

How to configure HA (High Availability) for support VPN more than 10,000 site by using Mikrotik product

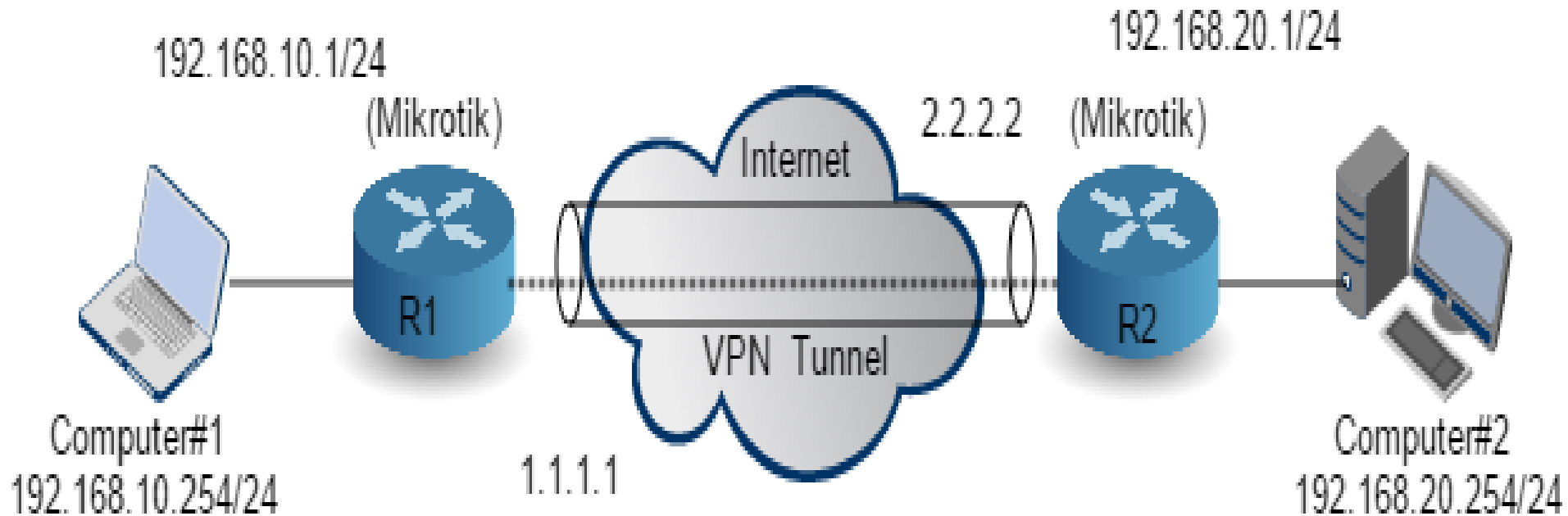
Tawan Thongpook
Mikrotik Certified Thailand

