Vantage Report

Support Notes

Version 2.3

Feb. 2006

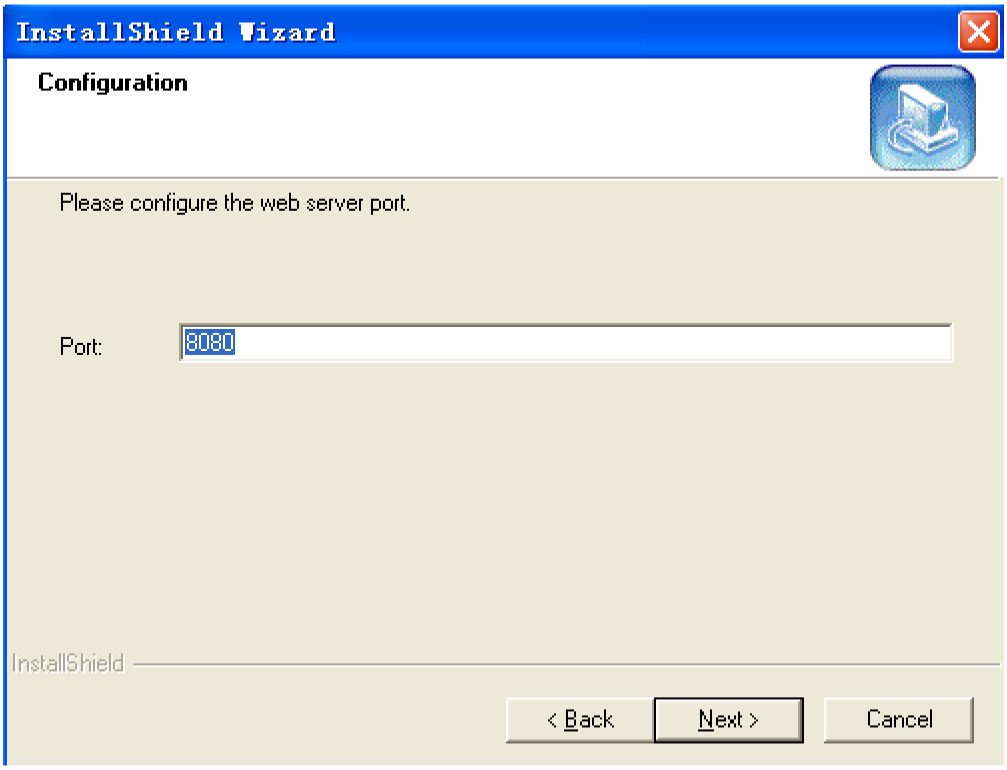
INDEX

Application Notes

General Application Notes

How to enable customized Web Server port when installing VRPT?

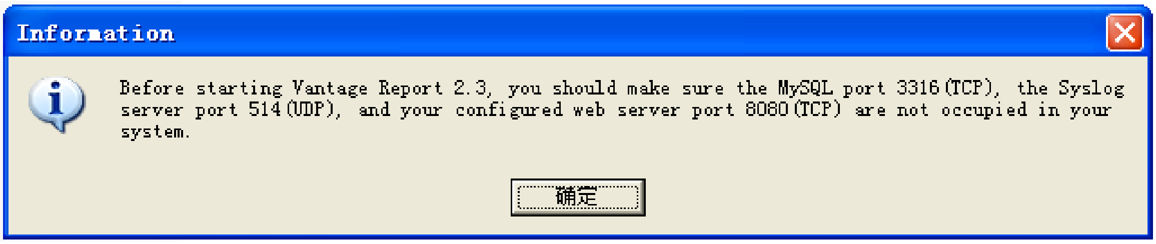
User could change the default TCP port 8080 to customized one when installing VRPT. Please do such change in Configuration step.



Please configure the web server port.

Port: 8080

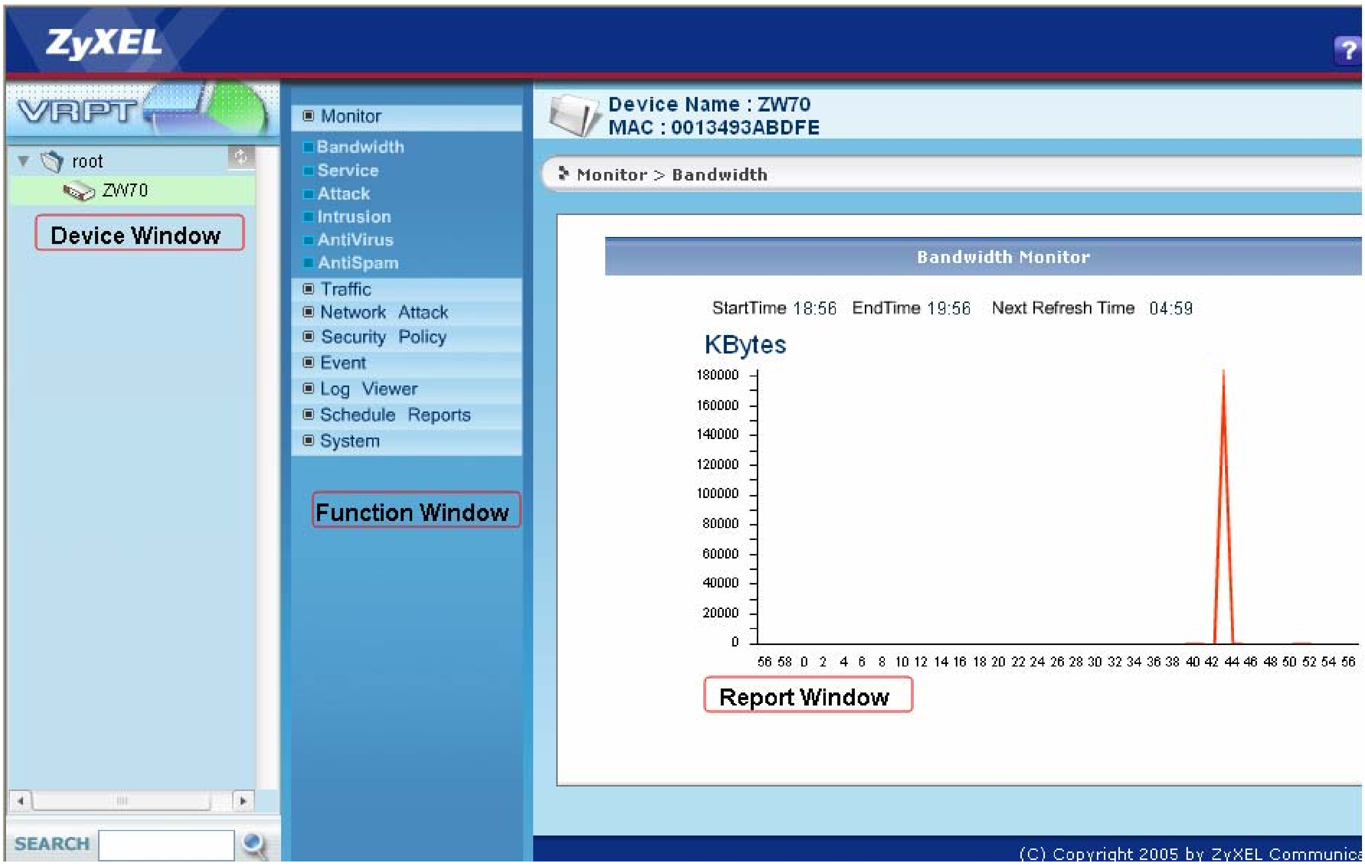
After user finishes installation, VRPT system will pop up such windows to remind the important system message. If Web server port is customized during installation, it will remain unchanged unless user reinstalls VRPT again and follows above step to change.



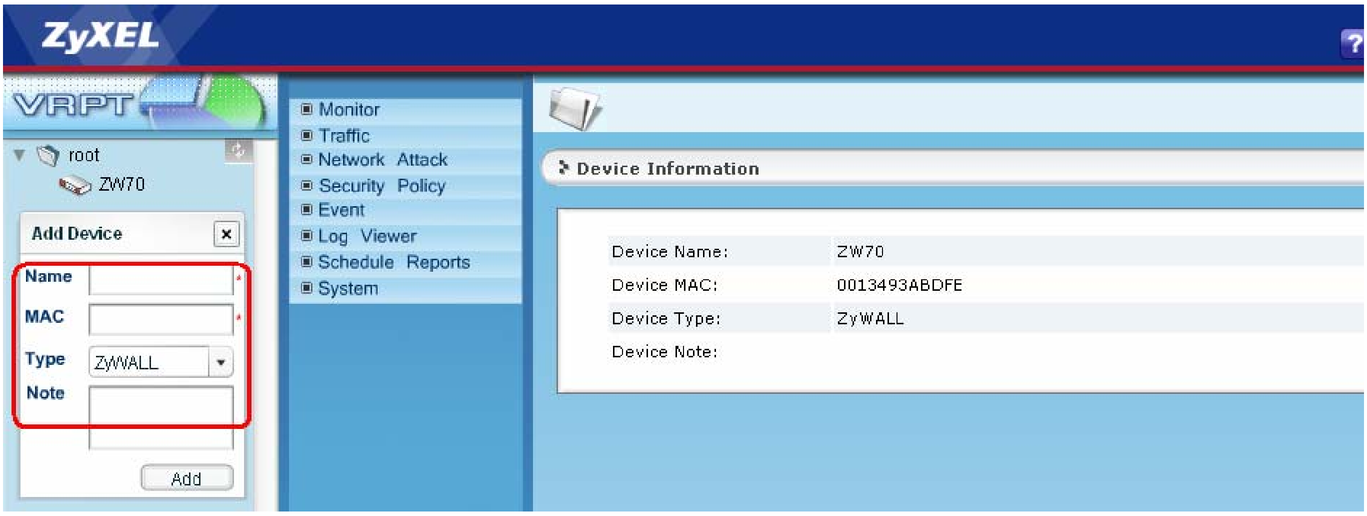
Before starting Vantage Report 2.3, you should make sure the MySQL port 3316(TCP), the Syslog server port 514(UDP), and your configured web server port 8080(TCP) are not occupied in your system.

Adding Device to Device Tree of VRPT

VRPT 2.3 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.



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.



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.

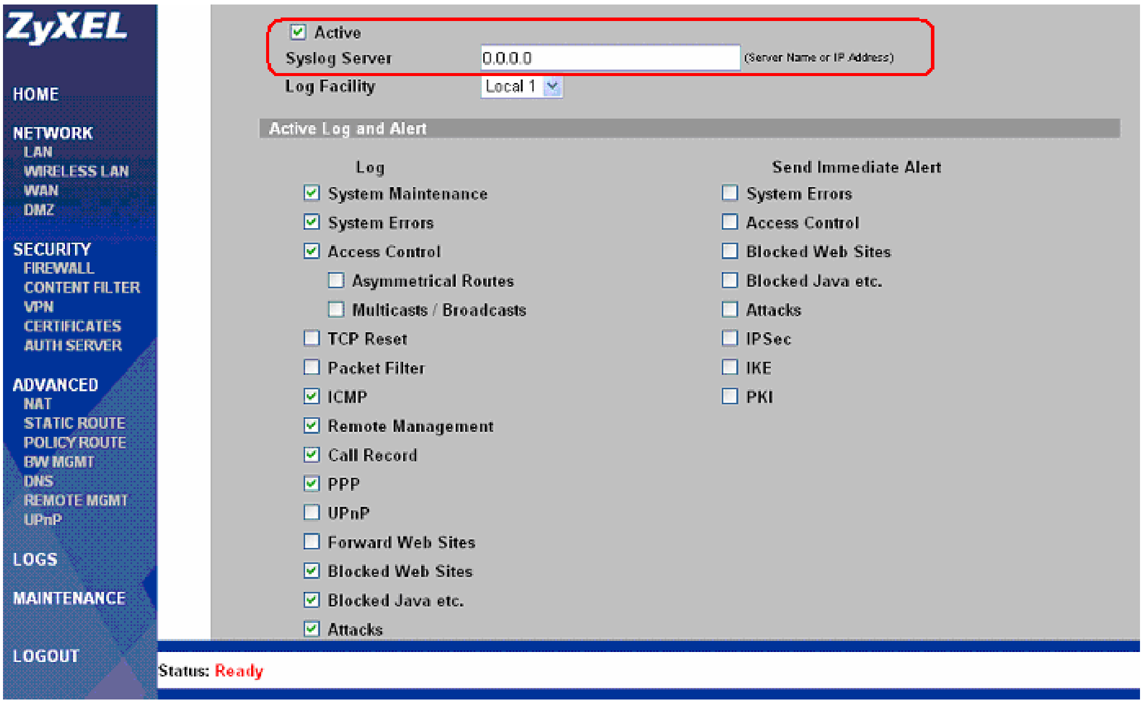
If user once removes a device from **Device Tree**, all the historical info about it will be removed by VRPT. And the process will take a period of time.

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.

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.



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

Active Log and Alert

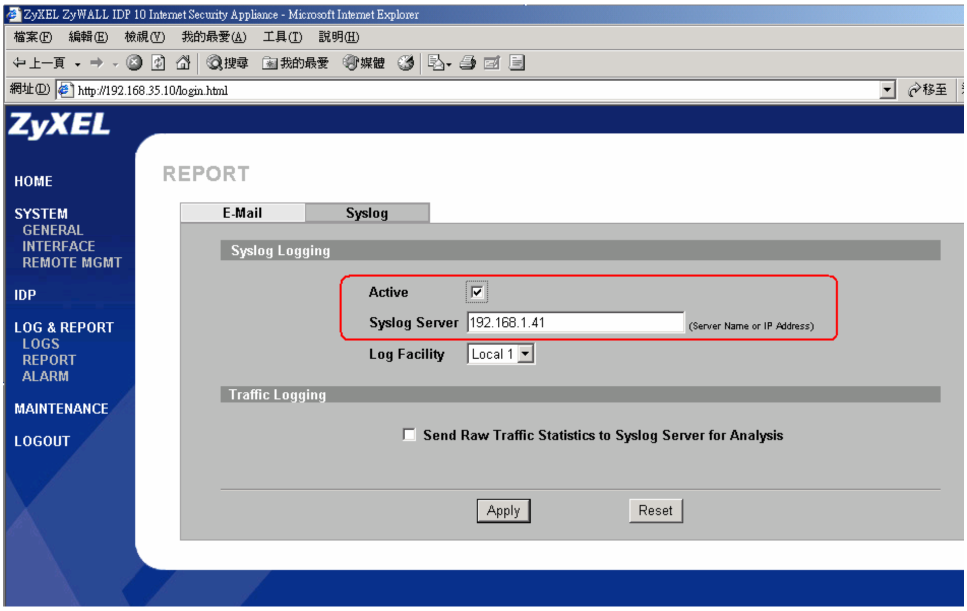
Log	Send Immediate Alert
☑ System Maintenance	□ System Errors
☑ System Errors	□ Access Control
☑ Access Control	□ Blocked Web Sites
□ Asymmetrical Routes	□ Blocked Java etc.
□ Multicasts / Broadcasts	□ Attacks
□ TCP Reset	□ IPSec
□ Packet Filter	□ IKE
☑ ICMP	□ PKI
☑ Remote Management	
☑ Call Record	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

Status: Ready

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.


ZyXEL ZyWALL IDP 10 Internet Security Appliance - Microsoft Internet Explorer
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
上一頁 搜尋 我的最愛 媒體
網址(D) http://192.168.35.10/login.html
移至
ZyXEL
HOME
SYSTEM
GENERAL
INTERFACE
REMOTE MGMT
IDP
LOG & REPORT
LOGS
REPORT
ALARM
MAINTENANCE
LOGOUT
E-Mail
Syslog
Apply
Reset

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

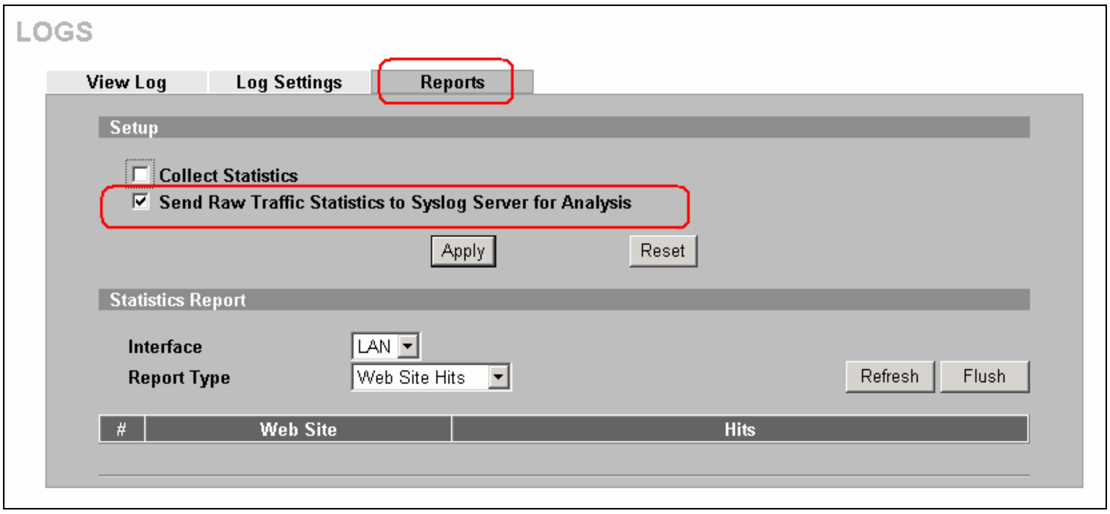
After activing the Syslog Server you should select the log types you want to send that are listed under the left side of **Active Log and Alert** (for ZyWALL,IDP) or under **Log** (for xDSL) column on this web page.

