---|---|---|---|
| others | 🟦 | 8 | 40% | 16.000 | 40% | |
| domain | 🟧 | 4 | 20% | 8.000 | 20% | |
| http | 🟪 | 2 | 10% | 4.000 | 10% | |

Protocol type' others' assumes large amount of events and bandwidth. From all the symptoms administrator could infer that this user is downloading large files and the protocol is not in the standard list of device. This kind of operation effects other user's normal usage. Administrator locates the error host according to the direction of the Bandwidth and he may find the definite root cause by setting customized service. Administrator can add firewall rule with its direction according to the Bandwidth direction to control the network condition.
Also, administrator could go to **Traffic**>>**Bandwidth**>>**Top Protocols** report for help.

### Using Customized Service to Determine Illegal Usage

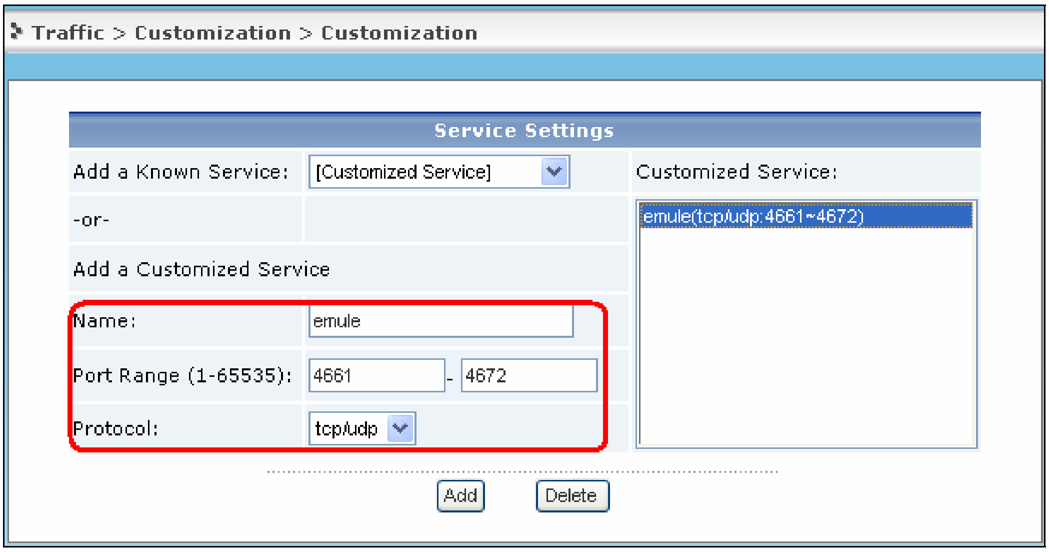
Here comes a scenario: administrator could determine the problematical host while he still can not find the root cause because the protocol type shows as 'others'. Currently he can find the relation between top protocol and host and then trace the destination IP address. Always this IP address will give you some clues to find out the customized service. After that he goes to **Traffic**>>**Customization**>>**Customization** to adds emule as try.
1. Go to select the device type for customization service.



Traffic > Customization > Customization

| Platform Selection | |
|---|---|
| ● | ZyNOS (Including Prestige, ZyWALL IDP 10, ZyWALL Series except ZyWALL 1050) |
| ○ | ZLD (Including ZyWALL 1050) |

2. Go to create customization service.



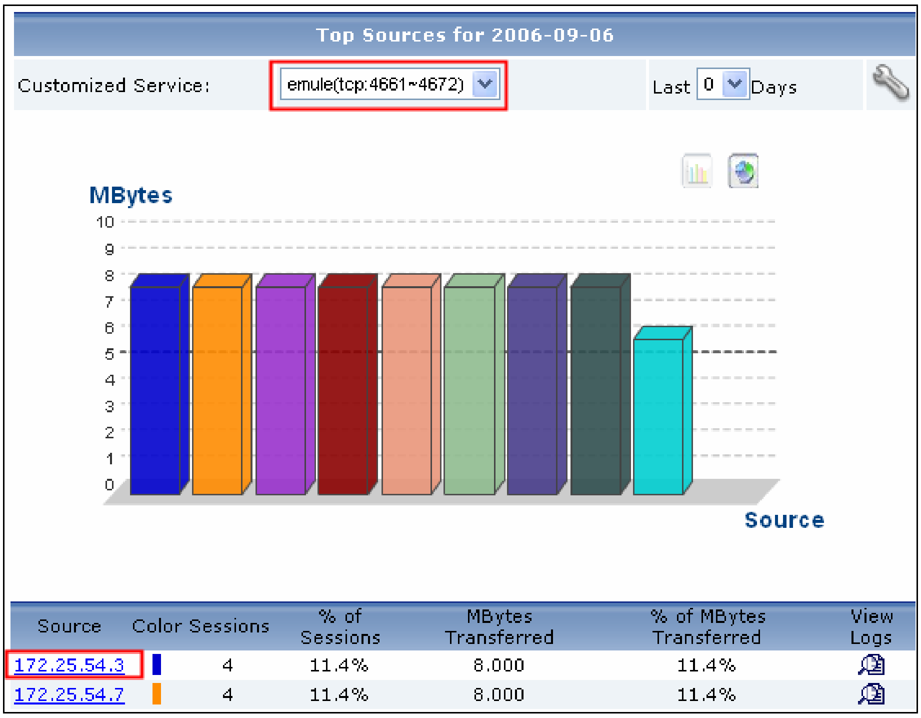
Traffic > Customization > Customization

Service Settings

| | | |
|---|---|---|
| Add a Known Service: | [Customized Service] | Customized Service: |
| -or- | | emule(tcp/udp:4661~4672) |
| Add a Customized Service | | |
| Name: | emule | |
| Port Range (1-65535): | 4661 - 4672 | |
| Protocol: | tcp/udp | |

Excited result appears! Users is using emule to download media material.

**Traffic**>>**Customization**>>**Top Sources.**



Top Sources for 2006-09-06

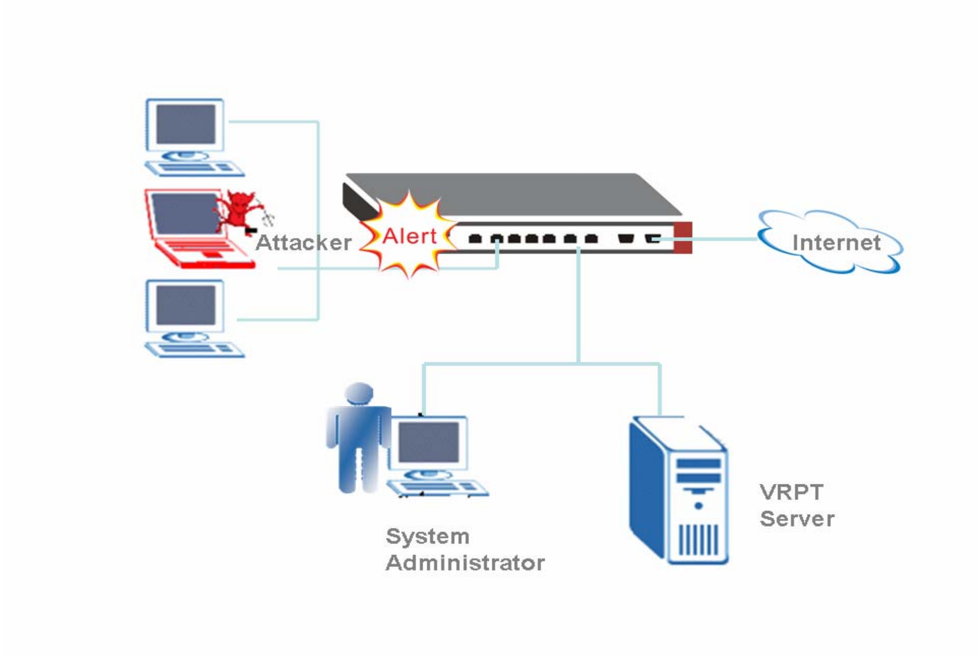
Customized Service: emule(tcp:4661~4672)    Last 0 Days

| Source | Color | Sessions | % of Sessions | MBytes Transferred | % of MBytes Transferred | View Logs |
|---|---|---|---|---|---|---|
| 172.25.54.3 | 🟦 | 4 | 11.4% | 8.000 | 11.4% | |
| 172.25.54.7 | 🟧 | 4 | 11.4% | 8.000 | 11.4% | |

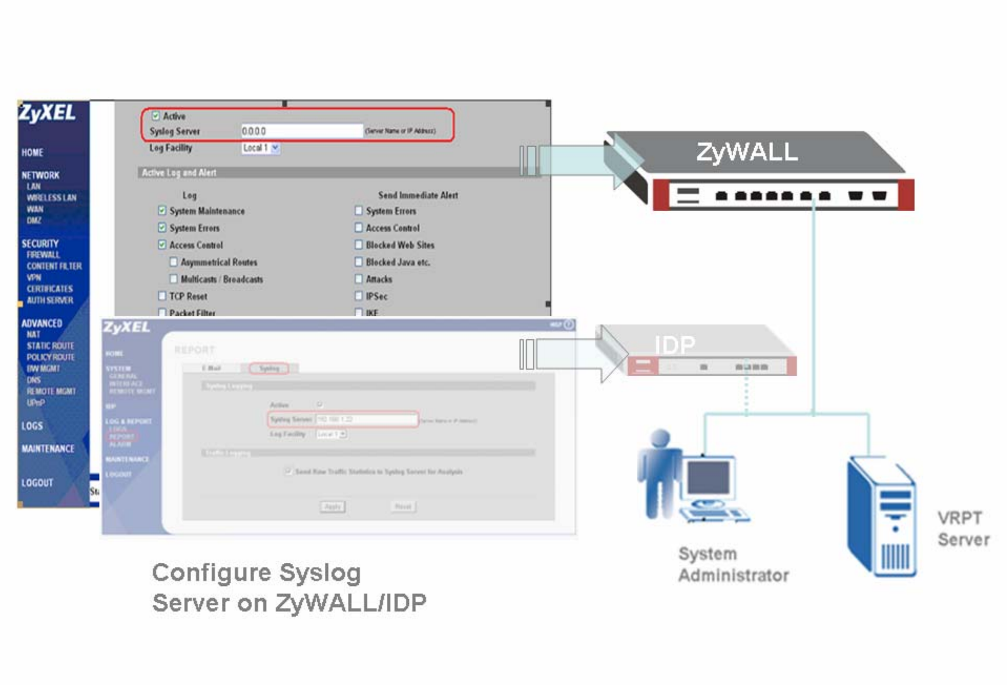
## the Suggested Countermeasure for UTM Report

**Intrusion** report

VRPT supports intrusion report for IDP 10 and ZyWALL with firmware version 4.0. It provides reports based on Top Intrusion, Top Sources (attacker), Top Destinations(victim) and Severity. These reports are under **Network Attack** >>**Intrusion** menu. Following is an example to illustrate that an internal host is conducting network treat (e.g. infected by Trojan or DoS) and passing through device. VRPT will obtain the Syslogs from device for analysis.



