

# *Vantage CNM*

---

*Centralized Network Management*

## Support Note

Version 2.3

11/2006



# Contents

<b>Contents</b> .....	1
1 Application Notes.....	5
1.1 Firmware & Model list Support .....	5
1.2 Installation Scenario/Deployment Suggestion .....	7
1.2.1 Single Server for CNM & VRPT .....	8
1.2.2 install CNM and VRPT on Different ServerInstalling .....	12
1.2.3 Installing Multiple VRPT Servers .....	15
1.3 Upgrade (Migration) from existing CNM instrallation .....	19
1.3.1 From CNM 2.2 and CNM 2.3 Lite .....	19
1.3.2 From CNM 2.0/2.1 .....	23
1.3.2.1 CNM Server Installation.....	25
1.3.2.2 VRPT Server Installation .....	25
1.3.2.3 CNM Activation.....	25
1.4 A scenario for Vantage application .....	29
1.5 Domain Control of devices & accounts.....	31
1.5.1 Account Setup.....	32
1.5.2 Folder Setup.....	32
1.5.3 Device Registration .....	33
1.5.4 Enable/Setup Vantage Function on ZyXEL Devices.....	34
1.6 UTM Management .....	35
1.6.1 Centralized License Management .....	35
1.6.1.1 Device Registration & License Activation/Upgrade .....	35
1.6.1.2 License Monitor to view license status of all devices .....	37
1.6.1.3 License Expire Notification .....	38
1.6.2 Policy Enforcement.....	38
1.6.2.1 Configure UTM policy .....	38
1.6.2.2 Apply group configuration of UTM policy .....	42
1.6.2.3 Signature backup and restore for these ZyXEL devices.....	45
1.6.3 Read UTM report for all the devices in the network .....	47
1.6.3.1 Set the VRPT server for all the devices in the Network.....	47
1.6.3.2 Viewing UTM Report .....	47
1.6.4 Alarm Monitoring and Alerting.....	49
1.6.4.1 Alarm Monitor .....	50
1.6.4.2 Alarm Search.....	51
1.7 VPN Management.....	54
1.7.1 Creating VPN tunnel by VPN Editor (One-click VPN) .....	54
1.7.1.1 Use delete button to delete a tunnel .....	57
1.7.1.2 Use Force button to delete a tunnel.....	58
1.7.2 Monitor Status of VPN Tunnel.....	59

1.8	Device Maintenance .....	60
1.8.1	Firmware Management and upgrade.....	60
1.8.1.1	Firmware Management.....	60
1.8.1.2	Group Firmware Upgrade Process .....	61
1.8.1.3	Schedule Firmware Upgrade .....	62
1.8.1.4	Firmware Upgrade Report .....	63
1.8.2	Configuration file backup and restore .....	64
1.8.2.1	Backup and Restore .....	64
1.8.2.2	Group Configuration Backup .....	66
1.9	Real-time Monitoring, Alerting and Comprehensive Graphic Reporting	67
1.9.1	Monitoring (Device Online/Offline, Device Alarm) .....	67
1.9.1.1	Device Online/Offline.....	67
1.9.1.2	Device Alarm .....	68
1.9.2	Alerting (Email Notification) .....	69
1.9.3	Reporting (Traffic Report / Network Attack Report / UTM Report) .....	71
1.9.3.1	Setting VRPT server for managed device.....	71
1.9.3.2	Viewing report of managed devices.....	73
1.9.3.3	Configuring Schedule Report.....	85
2	FAQ .....	89
2.1	Where to download CNM software and patches?.....	89
2.2	How many types of license does ZyXEL offer?.....	89
2.3	What OS does Vantage CNM server support? .....	89
2.4	Will Vantage CNM support Microsoft Vista? .....	89
2.5	What browser does Vantage CNM server support?.....	89
2.6	Does Vantage CNM support IE 7.0?.....	89
2.7	What device and f/w version is supported by Vantage CNM 2.3? .....	89
2.8	What is the max number of devices that Vantage CNM 2.3 supports? .	92
2.9	What is OTV (Object Tree View), Content Screen ...etc? .....	92
2.10	Why can't I get complete OTV (Object Tree View)?.....	92
2.11	When I login to Vantage, I get this error message "HTTP Status 500 - No Context configured to process this request".....	92
2.12	My Internet Explorer (IE) does not trust the Certificate from Vantage server, should I trust it?.....	93
2.13	How can I skip the warning message of Certificate when I login the CNM? .....	93
2.14	When create an administrator in SYSTEM>>Administrators, what's the difference between Name and UID? .....	95
2.15	When a SUPER user changes the NORMAL USER's profile, the access permission of normal user should be changed. But what should be done to make the change effective?.....	96

2.16 Which MAC address should I input when register a device? .....	96
2.17 What should I do if I want to register hundreds of devices at one time? .....	96
2.18 Where can I get examples of the XML files? .....	96
2.19 What's the difference between System>>Log and Monitor>>Alarm?....	96
2.20 Why I can not receive the Alert/Alarm mails? .....	96
2.21 What should I do if I configure something on device but would like to synchronize the configuration with settings on Vantage? .....	98
2.22 If my Vantage server is behind a NAT/Firewall router, and I would like to allow outsiders to connect Vantage server's management interface from Internet. What should I do?.....	98
2.23 On each device, we should enter Vantage Server's IP address as the manager IP, but how many management IP can each device have?.....	98
2.24 When accessing Vantage Server by Internet Explorer, why does my web browser shut down without any caution sometimes? .....	98
2.25 I can upload firmware from "Firmware Management" page, but this firmware is not available in "Firmware Upgrade" page. What's wrong? .....	99
2.26 How can I see the report for a device? .....	99
2.27 Why do I get the message 'Pop-up blocked' when I try to login Vantage server?.....	99
2.28 When I want to delete VPN rules of a certain device, it seems the rules can't be deleted? .....	100
2.29 In OTV, a device is shown with green, but why it is shown with status of "off" on right window? .....	100
2.30 Currently, my device is managed by CNM server with no encrypt-mode. And it's green in OTV. Then if I want to use encrypt mode with DES algorithm, what should I do?.....	100
2.31 If I want to re-install the CNM but not lose my configuration, what should I do?.....	101
2.32 I have registered the MAC address of devices supported in the list, and the activation on device "cnm active 1" & "cnm managelp xxxxx". But the device in OTV is gray, what should I do? .....	102
2.33 Why the configuration between device & CNM is not consistent with each other?.....	102
2.34 After I have reinstalled the CNM, where could I get the new service key and activation key? .....	102
2.35 Why I can not see the "Reinstall" button when I login my www.myzyxel.com? .....	103
2.36 How to apply the one-click VPN feature in VPN editor? .....	103
2.37 When using "monitor>>VPN editor" to create a rule between 2 devices, why the line between them is dotted? Does it mean it fail? .....	104
2.38 Where can I change the number of days in	

“report>>bandwidth>>summary”? .....	104
2.39 Where can I create one time report? .....	104
3 Trouble Shooting .....	106
3.1 Trouble between Vantage Server & Client.....	106
3.2 Trouble between Vantage Server & ZyXEL devices .....	106
3.3 Trouble between Vantage Server & Vantage Report .....	107
3.4 Trouble in migration .....	107

# 1 Application Notes

Vantage CNM (Centralized Network Management) is a browser-based global management solution that allows an administrator from any location to easily configure, manage, monitor and troubleshoot ZyXEL devices located worldwide. See the *Vantage CNM User's Guide* for details.

## 1.1 Firmware & Model list Support

Device Model	Device F/W	New CNM 2.3 features	Reporting Function
ZyWALL 5	3.64XD5 and later	Same as CNM 2.2	Traffic Report Attack Report VPN Report Web Usage Report Log Report
	4.00XD11 and 4.00XD12	IDP/AV/AS/CF myZyXEL.com Registration WLAN Zone enhancement	UTM Report Traffic Report Attack Report VPN Report Web Usage Report Log Report
	4.01XD4 and later	Remote management Redundant IPSec tunnel Firewall/AV/AS/IDP WLAN zone enhancement	UTM Report Traffic Report Attack Report VPN Report Web Usage Report Log Report
ZyWALL 35	3.64WZ5 and later	Same as CNM 2.2	Traffic Report Attack Report VPN Report Web Usage Report Log Report
	4.00WZ11and 4.00WZ12	IDP/AV/AS/CF myZyXEL.com Registration WLAN Zone enhancement	UTM Report Traffic Report Attack Report VPN Report

	4.01WZ4 and later	Remote management Redundant IPSec tunnel Firewall/AV/AS/IDP WLAN zone enhancement	Web Usage Report Log Report
<b>ZyWALL 70</b>	3.65WM1 and later	Same as CNM 2.2	Traffic Report Attack Report VPN Report Web Usage Report Log Report
	4.00WM11 and 4.00WM12	IDP/AV/AS/CF myZyXEL.com Registration WLAN Zone enhancement	UTM Report Traffic Report Attack Report
	4.01WM4 and later	Remote management Redundant IPSec tunnel Firewall/AV/AS/IDP WLAN zone enhancement	VPN Report Web Usage Report Log Report
<b>ZyWALL P1</b>	3.64XJ5 and later	Same as CNM 2.2	Traffic Report Attack Report VPN Report Web Usage Report Log Report
<b>ZyWALL 10W</b>	3.64WH13 and later	Same as CNM 2.2	Attack Report Web Usage Report Log Report
<b>ZyWALL 2</b>	3.62WK12 and later	Same as CNM 2.2	Attack Report Web Usage Report Log Report
<b>ZyWALL 2+</b>	4.00XU2	Same as CNM 2.2	Traffic Report Attack Report VPN Report Web Usage Report Log Report

	4.01XU1 and later	Remote management Redundant IPSec tunnel NAT over IPSec	Traffic Report Attack Report VPN Report Web Usage Report Log Report
<b>P662HW-61</b>	3.40QR8 and 3.40QR9	Same as CNM 2.2	Attack Report Web Usage Report Log Report
<b>P662H-61</b>	3.40QR8 and 3.40QR9	Same as CNM 2.2	Attack Report Web Usage Report Log Report
<b>P662HW-D1</b>	3.40AGZ3 and later	Same as CNM 2.2 Wireless	Attack Report Web Usage Report Log Report
<b>P662H-D1</b>	3.40AGZ3 and later	Same as CNM 2.2	Attack Report Web Usage Report Log Report
<b>P653HWI-17</b>	3.40PN4 and later	Same as CNM 2.2	Attack Report Web Usage Report Log Report

## 1.2 Installation Scenario/Deployment Suggestion

**TCP/IP ports are used on CNM & VRPT server**

Vantage CNM Server		
Protocol Type	Port Number	Usage
UDP	11864	ZLD Device (e.g. ZW1050) communicates to CNM Server through UDP 11864
UDP	1864	ZyNOS Device communicates to CNM Server through UDP 1864
TCP	8080	CNM client (browser) connects to CNM Server through TCP 8080 Device communicates to CNM Server through TCP 8080 (for TR069)
TCP	443	CNM client (browser) connects to CNM Server through TCP 443



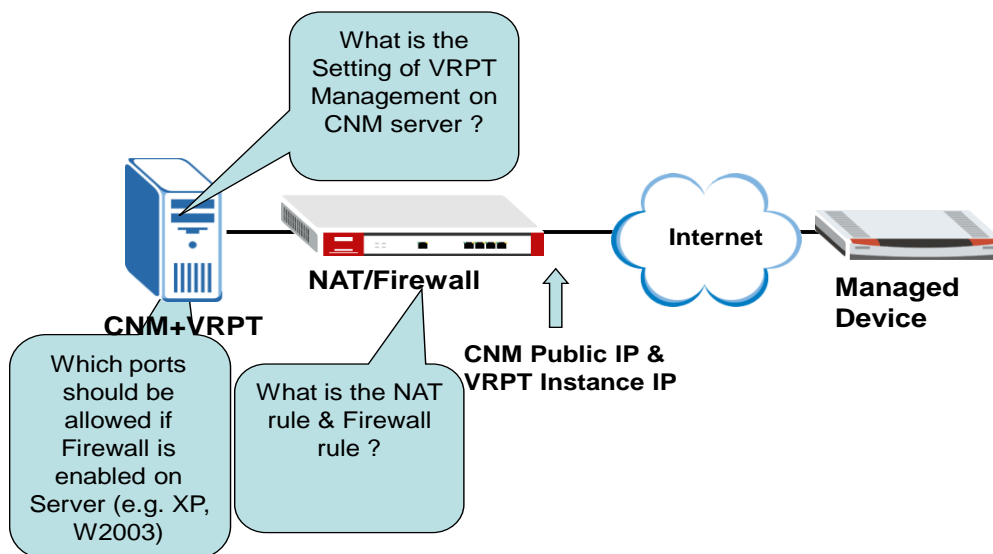
VRPT Server		
UDP	514	Device sends syslog to VRPT Server for logging and reporting
TCP	1099	CNM communicates to VRPT Server to retrieve reports and maintenance
FTP Server		
TCP	20/21	Device connects to FTP server for firmware upgrade/configure backup/restore

### 1.2.1 Single Server for CNM & VRPT

For a SI/Reseller who maintains less than 50 devices, both CNM (for management) and VRPT (for reporting) can be installed on the same server. Below is an example of the network topology and Hardware requirement.

CNM & VRPT Server	
CPU	Intel P4 3.2+ GHz
Memory	2GB and higher
Hard Disk	250GB and higher

### Installing CNM & VRPT on Same Server









1. On the NAT/Firewall, same public IP can be used as the public IP of CNM & VRPT Server. Forward Port **1864(UDP)**, **11864 (UDP)**, **8080 (TCP)**, **443 (TCP)**, **514 (UDP)** and **1099 (TCP)** to the CNM+VRPT Server
2. If you want your LAN subnet to access vantage server via WAN interface of NAT/Firewall, "ip nat loopback" should be checked.

For ZyNOS-based ZyWALL using as the NAT gateway, please check if the

command “*ip nat lookback*” is enabled.

For ZLD gateway (e.g. ZW1050) a policy route should be set.

a. Go to **Configuration>>Object>>Address**, set addresses for vantage server’s WAN, LAN and your Lan subnet.

#	Name	Type	Address	
1	LAN_SUBNET	SUBNET	192.168.1.0/24	 
2	CNM_internal	HOST	192.168.1.34	 
3	CNM_WAN	HOST	172.25.24.100	 

b. Go to **Configuration>>Policy>>Virtual Server**, set a rule as below to map your vantage server’s Wan IP to internal IP.

Name: CNM  
 Interface: ge1  
 Original IP: CNM\_WAN  
 Mapped IP: 192.168.1.34  
 Mapping Type: Any

\* Please make sure the firewall allows virtual server traffic.  
 \* Please create a corresponding policy route (NAT 1:1) if the virtual server will also establish con

OK Cancel

c. Go to **Configuration>>Policy>>Route**, click add icon, and configuration a rule as below to achieve loopback.

**Configuration**

Enable  
 Description: CNM (Optional)

**Criteria**

User: any  
 Incoming: Interface / ge1  
 Source Address: LAN\_SUBNET  
 Destination Address: CNM-internal  
 Schedule: none  
 Service: any

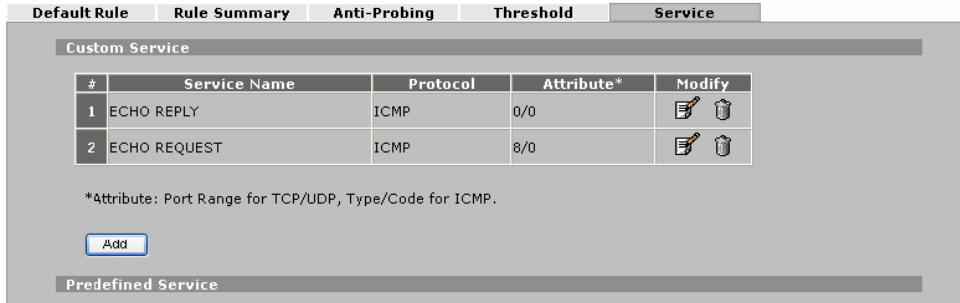
- Port **1864(UDP)**, **11864 (UDP)**, **8080 (TCP)**, **443 (TCP)**, **514 (UDP)** and **1099 (TCP)** have to be opened in Firewall and forwarded to CNM+VRPT Server
- If FTP Server is installed on the same machine, please also open **20/21 (TCP)** and firewall policy on gateway.
- Configure the public IP that mapped to VRPT in **System>>VRPT Management** of CNM

Here’s a configuration Example:

IP Assignment	
CNM & VRPT Server	192.168.1.33
WAN IP of NAT router	172.25.21.41

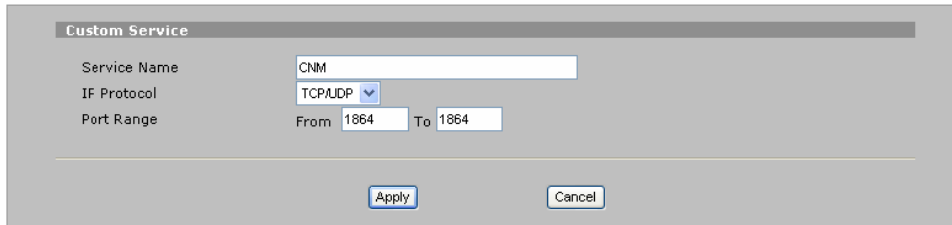
Go to the WEB GUI of ZyWALL, and configure the NAT rule and the firewall rule:  
**In Firewall>>Service**

**FIREWALL**



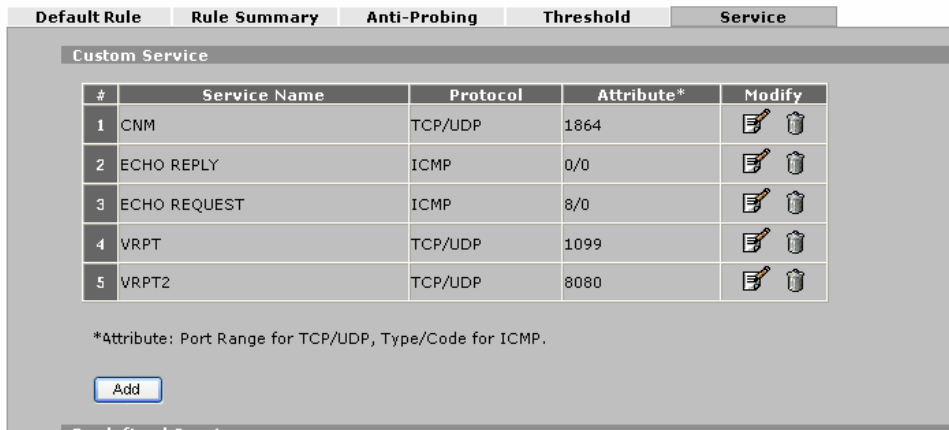
Add port **1864**, **1099** and **8080** to Custom Service:

**FIREWALL - EDIT CUSTOM SERVICE**



Then these ports could be used in firewall rule that we will define later.

**FIREWALL**



Then, go to **Firewall>>Rule Summary WAN-to-LAN**

FIREWALL

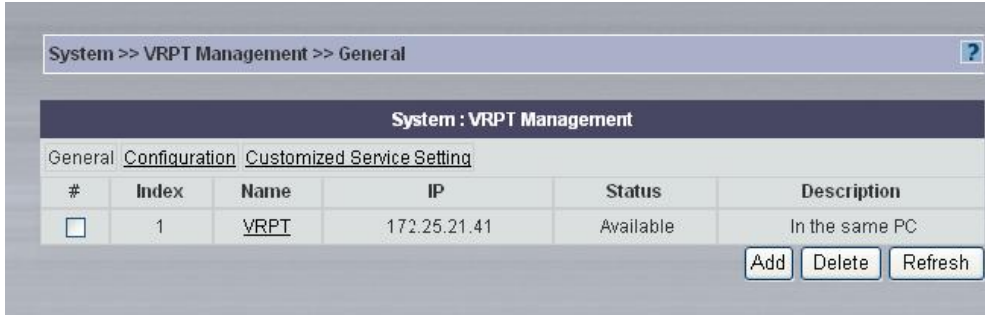
Please press the **Insert** to add the **CNM (1864, 11864)**, **VRPT (1099)**, **VRPT2 (8080)**, **HTTPS (443)** and **SYSLOG (514)** to the selected Service.

Then, go to **NAT** and make sure all ports are forwarded to the Server. Go to **Advanced>>NAT>>Port Forwarding**; forward the port **514, 1099, 1864, 11864** and **8080** and **443** to your server's IP Address

NAT

#	Active	Name	Incoming Port(s)	Port Translation	Server IP Address
1	<input checked="" type="checkbox"/>	VRPT	1099 - 1099	1099 - 1099	192 . 168 . 1 . 33
2	<input checked="" type="checkbox"/>	CNM	1864 - 1864	1864 - 1864	192 . 168 . 1 . 33
3	<input checked="" type="checkbox"/>	VRPT2	514 - 514	514 - 514	192 . 168 . 1 . 33
4	<input checked="" type="checkbox"/>	CNM2	8080 - 8080	8080 - 8080	102 . 168 . 1 . 33
5	<input checked="" type="checkbox"/>	https	443 - 443	443 - 443	192 . 168 . 1 . 33
6	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0

Then, go to **System>>VRPT Management**, you can find that the status of VRPT become **Available**.



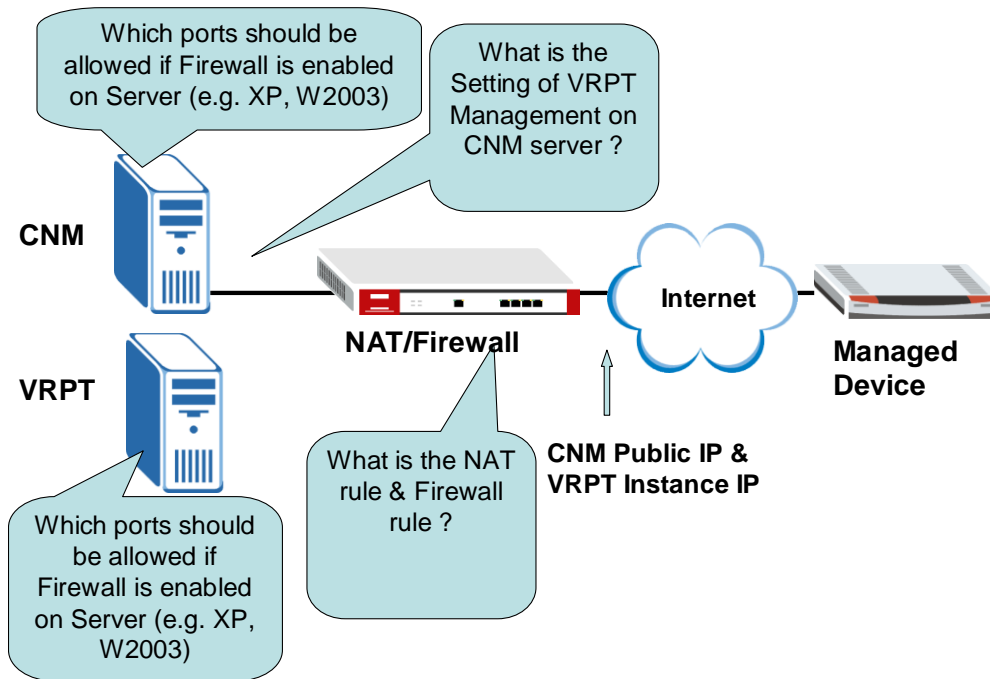
### 1.2.2 install CNM and VRPT on Different ServerInstalling

For a SI/Reseller who maintains less than 100 devices but better performance is wanted for management & reporting, CNM (for management) and VRPT (for reporting) could be installed separately to achieve this. Below is an example of the network topology and Hardware requirement.

<b>Management Server (Vantage CNM)</b>	
CPU	Intel Pentium IV 3.2 GHz or higher
Memory	2GB or higher
Hard Disk	80GB or higher
<b>Reporting Server (Vantage Report for CNM)</b>	
CPU	Intel Pentium IV 3.2 GHz or higher
Memory	1GB or higher
Hard Disk	200GB or higher

**Note:** Reporting Server can handle <=1500 logs/sec

## Installing CNM & VRPT on Different Servers



1. On the NAT/Firewall, same public IP can be used as the public IP of CNM & VRPT Server. Forward **Port 1864(UDP), 11864 (UDP), 8080 (TCP), 443 (TCP)** to CNM Server and forward **514 (UDP) and 1099 (TCP)** to VRPT Server
2. If you want your LAN subnet to access vantage server via WAN interface, “ip nat loopback” should be checked.

For ZyNOS-based ZyWALL using as the NAT gateway, please check if the command “*ip nat loopback*” is enabled.

For ZLD gateway (e.g. ZW1050) a policy route should be set. Please refer to [1.2.1 Single Server for CNM & VRPT](#).

3. If firewall is enabled on the server, Allow **1864(UDP), 11864 (UDP), 8080 (TCP), 443 (TCP)** on CNM Server and allow **514 (UDP) and 1099 (TCP)** on VRPT Server
4. Configure the public IP that mapped to VRPT in **System>>VRPT Management** of CNM

Here’s a configuration Example:

IP Assignment	
CNM Server	192.168.1.33
VRPT Server	192.168.1.34
WAN IP of NAT router	172.25.21.41

In the NAT Router/Firewall, add the port 1864, 11864, 1099, and 8080 in the service:  
**Security>>Firewall>>Service**

FIREWALL

Default Rule	Rule Summary	Anti-Probing	Threshold	Service
<b>Custom Service</b>				
#	Service Name	Protocol	Attribute*	Modify
1	CNM	TCP/UDP	1864	
2	ECHO REPLY	ICMP	0/0	
3	ECHO REQUEST	ICMP	8/0	
4	VRPT	TCP/UDP	1099	
5	VRPT2	TCP/UDP	8080	

\*Attribute: Port Range for TCP/UDP, Type/Code for ICMP.

Forward port 11864, 1864, 1099, 8080,514 and 443 port in the firewall configuration, direction of **WAN-to-LAN**

**Edit Source Address**

Address Editor

Address Type: Any Address

Start IP Address: 0 . 0 . 0 . 0

End IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Source Address(es): Any

**Edit Destination Address**

Address Editor

Address Type: Any Address

Start IP Address: 0 . 0 . 0 . 0

End IP Address: 0 . 0 . 0 . 0

Subnet Mask: 0 . 0 . 0 . 0

Destination Address(es): Any

**Edit Service**

Available Services (See [Service](#))

DNS(TCP/UDP:53)  
FINGER(TCP:79)  
FTP(TCP:20,21)

Selected Service(s)

\*CNM(TCP/UDP:1864)  
\*VRPT(TCP/UDP:1099)  
\*VRPT2(TCP/UDP:8080)

Forward Port 11864, 1864, 8080 and 443 to CNM server and port 1099 and 514 to VRPT in NAT configuration:

NAT

NAT Overview		Address Mapping	Port Forwarding	Port Triggering	
<b>Port Forwarding Rules</b>					
Default Server		0 . 0 . 0 . 0		Go To Page 1	
#	Active	Name	Incoming Port(s)	Port Translation	Server IP Address
1	<input checked="" type="checkbox"/>	VRPT	1099 - 1099	1099 - 1099	192 . 168 . 1 . 34
2	<input checked="" type="checkbox"/>	CNM	1864 - 1864	1864 - 1864	192 . 168 . 1 . 33
3	<input checked="" type="checkbox"/>	VRPT2	514 - 514	514 - 514	192 . 168 . 1 . 34
4	<input checked="" type="checkbox"/>	CNM2	8080 - 8080	8080 - 8080	102 . 168 . 1 . 33
5	<input checked="" type="checkbox"/>	Https	443 - 443	443 - 443	192 . 168 . 1 . 33
6	<input type="checkbox"/>		0 - 0	0 - 0	0 . 0 . 0 . 0

Then, go to **System>>VRPT Management**, you can find that the status of VRPT turns **Available**.



### 1.2.3 Installing Multiple VRPT Servers

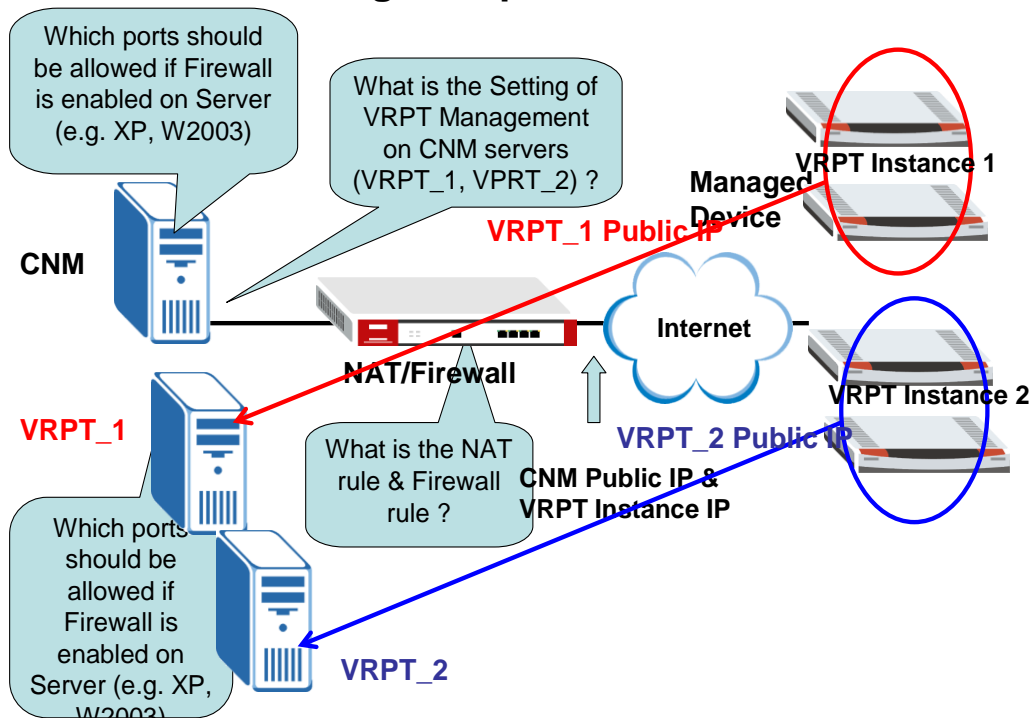
For a SI or MSP who maintains more than 100 devices, CNM (for management) and more than one VRPT (for reporting) should be installed on different Server. Below is the illustration of the network topology and recommended hardware platform.

<b>Management Server (Vantage CNM)</b>	
CPU	Intel Pentium IV 3.2 GHz or higher
Memory	2GB or higher
Hard Disk	80GB or higher
<b>Reporting Server (Vantage Report for CNM)</b>	
CPU	Intel Pentium IV 3.2 GHz or higher
Memory	1GB or higher
Hard Disk	200GB or higher

**Note:** Reporting Server can handle <=1500 logs/sec



### Installing Multiple VRPT Servers



1. On the NAT/Firewall, same public IP can be used as the public IP of CNM & VRPT Server. Forward Port 1864(UDP), 11864 (UDP), 8080 (TCP), 443 (TCP) to CNM Server and forward 514 (UDP) and 1099 (TCP) to VRPT Server
2. If you want your LAN subnet to access vantage server via WAN interface, “ip nat loopback” should be checked.

For ZyNOS-based ZyWALL using as the NAT gateway, please check if the command “*ip nat loopback*” is enabled.

For ZLD gateway (e.g. ZW1050) a policy route should be set. Please refer to [1.2.1 Single Server for CNM & VRPT](#).

