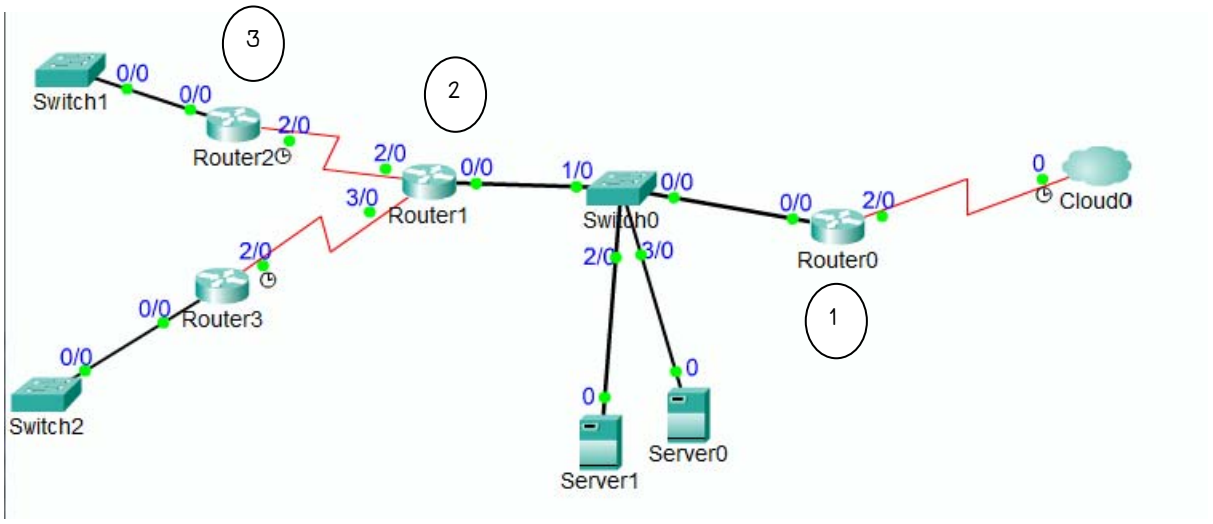


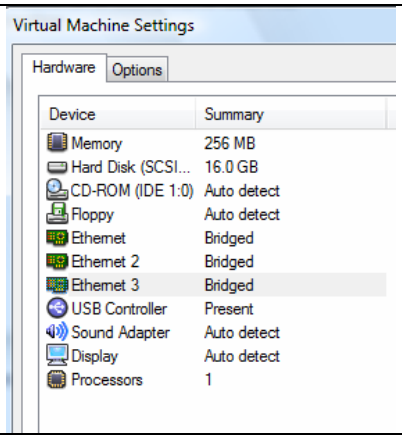
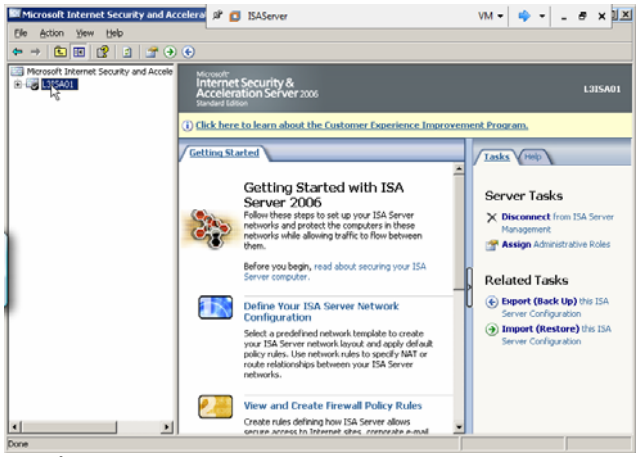
การออกแบบบริการใช้งาน Internet

กลุ่มผู้ใช้	**ระดับการใช้บริการ**	**บริการที่ให้**
เรา	1	All Internet Access 100%
ผู้บริหาร	1	All Internet Access 100%
เจ้าหน้าที่ด้านไอที	2	All Internet Access 50% RDP, FTP, SSH, ...
เจ้าหน้าที่ธุรการ	4	HTTP 50% Off-peak 100% SSH
นักเรียน	5	HTTP 50%

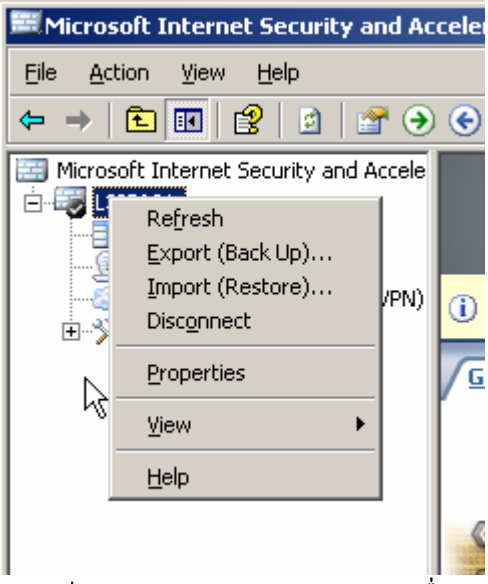
ตารางการใช้งานจากภายนอก

เครื่องแม่ข่าย	บริการที่ให้	คำอธิบาย
Webserver01	HTTP FTP	เพื่อประชาสัมพันธ์หน่วยงาน และมีระบบสมาชิกสำหรับแลกเปลี่ยนข้อมูลหรือมีการสอบออนไลน์ผ่านอินเทอร์เน็ต
MailServer	SMTP, POP3	ให้ผู้ใช้สามารถที่ส่งจดหมายอิเล็กทรอนิกส์เข้ามาภายในองค์กร
E-learning	HTTP, HTTPS	มีระบบสมาชิกในการเข้าใช้ และดูบทเรียน รวมถึงการส่งงานผ่านอินเทอร์เน็ต
Remote Desktop Protocol	RDP	เพื่อเข้ามาบริหารงานจากที่บ้าน

