

Vantage Report

Centralized Logging & Reporting Analyzer

Support Notes

Version 2.2

June. 2005



INDEX

FAQ	3
Product FAQ	3
What is Vantage Report (VRPT) ?	3
Which operating systems are supported by VRPT Server ?	3
Which reports are supported by VRPT ?	3
Which types of devices are by VRPT ?	3
How many devices are supported by VRPT ?	4
Which components are included by VRPT ?	4
How to install VRPT server on the PC ?	4
How to access VRPT ?	4
How long will raw data (device logs) be stored in VRPT database ?	5
Application Notes	6
General Application Notes	6
Adding device to device maintenance list of VRPT	6
How to forward device log to VRPT for analysis and report ?	7
How to enable traffic log feature on ZyWALL ?	9
VRPT Server Setup	10
Advanced Application Notes	12
Using Schedule Report	12
How to check bandwidth usage ?	14
How to check Intrusion events ?	15
Trouble Shooting	17
What to check if you can not access the GUI of VRPT Server?	17
Why can't I get the PIE chart, even no data in monitor?	17

FAQ

Product FAQ

What is Vantage Report (VRPT) ?

Vantage Report (VRPT), a web-based centralized reporting system for quickly and conveniently collecting and analyzing a distributed network, provides system administrator a simple and direct method of monitoring multiple ZyWALL Internet security and IDP appliances. VRPT 2.2 supports Bandwidth usage/Service/Web Filter/Attack/Intrusion/Authentication reports. Administrator can generate a report by online-query or schedule report daily/weekly.

Which operating systems are supported by VRPT Server ?

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

Which reports are supported by VRPT ?

VRPT can analyze and generate reports based on syslog from ZyWALL series and ZyWALL IDP10. There are two types of logs from devices: Event log and Traffic log. Event logs include many kinds of message which are related to the events on ZyWALL & IDP10. For example: DoS/DDoS attack, Web Access Block, Network Intrusion and so on. The other type of log, traffic log, is for statistic report about traffic passing through the device. When a session is initiated, ZyWALL, starts monitoring the traffic usage and send a log to VRPT when the session is terminated. Traffic log contains some information like source/destination/protocol/traffic load and so on. VRPT can generate Bandwidth/Service report based on the information.

Which types of devices are by VRPT ?

ZyWALL IDP10 with firmware 2.00

ZyWALL 2/10W with firmware 3.62

ZyWALL 5 with firmware 3.62 and later

ZyWALL 35/70 with firmware 3.63 and later

Therefore, no Bandwidth/Service report for ZyWALL 2/10W due to traffic log support.

How many devices are supported by VRPT ?

There is not limitation on the device number. However, we recommend less than 25 units according to estimated logs and performance.

Which components are included by VRPT ?

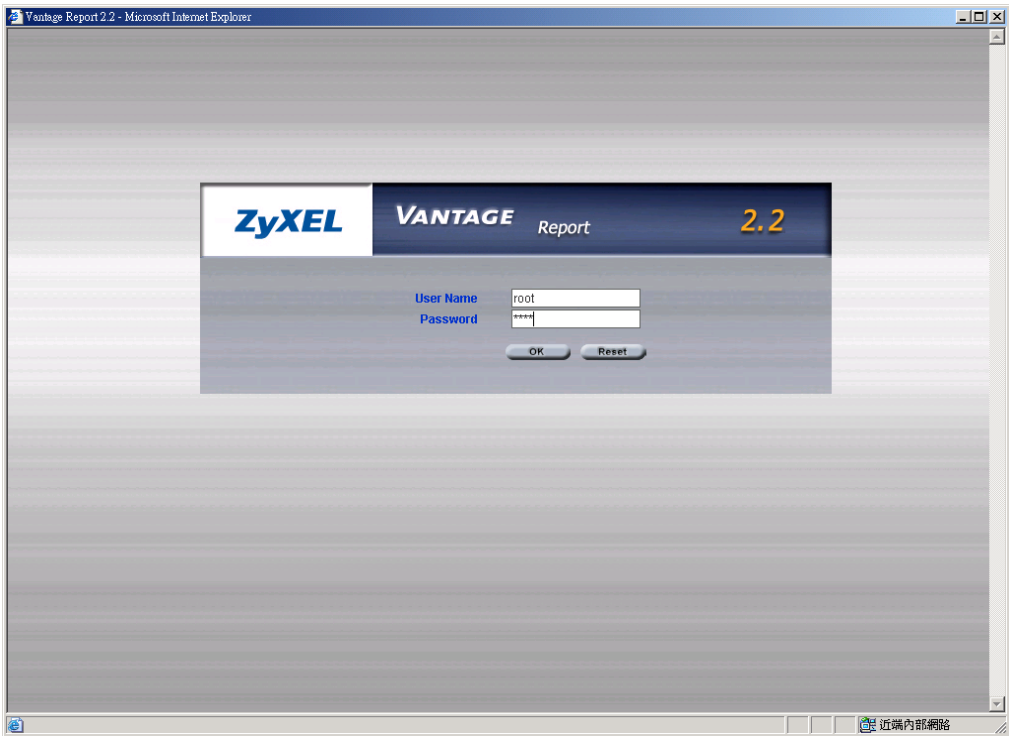
VRPT includes a Kiwi syslog receiver for collecting device log, MySQL database for storing the log for further analysis, an analysis/reporting module to generate report according to user' s request and schedule setting, tomcat web server to provide user-friendly interface.

How to install VRPT 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 KiWi syslog/MySQL/Tomcat on your computer. Make sure these applications are not running before installation.

How to access VRPT ?