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. 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

#	Web Site	Hits

Fig.7 Enable Traffic Log on ZyWALL

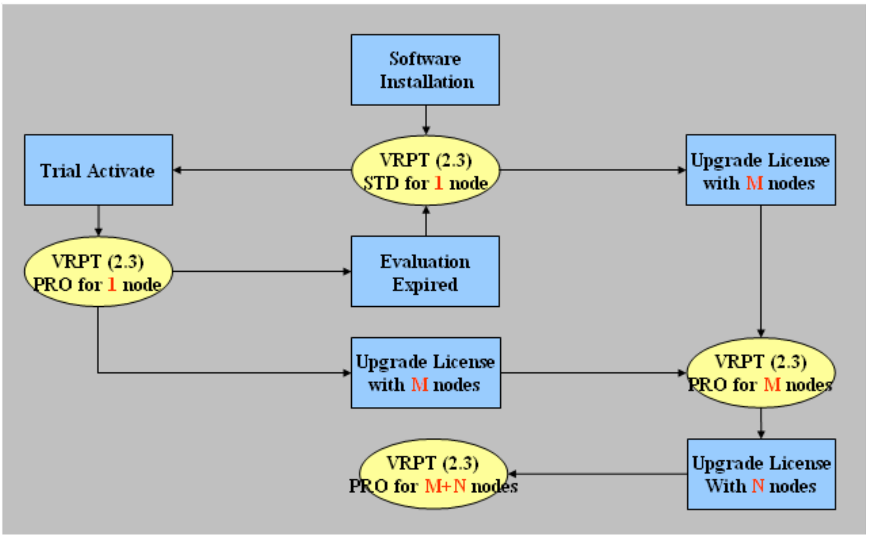
2. Enable Traffic Logs from SMT (Telnet/Console) menu 24.3.2

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

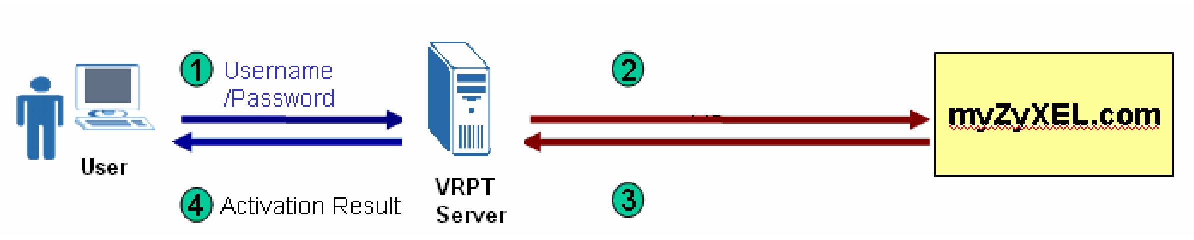
Below is a brief flow that describes the evolvement from standard (STD) to professional version (PRO).


Software Installation
VRPT (2.3) STD for 1 node
Trial Activate
Upgrade License with M nodes
VRPT (2.3) PRO for 1 node
Evaluation Expired
Upgrade License with M nodes
VRPT (2.3) PRO for M nodes
VRPT (2.3) PRO for M+N nodes
Upgrade License With N nodes

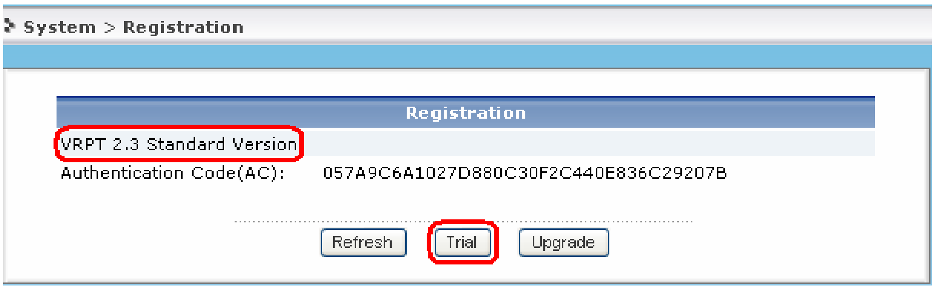
When user installs VRPT 2.3, VRPT will show as standard version (STD). If user wants to upgrade to professional version (PRO), there's two way to achieve it. One is to achieve it by trial activation. But this kind of PRO (Trial) has time restriction (30 days). Also in this Trial version, user only can manage one node (device). The other is to upgrade to final PRO by inputting legal license user ever bought.

There are other two kinds of license. One kind supports 5 nodes, That means 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 2.3 can managed is 25.

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



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



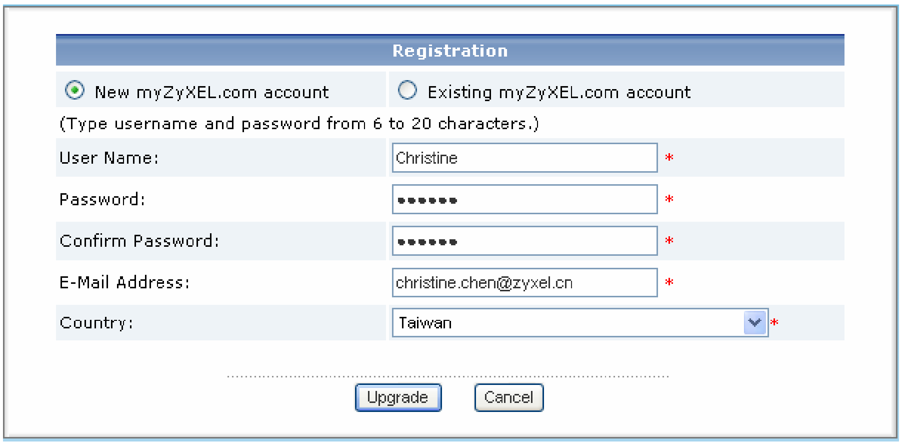
System > Registration

Registration

VRPT 2.3 Standard Version

Authentication Code(AC): 057A9C6A1027D880C30F2C440E836C29207B

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 *

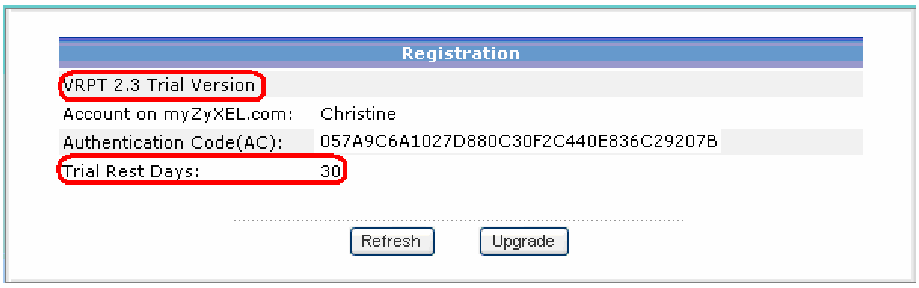
Password: •••••• *

Confirm Password: •••••• *

E-Mail Address: christine.chen@zyxel.cn *

Country: Taiwan *

3. VRPT 2.3 will send the **User Name, Password,** Trial License key(T-VR0001) and other information to myZyxel.com.



Registration

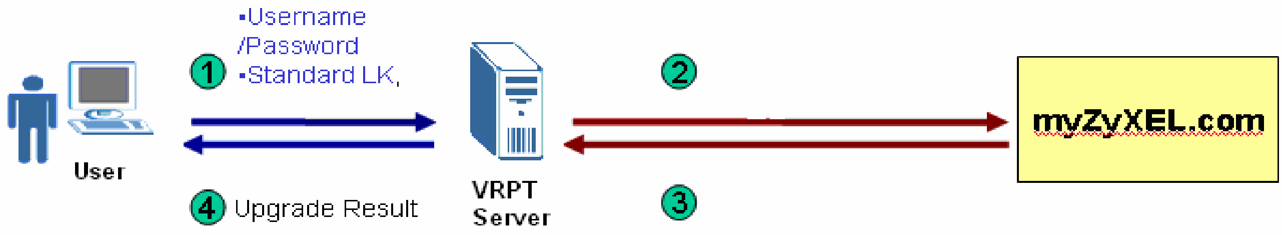
VRPT 2.3 Trial Version

Account on myZyXEL.com: Christine

Authentication Code(AC): 057A9C6A1027D880C30F2C440E836C29207B

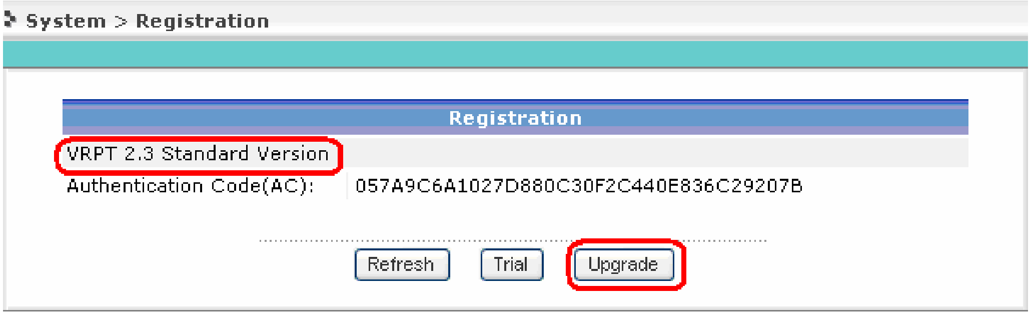
Trial Rest Days: 30

- **VRPT Service Activation-Install to Professional**



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**



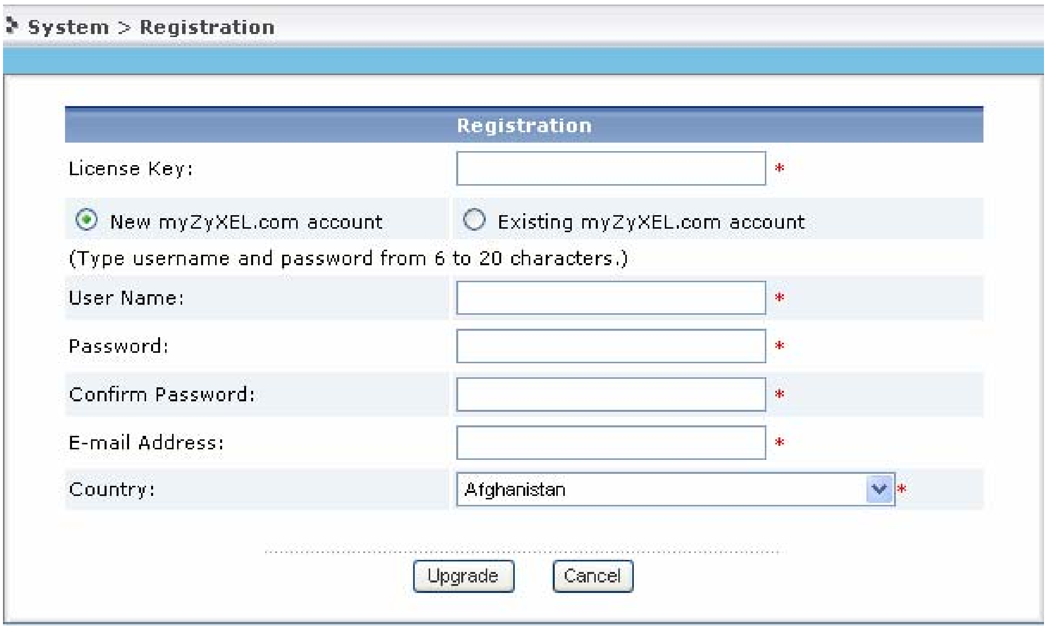
System > Registration

Registration

VRPT 2.3 Standard Version

Authentication Code(AC): 057A9C6A1027D880C30F2C440E836C29207B

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: *

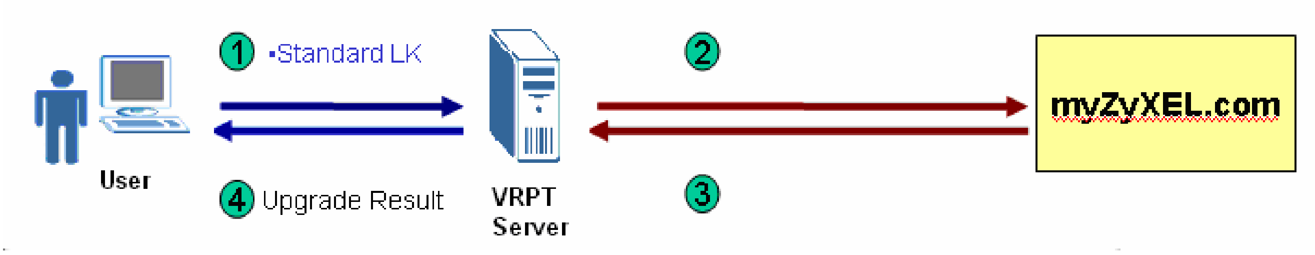
Confirm Password: *

E-mail Address: *

Country: Afghanistan *

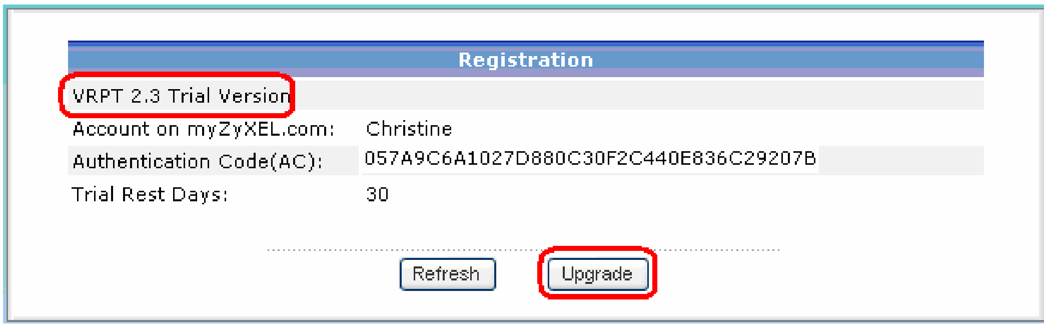
3. VRPT will send such items and other information to myZyXEL.com and complete authentication.

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



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

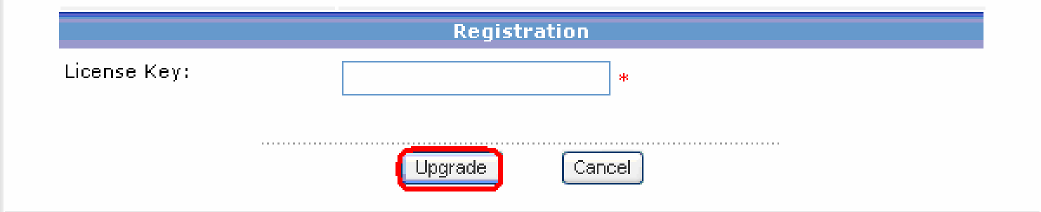
1. Click **Upgrade** button.