1. Configure VRPT Server as the Syslog Server on ZyWALL (with f/w 4.0 or later )or IDP.



☑ Active
Syslog Server 0.0.0.0 (Server Name or IP Address)
Log Facility Local 1

Active Log and Alert

| Log | Send Immediate Alert |
|---|---|
| ☑ System Maintenance | □ System Errors |
| ☑ System Errors | □ Access Control |
| ☑ Access Control | □ Blocked Web Sites |
| □ Asymmetrical Routes | □ Blocked Java etc. |
| □ Multicasts / Broadcasts | □ Attacks |
| □ TCP Reset | □ IPSec |
| □ Packet Filter | □ IKE |

REPORT

E-Mail | Syslog

Syslog Logging

Active ☑
Syslog Server 192.168.1.22 (Server Name or IP Address)
Log Facility Local 1

Traffic Logging

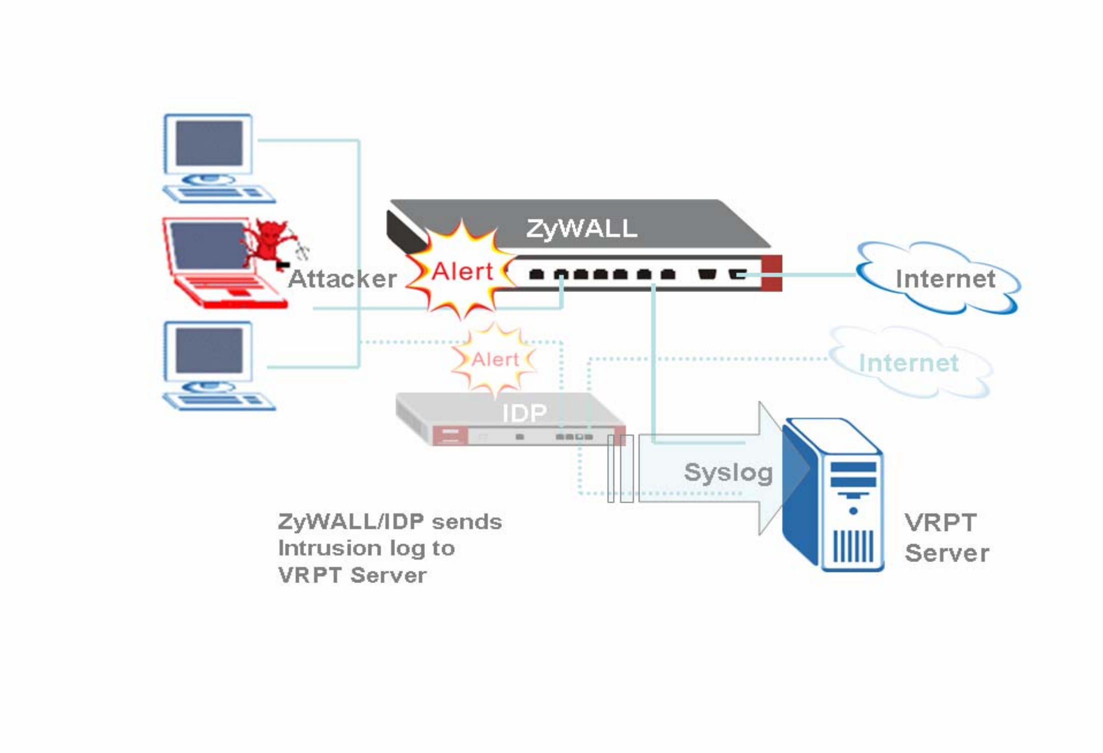
☑ Send Raw Traffic Statistics to Syslog Server for Analysis

Apply Reset

Configure Syslog
Server on ZyWALL/IDP

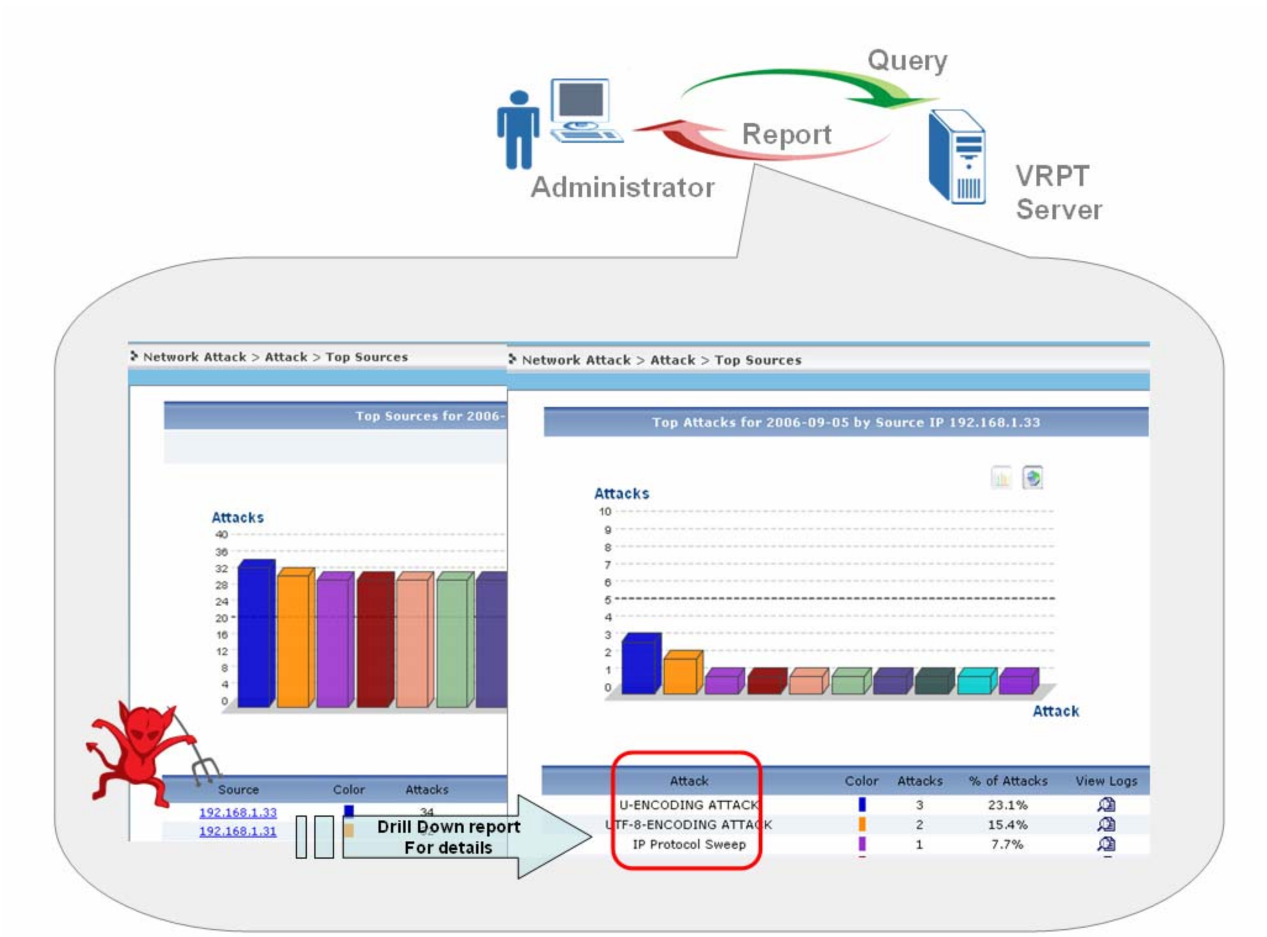
2. When ZyWALL or IDP detects intrusion events, it will generate Syslog and forward to VRPT

Server.



3. Through the Report, system administrator can easily find out the intrusion event and the source/destination of the threat of network.

And drill-down report of Intrusion report allows user to view the intrusion events by querying Intrusion signatures hit by attacker. In this sample attacker with the IP address 10.1.1.5 is the target for administrator to deal with. Also user could use scheduled report for reminding.


Query
Report
Administrator
VRPT
Server
Network Attack > Attack > Top Sources
Top Sources for 2006-
Attacks
Network Attack > Attack > Top Sources
Top Attacks for 2006-09-05 by Source IP 192.168.1.33
Attacks
Attack
Drill Down report
For details

| Source | Color | Attacks |
|---|---|---|
| 192.168.1.33 | 🟦 | 34 |
| 192.168.1.31 | 🟧 | |

| Attack | Color | Attacks | % of Attacks | View Logs |
|---|---|---|---|---|
| U-ENCODING ATTACK | 🟦 | 3 | 23.1% | |
| UTF-8-ENCODING ATTACK | 🟧 | 2 | 15.4% | |
| IP Protocol Sweep | 🟪 | 1 | 7.7% | |

Here are some hints for administrator to trace the intrusion. Here Top means top ten except Top Severtriy..

The advanced query (Drill down report ) can be Top Intrusions/Top Sources/Top Destinations/By Severity.

Below are relationships between basic query and advanced query (drill down report).

Top Intrusion (Signature)-----Top Host

Top Sources--------Top Signature

Top Destinations---Top Signature

Top Severity------Top Signature

Here Severity includes eight types. The table below shows the types with meanings.

| Type | Meaning |
|---|---|
| Emergency: | system is unusable |
| Alert | action must be taken immediately |

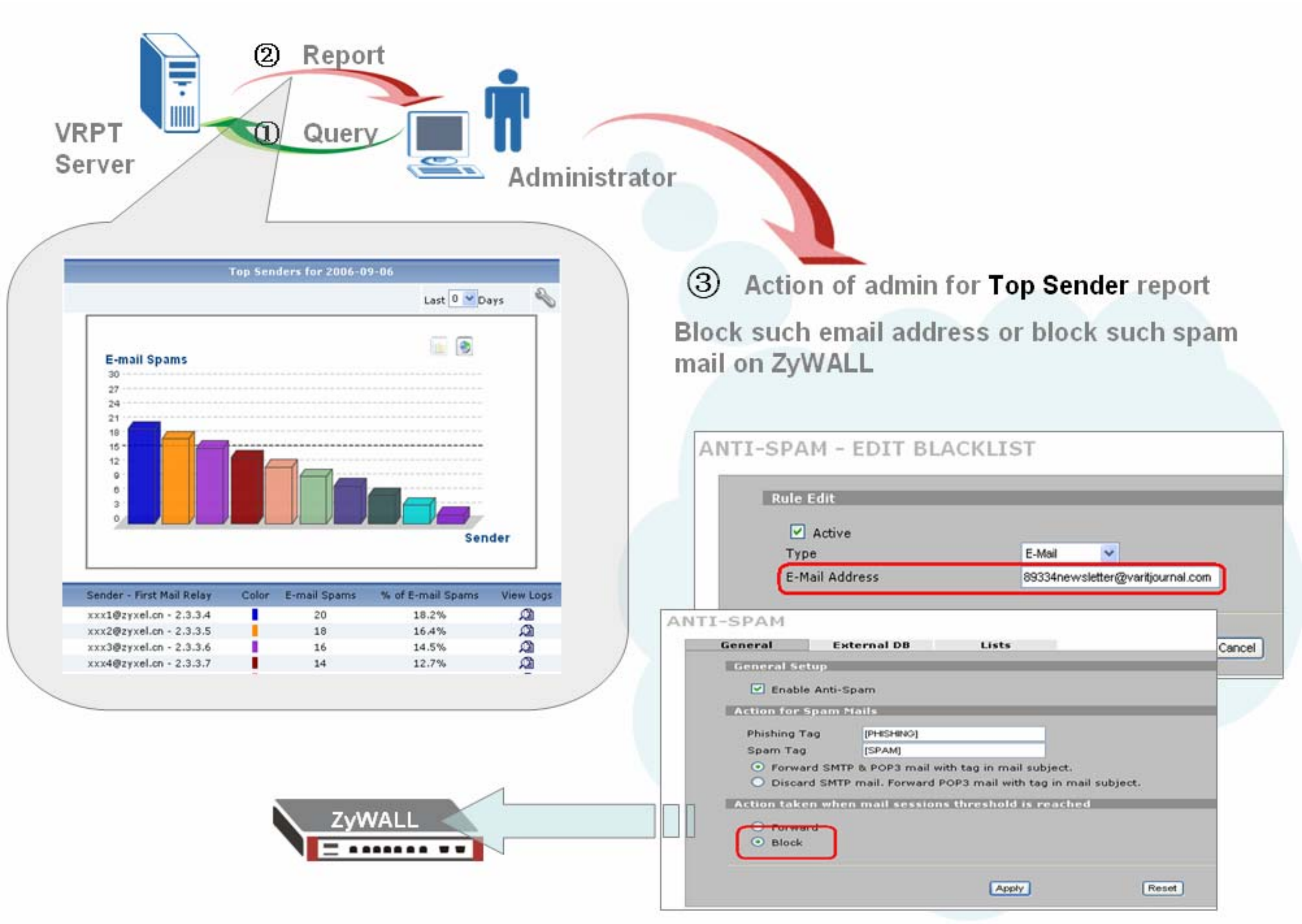
| | |
|---|---|
| Critical | critical conditions |
| Error | error conditions |
| Warning | warning conditions |
| Notice | normal but significant condition |
| Informational | informational messages |
| Debug | debug-level messages |