3. If firewall is enabled on the server, Allow 1864(UDP), 11864 (UDP), 8080 (TCP), 443 (TCP) on CNM Server and allow 514 (UDP) and 1099 (TCP) on VRPT Server
4. Configure the public IP that mapped to VRPT in **System>>VRPT Management** of CNM

**Note:** Full feature NAT must be used to make more than 1 VRPT server visible to all devices on the internet (as port that used for receiving logs is fixed), which means different Public IP address has to be mapped to different VRPT server. But 1 VRPT could share the same Public IP address with CNM.

Here’s a configuration example:

IP Assignment	
CNM Server	192.168.1.33
VRPT Server 1	192.168.1.2

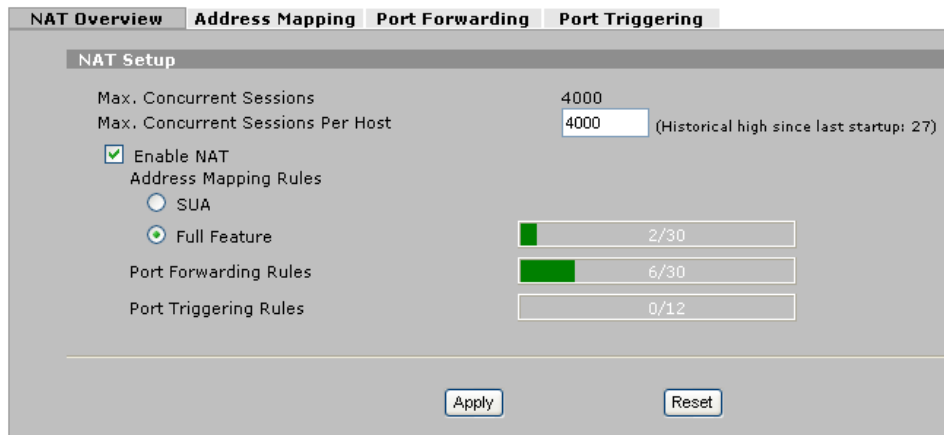
VRPT Server 2	192.168.1.3
Public IP of NAT Router	172.25.24.202~172.25.24.203

Full-feature NAT setting		
Source IP address	NAT Type	Public IP address
192.168.1.2	One-to-one	172.25.24.203
192.168.1.3-192.168.1.254	Many-to-one	172.25.21.202

Step1. Make sure the ports of 1864, 1099, 514, 443, 8080 and 21 are allowed in the WAN-to-LAN rule of the firewall setting.

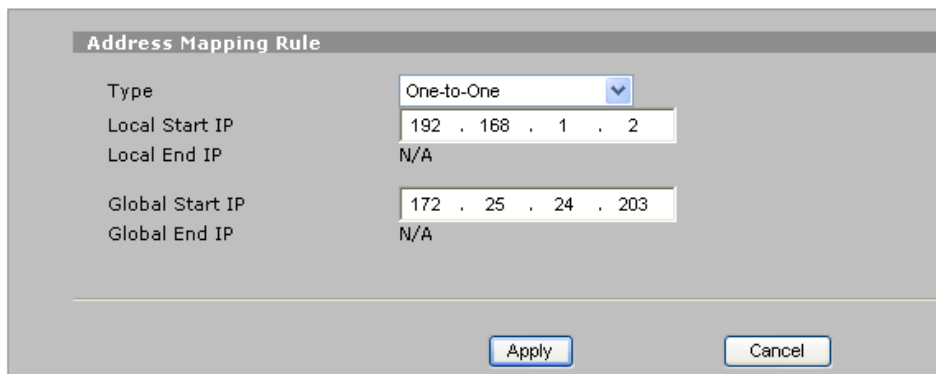
Step2. Go to **Advanced>>NAT>>NAT Overview**, choose the **Full-feature** and configure the Address Mapping.

**NAT**



Step3. Configure the **One-to-One** rule,

**NAT - ADDRESS MAPPING**



Step4. Configure the **Many-To-One** rule.

NAT - ADDRESS MAPPING

**Address Mapping Rule**

Type: Many-to-One

Local Start IP: 192 . 168 . 1 . 3

Local End IP: 192 . 168 . 1 . 254

Global Start IP: 172 . 25 . 24 . 202

Global End IP: N/A

Apply Cancel

Step5, Check the NAT mapping is the same as below:

NAT

NAT Overview Address Mapping Port Forwarding Port Triggering

**SUA Address Mapping Rules**

#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type
1	0.0.0.0	255.255.255.255	0.0.0.0	N/A	M-1
2	N/A	N/A	0.0.0.0	N/A	Server

**Full Feature Address Mapping Rules**

#	Local Start IP	Local End IP	Global Start IP	Global End IP	Type	Modify
1	192.168.1.2	N/A	172.25.24.203	N/A	1-1	
2	192.168.1.3	192.168.1.254	172.25.24.202	N/A	M-1	
3	N/A	N/A	0.0.0.0	N/A	Server	
4	...	...	...	...	-	

Step6. Configure the port forwarding, forward the port 1099, 8080,514, 443, 1864 and 21 port to the 192.168.1.33 (for **One-To-One** mapping of VRPT (192.168.1.2), no port forwarding is needed).

NAT

NAT Overview Address Mapping Port Forwarding Port Triggering

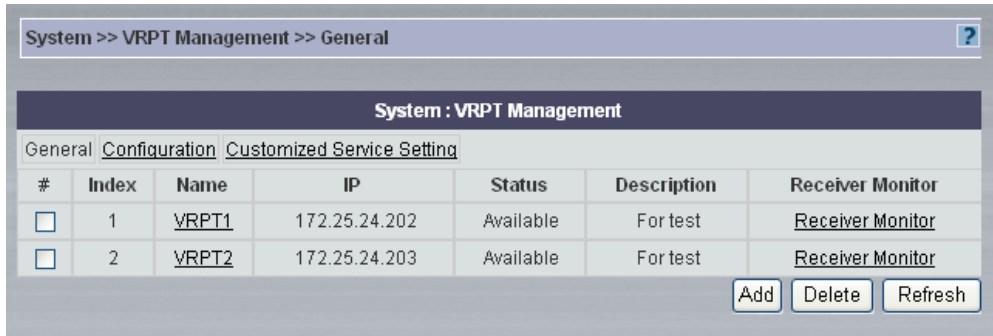
**Port Forwarding Rules**

Default Server: 0 . 0 . 0 . 0

Go To Page 1

#	Active	Name	Incoming Port(s)	Port Translation	Server IP Address
1	<input checked="" type="checkbox"/>	CNM	1864 - 1864	1864 - 1864	192 . 168 . 1 . 33
2	<input checked="" type="checkbox"/>	CNM2	8080 - 8080	8080 - 8080	192 . 168 . 1 . 33
3	<input checked="" type="checkbox"/>	FTP	21 - 21	21 - 21	192 . 168 . 1 . 33
4	<input checked="" type="checkbox"/>	HTTPS	443 - 443	443 - 443	192 . 168 . 1 . 33
5	<input checked="" type="checkbox"/>	VRPT	1099 - 1099	1099 - 1099	192 . 168 . 1 . 34
6	<input checked="" type="checkbox"/>	syslog	514 - 514	514 - 514	192 . 168 . 1 . 34

Step7, add the two VRPT servers IP to the CNM, and then check its status.

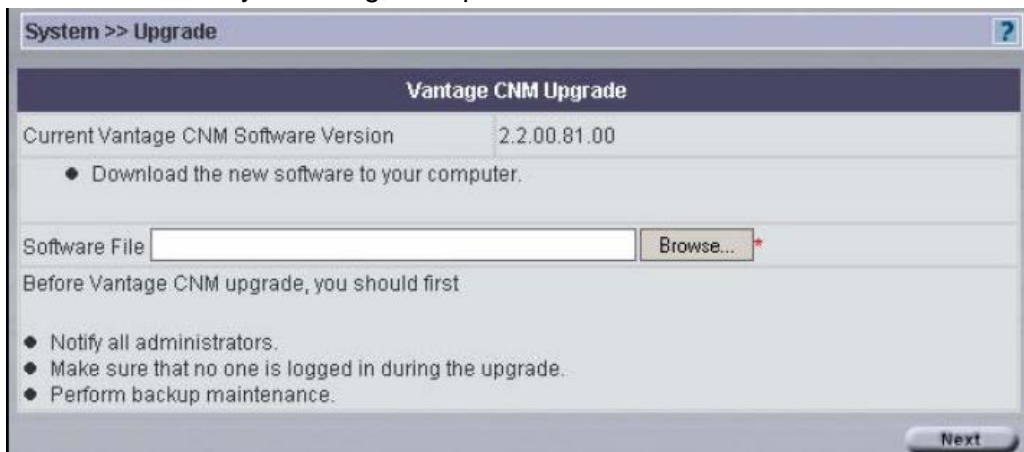


## 1.3 Upgrade (Migration) from existing CNM installation

### 1.3.1 From CNM 2.2 and CNM 2.3 Lite

If the existed CNM major version is 2.2, and the minor version is less than 00.61.03, you will need to upgrade CNM to the version 2.2.00.61.03 firstly. Please get CNM 2.2 upgrade patch from download library ([http://www.zyxel.com/web/support\\_download.php](http://www.zyxel.com/web/support_download.php)) or CD and upgrade the CNM step by step. The upgrade procedures have to be 2.2.00.61.00 → 2.2.00.61.01 → 2.2.00.61.02 → 2.2.00.61.03, which means 2.2.00.61.03 cannot be upgraded directly to 2.2.00.61.00 or 2.2.00.61.01

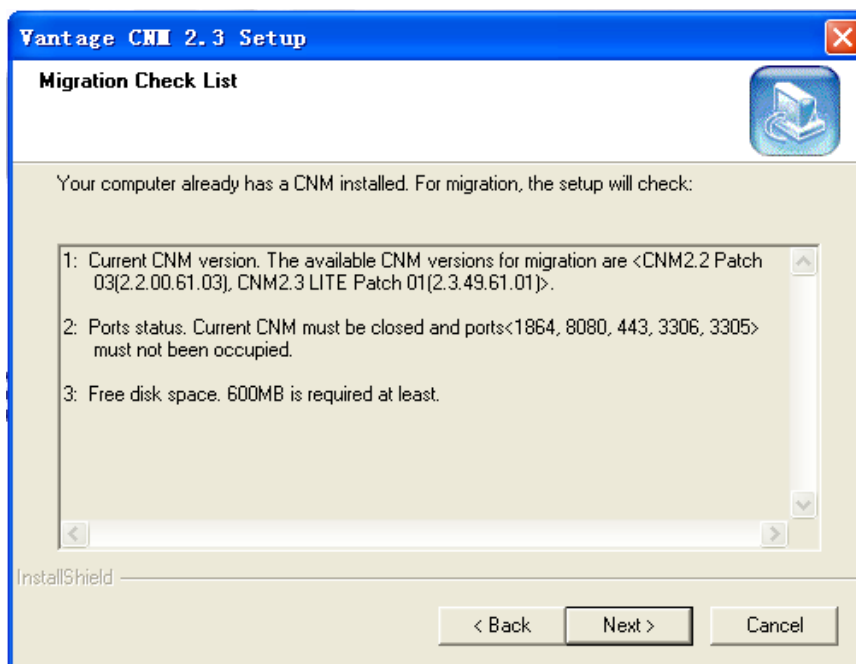
To perform the upgrade in CNM server, Login CNM 2.2, go to **System>>Upgrade**, select the correct file by browsing, then press **Next**



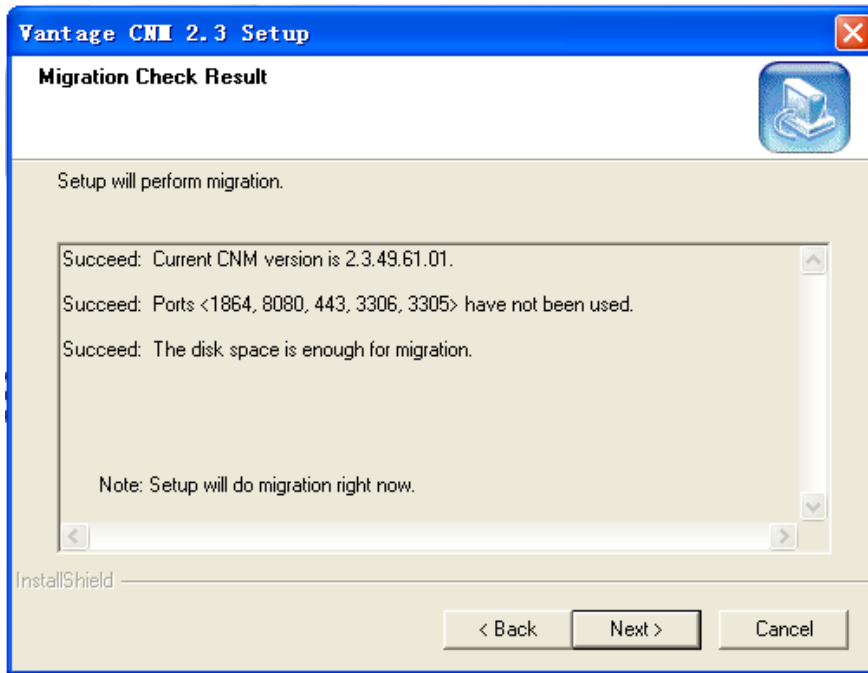
If the existed CNM is 2.3.49.61.00 or 2.3.49.61.01, you could just upgrade your CNM directly using the install package.

After you upgrade your CNM 2.2 to 00.61.03 patch or you have CNM 2.3 LITE version, just follow the step to upgrade the CNM to 2.3 standard version.

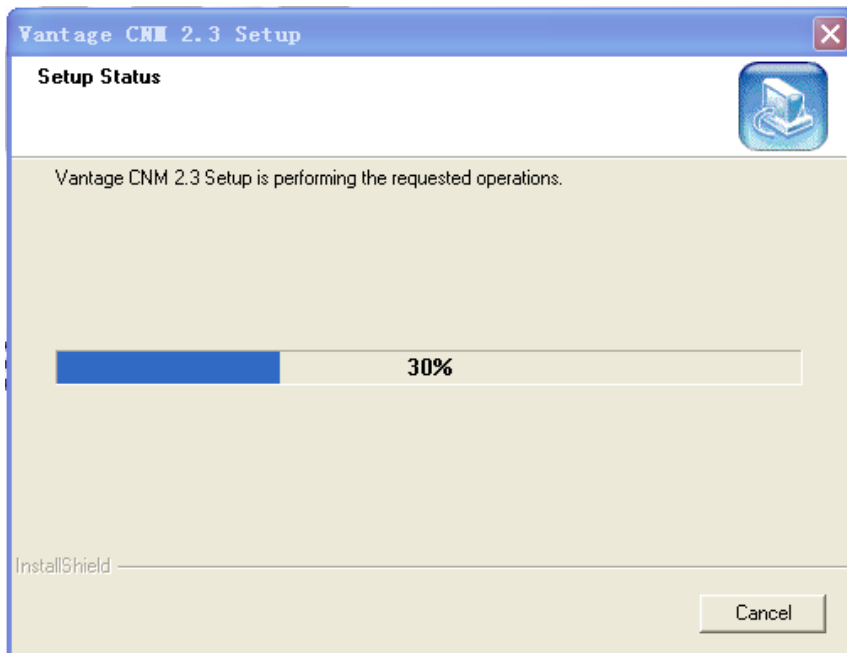
1. If you have existed CNM running, please shut it down first.
2. Please make sure the port 1864, 8080, 443, 3306 in your system is not occupied.
3. Please make sure the available space in the disk with pervious CNM installation is more than 600MB.
4. Then run the install package "2.3.00.61.00.zip" to do the migration.
5. The installation will check the migration condition to make sure everything is available.



6. Confirm the check result.



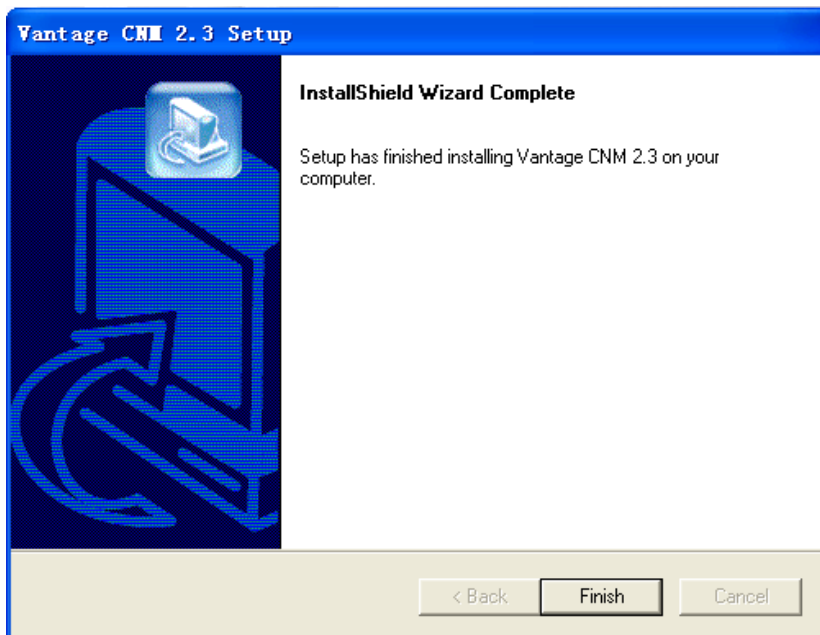
- 7. The program will install CNM 2.3 first.

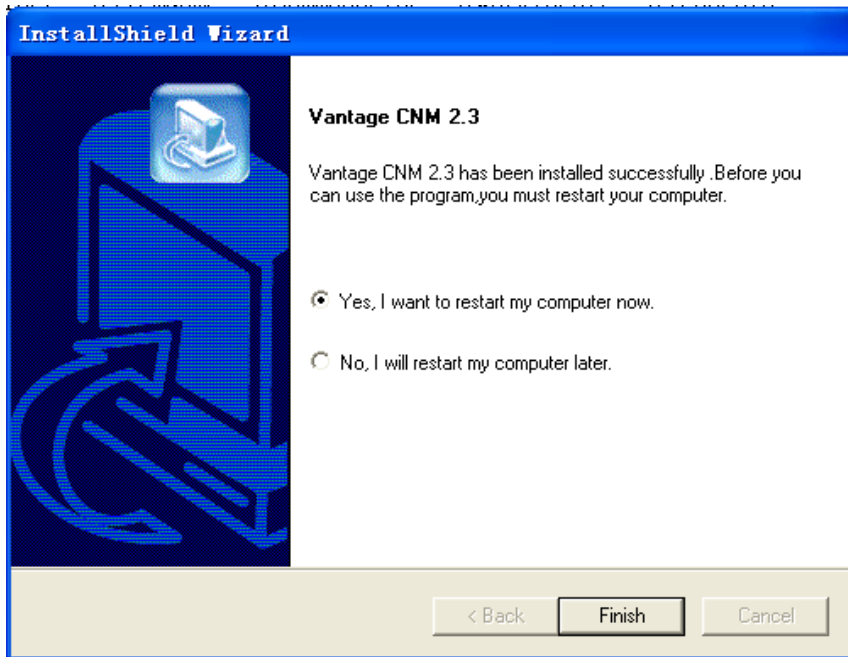


- 8. Then begin the migration.

```
C:\WINDOWS\system32\cmd.exe
DataMigration - WirelessCard Function [3] is doing migration...
DataMigration - WirelessCard Function [4] is doing migration...
DataMigration - WirelessCard Function [5] is doing migration...
DataMigration - WirelessCard Function [6] is doing migration...
DataMigration - WirelessCard Function [7] is doing migration...
DataMigration - WirelessCard Function [8] is doing migration...
DataMigration - WirelessCard Function [9] is doing migration...
DataMigration - WirelessCard Function [10] is doing migration...
DataMigration - WirelessCard Function [11] is doing migration...
DataMigration - WirelessCard Function [12] is doing migration...
DataMigration - WirelessCard Function [13] is doing migration...
DataMigration - WirelessCard Function [14] is doing migration...
DataMigration - Wan Function [0] is doing migration...
DataMigration - Wan Function [1] is doing migration...
DataMigration - Wan Function [2] is doing migration...
DataMigration - Wan Function [3] is doing migration...
DataMigration - Wan Function [4] is doing migration...
DataMigration - Wan Function [5] is doing migration...
DataMigration - Wan Function [6] is doing migration...
DataMigration - Wan Function [7] is doing migration...
DataMigration - Wan Function [8] is doing migration...
DataMigration - Wan Function [9] is doing migration...
DataMigration - Wan Function [10] is doing migration...
DataMigration - Wan Function [11] is doing migration...
DataMigration - Firewall Function [0] is doing migration...
DataMigration - Firewall Function [1] is doing migration...
DataMigration - Firewall Function [2] is doing migration...
DataMigration - Firewall Function [3] is doing migration...
DataMigration - Firewall Function [4] is doing migration...
DataMigration - Firewall Function [5] is doing migration...
DataMigration - Firewall Function [6] is doing migration...
DataMigration - Firewall Function [7] is doing migration...
DataMigration - Firewall Function [8] is doing migration...
DataMigration - Firewall Function [9] is doing migration...
DataMigration - Firewall Function [10] is doing migration...
DataMigration - Firewall Function [11] is doing migration...
DataMigration - Firewall Function [12] is doing migration...
DataMigration - Firewall Function [13] is doing migration...
```

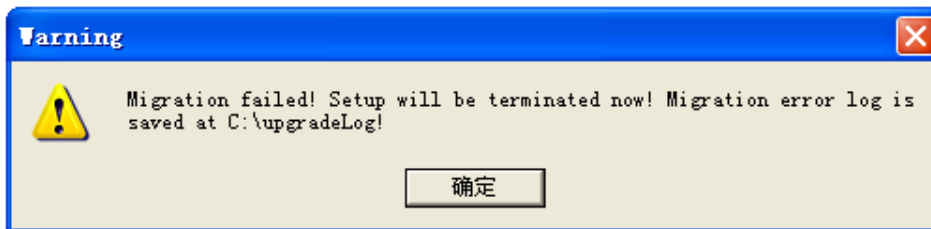
- 9. If migrate successfully from CNM 2.2, you will be asked to restart you computer.





If migrate is successfully done from CNM 2.3 Lite, there will be no need to restart your computer.

10. If the migration is failed, there will be a warning message. You can read the upgrade log in directory "upgradeLog" in your primary hard drive disk, upgrade utility will automatically do the rollback for all changes so pervious version won't be affected



### 1.3.2 From CNM 2.0/2.1

If the existed CNM major version is 2.0/2.1, you should upgrade it to version 2.2 and then upgrade from version 2.2 to version 2.3. Please get CNM 2.2 upgrade patch from download library or CD and upgrade the CNM step by step. As for upgrade from version 2.2 to version 2.3, please refer to [1.3.1 From CNM 2.2 and CNM 2.3 Lite.](#)

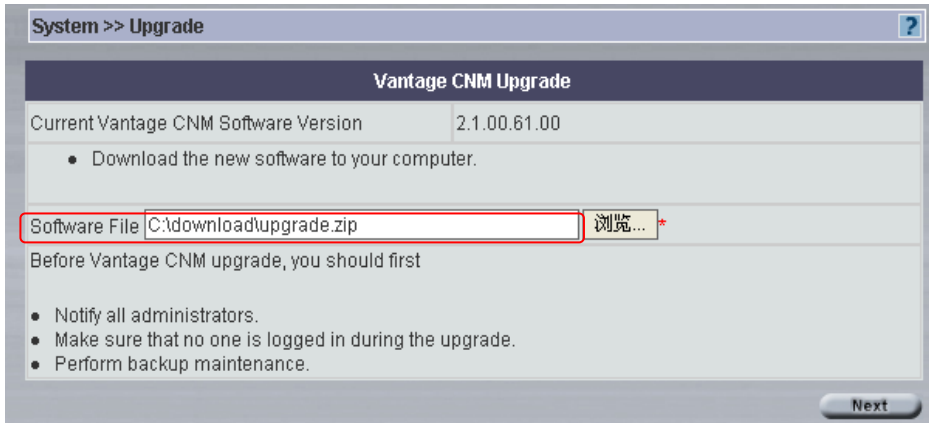
If the current version is 2.0.00.61.XX, the upgrade step is: 2.0.00.61.XX to 2.1.00.61.11 → 2.2.00.61.00 → 2.2.00.61.01 → 2.2.00.61.02 → 2.2.00.61.03.

If the current version is 2.1.00.61.00/01, the upgrade step is: 2.1.00.61.00/01 to 2.1.00.61.11 → 2.2.00.61.00 → 2.2.00.61.01 → 2.2.00.61.02 → 2.2.00.61.03.

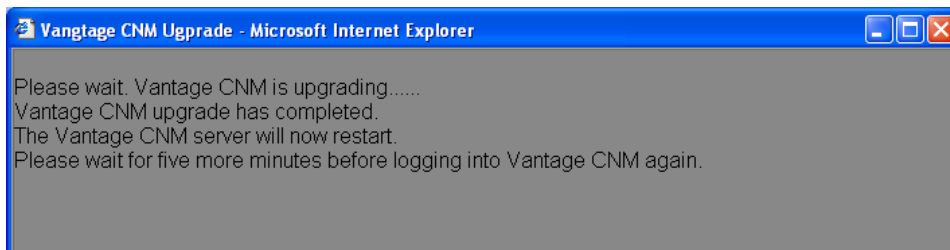
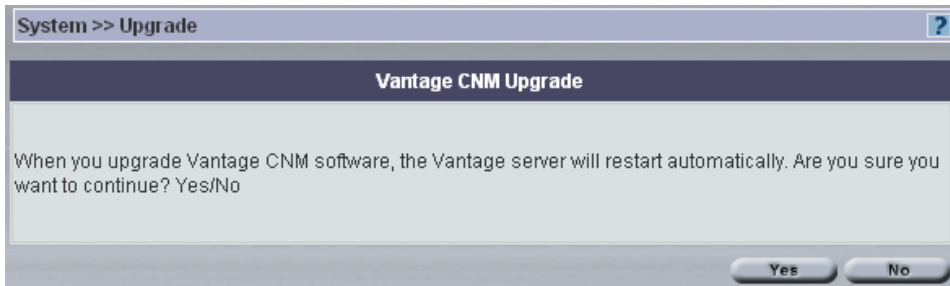
Here're the steps:



1. Login Vantage CNM using **root** account.
2. Click menu **System>>upgrade**, and then select the Vantage CNM upgrade zip file.



3. Click **Yes**, then Vantage CNM browser disappears and a new window popup shown down below.



It will take about five minutes to complete the upgrade progress. Then restart of Vantage is needed.

**Note:** Windows OS and Linux OS use different patch of Vantage CNM.

The Path for the log is at

"X:\CNM\_install\_directory\ZYCNM\_DEPLOY\_BED\log\upgrade.log"

Since the upgrade process from version 2.0/2.1 to 2.3 STD is complicated, we recommend customer to uninstall the existed version before installing CNM version 2.3. For the brand-new installation, please refer to steps below:

### 1.3.2.1 CNM Server Installation

1. Run Vantage CNM 2.3 (2.3.00.61.00.exe) on the server which is for CNM
2. If server is running windows XP SP2 or 2003, make sure UDP1864 & TCP8080, 443 is allowed by Firewall
3. If the CNM Server is placed behind a NAT Firewall router, Configure NAT and Firewall:
  - a. Forward UDP 1864 to CNM Server (Devices to CNM server by SGMP)
  - b. Forward TCP 8080, 443 to CNM Server (Devices to CNM server by TR-069 & CNM client to CNM server)
4. Check if the Server is running and port (UDP 1864, TCP 8080, TCP443) is opening thru "netstat -an"
5. If installation failed, check "*C:\Program Files\ZyXEL\Vantage CNM 2.3\logs\vantage.log*"

### 1.3.2.2 VRPT Server Installation

1. Run Vantage Report for CNM on the server which is set for VRPT
2. If server is running windows XP SP2 or 2003, make sure UDP514 & TCP1099 is allowed by Firewall
3. If the VRPT Server is placed behind a NAT Firewall router, config NAT and Firewall:
  - a. Forward UDP 514 to VRPT Server (devices send syslog to the VRPT)
  - b. Forward TCP 1099 to VRPT Server (management between CNM to VRPT)
4. Check if the Server is running and port (UDP 514, TCP 1099) is opening thru "netstat -an"
5. If installation failed, check "*C:\Program Files\ZyXEL\Vantage Report for CNM\vrpt\log\output.log*"

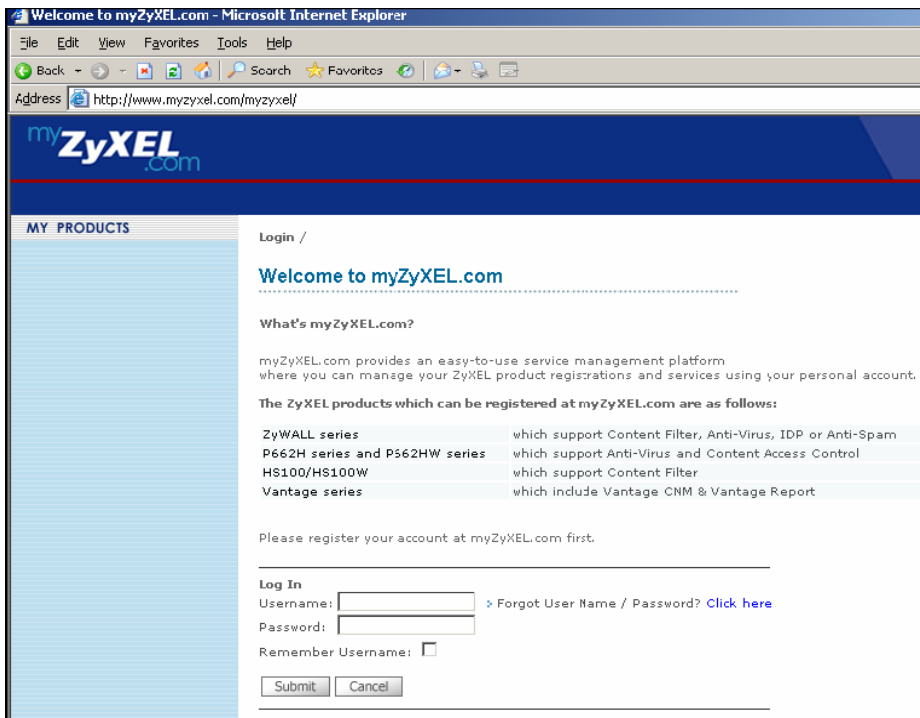
CNM has to be activated in myzyxel.com using licence key. Please refer to the steps below:

### 1.3.2.3 CNM Activation

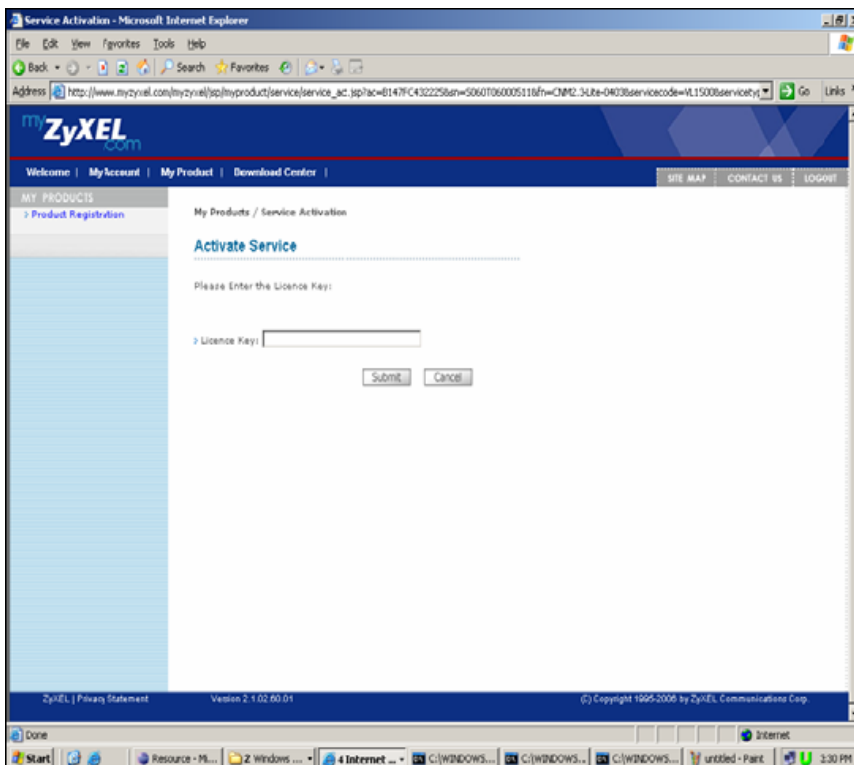
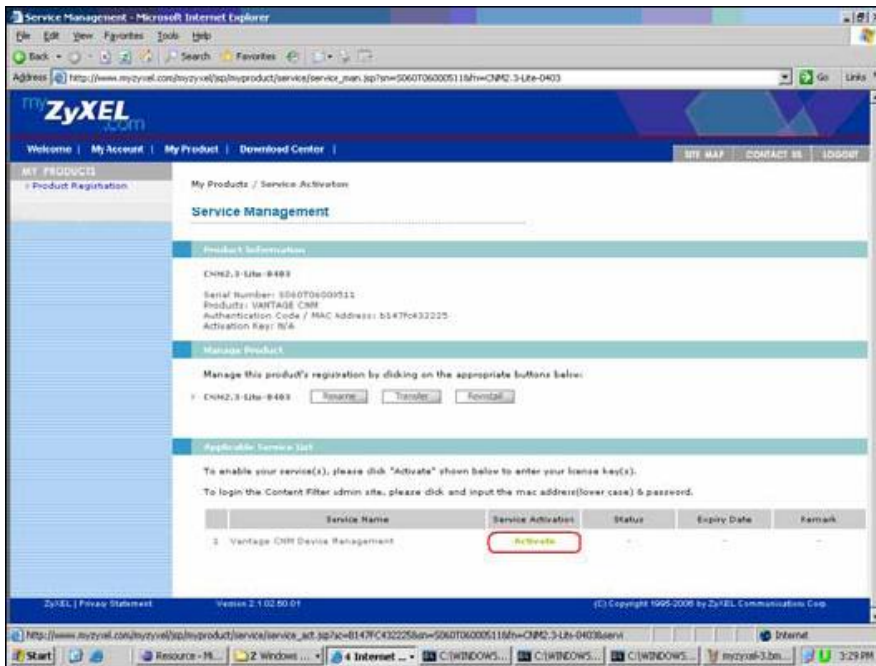
- a. Open browser to connect to CNM: <http://<CNM Server IP>:8080> or <https://<CNM Server IP>> (on CNM)
- b. Login server by entering the default username/password: root/root (on CNM)
- c. Server will prompt Authentication Code and request Activation Key & Service Set Key (on CNM)

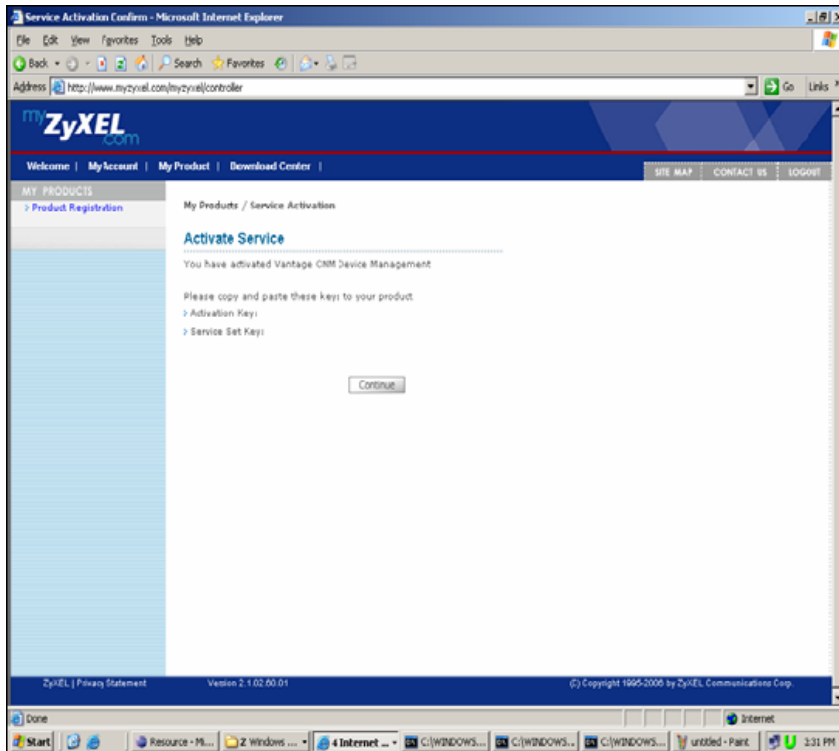


- d. Open a browser and connect to myZyXEL.com <http://www.myzyxel.com> (on myZyXEL.com)
- e. Login by entering myZyXEL user account (on myZyXEL.com)

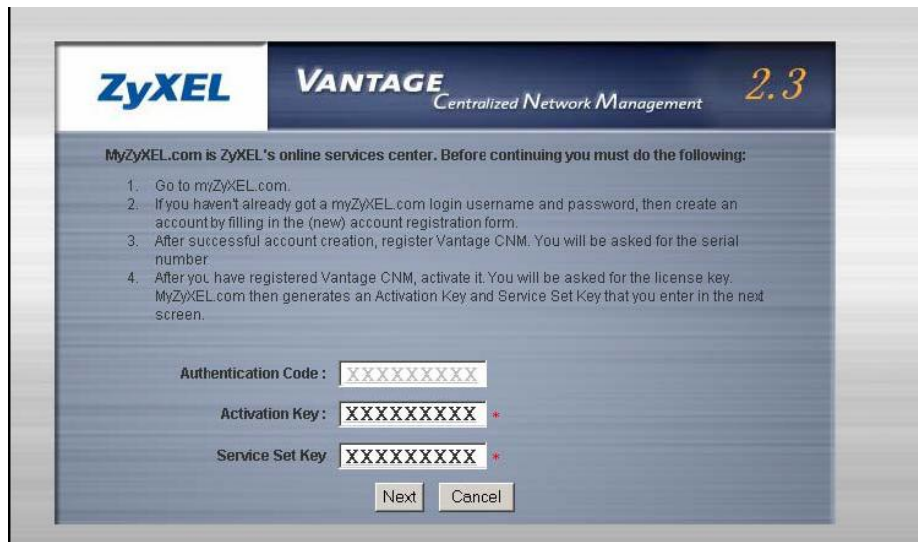


- f. Register a new product with Serial Number and Authentication Code (from step iii) (on myZyXEL.com)
- g. Activate service and enter License Key to get Activation Key and Service Set Key (SSK) (on myZyXEL.com)





h. Copy Activation Key and Service Set Key (SSK) to CNM server (on CNM)



i. Click Next and Login CNM Server successfully (on CNM)

**Note: Please check status of FTP and VRPT server in CNM after the installation**

FTP Server	
System>>Status	Make sure the FTP server is ready for firmware upgrade

<b>Add VRPT Server to CNM</b>	
System>>VRPT Management:	Add VRPT Server to CNM for reporting, Check the status of VRPT Server is available.

## 1.4 A scenario for Vantage application

In the following application note, we will introduce how to use Vantage to conduct UTM, VPN Management and device maintenance over multiple ZyXEL appliances in **MSP (Managed Service Provider)** environment.

We will also introduce how to use the report function of CNM.

We assume customer reading this chapter has already done basic setups including:

Vantage CNM Server and FTP server setup and activation on Windows Operating System and also connection between Vantage server and FTP server is ok.

Customers, who have not finished the preceding operations yet, please refer to detailed steps in *Quick Start Guide of Vantage CNM 2.3*.

Jim is a principal of company M, a local Managed services provider. He always receives many requests from small & medium- sized companies in the hope that M company would help them find a reliable and cost effective solution to maintenance their network. Here comes A Company and B Company.

A Company is a medium-sized company with 300 employees. There are N branches all over the country. Almost 80 percents of A Company's employees need to use the Internet in daily work. They would like to use UTM function to protect their network and want to maintain the devices centrally. They also need a report about the UTM and the Internet usage of the company.

B Company is a small-sized company with only one branch in another city. They want to share their resources and information across HQ and Branch without compromising their security. By deploying the ZyWALL's VPN feature they could be confident that only trusted users could access the company's network. They would like a report for their bandwidth management, security status and Internet usage as well.

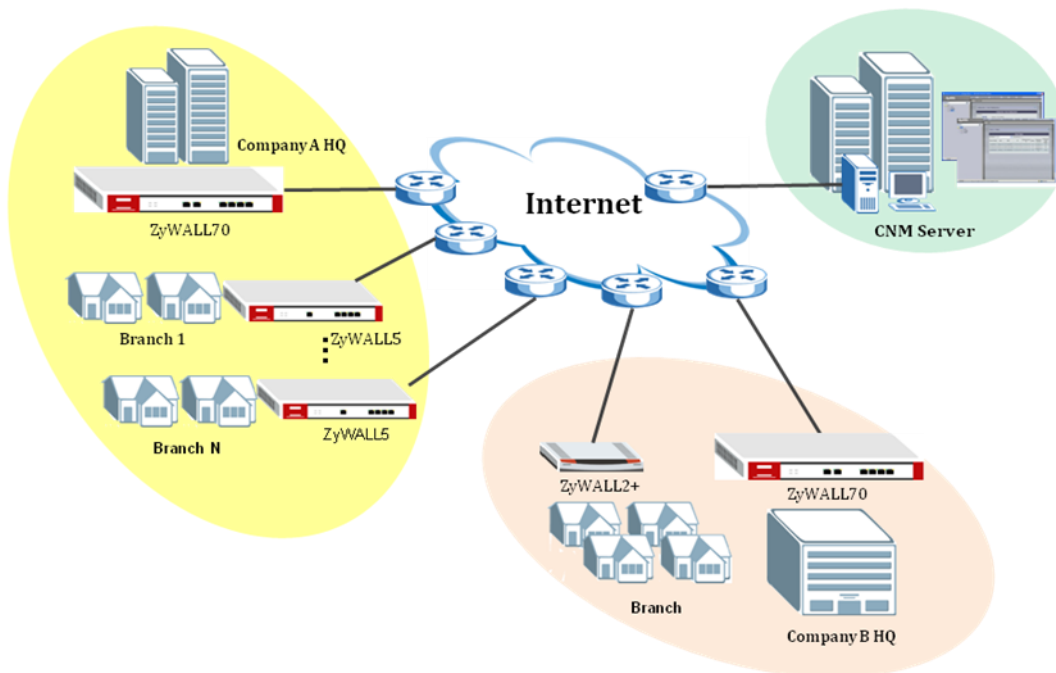
M Company's solution for A Company and B Company with ZyXEL appliances and Vantage CNM:

<b>UTM Management</b>	<ol style="list-style-type: none"> <li>1. Centralized License Management</li> <li>2. Policy Enforcement</li> <li>3. UTM Report</li> <li>4. Active Monitoring and Alerting</li> </ol>
<b>VPN Management</b>	<ol style="list-style-type: none"> <li>1. Security VPN tunnel establishment</li> <li>2. View VPN Tunnel Status</li> </ol>

<b>Device Maintenance</b>	<ol style="list-style-type: none"> <li>1. Firmware management and upgrade</li> <li>2. ROM file backup and restore</li> </ol>
<b>Monitor, Alerting &amp; Reporting</b>	<ol style="list-style-type: none"> <li>1. Device alarm, alert and notify</li> <li>2. Monitor the Internet usage and security status via device report</li> </ol>

The following picture shows the network for M's solution.

The companies are connected to the Internet via DSL connections and gain static Public IPs from ISP. A company uses a ZyWALL 70 in HQ and ZyWALL 5 in all branches as the firewall to protect the company network. B Company uses a ZyWALL 70 in HQ and a ZyWALL 2 plus in the branch as firewall to protect the company work.



The following diagram depicts the network environment & IP address assignments of this example.

**A Company:**

Device Name	AHQZW70	BR1ZW5	BR2ZW5
Device Type	ZyWALL70	ZyWALL5	ZyWALL5
Administrator	John		
IP Address	WAN: 172.25.24.100 LAN: 192.168.1.0 Mask: 255.255.255.0	WAN: 172.25.24.45 LAN: 192.168.2.0 Mask: 255.255.255.0	WAN: 172.25.24.202 LAN: 192.168.3.0 Mask: 255.255.255.0

**B Company:**

Device Name	BHQZW70	BRZW2Plus
Device Type	ZyWALL70	ZyWALL2 Plus
Administrator	Tom	
IP Address	WAN: 172.25.24.90 LAN: 192.168.1.0 Mask: 255.255.255.0	WAN: 172.25.24.24 LAN: 192.168.2.0 Mask: 255.255.255.0

**Vantage server:**

	CNM server	FTP server
Administrator	root	
IP Address	WAN: 172.25.24.119 Mask: 255.255.255.0	WAN: 172.25.24.119 Mask: 255.255.255.0

Please note that Vantage can only manage ZyXEL devices which support CNM (Central Network Management). You can check if your ZyXEL devices support Vantage from Users Guide/Data Sheet which is available on ZyXEL WEB site (<http://www.zyxel.com>) or you can go to the devices' SMT menu, and issue this command **cnm**, for those devices which support CNM, you can get the following result.

```

ras> cnm
active    sgid      managerlp  debug
reset     encrykey  encrymode  keepalive
version tr069
    
```

In the following, we are going to show how to configure Vantage and ZyXEL devices step by step.

## 1.5 Domain Control of devices & accounts

Before proceeding, please login to Vantage server via typing this URL <http://<vantage server's IP>>. In this example, it should be <http://172.25.24.119:8080>. The default User Name and Password are **root/root**, users can change the default password later.

To complete this application, users need to finish the following items step by step.

**Account Setup:** Define different user privileges for John in A Company and in B Company. Account **root** can manage the whole Vantage operations and security appliances.

**Folder Setup:** Define different group folder for different companies and different



branch offices and associate each folder to the corresponding manager.

**Device Registration:** Register the managed devices to Vantage, and associate the device manager to each device.

It may take several seconds to load Java applet. Please wait until the root icon appears in the left frame of Vantage window. Make sure you have focus on one icon in the left frame of Vantage window, every time before you would like to configure Vantage server, so that the links on control panel can be shown and clicked.

### 1.5.1 Account Setup

1. Create a super user - **John**, to manage the whole Vantage operations and security appliances in headquarter.
  - a. Click **SYSTEM>>Administrators>>Add** button.
  - b. Let UID=**John**, Password=**1234**, and fill in the fields of E-mail address, Contact address, Telephone Number and Note. Click **Next** button
  - c. Select User Group=**Super**, then click **Apply** button.

**Note:** Privilege Group **Normal** will make this administrator account could only do some basic configuration. You could also select **Custom** to choose the permissions for this administrator account.

2. Create a super user - **Tom**, to manage the whole Vantage operations and security appliances in headquarter:
  - a. Click **SYSTEM>>Administrators>>Add** button.
  - b. Let UID=**Tom**, Password=**1234**, and fill in the fields of E-mail address, Contact address, Telephone Number and Note. Click **Next** button.
  - c. Select User Group=**Super**, then click **Apply** button.

After you complete, you should get administrators list like this,

System >> Administrators					
System : View Administrator List					
#	Index	Name	Login ID	Status	Description
	1	root	<u>root</u>	enable:login	DEFAULT USER
<input type="checkbox"/>	2	Tom	<u>Tom</u>	enable:logout	administrator in HQ of B Company
<input type="checkbox"/>	3	John	<u>John</u>	enable:logout	administrator in HQ of A Copmany

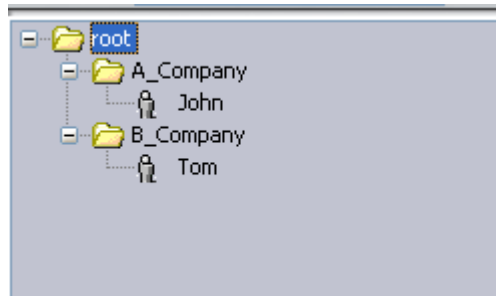
Add Delete

### 1.5.2 Folder Setup

1. Create group folder for A Company
  - Right click on **Root>>Add Folder>>Add Group Folder**; give this group folder a name, **A\_Company**.
  - Right click on **Root>>Associate**, select **John** from the popped out association list.

2. Create group folder for B Company.
  - Right click on **Root>>Add Folder>>Add Group Folder**; give this group folder a name, **B\_Company**.
  - Right click on **Root>>Associate**, select **Tom** from the popped out association list.

After you complete, you should be able to get the following Object Tree in Main View type.

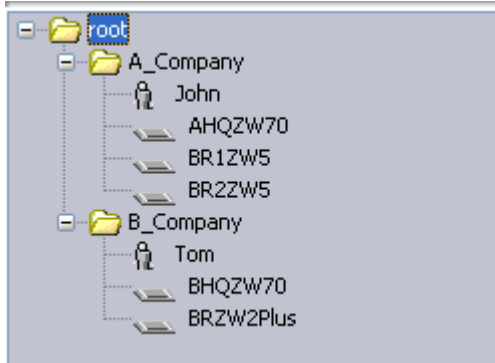


### 1.5.3 Device Registration

1. Add 3 ZyWALL devices in folder **A\_Company**.
  - Click **A\_Company** icon on OTV (Object Tree View). On right side, select **DEVICE>>Registration**.
  - Select **No**, for not to associate the device to a customer, then click **Next**. Select **Manual Add**, and click **Next**
  - Input the MAC address of LAN interface of ZyWALL70 in HQ.
  - Give this device a name, **AHQZW70**.
  - Select the corresponding Device Type, click **Apply**
  - Input the MAC address of LAN interface of ZyWALL5 in branch 1.
  - Give this device a name, **BR1ZW5**.
  - Select the corresponding Device Type, click **Apply**
  - Input the MAC address of LAN interface of ZyWALL5 in branch 2.
  - Give this device a name, **BR2ZW5**.
  - Select the corresponding Device Type, click **Apply**
  - If you have multiple devices, please repeat the above steps until all devices are added.
2. Add 2 ZyWALL devices in folder **B\_Company**
  - Choose **B Company** icon in Object Tree, select **DEVICE>>Registration**
  - Select **No**, for not to associate the device to a customer, then click **Next**. Select **Manual Add**, and click **Next**.
  - Input the MAC address of LAN interface of **ZyWALL70 in HQ**.
  - Give this device a name, **BHQZW70**.
  - Select the corresponding Device Type, click **Apply**
  - Input the MAC address of LAN interface of **ZyWALL2 Plus** in Branch.

- Give this device a name, **BRZW2Plus**.
- Select the corresponding Device Type, click **Apply**
- If you have multiple devices, please repeat the above steps until all devices are added.

After finishing the above 2 items, you should get OTV on the left frame like this,



### 1.5.4 Enable/Setup Vantage Function on ZyXEL Devices

Vantage CNM is disabled on the device by default. There are two ways to enable Vantage function on ZyXEL Devices.

#### 1. SMT menus

Please telnet to ZyXEL devices and go to SMT menu 24.8, then issue the following commands.

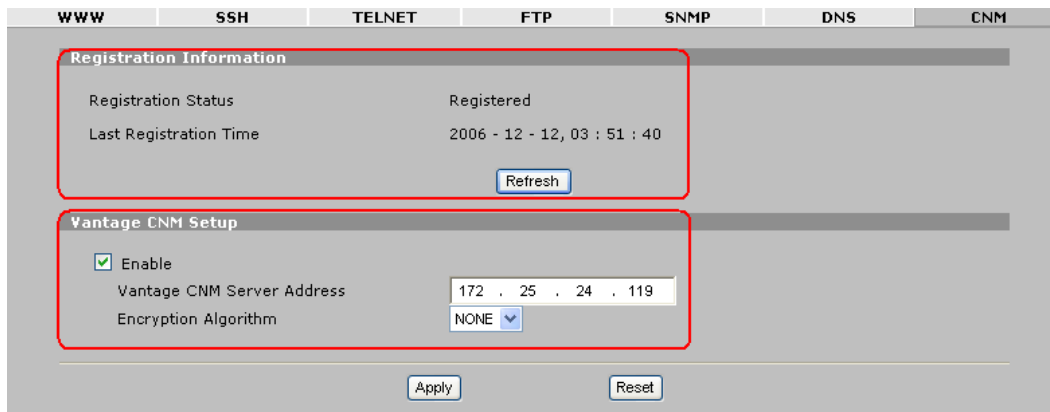
```

ras> cnm active 1
ras> cnm managerIp 172.25.24.119
    
```

172.25.24.119 is Vantage Server's IP address.

#### 2. WEB GUI Configuration

Login to the GUI interface of ZyXEL devices and go to **ADVANCED>>REMOTE MGMT** in the navigation panel and then click **CNM** tab to configure your device's Vantage CNM settings.

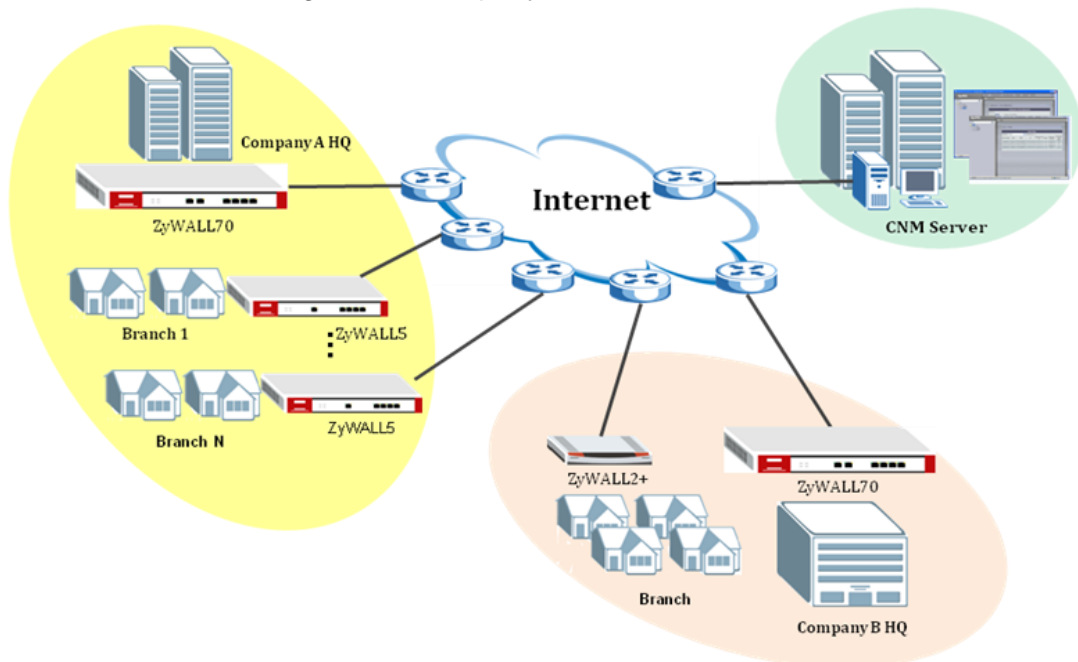


In **Registration Status** field, it displays **Registering** when the ZyXEL device first connects with the Vantage server and then **Registered** after it has been successfully registered with the Vantage server. **Last Registration Time** displays the last date and time that the ZyXEL device registered with the Vantage server. Enter the Vantage server's IP to **Vantage CNM Server Address** field, select **Enable** check box, and click Apply to enable Vantage function.

## 1.6 UTM Management

As for the detailed information about the whole scenario, please refer to [1.4 A scenario for Vantage application](#).

A Company is a medium-sized company with 300 employees. There are N branches all over the country. Almost 80 percents of A Company's employees need to use the Internet in daily work. They would like to use UTM function to protect their network and want to maintain the devices centrally. They also need a report about the UTM and the Internet usage of the company.



### 1.6.1 Centralized License Management

#### 1.6.1.1 Device Registration & License Activation/Upgrade

Select the device which needs to be registered, then go to **Device>>Service Registration**, you can see the **Service Registration** page. The selected device registration status will be shown in this page.

If the device is not registered, select **New myZyXEL.com account** and enter the corresponding info needed to register the device as below. Click **Apply**.

**Service Registration**

Registration    Service

Device Registration

The device is not registered

New myZyXEL.com account     Existing myZyXEL.com account

User Name    ACompanyJohn \*        User Name is available.

Password    ●●●●●● \*    (Type username and password from 6 to 20 characters.)

Confirm Password    ●●●●●● \*

E-Mail Address    sherry.liu@zyxel.cn \*

Country    China \*   

Service Activation

Content Filtering 1-month Trial

Anti Spam 3-month Trial

IDP/AV 3-month Trial

**Service Registration**

Registration    Service

Device Registration

Registration is going on, please wait..

New myZyXEL.com account     Existing myZyXEL.com account

User Name    ACompanyJohn \*

Password    ●●●●●● \*

Confirm Password    ●●●●●● \*

E-Mail Address    sherry.liu@zyxel.cn \*

Country    China \*   

Service Activation

Content Filtering 1-month Trial (Service has been activated.)

Anti Spam 3-month Trial (Service has been activated.)

IDP/AV 3-month Trial (Service has been activated.)

Wait for a few minutes until you see **User Name** and **Password** fields turn to grey. It shows that the device has been registered successfully.

**Service Registration**

Registration    Service

Device Registration

Existing myZyXEL.com account

User Name    ACompanyJohn \*

Password    ●●●●●● \*

Service Activation

Content Filtering 1-month Trial (Service has been activated.)

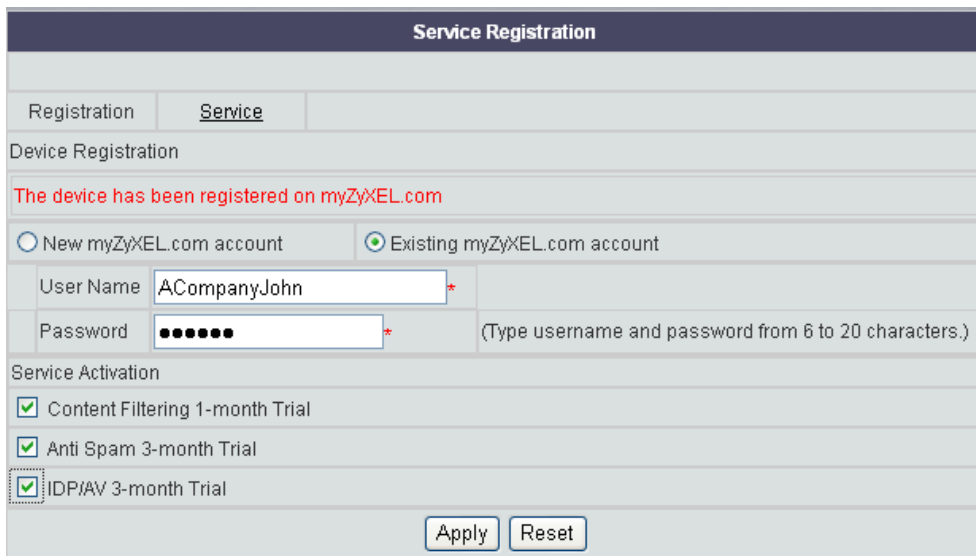
Anti Spam 3-month Trial (Service has been activated.)

IDP/AV 3-month Trial (Service has been activated.)

Go to **Service Registration>>Service**, you can find the services (**CF, AS** and **AV**) are activated. Also you can update your **license key** or refresh your **service license** in this page.



If you already have an account exist in myZyXEL.com, then all you have to do is select **Existing myZyXEL.com account** and enter your username password, select IDP/AV and AS 3 months trial version to activate.



All the devices in A Company can be registered in Vantage server, just repeat the above steps.

**1.6.1.2 License Monitor to view license status of all devices**

Go to **Monitor>>License Monitor**, you can see the detailed information of the UTM service status in all the devices which have registered to Vantage sever. Also you can **Refresh/Active/Update** your service license in this page.

License Monitor						
All Service <input type="button" value="v"/>						
Device	Refresh	Service	Status	Registration Type	Expiration Day	Activate/Upgrade
WrootA_CompanyBR2ZW5 (001349D429B0)	<input type="button" value="Refresh"/>	AV/IDP	Inactive	-	-	-
		AS	Inactive	-	-	-
		CF	Inactive	-	-	-
WrootB_CompanyABHQZW70 (0013493ABDFE)	<input type="button" value="Refresh"/>	AV/IDP	Active	Standard	2007-03-22	<input type="button" value="Upgrade"/>
		AS	Active	Standard	2007-05-16	<input type="button" value="Upgrade"/>
		CF	Active	Standard	2007-02-09	<input type="button" value="Upgrade"/>
WrootA_CompanyBR1ZW5 (00134984660F)	<input type="button" value="Refresh"/>	AV/IDP	Active	Standard	2008-04-11	<input type="button" value="Upgrade"/>
		AS	Active	Standard	2008-04-11	<input type="button" value="Upgrade"/>
		CF	Active	Standard	2007-11-13	<input type="button" value="Upgrade"/>
WrootA_CompanyAHQZW70 (00134907188E)	<input type="button" value="Refresh"/>	AV/IDP	Active	Standard	2007-06-16	<input type="button" value="Upgrade"/>
		AS	Active	Standard	2007-06-09	<input type="button" value="Upgrade"/>
		CF	Active	Standard	2007-06-20	<input type="button" value="Upgrade"/>

### 1.6.1.3 License Expire Notification

If your ZyXEL device's license has been expired, you can find the expired information in Vantage.

Go to **Monitor>>License Monitor**, the detailed information of the UTM service status in all the devices which have registered to Vantage sever will be shown in this screen. Below sample shows the license information of BR1ZW5. You can find that service **AV/IDP** and **CF** has been expired, and the **Status** of them is **Inactive**. You can check up the device expiration time from **Expiration Day** list.