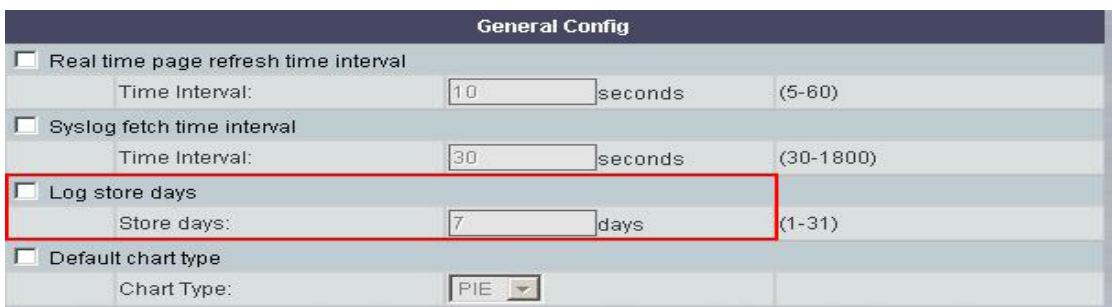
Once you install VRPT server, you can access VRPT by browser. Currently we only support IE 6.0 and later. Please type <http://<VRPT Server IP>:8080/vrpt> in the URL field. Press enter and a pop-up window will be prompt for login. If you can not see the window, please check your browser setting and make sure pop-up is not blocked.



Default username/password is root/root.

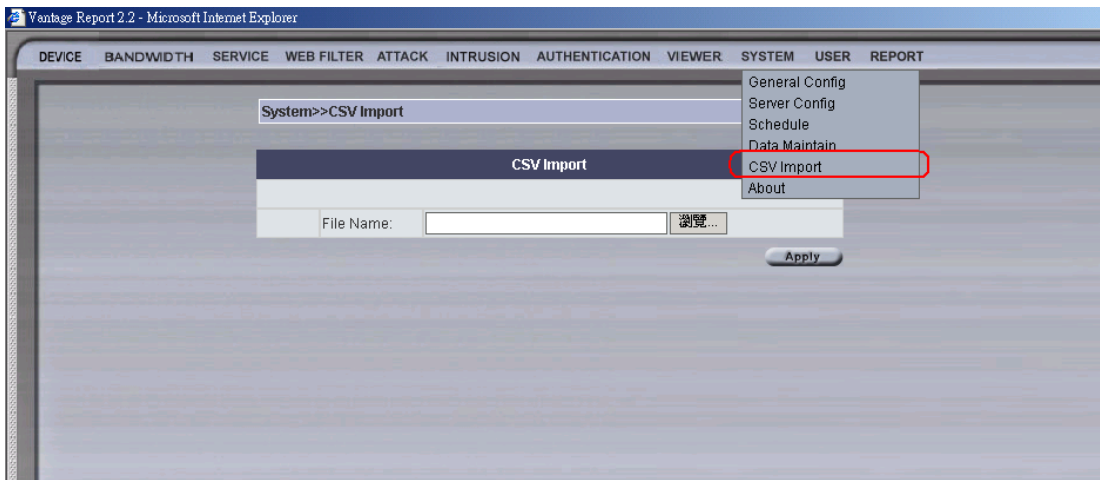
How long will raw data (device logs) be stored in VRPT database ?

Under System>>General Config, user can decide Log store days. VRPT will keep only those logs which are within the value.



Old logs will be purged from system and saved as CSV file. These CSV files will be located under <VRPT installation directory> (default C:\Program Files\ZyXEL\Vantage Report) \backup. User can read the CSV file by Microsoft Excel. The naming will be something like auto_20050317000003.csv. It means the log file is formed on 03/17/2005 at 00:00:03.

Raw data (CSV files) can be imported to VRPT database through System>>CSV Import.