Registration

VRPT 2.3 Trial Version	
Account on myZyXEL.com:	Christine
Authentication Code(AC):	057A9C6A1027D880C30F2C440E836C29207B
Trial Rest Days:	30

2. Input **License.**



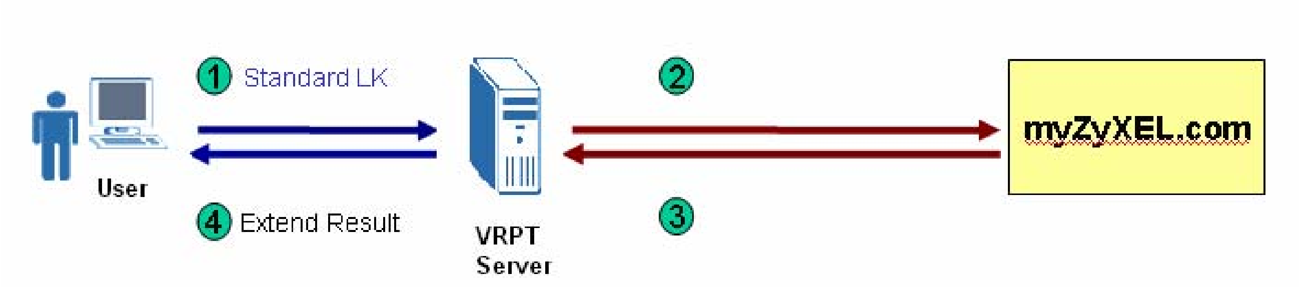
Registration

License Key: *

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

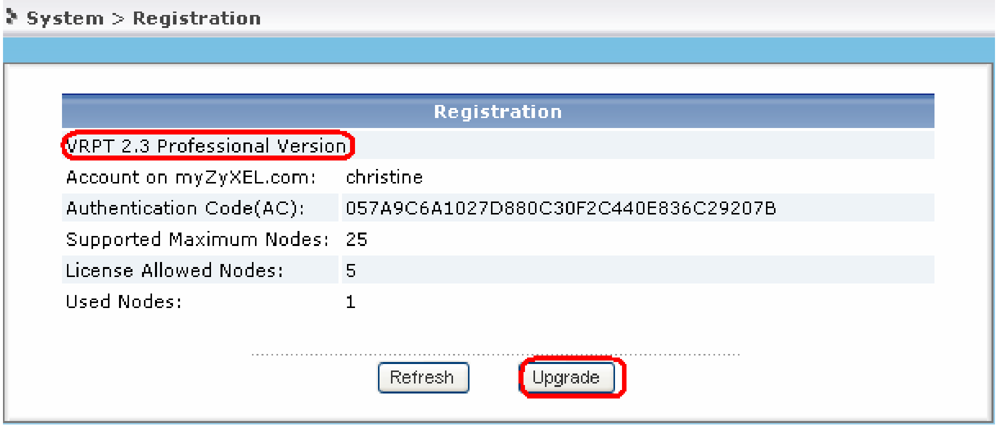
NOTE: If user reinstalls VRPT at same machine with OS untouched and it was professional version already, VRPT will remain as professional status.

- **VRPT Service Extend–Profession to Profession version**



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

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

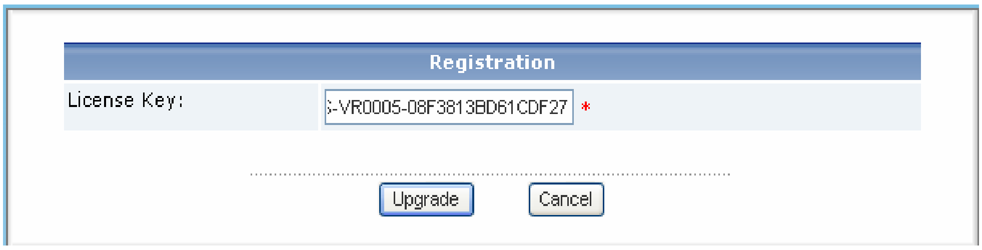

System > Registration

Registration

VRPT 2.3 Professional Version

Account on myZyXEL.com:	christine
Authentication Code(AC):	057A9C6A1027D880C30F2C440E836C29207B
Supported Maximum Nodes:	25
License Allowed Nodes:	5
Used Nodes:	1

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 2.3 and Their Supported Feature

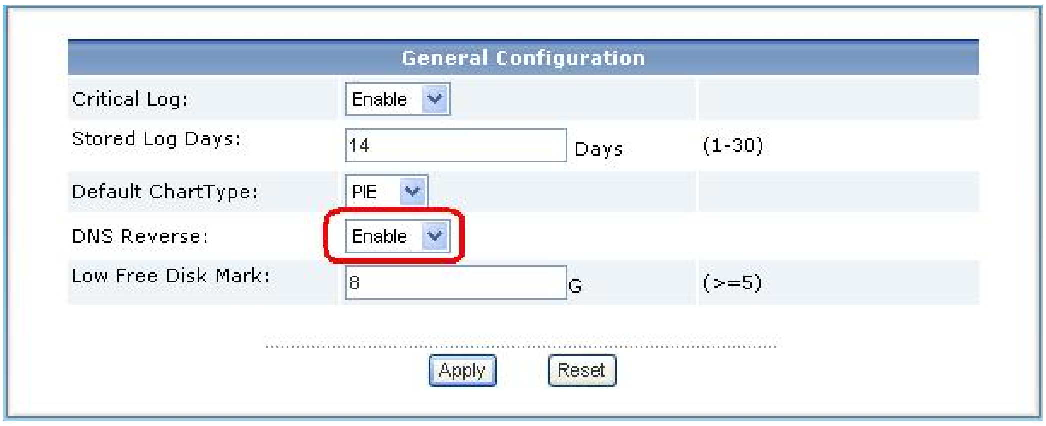
There are two main version types: Standard (STD) version and Professional (PRO) version. The table below shows the features they support. Trial status has the same features as PRO version.

	Standard (STD) version	**Professional (PRO) version**
Num of supported nodes	1	25
Number of Scheduled Report	20	500
Report Format	PDF only	PDF & HTML
Drill-down Report	1 layer	2 layers
Traffic Report by Direction	All	All/Inbound/outbound/WAN-LAN/WAN-DMZ/WAN-WAN/LAN-LAN/LAN-WAN/LAN-DMZ/DMZ-WAN/DMZ-LAN/DMZ-DMZ
Web Filter Report by Category	No	Yes
Reverse DNS Lookup	No	Yes
Bandwdith Report	Yes	Yes
Service Report	Yes	Yes
Web Filter Report	Yes	Yes
Attack Report	Yes	Yes
Intrusion Report	No	Yes
AntiVirus Report	No	Yes
AntiSpam Report	No	Yes

Authentication Report	Yes	Yes

The Way to Use Reverse DNS Function

VRPT 2.3 supplies reverse DNS 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.



General Configuration

Critical Log: Enable

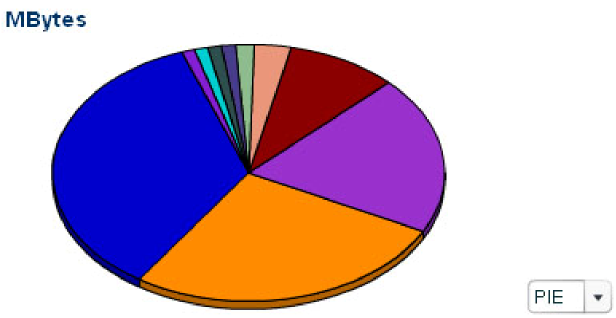
Stored Log Days: 14 Days (1-30)

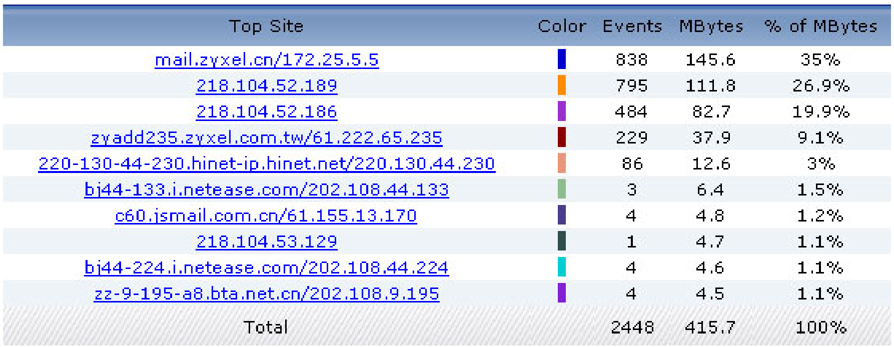
Default ChartType: PIE

DNS Reverse: Enable

Low Free Disk Mark: 8 G (>=5)

Please see the sample as following.

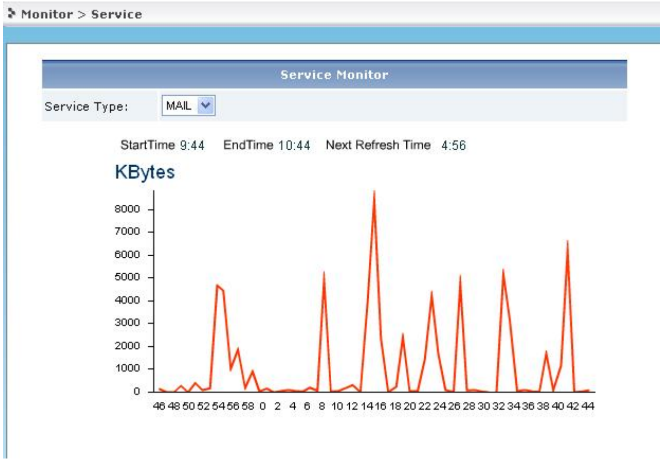




Top Site	Color	Events	MBytes	% of MBytes
mail.zyxel.cn/172.25.5.5	■	838	145.6	35%
218.104.52.189	■	795	111.8	26.9%
218.104.52.186	■	484	82.7	19.9%
zyadd235.zyxel.com.tw/61.222.65.235	■	229	37.9	9.1%
220-130-44-230.hinet-ip.hinet.net/220.130.44.230	■	86	12.6	3%
bj44-133.i.netease.com/202.108.44.133	■	3	6.4	1.5%
c60.jsmail.com.cn/61.155.13.170	■	4	4.8	1.2%
218.104.53.129	■	1	4.7	1.1%
bj44-224.i.netease.com/202.108.44.224	■	4	4.6	1.1%
zz-9-195-a8.bta.net.cn/202.108.9.195	■	4	4.5	1.1%
Total		2448	415.7	100%

Monitor Function for Live Check

There is a special menu in VRPT 2.3 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.

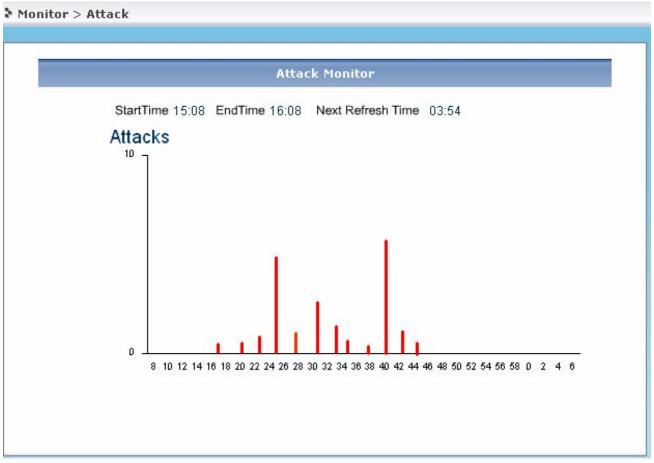


Monitor > Service

Service Monitor

Service Type: MAIL

StartTime 9:44 EndTime 10:44 Next Refresh Time 4:56



Monitor > Attack

Attack Monitor

StartTime 15:08 EndTime 16:08 Next Refresh Time 03:54

Bandwidth /Service Monitor Report

Coordinate	Meaning	Unit
Xaxis	Lease time	Minute
Yaxis	bandwidth	Kbytes

Attack/Intrusion/AntiVirus/AntiSpam Monitor Report

Coordinate	Meaning	Unit
Xaxis	Lease time	minute
Yaxis	Number of the events	

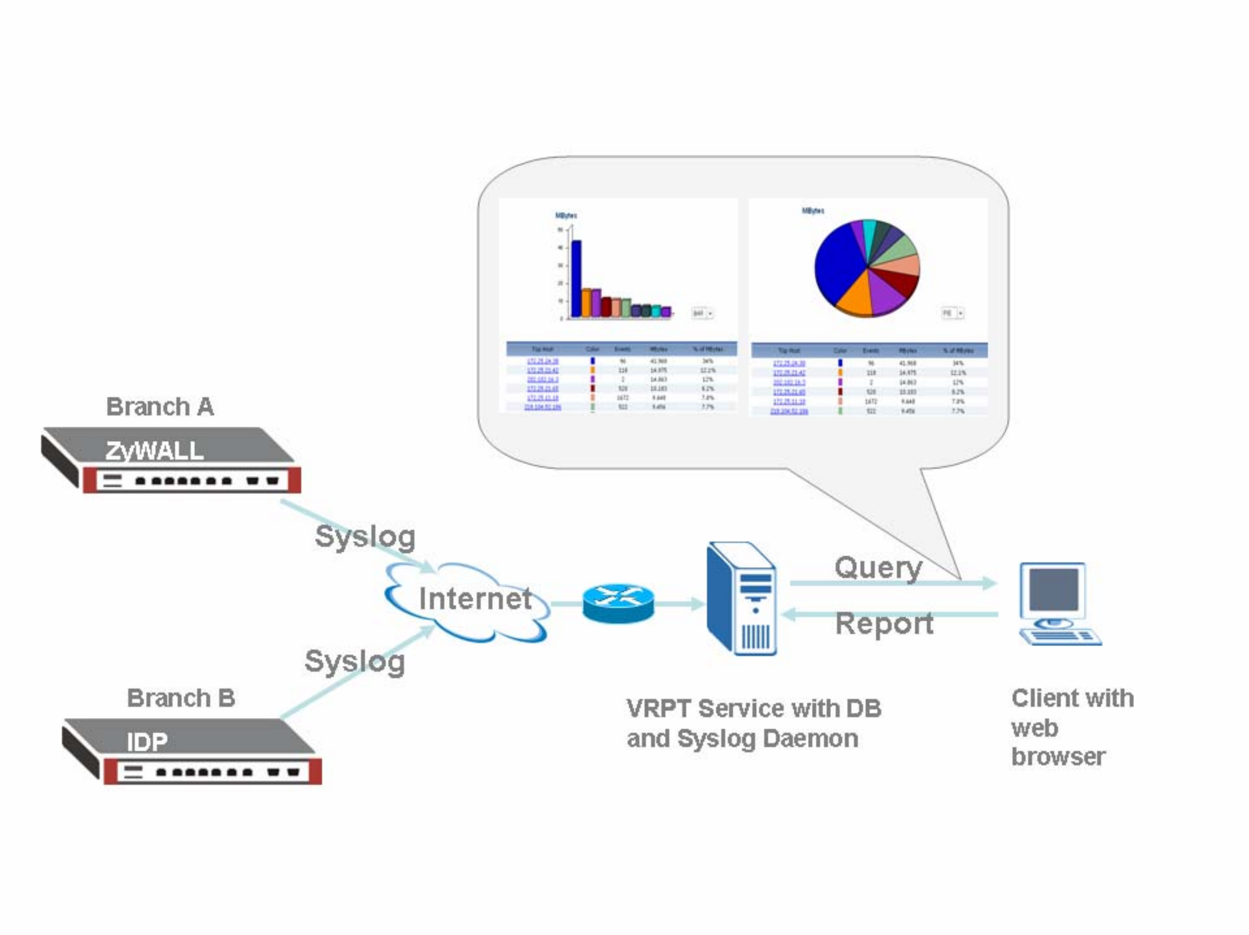
NOTE: You should select a device from **Device Tree** before querying a report from VRPT.

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.

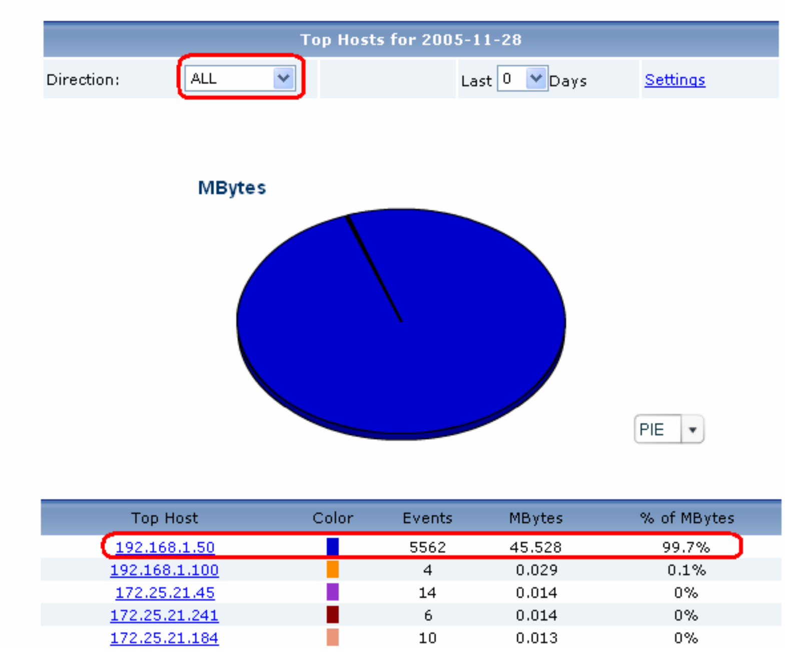
Please select a device from the **Device Tree** by clicking before querying a report.