License Monitor						
All Service <input type="button" value="v"/>						
Device	Refresh	Service	Status	Registration Type	Expiration Day	Activate/Upgrade
WrootA_CompanyBR1ZW5 (001349442572)	<input type="button" value="Refresh"/>	AV/IDP	Inactive	Trial	2006-07-03	<input type="button" value="Upgrade"/>
		AS	Active	Standard	2007-11-08	<input type="button" value="Upgrade"/>
		CF	Inactive	Trial	2006-05-04	<input type="button" value="Upgrade"/>

## 1.6.2 Policy Enforcement

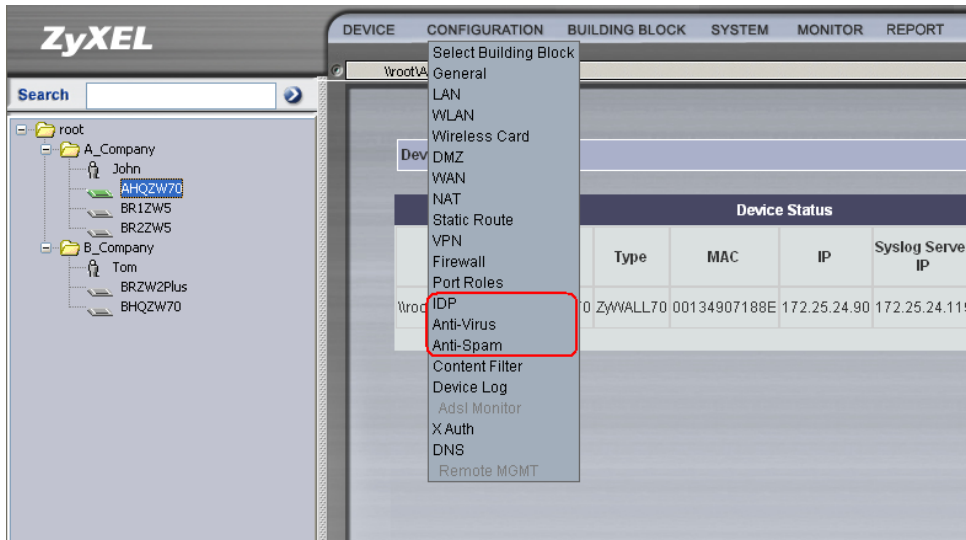
The ZyWall UTM is designed to protect network-based security. It functions to protect networks from intrusions/Virus/Spams while allowing safe Internet access. In Vantage, you can create your own rules for ZyXEL devices according to the applications in your network.

### 1.6.2.1 Configure UTM policy

Jim can configure **UTM (IDP, Anti-Virus, Anti-Spam)** in Vantage sever. Below list

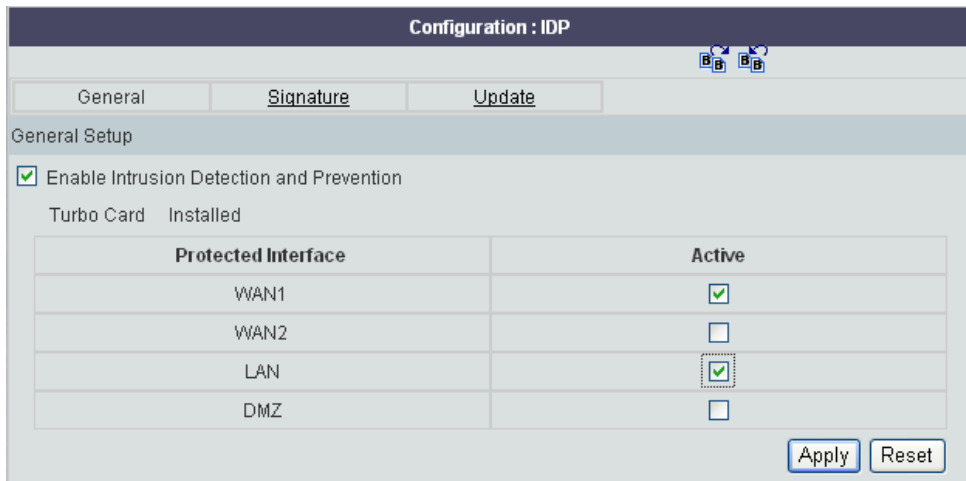
the steps of configuration about IDP for AHQZW70.

**Note:** Your device must have a turbo card installed to use the IDP feature.




Step 1. Go to **Configuration>>IDP**, you can see the **IDP>>General** screen as shown next. It is the same as the IDP configuration page in GUI except the **Backup & Restore** field.

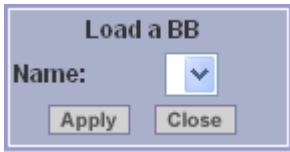
Step 2. Check **Enable Intrusion Detection and Prevention** check box to enable IDP function, active WAN1 and LAN **Protected Interfaces**, and click **Apply** to save the settings.




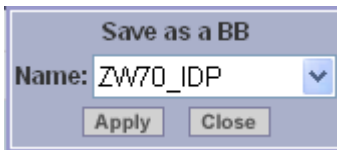
You can see these two icons (, ) showed in this page.

Click , you can load an existed BB(Building Block) of IDP **General Setup** to your device. If there is not any existed BB of IDP available, the **Name** field will be blank.





Click , you can save your IDP **General setup** as a new configuration BB and it is then available to apply to other devices of the same type. You should enter a name for this new BB in the **Name** field as showed below.

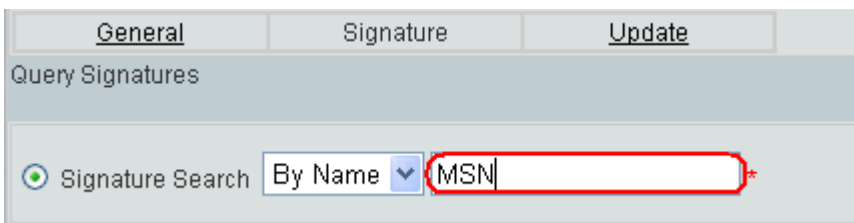


You can find the configuration BB you just saved for IDP **General Setup** in **Building Block>>Configuration BB**.

Building Block >> Configuration BB						
Building Block : Configuration BB						
	Index	Name	Model	Firmware	Feature	Note
<input type="checkbox"/>	1	ZW70_IDP	ZyWALL70	4.00	Idp	A_Company_HQZW70

Add Delete

Step 3. Go to **IDP>>Signature**, configure signatures according to your application. Here A Company would like to block MSN utilization to ensure maximum productivity for all 300 employees. Click **Switch to query view**, Query Signatures screen will be shown next. Enter MSN to **Signature Search** field. Click **Search**.



Step 4. All signatures refer to MSN will be shown in next shown screen. Set action for all to **Drop Session**, and then click **Apply**. Thus all the employees in HQ behind ZyWALL 70 can not log on MSN now.

Configure Signatures

Name	ID	Severity	Type	Platform	Active	Log	Alert	Action
CHAT.MSN.login.attempt	1050362	Low	IM		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Drop Session
CHAT.MSN.8.0.message	1050363	Low	IM		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Drop Session
CHAT.MSN.user.search	1050367	Low	IM		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Drop Session
CHAT.MSN.6.x.>4.x.file.transfer.request	1050935	Low	IM		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Drop Session
CHAT.MSN.6.x.login.attempt.<1024	1051207	Low	IM		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Drop Session
CHAT.MSN.6.x.message.<1024	1051240	Low	IM		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Drop Session
CHAT.MSN.login.via.hopster	1051251	Low	IM		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Drop Session
CHAT.Web.MSN.login.attempt-1	1051694	Low	IM		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Drop Session
CHAT.Web.MSN.login.attempt-2	1051695	Low	IM		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Drop Session
CHAT.Web.MSN.login.attempt-3	1051696	Low	IM		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Drop Session
Worm.MSN.funny	1051704	High	VirusWorm		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Drop Session
CHAT.MSN.8.0.message-2	1051719	Low	IM		<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Drop Session
Worm.Bropia.(MSN.file.transfer)-1	1051787	High	VirusWorm		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Drop Session
Worm.Bropia.(MSN.file.transfer)-2	1051788	High	VirusWorm		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Drop Session
Worm.Bropia.(MSN.file.transfer.via.HTTP)	1051789	High	VirusWorm		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Drop Session

1 2 Next 1/2 Go

Apply Reset

Step 5. Go to **IDP>>Update**, the detailed signature information in the device will be shown in the screen. You can update the IDP and Anti-Virus Signature to the latest version with the online update server manually or set update be done automatically, click **Apply** to save the settings.

You can load a configuration BB for **Update** setting to your device or save your **Update** setting as a new configuration BB just as introduced in **Step 2**.

Configuration >> IDP >> Update

Configuration : IDP

General Signature Update

Signature Information

Current Pattern Version: v1.314

Release Date: 2006-11-16

Last Update: N/A

Current IDP Signatures: 1950

Signature Update

Service Status: License Active

Expiration Date: 2007-06-16

Synchronize the IDP and Anti-Virus Signature to the latest version with the online update server.

Update Server: myupdate.zywall.zyxel.com Update Now

Auto Update

Apply Reset

**Note:** Remember to make sure the IDP AV signatures are most updated thereby the ZyWALL UTM engine can stay in the best status.

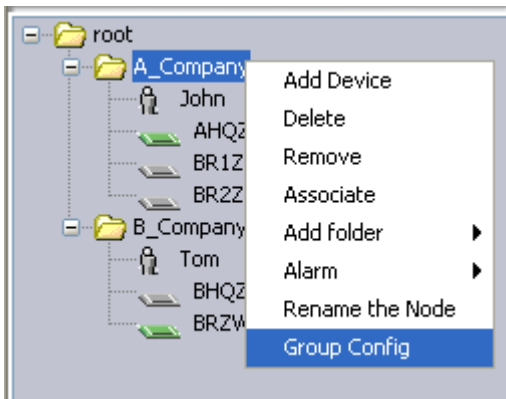
**1.6.2.2 Apply group configuration of UTM policy**

There are N branches of A Company all over the country. Jim would like to configure all these ZyWALL 5 in branches centrally since they have similar utilization refer to AV, AS, IDP, firewall and so on.

Vantage CNM group configuration is a way to configure batch devices which under a certain folder. Now Vantage CNM 2.3 can batch configure device's **General/AV/IDP/Firewall/AS/Signature Update/Device Log** feature. Below are detailed steps:

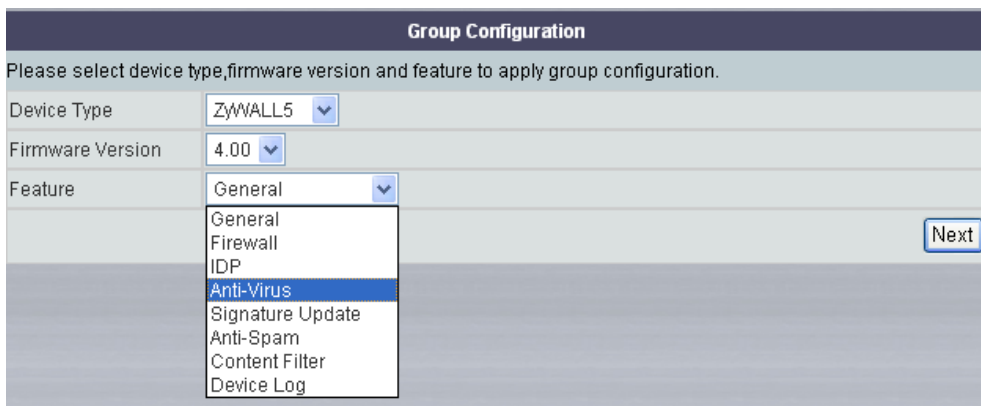
**Note:** only the administrator who has configured authority can do this job.

Step 1.Right click **A\_Company** icon and select **Group Config** in the popup menu. You can see the **Group Configuration** screen as shown next.



Step 2.You will be requested to select **Device Type**, **Firmware Version** and **Feature** to apply group configuration. Here should select **ZyWALL5**, **4.00** and take feature **Anti-Virus** for example, then click **Next** button.

**Note:** In **Device Type** field, it only shows the types in your selected group folder. In **A\_Company** group folder, it does not include ZyWALL 35 or ZyWALL2 Plus, so you can not find them in **Device Type** field.



Step 3.In next shown screen, all the device Name of the ZyWALL5 in all branches

of A Company will be listed. You should select the exact device you want to apply group configuration. Then click **Next** button.

**Group Configuration**

Please select devices to apply group configuration.

Device Type : ZyWALL5 | Firmware Version : 4.00 | Feature : Anti-Virus

	Index	Device Name	Turbo Card Status	License Status
<input checked="" type="checkbox"/>	1	WrootA_Company\BR2ZW5	Installed	Active
<input checked="" type="checkbox"/>	2	WrootA_Company\BR1ZW5	Installed	Active

Back Next

Step 4: In next shown Screen, you can **Create Building Block** to save your group configuration as a new configuration BB and it is then available to apply to other devices of the same type. Select **Existing Building Block**, you can load an existed BB of the selected feature setting to your device. Select **Reset Firewall Configuration to Default** will reset the firewall setting in your selected devices. Click Next button, you can see the **Configuration BB** screen as shown next.

**Note:** You must select the configuration BB of the same device type, feature and firmware as which you just selected for group configuration. In this example, **ZyWALL 70**, firmware **4.00** and feature **Firewall** is just selected, so you must load an existed BB for the same parameters.

**Group Configuration**

Please select Building Block templet or Reset to Default to apply group configuration.

Device Type : ZyWALL5 | Firmware Version : 4.00 | Feature : Anti-Virus

Select Building Block

- Create Building Block
- Existing Building Block None

Reset Anti-Virus Configuration to Default

Back Next

Step 5: In **Add/Edit Configuration BB** screen, type a **Name** to identify your Configuration BB and type some extra description of the BB in **Note** field. You can leave **Note** field as blank. For Create Mode, you can select **Create a BB Directly** to build a new one or select **Create a BB from another existed BB** to build your BB from an existed BB. Then click **Create** button to go to next screen.

Step 6: You can see **Configuration Firewall** screen will be shown next. You can configure firewall **Default Rule**, **Rule Summary**, **Anti-Probing**, **Threshold** and **Service** just as you configure them in device's Web GUI. After you configure all the parameters for the firewall, click **Save & Exit**.

Service	Active	Log	Alert	Protected Interface	Send Windows Message	Destroy File
FTP (TCP 20/21)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> LAN <input checked="" type="checkbox"/> WAN <input type="checkbox"/> DMZ	<input type="checkbox"/>	<input type="checkbox"/>
HTTP (TCP 80, 8080, 3128)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> LAN <input checked="" type="checkbox"/> WAN <input type="checkbox"/> DMZ	<input type="checkbox"/>	<input type="checkbox"/>
POP3 (TCP/UDP 110)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> LAN <input checked="" type="checkbox"/> WAN <input type="checkbox"/> DMZ	<input type="checkbox"/>	<input type="checkbox"/>
SMTP (TCP/UDP 25)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/> LAN <input checked="" type="checkbox"/> WAN <input type="checkbox"/> DMZ	<input type="checkbox"/>	<input type="checkbox"/>

Step 7: In this next shown screen, confirm the information for the group configuration including the **Device Type**, **Firmware Version**, **Feature** and **Building Block Name**, also the **Device Name** list. If all of them are correct, click **Apply** button to save the group configuration. The screen will come back as you can see in step 3. You can build another new group configuration.

Index	Device Name
1	\\rootA_Company\BR2ZW5
2	\\rootA_Company\BR1ZW5

**Group Configuration**

Please select device type, firmware version and feature to apply group configuration.

Device Type:

Firmware Version:

Feature:

Go to **Building Block>>Configuration BB**, you can see the group configuration BB you just created. Click the BB's **Name**, you can see the detailed info about this configuration BB and also you can change the current setting of the BB.

**Building Block : Configuration BB**

	Index	Name	Model	Firmware	Feature	Note
<input type="checkbox"/>	1	<a href="#">ZyW70_IDP</a>	ZyWALL70	4.00	Idp	A_Company_HQZW70
<input type="checkbox"/>	2	<a href="#">ZyWALL5_AV</a>	ZyWALL5	4.00	Anti-Virus	A_Company_BRZW5

### 1.6.2.3 Signature backup and restore for these ZyXEL devices

Go to **Device>>Signature Profile**, you can see the **Signature Backup & Restore** screen as shown below:

**Signature Backup & Restore**

Backup & Restore | Management

Select Type

IDP  Anti-Virus

**Backup Configuration**

Click Backup to save the current configuration of IDP to server or your computer.

Destination:  To Server

File Name:

Description:

To Computer

**Restore Configuration**

To restore a previously saved IDP configuration file to your system, browse to the configuration file and click Upload.

Resource:  From Server

File Name:

From Computer

File Path:

**Back to Factory Defaults**

Click Reset to clear all user-entered IDP configuration information and return to factory defaults.

In **Select Type** field, there are two items: IDP and Anti-Virus. In ZyNOS 4.00, only

**IDP** can be selected. In ZyNOS 4.01, **Anti-Virus** check box is available.

In **Backup Configuration** field, click **Backup** to save the current configuration of IDP/AV to server or your computer.

If you select **To Server**, a file name for the backup configuration file will be needed.

If you select **To Computer**, you should assign the path to save the backup configuration file.

In **Restore Configuration** field, to restore a previously saved IDP configuration file to your system, browse to the configuration file and click **Upload**.

In **Back to Factory Defaults** field, Click **Reset** to clear all user-entered IDP configuration information and return to factory defaults.

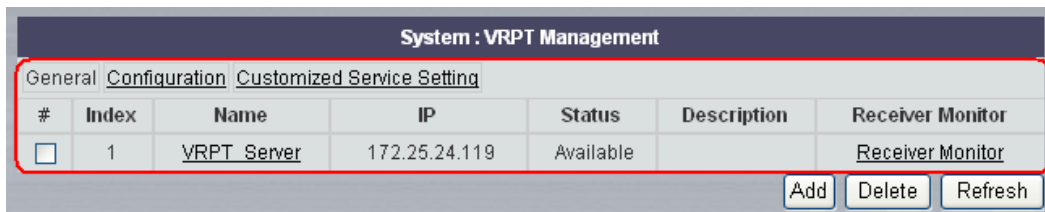
### 1.6.3 Read UTM report for all the devices in the network

ZyWALL's UTM function, coupled with Vantage's remote access reporting facility, M company can ensure hackers are locked out at entry point and A Company and B Company can carry on their daily jobs in a security environment, giving them peace of mind and putting them ahead of their competitors.

#### 1.6.3.1 Set the VRPT server for all the devices in the Network

You should make sure the configuration of **VRPT Management** has been done and the VRPT server is available. Please refer to [1.9.3.1 Setting VRPT server for managed devices](#).

When the setting has been done, you can see the current status of the VRPT server you just configured in next shown screen. Also you can configure more parameters for your VRPT server in **Configuration** and **Customized Service Setting** fields.



#### 1.6.3.2 Viewing UTM Report

ZyWALL's UTM function, coupled with Vantage's remote access reporting facility, M company can ensure A Company to carry on their daily jobs in a security environment, giving them peace of mind and putting them ahead of their competitors.

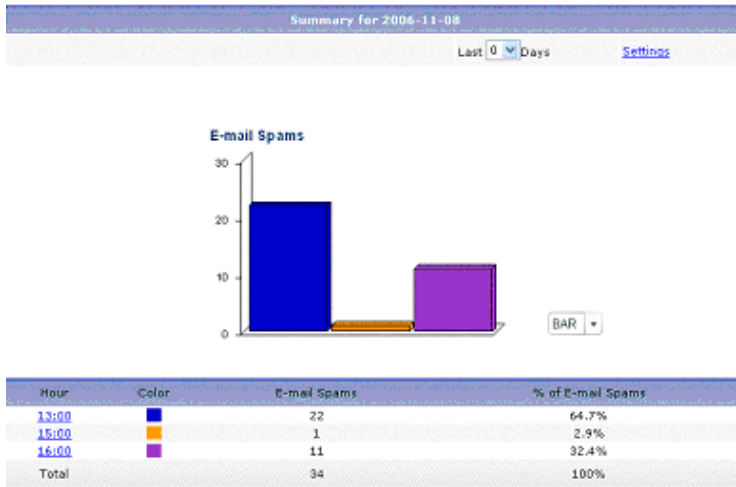
Take **AntiSpam** Report for example. For more UTM report, please see [1.9.3.2 Viewing report of managed devices>>UTM Report](#).

**Note:** John said:” I have a host of people troop into my office to complain about the Spam issue. We have to mainly use emails to develop our business, but when our employees start to receive fifteen to twenty junk mails everyday, it does take a long time to distinguish them out from those formal ones. Jim can resolve this issue well by using ZyWALL's Anti-Spam function and Vantage report to block Spam mails and trace the sender and source of the Spam mails.

**Note:** To look at anti-spam reports, each ZyXEL device must record anti-spam messages in its log. Refer to the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs>>Log Settings**, and make sure **Anti-Spam** is enabled.

For **AntiSpam Summary** report, administrator can look at the number of spam messages by time interval.





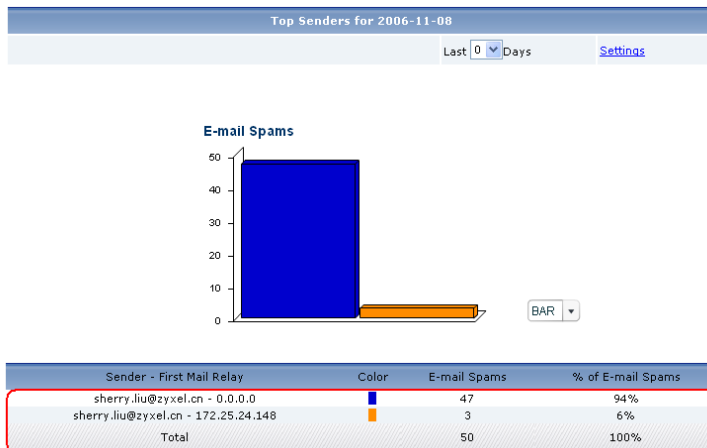
Click **settings**, the **Report Display Settings** screen appears. You can select a specific **Start Date** and **End Date** for your report. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System>>General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.

**Report Display Settings**

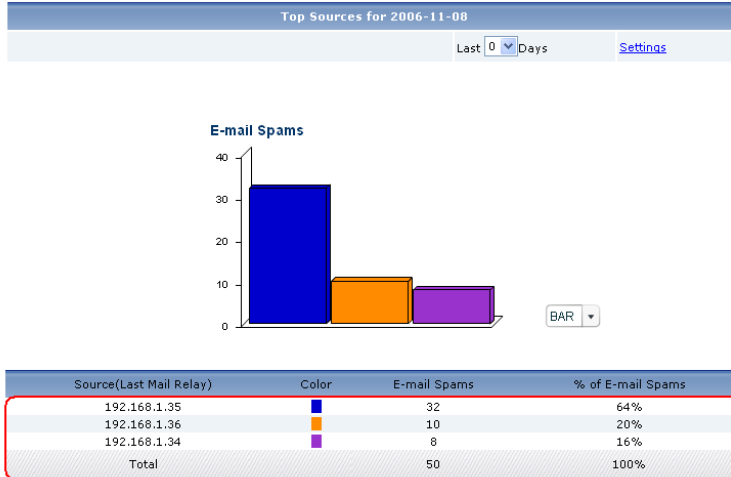
Start Date:	<input type="text" value="2006-11-08"/> <span style="float: right; font-size: small;">📅 *</span>
End Date:	<input type="text" value="2006-11-08"/> <span style="float: right; font-size: small;">📅 *</span>
<input type="button" value="Apply"/> <input style="margin-left: 100px;" type="button" value="Cancel"/>	

For **Top Senders** report, administrator could look at the top combinations of senders of spam messages and the first SMTP server to which the sender sends spam.

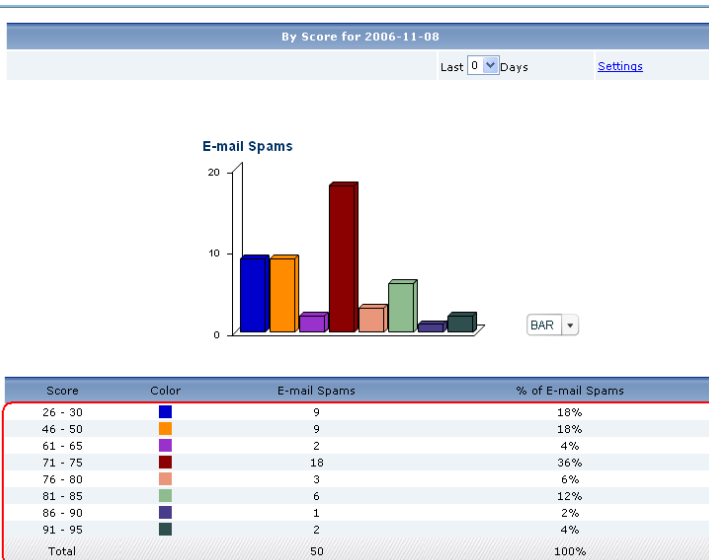
Administrator could block the senders if the senders are in the **Top Senders** report or block such spam mails address by adding them into blacklist.



For **Top Sources** report, administrator could look at the top sources of spam messages by number of messages and block such IP addresses by adding firewall rules. Please notice the direction of the firewall rules.



For **By Score** report, administrator could look at the top scores calculated for spam messages and then determine reasonable score threshold to control the quantity of spam mail on ZyWALL. .



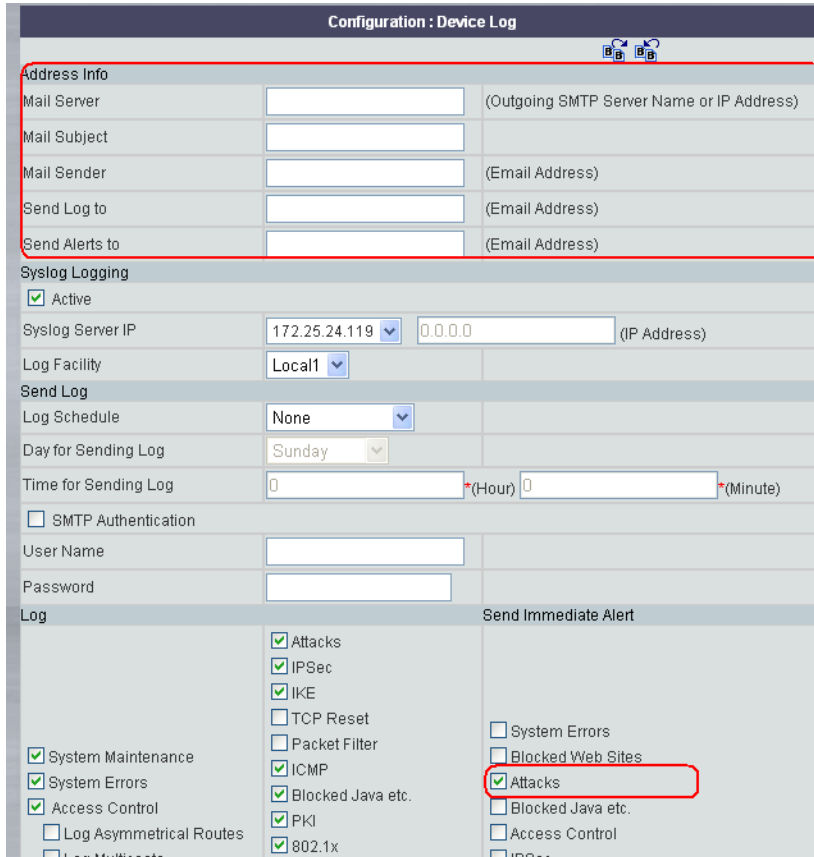
### 1.6.4 Alarm Monitoring and Alerting

M company can monitor that whether there is someone or attackers threat the network security in A Company and B Company in Vantage and take some effect measures to resolve the troubles.

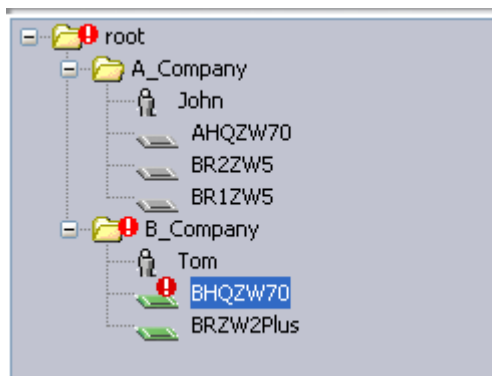
An alert is a type of log that warrants more serious attention. They include system errors, attacks and attempted access to blocked web sites or web sites with restricted web features such as cookies, active X and so on. Below is an example shows how to see alarm report in Vantage.

### 1.6.4.1 Alarm Monitor

Go to **Configuration>>Device Log**, select **Attacks** in **Send immediate Alert**. In **Address Info** field, you can set in your **Mail Server** and **Email Address** to let the log be sent to your mailbox. If this field is left blank, alerts will not be sent via e-mail.



Then when a device is under attack, a red exclamation mark will show up on device icon. And the status will be changed from **“On”** to **“On\_Alarm”**.

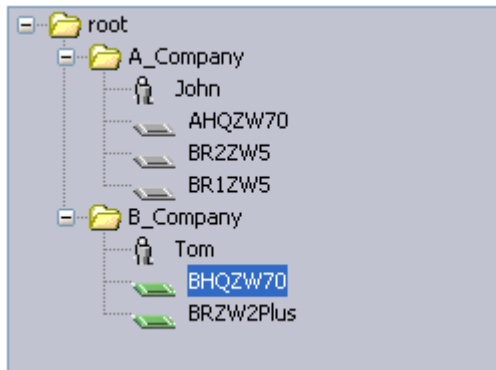


Device Status							
Device Name	Type	MAC	IP	Syslog Server IP	Status	Firmware Version	Extension Card Status
\\root\B_Company\BHQZW70	ZyWALL70	00134907188E	172.25.24.90	172.25.24.119	On_Alarm	4.00 (WM.11)	Turbo Card

Go to **Monitor>>Alarm>>Current**, administrator can see more detailed info about the Alarm.

Index	Device Name	Category	Severity	Time	Message	Responder	Response Time	Clear
1	BHQZW70		!	2006-11-17 17:14:21	ip spoofing - WAN UDP	Respond		Clear
2	BHQZW70		!	2006-11-17 17:14:16	ip spoofing - WAN UDP	Respond		Clear
3	BHQZW70		!	2006-11-17 17:14:04	ping of death. ICMP (Echo)	Respond		Clear
4	BHQZW70		!	2006-11-17 17:13:58	ip spoofing - WAN UDP	Respond		Clear
5	BHQZW70		!	2006-11-17 17:13:53	ping of death. ICMP (Echo)	Respond		Clear

Click **Clear All**, all of the Alarm info will be deleted and the red exclamation mark will disappear in the **MainView**.

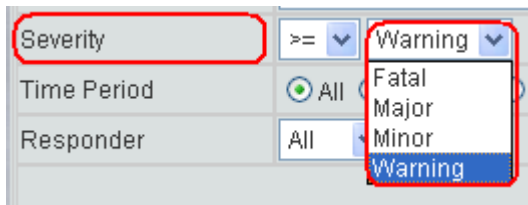


### 1.6.4.2 Alarm Search

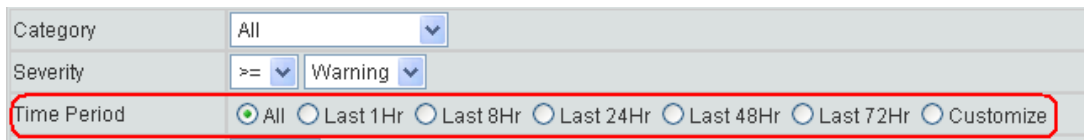
In **Category** field, administrator can select the category for the alarms which he wants to search.



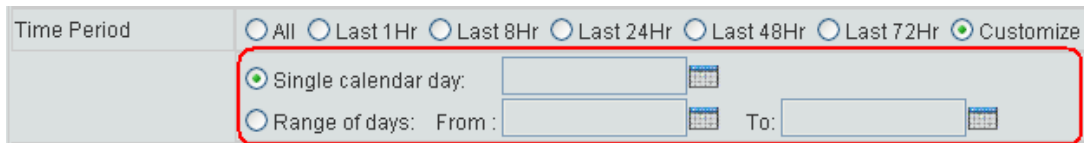
In **Severity** field, administrator can select the severity level for the alarms which he wants to search. If Warning is selected, all the alarms will be displayed in this screen.




In **Time Period** field, administrator can select the alarms happened in a specific time period, such as **Last 1 Hr**, **Last 8 Hr** and so on.



Administrator can customize the exact time period via selecting the **Customize** check box.