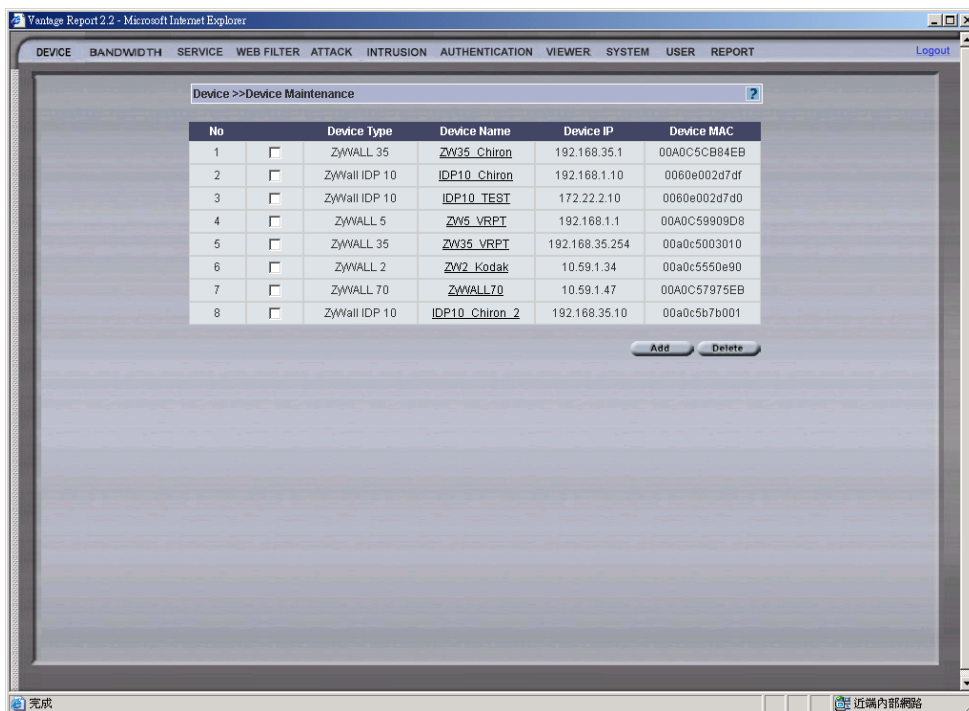


Application Notes

General Application Notes

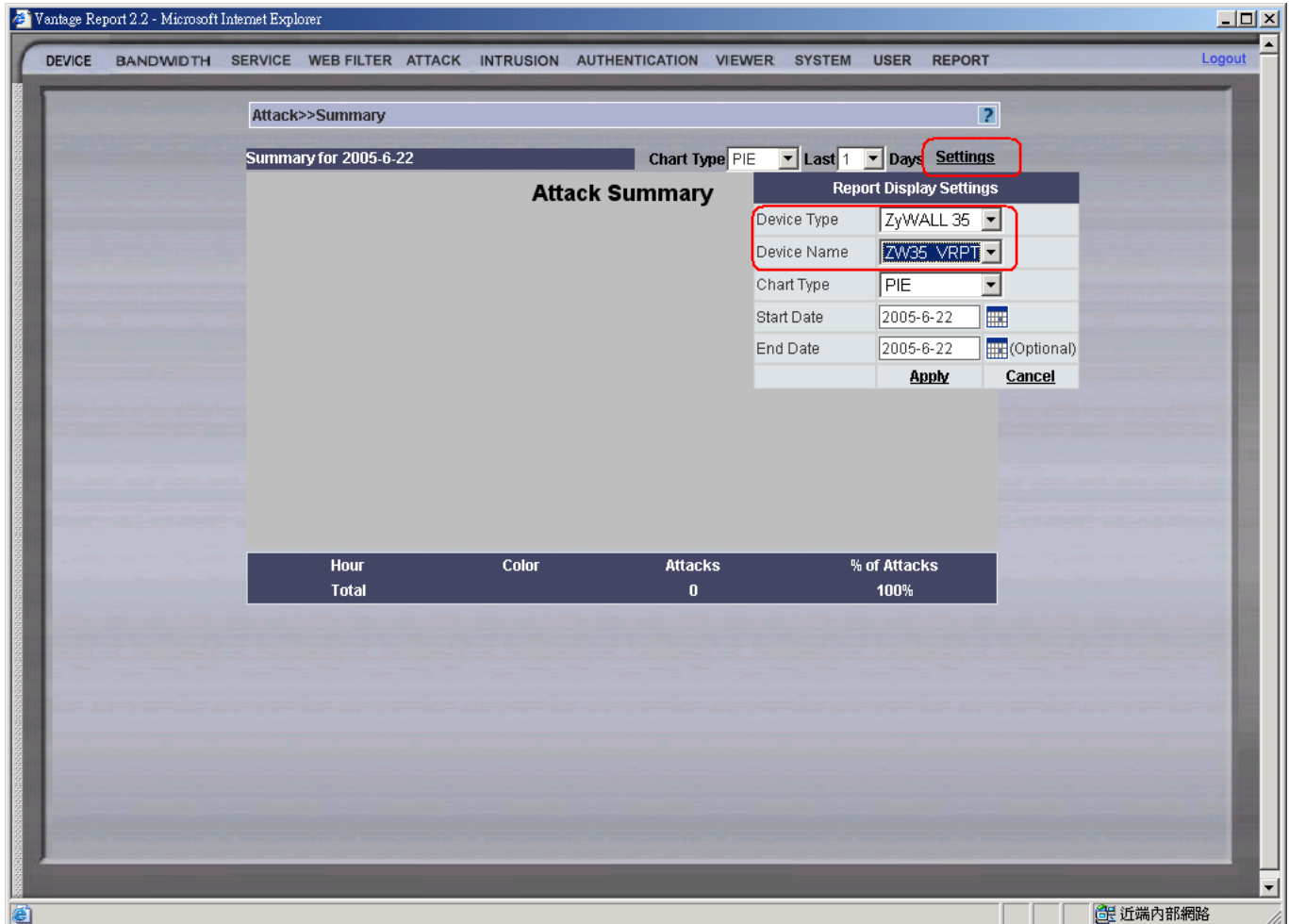
Adding device to device maintenance list of VRPT

VRPT 2.2 supports multiple devices. User can decide to generate reports for each single device or all devices. First of all, the devices must be added to device maintenance list of VRPT Device >> Device Maintenance.



Logs from these devices will be analyzed and imported to VRPT database. If the device doesn't exist in this list, its log will be dropped by VRPT. (User still can see the log on Kiwi).

If user needs to generate a report on a specific device, please click on “Settings” on the related report. User can select the device according to its Type and Name. Only those devices in device maintenance will be shown in the drop-down list. Note that the LAN MAC address must be correct. User can check the devID attribute in Kiwi syslog.

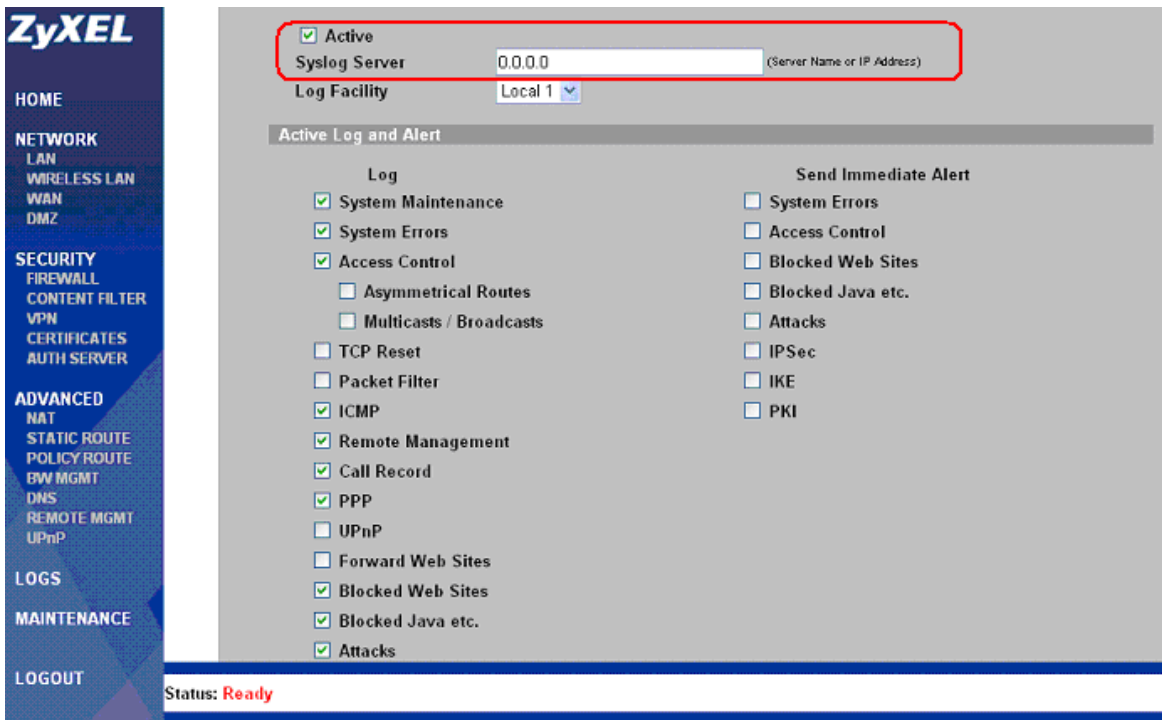


How to forward device log to VRPT for analysis and report ?