Drill Down Report

VRPT 2.3 supports Drill-down report for **Traffic** report, **Security Policy** report and **Network Attack** report except **Network Attack**>>**AntiSpam** report.

User could use such function for detailed information.

Here we give an example for bandwidth drill down usage.

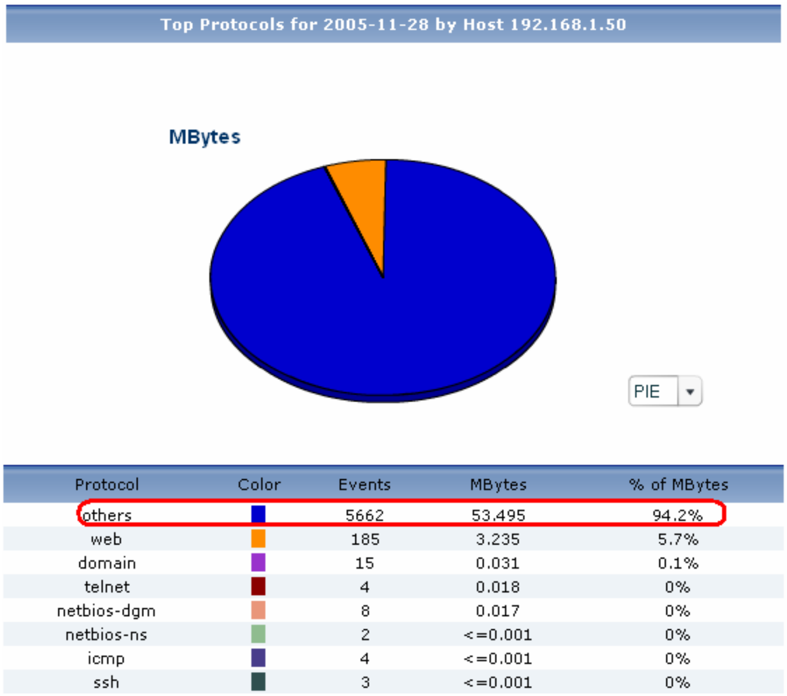


Top Hosts for 2005-11-28

Direction: ALL   Last 0 Days   Settings

Top Host	Color	Events	MBytes	% of MBytes
192.168.1.50	🟦	5562	45.528	99.7%
192.168.1.100	🟧	4	0.029	0.1%
172.25.21.45	🟪	14	0.014	0%
172.25.21.241	🟥	6	0.014	0%
172.25.21.184	🟧	10	0.013	0%

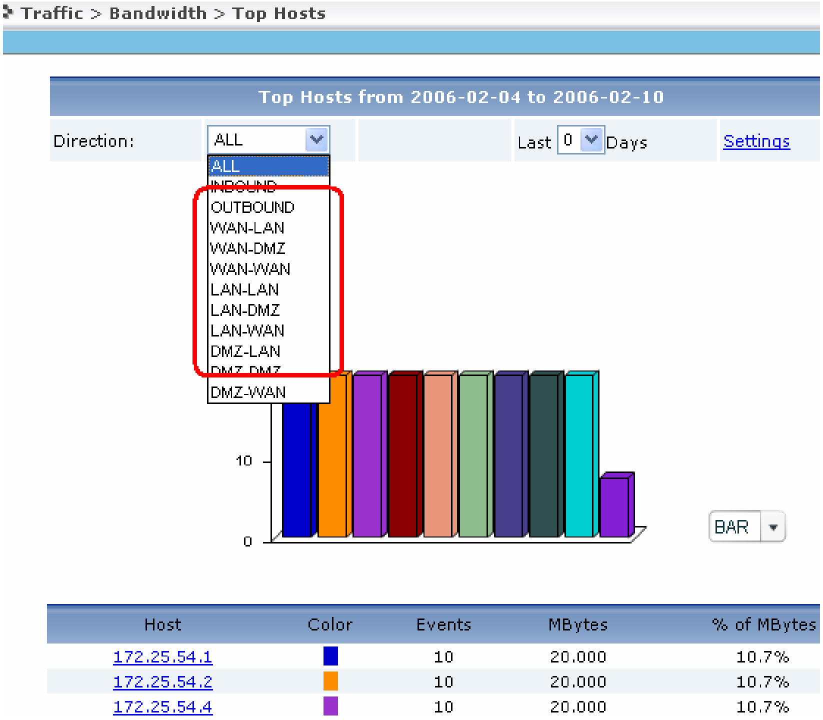
The drill down report shows the detailed report for IP address 192.168.1.50.



Top Protocols for 2005-11-28 by Host 192.168.1.50

Protocol	Color	Events	MBytes	% of MBytes
others	🟦	5662	53.495	94.2%
web	🟧	185	3.235	5.7%
domain	🟪	15	0.031	0.1%
telnet	🟥	4	0.018	0%
netbios-dgm	🟧	8	0.017	0%
netbios-ns	🟩	2	<=0.001	0%
icmp	🟦	4	<=0.001	0%
ssh	🟩	3	<=0.001	0%

Direction for Bandwidth Usage



Traffic > Bandwidth > Top Hosts

Top Hosts from 2006-02-04 to 2006-02-10

Direction: ALL

Last 0 Days

Settings

Host	Color	Events	MBytes	% of MBytes
172.25.54.1	🟦	10	20.000	10.7%
172.25.54.2	🟧	10	20.000	10.7%
172.25.54.4	🟪	10	20.000	10.7%

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 2.2 to VRPT 2.3?

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. He/she should input MAC address of LAN one by one, choose device type …etc. Now if user wants VRPT 2.3 to manage the devices that are in the charge of VRPT 2.2, all the job will be done well and fast by following such steps below and you can also check *Upgrade Note*.

1 Copy “migration” folder to VRPT 2.2 installed folder, for example, “C:\Program Files\ZyXEL\Vantage Report”.

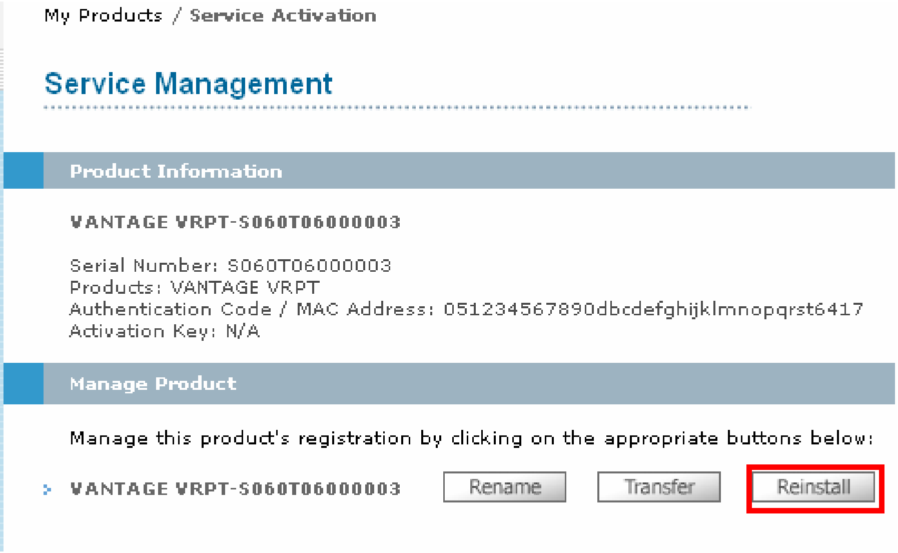
2. Start up VRPT 2.2.
3. Execute exportDeviceList.bat file to get device list. A file named Devices.xml will be produced in the migration folder.
4. Please save Devices.xml to other folder before uninstall VRPT 2.2. Migration folder will be deleted when uninstalling VRPT 2.2 and such .xml will be deleted if it is under default folder.
5. Stop Kiwi, Mysql and VRPT 2.2 and uninstall VRPT 2.2.
6. Install VRPT 2.3 and restart machine.
7. Upgrade licenses.
8. Import Devices.xml under **System**>>**Date Maintenance**>>**Device List Import & Export**>>**Device List Import**

License Migration When Re-installing VRPT 2.3

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.**

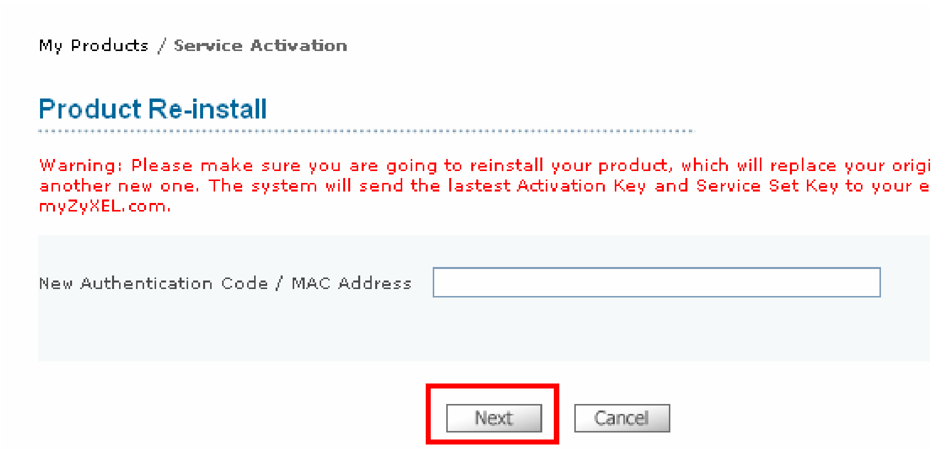


VANTAGE VRPT-S060T06000003

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

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

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.



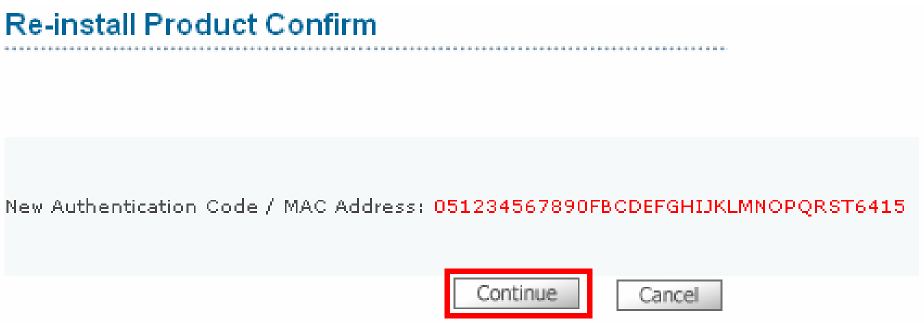
My Products / Service Activation

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.