Administrator should add two firewall rules for the target Source attacker for VRPT do not show the direction of Intrusion (LAN to WAN or WAN to LAN). The attacker may at LAN side or WAN side. For Destination report, administrator should focus its effort on monitor.

**AntiSpam** report

**AntiSpam** report is especially for ZyWALL 5/35/70 UTM AntiSpam feature. Using this kind of report, administrator will trace the sender and source of the Spam Mail. Also user could determine score threshold by checking score report.

1. Administrator could block the senders if the senders are in the **Top Senders** report or block such spam mails address by adding them into blacklist.



Top Senders for 2006-09-06

Last 0 Days

| Sender - First Mail Relay | Color | E-mail Spams | % of E-mail Spams | View Logs |
|---|---|---|---|---|
| xxx1@zyxel.cn - 2.3.3.4 | ■ | 20 | 18.2% | |
| xxx2@zyxel.cn - 2.3.3.5 | ■ | 18 | 16.4% | |
| xxx3@zyxel.cn - 2.3.3.6 | ■ | 16 | 14.5% | |
| xxx4@zyxel.cn - 2.3.3.7 | ■ | 14 | 12.7% | |

③ Action of admin for **Top Sender** report

Block such email address or block such spam mail on ZyWALL

ANTI-SPAM - EDIT BLACKLIST

Rule Edit

☑ Active

Type: E-Mail

E-Mail Address: 89334newsletter@varitjournal.com

Cancel

ANTI-SPAM

General | External DB | Lists

General Setup

☑ Enable Anti-Spam

Action for Spam Mails

Phishing Tag: [PHISHING]

Spam Tag: [SPAM]

● Forward SMTP & POP3 mail with tag in mail subject.

○ Discard SMTP mail. Forward POP3 mail with tag in mail subject.

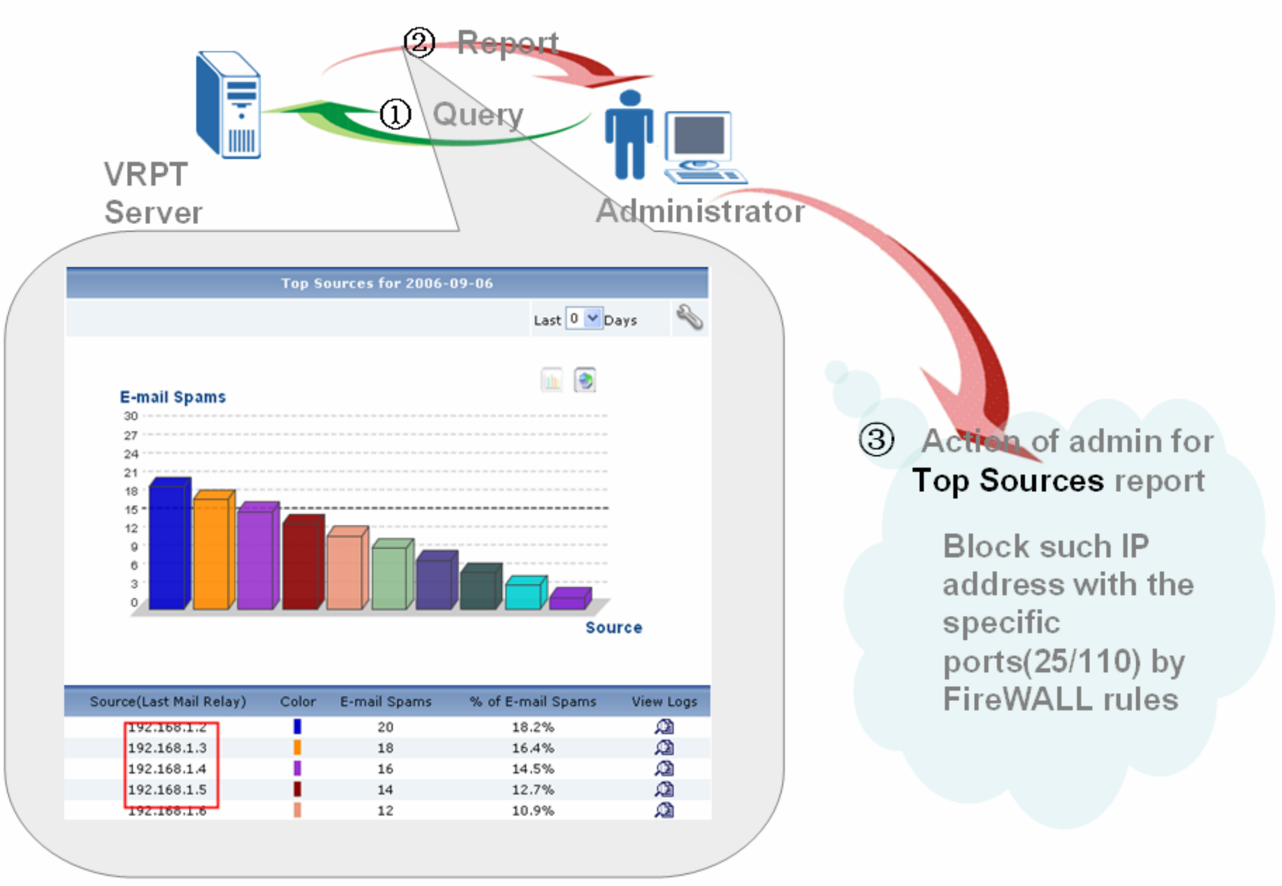
Action taken when mail sessions threshold is reached

○ Forward

● Block

Apply | Reset

2. For **Top Sources** report, administrator could block such IP addresses by adding firewall rules. Please still notice the direction of the rules as that of in the Intrusion scenario.

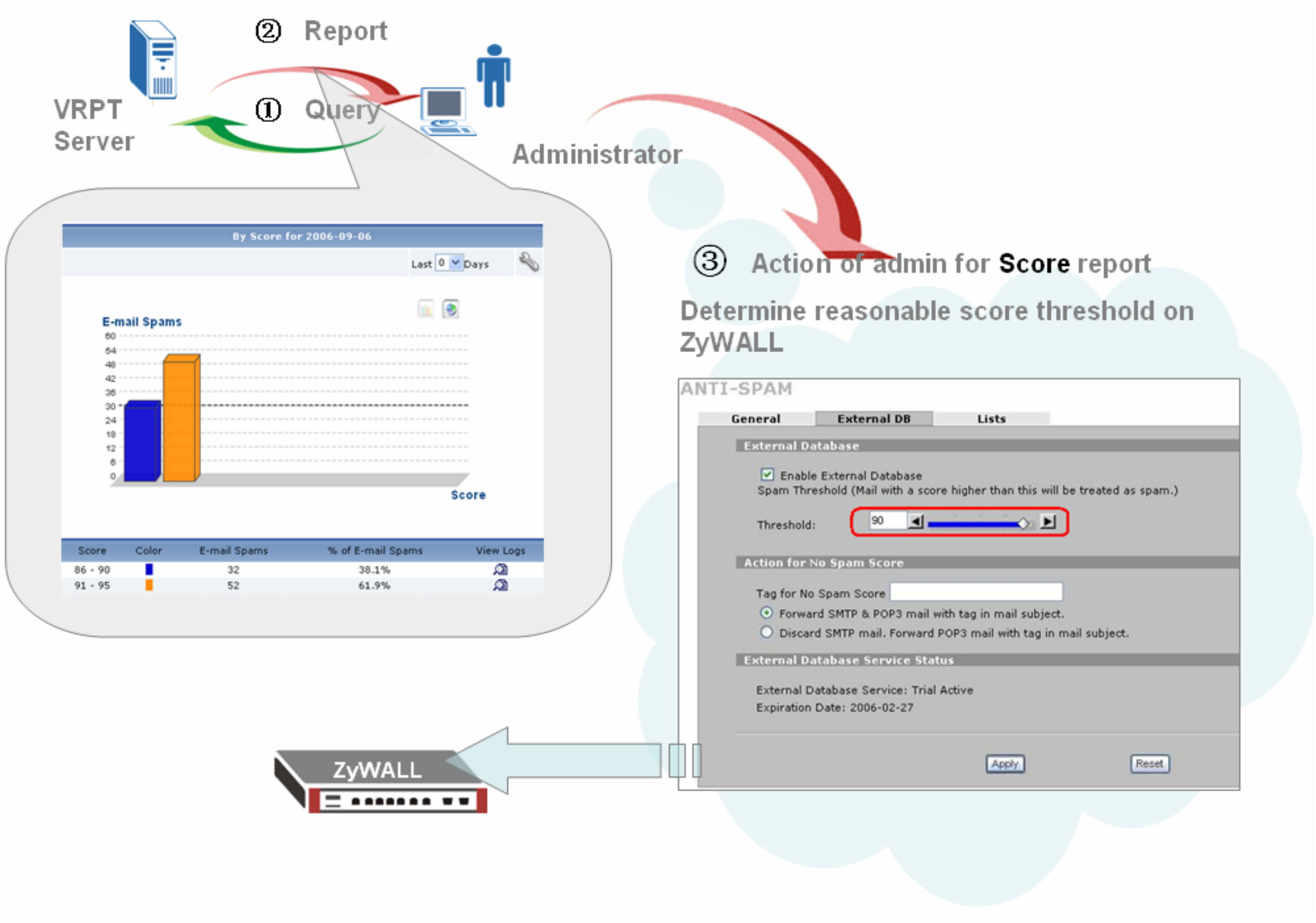

② Report
① Query
VRPT Server
Administrator
E-mail Spams
30
27
24
21
18
15
12
9
6
3
0
Source
③ Action of admin for Top Sources report
Block such IP address with the specific ports(25/110) by FireWALL rules

Top Sources for 2006-09-06

Last 0 Days

| Source(Last Mail Relay) | Color | E-mail Spams | % of E-mail Spams | View Logs |
|---|---|---|---|---|
| 192.168.1.2 | ■ | 20 | 18.2% | 🔍 |
| 192.168.1.3 | ■ | 18 | 16.4% | 🔍 |
| 192.168.1.4 | ■ | 16 | 14.5% | 🔍 |
| 192.168.1.5 | ■ | 14 | 12.7% | 🔍 |
| 192.168.1.6 | ■ | 12 | 10.9% | 🔍 |

3. User could determine score threshold for ZyWALL AntiSpam by **By Score** report. When AntiSpam function enables, MailShell server will return a score for each email passing through ZyWALL. Score report shows return score with its email quantity. See below sample. There are 16 emails with return score in the 86 to 90 range and 26 emails with return score in the 91 to 95 range in the BAR picture. Then administrator could determine reasonable score threshold to control the quantity of the spam mail on ZyWALL.