Topic

- Requirement
- Design
- Implement

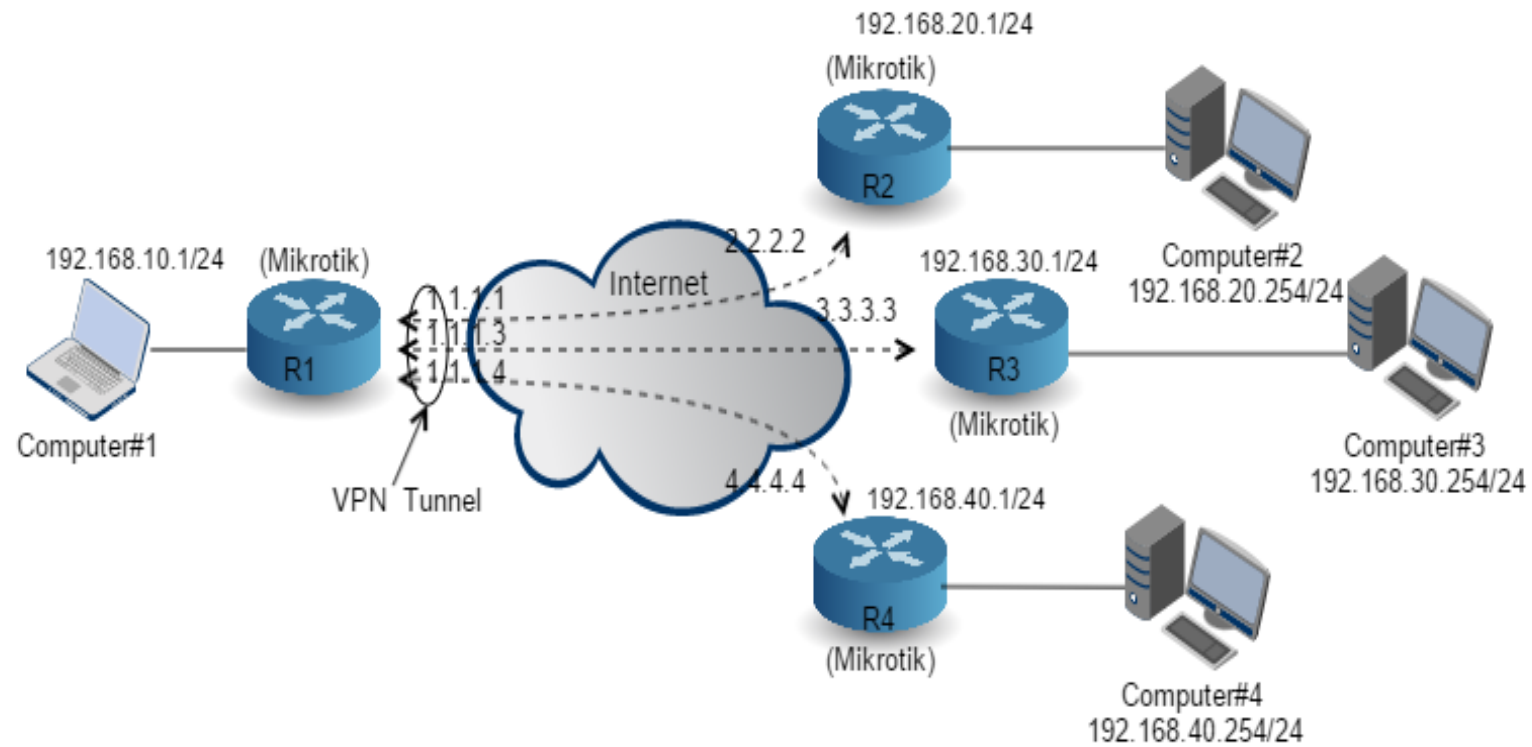
VPN

Virtual Private Network (VPN) คือการจำลองเราเครือข่ายสาธารณะ (**WAN**) มาทำเป็นท่อจำลองเพื่อเชื่อมเครือข่าย **LAN** มายังสาขาใหญ่ หรืออาจเชื่อมต่อสาขาย่อยกันเอง