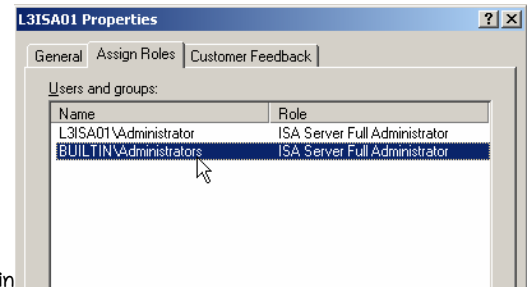
ปฏิบัติการ ISA Server 2006

กิจกรรม	สิ่งที่ดำเนินการ
การเปิดอิมเมจของ VMWare	1. คลิกที่ File > Open > ระบุตำแหน่งของไฟล์ .vmx ซึ่งอยู่ที่ d:\vmimage\isaserver\copyofWindows2003\... 2. พบว่าภายในจะมีการ์ด Network อยู่เพียงหนึ่งใบ 3. 192.168.10.x, 192.168.0.x
การเพิ่มการ์ด Network ใน VMWare	
การติดตั้ง ISA Server 2006	1. ใส่แผ่นซีดีรอม ISA server 2006 หรือดับเบิ้ลไฟล์ติดตั้ง ISA2K6Evl.exe 2. ระบุขั้นตอนตาม Wizard 3. ระบุยอมรับข้อตกลงการใช้ซอฟต์แวร์ 4. เลือกกำหนดติดตั้งเป็นแบบ typical 5. ใส่ Add range เครือข่ายภายใน 6. ไม่กำหนดให้ Non encrypt โดยคลิกปุ่ม next 7. รอระบบทำการติดตั้ง 5-15 นาที พบว่า ISA Server จะทำการบล็อก (Close rule)
การเริ่มใช้งาน ISA Server	1. คลิก Start > All Programs > Microsoft ISA Server > ISA Server Management  2. คลิกที่ Server Node จะเห็นเมนู Getting Started ถ้าต้องการศึกษากับ ISA Server ให้เลือกตามลำดับหมายเลข
การมอบหมายสิทธิ์ผู้ใ	1. ให้สร้างผู้ใช้ Computer Management > FWAdmin, FWAuditor

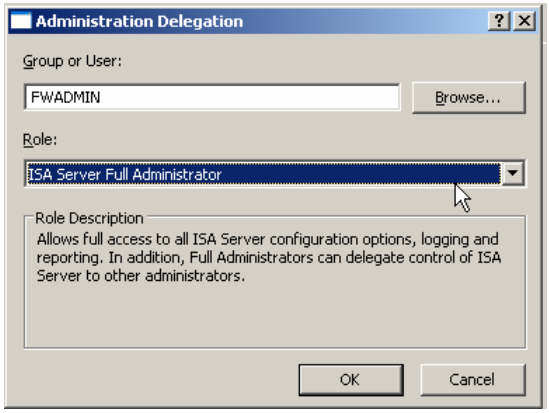
2. เปิด ISA Server Management
3. เลือกที่ Server Node คลิกขวาเลือกคำสั่ง Properties



4. คลิกแท็บ Assign Roles, คลิกปุ่ม Add ระบุชื่อ FWAdmin



5. กำหนดให้สิทธิ์เป็น ISA Server Full Administrator

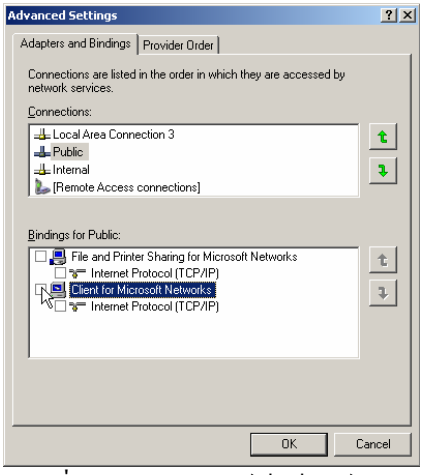


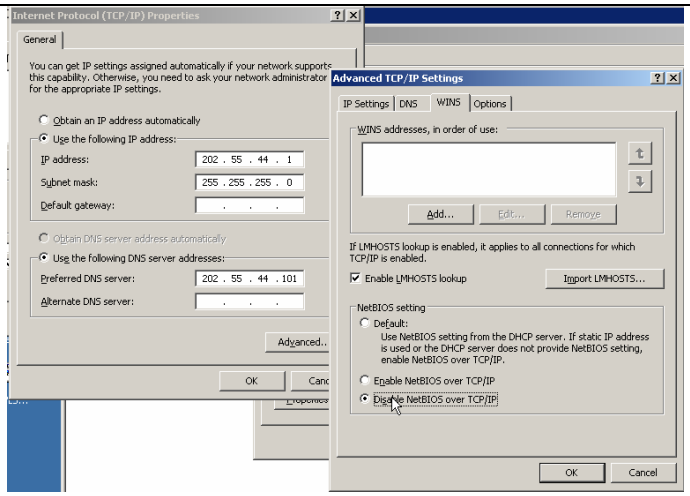
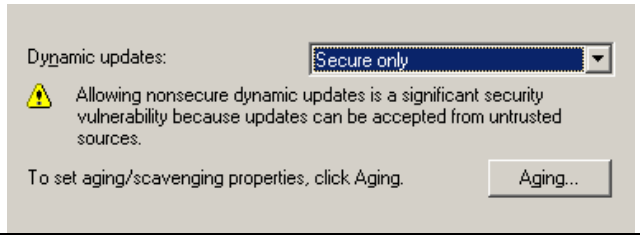
แสดงว่า FWAdmin เป็นผู้ใช้ธรรมดาใน OS แต่เป็นผู้บริหาร Firewall

6. ทำแบบเดียวกันแต่เปลี่ยนเป็น FWAuditor ให้สิทธิเป็น ISA Server Monitor Auditor

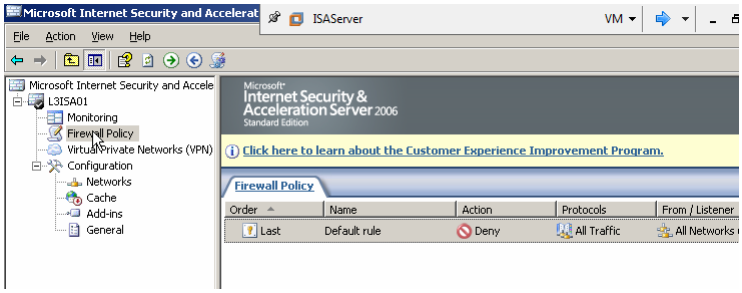
Name	Role
L3ISA01\Administrator	ISA Server Full Administrator
BUILTIN\Administrators	ISA Server Full Administrator
fwadmin	ISA Server Full Administrator
fwauditor	ISA Server Monitoring Auditor

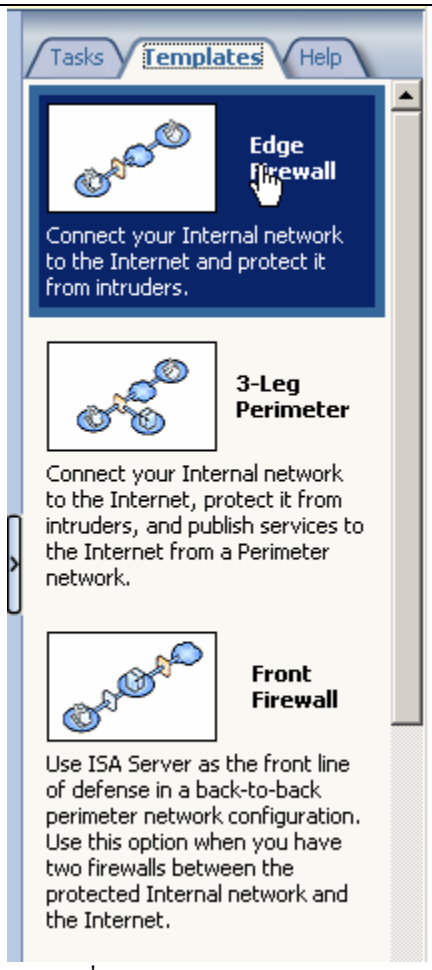
7. ทุกครั้งที่กำหนดเสร็จให้คลิกปุ่มApply, และคลิกปุ่ม OK