By Score for 2006-09-06

Last 0 Days

| Score | Color | E-mail Spams | % of E-mail Spams | View Logs |
|---|---|---|---|---|
| 86 - 90 | 🟦 | 32 | 38.1% | |
| 91 - 95 | 🟧 | 52 | 61.9% | |

③ Action of admin for **Score** report

Determine reasonable score threshold on ZyWALL

ANTI-SPAM

General | External DB | Lists

External Database

☑ Enable External Database
Spam Threshold (Mail with a score higher than this will be treated as spam.)

Threshold: 90

Action for No Spam Score

Tag for No Spam Score
● Forward SMTP & POP3 mail with tag in mail subject.
○ Discard SMTP mail. Forward POP3 mail with tag in mail subject.

External Database Service Status

External Database Service: Trial Active
Expiration Date: 2006-02-27

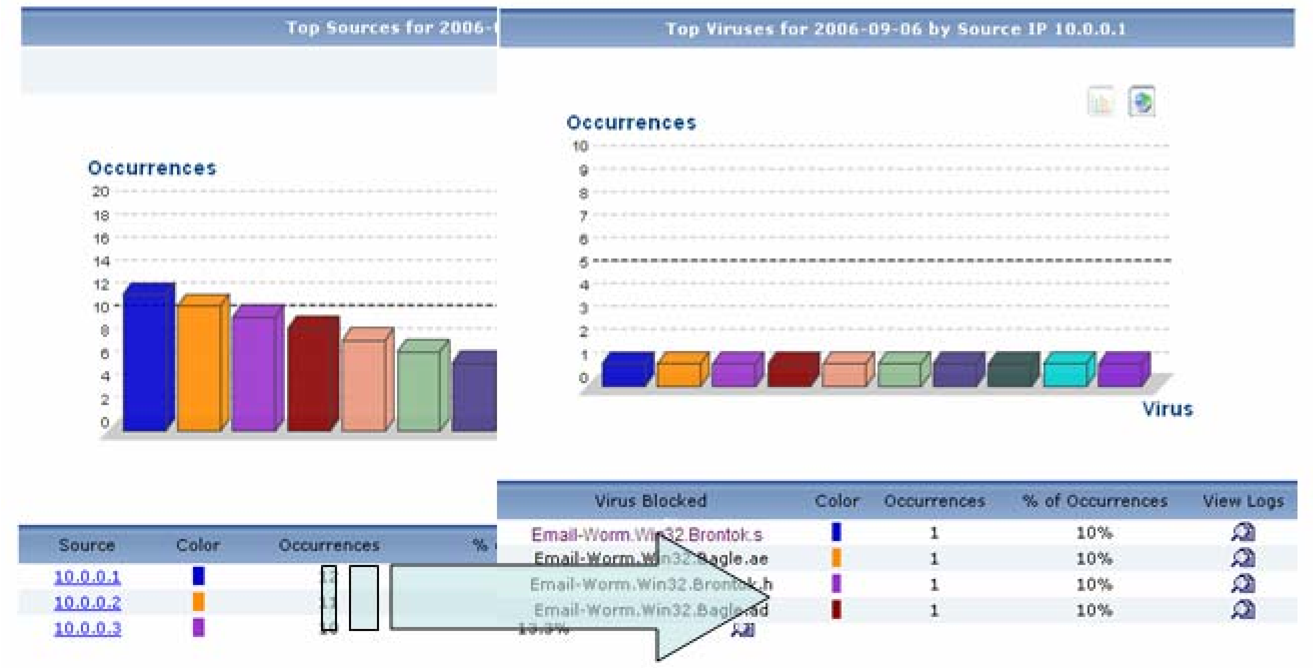
Apply Reset

**AntiVirus** report

Under **Network Attack**>>**AntiVirus** menu, user could find **Top Viruses, Top Sources and Top Destinations** report. Administrator could monitor top virus types and block such destination and source by firewall rules.

See below sample.

There's a top AV source with the IP address 10.0.0.4. User could find the detailed AV type by checking drill down report. According to the information, user could add firewall rule to block hacker's IP address. But please still notice the firewall rule direction. User should add both LAN to WAN and WAN to LAN directions.



| Source | Color | Occurrences | % |
|---|---|---|---|
| 10.0.0.1 | 🟦 | 12 | |
| 10.0.0.2 | 🟧 | 11 | |
| 10.0.0.3 | 🟪 | 10 | 13.3% |

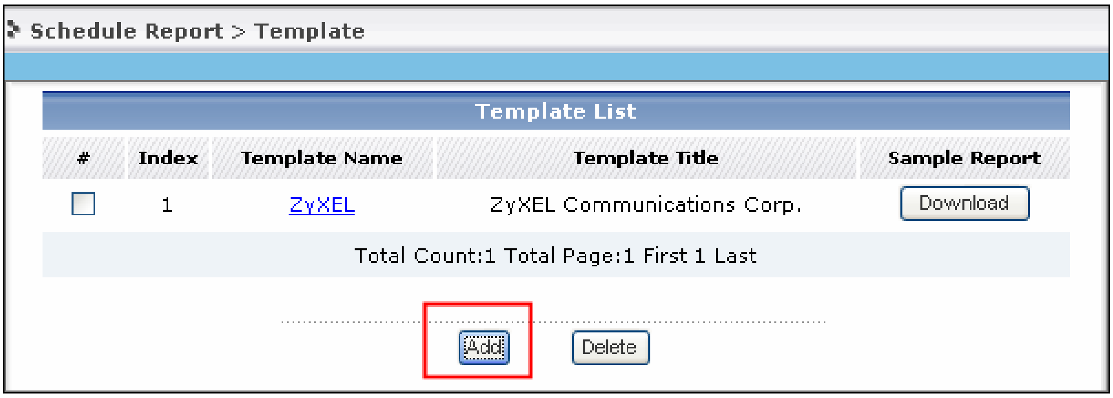
| Virus Blocked | Color | Occurrences | % of Occurrences | View Logs |
|---|---|---|---|---|
| Email-Worm.Win32.Brontok.s | 🟦 | 1 | 10% | |
| Email-Worm.Win32.Bagle.ae | 🟧 | 1 | 10% | |
| Email-Worm.Win32.Brontok.h | 🟪 | 1 | 10% | |
| Email-Worm.Win32.Bagle.ad | 🟥 | 1 | 10% | |

Also you can monitor the popularity and occurrence about the specify virus by searching **Top Virus** report. Normally it reflects the trend of virus.

### the Suggested Countermeasure for Schedule Template

Here comes a scenario. There is a company A that promotes ZyWALL series. This company does not have the ability to develop network management software but he knows VRPT. While company A still wants its customers to believe their network is in the charge of himself not the other third part software. Schedule template helps this kind of company to achieve their goal. Please see the magic function.

**1. Go to** Schedule Report>>Template **to Add a template.**

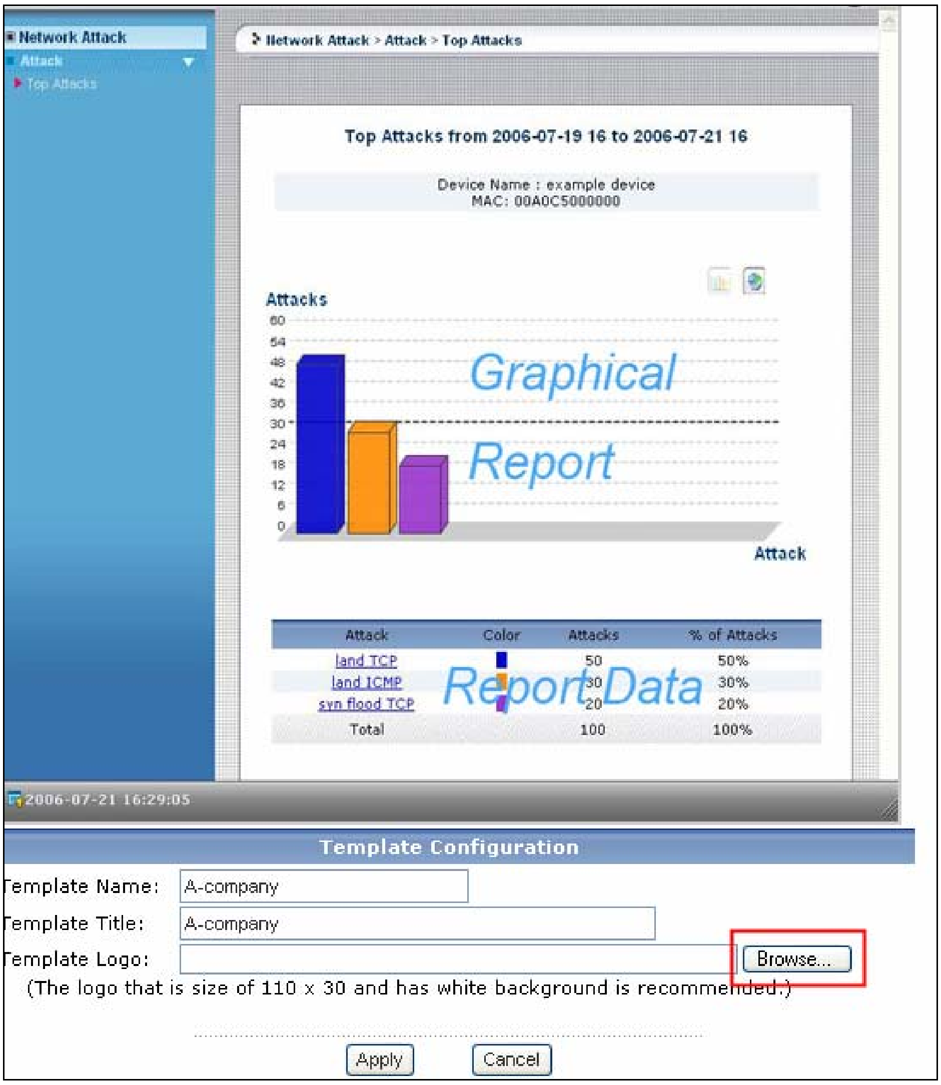

Schedule Report > Template

Template List

| # | Index | Template Name | Template Title | Sample Report |
|---|---|---|---|---|
| ☐ | 1 | ZyXEL | ZyXEL Communications Corp. | Download |

Total Count:1 Total Page:1 First 1 Last

2. Besides entering customized template name and title, the most import thing is to determine the customized logo. Make sure you have prepared the logo picture before creating template.