S-M-L

1 -> 2 -> 5 -> 10 -> 50 -> 100 -> 10,000

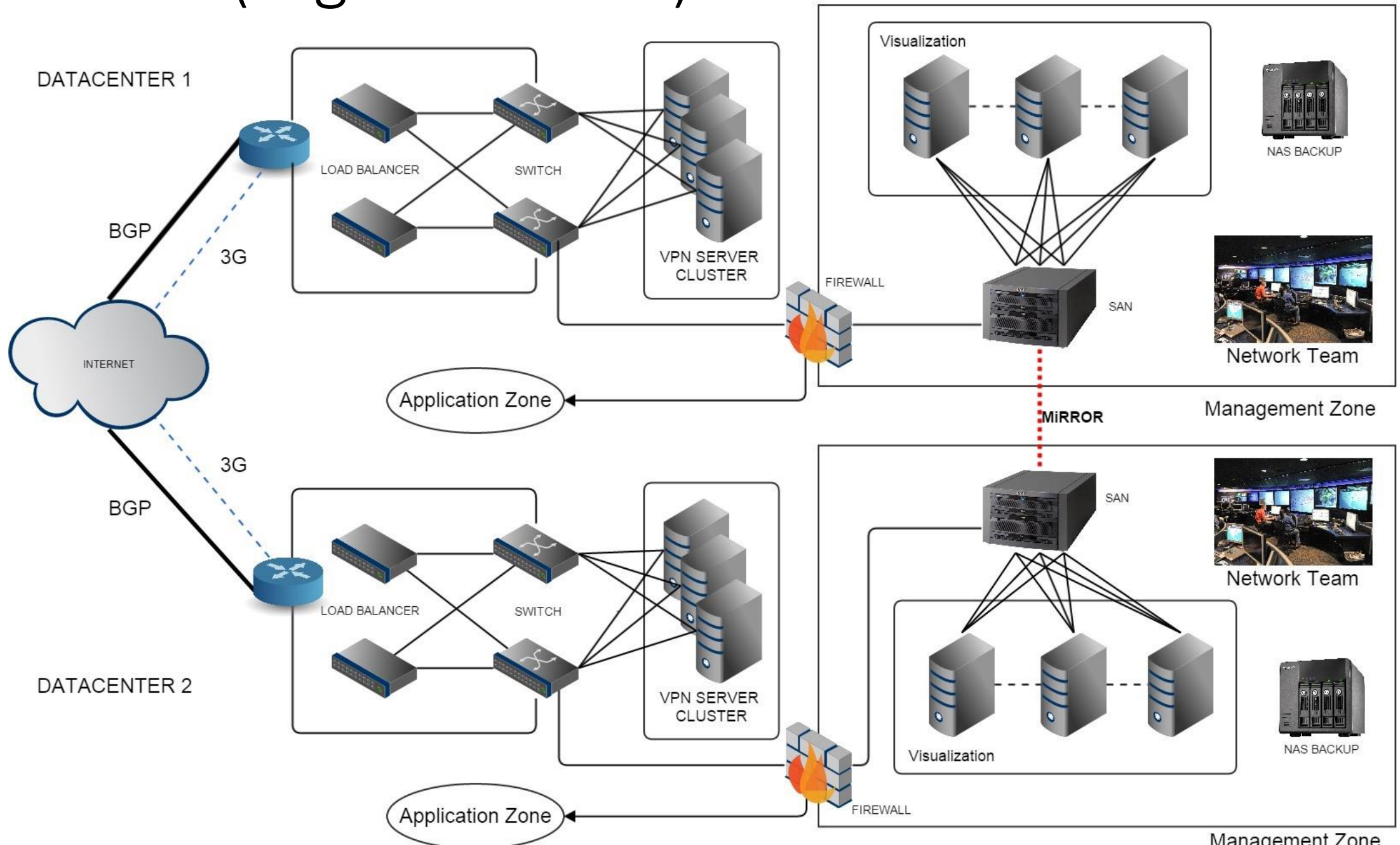


การออกแบบ VPN ที่มีมากกว่า 10,000

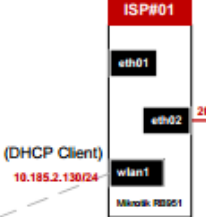
สิ่งที่ต้องคำนึงถึง

1. ต้องไม่ล้ม (High Available)
2. ต้องขยายได้ไม่จำกัด (Scalability)
3. ต้องอิสระ (Independency)
4. ต้องง่ายต่อการติดตั้ง (Easy to Install)
5. ต้องดูแลได้ (Manageability)

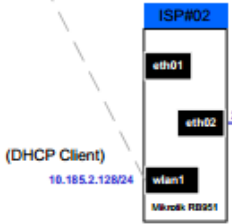
ต้องไม่ล้ม (High Available)



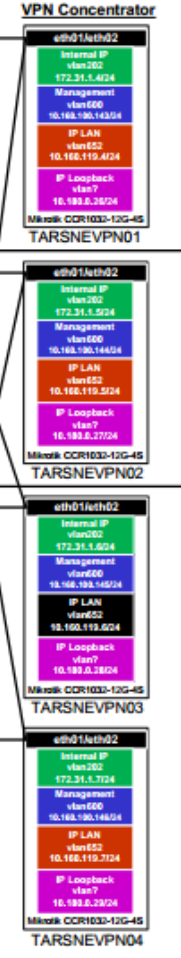
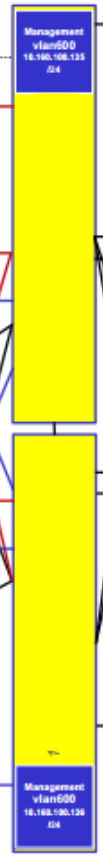
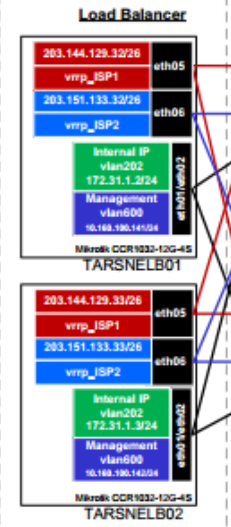
10.185.2.0/24
Router
Request I2tp to
203.144.129.31
203.151.133.31



VRRP_ISP1:
VRRP_ISP2:



172.31.1.0/24
VLAN 202
(สำหรับ Internal IP ที่จะรับจาก Mikrotik)