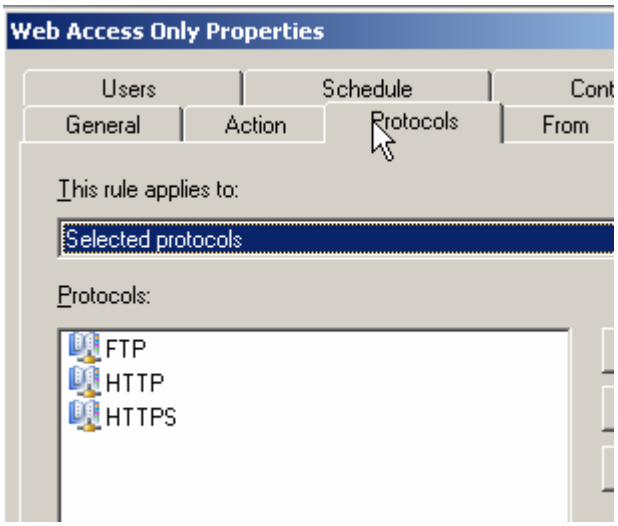
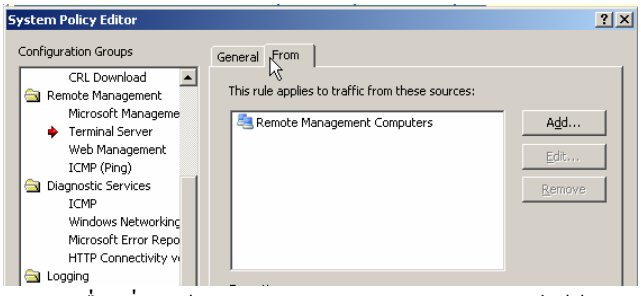
	ทดสอบการใช้งาน 1. ล็อกออฟ และล็อกออนด้วย FWAdmin 2. ไปเปิด ISA Server Management System Admin > Admin OS (Administrator) ผู้ดูแลระบบปฏิบัติการ Network Admin > FW Admin (FWAdmin) ผู้บริหารงานไฟร์วอลล์ Auditor > FW Auditor (FWAuditor)ตรวจสอบกิจกรรมที่ดำเนินการของ FWAdmin
การดำเนินการเพื่อให้ ISA Server มีความปลอดภัย	1. จัดเก็บเครื่องไว้ในพื้นที่ปลอดภัย - การควบคุมบุคคลภายนอก - ระบบปรับอากาศ - ระบบป้องกันไฟฟ้าดับ 2. พิจารณากฎ 4 As - ตรวจสอบตัวตน (logon) - การให้สิทธิ์ (การมอบหมายหน้าที่) - การบันทึกกิจกรรมที่ดำเนินการ (ล็อก) - การสำรอง หรือสำเนากันค่ากำหนดต่างเสียหาย (สำรอง)
การอุดช่องโหว่ของ ISA Server	1. ล็อกออนด้วย Administrator 2. ไปที่ Properties ของ My Network Places 3. คลิกที่เมนู Advanced > Advanced Settings  เลือกที่ขานอก และเคลียร์เช็กบ็อกซ์ของ File and Printer Sharing for Microsoft Networks, Client for Microsoft Networks ออก 4. ใน Network Interface ขานอกให้เข้าไปที่ Properties > Internet Protocol Properties > ไปที่แท็บ WINS ให้เลือก Disable NetBIOS over TCP/IP

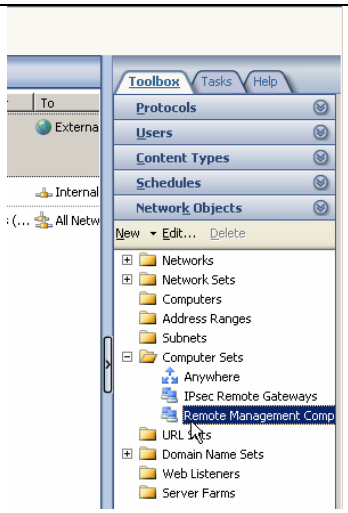
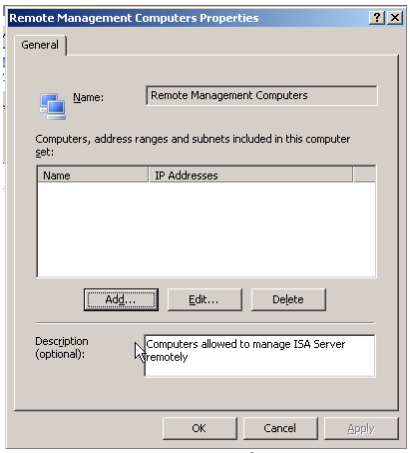
	 5. เคลียร์เช็กบ็อกซ์ Enable LMHOSTS lookup ออก 6. ไปที่ DNS Server (ถ้ามี) และระบุไม่ให้มีการ automatic update (None) หรือกำหนดเป็น Secure Only ไม่ให้ใช้ Non secure or Secure 
สิ่งที่ควรเข้าใจเกี่ยวกับ ISA Server	ประกอบด้วยการดำเนินการ 5 ส่วนประกอบหลัก - Network (Internal, External, Local) - Firewall Policy (Access control:Out, Publishing:In) - Caching - VPN Server (VPN Client, ISA:Back to Back) - Monitor 
การกำหนดค่า Network	เราพบว่าตอนที่เราติดตั้งระบบจะให้กำหนดหมายเลข IP

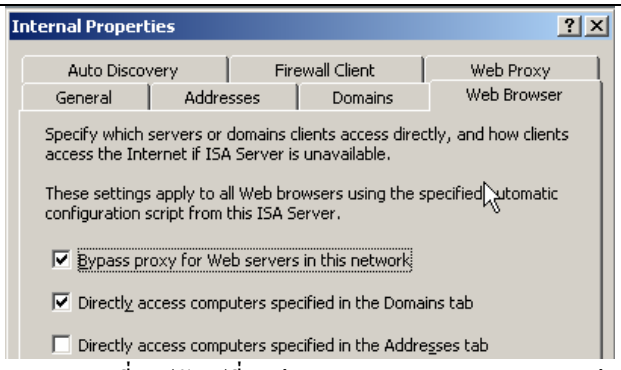
	192.168.0.1-192.168.0.255 > Internal ที่เหลือเป็น External หมายเลข IP ของ ISA จะเป็น Local การกำหนดดำเนินการที่ Server Node > Configuration > Networks  ภายใน Networks จะแบ่งเป็น External เครือข่ายทั้งหมดที่นอกเหนือจาก Local Host และ Internal Internal คือเครือข่ายที่ระบุตอนติดตั้ง (เครือข่ายภายใน) Local Host คือเครื่อง ISA Server Quarantine VPN คือกลุ่มเครื่องกักกัน VPn Client คือเครื่องที่เข้าใช้ VPN Server Network Sets คือการเอารายการของ Networks มาสร้างกลุ่ม All Network หมายถึงทุกเครือข่าย All Protected Network หมายถึงทุกเครือข่ายยกเว้น External Rules คือการกำหนดเส้นทางในการวิ่ง มี 2 ประเภทคือ Route, NAT Private > Private (Route) Public > Public (Router) Private > Public (NAT) VPN Client > Internal (Route) Internal > External (NAT) Local host > All Network (Route)
การสร้างเครือข่ายใหม่	1. คลิกที่ Server Node > Configuration > Network > Networks 2. คลิก Create a New network รายการด้านขวา