Click icon  , a calendar screen will be popped out, administrator can select a specific day for a range of days for the alarms he wants to search.



Go to **Monitor>>Alarm>>Historical**, if the **Device** check box in **Type** field is selected, all alarms the device has received will be displayed in this screen. Administrator can find the device information in **Device/Group** field automatically. Administrator also can search the alarms in this screen as we mentioned above.

**Monitor : Alarm**

Current  Historical

Type  Device  CNM

Device/Group  All  Device/Group(Name) \root\B\_Company\BHQZY

Category All

Severity >= Warning

Time Period  All  Last 1Hr  Last 8Hr  Last 24Hr  Last 48Hr  Last 72Hr  Customize

Responder All

Retrieve

Index	Device Name	Category	Severity	Time	Message	Responder	Response Time
1	BHQZW70		!	2006-11-17 17:13:53	ping of death. ICMP (Echo)		
2	BHQZW70		!	2006-11-17 17:13:58	ip spoofing - WAN UDP		
3	BHQZW70		!	2006-11-17 17:14:04	ping of death. ICMP (Echo)		
4	BHQZW70		!	2006-11-17 17:14:16	ip spoofing - WAN UDP		
5	BHQZW70		!	2006-11-17 17:14:21	ip spoofing - WAN UDP		
6	BHQZW70		!	2006-11-17 17:15:22	ip spoofing - WAN UDP		

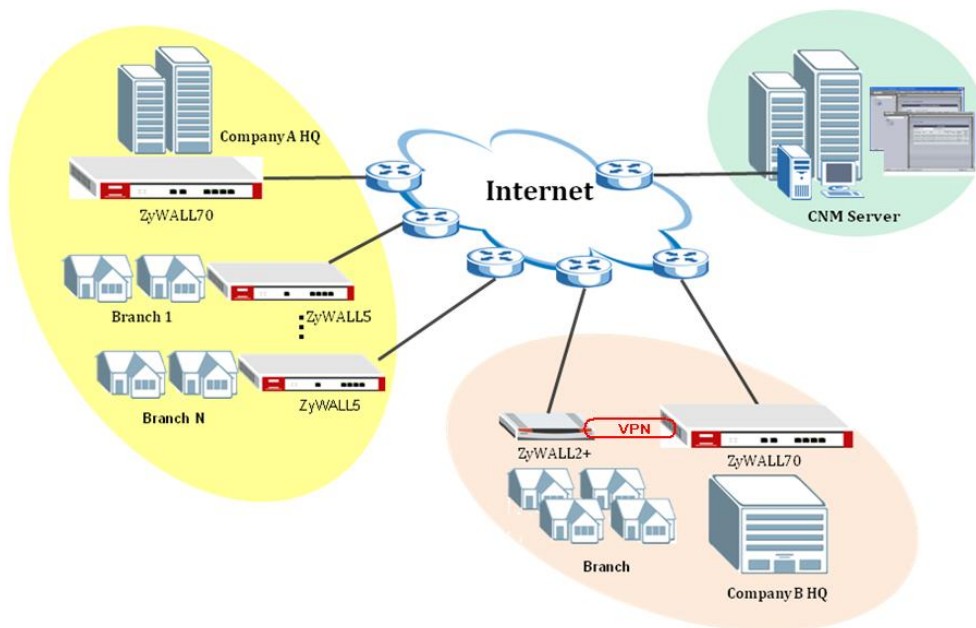
If the **CNM** check box in **Type** field is selected, all alarms of all devices registered to Vantage will be displayed in this screen.

Monitor : Alarm								
Current		Historical						
Type	<input type="radio"/> Device <input checked="" type="radio"/> CNM							
Severity	>= Warning <ul style="list-style-type: none"> <li>Fatal</li> <li>Major</li> <li>Minor</li> <li>Warning</li> </ul>							
Time Period	<input checked="" type="radio"/> All <input type="radio"/> Last 8Hr <input type="radio"/> Last 24Hr <input type="radio"/> Last 48Hr <input type="radio"/> Last 72Hr <input type="radio"/> Customize							
Responder	<input type="radio"/> All <input checked="" type="radio"/> Warning							
Retrieve								
Index	Source	Category	Severity	Time	Message	Responder	Response Time	
1	BRZW2Plus		!	2006-11-17 17:22:12	ping of death. ICMP(Echo)			
2	BRZW2Plus		!	2006-11-17 17:22:22	ping of death. ICMP(Echo)			
3	BRZW2Plus		!	2006-11-17 17:20:27	ping of death. ICMP(Echo)			
4	BRZW2Plus		!	2006-11-17 17:20:38	ping of death. ICMP(Echo)			

## 1.7 VPN Management

### 1.7.1 Creating VPN tunnel by VPN Editor (One-click VPN)

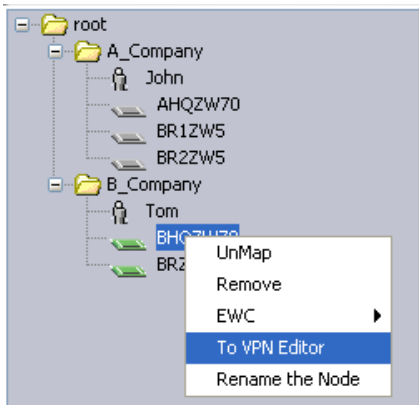
As for the detailed information about the whole scenario, please refer to [1.4 A scenario for Vantage application](#).



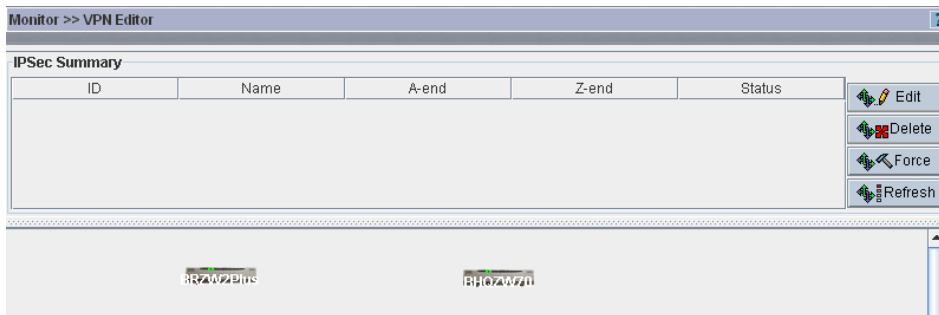
B Company is a small-sized company with only one branch in another city. They want to share their resources and information across HQ and Branch without compromising their security. Administrator in M can use One Click VPN feature to realize this security application in B Company. Below list the steps to show how to build up a VPN tunnel between HQ and branch.

Step 1. Right clicks **BHQZW70's** icon and select **To VPN Editor** in the popup

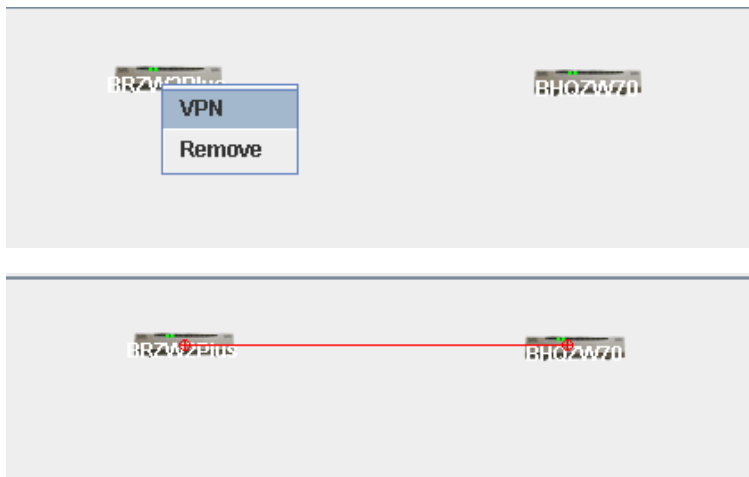
menu.



Step 2. Right-click **BRZW2Plus's** icon and select **To VPN Editor** in the popup menu, you can see the **VPN Editor** screen as shown next.



Step 3. Right-click **BRZW2Plus's** icon and select **VPN** in the popup menu. Click the icon again and drag (you should see a red line) to **BHQZW70**, then release the mouse button.



Step 4. You can see the **Tunnel IPSec Detail** screen as shown next. Note that information in some fields has been automatically generated for you when you configure VPN this way. You can change the automatically configured information to set up the tunnel.

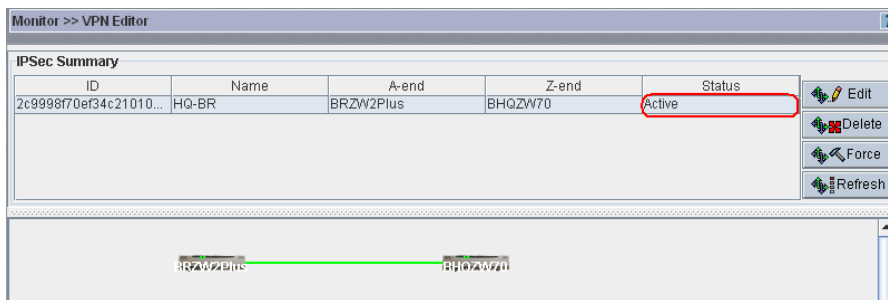
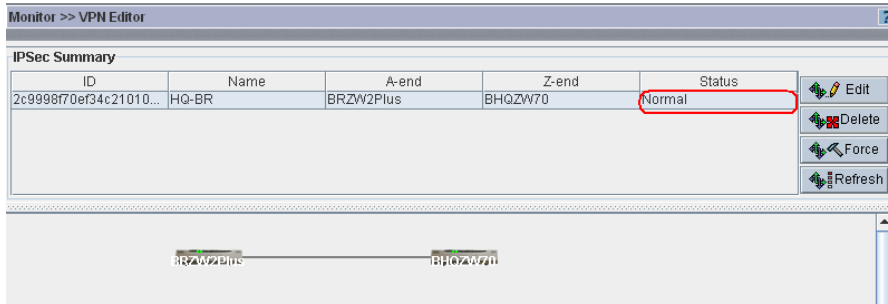


Step 5. Click **Apply** to go to an **IPsec summary** screen. The Tunnel Summary shows the **Name** of your tunnel, **A-End** and **Z-End** devices and the current tunnel **Status**.

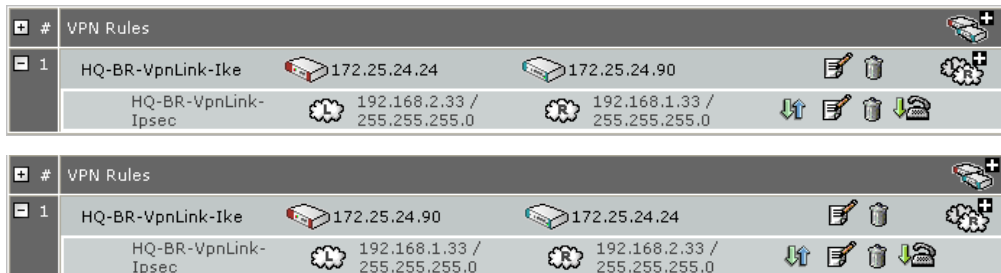
You can see a gray dashed line between the devices. It means that the Vantage server has not yet synchronized VPN tunnel information with both devices.

ID	Name	A-end	Z-end	Status
2c999870ef34c21010...	HQ-BR	BRZW2Plus	BHQZW70	To_be_created

When the status changes to **Normal**, you can see a gray solid line showed between the devices icon. It means that the VPN tunnel is set up between the devices but the tunnel is not active yet (no traffic). When there is traffic in the tunnel, the line will turn green and current tunnel **Status** is **Active**.



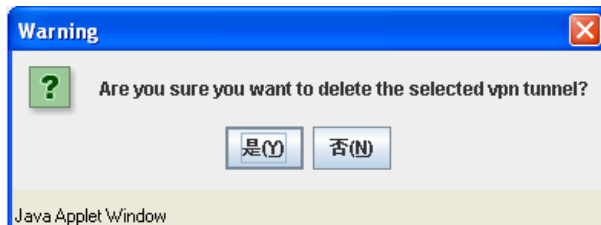
When finishing the connection of the security tunnel, you can check the same scene in the WEB GUI as follows.



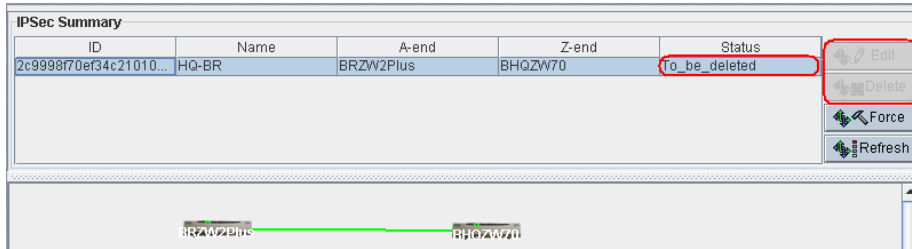
One day, B Company think that the tunnel is not necessary any more or when there are somebody can threaten the security for this tunnel, administrator can delete the tunnel conveniently in Vantage.

### 1.7.1.1 Use delete button to delete a tunnel

Select the exact ID of the tunnel which should be deleted, click **Delete**, a warning screen will be popped out. Click **Y** to delete the selected tunnel.



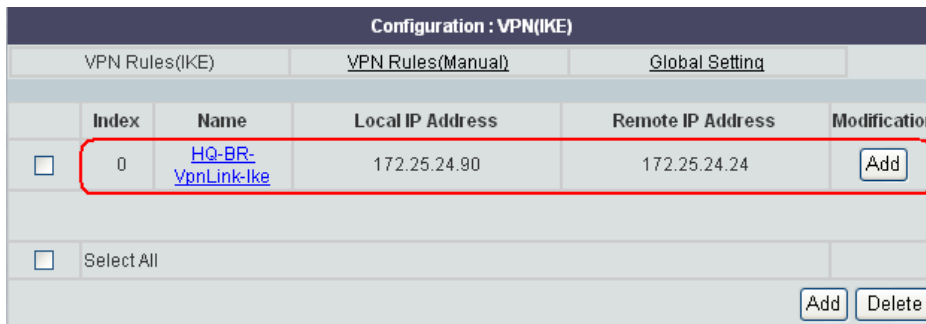
You will see the **Edit** and **Delete** fields are turned grey and the status of this tunnel in **IPsec Summary** is change to **To\_be\_deleted**.



Wait for a few seconds, you will find that the **Edit** and **Delete** fields are available again. The info about the tunnel you deleted just now and the green solid line between the two gateways are all disappeared.



Select one of the gateway **BHQZW70**'s icon and go to **Configuration>>VPN**, you can find all parameters of phase 2 are deleted. That means the tunnel has been deleted successfully.



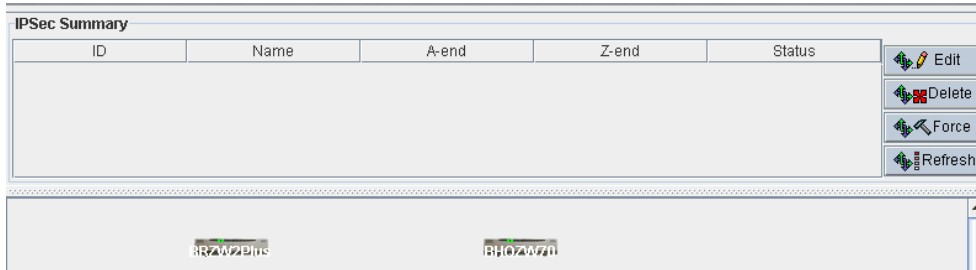
**Note:** When you use **Delete** button to delete a tunnel, both the two gateways of this tunnel should be online. Only when Vantage server receives the reply from both of the gateways, the tunnel can be deleted successfully. If one of them is offline, the tunnel can not be deleted until the gateway is online again.

**1.7.1.2 Use Force button to delete a tunnel**

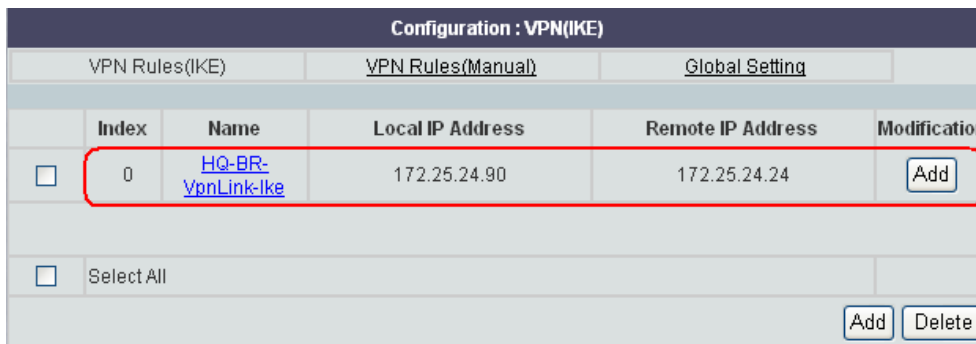
Select the exact ID of the tunnel which should be deleted, click **Force**, a warning screen will be popped out. Click **Y** to delete the selected tunnel.



You will find that all the info about the tunnel you deleted just now and the green solid line between the two gateways are disappeared at once.



Select one of the gateway **BHQZW70's** icon and go to **Configuration>>VPN**, you can find all parameters of phase 2 are deleted.



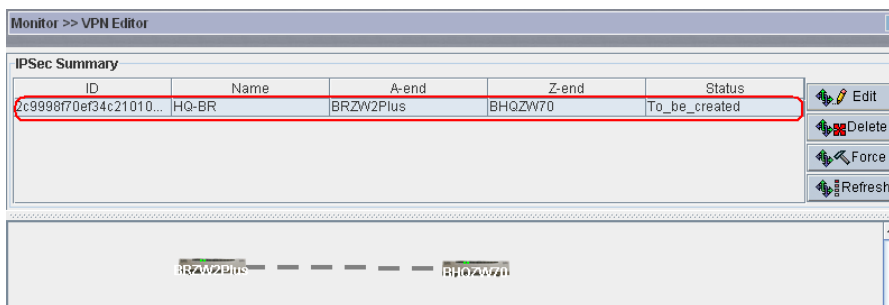
**Note:** When you use **Force** button to delete a tunnel, the tunnel will be deleted at once, no matter whether the gateway is online. If one of them is offline, the VPN configuration will be changed when it is online again.

### 1.7.2 Monitor Status of VPN Tunnel

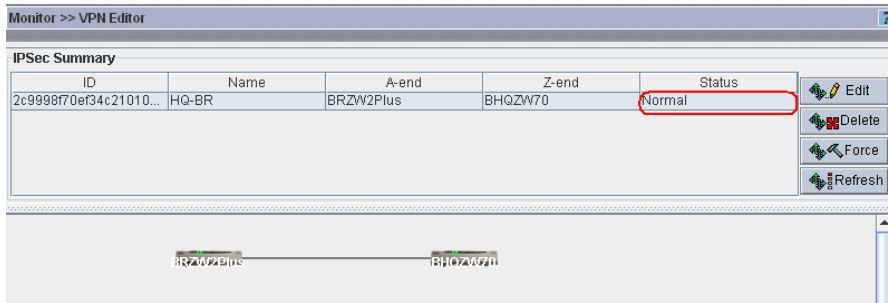
Administrator can view VPN tunnel status in **VPN Editor** Screen. If there is any problem with the VPN tunnel, administrator can trouble shooting via checking the tunnel's status in Vantage.

The **Tunnel Summary** shows the **Name** of your tunnel, **A-End** and **Z-End** devices and the current tunnel **Status**.

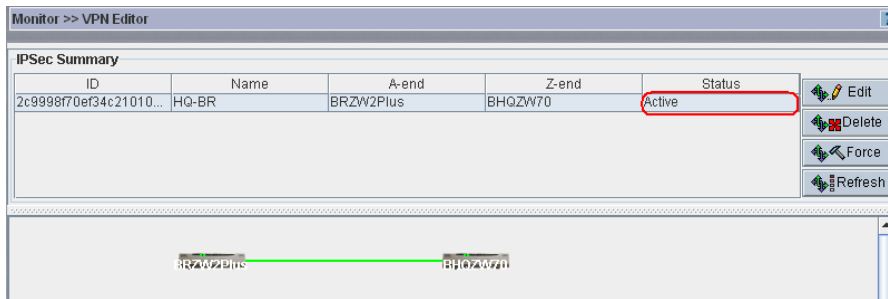
When the status is **To\_be\_created**, it means that the Vantage server has not yet synchronized VPN tunnel information with both devices. In this case, you can see a gray dashed line between the devices.



When the status is **Normal**, it means that the VPN tunnel is set up between the devices but the tunnel is not active yet (no traffic). In this case, you can see a gray solid line between the devices.



When the status changes to **Active**, it means there is traffic going through in the tunnel. In this case, you can see a green line between the devices.



## 1.8 Device Maintenance

As for the detailed information about the whole scenario, please refer to [1.4 A scenario for Vantage application](#).

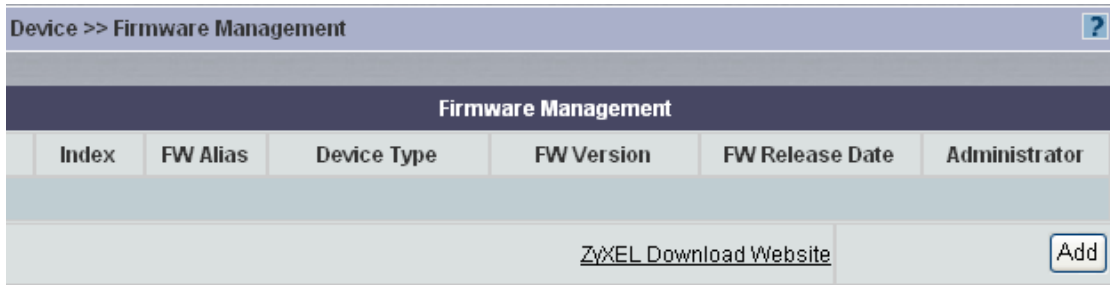
### 1.8.1 Firmware Management and upgrade

#### 1.8.1.1 Firmware Management

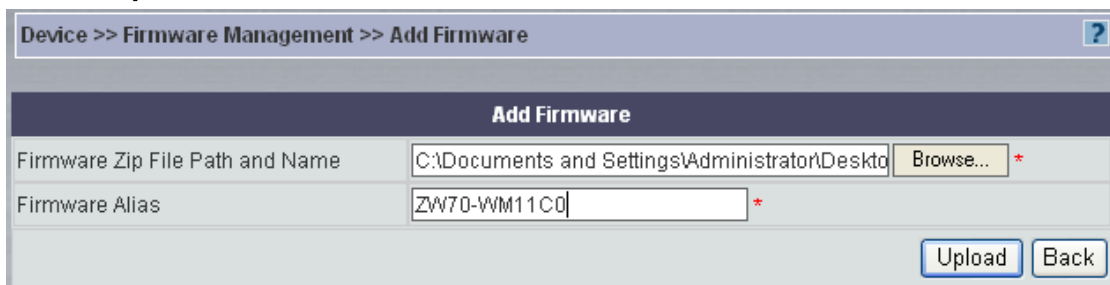
M company can use the Vantage **Firmware Management** screen to download ZyXEL device firmware from the ZyXEL FTP site to Vantage. After downloading it to Vantage, administrator can then upload it from Vantage to the target devices in A Company and B Company. All firmware is downloaded to one repository within Vantage. Administrator should subscribe to the ZyXEL mailing lists to be regularly informed of new firmware versions.

Go to **Device>>Firmware Management**, you can found detailed info about the current firmawre in your Vantage, such as **FW Version**, **Device Type** and so on. Click **ZyXEL Download Website** to go to the ZyXEL Website and download. Please make sure Internet in your network is available.

Click Add to download a firmware from your local computer.



In the next screen, you are requested to browse the **Firmware Zip File Path and Name** which you want to download from. Enter a firmware name in **Firmware Alias** field. Click **Upload**.



Then you can find all the firmware info in **Firmware Management** screen.

**Note:** You can only delete firmware downloads done by you or an administrator within your domain. You can not edit an existing firmware in Vantage. You can only delete it.

Firmware Management						
	Index	FW Alias	Device Type	FW Version	FW Release Date	Administrator
<input type="checkbox"/>	1	ZW70-WM11C0	ZyWALL70	4.00(WM.11)	08/07/2006	root
<input type="checkbox"/>	2	ZW5-XD12C0	ZyWALL5	4.00(XD.12)	09/06/2006	root
<input type="checkbox"/>	3	ZW5-XD12C0	ZyWALL5	4.01(XD.1)	09/04/2006	root
<input type="checkbox"/>	4	ZW70-WM11C0	ZyWALL70	4.01(WM.1)	09/07/2006	root
<input type="checkbox"/> Select All						
<a href="#">ZyXEL Download Website</a>						<input type="button" value="Add"/> <input type="button" value="Delete"/>

### 1.8.1.2 Group Firmware Upgrade Process

M company can use the **Device Firmware Upload** screen to download firmware to devices from Vantage. Administrator may upload firmware to several homogeneous device at the same time such as all ZyWALL 5 in branches of A Company or the two ZyWALL 70 in A Company and B Company. Vantage can upload firmware from 20 to 50 devices at a time depending on your network bandwidth. Go to **Type View** in the main screen to view files containing devices of the same type.

Select folder **A\_Company**, go to **Device>>Firmware Upgrade**.

Select the candidate devices(of that model type for the group selected).

Index	FW Alias	Device Type	FW Version	FW Release Date	Administrator	
<input type="radio"/>	1	ZW5-XD12C0	ZyWALL5	4.00(XD.12)	09/06/2006	root
<input type="radio"/>	2	ZW5-XD12C0	ZyWALL5	4.01(XD.1)	09/04/2006	root

Index	Device Name	Current FW Version	Upgrade Status	Other	
<input type="checkbox"/>	1	\\rootA_Company\BR1ZW5	4.00(XD.11)b1	Device is offline.	
<input type="checkbox"/>	2	\\rootA_Company\BR2ZW5	4.00(XD.11)b1	Ready to upgrade.	

Select All

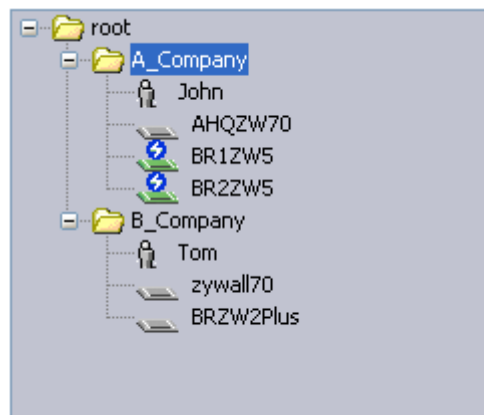
**Note:** You should upgrade the firmware to the device when the **Upgrade Status** is **Ready to upgrade**.

Index	Device Name	Current FW Version	Upgrade Status	Other	
<input type="checkbox"/>	1	\\rootA_Company\BR1ZW5	4.00(XD.11)b1	Device is offline.	
<input type="checkbox"/>	2	\\rootA_Company\BR2ZW5	4.00(XD.11)b1	Ready to upgrade.	

Click **Apply** to begin the group firmware upgrade process.

You can see the **Upgrade Status** of the devices turn to **upgrading** and two blue lightning marks are added on the devices' icon. When the upgrade process is done, it will turn to **Ready to upgrade** again and the blue lightning marks will disappear.

Index	Device Name	Current FW Version	Upgrade Status	Other	
<input type="checkbox"/>	1	\\rootA_Company\BR1ZW5	4.00(XD.11)b1	upgrading.	<a href="#">Remove</a>
<input type="checkbox"/>	2	\\rootA_Company\BR2ZW5	4.00(XD.11)b1	upgrading.	<a href="#">Remove</a>



### 1.8.1.3 Schedule Firmware Upgrade

Alternatively, you can schedule when you want firmware upgrades to start.

Select **Firmware** by picking a node.

Select the candidate devices (of that model type for the node selected)

Select the **Customized Time** checkbox.

Fill in the **Customized Time** fields to schedule a firmware upgrade start time. Type a date in yyyy.mm.dd format followed by the time in hh format.

Type some extra information in the **Description** field. This description appears in the firmware upgrade report screen when the upgrade is logged.

Click **Apply** to begin the device upgrade process.

**Advisory Notes on Firmware Upgrade:** It is advisable to upgrade firmware during periods of low network activity, since each device must restart after firmware upload. You should also notify device owners before you begin the upload.

### 1.8.1.4 Firmware Upgrade Report


Go to **Monitor>>Firmware Report**, **Firmware Upgrade Report** will be shown next. Administrator can get the details of firmware uploaded to Vantage in this screen.

**Index** displays the upgrade list number. **Administrator** displays the administrator who performed the upgrade. **Action Time** displays the time at which the upgrade was performed. **Description** displays a description entered in data maintenance prior to uploading. Select **Purge** to clear selected reports.

Firmware Upgrade Report					
	Index	Administrator	Action Time	Description	
<input type="checkbox"/>	1	root	2006-11-2 10:23:51	2006-11-2 10:23:51	<a href="#">Detail</a>
<input type="checkbox"/>	2	root	2006-11-2 11:08:47	2006-11-2 11:08:47	<a href="#">Detail</a>
<input type="checkbox"/>	3	root	2006-12-7 14:42:27	2006-12-7 14:42:27	<a href="#">Detail</a>
<input type="checkbox"/>	4	root	2006-11-17 15:26:53	2006-11-17 15:26:53	<a href="#">Detail</a>
<input type="checkbox"/>	5	root	2006-12-7 14:42:27	2006-12-7 14:42:27	<a href="#">Detail</a>

Click **Detail**, Administrator can get the details of firmware uploaded to Vantage in this screen. **Device Name** displays the device folder path and name. **Upgrade Time** displays the data and time at which the upgrade was performed. **Status** displays a current upgrade status description.



Firmware Upgrade Action Detail			
Device Name	Upgrade Time	Status	Notifications
WrootA_Company\BR1ZW5	2006-12-07 14:42:27	success	

Click the icon of Notification, the **Notification** screen will be popped out. Administrator can use this screen to enable sending of notifications of firmware upgrades to **Device Owners**, to a **root** administrator or to specific other administrators. Type an e-mail address in the **Other(s)** field to send notifications of firmware upgrades to specific contacts.

Notifications	
Active	Name
<input type="checkbox"/>	Device Owner
<input type="checkbox"/>	root
<input type="checkbox"/>	Tom
<input type="checkbox"/>	John
Other(s)	<input type="text"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

## 1.8.2 Configuration file backup and restore

Administrator select a device and then use the Backup screen to save the device's configuration file to either Vantage or your computer(from which you're accessing Vantage).

### 1.8.2.1 Backup and Restore

Go to **Device>>Configuration File**, the **Backup & Restore** screen is shown next.

**Backup & Restore** configuration allows user to back up the current configuration to a file on your computer and restore a configuration file to your device. Once your device's configuration is configured and functioning properly, it is highly recommended that you back up your configuration file before making configuration changes. The backup configuration file will be useful in case you need to return to your previous settings.

The screenshot shows the 'Configuration File' management interface. It has two main sections: 'Backup' and 'Restore'.  
**Backup Section:** The 'Destination' is set to 'To Server'. There are input fields for 'File Name' and 'Description'. The 'To Computer' option is unselected. A 'Backup' button is at the bottom right.  
**Restore Section:** The 'Resource' is set to 'From Server'. There is a dropdown menu for 'File Name'. The 'From Computer' option is unselected. There is a 'Browse...' button and an 'Upload' button at the bottom right.