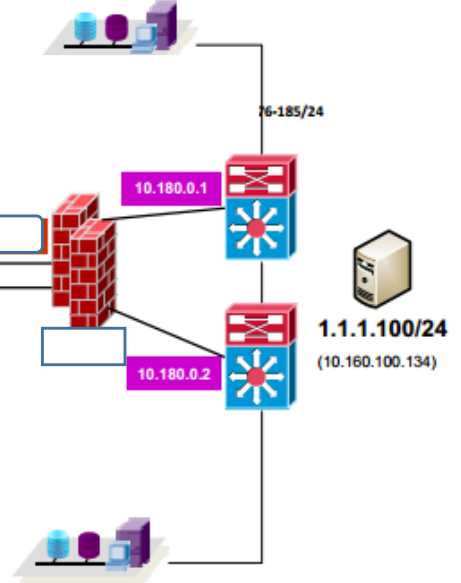


OSPF
LB : 10.180.0.x
OSPF Process 100
OSPF Area 0
Network Loopback & GRE
Only

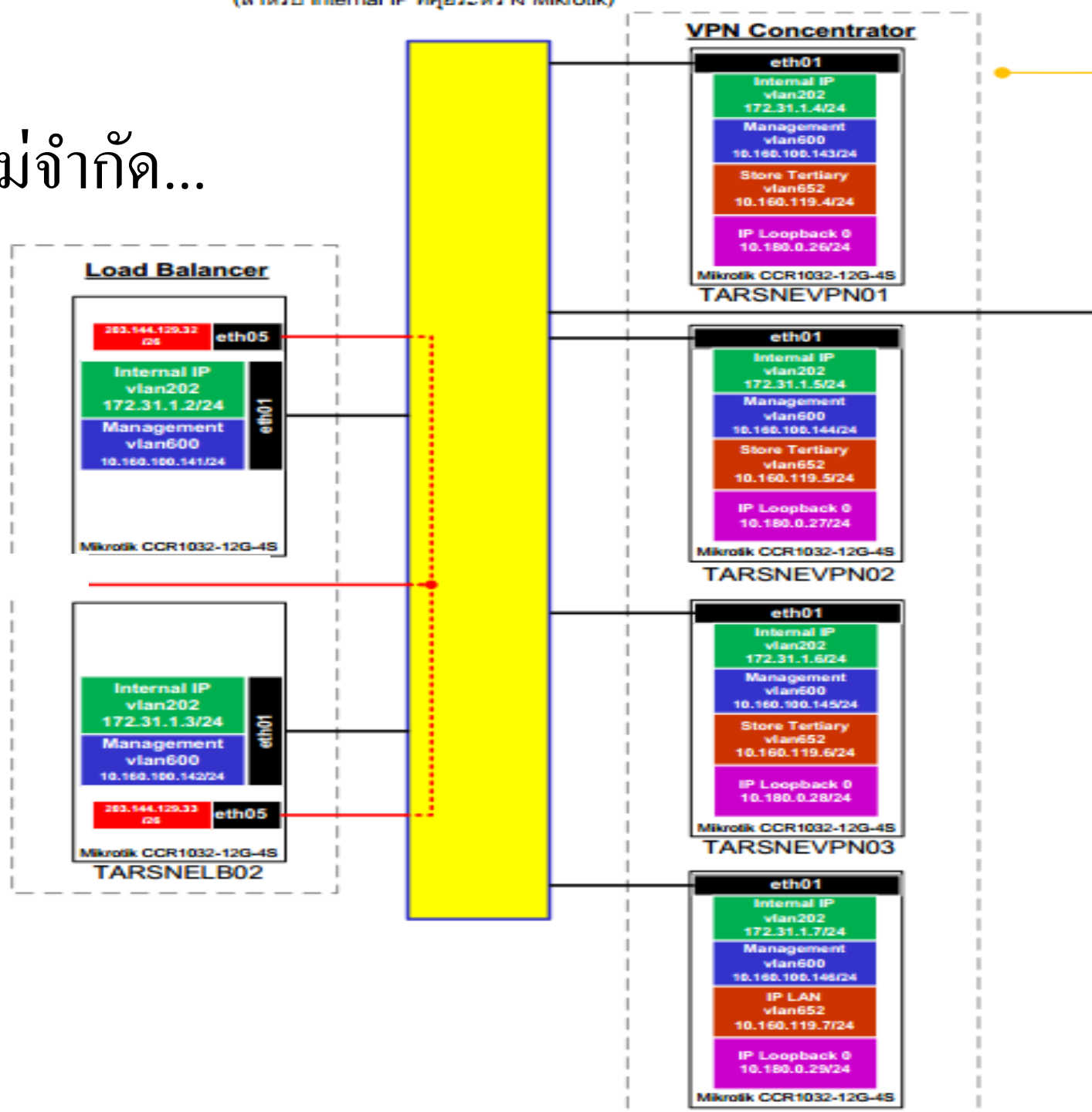
BGP
LB : 10.180.0.x
BGP AS:65100
BGP : Neighbor 10.180.0.1,
10.180.0.2
Redist Static to BGP

VLAN 652

IP LAN :

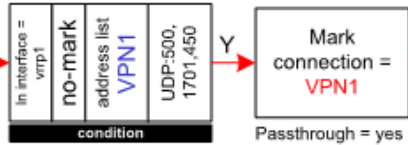


ขยายได้ไม่จำกัด...