Top Attacks from 2006-07-19 16 to 2006-07-21 16

Device Name : example device
MAC: 00A0C5000000

| Attack | Color | Attacks | % of Attacks |
|---|---|---|---|
| land TCP | 🟦 | 50 | 50% |
| land ICMP | 🟧 | 30 | 30% |
| syn flood TCP | 🟪 | 20 | 20% |
| Total | | 100 | 100% |

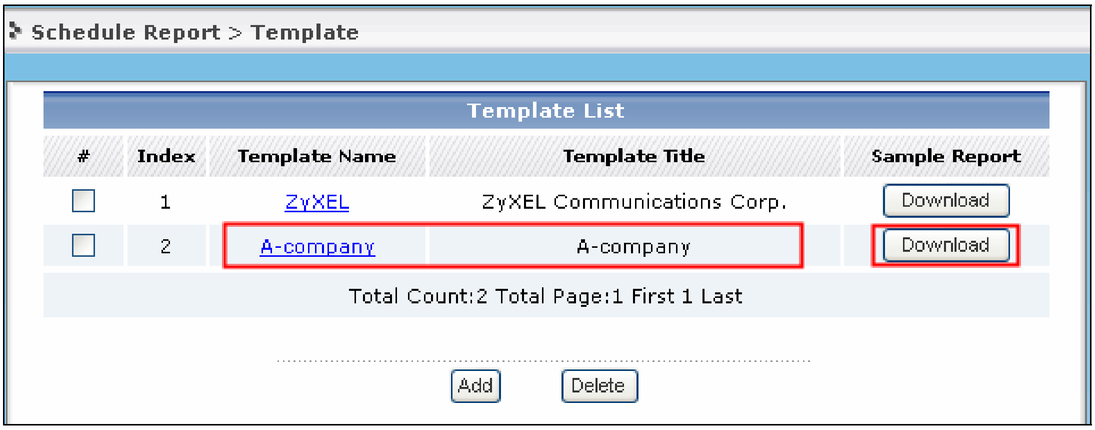
Template Configuration

| | |
|---|---|
| Template Name: | A-company |
| Template Title: | A-company |
| Template Logo: | Browse... |

(The logo that is size of 110 x 30 and has white background is recommended.)

Apply Cancel

3. To preview the template you can download it and check the details.



Schedule Report > Template

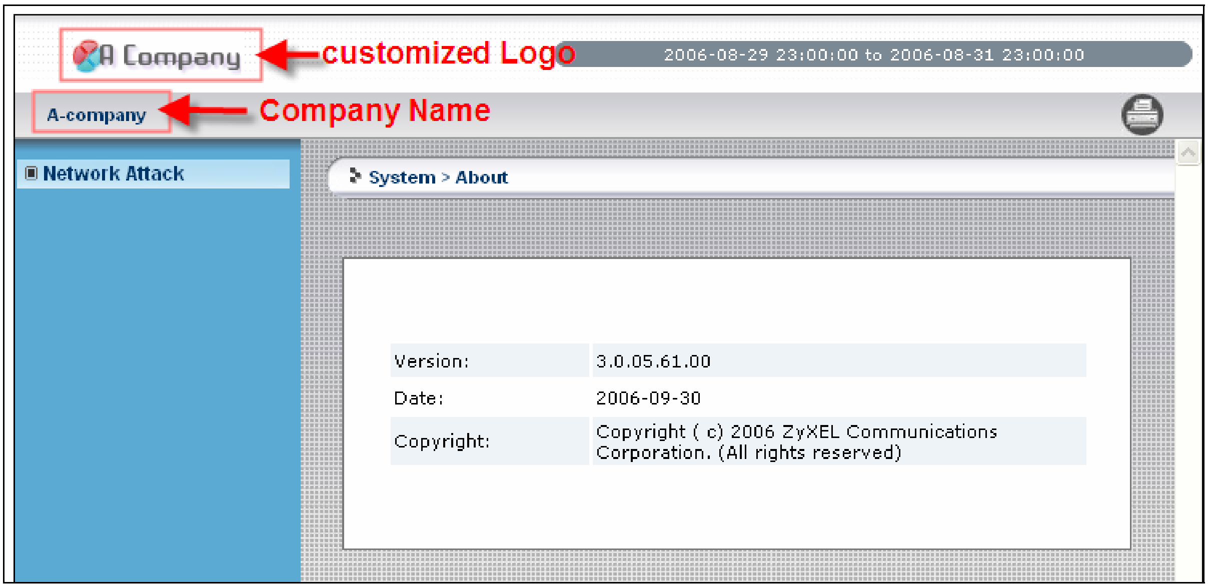
Template List

| # | Index | Template Name | Template Title | Sample Report |
|---|---|---|---|---|
| □ | 1 | ZyXEL | ZyXEL Communications Corp. | Download |
| □ | 2 | A-company | A-company | Download |

Total Count:2 Total Page:1 First 1 Last

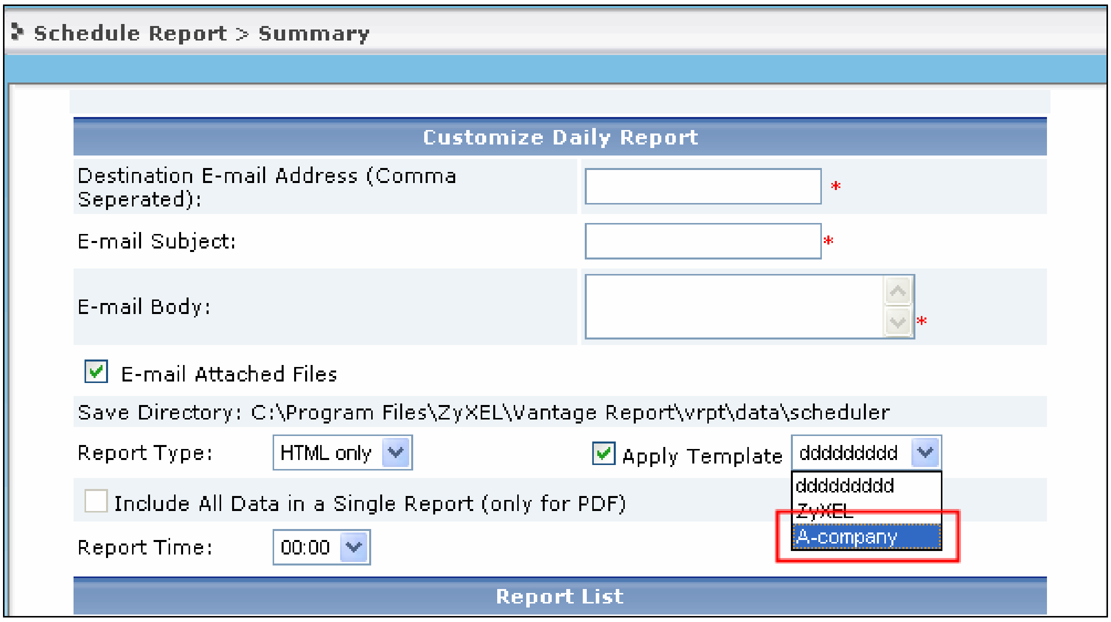
Add Delete

The below picture illustrates the template we created for company A.



|  |  |
|---|---|
| Version: | 3.0.05.61.00 |
| Date: | 2006-09-30 |
| Copyright: | Copyright ( c) 2006 ZyXEL Communications Corporation. (All rights reserved) |

After creating the template, you can apply it for your customized schedule report.


Schedule Report > Summary

Customize Daily Report

Destination E-mail Address (Comma Seperated): *

E-mail Subject: *

E-mail Body: *

☑ E-mail Attached Files

Save Directory: C:\Program Files\ZyXEL\Vantage Report\vrpt\data\scheduler

Report Type: HTML only ☑ Apply Template dddddddd

□ Include All Data in a Single Report (only for PDF)

Report Time: 00:00

Report List

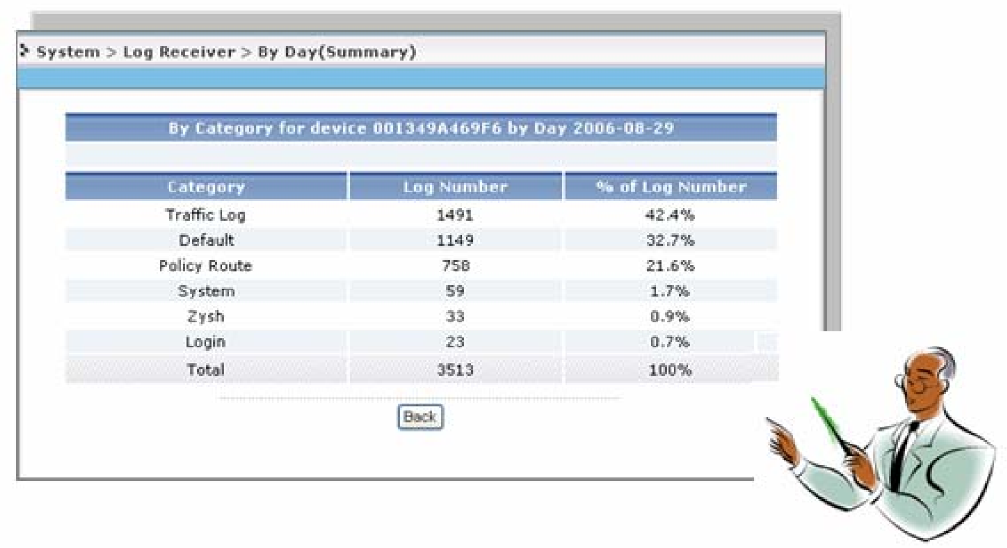
### the Benefit of Log Receiver

There’s a lot of work for MIS everyday. Total PC maintenance job, company web site system maintenance, internal DB maintenance… But boss still want me to give out the overall statistics about the network condition in short form every day or over a period of time. What can I do? Hey, **Log Receiver** can you pull you out of heavy work.

1. **By Day** report

Log Receiver by days under **System**>>**Log Receiver** shows concise statistics of network condition everyday. It is a good tool to look through network before going to every detailed report. This picture illustrates the condition before a MIS has the Log Receiver report.

This picture illustrates the MIS engineer that has the log receiver report.