If you want to backup the configuration file **To Server**, you will be requested to enter a name in **File Name** field and type a note in **Description** field for your configuration file. Select **To Computer** to give the download destination to your computer.

This screenshot shows the 'Backup' section of the interface. The 'Destination' is 'To Server'. The 'File Name' field is highlighted with a red box and contains the text 'ZW2plus\_Romfile'. The 'Description' field contains 'B\_Company\_Branch'. The 'To Computer' option is unselected. A 'Backup' button is visible at the bottom right.

When restore a configuration **From Server**, if there are existed files available on the server for your device, they will all be shown in **File Name** field. If there is no files available, the **File Name** field will be blank and you can not restore a configuration file for your device from server. Select **From Computer** to give the download resource from your computer.

This screenshot shows the 'Restore' section of the interface. The 'Resource' is 'From Server'. The 'File Name' dropdown menu is highlighted with a red box and shows the selected file 'ZW2plus\_Romfile1163754252523.rom'. The 'From Computer' option is unselected. There is a 'Browse...' button and an 'Upload' button at the bottom right.

### 1.8.2.2 Group Configuration Backup

M company can use the **Backup** screen to backup configuration of several homogeneous device at the same time such as all ZyWALL 5 in branches of A Company or the two ZyWALL 70 in A Company and B Company. Go to **Type View** in the main screen to view files containing devices of the same type.

Select folder **A\_Company**, go to **Device>>Configuration File>>Backup**, all the devices in this group are displayed in this screen. Administrator should select **Ready** in **By Status** field since only the status of the device is ready, the configuration can be backedup.

**Configuration File**

Management | Backup

Romfile Name:

Note:

By Status: All (Please select the Ready devices by status to do backup.)

Index	Device Name	Model Name	Firmware Version	Status
1	\\rootA_Company\AHQZW70	ZyWALL70	4.00	Offline
2	\\rootA_Company\BR2ZW5	ZyWALL5	4.00	Ready
3	\\rootA_Company\BR1ZW5	ZyWALL5	4.00	Ready

All the devices which status is **Ready** will be shown as below. Select the devices you want to backup the configuration file. Type a name for the configuration file you want to backup in **Romfile Name** field and make some description in **Note** field. Click **Backup** to start the backup process.

**Configuration File**

Management | Backup

Romfile Name: BRZW5

Note: A\_Company

By Status: Ready (Please select the Ready devices by status to do backup.)

	Index	Device Name	Model Name	Firmware Version	Status
<input checked="" type="checkbox"/>	1	\\rootA_Company\BR2ZW5	ZyWALL5	4.00	Ready
<input checked="" type="checkbox"/>	2	\\rootA_Company\BR1ZW5	ZyWALL5	4.00	Ready

Select All

Backup Reset

Go to **Management**, you can find the detailed record for the backup you just done. **File Name** displays the name of the configuration file you just backedup. **Time** displays the data and time at which the backup was performed. **Note** displays the

description you made for the configuration file. **Count** displays a current backup status description.

Configuration File						
Management			Backup			
Index	File Name	Time	Admin	Note	Count (Succeed/Total)	
<input type="checkbox"/>	1	BRZW5	2006-12-07 19:06:07	root	A_Company	2 / 2
<input type="checkbox"/> Select All						
						Delete

## 1.9 Real-time Monitoring, Alerting and Comprehensive Graphic Reporting

Vantage is a cost-effective solution that allows the administrator from any location to easily configure, manage, monitor and troubleshoot ZyXEL devices. As for the detailed information about the whole scenario, please refer to [1.4 A scenario for Vantage application](#).

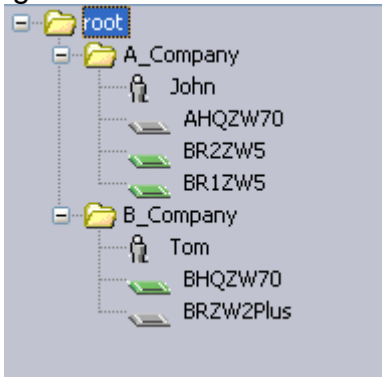
### 1.9.1 Monitoring (Device Online/Offline, Device Alarm)

#### 1.9.1.1 Device Online/Offline

Administrator can check the status of every device belonging to A Company or B Company by clicking **A\_Company** icon or **B\_Company** icon in the left frame, then select **DEVICE>>Status**. And John/Mary can check the status of devices in their own company clicking A\_Company/B\_Company. The Status of each device is on when the device is able to talk with Vantage server. And managers can also have a quick by checking the color of the device icon. It will be green if the status is on. Different display of the icon has different meaning; please check User's Guide for the details.

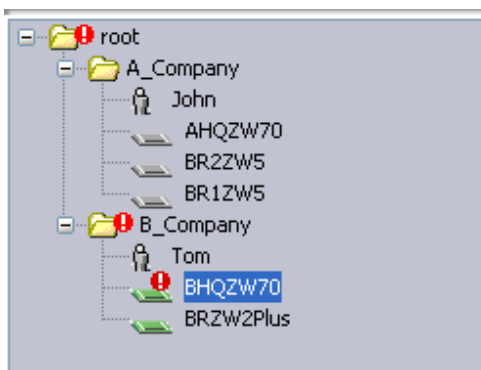
Device Status								
By Status		All		Total devices: 5				
Device Name	Type	MAC	IP	Syslog Server IP	Status	Firmware Version	Extension Card Status	
\root\A_Company\AHQZW70	ZyWALL70	0013493ABDFE	172.25.24.100	172.25.24.119	Off	4.00 (WM.11)	N/A	
\root\A_Company\BR2ZW5	ZyWALL5	00134953FAAF	172.25.24.138	172.25.24.119	On	4.00 (XD.11)b1	N/A	
\root\A_Company\BR1ZW5	ZyWALL5	00134984660F	172.25.24.90	172.25.24.119	On	4.00 (XD.11)b1	N/A	
\root\B_Company\BHQZW70	ZyWALL70	00134907188E	172.25.24.173	172.25.24.119	On	4.00 (WM.11)	Turbo Card	
\root\B_Company\BRZW2Plus	ZyWALL 2 Plus	00134980CDEA	172.25.24.24	172.25.24.119	Off	4.00 (XU.2)	N/A	

If the communication between Devices and Vantage is good, then the device icons would turn to green. It may take 5 minutes at most to let your Java Plug-in refresh the icons.



### 1.9.1.2 Device Alarm

When a device is under attacks, a red exclamation mark will show up on device icon. And the Status will be changed from "On" to "On\_Alarm".

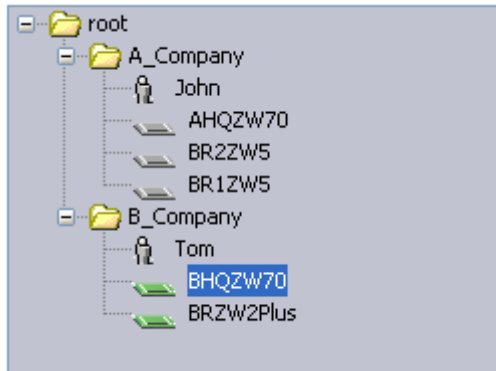


Device Status								
Device Name	Type	MAC	IP	Syslog Server IP	Status	Firmware Version	Extension Card Status	
\root\B_Company\BHQZW70	ZyWALL70	00134907188E	172.25.24.90	172.25.24.119	On_Alarm	4.00 (WM.11)	Turbo Card	

Go to **Monitor>>Alarm>>Current**, administrator can see more detailed info about the Alarm.

Index	Device Name	Category	Severity	Time	Message	Responder	Response Time	Clear
1	BHQZW70		!	2006-11-17 17:14:21	ip spoofing - WAN UDP	Respond		Clear
2	BHQZW70		!	2006-11-17 17:14:16	ip spoofing - WAN UDP	Respond		Clear
3	BHQZW70		!	2006-11-17 17:14:04	ping of death. ICMP (Echo)	Respond		Clear
4	BHQZW70		!	2006-11-17 17:13:58	ip spoofing - WAN UDP	Respond		Clear
5	BHQZW70		!	2006-11-17 17:13:53	ping of death. ICMP (Echo)	Respond		Clear

Click **Clear All**, all of the Alarm info will be deleted and the red exclamation mark will disappear in the **MainView**.



### 1.9.2 Alerting (Email Notification)

Vantage can send automatic e-mails to people for events that may warrant immediate attention. You can configure someone Vantage should automatically notify when an administrator performs firmware upgrade or there are device logs and/or alarms or device offline or device service expiration.

To achieve this, you should configure a SMTP server for e-mail notifications.

Go to **System>>Preference**, Servers screen will be shown. You can configure these servers as you install Vantage or after you install it in this screen.

You should know the SMTP server's **IP or Domain Name**, a user account as **Mail Sender** and its **Username** and **Password**, or e-mail notifications will not work in Vantage if these are incorrectly configured.

System : Preferences			
Server	Notifications	User Access	User Group
<input type="checkbox"/> Vantage CNM Server			
Public IP Address	172.25.24.119 *		
Web HTTPS Port	443		
Web HTTP Port	8080		
<input type="checkbox"/> FTP Server			
IP or Domain Name	172.25.24.119 *		
User Name	vantage *		
Password	***** *		
<b>VRPT Management</b>			
<input checked="" type="checkbox"/> Mail Server			
IP or Domain Name	ms01.zyxel.cn *		
Mail Sender	sherry.liu@zyxel.cn *		
User Name	zycn\w00593		
Password	*****		
		Apply	Reset

After SMTP Server has been configured correctly, go to **Notifications**, notifications screen will shown next. You can configure notifications for **Firmware Upgrade, Logs, Alarms, Device Offline** and **UTM Device Service Expire**.

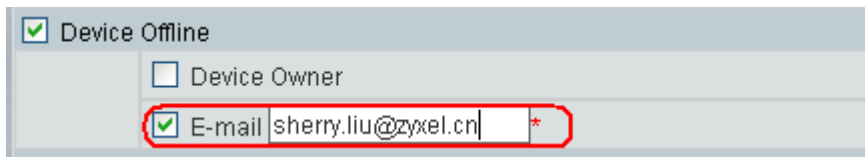
System : Preferences			
Server	Notifications	User Access	User Group
<input type="checkbox"/> Firmware Upgrade			
	<input type="checkbox"/> Device Owner		
	<input type="checkbox"/> E-mail		
<input type="checkbox"/> Logs			
	<input type="checkbox"/> E-mail		
<input type="checkbox"/> Alarms			
Send alarm report to :			
	<input type="checkbox"/> Device Owner		
	<input type="checkbox"/> E-mail		
Send device alarm notification to Device Owner :			
	<input checked="" type="radio"/> Immediately		
	<input type="radio"/> Active Alarm Consolidation Period	1 *	(1 - 60 minutes)
<input type="checkbox"/> Device Offline			
	<input type="checkbox"/> Device Owner		
	<input type="checkbox"/> E-mail		
<input type="checkbox"/> UTM Device Service Expire			
	<input type="checkbox"/> Device Owner		
	<input type="checkbox"/> E-mail		
Note: Expire Notification will be send at 30-days,10-days or 0-day before Expiration Day.			
		Apply	Reset

**Device Owner** is a variable that refers to the e-mail address of the device owners

(Configured in **Configuration>>General>>Owner Info** screen). Select **Device Owner** check box will have an e-mails automatically sent to the selected device owner e-mail address. You can have the notifications e-mails sent to new or existing e-mail addresses via entering them in **Email** field(If you want to enter multiple e-mail addresses, separate them by commas).

You can set **Send device alarm notification to Device Owner** to **Immediately** or to **Active Alarm Consolidation Period(1-60 minutes)** as you want.

Jim set notifications for **Device Offline** be sent to sherry.liu@zyxel.cn. So if the device is offline, sherry will get the notification e-mails as below.



The mail will show the detailed information of the device which is offline, such as **Device Name, Device Type, Device MAC** and **Device Offline Time**.



### 1.9.3 Reporting (Traffic Report / Network Attack Report / UTM Report)

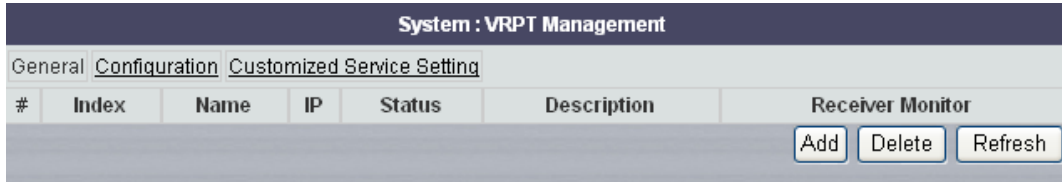
The report function can supply essential firewall traffic reports, identifies suspicious activities, monitors network activity, tracks bandwidth usage and reveals questionable web surfing. It allows you to reveal if your network is experiencing significant number of critical events. The Attacks reports list the suspicious activities, frequencies and the source. It also allows you to provide the bandwidth measurements to support a bandwidth budget tailored to your organization’s needs.

#### 1.9.3.1 Setting VRPT server for managed device

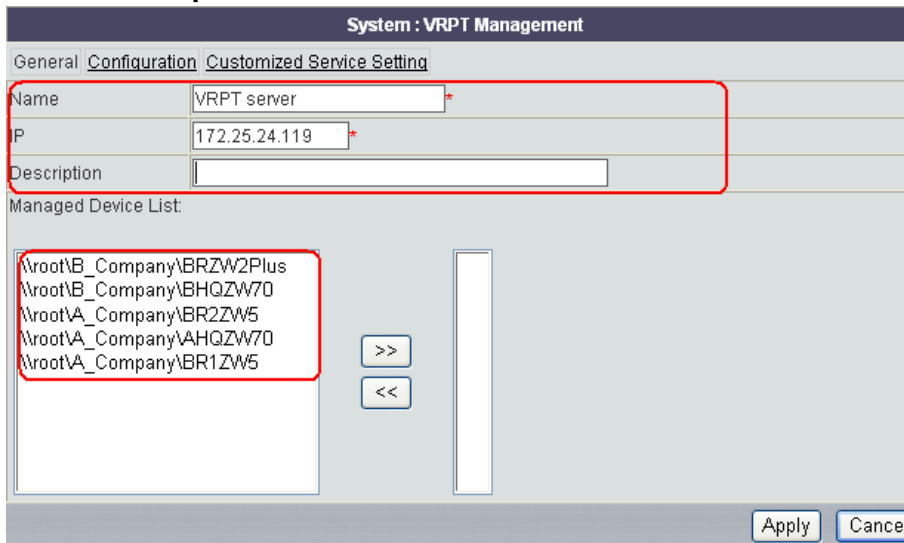
To get the report in CNM, you should make sure the configuration of **VRPT Management** has been done and the VRPT server is available. Below list the steps to Register your devices to VRPT server.



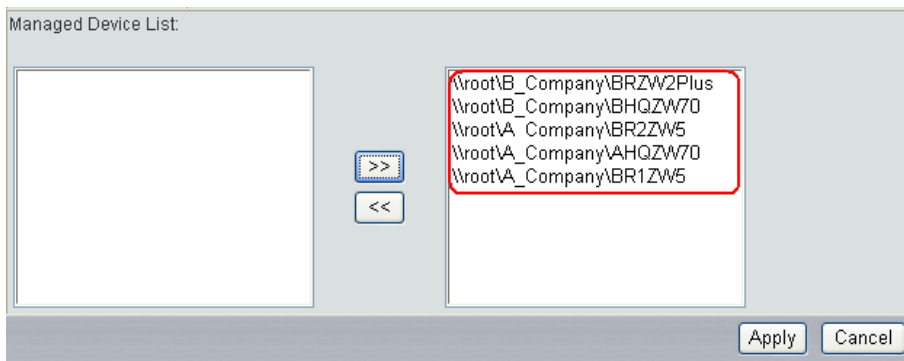
Step 1. Go to **System>>VRPT Management**, you will see the **General** configuration screen. If there is no VRPT server's info exists, click **Add** button to add a VRPT server for your device.



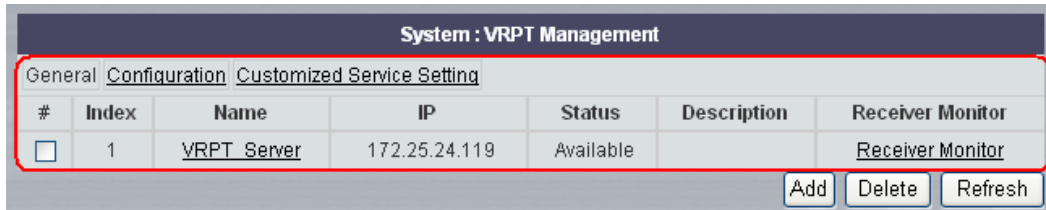
Step 2. Type a name for your VRPT server in **Name** field and its IP address in **IP** field. Also type some extra description of the VRPT server in **Description** field. You can leave **Description** field as blank.



Add your device name to the **Managed Device List**, then click **Apply** button to save the configuration.

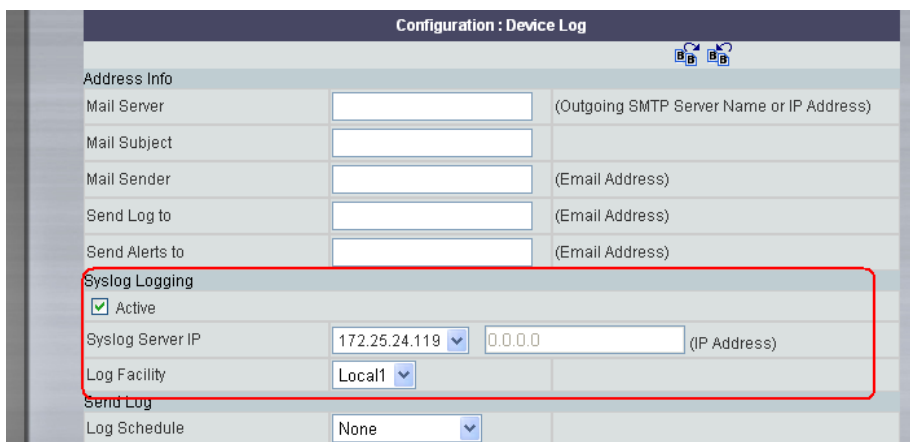


Then you can see the current status of the VRPT server you just configured in next shown screen. Also you can configure more parameters for your VRPT server in **Configuration** and **Customized Service Setting** fields.



Step 3. Make sure the Syslog Logging in your device is enabled.

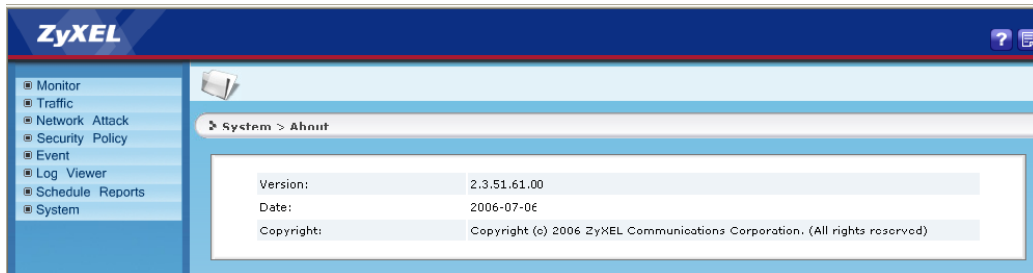
Go to **Configuration>>Device Log**, you can find whether **Syslog Logging** has been enabled and the IP address of the CNM server has been filled in the Syslog Server IP field.



### 1.9.3.2 Viewing report of managed devices

After all the configuration steps introduced above, go to **Report>>Report**, you can see the VRPT report for your device in Vantage.

Go to **Report>>Report**, you can see the **Vantage Report** screen as shown next. The current release and copyright for Vantage Report is showed on this screen.

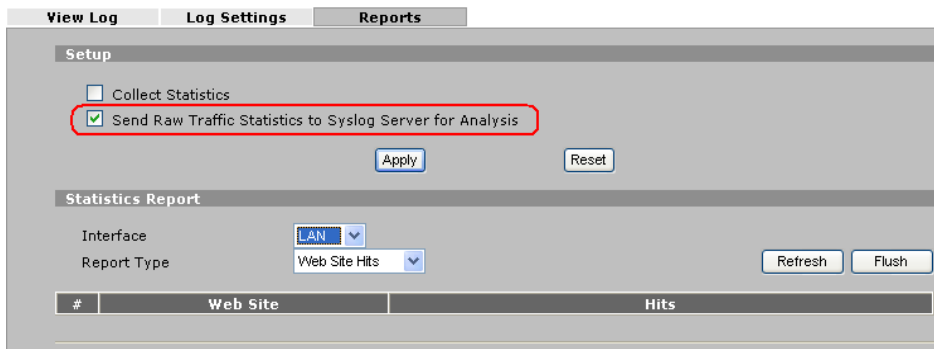


**Monitor** is a special menu in VRPT for live monitor according to the logs received during the last 60 minutes. Live monitor report for **Bandwidth** and **Service** will be shown as continuous curves for they are generated by traffic logs. While live report for **Attack**, **Intrusion**, **AntiVirus** and **AntiSpam** will expose to you as discrete picture for it monitors event logs.

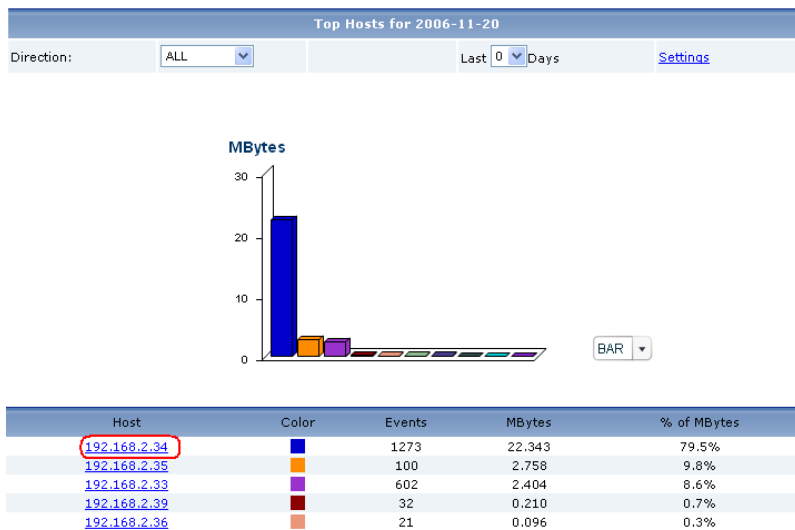
**1.9.3.2.1 Bandwidth Report**

One day the employees in Branch 1 of A Company complain the network of the company is so bad that they even can not send and receive the E-mails properly. All the traffic go through the AHQZW70. Then Administrator in M company will go to Vantage and check the Bandwidth report for the ZyWALL 70 and takes some measures to resolve this problem. Below is a sample to show how to check the bandwidth usage.

You need to enable the traffic log on the device. Right click the device's icon, select **EWC>>HTTP** to login to the GUI configuration page (make sure firewall has been disabled), then go to **Logs>>Reports**, enable **Send Raw Traffic Statistics to Syslog Server for Analysis**, thus you can get the bandwidth usage report in Vantage.



In Vantage, check **Traffic>>Bandwidth>>Top Hosts**, administrator find the below report. It shows the user with IP address 192.168.2.34 is on the top of the list.



Enter the drill down menu of it to check further. It will show the top ten protocols by Host 192.168.2.34 as below.

Top Protocols for 2006-11-20 by Host 192.168.2.34



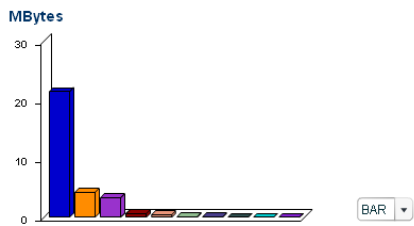
Protocol	Color	Events	MBytes	% of MBytes
others	Blue	915	20.461	87.6%
https	Orange	69	1.679	7.2%
http	Purple	139	1.062	4.5%
netbios-ns	Red	15	0.058	0.3%
pop3	Light Blue	7	0.028	0.1%
domain	Green	46	0.026	0.1%
msn	Dark Blue	2	0.017	0.1%
netbios-dgm	Dark Green	13	0.013	0.1%
icmp	Cyan	97	0.011	0%
ssdp	Pink	1	0.002	0%
Total		1304	23.356	100%

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.

Top Protocols for 2006-11-20

Direction: ALL Last 0 Days Settings



Protocol	Color	Events	MBytes	% of MBytes
others	Blue	1077	21.426	70.5%
http	Orange	624	4.269	14%
https	Purple	118	3.334	11%
netbios-ns	Red	844	0.623	2%
netbios-dgm	Light Blue	1154	0.456	1.5%
pop3	Green	42	0.115	0.4%
domain	Dark Blue	98	0.086	0.3%
msn	Dark Green	4	0.044	0.1%
pop3	Cyan	8	0.029	0.1%
snmp	Pink	6	0.028	0.1%
Total		3975	30.408	100%

**1.9.3.2.2 Attack report**

Administrator can get the report for attack on the devices in A Company which we mentioned in **Device Maintenance>>3. Device alarm, alert and notify**.

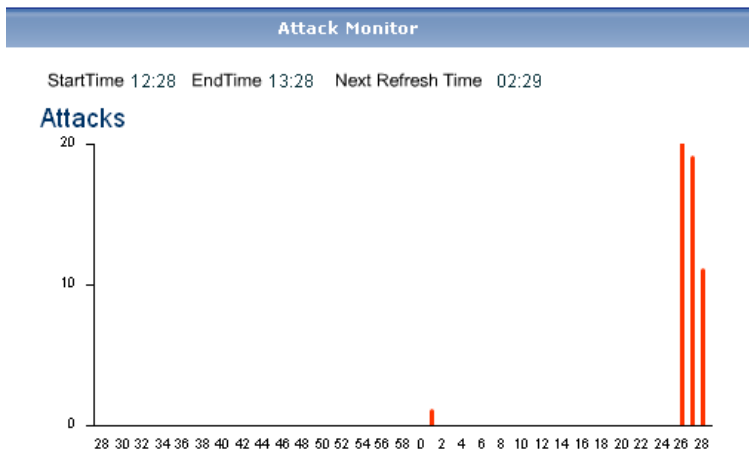
**Note:** To look at attack reports, each ZyXEL device must record DoS attacks in its log. See the User's Guide for each ZyXEL device for more information. In most devices, go to **Logs >> Log Settings**, and make sure **Attacks** is enabled.

For **Attack Monitor** report, administrator can monitor the number of Denial-of-Service(DoS) attacks detected by the selected device's firewall.

Please check the below tables for coordinate information of the report.

Attack Monitor Report

Coordinate	Meaning	Unit
X axis	Lease time	Minute
Y axis	Number of the attacks	



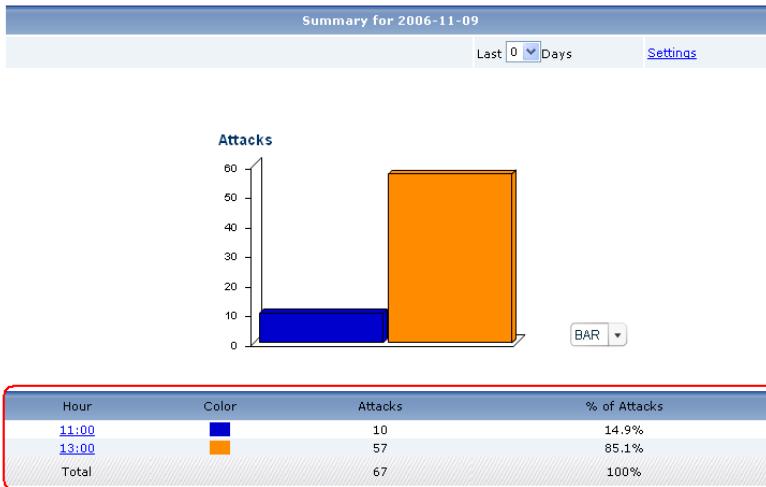
For **Attack Summary** report, administrator can look at the number of DoS attacks detected by time interval. Click **Settings**. The **Report Display Settings** screen appears.

Report Display Settings	
Start Date:	2006-11-08 *
End Date:	2006-11-08 *
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Select a specific **Start Date** and **End Date**. The date range can be up to 30 days long, but you cannot include days that are older than **Store Log Days** in **System >> General Configuration**. Click **Apply** to update the report immediately, or click **Cancel** to close this screen without any changes.

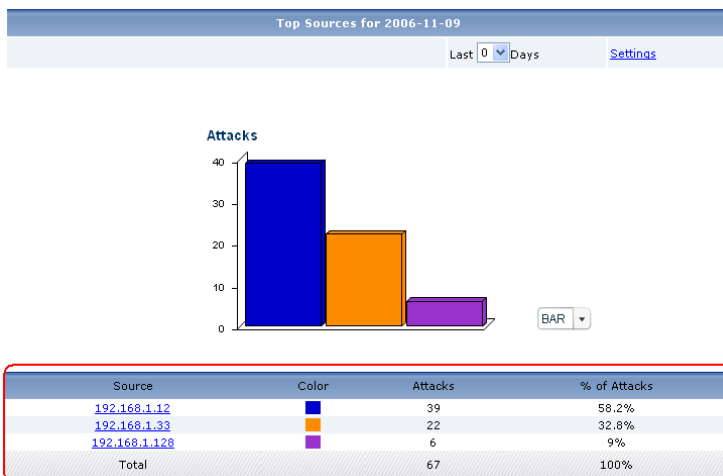
In the sample report below, there are 10 attacks happen during 11:00 and 57

attacks happen during 13:00.



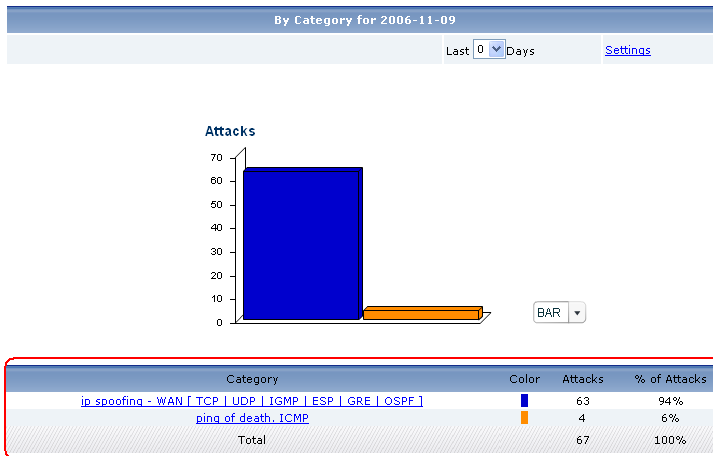
For **Attack Summary** report, administrator can look at the top sources of DoS attacks by number of attacks the selected device stopped and can block such IP addresses by adding firewall rules. Please notice the direction of the firewall rules.

Click on a source to look at the top categories of DoS attacks by the selected source. The **Top Attack Sources Drill-Down** report appears.



For **Attack>>By Category** report, administrator can look at the top categories of DoS attacks the selected device stopped by number of attacks.

Click on a category to look at the top sources of DoS attacks in the selected category. The **Top Attack Categories Drill-Down** report appears.



User can search all the logs for Attacks in **Log Viewer>>All Logs**. Below is a sample log report about Attacks for AHQZW70.

