

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 และมี ระบบสมาชิกสำหรับแลกเปลี่ยนข้อมูล หรือมีการสอบออนไลน์ผ่าน อินเทอร์เน็ต
MailServer	SMTP, POP3	ให้ผู้ใช้สามารถที่ส่งจดหมาย อิเล็กทรอนิกส์เข้ามาภายในองค์กร
E-learning	HTTP, HTTPS	มีระบบสมาชิกในการเข้าใช้ และดู บทเรียน รวมถึงการส่งงานผ่าน อินเทอร์เน็ต
Remote Desktop Protocol	RDP	เพื่อเข้ามาบริหารงานจากที่บ้าน

ปฏิบัติการ ISA Server 2006

กิจกรรม	สิ่งที่ดำเนินการ
การเปิดอิมเมจของ VMWare	 คลิกที่ File > Open > ระบุตำแหน่งของไฟล์ .vmx ซึ่งอยู่ที่ d:\vmimage\isaserver\copyofWindows2003\ พบว่าภายในจะมีการ์ด Network อยู่เพียงหนึ่งใบ 192.168.10.x, 192.168.0.x
ווזנשא Network וע VMWare	Hardware Options Device Summary Memory 256 MB Hard Disk (SCSI 16.0 GB CD-ROM (IDE 1:0) Auto detect Hoppy Auto detect Roppy Auto detect Broppy Auto detect Wement Bridged Ethemet Bridged USB Controller Present W Sound Adapter Auto detect Display Auto detect Processors 1
การติดตั้ง ISA Server 2006	 ใส่แผ่นซีดีรอม ISA server 2006 หรือดับเบิ้ลไฟล์ติดตั้ง ISA2K6Evl.exe ระบุขั้นตอนตาม Wizard ระบุขอมรับข้อตกลงการใช้ซอฟต์แวร์ เลือกกำหนดติดตั้งเป็นแบบ typical ใส่ Add range เกรือข่ายภายใน ไม่กำหนดให้ Non encrypt โดยกลิกปุ่ม next รอระบบทำการติดตั้ง 5-15 นาที พบว่า ISA Server จะทำการบล็อก (Close rule)
การเริ่มใช้งาน ISA Server	 กลิ๊ก Start > All Programs > Microsoft ISA Server > ISA Server Management เมาะสามารถาง เกิดสามารถาง เกิงสามารถาง เกิดสามารถาง เกิงสามารถาง เกิงสามา
การมอบหมายสิทธิ์ผู้ใ	1. ให้สร้างผู้ใช้ Computer Management > FWAdmin, FWAuditor

2.	เปิด ISA Server Management
3.	เลือกที่ Server Node คลิกขวาเลือกคำสั่ง Properties
	I Microsoft Internet Security and Acceler
	File Action View Help
	Microsoft Internet Security and Accele
	Refresh
	Import (Restore)
	Properties
ц	ๆ คลิกแท็บ Assian Roles, คลิกปุ่ม Add ระบุชื่อ
ч. 	L3ISA01 Properties
	General Assign Roles Customer Feedback
	Users and groups:
	L3ISA01VAdministrator ISA Server Full Administrator BUILTINVAdministrators ISA Server Full Administrator
	FWAdmin
5.	กำหนดให้สิทธิ์เป็น ISA Server Full Administrator
	Administration Delegation
	Group or User:
	FWADMIN Browse
	Role:
	ISA Server Full Administrator
	Role Description Allows full access to all ISA Server configuration options, logging and
	reporting. In addition, Full Administrators can delegate control of ISA Server to other administrators.
	แสดงวา FWAdmin เบนผู้เชธรรมดา ใน OS แตเบนผู้บรหาร Firewall
6.	ทำแบบเดียวกันแต่เปลี่ยนเป็น FWAuditor ให้สิทธิ์เป็น ISA Server Monitor
	Name Role
	BUILTIN Administrators ISA Server Full Administrator
	fwadmin ISA Server Full Administrator fwauditor ISA Server Maniforing Auditor
	Towards Toward Monitoring Additor
	Auditor
7.	ทุกครั้งที่กำหนดเสร็จให้คลิกปุ่มApply, และคลิกปุ่ม OK

	ทคสอบการใช้งาน	
	1. ลี่อกออฟ และลี่อกออนด้วย FWAdmin	
	2. ไปเปิด ISA Server Management	
	System Admin > Admin OS (Administrator) ผู้ดูแถระบบปฏิบัติการ	
	Network Admin > FW Admin (FWAdmin) ผู้บริหารงานไฟร์วอลล์	
	Auditor > FW Auditor (FWAuditor)ตรวจสอบกิจกรรมที่ดำเนินการของ FWAdmin	
การดำเนินการเพื่อให้ ISA	1. จัดเก็บเครื่องไว้ในพื้นที่ปลอดภัย	
Server มีความปลอดภัย	- การควบคุมบุคคลภายนอก	
	- ระบบปรับอากาศ	
	- ระบบป้องกันไฟฟ้าดับ	
	2. พิจารณากฎ 4 As	
	- ตรวจสอบตัวตน (logon)	
	 การให้สิทธิ์ (การมอบหมายหน้าที่) 	
	 การบันทึกกิจกรรมที่ดำเนินการ (ล็อก) 	
	 การสำรอง หรือสำเนากันก่ากำหนดต่างเสียหาย (สำรอง) 	
การอุดช่องโหว่ของ ISA	1. ลี้อกออนด้วย Administrator	
Server	2. ไปที่ Properties ของ My Network Places	
	3. คลิกที่เมนู Advanced > Advanced Settings	
	Advanced Settings ? X Adapters and Bindings Provider Order	
	Networks, Client for Microsoft Networks ออก	
	4. ใน Network Interface ขานอกให้เข้าไปที่ Properties > Internet Protocol	
	Properties > ไปที่แทีบ WINS ให้เลือก Disable NetBIOS over TCP/IP	