VRPT analyzes the syslogs from device. Therefore, user has to configure VRPT server as the Syslog server on device.

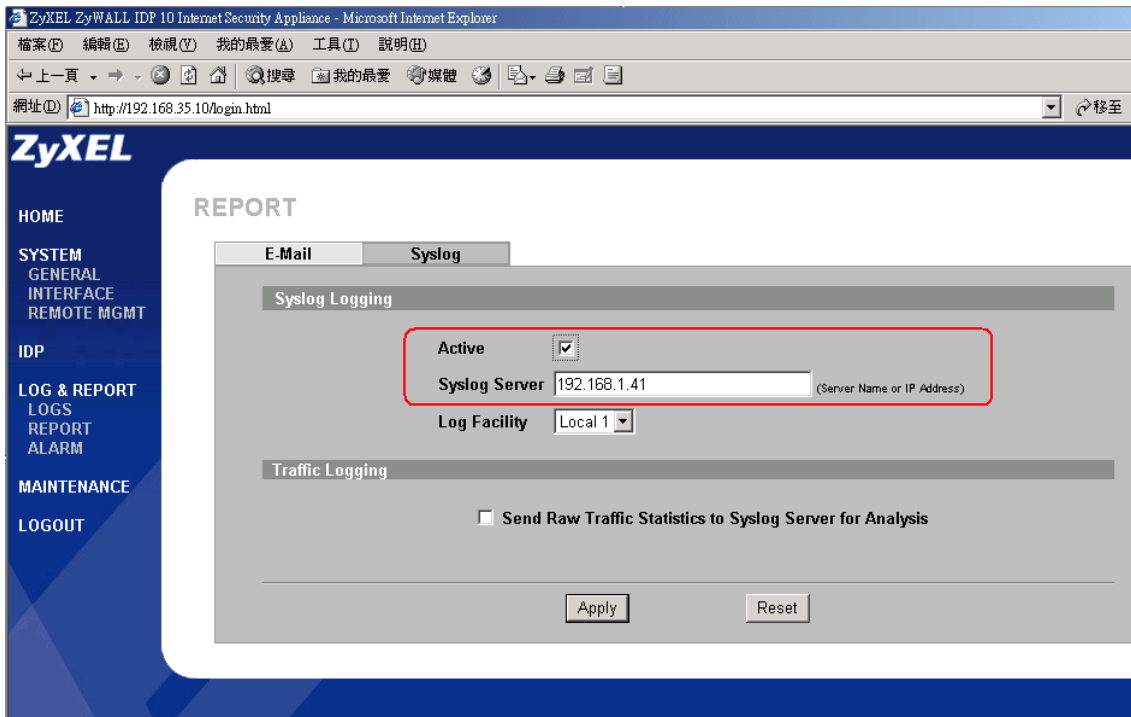
(1) From GUI (eWC)

For ZyWALL, enter LOGS>>Log Settings to enable the Syslog logging and key in the server name or the IP address of VRPT server.



The setting of Log Facility doesn't matter for VRPT report.

For IDP10, enter REPORT>>Syslog and key in the server name or the IP address of VRPT server.



(2) From SMT (Telnet/Console) menu24.3.2 (only for ZyWALL, not IDP10)

Menu 24.3.2 - System Maintenance - Syslog Logging

Syslog:

Active= Yes

Syslog Server IP Address= 172.25.21.77

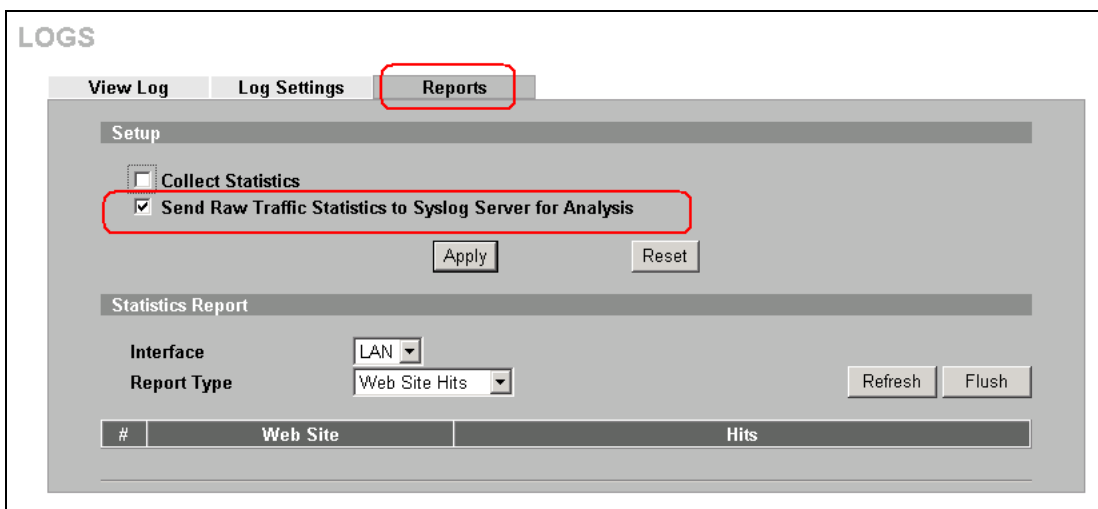
Log Facility= Local 1

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.