Select All Logs

Day: 2006-11-09 Start Time: 00:00 End Time: 24:00 Days Start Date: End Date: Advanced Search

Category: Attacks Search Reset

Time	Source:Port	Destination:Port	Category	Message
2006-11-09 11:53:46	192.168.1.128:137	192.168.1.255:137	Attacks	ip spoofing - WAN UDP
2006-11-09 11:53:45	192.168.1.128:137	192.168.1.255:137	Attacks	ip spoofing - WAN UDP
2006-11-09 11:53:44	192.168.1.128:137	192.168.1.255:137	Attacks	ip spoofing - WAN UDP
2006-11-09 11:53:23	192.168.1.33	172.25.24.148	Attacks	ping of death. ICMP (Echo)
2006-11-09 11:53:18	192.168.1.33	172.25.24.148	Attacks	ping of death. ICMP (Echo)
2006-11-09 11:53:12	192.168.1.33	172.25.24.148	Attacks	ping of death. ICMP (Echo)
2006-11-09 11:53:07	192.168.1.33	172.25.24.148	Attacks	ping of death. ICMP (Echo)

Total Count:67 Total Page:7 First 1 2 3 4 5 6 7 Last Go

### 1.9.3.2.3 UTM report

Administrator can get the report for security UTM in A Company which we mentioned in **UTM Management**.

There are three UTM items (**Intrusion, AntiVirus and AntiSpam**) showed under the **Monitor** and **Network Attack** field.



Below are sample reports for the UTM reports (**Intrusion**, **AntiVirus** and **AntiSpam**) of AHQZW70.

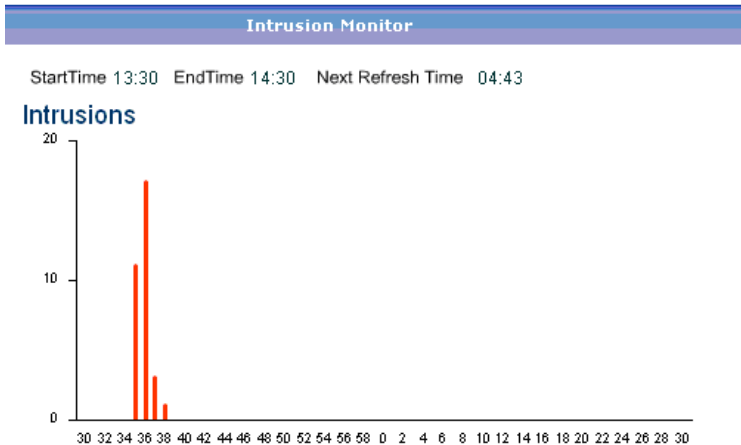
Please check the below tables for coordinate information of the report.

Intrusion/AntiVirus/AntiSpam Monitor Report

Coordinate	Meaning
X-axis	Lease time
Y-axis	Number of the events

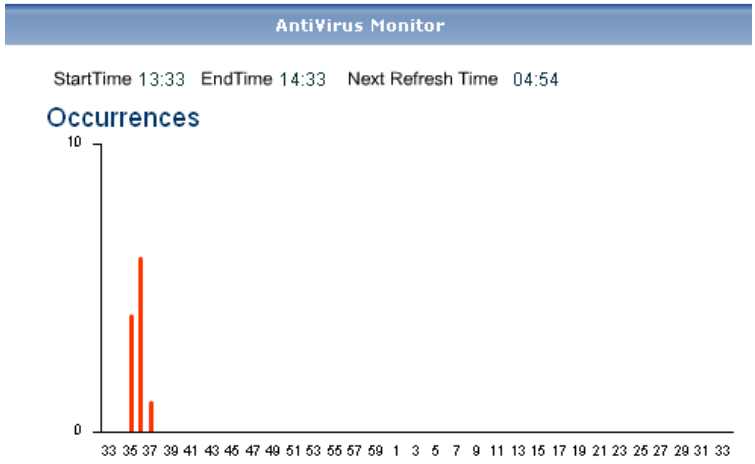
The x axis of each report shows the lease time. The Y axis of each report shows the number of intrusions/Virus/Spam detected by the selected device's **Intrusion/AntiVirus/ AntiSpam** feature each minute.

Use **Intrusion Monitor** report to monitor the number of intrusions detected by AHQZW70.

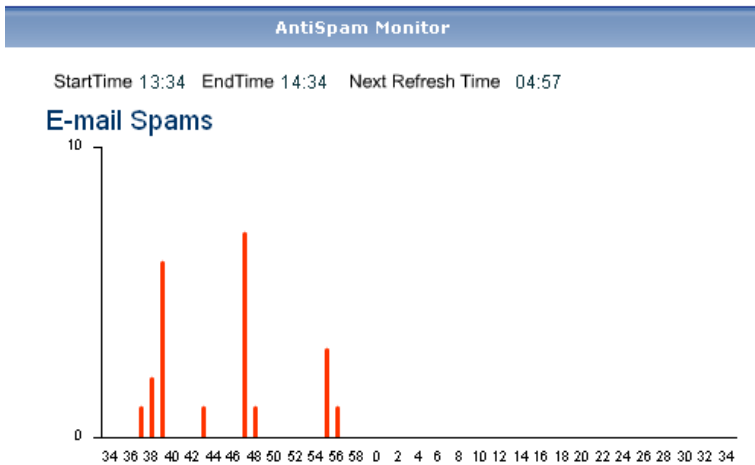


Use **AntiVirus Monitor** report to monitor the number of virus occurrences prevented by AHQZW70.



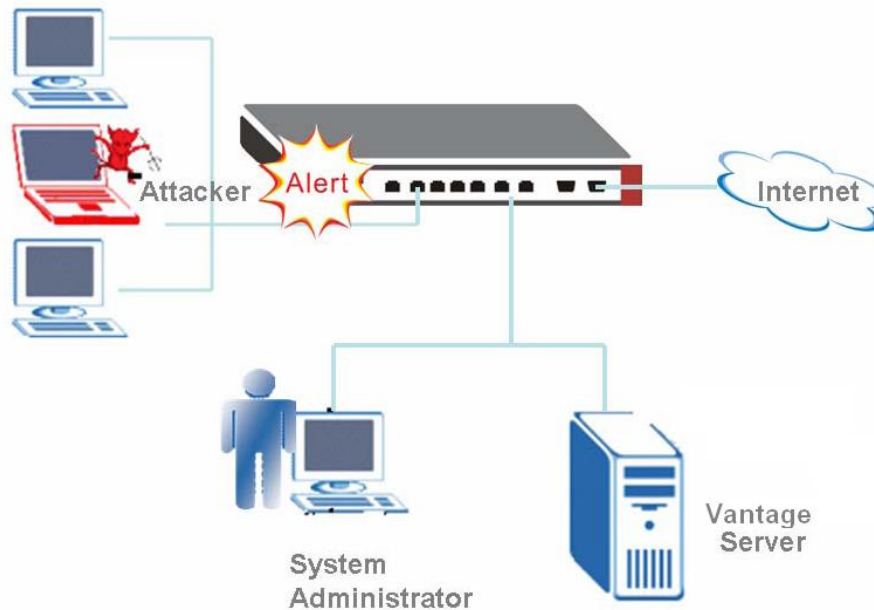


Use **AntiSpam Monitor** report to monitor the number of spam message stopped by AHQZW70.

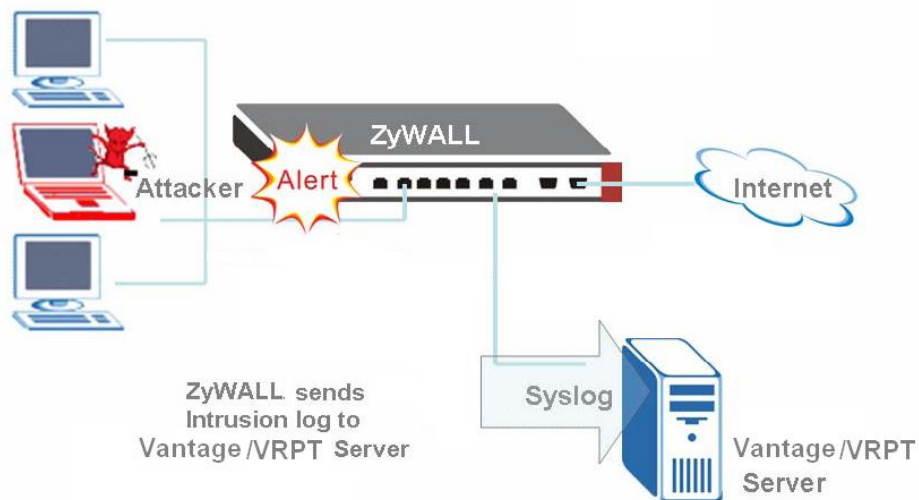


**1.9.3.2.3.1 IDP Report**

VRPT supports intrusion report for 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.

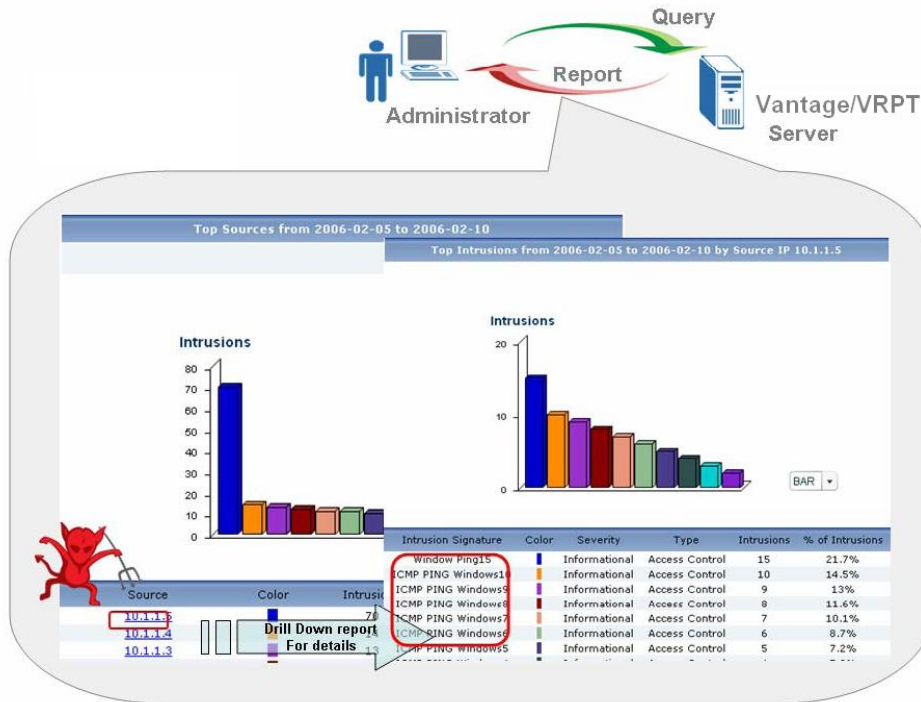


When ZyWALL detects intrusion events, it will generate Syslog and forward to VRPT Server.



Get the report from Vantage, 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. Also user could use scheduled report for reminding.



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

The advanced query (Drill down report) can be **Top Intrusions/TopSources/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

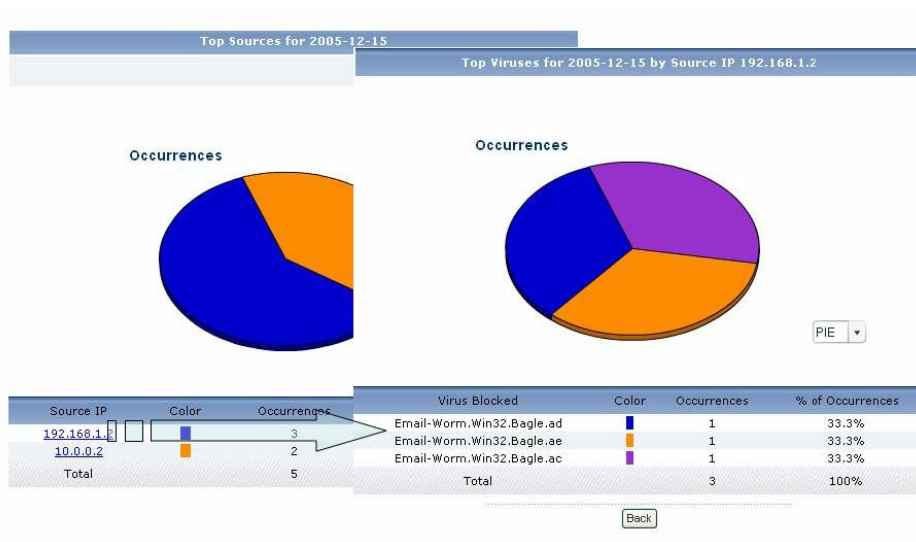
Warning	warning conditions
Notice	normal but significant condition
Informational	informational messages
Debug	debug-level messages

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

**1.9.3.2.3.2 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.

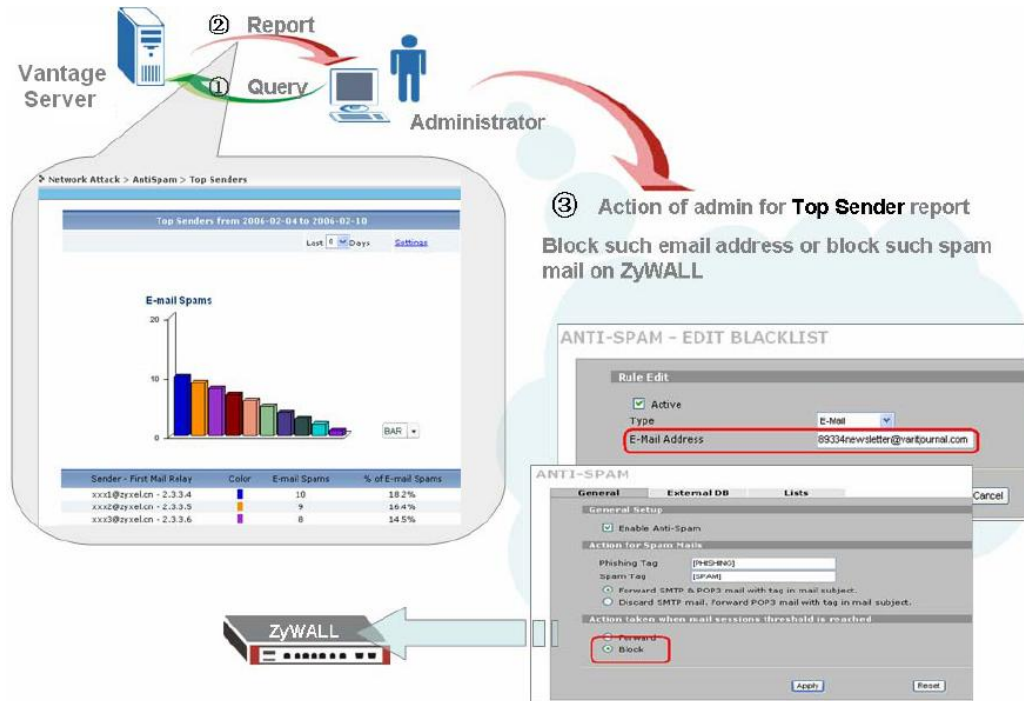


**1.9.3.2.3.3 AntiSpam Report**

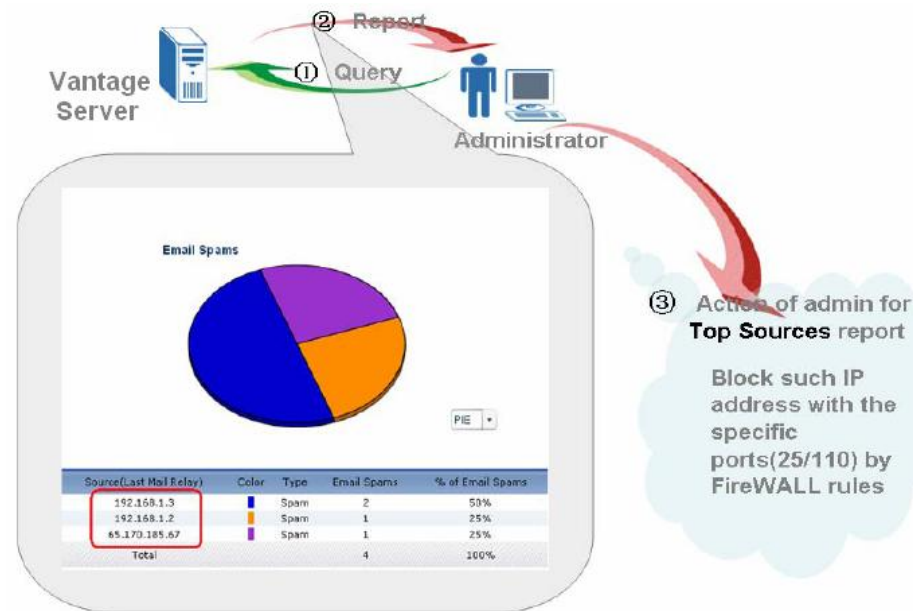
**AntiSpam** report is especially for ZyWALL 5/35/70 UTM AntiSpam feature. Using this kind of report, administrator will trace the sender and source of the Spam Mail. Also user could determine score threshold by checking score report.

- 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.

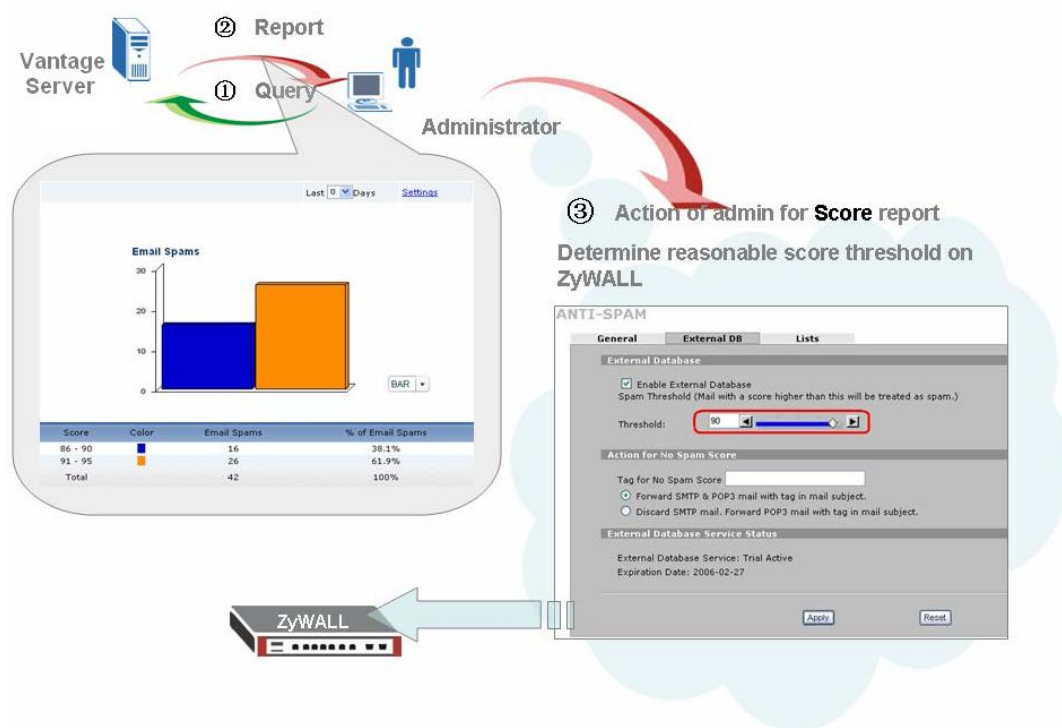


2. For **Top Sources** report, administrator could block such IP addresses by adding firewall rules. Please still notice the direction of the rules as that of in the Intrusion scenario.



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.



### 1.9.3.3 Configuring Schedule Report

Jim would like to get the schedule report for UTM in A Company and B Company in order to know the statistical status of their security.

Vantage 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.

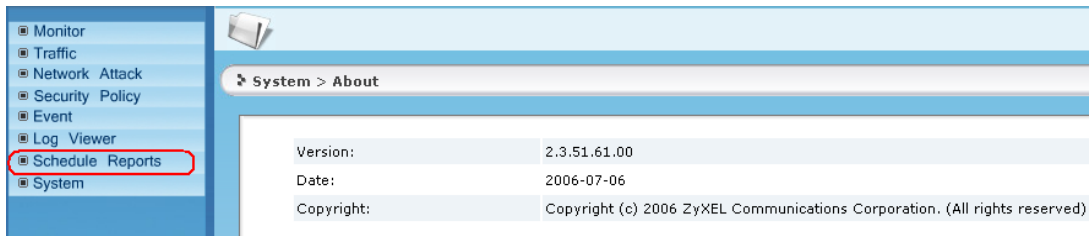
**Note:** To send scheduled reports by e-mail, you have to enter the SMTP mail server settings first.

Go to **VRPT Management>>Configuration**, enter the SMTP mail server and your account/password to the corresponding bank in this screen, also input **Sender/Receiver E-mail**, then click **Apply** to save the configuration.

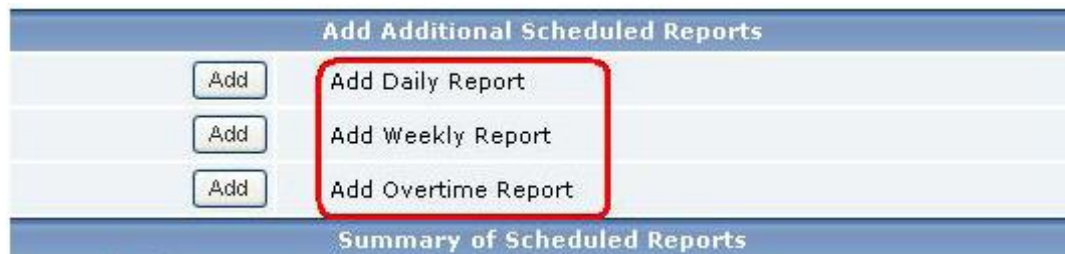
System : VRPT Management	
<a href="#">General</a>   <a href="#">Configuration</a>   <a href="#">Customized Service Setting</a>	
<b>General Configuration</b>	
Stored Log Days:	<input type="text" value="7"/> Days (1-30)
Default Chart Type:	<input type="button" value="BAR"/>
DNS Reverse:	<input type="button" value="Disable"/>
Low Free Disk Mark:	<input type="text" value="8"/> G (>=5)
<b>Server Configuration</b>	
SMTP IP Address or Domain Name:	<input type="text" value="ms01.zyxel.cn"/> *
User Name:	<input type="text" value="Jimjw00593"/>
Password:	<input type="password" value="....."/>
Sender E-mail:	<input type="text" value="Jim@zyxel.cn"/> *
Receiver E-mail:	<input type="text" value="Jim@zyxel.cn"/> *
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

Go to **Report>>Report**, you can see the **Vantage Report** screen as shown next. The current release and copyright for Vantage Report is showed on this screen.

**Note:** please make sure the configuration of **VRPT Server** has been done and the VRPT server is available. Please refer to [1.9.3.1 Setting VRPT server for managed devices](#).



Step 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.

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

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.

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.

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.

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.

Finally user should choose the report he/she wants from **Report List**. Jim chooses all the items for UTM from **Report List**.

**Customize Overtime Report**

Destination E-mail Address (Comma Seperated): sherry.liu@zyxel.cn \*

E-mail Subject: UTM report \*

E-mail Body: overtime report generated by CNM \*

E-mail Attached Files

Save Directory: d:\Program Files\ZyXEL\Vantage CNM 2.3\vrpt\data\scheduler

Report Type: **HTML only** (dropdown menu open showing HTML only, PDF only, both)

Include All Data in a single report (only for PDF)

Start Date: [calendar icon] \* End Date: 2006-12-12 [calendar icon] \*

**Report List**

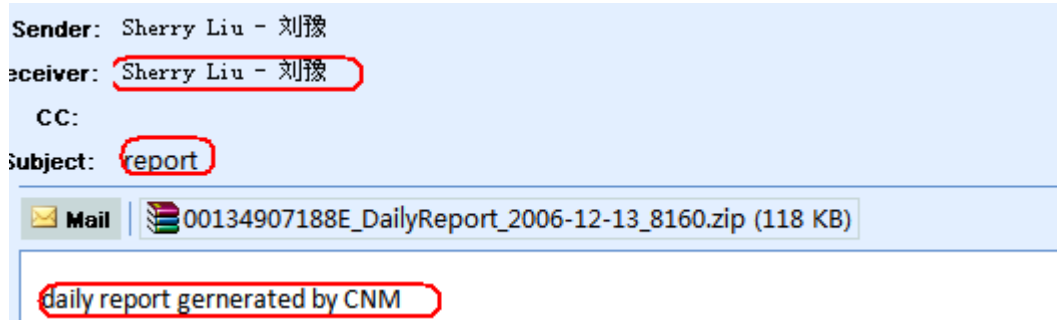
<input type="checkbox"/> Bandwidth Summary	<input checked="" type="checkbox"/> Attack Summary	<input checked="" type="checkbox"/> AntiVirus Top Sources
<input type="checkbox"/> Bandwidth Top Hosts	<input checked="" type="checkbox"/> Attack Top Sources	<input checked="" type="checkbox"/> AntiVirus Top Destinations
<input type="checkbox"/> Bandwidth Top Protocols	<input checked="" type="checkbox"/> Attack By Category	<input checked="" type="checkbox"/> AntiSpam Summary
<input type="checkbox"/> WEB Top Sites	<input checked="" type="checkbox"/> Intrusion Summary	<input checked="" type="checkbox"/> AntiSpam Top Senders
<input type="checkbox"/> WEB Top Hosts	<input checked="" type="checkbox"/> Intrusion Top Intrusions	<input checked="" type="checkbox"/> AntiSpam Top Sources
<input type="checkbox"/> FTP Top Sites	<input checked="" type="checkbox"/> Intrusion Top Sources	<input checked="" type="checkbox"/> AntiSpam By Score
<input type="checkbox"/> FTP Top Hosts	<input checked="" type="checkbox"/> Intrusion Top Destinations	<input type="checkbox"/> WEB Blocked Summary
<input type="checkbox"/> MAIL Top Sites	<input checked="" type="checkbox"/> Intrusion By Severity	<input type="checkbox"/> WEB Blocked Top Sites
<input type="checkbox"/> MAIL Top Hosts	<input checked="" type="checkbox"/> AntiVirus Summary	<input type="checkbox"/> WEB Blocked Top Hosts
<input type="checkbox"/> Customization Top Destinations	<input type="checkbox"/> 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

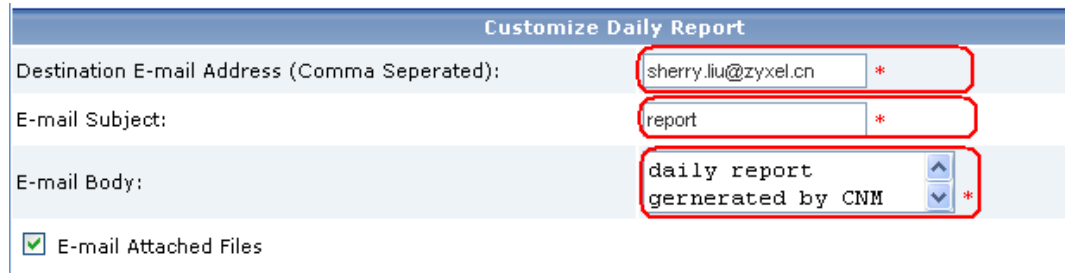


you get each time you've set will show nothing if you set "log store day=1". The date in the PDF /HTML file is the day before.

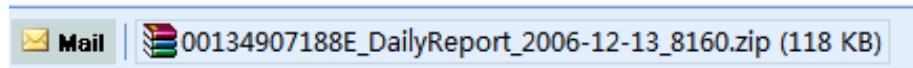
Below picture shows daily report sample received by user.



Here receiver 'Sherry.liu', subject 'report' and the mail body 'daily report generated by CNM' match the **Destination E-mail Address**, **E-mail Subject** and **E-mail Body** under **Schedule Reports>>Schedule Reports**.



All the customized reports are included in the .zip file with the name '00134907188E\_Daily Report\_2006-12-13\_8160'. And '00134907188E' 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 larger than 2M bytes.

## **2 FAQ**

### **2.1 Where to download CNM software and patches?**

CNM software and patches can be downloaded from <http://www.zyxel.com>.

### **2.2 How many types of license does ZyXEL offer?**

ZyXEL provides six kinds of license for Vantage CNM; they are 10, 25, 50, 100, 300 and 1000 nodes. However, user can combine any licenses to make their desired number of nodes. You can try Vantage CNM service, the trial period is 90 days and the max number of nodes it supports is 100.

### **2.3 What OS does Vantage CNM server support?**

CNM Server supports Windows XP Professional SP2, Windows 2000 SP4 and Windows 2003 Server SP1 English version. But it doesn't support Linux so far.

### **2.4 Will Vantage CNM support Microsoft Vista?**

Microsoft Vista will be supported from Vantage CNM 2.3 patch 1.

### **2.5 What browser does Vantage CNM server support?**

CNM Server supports IE version 6.0 or above, Firefox version 1.5 or above.

### **2.6 Does Vantage CNM support IE 7.0?**

IE 7.0 will be supported from Vantage CNM 2.3 patch 1.

### **2.7 What device and f/w version is supported by Vantage CNM 2.3?**

For more up to date information, please check the release note of each firmware release.

And currently, this is the list.