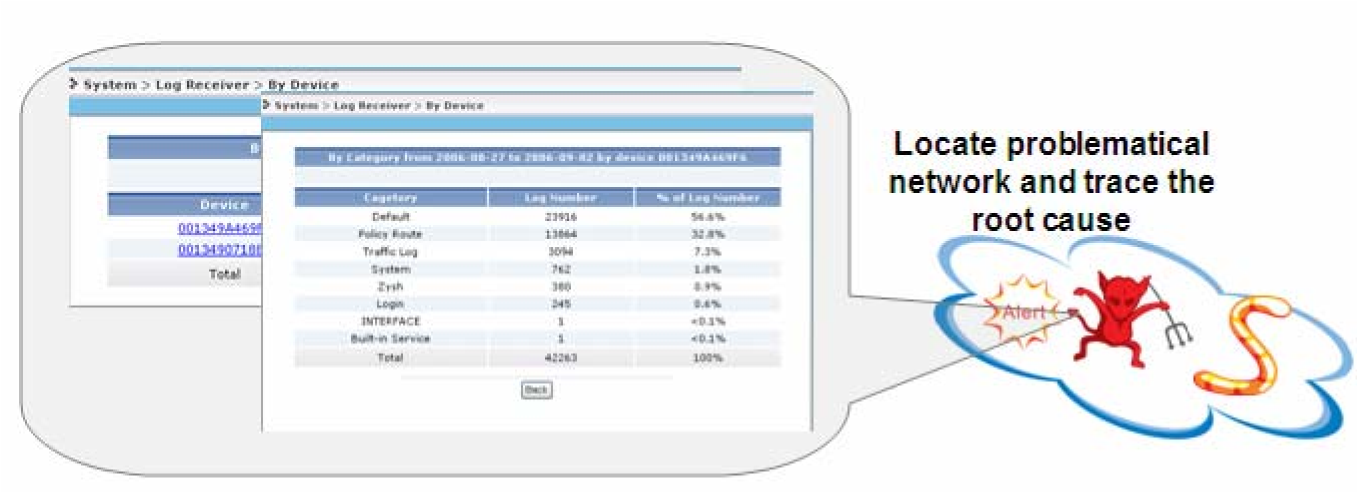

System > Log Receiver > By Day(Summary)

By Category for device 001349A469F6 by Day 2006-08-29

| Category | Log Number | % of Log Number |
|---|---|---|
| Traffic Log | 1491 | 42.4% |
| Default | 1149 | 32.7% |
| Policy Route | 758 | 21.6% |
| System | 59 | 1.7% |
| Zysh | 33 | 0.9% |
| Login | 23 | 0.7% |
| Total | 3513 | 100% |

2. **By Device** report

Also Log Receiver speeds up the process to diagnose the network. Always the number of logs directly reflects the network condition belongs to the specific device. By Device report help us to locate the problematical network quickly. Then user can trace the root cause by looking into specific report and take action on ZyWALL device.



System > Log Receiver > By Device

| Device |
|---|
| 001349A469F |
| 0013490718 |
| Total |

System > Log Receiver > By Device

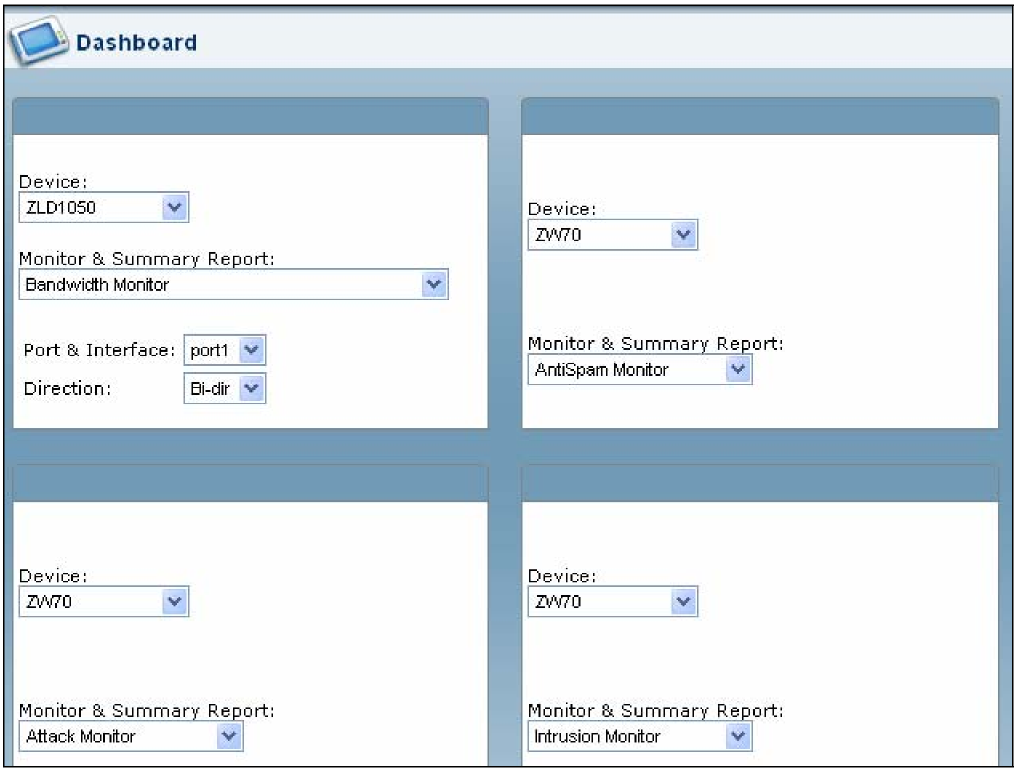
By Category from 2006-08-27 to 2006-09-02 by device 001349A469F6

| Cagetory | Log Number | % of Log Number |
|---|---|---|
| Default | 23916 | 56.6% |
| Policy Route | 13864 | 32.8% |
| Traffic Log | 3094 | 7.3% |
| System | 762 | 1.8% |
| Zysh | 380 | 0.9% |
| Login | 245 | 0.6% |
| INTERFACE | 1 | <0.1% |
| Built-in Service | 1 | <0.1% |
| Total | 42263 | 100% |

## Dashboard for Quick View of Network

MIS engineer always begins his work like this: take about 10 minutes to take a quick view of network healthy. At this moment, not all the reports are necessary to pop out to windows. Maybe the VPN usage is the first concerns for ZyWALL 1050 and Attack report is most important for another ZyWALL device because attack is very heavy these days. So most import reports accompanying with most import devices(network) are taken into consideration. Dashboard report gives a platform to achieve this goal.

1. to set the profile for dashboard



Dashboard

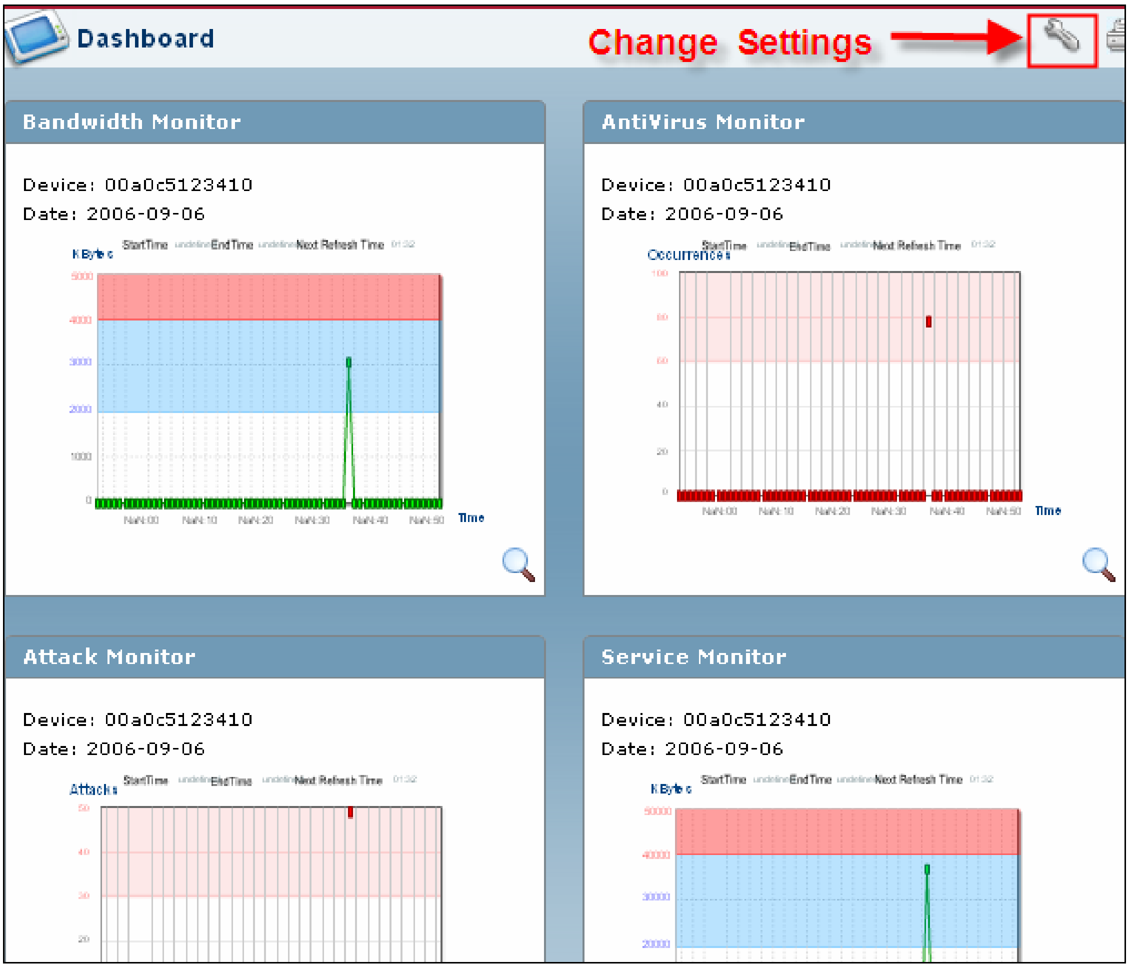
Device: ZLD1050
Monitor & Summary Report: Bandwidth Monitor
Port & Interface: port1
Direction: Bi-dir

Device: ZW70
Monitor & Summary Report: AntiSpam Monitor

Device: ZW70
Monitor & Summary Report: Attack Monitor

Device: ZW70
Monitor & Summary Report: Intrusion Monitor

2. You can view the dash board every time when you enter **Dashboard** menu and also you can change the profile by clicking the icon on the right top.



Bandwidth Monitor

Device: 00a0c5123410
Date: 2006-09-06

AntiVirus Monitor

Device: 00a0c5123410
Date: 2006-09-06

Attack Monitor

Device: 00a0c5123410
Date: 2006-09-06

Service Monitor

Device: 00a0c5123410
Date: 2006-09-06

**NOTE**: Only the admin has the right to establish and change dashboard profiles.

### Simple Solution for an MIS Administrator

Vantage Report is a useful and convenient tool for MIS administrator to manage device and network.

Before managing the network, an MIS engineer should add devices into device list and also configure the **Server Configuration** under **System** (please find the sample in Schedule report application). Also configure the device for log settings.

1. You can begin your work by looking into **Dashboard** board report. Most important network with the most important report will pop out.
2. On working hours, monitor will give live statistics. It gives the first alarm when the abnormal occur. Especial the **AntiSpam**, **AntiVirus** and **Intrusion** report.
3. Before finishing daily job, **Log Receiver** gives out brief view of network. You can look into detailed data in daily or weekly **Schedule Report**. **Schedule Template** can customize

your report. Customized Logo is included.