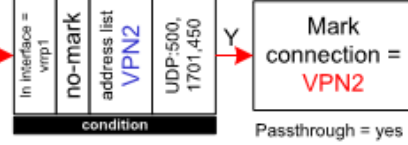


Prerouting Mangle

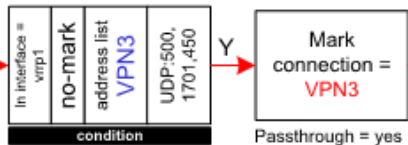
0# Mangle the public store IP from address list



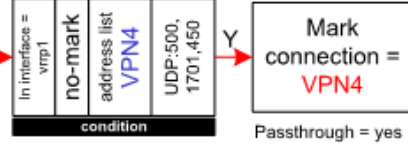
1# Mangle the public store IP from address list



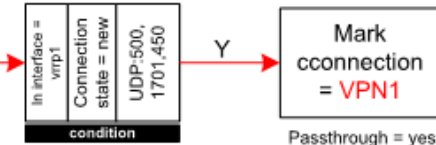
2# Mangle the public store IP from address list



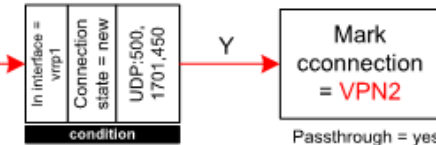
3# Mangle the public store IP from address list



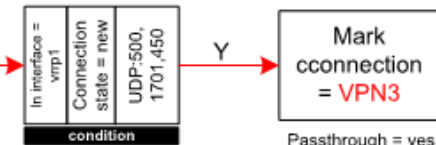
4# Mangle new connection by using nth (1/4) to VPN1



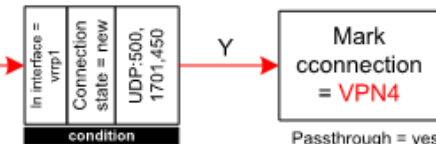
6# Mangle new connection by using nth (2/4) to VPN2



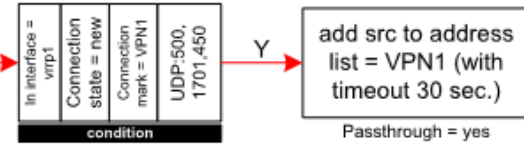
8# Mangle new connection by using nth (3/4) to VPN1



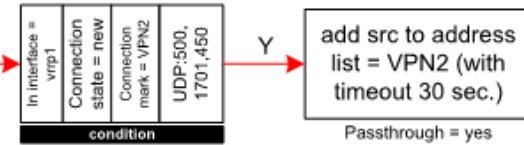
10# Mangle new connection by using nth (4/4) to VPN2



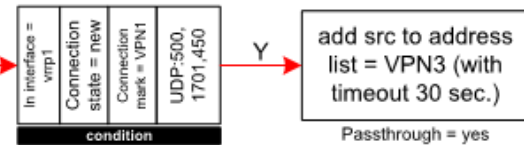
5# add source IP of mark "VPN1" connection into address list VPN1



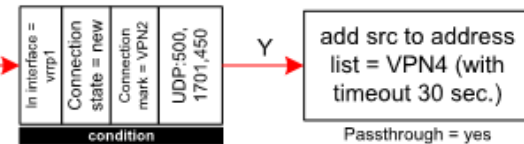
7# add source IP of mark "VPN2" connection into address list VPN2



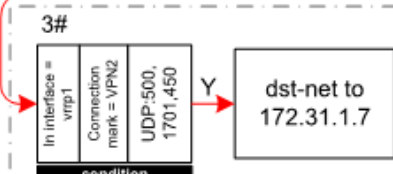
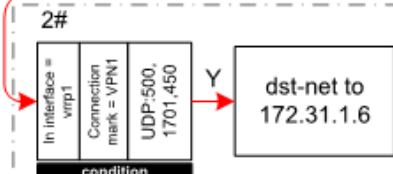
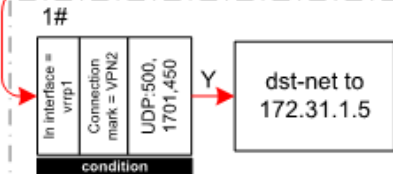
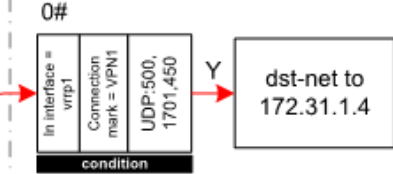
9# add source IP of mark "VPN3" connection into address list VPN3



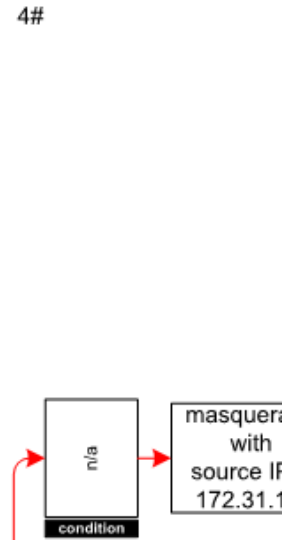
11# add source IP of mark "VPN4" connection into address list VPN4