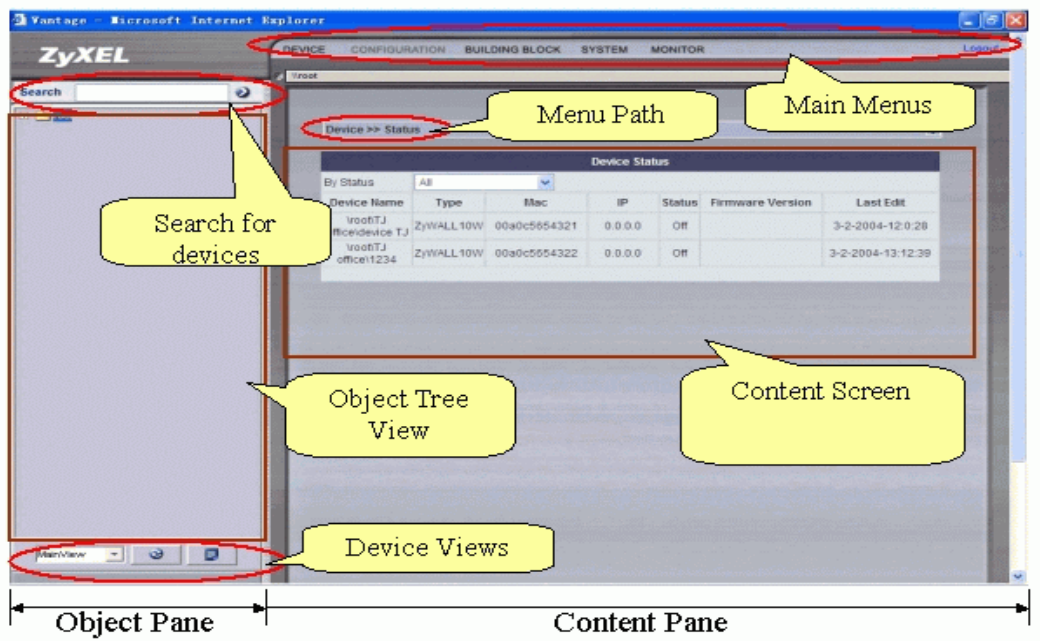
<b>Device Model</b>	<b>Device FW</b>	<b>New CNM 2.3 features</b>	<b>Reporting Function</b>
<b>ZyWALL 5</b>	3.64XD5 and later	Same as CNM 2.2	Traffic Report Attack Report VPN Report Web Usage Report Log Report
	4.00XD11&4.00XD12	IDP/AV/AS/CF myZyXEL.com Registration WLAN Zone enhancement	UTM Report Traffic Report Attack Report VPN Report Web Usage Report Log Report
	4.01XD4 and later	Remote management Redundant IPSec tunnel Firewall/AV/AS/IDP WLAN zone enhancement	UTM Report Traffic Report Attack Report VPN Report Web Usage Report Log Report
<b>ZyWALL 35</b>	3.64WZ5 and later	Same as CNM 2.2	Traffic Report Attack Report VPN Report Web Usage Report Log Report
	4.00WZ11 & 4.00XZ12	IDP/AV/AS/CF myZyXEL.com Registration WLAN Zone enhancement	UTM Report Traffic Report Attack Report VPN Report Web Usage Report Log Report
	4.01WZ4 and later	Remote management Redundant IPSec tunnel Firewall/AV/AS/IDP WLAN zone enhancement	UTM Report Traffic Report Attack Report VPN Report Web Usage Report Log Report
<b>ZyWALL 70</b>	3.65WM1 and later	Same as CNM 2.2	Traffic Report Attack Report VPN Report Web Usage Report Log Report
	4.00WM11&4.00WM12	IDP/AV/AS/CF myZyXEL.com Registration WLAN Zone enhancement	UTM Report Traffic Report Attack Report

	4.01WM4 and later	Remote management Redundant IPSec tunnel Firewall/AV/AS/IDP WLAN zone enhancement	VPN Report Web Usage Report Log Report
<b>ZyWALL P1</b>	3.64XJ5 and later	Same as CNM 2.2	Traffic Report Attack Report VPN Report Web Usage Report Log Report
<b>ZyWALL 10W</b>	3.64WH13 and later	Same as CNM 2.2	Attack Report Web Usage Report Log Report
<b>ZyWALL 2</b>	3.62WK12 and later	Same as CNM 2.2	Attack Report Web Usage Report Log Report
<b>ZyWALL 2+</b>	4.00XU2	Same as CNM 2.2	Traffic Report Attack Report VPN Report Web Usage Report Log Report
	4.01XU1 and later	Remote management Redundant IPSec tunnel NAT over IPSec	Traffic Report Attack Report VPN Report Web Usage Report Log Report
<b>P662HW-61</b>	3.40QR8 and 3.40QR9	Same as CNM 2.2	Attack Report Web Usage Report Log Report
<b>P662H-61</b>	3.40QR8 and 3.40QR9	Same as CNM 2.2	Attack Report Web Usage Report Log Report
<b>P662HW-D1</b>	3.40AGZ3 and later	Same as CNM 2.2	Attack Report Web Usage Report Log Report
<b>P662H-D1</b>	3.40AGZ3 and later	Same as CNM 2.2 Wireless	Attack Report Web Usage Report Log Report
<b>P653HWI-17</b>	3.40PN4 and later	Same as CNM 2.2	Attack Report Web Usage Report Log Report

## 2.8 What is the max number of devices that Vantage CNM 2.3 supports?

At the time this document is composed, Vantage supports up to 1000 devices. For most up to date information please check the latest release note of Vantage CNM.

## 2.9 What is OTV (Object Tree View), Content Screen ...etc?



## 2.10 Why can't I get complete OTV (Object Tree View)?

On Vantage client, you don't need to install additional software to access Vantage Server. But you should use IE(Internet Explorer) to access Vantage server, please make sure the IE you use is Version 6.0 or above. And if you have Java plug-in installed on your computer already, please verify if Java plug-in version is not later than 1.5.0. If it is, you should remove the plug in from Control panel, and install a new one. Vantage client will be triggered to download the latest Java plug-in when it logs in to Vantage server for the first time if without Java plug-in.

## 2.11 When I login to Vantage, I get this error message "HTTP Status 500 - No Context configured to process this request".

Make sure your Vantage server is already running first. When Vantage service is ready, the icon on system tray should turn to blue. Otherwise, if it's starting, it's green. If you see this error message when connecting to Vantage server, please make sure

that you type the URL correctly, <http://<Vantage Server's IP:8080>>. Please note that the URL is case sensitive.

## 2.12 My Internet Explorer (IE) does not trust the Certificate from Vantage server, should I trust it?

You should trust it in order to access Vantage server

## 2.13 How can I skip the warning message of Certificate when I login the CNM?

You can import a certificate which is applied by a trusted CA into your Vantage server then it will not show the warning message. Please refer to the steps below:

1. Go to **System >> Certificate Mage**, click **Create CSR**, then input certificate request information. In Common Name field, you should fill in your vantage server's IP address.

Create CSR	
Input Certificate Request Information	
Certificate Alias	sherry *
Common Name	172.25.24.119 *
Organization Unit	zyxel *
Organization Name	cso *
Locality Name	wuxi *
State Name	jiangsu *
Country	cn *
Validity	2007-01-09 * Format: yyyy-MM-dd
KeyStore Type Option	
KeyStore Type	jks *

2. Apply a certificate from trusted CA using the CSR you just created, then import the certificate into your vantage server.

Notes: You can get CA from verisign.com, thawte.com, trustcenter.de and so on.

CSR(Certificate Signing Request) Key

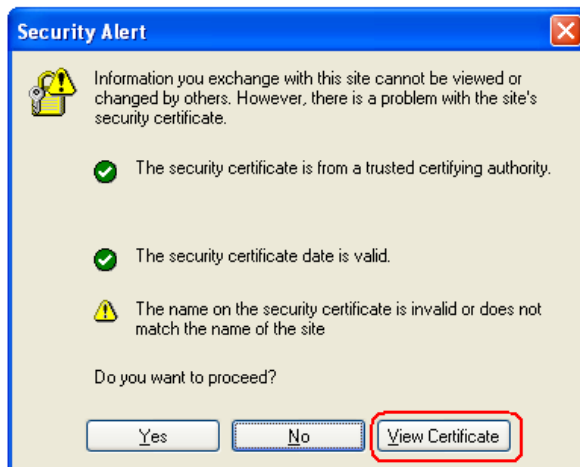
```
MIIBpDCCAQ0CAQAwZDELMAkGA1UEBhMCY24xEDA0BgNVB
AgTB2ppYW5nc3UxDALBgNVBAcTBHd1
eGkxDDAKBgNVBAoTA2NzbzEOMAwGA1UECxFenl4ZWwxFjA
UBgNVBAMTDTE3Mi4yNS4yNC4xMTkw
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAIQSSKaulyGQ
0NGJVPAYHY3diM3aLmnMvA/CrVUu
VfcfapjAP3B6nKQmo66JWSJyQi70mMNN8QnC2b7UXKmFF2d
2NEyUBgKVcmnQkaRcJa0u5WAc3Mpc
bcEKyt04zJa0WVGmq/O+FY26whmKZVt8gtCQfBB0ljx4lebchihz
8D4RAgMBAAAGgADANBgkqhkiG
9w0BAQQFAA0BgQAJw/9t8cEH+GoGYdtbKVP2X/m7iKqrrgwx8
OioCSNC+puTXS0WqgdLfiw/Mohd
```

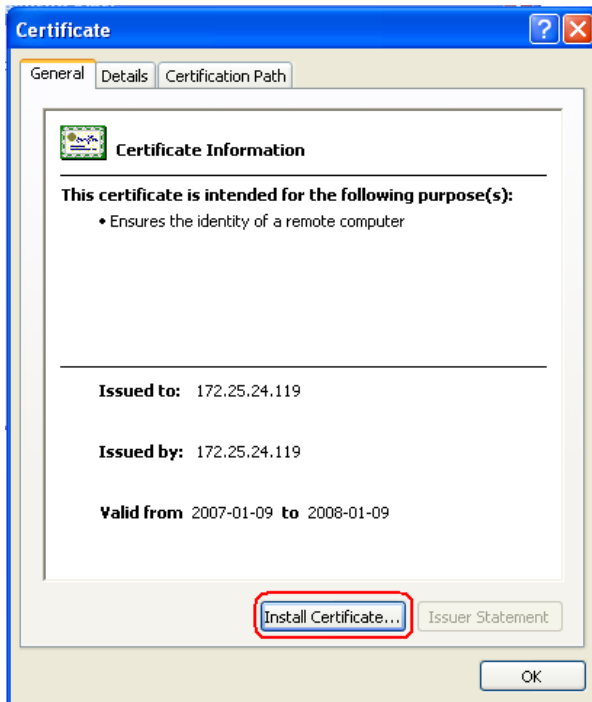


- 3. If the certificate is imported successfully, you can get the detailed information of the certificate as below.



- 4. When you login the vantage server at the first time after importing the Certificate, you will see the error message either. Click the icon, a warning window will be shown next. Click **View certificates**, and install the certificate into your IE browser.





5. If the certificate is imported successfully, the message will be shown as below:



6. Logout and then login the vantage server again, you will not see the warning message.

**Note:** In vantage server, certificate with format "PEM (Base-64) encoded X.509" is supported.

## 2.14 When create an administrator in SYSTEM>>Administrators, what's the difference between Name and UID?

Login Name is the name administrator needs to input in order to log in Vantage server; Name is identification easier for users to memorize.



## **2.15 When a SUPER user changes the NORMAL USER's profile, the access permission of normal user should be changed. But what should be done to make the change effective?**

Logout, then login again. If user login and is operating in the system now, his template cannot be changed.

## **2.16 Which MAC address should I input when register a device?**

LAN MAC address

## **2.17 What should I do if I want to register hundreds of devices at one time?**

Users can edit all of devices' MAC address, Model type, and Model name...etc in one XML file, and then import the XML file into Vantage.

**DEVICE>>Registration>>Associate** to a customer (either yes or no will do)>>**Import** from a Configuration File.

## **2.18 Where can I get examples of the XML files?**

After you install Vantage on your system, you would get the XML file in this path, {Installed path}/\conf\xmlImportExample. You can open this file via editor software.

But note XML fields must not contain a "return" character. EX, below is forbidden:

```
<mac>00a0c544e2a7
</mac>
```

You must write the field in one line, like this <mac>00a0c544e2a7</mac>

## **2.19 What's the difference between System>>Log and Monitor>>Alarm?**

For **Monitor>>Alarm**, it includes system's alarm and devices' alert (attack).

For **System>> Log**, it includes normal operations, add device, delete device...etc. are recorded here.

## **2.20 Why I can not receive the Alert/Alarm mails?**

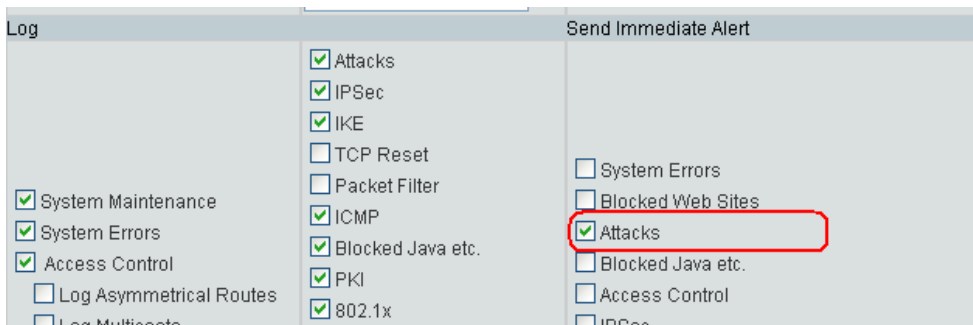
Step1. Go to **System>>Preferences**, check if the SMTP server is configured correctly.

System : Preferences			
Server	Notifications	User Access	User Group
<input type="checkbox"/> Vantage CNM Server			
Public IP Address	172.25.24.119 *		
Web HTTPS Port	443		
Web HTTP Port	8080		
<input type="checkbox"/> FTP Server			
IP or Domain Name	172.25.24.119 *		
User Name	vantage *		
Password	..... *		
<u>VRPT Management</u>			
<input checked="" type="checkbox"/> Mail Server			
IP or Domain Name	ms01.zyxel.cn *		
Mail Sender	sherry.liu@zyxel.cn *		
User Name	zycnlw00593		
Password	.....		
		Apply	Reset

Step2. Go to **Notifications**, check if the **Send alarm report to field** is configured correctly.

System : Preferences			
Server	Notifications	User Access	User Group
<input type="checkbox"/> Firmware Upgrade			
<input type="checkbox"/> Device Owner			
<input type="checkbox"/> E-mail [ ] *			
<input type="checkbox"/> Logs			
<input type="checkbox"/> E-mail [ ] *			
<input type="checkbox"/> Alarms			
Send alarm report to :			
<input type="checkbox"/> Device Owner			
<input type="checkbox"/> E-mail [ ] *			
Send device alarm notification to Device Owner :			
<input checked="" type="radio"/> Immediately			
<input type="radio"/> Active Alarm Consolidation Period [ 1 ] * (1 - 60 minutes)			
<input type="checkbox"/> Device Offline			
<input type="checkbox"/> Device Owner			
<input type="checkbox"/> E-mail [ ] *			
<input type="checkbox"/> UTM Device Service Expire			
<input type="checkbox"/> Device Owner			
<input type="checkbox"/> E-mail [ ] *			
Note:Expire Notification will be send at 30-days,10-days or 0-day before Expiration Day.			
		Apply	Reset

Step3. Go to **Configuration>>Device Log**, check if the **Attacks** check box is enabled.



## 2.21 What should I do if I configure something on device but would like to synchronize the configuration with settings on Vantage?

Go to **Vantage>>DEVICE>>Synchronize**, then select **device overwrite Vantage**.

Once configuration is changed on device by local administrator with console port, no information is sent to CNM server. As a root manager, you should do the action mentioned above to synchronize.

Therefore, when managing so many devices at certain time, we should coordinate with each local administrator.

## 2.22 If my Vantage server is behind a NAT/Firewall router, and I would like to allow outsiders to connect Vantage server's management interface from Internet. What should I do?

Please make sure you have forwarded TCP port 8080 and 443 in configuration of NAT and Firewall.

## 2.23 On each device, we should enter Vantage Server's IP address as the manager IP, but how many management IP can each device have?

One device should be under one CNM's management domain. So a device can have only one manager IP.

## 2.24 When accessing Vantage Server by Internet Explorer, why does my web browser shut down without any caution sometimes?

There are three possible causes:

1. Check IE version is 6.0 or later.
2. Lack of system resources. Please check if your system memory is sufficient on Vantage server and Vantage client. Please refer to Vantage Quick Installation Guide for CPU/Memory requirements.

3. The popped up window is killed by other applications. Some "advertisement killer" applications may kill Vantage popped up window. If there is Ad.killer on your Vantage client system, please turn it off.

**2.25 I can upload firmware from “Firmware Management” page, but this firmware is not available in “Firmware Upgrade” page. What’s wrong?**

Please make sure the firmware package (zip file) is downloaded from ZyXEL public WEB site. The package should include 3 files:

<b>*.xml</b>	This file describes the product line, model name, version, and release date of this firmware package.
<b>*.bin</b>	The firmware file
<b>*.rom</b>	The default configuration file for this firmware

Please note the firmware package users download from <http://www.zyxel.com> also includes release note in PDF, users don’t need to remove this file from the zip file. This file won’t affect Vantage’s operation, but this file will be ignored by Vantage.

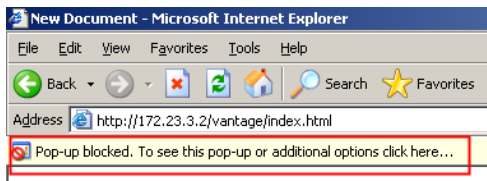
**2.26 How can I see the report for a device?**

To see the report for a specific device, select the device from OTV tree and click the report correspondingly.

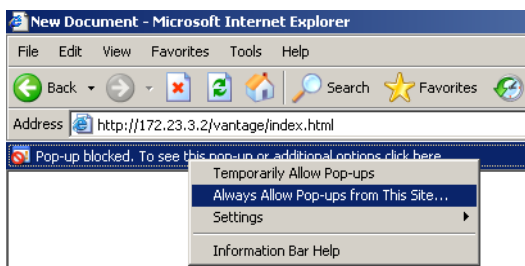
Please note that the device should be added to VRPT first. More detailed info please refer to [1.9.3.1 Setting VRPT server for managed device](#)

**2.27 Why do I get the message ‘Pop-up blocked’ when I try to login Vantage server?**

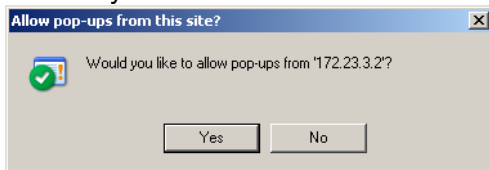
In Windows XP SP2, Pop-up windows will be blocked by default, this might affect CNM when login. It will show a bar with the message as below.



Right click the bar and choose “Always Allow Pop-ups from This Site”.



Click **Yes** to double confirm. Then the Vantage login window can pop up successfully.



## 2.28 When I want to delete VPN rules of a certain device, it seems the rules can't be deleted?

It's caused by time delay. Choose one of them, deleting it, wait for some time. It takes time to synchronize between two sides. Otherwise, try more times. Or you can use Force delete to delete a tunnel constrainedly.

You can refer to [1.7.1.2 Use Force button to delete a tunnel](#)

## 2.29 In OTV, a device is shown with green, but why it is shown with status of "off" on right window?

It's normal. Because, time needed to synchronize with two sides and then show us the real status. And vice versa, maybe status is **off** in right window but gray icon in the left.

Suggestion: before some operation, try to refresh the OTV with fresh button at left-bottom.

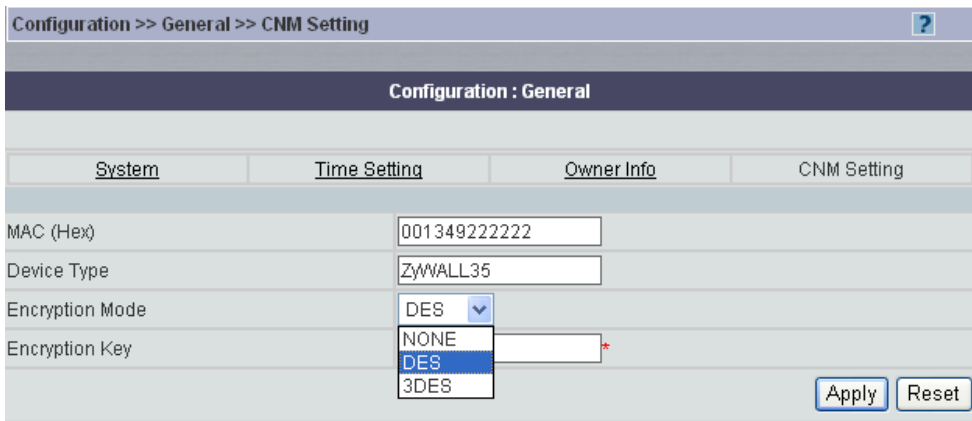
## 2.30 Currently, my device is managed by CNM server with no encrypt-mode. And it's green in OTV. Then if I want to use encrypt mode with DES algorithm, what should I do?

You should use same settings on both sides and reset the states on devices.

For example, in **configuration>>General>>CNM Setting**, choose the algorithm you want. Here, I select DES. And key is "12345678".

**Note:** after you applied it, this doesn't send to device to synchronize.

It's used in local database. Usually CNM server uses a unique ID to separate lots of devices and use that ID to query info for that device, including encryption mode, key. Then it decides whether to decrypt those packets for search further info about it. Therefore, remember, settings here for encryption takes effect locally merely.



So, you have to change the configuration of you device. For example, if we adopt DES with 12345678, 3 commands should be executed in command line mode of ZyWALL:

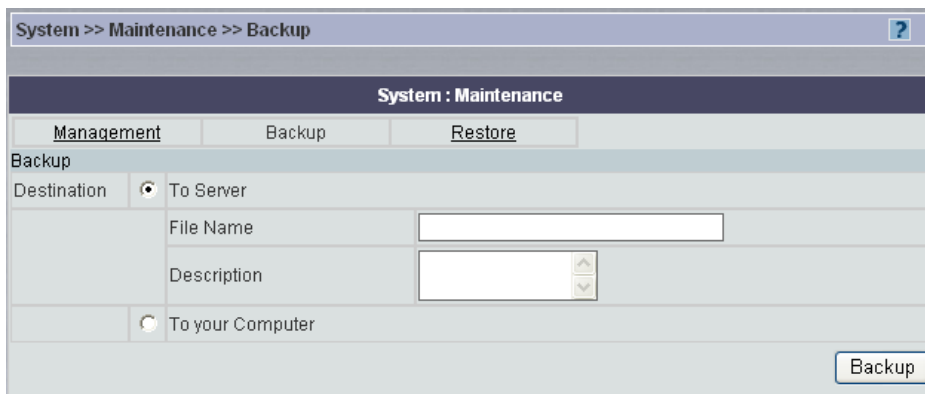
- cnm encrymode 1
- cnm encrykey 12345678
- cnm reset

### 2.31 If I want to re-install the CNM but not lose my configuration, what should I do?

Use the backup feature in **maintenance**

Backup file is a zip file, it represent all backup data for the whole system, including database files (backup.sql & vrpt.sql), VRPT’s schedule folder and rom/log/firmware folder in Vantage FTP. Therefore, you can backup the configuration first and then restore it to CNM server before re-installing the CNM.

Go to **system>>maintenance>>Backup**



If you choose **To Server**, then it will be placed under folder **Vantage-CNM-2.3 /data/backup**. It’s a zip file. Here, we suggest use **To your Computer**. Otherwise, when uninstalling the CNM, those folders and files will be deleted of course.

1. Re-install
2. Re-activate
3. Restore backed up file in “maintenance>>restore”.

### 2.32 I have registered the MAC address of devices supported in the list, and the activation on device “cnm active 1” & “cnm managelp xxxxx”. But the device in OTV is gray, what should I do?

1. Make sure your F/W version is supported by CNM version of CNM version you used.
2. Make sure the routing between them has no problem.
3. Make sure the MAC address is LAN MAC.
4. When registered that model, confirm you chose the corresponding model type.
5. Make sure working mode is the same. That is no encryption both or encryption mode both.

### 2.33 Why the configuration between device & CNM is not consistent with each other?

Once configuration is changed on device by local administrator with console port, no information is sent to CNM server. As a root manager, you should do the action to synchronize by using **Device>>Synchronize**.

Therefore, when managing so many devices at certain time, we should coordinate with each local administrator.

### 2.34 After I have reinstalled the CNM, where could I get the new service key and activation key?

After reinstallation, when you log in with root account, new keys are required.

You have to use the new authentication to obtain them.

Just go to [www.myzyxel.com](http://www.myzyxel.com). Login with your account set before. And choose the item. Then click **reinstall**.

The screenshot displays a management interface for a ZyXEL device. It features a blue header bar labeled 'Product Information' and another labeled 'Manage Product'. Under 'Product Information', the device name 'csojoe' is listed, along with its serial number, product name, authentication code, and activation key. The 'Manage Product' section provides instructions on how to manage the registration and includes three buttons: 'Rename', 'Transfer', and 'Reinstall'.

```
Product Information
csojoe
Serial Number: S060T04000172
Products: VANTAGE CNM
Authentication Code / MAC Address: df0290be948b
Activation Key: 0A9401C9810AB948B9D234075D901A4085955A2BB5F773281

Manage Product
Manage this product's registration by clicking on the appropriate buttons below:
csojoe [Rename] [Transfer] [Reinstall]
```

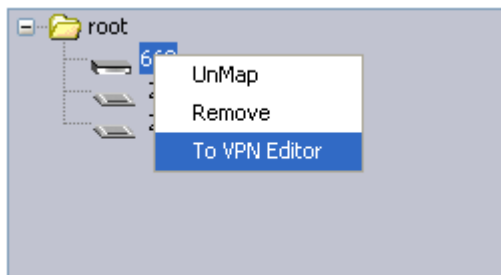
**2.35 Why I can not see the “Reinstall” button when I login my www.myzyxel.com?**

Only the CNM Standard version can be un-installed, for the CNM trial version, it can only be installed for once.

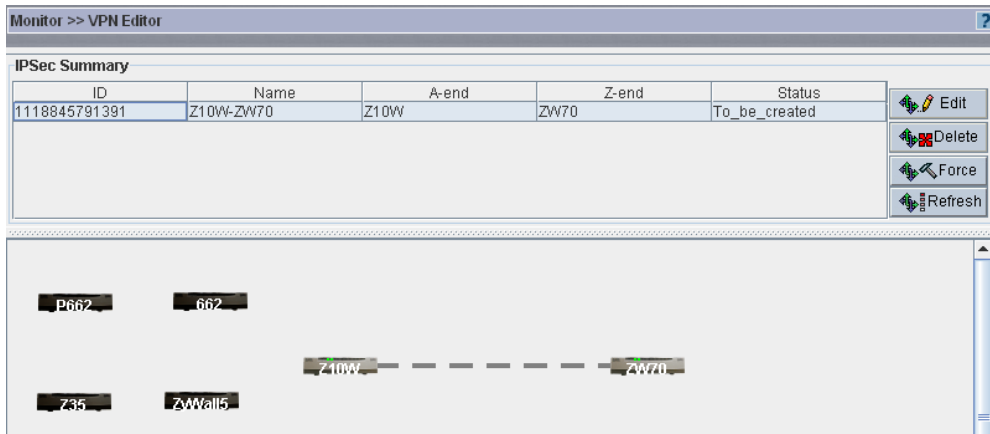
**2.36 How to apply the one-click VPN feature in VPN editor?**

You can get the explanation from the name of one-click. But the constraint there should be no NAT devices appear between the 2 devices that you want to create VPN tunnels on.

Right click on the device that you want to put in VPN editor, and click **to VPN Editor**

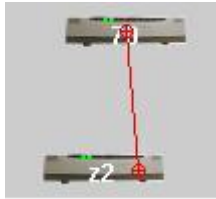


Then you will see the following page.



1. Right click one of the online devices.
2. Click on this “VPN” label.
3. Keep clicking the left button of mouse, and then move the cursor onto the ZyWALL70.
4. Release left button of mouse.





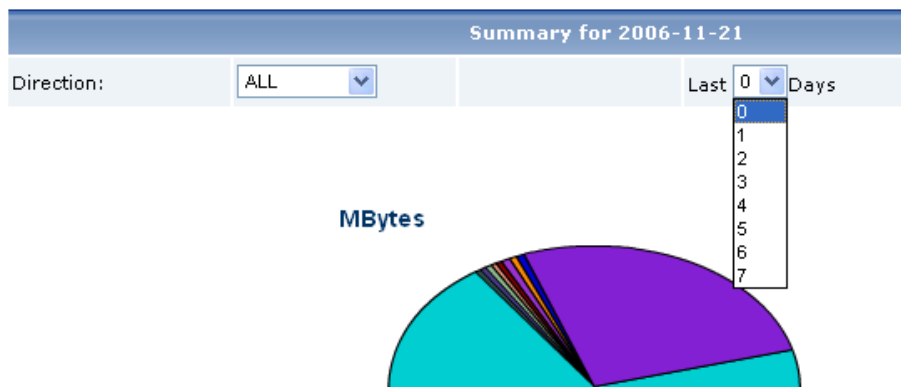
Then the configuration page is shown to you for those 2 devices.  
 More info, please refer to [1.7.1 Creating VPN tunnel by VPN Editor \(One-click VPN\)](#)

**2.37 When using “monitor>>VPN editor” to create a rule between 2 devices, why the line between them is dotted? Does it mean it fail?**

- After creating a tunnel between 2 devices, there should be a line between them.
- a) A gray dashed line means that the CNM server has not yet synchronized VPN tunnel information with both devices. This may be because CNM hasn't so far communicated with one of the devices.
  - b) A gray solid line means that the VPN tunnel is set up between the devices but the tunnel is not active yet(no traffic).
  - c) A green solid line means an active tunnel (with traffic) between the ZyXEL devices.

**2.38 Where can I change the number of days in “report>>bandwidth>>summary”?**

Yes, you can change it. Here, you can select from 1~7.

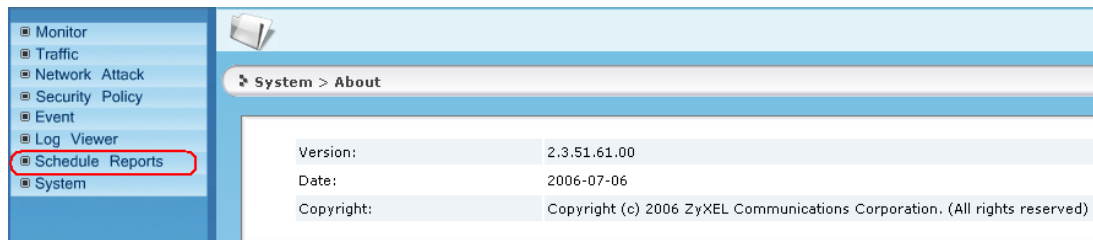


And if you want to increase the number, go to **System>>VRPT management>>Configuration**, there, number of days for storing logs is consistent with the number of days you can get summary like above.

**2.39 Where can I create one time report?**

Go to **Report>>Report**, you can see the **Vantage Report** screen as shown next.

The current release and copyright for Vantage Report is showed on this screen.



Then go to Schedule Reports>>Schedule Reports>>Add Daily Report.



More info, please refer to [1.9.3.3 Configuring Schedule Report](#)

## 3 Trouble Shooting

### 3.1 Trouble between Vantage Server & Client

Step1. Install the latest Java from the [www.java.com](http://www.java.com) before your client visit the Vantage Server.

**Note:** The Java plug-in version should be or later than 1.5.0.

Step2. Check if the routing between Server & Client is ok. If Vantage is behind a NAT router, you should forward TCP port 8080 and 443.

Step3. Collect logs from Vantage Server from "[<Installed folder>\logs\](#)"

### 3.2 Trouble between Vantage Server & ZyXEL devices

Step1. Check packets can be sent between Vantage & devices. If Vantage is behind a NAT router, then you should forward UDP port 1864. So CNM server can be accessed from outside. If ZyXEL devices are behind a NAT/Firewall device, you should forward UDP port 1865.

Step2. Check if the encryption mode & encryption key configurations are the same on both Vantage Server & devices.

Step3. Check firmware version of the devices to make sure it supports Vantage Server's current version.

Step4. Collect logs from Vantage Server for technical support's reference.

#### **On Device, please do following:**

1. Using Terminal program to access ZyWALL via Console
2. Use "sys baud 5" to set console speed to 115200.
3. Turn on CNM debugging in SMT Menu 24.8 by "cnm debug 1"
4. Save the dumps into one file.

**On Server:** Please collect Vantage server's logs from "[<Installed folder>\logs\](#)"

### 3.3 Trouble between Vantage Server & Vantage

#### Report

Step1. Check if the Vantage report is running by checking if the port 514 is available from the “netstat -a” in the command line

**Note:** If your OS is Windows XP sp2, you should forward port 1099 and port 514 on the windows firewall setting.

Step2. If the CNM and VRPT are installed in the different server, make sure the routing among Vantage CNM & VRPT server is ok.

Step3. If the CNM and VRPT are both behind the NAT, please check the NAT port forwarding rule and firewall rule, for more details please refer to the CNM deployment, scenario A/B/C.

### 3.4 Trouble in migration

Step1. Check if CNM has been stopped.

Step2. Check if CNM version is 2.2 Patch3 or CNM2.3 Lite (patch1).

Step3. Check if one port or ports are occupied (1864, 8080, 443, 3306, and 3305), usually, the Web server and SQL server will take this port.

Step4. Check if the free disk space in the destination folder is larger than 600M.

Step5. If the data migration fails, send the log [c:\upgradeLog](#) to Zyxel support.