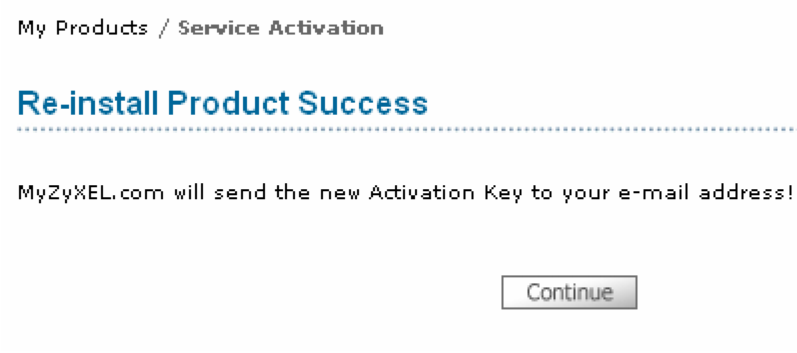
New Authentication Code / MAC Address

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

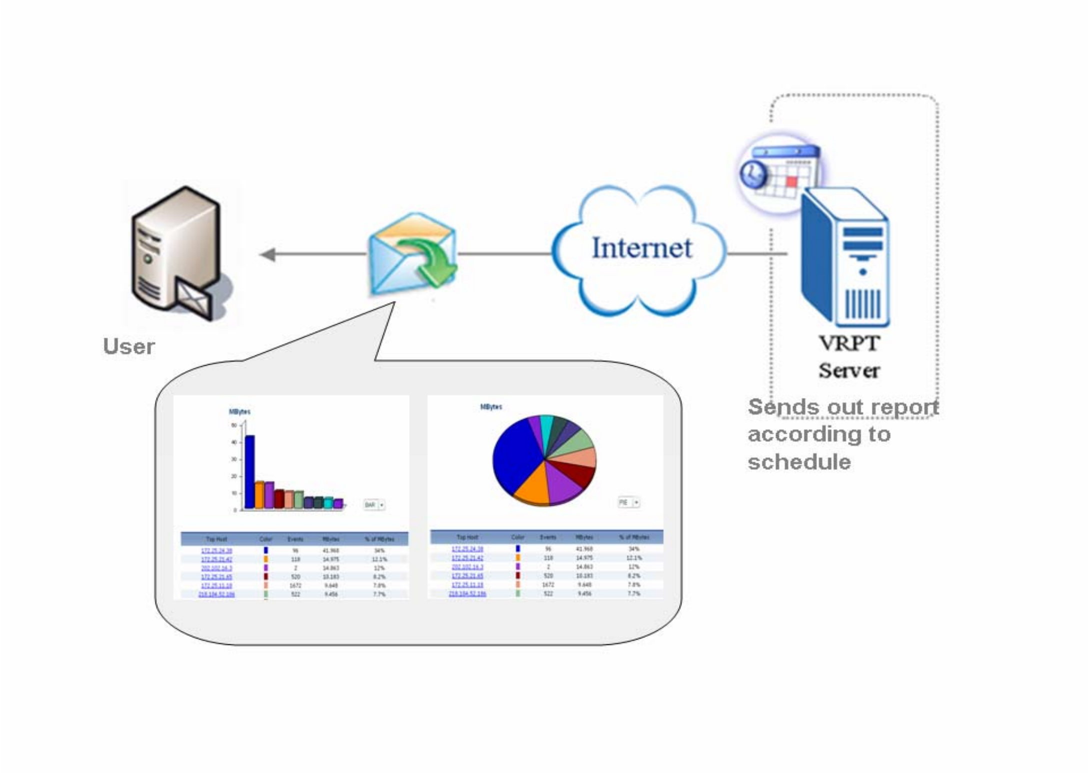
Re-install Product Success

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

Advanced Application Notes

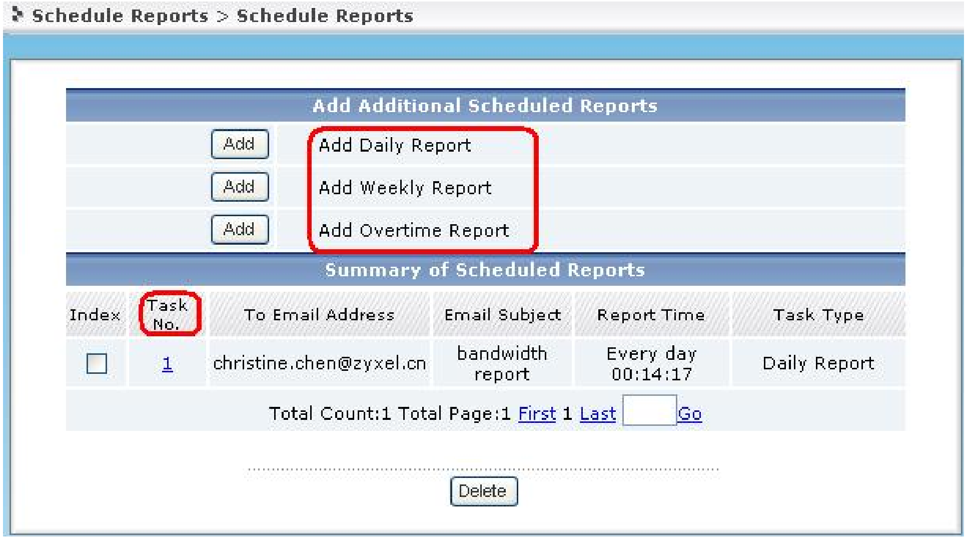
Using Schedule Report

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

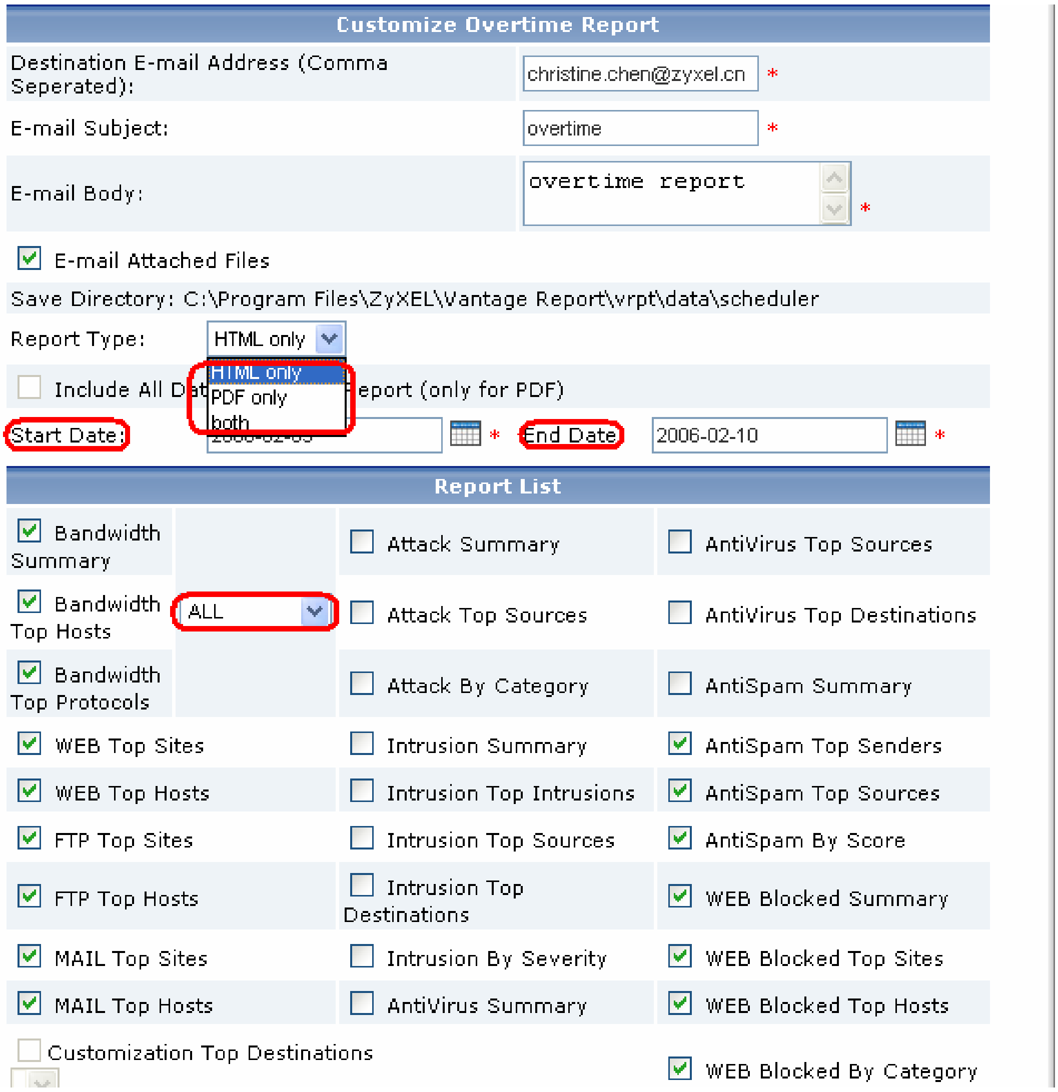
Summary of Scheduled Reports

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. You may include two of them in your scheduled report by choose **both** in the drop down menu.
2.3. 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**.



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

□ Include All Dat eport (only for PDF)

Start Date: 2006-02-03 * End Date 2006-02-10 *

Report List

☑ Bandwidth Summary	□ Attack Summary	□ AntiVirus Top Sources
☑ Bandwidth Top Hosts ALL	□ Attack Top Sources	□ AntiVirus Top Destinations
☑ Bandwidth Top Protocols	□ Attack By Category	□ AntiSpam Summary
☑ WEB Top Sites	□ Intrusion Summary	☑ AntiSpam Top Senders
☑ WEB Top Hosts	□ Intrusion Top Intrusions	☑ AntiSpam Top Sources
☑ FTP Top Sites	□ Intrusion Top Sources	☑ AntiSpam By Score
☑ FTP Top Hosts	□ Intrusion Top Destinations	☑ WEB Blocked Summary
☑ MAIL Top Sites	□ Intrusion By Severity	☑ WEB Blocked Top Sites
☑ MAIL Top Hosts	□ AntiVirus Summary	☑ WEB Blocked Top Hosts
□ Customization Top Destinations		☑ WEB Blocked By Category

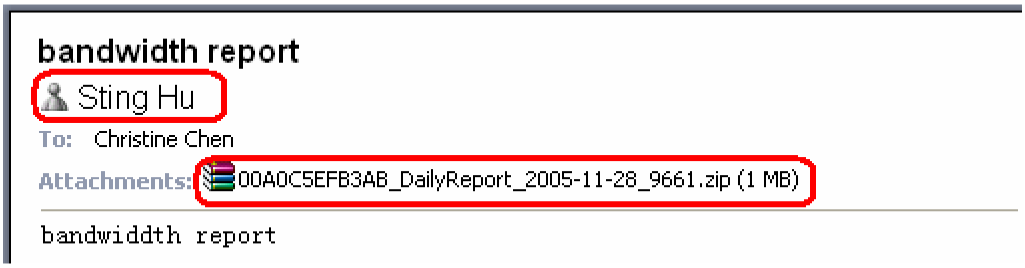
NOTE : If you want to add a daily report, do not set the value for log storing days as 1. Because the daily report only reports log statistics yesterday. That is to say the mail you get each time you've set will show nothing if you set "log store day=1". The date in the PDF /HTML file is the day before.

If you choose the direction for Bandwidth, both **Bandwidth Summary** and **Bandwidth Top Hosts** will apply this direction.

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

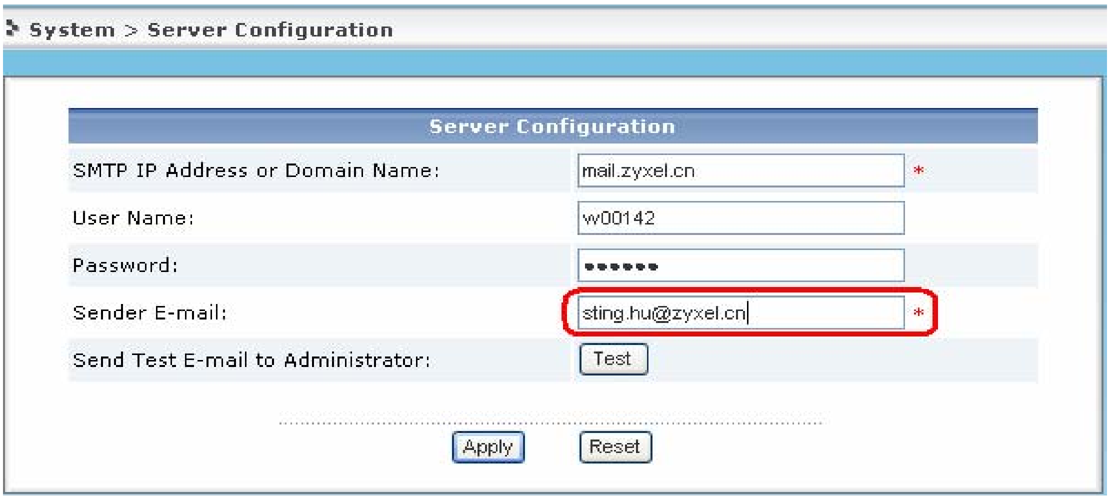
Sting Hu

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

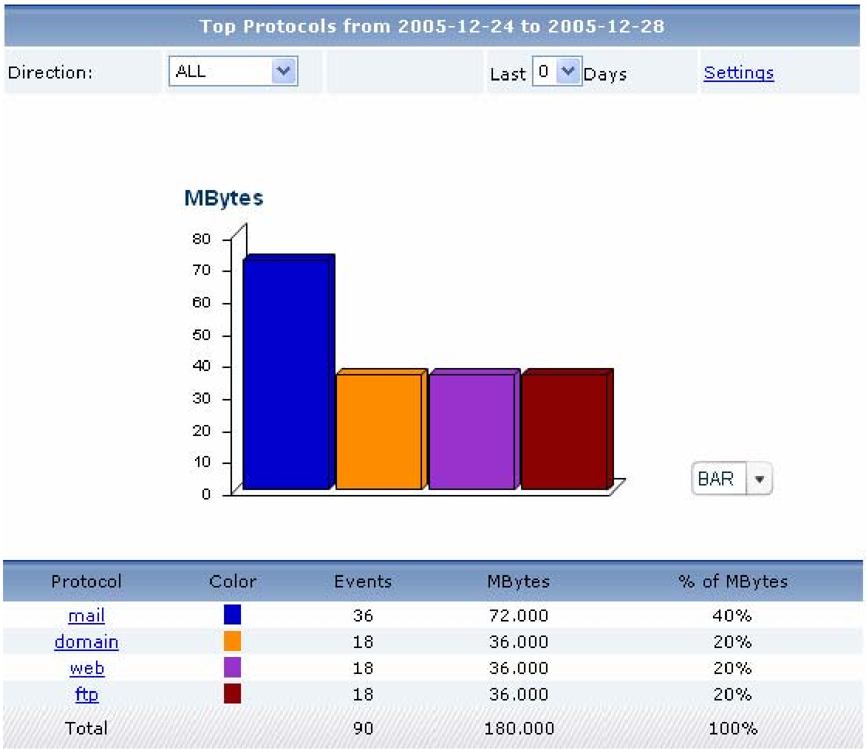
Server Configuration

SMTP IP Address or Domain Name:	mail.zyxel.cn *
User Name:	w00142
Password:	••••••
Sender E-mail:	sting.hu@zyxel.cn *
Send Test E-mail to Administrator:	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



Top Protocols from 2005-12-24 to 2005-12-28

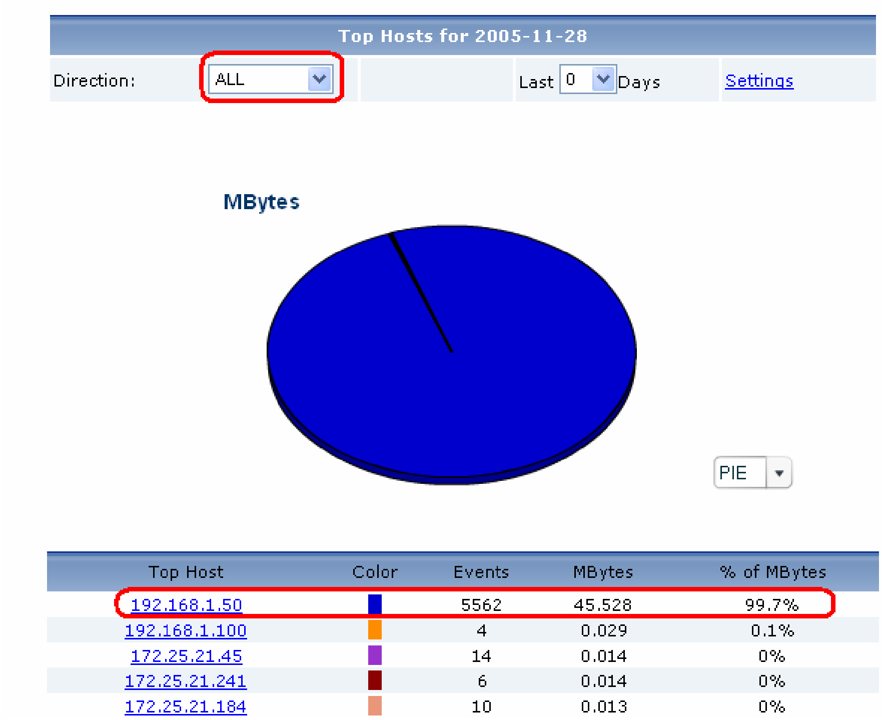
Direction: ALL Last 0 Days Settings

Protocol	Color	Events	MBytes	% of MBytes
mail	🟦	36	72.000	40%
domain	🟧	18	36.000	20%
web	🟪	18	36.000	20%
ftp	🟥	18	36.000	20%
Total		90	180.000	100%

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.

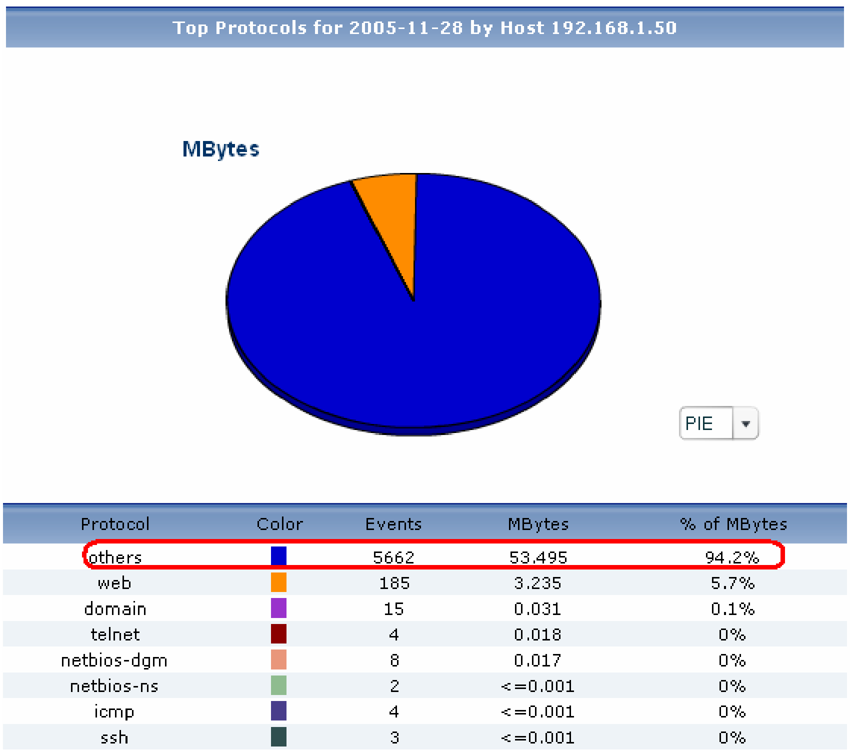


Top Hosts for 2005-11-28

Direction: ALL Last 0 Days Settings

Top Host	Color	Events	MBytes	% of MBytes
192.168.1.50	🟦	5562	45.528	99.7%
192.168.1.100	🟧	4	0.029	0.1%
172.25.21.45	🟪	14	0.014	0%
172.25.21.241	🟥	6	0.014	0%
172.25.21.184	🟫	10	0.013	0%

It shows the users with IP address 192.168.1.50 is on the top of the list. Administrator could enter the drill down menu of it to check further. See below.



Top Protocols for 2005-11-28 by Host 192.168.1.50

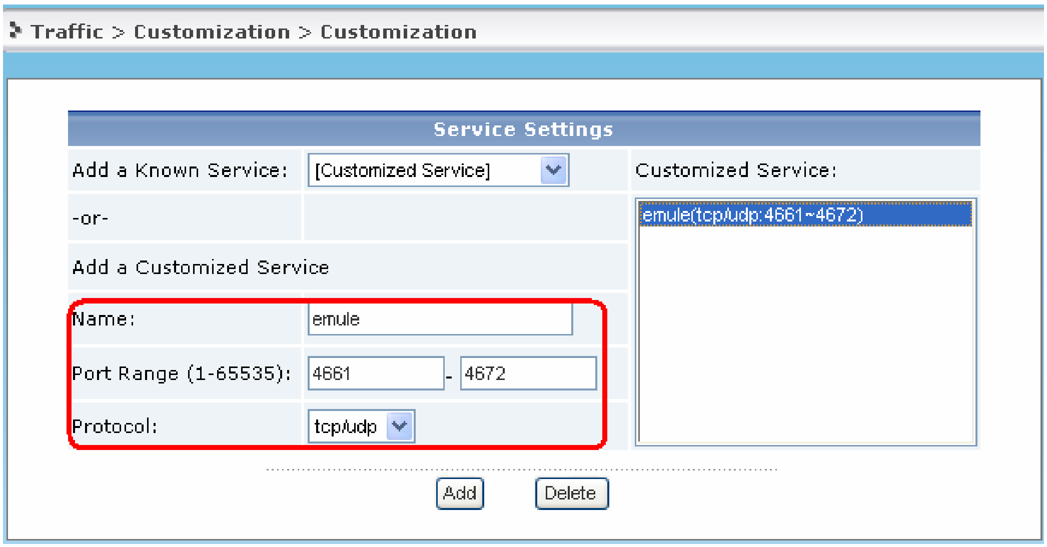
Protocol	Color	Events	MBytes	% of MBytes
others	🟦	5662	53.495	94.2%
web	🟧	185	3.235	5.7%
domain	🟪	15	0.031	0.1%
telnet	🟥	4	0.018	0%
netbios-dgm	🟫	8	0.017	0%
netbios-ns	🟩	2	<=0.001	0%
icmp	🟪	4	<=0.001	0%
ssh	⬛	3	<=0.001	0%

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 may consume a lot if NAT session (with large number of events) while this effect 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

In the last application administrator could determine the error host while he still can not find the root operations of the host user. The report implies that event usage is much large and P2P usage is very popular these days. Then administrator plans to add a customized service as a try. He goes to **Traffic**>>**Customization**>>**Customization** and adds emule as a customized service.