Destination NAT



Source NAT



ต้องอิสระ (Independent)

- ตัว **Server VPN** จะมีความอิสระต่อกันโดยมีการกระจายโหลดไปตามค่า **Maximum** ที่เรากำหนดขึ้น ในกรณีนี้เรากำหนดให้ตัวหนึ่ง **Load** ไม่เกิน **2,000 Client** ต่อ **1 VPN Server**
- เครื่อง **Client** สามารถกำหนดหาเส้นทางเลือกเองได้ในกรณีถ้าเชื่อมต่อ **VPN Server 1** ไม่ได้ก็จะไปยัง **Server 2** ไปเรื่อยๆ โดยดูจากเวลาที่ **Respond**

ต้องง่ายต่อการติดตั้ง

- ระบบนี้ได้พัฒนาต่อเพื่อให้ติดตั้งได้ง่ายที่สุด เพราะได้กำหนด **Config** มากจากส่วนกลางไปยังอุปกรณ์โดยตรงเมื่อนำอุปกรณ์มาเสียบเข้าระบบ จะทำการเชื่อมต่อเข้าสู่สำนักงานใหญ่ได้อัตโนมัติ หรือรอกการอนุมัติได้
- สายสัญญาณทุก **port** ได้ใช้การกำหนดสีแทนเพื่อสื่อสารกับช่างได้ง่าย
- มีการพัฒนา **Application** บนมือถือที่จะทำการส่งตำแหน่ง **GPS** และ **SN** พร้อมสภาพการติดตั้งไปยังระบบทันทีเพื่อส่งมอบงานให้แล้วเสร็จ

Dashboard Login

Email

admin

Password

.....

Log in

Stay logged in

เข้าสู่ระบบ

Network Management Systems & Mikrotik

Introducing of the RouterBOARD



Search dashboard

Template : ทั้งหมด | โชน : ทั้งหมด | ภาค : ทั้งหมด | จำกัด : 100 | คำค้นหา : (ถ้ามี) ค้นหา

Dashboard

HQ Install (Dummy)

เริ่มต้นการติดตั้ง Dummy Config ให้กับ Mikrotik

1 %

Device IP : 192.168.66.1

Username : admin

Password : default mikrotik password

Start HQ Install

Provisioning

HQ Install (Dummy)

Dummy List

Manual Approve

Auto Approve

Approve List

Group Deployment

Import / Export

Member Management

Template Management

Server VPN

Server Dummy

Summary Report

Monitor

Event / History

Backup / Restore

Help

Quick Set
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
OpenFlow
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.nf
Manual
New WinBox
Exit

PPP

Interface PPPoE Servers Secrets Profiles Active Connections

PPP Scanner PPTP Server SSTP Server L2TP Server OVPN Server

Name	Type	L2 MTU	Tx	Rx	Tx Paq
ยังไม่มี Connection					

ยังไม่มี Connection

File List

Backup Restore Find

File Name	Type	Size	Creation Time
ยังไม่มีไฟล์ใดๆ			

ยังไม่มีไฟล์ใดๆ

0 items 18.1 MiB of 128.0 MiB used 85% free



admin | [ข้อมูลส่วนตัว](#) | [ออกจากระบบ](#)

Search dashboard

Template : ทั้งหมด | โชน : ทั้งหมด | ภาค : ทั้งหมด | จำกัด : 100 | คำค้นหา : (ถ้ามี)

- Dashboard
- Provisioning
- HQ Install (Dummy)
- Dummy List
- Manual Approve
- Auto Approve
- Approve List
- Group Deployment
- Import / Export
- Member Management
- Template Management
- Server VPN
- Server Dummy
- Summary Report
- Monitor
- Event / History

Configure Wizard

เริ่มการส่งไฟล์ที่ตั้งค่าแล้วไปยังอุปกรณ์ Mikrotik

25 %



Device IP : 192.168.66.1
 Username : admin
 Password :
 Status : **Connected**
 Serial Number : 4AC802F2274F
 Version : 6.15
 Board-Name : RB951Ui-2HnD
 Chosen Template : Dummy

เมื่อ สามารถเชื่อมต่อกับอุปกรณ์ได้ ระบบก็พร้อมที่จะทำการ FTP ไฟล์ dummy เข้าสู่อุปกรณ์

Quick Set

- Interfaces
- Wireless
- Bridge
- PPP
- Switch
- Mesh
- IP
- IPv6
- MPLS
- OpenFlow
- Routing
- System
- Queues
- Files
- Log
- Radius
- Tools
- New Terminal
- MetaROUTER
- Partition
- Make Supout.rif
- Manual
- New WinBox
- Exit