(1) From GUI (eWC)

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



(2) From SMT (Telnet/Console) menu 24.3.2

Enter its SMT Menu24.8 and type:

sys log load

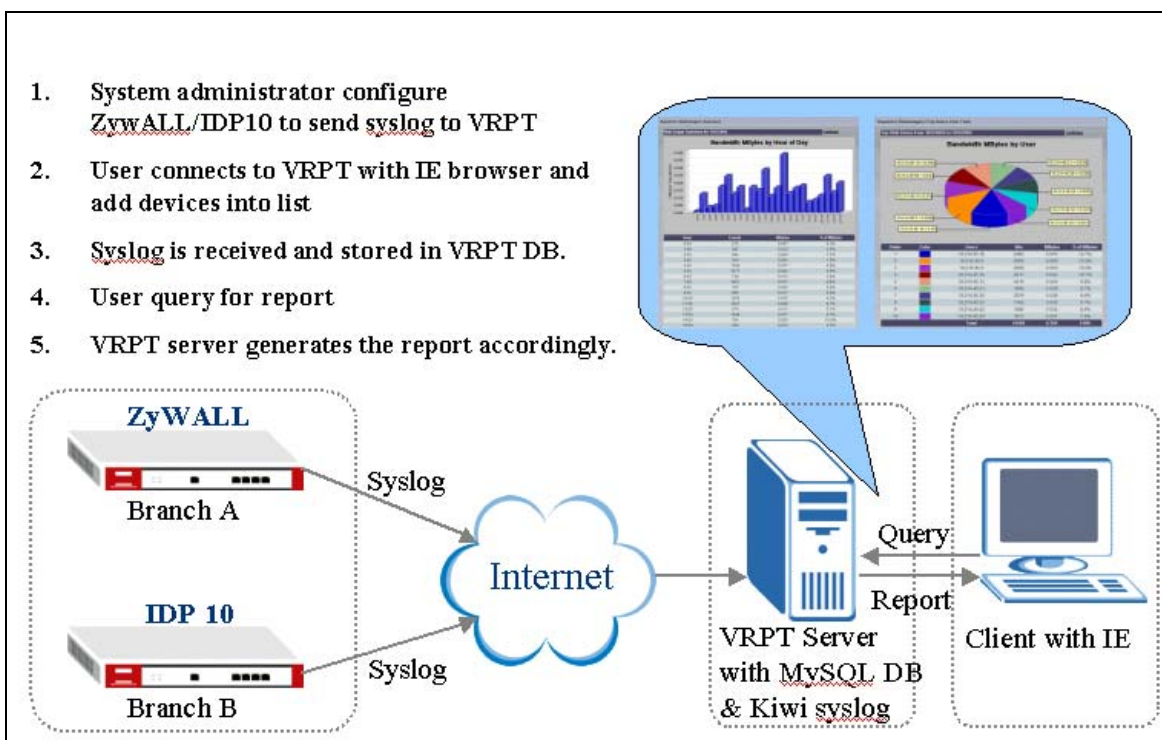
sys log cat traffic 1

sys log save

VRPT Server Setup

Setup VRPT could be very easy. Take following steps to get reports on VRPT.

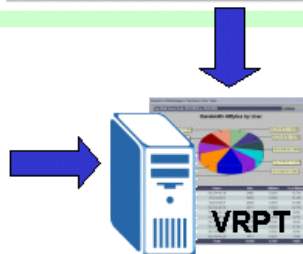
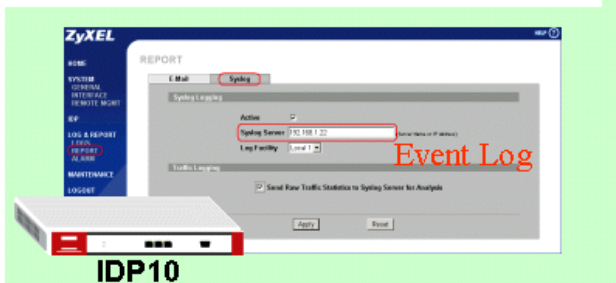
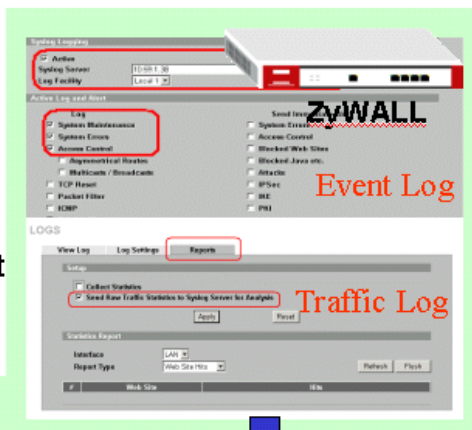
1. System administrator configure ZyWALL/IDP10 to send syslog to VRPT.
2. User connects to VRPT with IE browser and add devices into list.
3. Syslog is received and stored in VRPT DB.
4. User query for report
5. VRPT server generates the report accordingly.



configure ZyWALL/IDP10 to send syslog to VRPT.

Configure ZyWALL & IDP to send syslog to VRPT

- Activate Syslog function on ZyWALL/IDP10
- Configure VRPT as Syslog server
- Select required log category for reporting: ZyWALL supports Event log & Traffic Log; IDP10 support Event (Intrusion) log

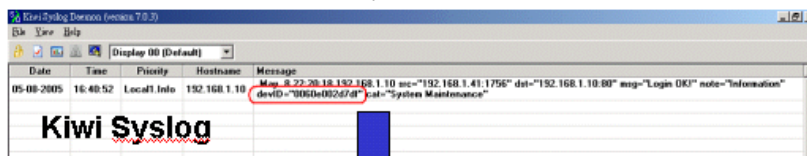


Add devices into list.