Traffic > Customization > Customization

Service Settings

Add a Known Service: [Customized Service]

-or-

Add a Customized Service

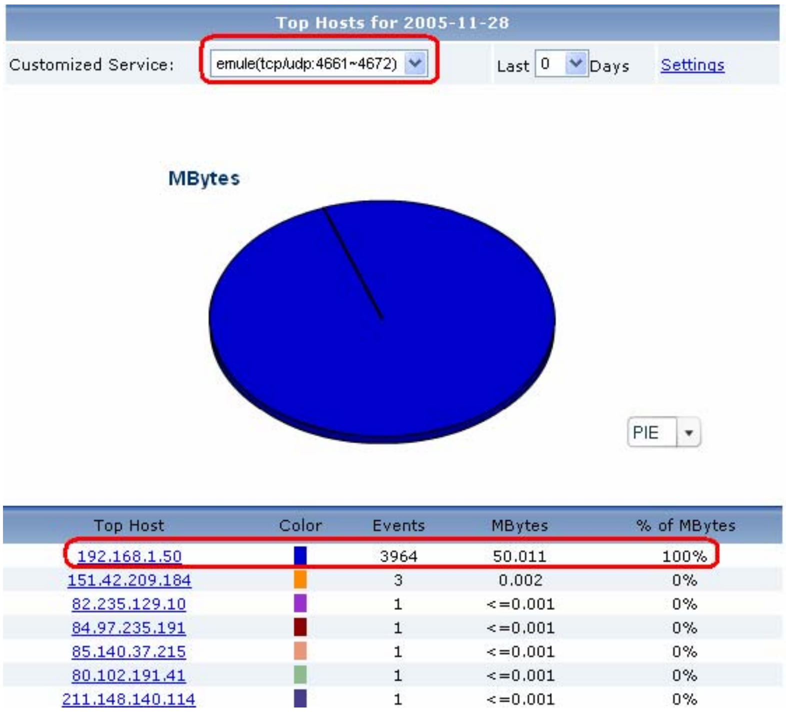
Name: emule

Port Range (1-65535): 4661 - 4672

Protocol: tcp/udp

Customized Service: emule(tcp/udp:4661~4672)

Excited result appears! User with the address 192.168.1.50 is using emule to download large files under **Traffic**>>**Customization**>>**Top Hosts.**

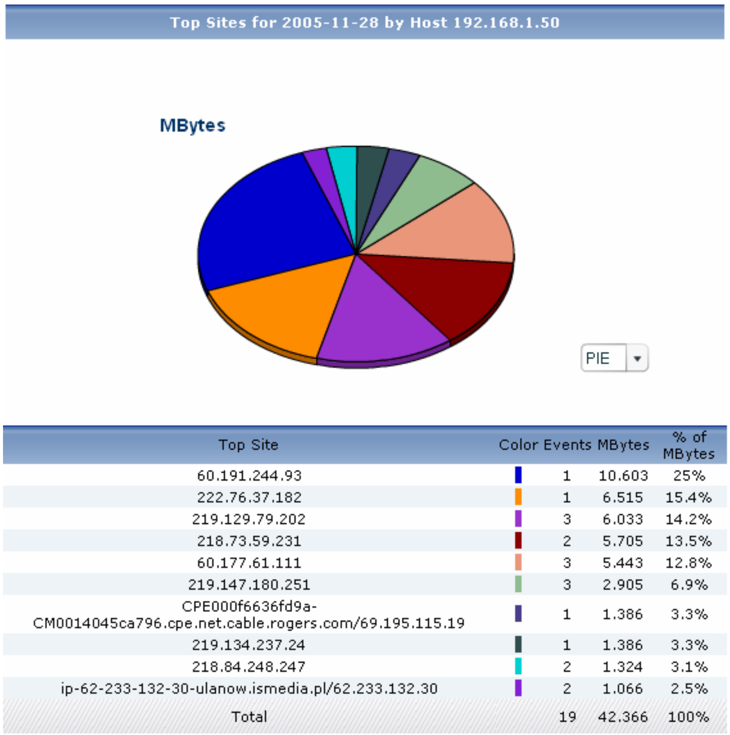


Top Hosts for 2005-11-28

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

Top Host	Color	Events	MBytes	% of MBytes
192.168.1.50	■	3964	50.011	100%
151.42.209.184	■	3	0.002	0%
82.235.129.10	■	1	<=0.001	0%
84.97.235.191	■	1	<=0.001	0%
85.140.37.215	■	1	<=0.001	0%
80.102.191.41	■	1	<=0.001	0%
211.148.140.114	■	1	<=0.001	0%

By entering the drill down link of 192.168.1.50, administrator goes to further check the web site the user is accessing. He also could get the web site IP address and its DNS. These are really some websites for customers to download the media material. Please see below result.

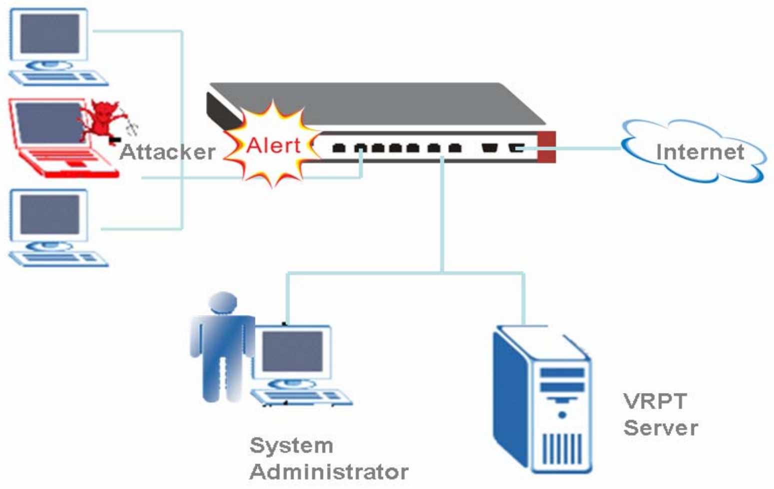


Top Sites for 2005-11-28 by Host 192.168.1.50

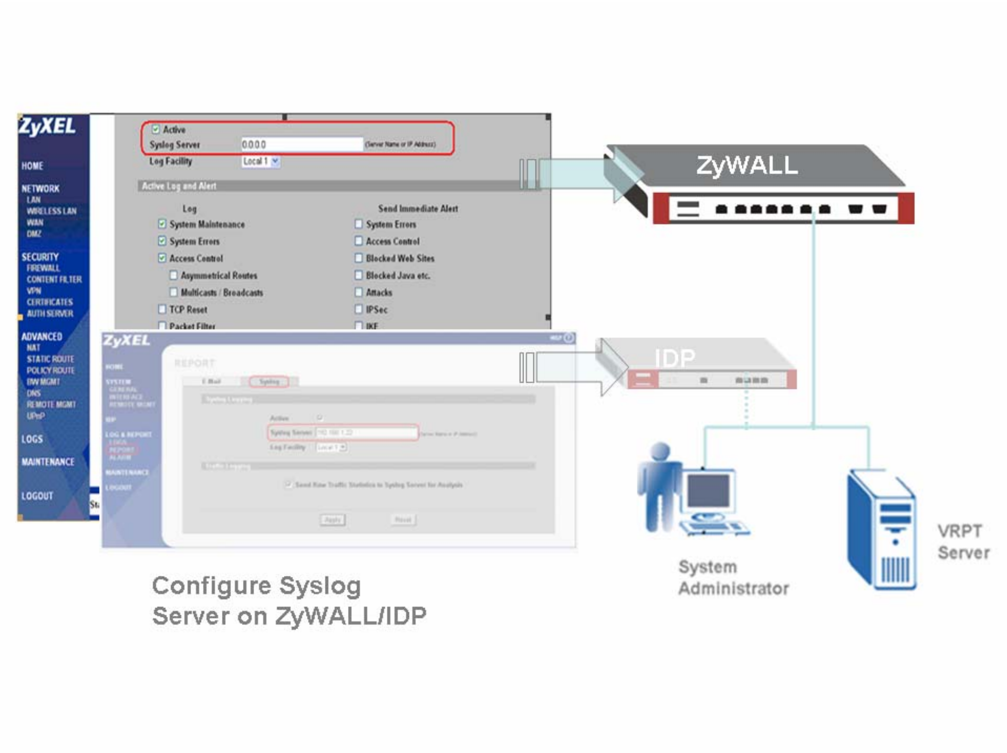
Top Site	Color	Events	MBytes	% of MBytes
60.191.244.93	■	1	10.603	25%
222.76.37.182	■	1	6.515	15.4%
219.129.79.202	■	3	6.033	14.2%
218.73.59.231	■	2	5.705	13.5%
60.177.61.111	■	3	5.443	12.8%
219.147.180.251	■	3	2.905	6.9%
CPE000f6636fd9a-CM0014045ca796.cpe.net.cable.rogers.com/69.195.115.19	■	1	1.386	3.3%
219.134.237.24	■	1	1.386	3.3%
218.84.248.247	■	2	1.324	3.1%
ip-62-233-132-30-ulanow.ismedia.pl/62.233.132.30	■	2	1.066	2.5%
Total		19	42.366	100%

How to check Intrusion Events for ZyXEL device?

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.



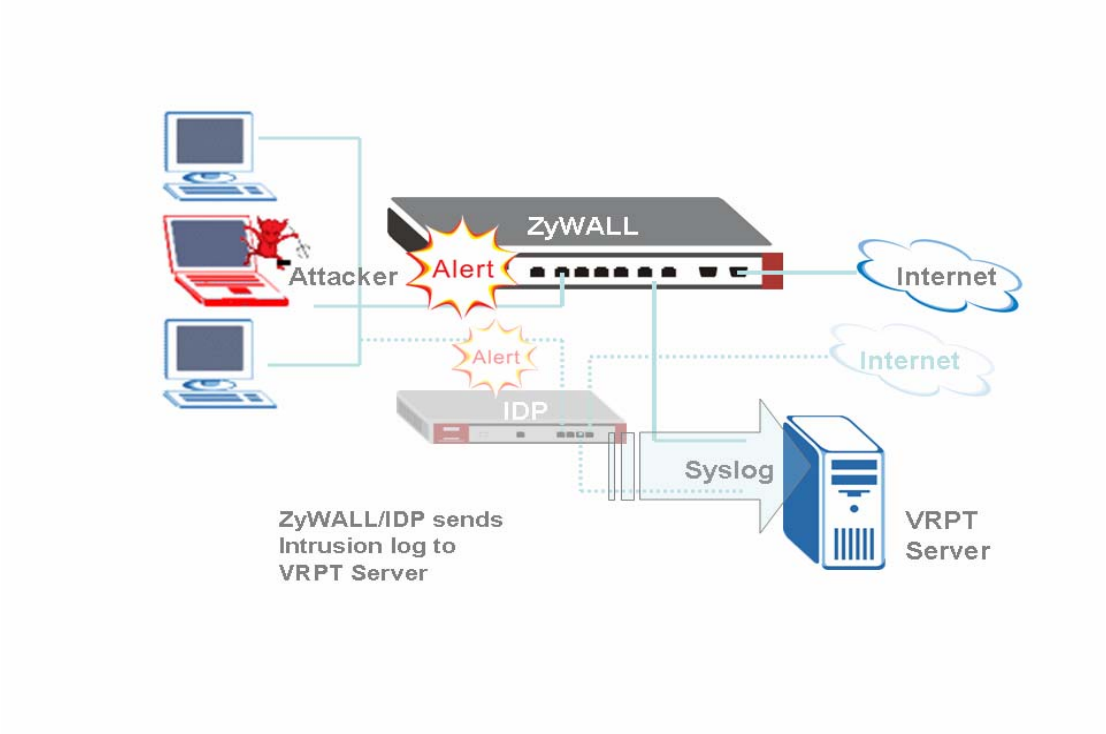
☑ Active
Syslog Server 0.0.0.0 (Server Name or IP Address)
Log Facility Local 1

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

Configure Syslog Server on ZyWALL/IDP

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

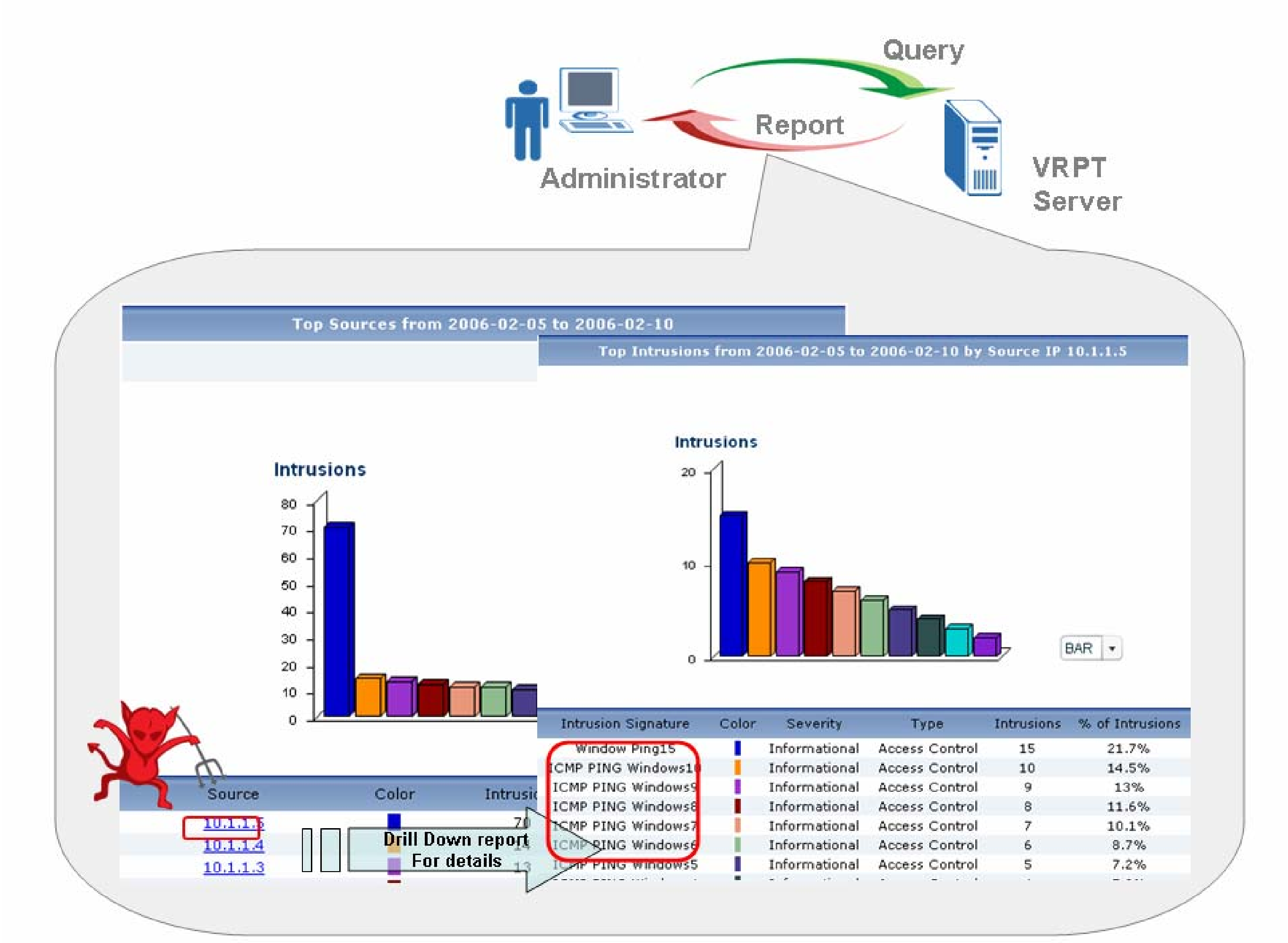


ZyWALL/IDP sends Intrusion log to VRPT Server

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.