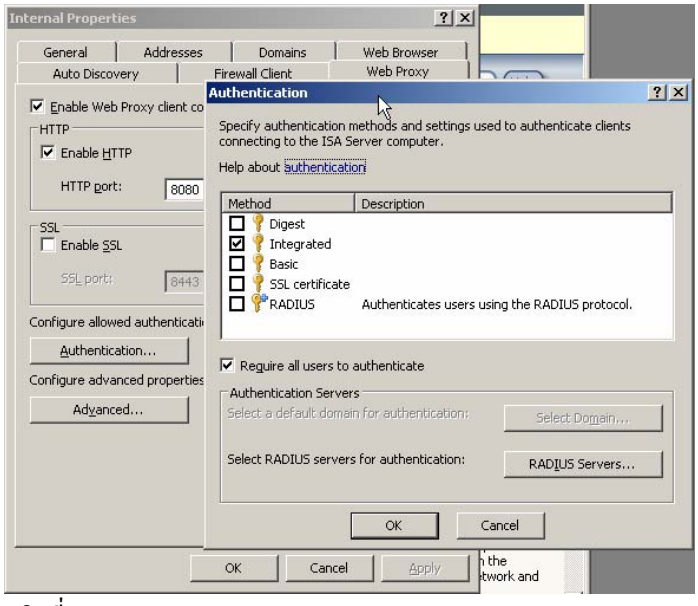
	 3. ใส่ชื่อ Network Name, คลิกปุ่ม Next 4. ระบุ Network type เช่น Internal, คลิกปุ่ม Next 5. ระบุช่วงหมายเลข IP, คลิก Next, คลิกปุ่ม Finish 6. คลิกปุ่ม Apply, คลิก OK 7. เราต้องกำหนด Rules โดยถ้าเป็น Private กับ Private ให้กำหนดเป็น Route
ทำไมติดตั้ง ISA Server แล้วออก Internet ไม่ได้	เนื่องจาก ISA Server เป็นกฎปิด - ให้ไปที่ firewall policy ตรวจสอบว่าปิดจริงหรือไม่  ถ้าต้องการเปิดให้ใช้ทำอย่างไร 1. ใช้ Network Template 2. สร้าง Access Control Policy Network Template 1. คลิก Server Node > Configuration > networks 2. คลิกที่แท็บ Templates 3. ระบุชนิดของ Firewall

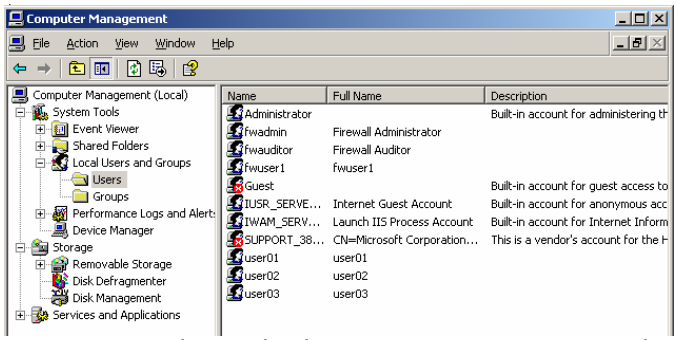
	 4. ให้คลิกที่ Edge Firewall 5. คลิกปุ่มNext 6. คลิก Next อีก 2 ครั้ง 7. เลือก Unrestricted Internet Access, คลิกปุ่ม Next, คลิกปุ่ม Finish 8. คลิกปุ่ม Apply, คลิก OK ทดสอบโดยใช้ 1. เปิด Browser ไปพิมพ์ URL http://www.internet.com 2. ftp 202.55.44.101 ระบุชื่อ Anonymous แล้วเคาะ Enter 2 ครั้ง พิมพ์ Ls 3. Ping 202.55.44.101 4. Telnet 202.55.44.101, พิมพ์ว่า Yes ระบุชื่อ Administrator รหัสผ่าน password 5. แสดงว่ามีพอร์ต - 21 - 23 - 80 - 53 - Protocol ID 1
การกำหนดให้เฉพาะ Web Access	1. ไปที่ Server Node > configuration > Networks > คลิกที่แท็บ Templates (ด้านซ้าย) 2. คลิกที่ Edge Firewall, คลิกปุ่ม Next 3 ครั้ง แล้วเลือก Limited Web Access Only,

	คลิกปุ่ม Next แล้วคลิกปุ่ม Finish 3. คลิกปุ่ม Apply, คลิกปุ่ม OK 4. ตรวจสอบดูใน Firewall Policy  ทดสอบลูกข่าย 1. ลองเปิด Browser ใช้ได้ 2. ใช้ Telnet ไม่ได้ 3. ใช้ FTP ได้ 4. Ping ไม่ได้
กรณีที่ลูกข่ายออกอินเทอร์เน็ต	1. ตรวจสอบที่ Default Gateway ว่าระบุไปยังขา ISA Server หรือไม่ 2. ตรวจสอบหมายเลข IP ว่าตรงกับตามโครงสร้างระบบเครือข่ายหรือไม่
ถ้าต้องการใช้ Remote Desktop มาเข้าที่ ISA Server ทำอย่างไร	1. ให้เปิด ISA Server Management 2. คลิกขวาที่ Firewall Policy > Edit System Policy 3. ไปดูรายการ Remote Management > TerminalServer  พบว่าเครื่องที่จะใช้ Remote Management Computers ได้ต้องอยู่ในกลุ่ม Remote Management Computers ทำอย่างไร 4. ให้ไปที่Tool box