Add your devices to Device Maintenance List



Device



Kiwi Syslog



Import to DB for analysis

No	Device Type	Device Name	Device IP	Device MAC
1	ZyWALL 35	ZY35_Chiron	192.168.35.1	00A0C5CB84EB
2	ZyWall IDP 10	IDP10_Chiron	192.168.1.10	0060e002d7df
3	ZyWall IDP 10	IDP10_1	192.168.1.1	00A0C5111111
4	ZyWall IDP 10	IDP10_2	192.168.1.2	00A0C5222222

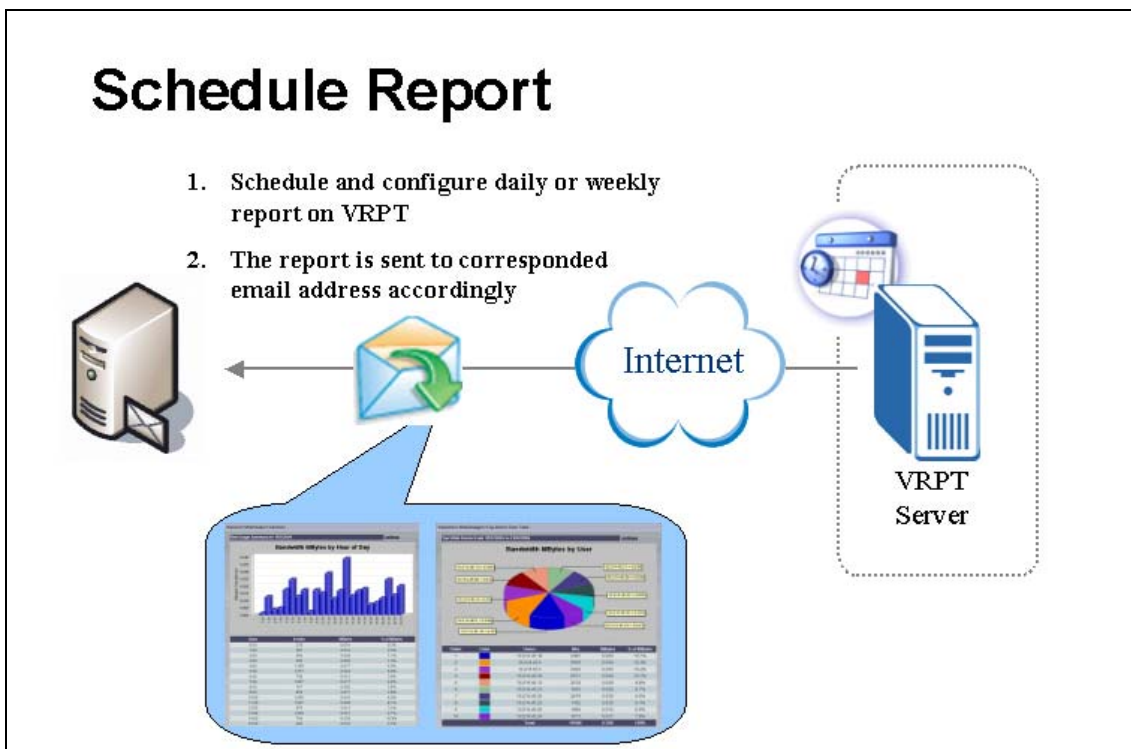
Drop

If device logs are received by Kiwi but not imported into VRPT database (not feasible in Log Monitor), check if the device is registered under device maintenance list. Note that the LAN MAC address must be correct. User can check the devID attribute in Kiwi syslog.

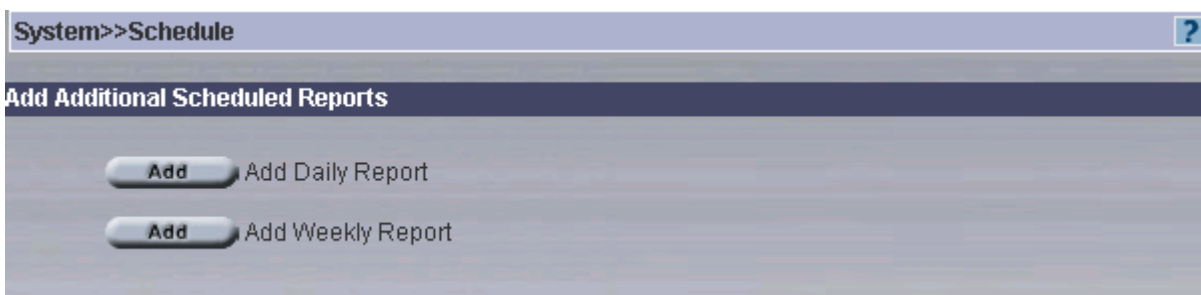
Advanced Application Notes

Using Schedule Report

VRPT provides support for emailing and archiving daily and weekly reports. User can create schedule report (daily/weekly). VRPT will generate the report and send to receiver automatically.



Go to System>>Schedule for adding schedule reports. There are two kinds of schedule reports (Daily & Weekly) available.



Take daily report for example. Add daily scheduled report”, e-mail address, subject, body. And you can

decide whether you want to save report to VRPT server. Suggest select “Include all data in a single report”, then in the mail you get in future, all statistics are included in a single PDF file, easy to read. Otherwise, each item in report list will form a PDF file.

Add Daily Scheduled Report

Destination email address (semicolon separated): john.yan@zyxel.cn Email subject: test for vantage

Email attached files Email body: can you see me ??

Save report to VRPT server

Save directory: /root/Vantage-CNM-2.1/ZYCNM_DEPLOY_BED/vrpt/schedule/ test-26/11/2004

Zip Emailed/archived reports into a single file

Include all data in a single report Time to submit: 23 : 59

Report List

<input checked="" type="checkbox"/> Bandwidth Summary	<input checked="" type="checkbox"/> Top Users of Bandwidth	<input checked="" type="checkbox"/> Service Summary
<input type="checkbox"/> Web Summary	<input type="checkbox"/> Top Sites of Web Usage	<input type="checkbox"/> Top Users of Web Usage
<input type="checkbox"/> Web Filter Summary	<input type="checkbox"/> Top Sites of Web Filter	<input type="checkbox"/> Top Users of Web Filter
<input type="checkbox"/> FTP Summary	<input type="checkbox"/> Top Users of FTP Usage	<input type="checkbox"/> Mail Summary
<input type="checkbox"/> Top Users of Mail Usage	<input type="checkbox"/> VPN Summary	<input type="checkbox"/> Top Users of VPN Usage
<input type="checkbox"/> Attack Summary	<input checked="" type="checkbox"/> Attack by Category	<input type="checkbox"/> Attack by Source
<input type="checkbox"/> Device Errors	<input type="checkbox"/> Successful Login	<input type="checkbox"/> Failed Login

If you want to add a daily report, do not fill in 1 day for log storing days.