Source	Color	Intrusi
10.1.1.5	■	70
10.1.1.4	■	14
10.1.1.3	■	13

Intrusion Signature	Color	Severity	Type	Intrusions	% of Intrusions
Window Ping15	■	Informational	Access Control	15	21.7%
ICMP PING Windows10	■	Informational	Access Control	10	14.5%
ICMP PING Windows9	■	Informational	Access Control	9	13%
ICMP PING Windows8	■	Informational	Access Control	8	11.6%
ICMP PING Windows7	■	Informational	Access Control	7	10.1%
ICMP PING Windows6	■	Informational	Access Control	6	8.7%
ICMP PING Windows5	■	Informational	Access Control	5	7.2%

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**

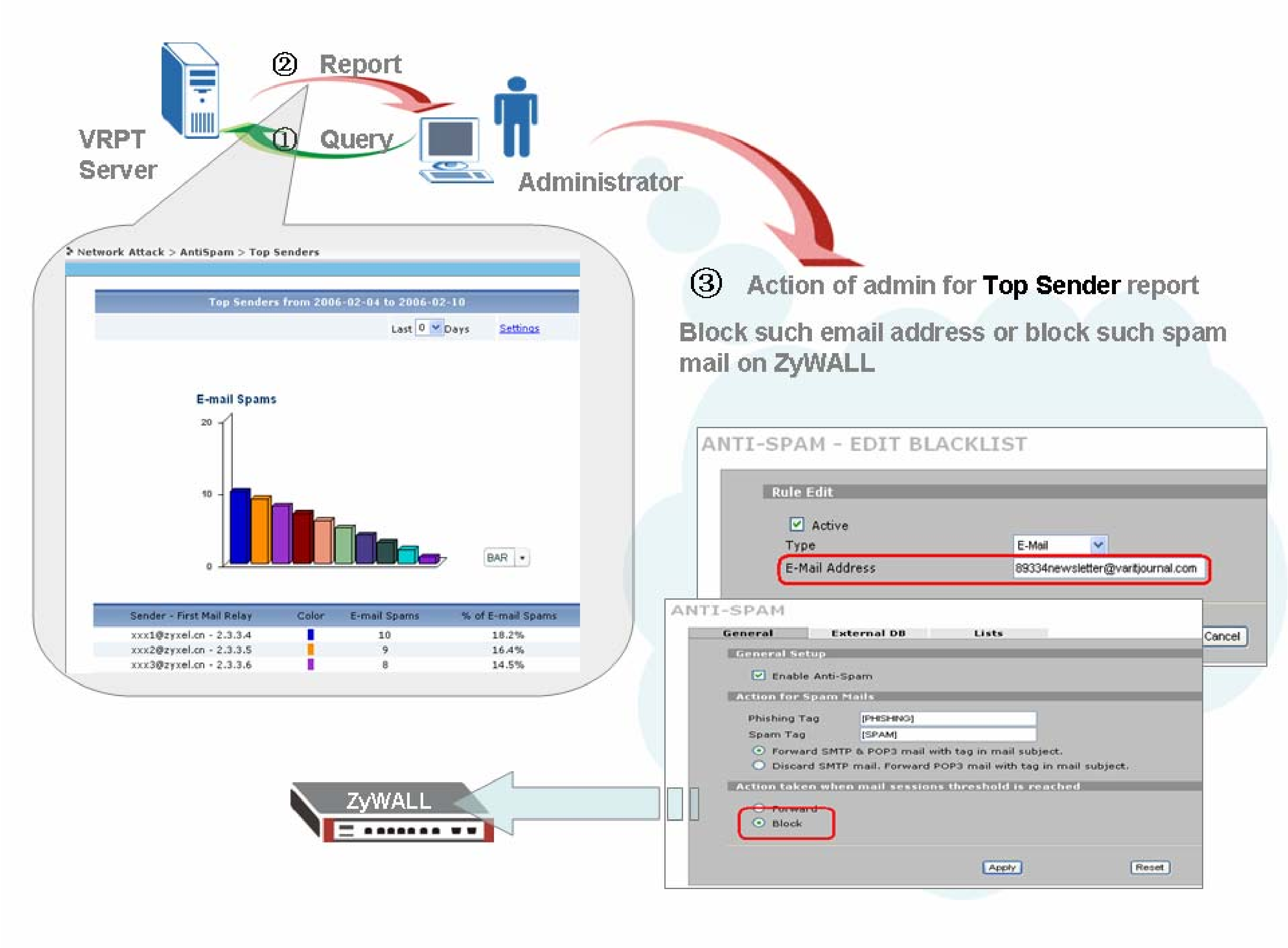
Emergency:	system is unusable
Alert	action must be taken immediately
Critical	critical conditions
Error	error conditions
Warning	warning conditions
Notice	normal but significant condition
Informational	informational messages
Debug	debug-level messages

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.

the Suggested Countermeasure for 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.



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

Block such email address or block such spam mail on ZyWALL

Network Attack > AntiSpam > Top Senders

Top Senders from 2006-02-04 to 2006-02-10

Last 0 Days Settings

Sender - First Mail Relay	Color	E-mail Spams	% of E-mail Spams
xxx1@zyxel.cn - 2.3.3.4	▮	10	18.2%
xxx2@zyxel.cn - 2.3.3.5	▮	9	16.4%
xxx3@zyxel.cn - 2.3.3.6	▮	8	14.5%

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.

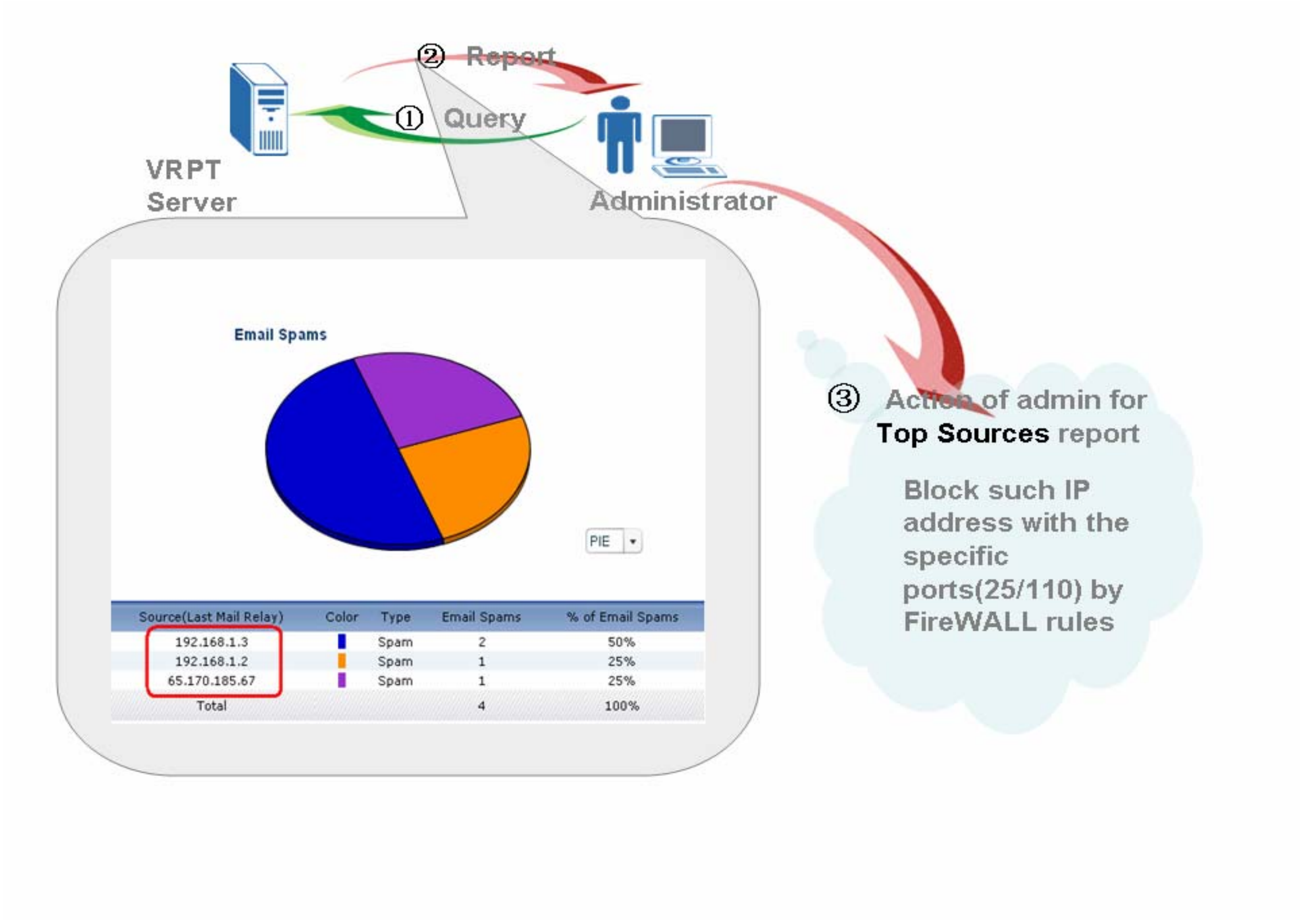
Action taken when mail sessions threshold is reached

○ Forward

● Block

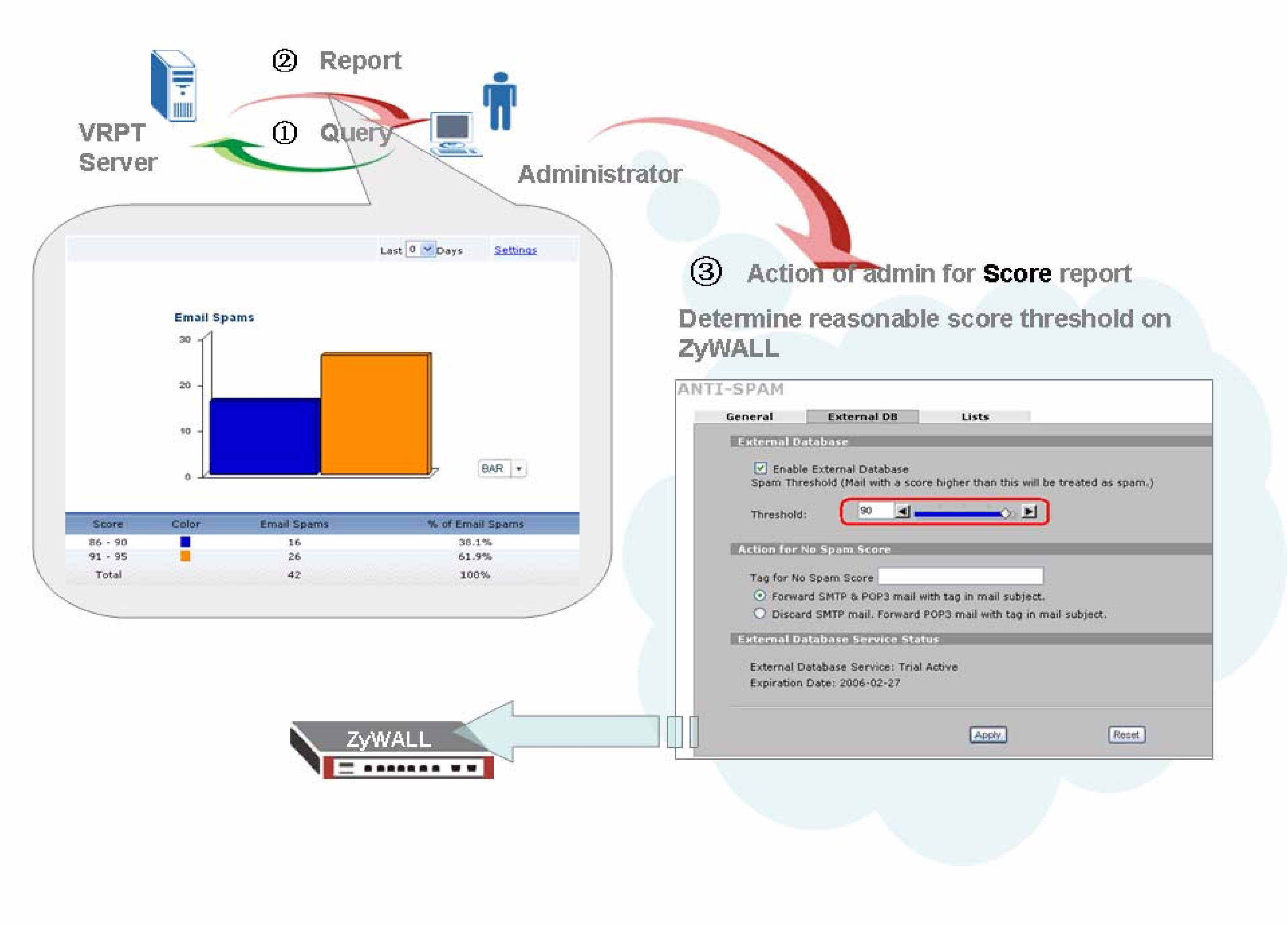
Apply Reset

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
Email Spams
PIE
③ Action of admin for Top Sources report
Block such IP address with the specific ports(25/110) by FireWALL rules

Source(Last Mail Relay)	Color	Type	Email Spams	% of Email Spams
192.168.1.3	🟦	Spam	2	50%
192.168.1.2	🟧	Spam	1	25%
65.170.185.67	🟪	Spam	1	25%
Total			4	100%

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.



Score	Color	Email Spams	% of Email Spams
86 - 90	🟦	16	38.1%
91 - 95	🟧	26	61.9%
Total		42	100%

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

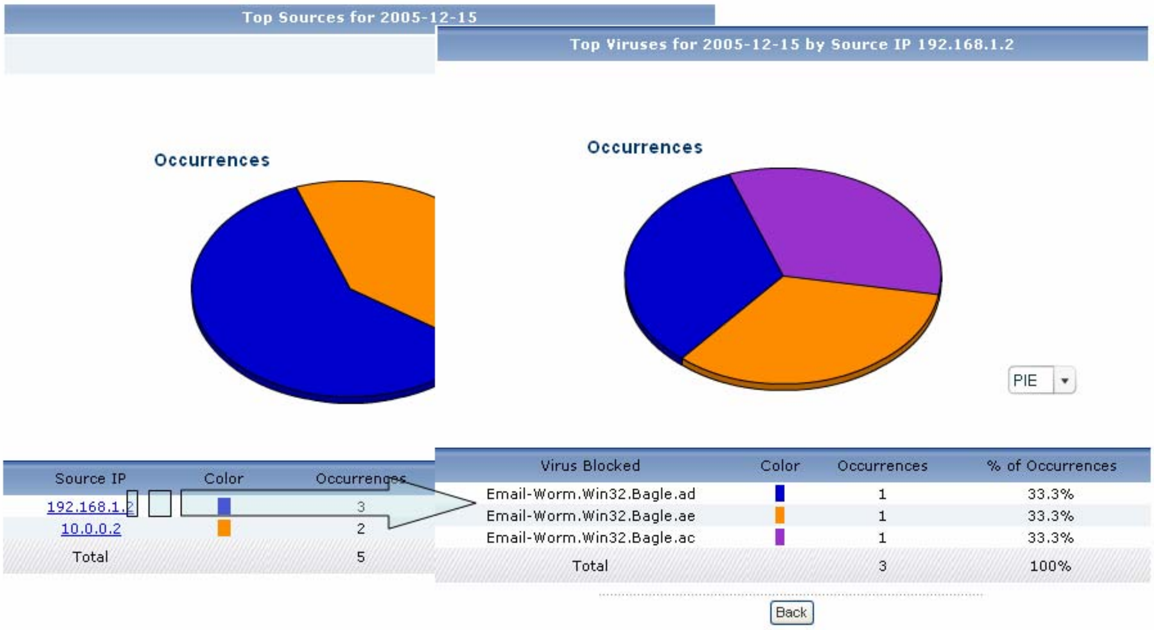
External Database Service: Trial Active
Expiration Date: 2006-02-27

Apply | Reset

the Suggested countermeasure for 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 192.168.1.2. User could find the detailed AV type by checking drill down report. According to the information, user could add firewall rule to block such IP address. But please still notice the firewall rule direction. User should add both LAN to WAN and WAN to LAN directions.



Top Sources for 2005-12-15

Top Viruses for 2005-12-15 by Source IP 192.168.1.2

Source IP	Color	Occurrences
192.168.1.2	🟦	3
10.0.0.2	🟧	2
Total		5

Virus Blocked	Color	Occurrences	% of Occurrences
Email-Worm.Win32.Bagle.ad	🟦	1	33.3%
Email-Worm.Win32.Bagle.ae	🟧	1	33.3%
Email-Worm.Win32.Bagle.ac	🟪	1	33.3%
Total		3	100%

All Logs and Critical Logs under View Logs

Log>>**Viewer** >>**All Logs** will show all the logs accepted by VRPT. It will need VRPT about 30 minutes to load these heavy data. Here 30 minutes means the interval between VRPT receives and shows such log under **Log**>>**Viewer**>>**All Logs**. In order to convenience user to check important logs in a short duration, VRPT supplies **Critical Logs** for checking. Every 1 minute Critical will refresh its logs. There are several log types are been defined by VRPT as critical logs. They are logs about Attack, TCP Reset, Access Control, PPP, IDP, Anti-Virus, Anti-Spam, System Maintenance and System Error.

The configuration for Critical log is in file with the name critical_log_criterion.properties. We strongly do **NOT** recommend user to change it.