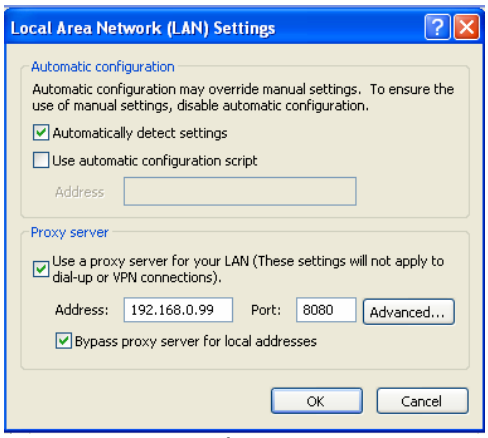
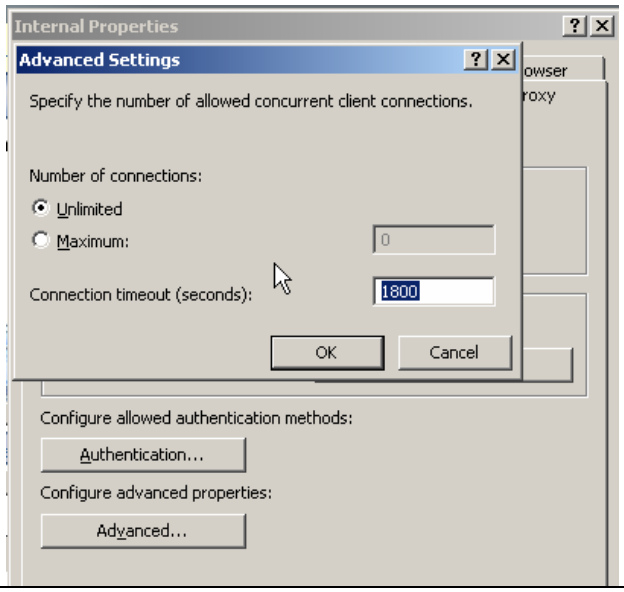
	 เข้าไปในรายการของ Network Objects, คลิกที่ Computer Sets > Remote Management Computer, คลิกที่ Edit  คลิกปุ่ม Add ระบุเป็นเครื่อง หรือช่วงหมายเลข IP ที่ต้องการ, คลิกปุ่ม OK สองครั้ง อย่าลืม Enable Remote Desktop ด้วยนะจ๊ะ
ถ้าต้องการบริหารงาน ISA Server จากลูกข่ายภายในทำได้อย่างไร	1. ติดตั้ง ISA server จากแผ่นซีดีรอมของ ISA Server 2006 2. แล้วเรียก ISA Server Management ด้วยบุคคลที่มีสิทธิ์ในการบริหารงาน
การติดตั้ง Microsoft firewall Client	1. เข้าไปในแผ่นซีดีรอมของ ISA Server จะมีโฟลเดอร์ client 2. ดับเบิ้ลคลิกไฟล์ setup.exe ซึ่ง ISA Server จะมี Firewall client อยู่แล้ว
การกำหนดค่าควบคุมลูกข่าย	1. ไปที่ ISA Server Management > Server Node > Configuration > Networks > Networks tab > ดับเบิ้ลคลิกที่ Internal

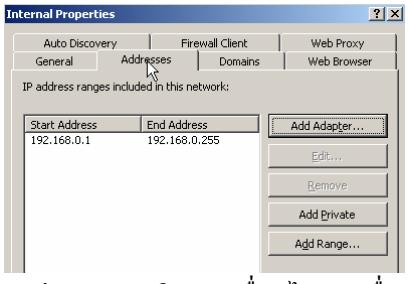
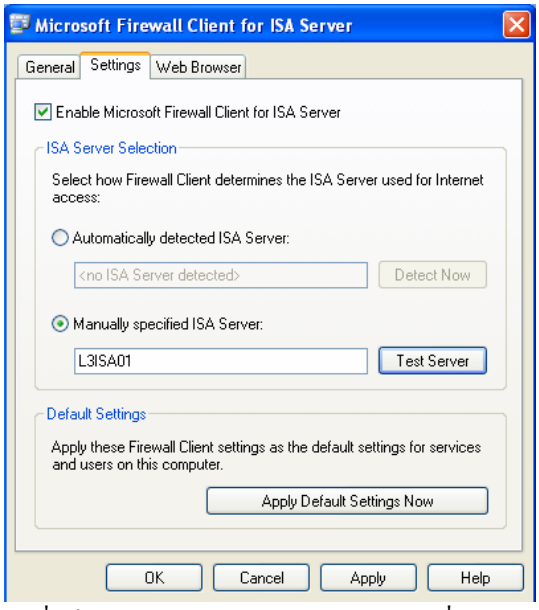
<table>
<tr>
<td></td>
<td> 

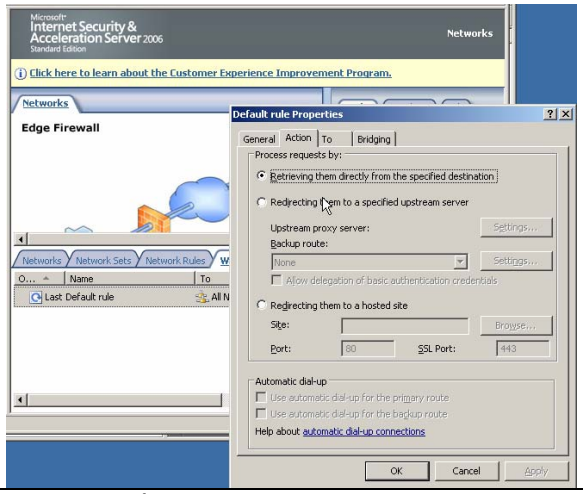
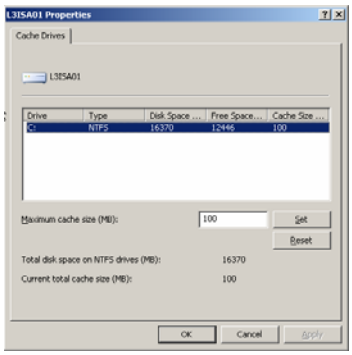
เราสามารถที่จะปรับเปลี่ยนค่า Firewall Client, Web Proxy ส่วน SecureNAT ไม่ต้องทำอะไรให้กำหนดเฉพาะ Default Gateway ผ่าน ISA Server เท่านั้น</td>
</tr>
<tr>
<td>การกำหนดบังคับให้ลูกข่ายต้องล็อกออนก่อนผ่าน Internet</td>
<td>1. ไปที่ ISA Server Management > Server Node > Configuration > Networks > Networks tab > ดับเบิ้ลคลิกที่ Internal
2. ไปที่แท็บ Web Proxy, คลิกที่ปุ่ม Authentication
 