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 file is the day before. Attention, here now, today is 2004-11-26 , but as you’ve seen in VRPT, it is 2004-11-25.

If you want the current statistics, you could go to “report>>one day report”, choose the date and apply. Or go to “Report>> One day report” to report the statistics of that day. Then you’ll get the report of that day till that moment. Click “Submit Now” and the report will be generated and forwarded immediately.

Add Additional Scheduled Reports


Add Daily Report

Add Weekly Report

Summary of Scheduled Reports

 Submit the report now, will not affect future scheduled reports

No.	To Email Address	E-Mail Subject	Schedule
1	<input checked="" type="checkbox"/> john.yan@zyxel.cn	test for vantage	Daily

From: john
To: John Yan - 严俊
Cc:
Subject: test for vantage
Attachments:  Bandwidth Summary etc_161311.pdf (151 KB)

can you see me ??

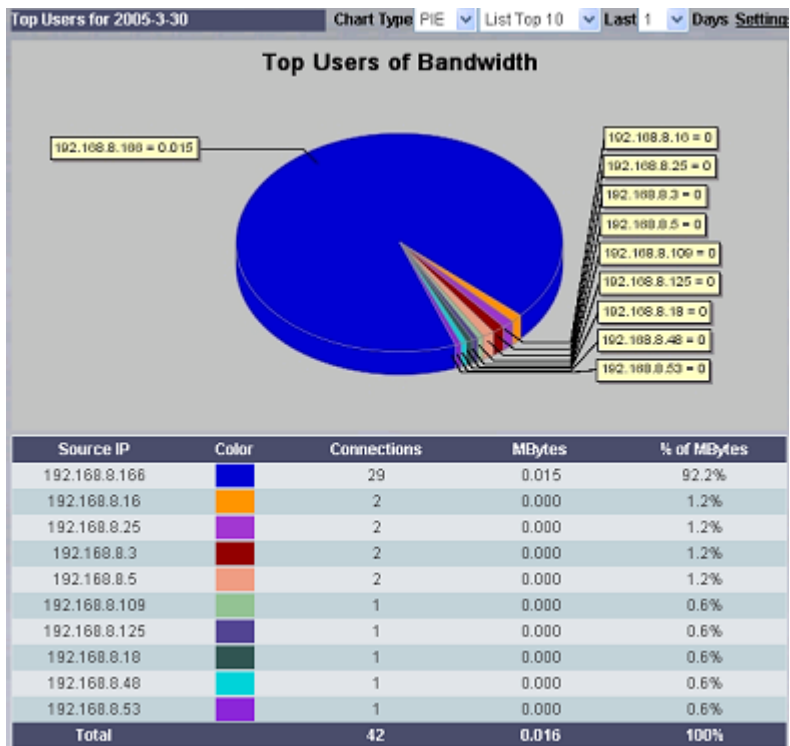
Here, the title “From” is just the settings in “System>>server config”, Mail Sender.

SMTP Server

IP Address Or Domain Name:	mail.zyxel.cn
User Name:	John.Yan@zyxel.cn
Password:	*****
Send Email:	John

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. Then the administrator will check the Bandwidth>>Top users of the VRPT, he finds that

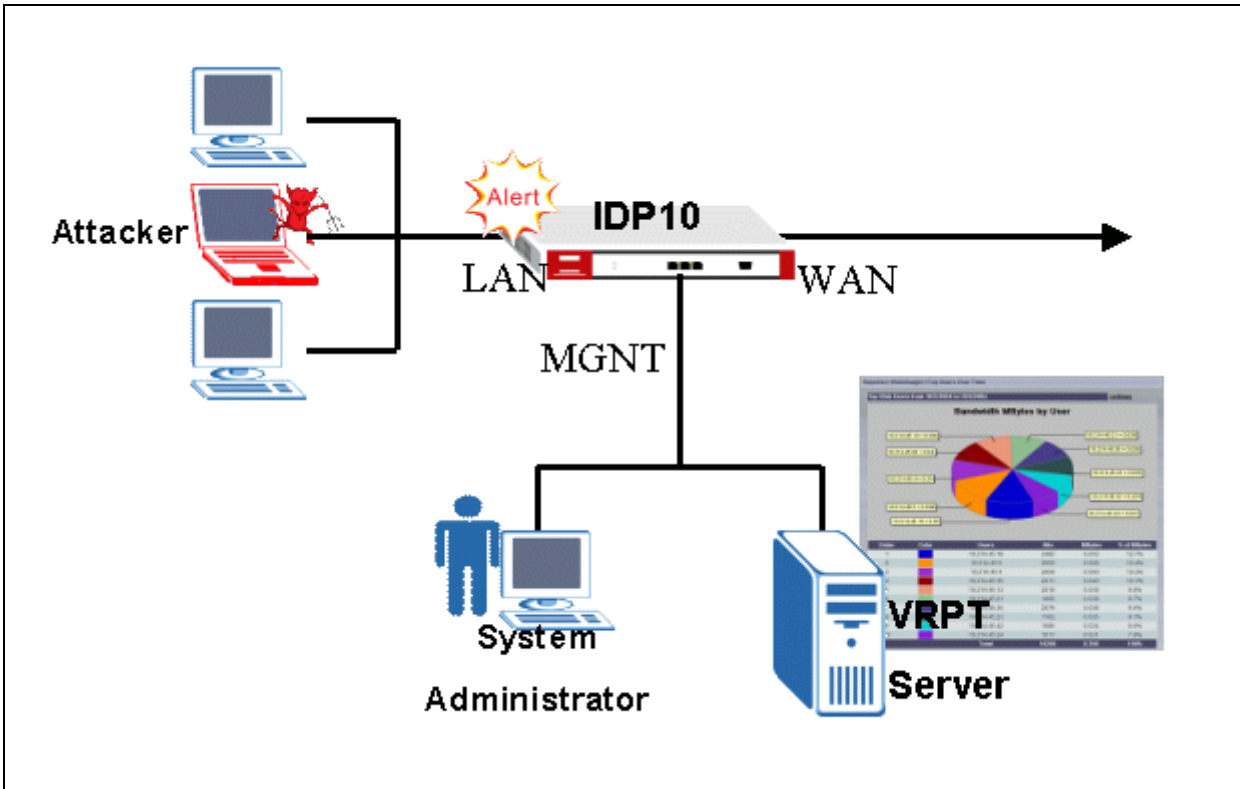


It shows the users 192.168.8.166 uses lots of the bandwidth of the company. He is downloading some big file through BT. It will occupy most of the network resource of the company, which may decrease the

productivity.