PPP

Interface | PPPoE Servers | Secrets | Profiles | Active Connections

PPP Scanner | PPTP Server | SSTP Server | L2TP Server | OVPN Server

Name	Type	L2 MTU	Tx	Rx	Tx Pad
0 items out of 7					

File List

Backup | Restore

File Name	Type	Size	Creation Time
0 items			

18.1 MiB of 128.0 MiB used | 85% free

- Dashboard
- Provisioning
- HQ Install (Dummy)
- Dummy List
- Manual Approve
- Auto Approve
- Approve List
- Group Deployment
- Import / Export
- Member Management
- Template Management
- Server VPN
- Server Dummy
- Summary Report
- Monitor
- Event / History
- Backup / Restore
- Help

Configure Wizard

ดำเนินการติดตั้งโปรแกรมเข้า Mikrotik



Device IP : 192.168.66.1
Username : admin
Password :
Execute Status : **Execution Successfully.**
Device Status : rebooting...

Finish

ทำการ **reset** อุปกรณ์ และ **restore** ค่า **config** ของ **dummy.rsc**

- Dashboard
- Provisioning
- HQ Install (Dummy)
- Dummy List
- Manual Approve
- Auto Approve
- Approve List
- Group Deployment
- Import / Export
- Member Management
- Template Management
- Server VPN
- Server Dummy

Dummy list

	#	Serial Number	Template Name	Create by	Created date	Status
<input type="button" value="Delete"/>	1	4AC802F2274F	dummy	admin	2015-07-23 02:09:35	Success

สถานะของอุปกรณ์ขึ้นเป็น **Success** (ในส่วนของ การตั้งค่า **dummy**)

Dashboard

Provisioning

HQ Install (Dummy)

Dummy List

Manual Approve

Auto Approve

Approve List

Group Deployment

Import / Export

Member Management

Number of Active Users : 1

ID	name	service	caller-id	address	uptime	Serial	Input Store ID	Status
1	ppp1	l2tp	192.168.66.1	2.2.2.10	53s	4AC802F2274F	Store ID	Pending

1

2

3

กรอก Store ID ให้ถูกต้อง หากผิด หรือไม่มีในเมนู Provisioning จะไม่สามารถ Approve ได้

กด Approve เพื่อเริ่มกระบวนการ

Dashboard

HQ Install (Dummy)

Manual Approve

Auto Approve

Direct Deployment

Group Deployment

Store Management

Member Management

Template Management

Firmware Management

Active Connection List

Dummy List

Approve List

Devices List

L2TP List

Server VPN

Server Dummy

Event / History

Template : ทั้งหมด | โชน : ทั้งหมด | ภาค : ทั้งหมด | จำนวน : 10000 | ค่าค้นหา : (ถ้ามี)