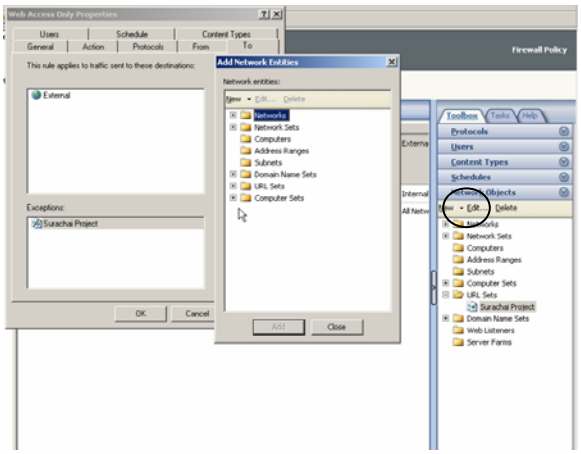
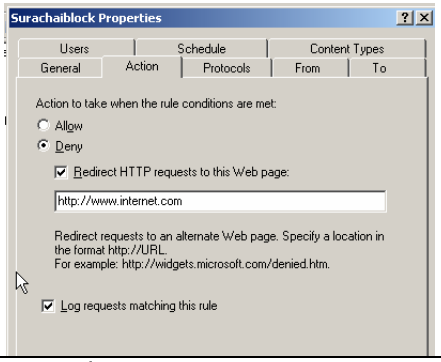
3. คลิกที่ Require all users to authenticate
4. รายชื่อที่ใช้ล็อกออนจะเป็นรายชื่อบนเครื่องที่ดำเนินการ (L3ISA01)
 

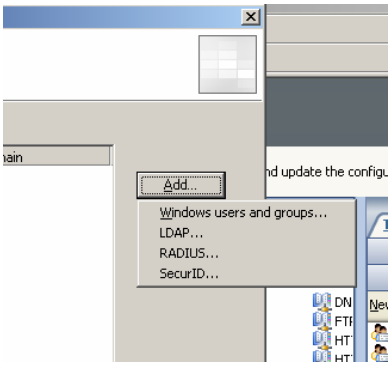
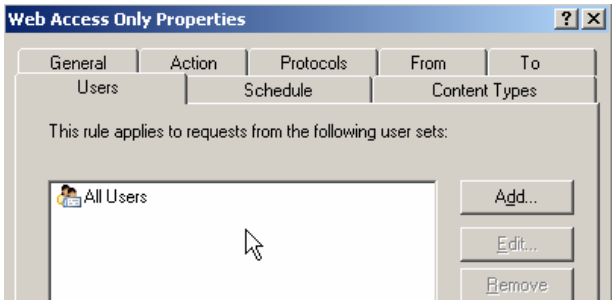
5. ถ้าต้องการใช้รายชื่อบนเครื่องอื่นให้กำหนดค่า RADIUS Server ซึ่ง Windows Server 2003 รองรับ RADIUS Server อยู่แล้ว แต่ต้องติดตั้ง IAS (Internet Authentication Server) ไว้ก่อน
ลูกข่ายที่ต้องการใช้ Web Proxy</td>
</tr>
</table>

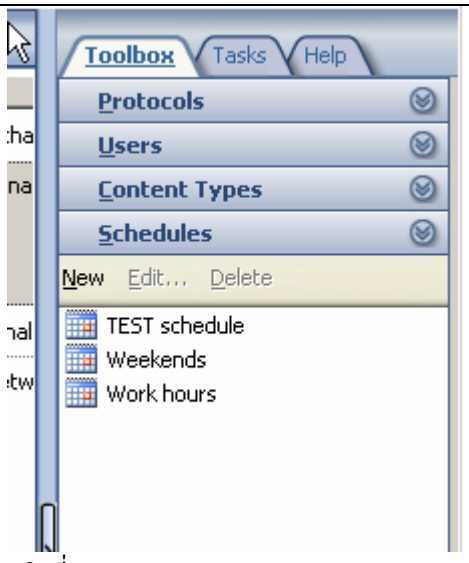
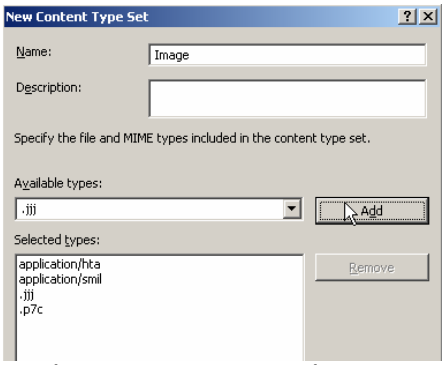
	1. เปิด Browser ไปที่ Options > Internet Options 2. คลิกที่แท็บ Connections > คลิกที่ LAN Settings  ระบุค่า IP และ Port ที่ตรงกับค่าบน ISA Server
การเซต Automatic Discovery บน ISA Server	1. จะใช้ร่วมกับ DHCP จะต้องแจกหมายเลข IP และค่า WPAD (Web Proxy Automatic Discovery) หมายเลข WPAD จะกำหนดโค้ด 252 และระบุ DNS ให้ไปหา WPAD.โดเมน 2. SecureNAT (Transparent)
กรณีที่ต้องการระบุระยะเวลารับรองของ Web Proxy	กำหนดที่ Advanced Settings ใส่ค่าเวลาที่เราต้องการเช่น 300 คือ 5 นาที 
การพิจารณาเงื่อนไขใน Firewall Policy	จะพิจารณาจากบนลงล่าง หมายถึงถ้าระบุว่า Deny ด้านล่าง (เงื่อนไขใดไม่ถูกกำหนดจะหมายถึง Deny)
ปัญหาการที่ ISA Server ไม่สามารถติดต่อภายนอกได้	1. ให้ตรวจสอบที่ Firewall Policy ดูเงื่อนไข - Allow - Source > Destination - Protocols - Schedule, User, Contents 2. ไปตรวจสอบค่ากำหนดของ Networks > Internal ถ้ามีการระบุว่า authentication ใน Web Proxy ผู้ใช้ต้องเชื่อมต่อโดเมน หรือเลือก

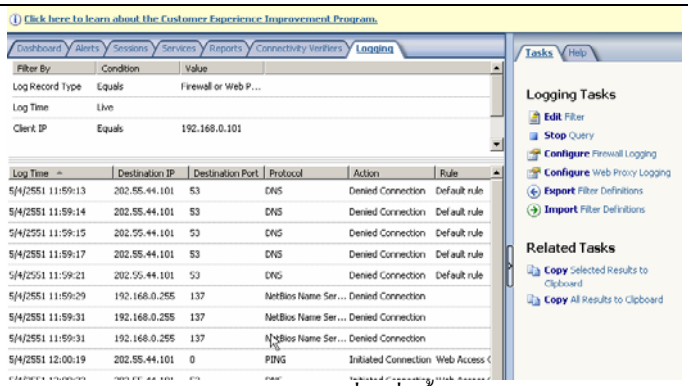
	Enable Web Proxy Client บน Browser ระบบจะ Popup ให้มีการล็อกออน (ถ้าไม่เช่นนั้นให้เอาออก) 
การกำหนดอนุญาตผู้ใช้	1. ISA Server ต้องเชื่อมต่อเข้ายังโดเมนของ AD (ไม่แนะนำ) 2. ISA Server ระบุใช้ RADIUS Server แทน
การติดตั้ง Firewall Client	1. ในแผ่นซีดีรอมของ ISA Server จะมีโฟลเดอร์ Client 2. ให้เลือกคำสั่ง Setup เพื่อติดตั้ง รองรับเฉพาะ Windows Platform 3. ระบบจะดึงค่ากำหนดจากเครื่องแม่ข่าย  ลูกข่ายสามารถพิจารณาเงื่อนไขบนเครื่องตนเองได้ 4. คลิกที่ Start > All Programs > Microsoft Firewall Client for ISA Server  5. ไปที่แท็บ Settings, เลือก Enable และระบุเครื่อง ISA Server 6. ต้องการดึงค่าใช้ปุ่ม Apply Default Settings Now
การกำหนด Indirect connection	กรณีที่ ISA Server ไม่ต่ออินเทอร์เน็ตโดยตรง เช่น ที่ hqr มี ISA Server หลักอยู่ แล้วให้ที่สำนักฯติดต่อผ่าน ISA Server HQR > Province > Area > Group 178 areas 2000 รายการ HQR >> Control Operators