4. Some check points will give clues for MIS engineer take action on device to optimize the network when analysing the detailed report.
   - Bandwidth usage is data to guarantee the special usage such as VoIP or email.
   - Top protocol report always reflects the services in use. If some service is nothing to do with work, such as FTP download or P2P download, you can trace the either the destination or the service port and then add firewall rule on device.
   - WEB report. You can block these website if it is nothing to do with the daily work and also trace the user if he always surfing the internet.
   - Check the UTM report to guarantee the security of the network. Please look the previous application and action of device for details.

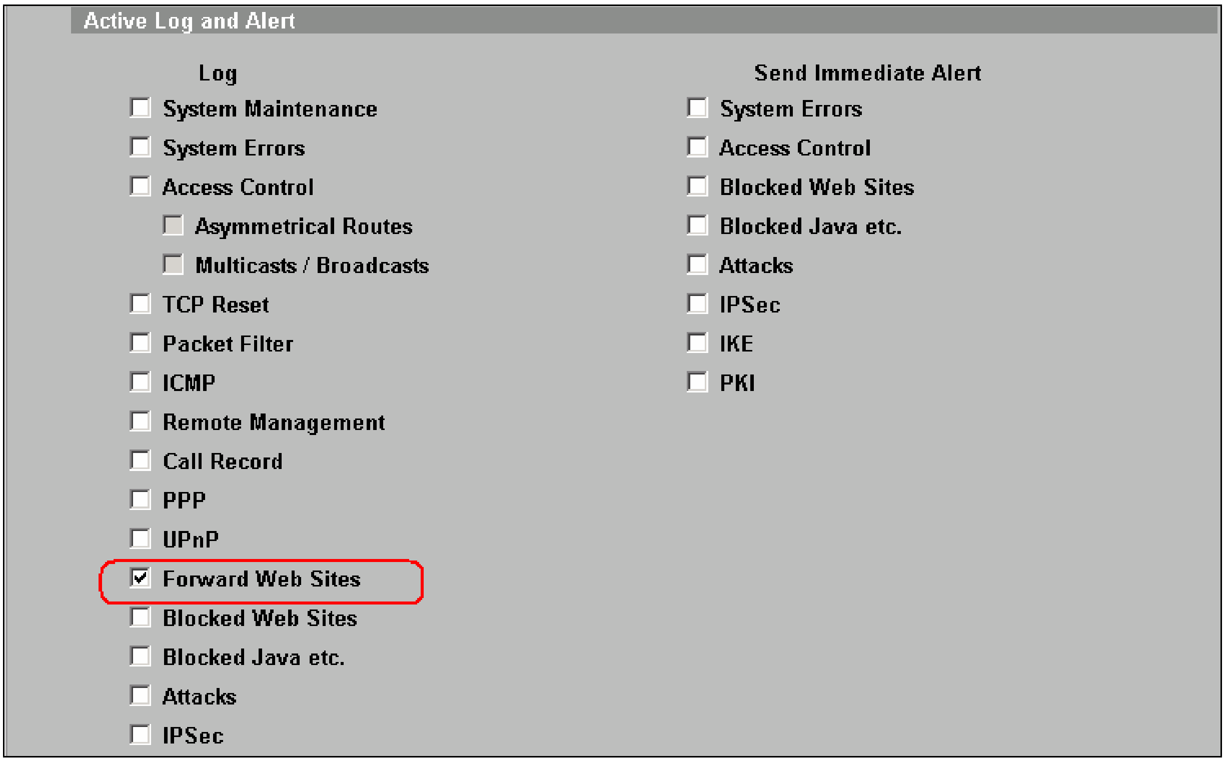
# Trouble Shooting

### What to check if you can not access the GUI of VRPT Server?

If the VRPT is behind the NAT/FireWall, please make sure the UDP port 514 is forwarded for the VRPT Server. Also you should forward TCP port 8080 by default. If you have customized the Web server port, you should forward such customized TCP port.

### What could be wrong with Security Policy stay empty also with web action ?

Please enable content filter service on ZyWALL and activate the log option “Forward Web Sites” or ‘Blocked Web Sites’.
**LOGS**>>**Log Setting**



Active Log and Alert

Log

□ System Maintenance
□ System Errors
□ Access Control
□ Asymmetrical Routes
□ Multicasts / Broadcasts
□ TCP Reset
□ Packet Filter
□ ICMP
□ Remote Management
□ Call Record
□ PPP
□ UPnP
☑ Forward Web Sites
□ Blocked Web Sites
□ Blocked Java etc.
□ Attacks
□ IPSec

Send Immediate Alert

□ System Errors
□ Access Control
□ Blocked Web Sites
□ Blocked Java etc.
□ Attacks
□ IPSec
□ IKE
□ PKI

### Why can't I start up VRPT 3.0 after installing it?

1. If you want to start up VRPT 3.0, the following content must be included in your machine's system Variables.
   PATH=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem; Here 'C' means system driver. You could check the system variables by following directory **System Properties>>Advanced>>Environment Variables>>System variables** on your PC.
2. if the problem is not in the range of a to b, please follow such steps to do so.
   2.1. Change log level as the following by editing file <vrpt_home>/vrpt/conf/log4j.properties
   Change the following lines:
   log4j.logger.com.zyxel.vantage.vrpt = INFO
   log4j.logger.com.zyxel.vantage.web = INFO
   to
   log4j.logger.com.zyxel.vantage.vrpt = DEBUG
   log4j.logger.com.zyxel.vantage.web = DEBUG
   2.2. Restart your VRPT3.0. And reproduce the problem.
   3.0. Send the log files in <vrpt_home>/vrpt/log folder to technical support person.

### Why do VRPT 3.0 shutdown automatically without any reason?

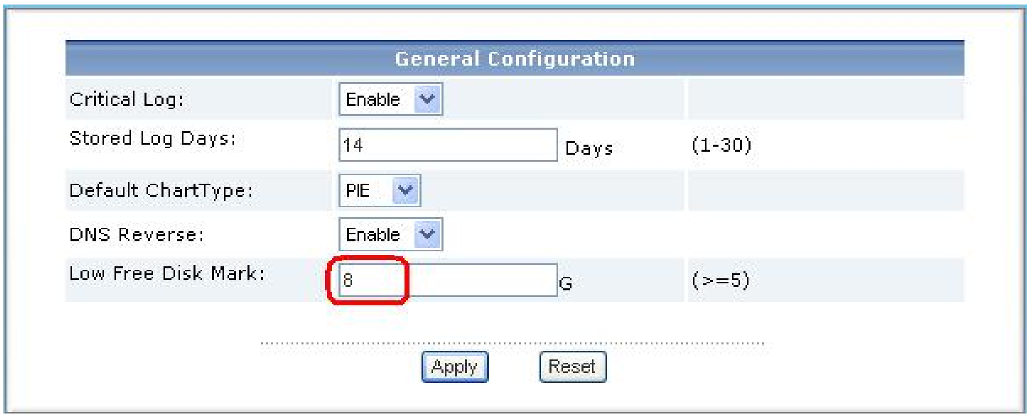
1. Please check the number of devices that are managed by VRPT 3.0. The number of the registered devices should be no more than the license allowed.
2. The AC from your system does not match the one in VRPT database. Please do not do any invalid copy.

### Why does my Web page come back to Login page?

1. Please make sure if your account still in the **User List**. If Administrator delete your account, the page will come back to log in page automatically.
2. Session time out. The default time is 15 minutes.

### Why there’s no new logs receive by VRPT 3.0?

1. Please make sure your configuration on device is right. Please go to previous part of support note at **How to forward device log to VRPT for analysis and report?** and at **How to enable traffic log feature on ZyWALL?**
2. Please make sure the connection between VRPT server and device is normal by PING.
3. Please make sure the free disk of VRPT3.0 home directory on server machine is no less than 800 MB. The default value for **Low Free Disk Mark** is 8GB. You could configure it under **System>>General Configuration** as following figure. When the free disk is less than **Low Free Disk Mark,** VRPT will send email to remind you of the issue. While when the free disk is less than 800MB, VRPT will stop receiving log. After the free disk recover to an available value, VRPT will receiver logs again.
4. In VRPT 3.0, the policy is changed. If the total logs of a device in database are over 10,000,000, VRPT will send notice mail. If the total logs of a device in database are over 15,000,000, VRPT will send alert mail and stop receiving the logs from this device. The logs from the other devices will not be affected.



General Configuration

| | | |
|---|---|---|
| Critical Log: | Enable | |
| Stored Log Days: | 14 Days | (1-30) |
| Default ChartType: | PIE | |
| DNS Reverse: | Enable | |
| Low Free Disk Mark: | 8 G | (>=5) |

**Is there any way to check if VRPT server has received Syslogs from device?**

User could go to <vrpt_home>\vrpt\log\logRecord.log to check the current status. Please go to release note for detailed information about it.

**Why VRPT 3.0 can not get any log even when I correctly add device in it?**

1. Please make sure the gateway before VRPT server has forward UDP 514.
2. Please make sure the connection between VRPT server and device is normal by PING.
3. Please make sure the firewall on VRPT server PC does not block UDP port 514. We take Windows XP for example. You should go to **Windows Firewall**>>**Advanced Settings**>>**Services** to add a special server for VRPT for such port.

# FAQ

## Product FAQ

**Q1: What is Vantage Report (VRPT)?**

ZyXEL VRPT, a centralized Log & Reporting System, build on Java Technology, for quickly and conveniently collecting or analyzing a distributed network, provides SMB MIS, reseller a simple method of monitoring the associated hardware and activities.

ZyXEL VRPT is an application that can collect, analyze logs which distributed by ZyXEL devices, and show user the statistics on web pages or send scheduled reports as Email to corresponding users. With VRPT, you can monitor network access, enhance security, and anticipate future bandwidth needs.

**Q2: Which operating systems are supported by VRPT 3.0 Server?**

Windows XP/2000/2003 now. Linux is not available for this version.

### Q3: What kind of reports supported by VRPT?

There are two types of logs from devices: Event log and Traffic log.
Event logs include many kinds of messages which are related to the events. For example: DoS/DDoS attack, Web Access Block, Network Intrusion Anti-Virus, Anti-Spam and so on. In VRPT, **Network Attack** report, **Event** report and **Security Policy** report are generated by event log information. We could call them event report.

The other type of log, traffic log, is for statistic report about traffic passing through the device. Traffic log contains some information like source/destination/protocol/traffic load and so on. **Traffic** report generated by VRPT is based on the traffic logs information. We could call them traffic report.

### Q4: Which types of devices are supported by VRPT 3.0?

| **Vantage Report 3.0**<br>**Test Matrix** | Vantage Report 3.0<br>Supports<br>Device F/W |
|---|---|
| **ZW 2/10W** | 3.62 |
| **ZW 5/35/70** | 3.62, 3.63, 3.64, 4.00 and later |
| **ZW P1** | 3.64 and later |
| **Prestige 662/652** | 3.40 |
| **IDP 10** | 2.00 |
| **ZW 1050** | 1.01 |

### Q5: How many devices are supported by VRPT 3.0 ?

VRPT3.0 can manage 100 units (device) according performance.

### Q6: Which components are included by VRPT 3.0?

VRPT includes a simple Syslog daemon for collecting device log, MySQL database for storing the log for further analysis, an analysis/reporting module to generate report according to user’s request and schedule setting, tomcat web server to provide user-friendly interface.