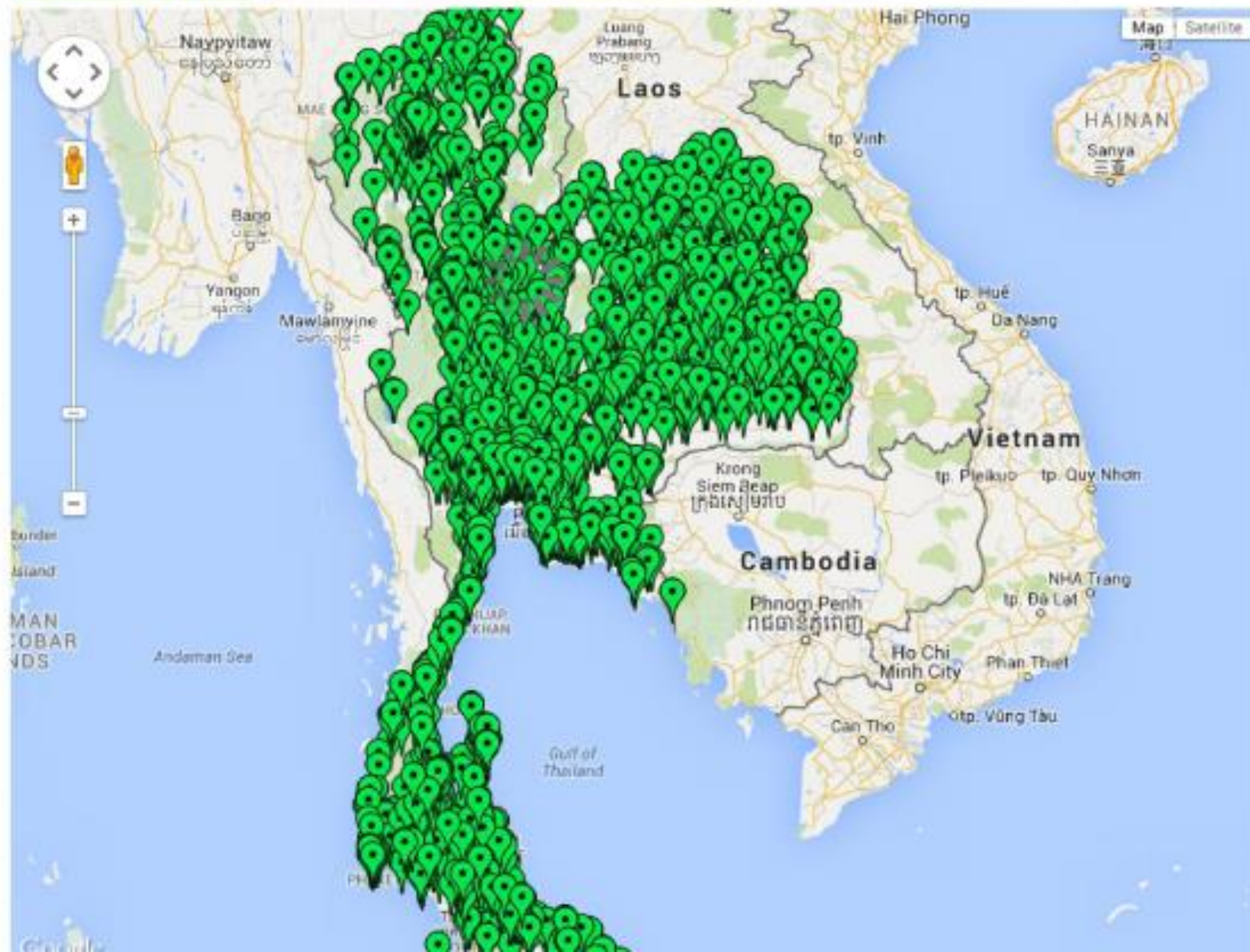
ค้นหา

ติดตั้งแล้ว : 7994 สาขา

กำลังติดตั้ง : 0 สาขา

กำลังหาลิขสิทธิ์ : 0 สาขา

ยังไม่ได้ติดตั้ง : 0 สาขา



Dashboard	Server list									
HQ Install (Dummy)	Create a new Server									
Manual Approve		#	Serial Number	Server Name	IP	Username	Password	Create by	Status	action
Auto Approve	Delete	1	558204568A61	MikroTik VPN Server [0]	192.168.88.250	admin	*****	admin_sne	Active	Disable it
Direct Deployment	Delete	2	5582053774F9	MikroTik VPN Server [1]	192.168.88.251	admin	*****	admin_sne	Active	Disable it
Group Deployment	Delete	3	558205529816	MikroTik VPN Server [2]	192.168.88.252	admin	*****	admin_sne	Active	Disable it
Store Management	Delete	4	558205B047BC	MikroTik VPN Server [3]	192.168.88.253	admin	*****	admin_sne	disabled	Active it
	Delete	5		VPN Server [1][1]	1.1.1.1	admin	*****	admin	disabled	Active it
Member Management	Delete	6		VPN Server [1][2]	1.1.1.2	admin	*****	admin	disabled	Active it
	Delete	7		VPN Server [1][3]	1.1.1.3	admin	*****	admin	disabled	Active it
Template Management	Delete	8		VPN Server [1][4]	1.1.1.4	admin	*****	admin	disabled	Active it
	Delete	9		VPN Server [1][5]	1.1.1.9	admin	*****	admin	disabled	Active it
Firmware Management	Delete	10		VPN Server [2][1]	1.1.1.5	admin	*****	admin	disabled	Active it
	Delete	11		VPN Server [2][2]	1.1.1.6	admin	*****	admin	disabled	Active it
	Delete	12		VPN Server [2][3]	1.1.1.7	admin	*****	admin	disabled	Active it
Active Connection List	Delete	13		VPN Server [2][4]	1.1.1.8	admin	*****	admin	disabled	Active it
Dummy List	Delete	14		VPN Server [2][5]	1.1.1.10	admin	*****	admin	disabled	Active it
Approve List										
Devices List										
L2TP List										
Server VPN										
Server Dummy	© 2015 CPALL - Zero Config Management privacy - terms									
Event / History										

ดูได้ง่ายทันทีที่สนใจและทันเวลา

- ระบบนี้ได้นำเอา **Netwatch, The Dude, Zabbix** มาช่วยในการทำงานร่วมกันอย่างลงตัวพร้อมกับรายงานผลปฏิบัติงานต่างๆ ให้แก่ผู้ดูแลได้อัตโนมัติ ผ่านทาง **SMS/EMAIL/Facebook/LINE** ได้