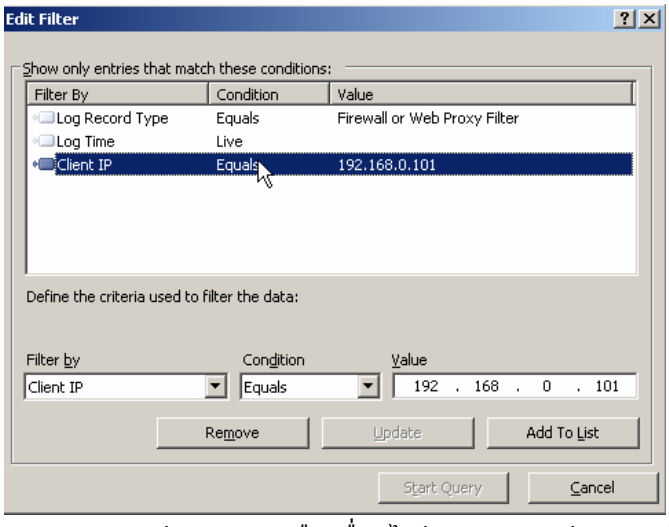
	ค่าที่กำหนดดำเนินการที่ ISA Server Management > Server Node > Configuration > Networks > Web Chaining> Last Default Rule ภายในกำหนดเป็น Redirecting them to a specified upstream server ให้ระบุเครื่อง ISA Server หลัก (Master) 
การกำหนด ISA server เป็น Cache Server	1. ไปที่ Server Node > Configuration > Cache 2. คลิกคำสั่ง define cache drive 3. ระบุขนาดที่เก็บ  เช่น 100 หมายถึง 100 MB คลิกปุ่ม Set 4. คลิกปุ่ม Apply, คลิก OK สองครั้ง ข้อควรระวังถ้าแคชเต็ม ระบบจะออก Internet ไม่ได้ ให้หมั่นเคลียร์แคชเป็นระยะโดยไปที่ c:\urlcache ลูกข่ายที่ต้องการใช้ Cache Server 1. เครื่อง ISA server ต้องระบุ Port สำหรับ Proxy โดยไปที่ Server Node > Configuration > Networks > Internal > Web Proxy tab ให้ระบุพอร์ตที่ต้องการ เช่น 8080 ถ้า ISA Server ต้องการให้ Authentication จะคลิกที่ปุ่ม Authentication แล้วเลือกวิธีการ (domain, radius, custom) 2. ต้องระบุ Internet Options ให้ใช้ Web Proxy มาที่เครื่อง ISA Server ถ้าขั้นตอนที่1 ระบุ 8080 ตรงนี้ต้องระบุ 8080 ด้วย

การกำหนด Cache มี 3 ขั้นตอน	1. กำหนดขนาดที่เก็บ 2. กำหนดเงื่อนไขที่เก็บ (Cache Rule) - FTP, HTTP - TTL, Min, MAX (Cache), Size - Content type (Dynamic) 3. การทำ Active Cache ระบบจะทำการดาวน์โหลดเว็บมาเก็บไว้ก่อน
ต้องการบล็อกเว็บที่อาจารย์สุรชัยนิยมใช้	1. เปิด ISA Server 2006 Management > Server Node > Firewall Policy 2. ด้านขวาจะมีแท็บ Toolbox  3. คลิกปุ่ม New เลือก URL Sets 4. ใส่ชื่อของ URL sets ที่ต้องการเช่น Surachai project 5. ใส่ค่าเว็บที่ไม่ต้องการ เช่น http://www.asiaxxx.com และอื่นๆ การนำไปใช้ 1. ไปที่ Access Rule ในรายการที่กำหนด 2. ไปที่แท็บ Destination, ด้านล่างจะมี Exception 3. คลิกปุ่ม Add เลือกรายการใน Network Objects 4. คลิก Close, คลิก OK 5. คลิก Apply และคลิก OK
กรณีที่เราต้องการ Redirect Web site หรือเงื่อนไขต่างๆ	เราต้องเลือก Deny จึงสามารถกำหนด Redirect ได้ 
ต้องจำกัดแบนด์วิดช์	ในเวอร์ชั่น ISA server 2000 แต่ในเวอร์ชั่น ISA server 2004, 2006 ไม่มี แนะนำให้ไปใช้ Hardware block (Juniper)

การกำหนด User	ISA Server สามารถระบุได้ 4 แบบ  - Windows users and groups ต้องนำเครื่องไปเชื่อมต่อกับโดเมน - LDAP ต้องระบุเครื่อง LDAP Server ไว้ก่อน - RADIUS ต้องระบุเครื่อง RADIUS Server ไว้ก่อน (Windows ติดตั้ง IAS Server) - SecurID ต้องติดตั้งแอพพลิเคชั่น SecurID ลงในเครื่อง วิธีการกำหนด 1. ไปที่ Server Node > Firewall Policy > ด้านขวาจะมี Tools ให้เลือก User แล้วคลิกขวาเลือกคำสั่ง New และระบุชื่อที่ต้องการ 2. ระบุชนิดของผู้ใช้ใส่ในรายการที่กำหนด การนำไปใช้ 1. ไปที่ Access Rule และระบุใช้แท็บ Users 
การควบคุมตารางเวลา	1. ไปที่ Server Node > Firewall Policy > Toolbox