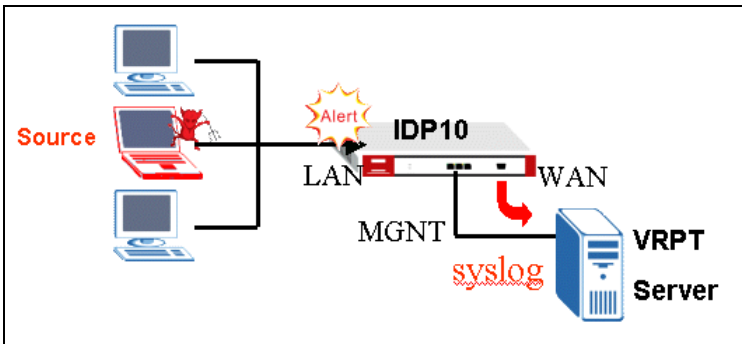
How to check Intrusion events ?

VRPT supports intrusion report based on the log from ZyWALL IDP10. It provides reports based on Intrusion Source (attacker), Destination (victim), type, signature and severity. Following is an example to illustrate that an internal host is conducting network treat (e.g. infected by Trojan) and passing through IDP10.



Step 1. Configure VRPT Server as the Syslog Server (Report>>Syslog) of IDP10

Step 2. When IDP10 detects intrusion events, it will generate syslog and forward to VRPT Server.



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

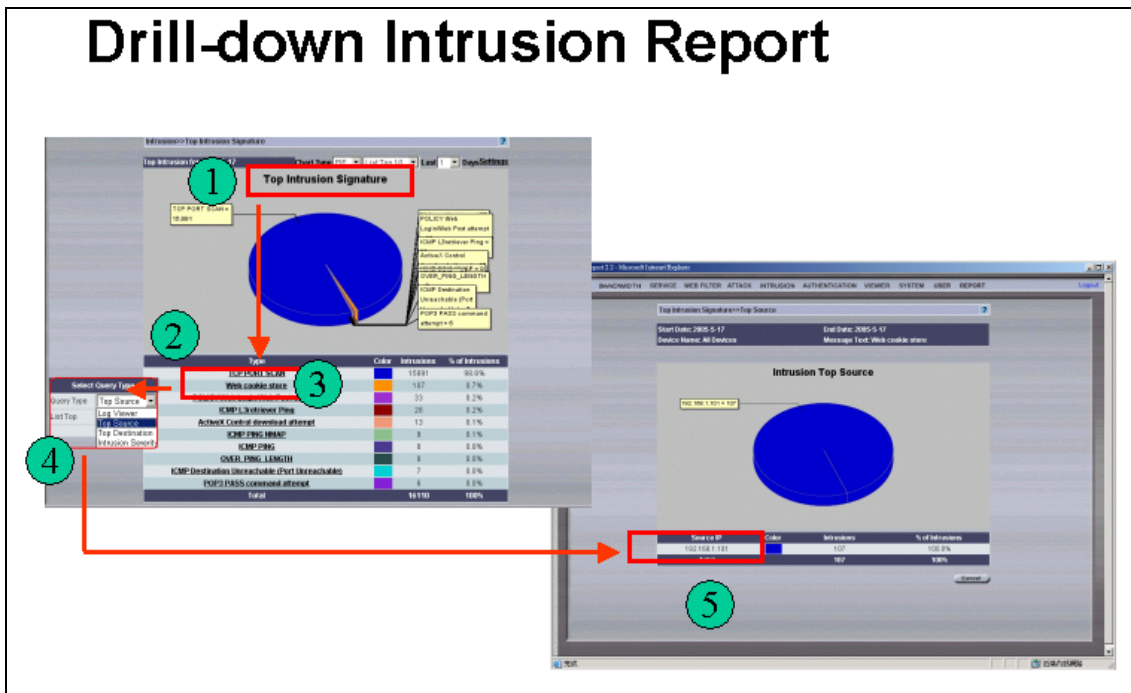
System Administrator Query VRPT Server
Report

Source IP	Count	Intrusions	% of Intrusions
192.168.1.101	107	107	100.0%
Total	107	107	100%

Signature	Count	Intrusions	% of Intrusions
TCP Flood (SCAN)	107	107	10.0%
Web Link Abuse	107	107	3.7%
SQLmap Web Login (Web Post) attempt	13	13	2.7%
SQLmap Database Query	13	13	2.7%
Armitage Control (Database) attempt	13	13	2.1%
SQLmap (MS-SQL)	8	8	2.1%
SQLmap (MySQL)	8	8	2.0%
SQLmap (Oracle) attempt	7	7	2.0%
SQLmap (Microsoft) attempt	6	6	2.0%
Total	1410	1410	100%

User can find drill-down report for Intrusion. Drill-down report allows user to view the intrusion event by querying Intrusion signature hit by attacker.

Drill-down Intrusion Report



For example:

1. Query by Top Intrusion Signature (Intrusion>>Top Intrusion Signature)
2. VRPT will generate top 10 Intrusion type according to Intrusion Signature
3. Select the specific type in the table, an advanced query can be applied to the selected intrusion event
4. The advanced query can be Log Viewer/Top Source/Top Destination
5. If top source is selected, the next window will show you the hosts who conducts most of the intrusion type.

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 Port 514 is forwarded for the VRPT Server.

Why can't I get the PIE chart, even no data in monitor?

- a. Currently, F/W 3.63(WM.0) or newer supports traffic log.
- b. Confirm the time settings on both sides are the same. The same time zone.
- c. Go to ZyNOS menu 24.3.2, enable the syslog function and set the IP address. Save and quit.