Trouble Shooting

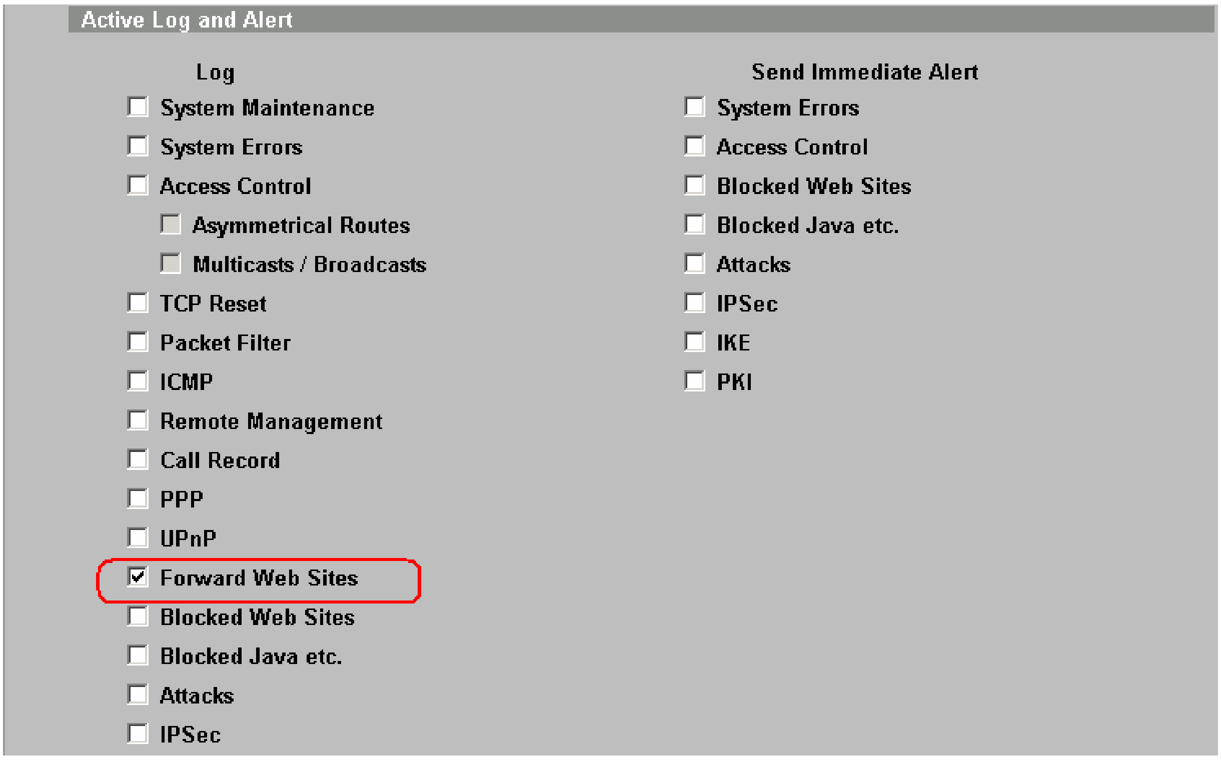
What to check if you can not access the GUI of VRPT Server?

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 change the Web server port when installing the VRPT, user 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 get the PIE chart, even no data in monitor?

1. Currently, ZyWALL firmware version 3.63 or newer supports traffic log.
2. Confirm the time settings on both sides are the same. The same time zone.
3. Go to ZyNOS SMT menu 24.3.2, enable the Syslog function and set the IP address. Save to

apply.

Why can’t I start up VRPT 2.3 after installing it?

1. If you want to start up VRPT 2.3, 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 VRPT2.3. And reproduce the problem.
   2.3. Send the log files in <vrpt_home>/vrpt/log folder to technical support person.

Why do VRPT 2.3 shutdown automatically without any reason?

1. Please check the number of devices that are managed by VRPT 2.3. 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?

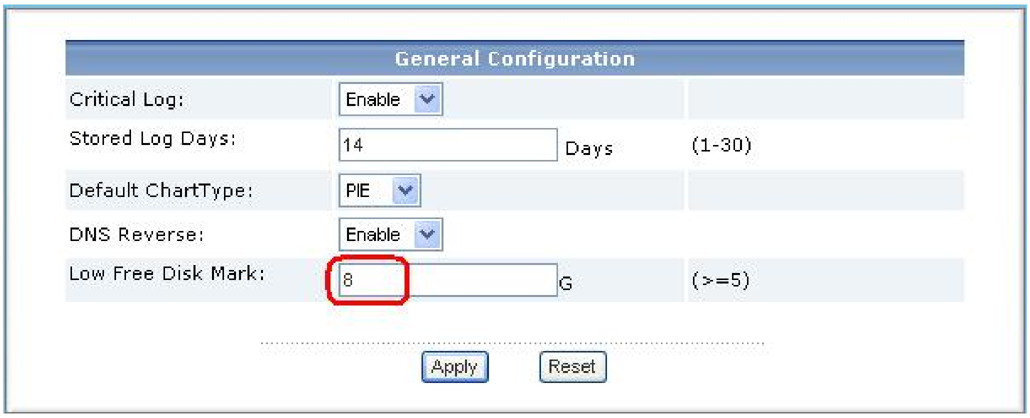
1. Please make sure if your account still in the **User List**. If Administrator delete your account, the page will come back to log in page automatically.
2. Session time out. The default time is 15 minutes.

Why there’s no new logs receive by VRPT 2.3?

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 VRPT2.3 home directory on server machine is no less than

600 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 600MB, VRPT will stop receiving log. After the free disk recover to an available value, VRPT will receiver logs again.

4. Please make sure the number of records in any database table is less than 15,000,000. If the number of the record in any table is large the specific value, VRPT will stop receiving new logs. And at the same time VRPT will send you alert email to remind you such thing and give you some hints to resolve the problem.



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 2.3 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 2.3 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 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: What is VRPT2.3 Feature and related Device Feature/Log?

VRPT feature	**Device Feature**
Monitor>>Bandwidth	All Traffic Logs
Monitor>>Service(WEB/FTP/MAIL/VPN)	Traffic Logs about Service
Monitor>>Attack/Intrution/AntiVirus/AntiSpam	Event logs about Attack/Intrution/AV/AS
Traffic>>Bandwidth>>Summary	Traffic Logs
Traffic>>Bandwidth>>Top Hosts	Top Ten Host Traffic Logs
Traffic>>Bandwidth>> Top Protocol	Top Ten Protocol Traffic Logs
Traffic>>WEB/FTP/Mail>>Top Sites	Top Ten Sites Traffic Log about Such Services, Mail service is about 'POP3/SMTP'
Traffic>>WEB>/FTP/Mail>Top Hosts	Top Ten Hosts Traffic Log about Such Services, Mail service is about 'POP3/SMTP'
Traffic>>Customization>>Top Destinations	Top Ten Destinations Traffic Log about Such Services
Traffic>>Customization>>Top Sources	Top Ten Sources Traffic Log about Such Services
Traffic>>VPN>>Top Peer Gateways	Top Ten remote Gateways of Traffic Log about VPN
Traffic>>VPN>>Top Hosts	Top Ten Host of Traffic Log about VPN
Network Attack>>Attack	Event Logs by Category is "Attack"

Network Attack>>Intrusion	Event Logs by Category is "Intrusion"
Network>>AntiVirus/AntiSpam	ZyWALL 5/35/70 with f/w 4.0 or later AntiVirus and AntiSpam event log
Security Policy	Web forward and Web Block Events Log
Event	Success or Fail Login Device, Events Log

Q5: Which types of devices are supported by VRPT 2.3?

IDP 10 with firmware 2.0
ZyWALL2/10W with firmware 3.62
ZyWALL5/ 35/70 with firmware 3.62,3.63, 3.64,3.65, 4.0 and later
ZyWALL P with firmware 1 3.64 and later
Prestige 662/652 with firmware 3.40

Q6: How many devices are supported by VRPT 2.3 ?

VRPT2.3 can manage 25 units (device) according performance.

Q7: Which components are included by VRPT 2.3?

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.

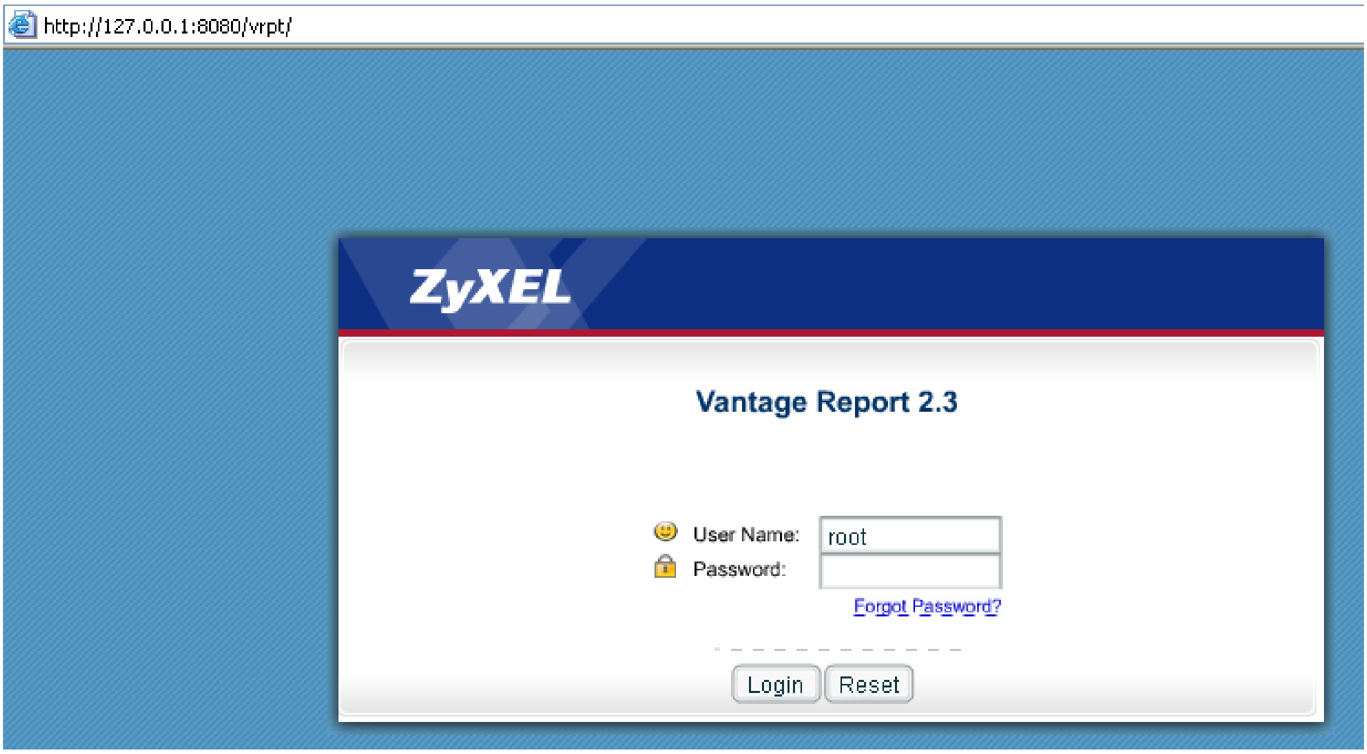
Q8: How to install VRPT 2.3 server on the PC?

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.

Q9: How to access VRPT 2.3 ?

After installing VRPT 2.3 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://127.0.0.1:8080/vrpt/

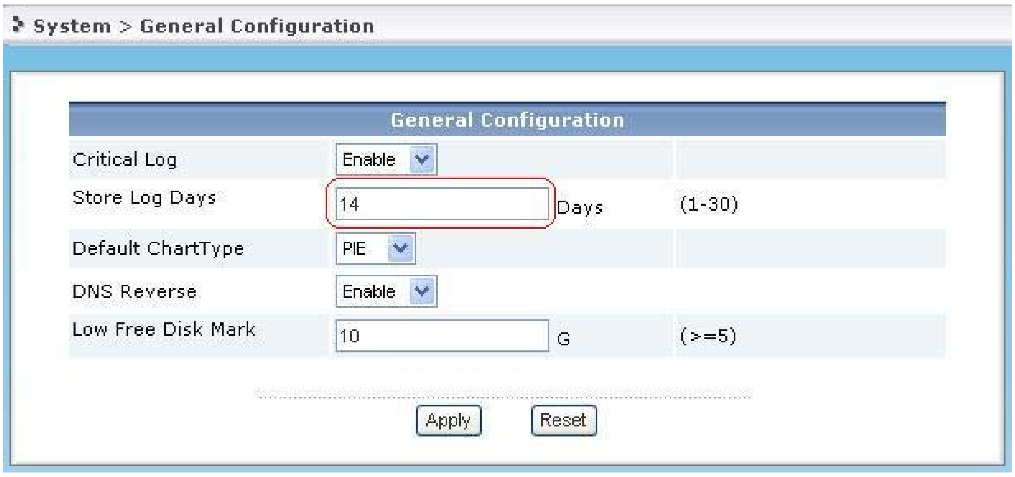
Vantage Report 2.3

User Name: root

Password:

Q10: How long will raw data (device logs) be stored in VRPT database?

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



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)

Old logs will be purged from system and saved as file with .csv postfix. These files will be located under VRPT installation directory and the default directory is C:\Program Files\ZyXEL\Vantage Report\ data\backup\db. The naming of file will be something like ftp-2005-10-25.csv. It denotes the log type which shown as ftp and the generating time. User can read them by Microsoft Excel or Ultra Edit.

Q11: How to check traffic logs report on VRPT 2.3 for ZyXEL xDSL product?

Unfortunately VRPT 2.3 can’t generate such report for ZyXEL xDSL product because such device could not send out traffic log currently.

Q12: How can I monitor VPN bandwidth or VPN Usage for ZyXEL xDSL product?

Under **Monitor>>Service>>VPN** or **VPN Usage** menu on VRPT 2.3, 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 2.3.

Q13: How can I check the Anti-Virus status for Prestige xDSL on VRPT 2.3?

Prestige xDSL devices can’t send out Anti-Virus event logs so VRPT 2.3 could not generate such report for xDSL Anti-Virus.

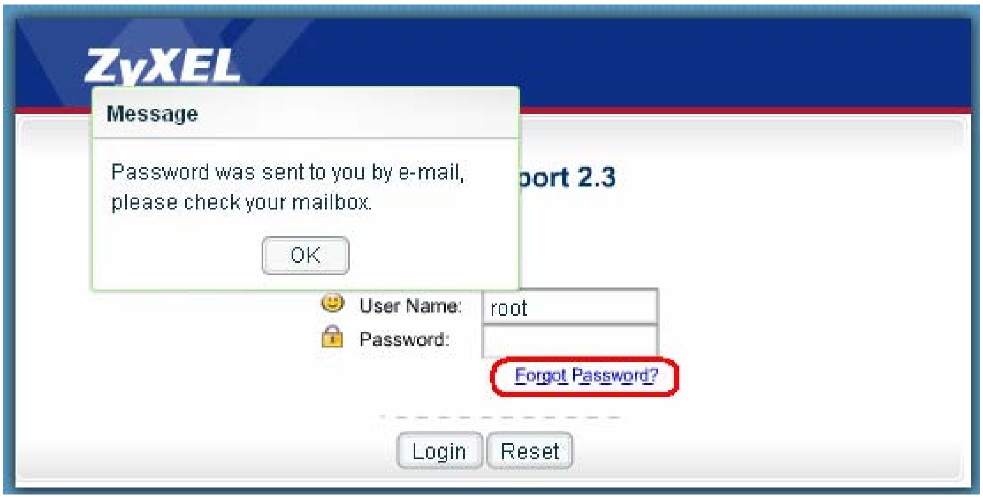
Q14: How can I check Intrusion/AntiVirus/AntiSpam report for ZyWALL series with f/w 3.63, 3.64 or 3.65?

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 2.3. It is normal without those UTM reports available when

ZyWALL are using those firmware versions.

Q15: 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.

Q16: Known Issue for Web Browser Supported by VRPT 2.3

The web browser supported by VRPT 2.3 are Microsoft IE 6.0 or later, Firefox 1.07 and later and Mozilla 1.7.2 and later. You could not login VRPT 2.3 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.

Q17: VRPT will be installed as a Window Service by default, is it right?

After you install VRPT 2.3 and restart your machine, VRPT will be started up. Under this circumstance it is normal for VRPT 2.3 to start up automatically because we install it as Windows service.

Q18: Log Time on VRPT 2.3

When VRPT 2.3 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.

Q19: Report Pattern for Schedule Reports

VRPT 2.3 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.

Q20: 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 2.3 User Guide. To get the source code covered under these licenses, please contact CSO team for Vantage Report Technical Support.

Q21: 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 2.3. 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.