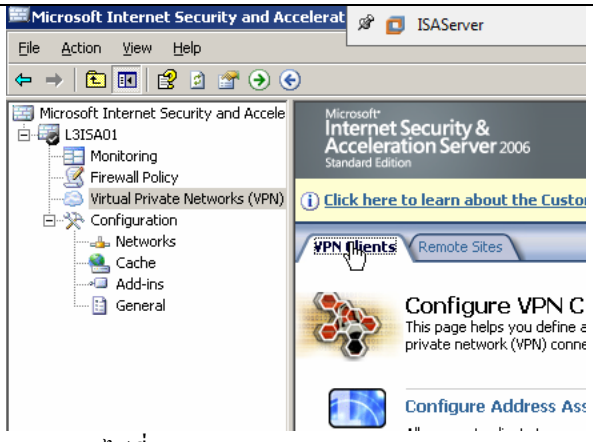
	 2. คลิกที่แถบ Schedules 3. คลิกปุ่ม New ใส่ชื่อ และช่วงเวลาที่ต้องการ การนำไปใช้ 1. ให้เข้าไปใน Access Rule, แท็บ Schedule 2. แล้วเลือกรายการที่ได้สร้างในตอนต้น
การกำหนดควบคุมเนื้อหา	ISA Server ได้มีการเซตไว้ให้เรียบร้อยแล้ว Content type ถ้าต้องการเพิ่มทำได้โดย 1. ไปที่ Server Node > Firewall Policy > Toolbox 2. แถบ Content Types > คลิกปุ่ม New 3. ระบุชื่อกฎ  4. ระบุชื่อไฟล์ และนามสกุลไฟล์ที่ต้องการบล็อก การนำไปใช้ 1. ให้เข้าไปใน Access Rule, แท็บ Content type 2. แล้วเลือกรายการที่ได้สร้างในตอนต้น
การตรวจสอบกิจกรรม ของผู้ใช้ ISA Server	1. ไปที่ Server Node > Monitor 2. คลิกที่แท็บ Logging

<table>
<tr>
<td></td>
<td>


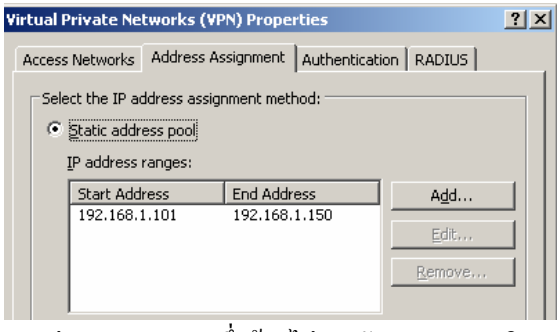
3. ด้านซ้ายจะมี Start query เราคลิกที่คำสั่งนี้
จะพบว่ากิจกรรมทั้งหมดจะถูกแสดงผล
4. ถ้าต้องการระบุเฉพาะเงื่อนไขที่ต้องการให้ไปคลิกที่ Edit filter


ระบุ Filter by เช่น client IP เลือกเงื่อนไขว่า Equals และค่า Value เช่น 192.168.0.101 คลิกปุ่มStart query จะพบว่าเงื่อนไขจะกำหนดให้แสดงผลเฉพาะรายการที่ระบุ</td>
</tr>
<tr>
<td>การป้องกันการจู่โจมจากภายนอก</td>
<td>

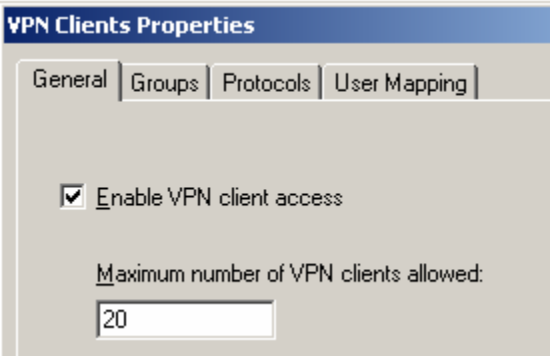

- IDS & DNS Attack การโจมตีระบบจากผู้บุกรุก
- Flood การยิงเครื่องให้ล่ม
- IP Protection การป้องกันโหลดของเครื่อง
1. ISA server Management > Server Node > Configuration > General > Additional Security Policy
กำหนดป้องกันการถูกโจมตีจากภายนอก</td>
</tr>
<tr>
<td>การป้องกันการดักฟัง</td>
<td>ISA Server จะมีบริการ VPN Server</td>
</tr>
</table>



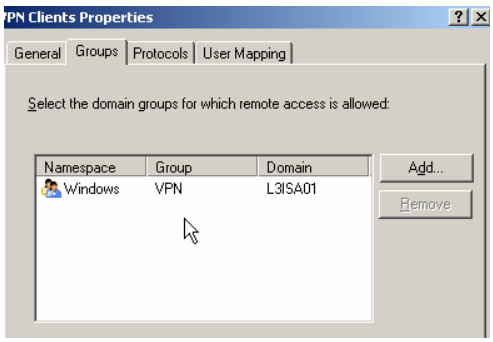
1. ไปที่ Server Node > Virtual Private Networks (VPN)
2. คลิกที่ Configure Address Assignment



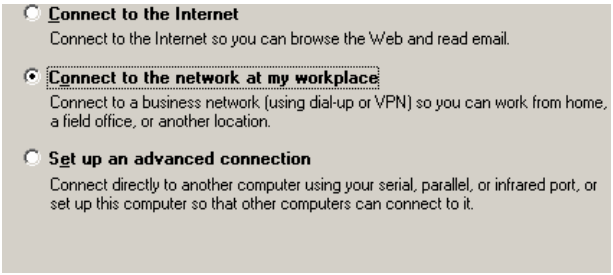
3. ระบุช่วงหมายเลข IP ซึ่งต้องไม่ตรงกับ Internal, คลิก OK



4. ไปที่คลิก Enable VPN Clients, ระบุจำนวน VPN Clients ที่ใช้
5. ไปที่ Specify Windows Users
6. คลิกระบุกลุ่มที่ต้องการ (เราต้องใส่สมาชิกในกลุ่มให้เรียบร้อยก่อน)



การทดสอบที่ลูกข่าย (อินเทอร์เน็ต)

	1. เปิด Network Connection 2. เลือก Create a new connection, คลิกปุ่ม Next 3. เลือก Connect to the network at my workplace, คลิกปุ่ม Next  4. เลือก Virtual Private Network Connection, คลิกปุ่ม Next 5. ใส่ชื่อ Connection, คลิก Next 2 ครั้ง 6. ใส่หมายเลข IP ของ ISA Server ขา Public 7. คลิกปุ่ม Next, คลิกปุ่ม Finish 8. ใส่ผู้ใช้ และรหัสผ่านที่ถูกต้อง
Web Publishing คืออะไร	โดยทั่วไป ISA Server จะกำหนด Access Rule หรือการเชื่อมต่อจากภายในสู่ภายนอก มีฟีเจอร์ชื่อว่า Web Publishing เป็นการให้ภายนอกติดต่อเข้าภายใน ตัวอย่างเช่น เรามีเว็บแม่ข่ายอยู่ที่ 192.168.0.11 ISA จะมีรูปแบบหลักๆอยู่ 2 แบบ - Web Publishing (พอร์ต 80, 443) - Server Publishing (Non-Web Publishing, any ports) เราต้องคิดก่อนว่า 1. IP ภายในอยู่ที่ไหน 2. ต้องการผ่านพอร์ตอะไร
การเข้าดูล็อก	1. เครื่องภายนอก(อินเทอร์เน็ต)เข้ามาดูเว็บภายในพบว่าในล็อกของ Web Server ขึ้นรายการ IP ของ ISA Server ขาในเท่านั้น ทำอย่างไร ตอบ ให้เปิดดูล็อกของ ISA Server ประกอบ