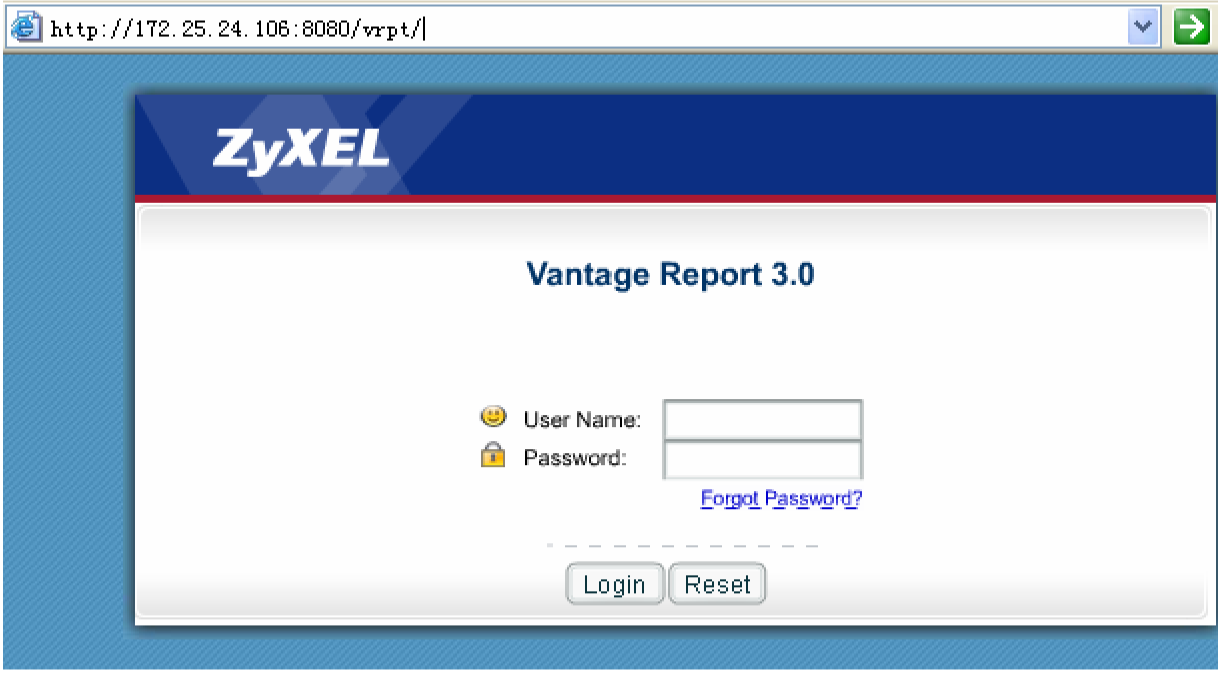
### Q7: How to install VRPT 3.0 server on the PC?

Please refer the hardware/software requirement and quick start guide (QSG) for installation procedure. Installation could be a very simple and straight forward. Just to remind that VRPT installation wizard will install MySQL/Tomcat on your computer. Make sure these applications are NOT running before installation.

### Q8: How to access VRPT 3.0 ?

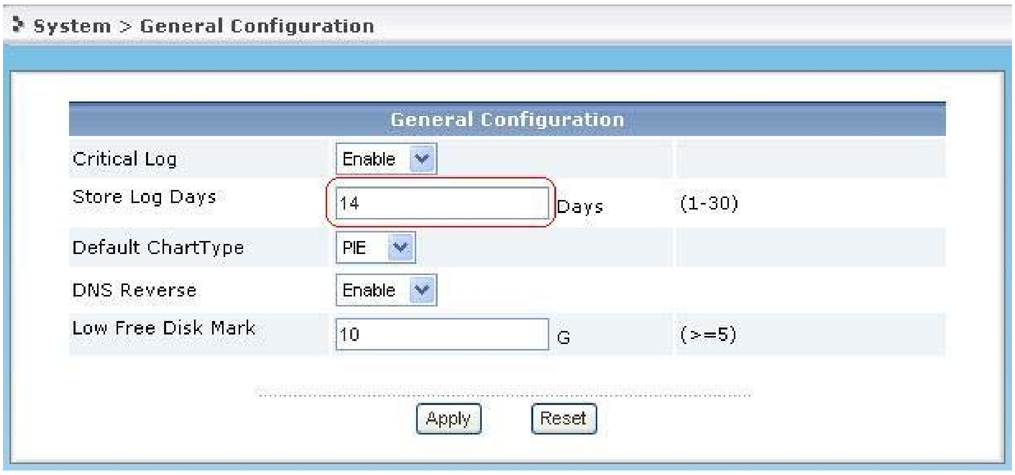
After installing VRPT 3.0 server, you could access VRPT by Microsoft IE 6.0 or later, Firefox 1.07 and later and Mozilla 1.7.12 and later. Please type http://<VRPT Server IP>:8080/vrpt at the remote site if your PC does not install VRPT server or http://localhost:8080/vrpt at local host in the URL field if your PC is VRPT server. The window is shown as below. Default username/password is root/root.

**NOTE**: If user changes Web Server port when installing VRPT, the port 8080 should be changed into customized port when accessing VRPT. Please go to previous part of support note at **How to enable customized Web Server port when installing VRPT?**
Make sure the access control rule is configured to allow UDP 514/ TCP 8080 if firewall is running on the VRPT server. Also if user uses customized port when installing VRPT, customized TCP port should be forwarded instead of TCP port 8080.


http://172.25.24.106:8080/vrpt/

### Q9: How long will raw data (device logs) be stored in VRPT database?

Under System>>General Config, you can determine Log store days. VRPT will keep only those logs which are within the configured days value .The default value is 7.



System > General Configuration

General Configuration

| | | |
|---|---|---|
| Critical Log | Enable | |
| Store Log Days | 14 Days | (1-30) |
| Default ChartType | PIE | |
| DNS Reverse | Enable | |
| Low Free Disk Mark | 10 G | (>=5) |

### Q10: How to check traffic logs report on VRPT 3.0 for ZyXEL xDSL product?

Unfortunately VRPT 3.0 can’t generate such report for ZyXEL xDSL product because such device could not send out traffic log currently.

### Q11: How can I monitor VPN bandwidth or VPN Usage for ZyXEL xDSL product?

Under **Monitor>>Service>>VPN** or **VPN Usage** menu on VRPT 3.0, report is generated by the traffic logs. While ZyXEL xDSL only send event logs for VPN issue. So far it is impossible for you to trace VPN issue for ZyXEL xDSL on VRPT 3.0.

### Q12: How can I check the Anti-Virus status for Prestige xDSL on VRPT 3.0?

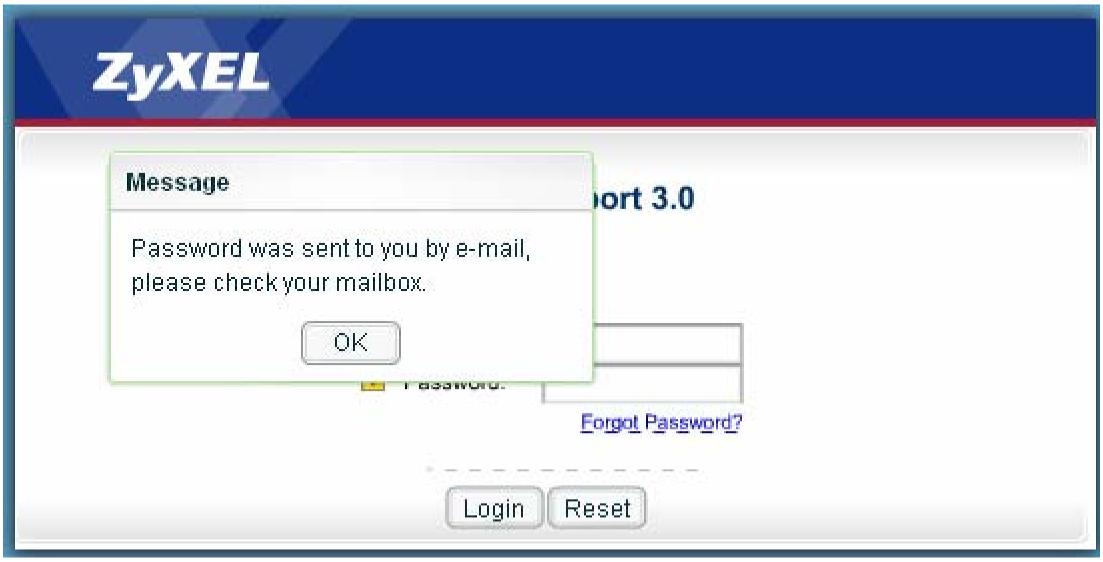
Prestige xDSL devices can’t send out Anti-Virus event logs so VRPT 3.0 could not generate such report for xDSL Anti-Virus.

### Q13: How can I check Intrusion/AntiVirus/AntiSpam report for ZyWALL series with f/w 3.63, 3.64 or 3.65?

ZyWALL series with f/w 3.62, 3.63, 3.64 and 3.65 do not support such functions so they will no send such event logs to VRPT 3.0. It is normal without those UTM reports available when ZyWALL are using those firmware versions.

### Q14: What can I do if I forget the password when logging in VRPT ?

You may click the **Forget Password** on the log in web then VRPT will send back your password via email.



Message

Password was sent to you by e-mail, please check your mailbox.

### Q15: Known Issue for Web Browser Supported by VRPT 3.0

The web browser supported by VRPT 3.0 are Microsoft IE 6.0 or later, Firefox 1.07 and later and Mozilla 1.7.2 and later. You could not login VRPT 3.0 by multiple Firefoxs or Mozillas on the same machine. That means when you login VRPT as a user you can not open another similar page for other user to login VRPT by using Firefox or Mozillas at the same time on single machine. Because Firefox and Mozilla will take them as the same session. And so far print function is not available in Firefox browser although there's a button on web page.

### Q16: VRPT will be installed as a Window Service by default, is it right?

After you install VRPT 3.0 and restart your machine, VRPT will be started up. Under this circumstance it is normal for VRPT 3.0 to start up automatically because we install it as Windows service.

### Q17: Log Time on VRPT 3.0

When VRPT 3.0 receives logs, it will replace the time of the logs as VRPT Server's current time. So it is normal for different devices that each has individual system time send logs with universal time on VRPT.

### Q18: Report Pattern for Schedule Reports

VRPT 3.0 supports two kinds of pattern for **Schedule Reports**. One is HTML pattern and the other is PDF pattern. HTML pattern report looks like offline VRPT report. The report looks the same style as you could see on live VRPT. It remains the drill down report and the link.

### Q19: Related General Public License about VRPT

Some components of the Vantage Report distribute with source code covered under one or more third party or open source licenses. We do not include full text of the licenses in this document. If you required them please go to Vantage Report 3.0 User Guide. To get the source code covered under these licenses, please contact CSO team for Vantage Report Technical Support.

### Q20: The meaning of AC related Registration and Activation with myZyXEL.com

AC is a short form of Authentication Code. It is generated by the software embedded in VRPT 3.0. AC is a hash code generated from user’s PC system. And AC is a useful item for myZyXEL.com to do authentication. Only partial of the info is used to create an ID for myZyXEL.com authentication.