	Internet Protocol (TCP/IP) Properties
	General
	You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator Advanced TTP/IP Settings 2 X
	for the appropriate IP settings. IP Settings DNIS WIDIS Options
	Obtain an IP address automatically WINS addresses, in order of use:
	IP address: 202 . 55 . 44 . 1
	Sybret mask: 255 . 255 . 0
	Add Edt Remoye
	Count for Server address addresses: If LMHOSTS lookup is enabled, it applies to all connections for which TCP/IP is enabled.
	Preferred DNS server: 202 . 55 . 44 . 101
	NetBIOS setting C Default:
	Lise NetBIOS setting from the DHCP server. If stabic IP address is used or the DHCP server does not provide NetBIOS setting, enable NetBIOS over TCP/IP.
	OK Canc C Epable NetBIOS over TCP/IP
	Concerning Trademices
	OK Cancel
	5. เกลียร์เช็กบ็อกซ์ Enable LMHOSTS lookup ออก
	6. ไปที่ DNS Server (ถ้ำมี) และระบุไม่ให้มีการ automatic update (None) หรือ
	กำหนดเป็น Secure Only ไม่ให้ใช้ Non secure or Secure
	Dynamic updates: Secure only
	Allowing nonsecure dynamic updates is a significant security vulnerability because updates can be accepted from untrusted
	r o set aging/scavenging properties, click Aging. Aging
สิ่งที่ควรเข้าใจเกี่ยวกับ	ประกอบด้วยการคำเนินการ 5 ส่วนประกอบหลัก
ISA Server	- Network (Internal External Local)
	- Firewall Policy (Access control: Out Publiching: In)
	- Caching
	VPN Server (VPN Client ISA Real to Real)
	- VFN Server (VFN Client, ISA.Dack (U Dack)
	Getting Started
	Getting Started with ISA Server 2006 Follow these steps to set up your ISA Server networks and protect the computers in these networks while allowing traffic to flow between them.
	Before you begin, read about securing your ISA Server computer.
	Define Your ISA Server Network Configuration
	Select a predefined network template to create your ISA Server network layout and apply default
	networks.
	View and Create Firewall Policy Rules
	Create rules defining how ISA Server allows secure access to Internet sites, corporate e-mail,
	system policy editor to define how ISA Server enables the infrastructure necessary to manage network security and connectivity. Read about system policy
	Define How ISA Server Caches Web Content
	Define a cache drive and then accelerate Web performance by specifying how Web content is downloaded to the cache and how often objects in the cache are updated.
	Configure VPN Access
	Enable and configure a secure virtual private network (VPN) for remote client access to the Internal network.
	Monitor your ISA Server Networks
การกำหนดค่า Network	เราพบุเว่าตอบเพี้เราติดตั้งระบบบละให้กำหบุดหบายเลข IP

	192.168.0.1-192.168.0.255 > Internal
	ที่เหลือเป็น External
	หมายเลข IP ของ ISA จะเป็น Local
	การกำหนดดำเนินการที่ Server Node > Configuration > Networks
	Microsoft Internet Security and Accelerat 🔗 👩 ISAServ
	Eile Action View Help
	$\Leftrightarrow \rightarrow \textcircled{1} \textcircled{2} \textcircled{2} \diamondsuit $
	Microsoft Internet Security and Accele Monitoring Firewall Policy Virtual Private Networks (VPN) Configuration Cache Add-ins General Microsoft Internet Security Acceleration Ser Standard Edition Click here to learn a Networks Edge
	ภายใน Networks จะแบ่งเป็น
	External เครือข่ายทั้งหมดที่นอกเหนือจาก Local Host และ Internal
	Internal คือเครือข่ายที่ระบุตอนติดตั้ง (เครือข่ายภายใน)
	Local Host กือเกรื่อง ISA Server
	Quarantine VPN คือกลุ่มเครื่องกักกัน
	VPn Client คือเกรื่องที่เข้าใช้ VPN Server
	Network Sets คือการเอารายการของ Networks มาสร้างกลุ่ม
	All Network หมายถึงทุกเครือข่าย
	All Protected Network หมายถึงทุกเครือข่ายยกเว้น External
	Roles คือการกำหนดเส้นทางในการวิ่ง
	มี 2 ประเภทคือ Route, NAT
	Private > Private (Route)
	Public > Public (Router)
	VPN Client > Internal (Route)
	Internal > External (NAT)
	Local host > All Network (Route)
การสร้างเครือข่ายใหม่	1. กลิกที่ Server Node > Configuration > Network > Networks
	 คลิก Create a New network รายการด้านขวา

	New Network Wizard	2
	Microsoft Internet Security & Acceleration Server 2006 This spec object	elcome to zard wizard helps yc cify one or more ct that can be u
	Network	work name: 3A1 continue, click N
	3. ใส่ชื่อ Network Name, กลิกปุ่ม Next	
	4. ระบุ Network type เช่น Internal, คลิกบ่	ุ่ม Next
	5. ระบุช่วงหมายเลข IP, คลิก Next, คลิกปุ่	ุ่ม Finish
	6. คลิกปุ่ม Apply, คลิก OK	
	7. เราต้องกำหนด Rules โดยถ้ำเป็น Private	e กับ Private ให้กำหนดเป็น Ro⊍te
ทำไม่ติดตั้ง ISA Server	เนื่องจาก ISA Server เป็นกฎปิด	
แล้วออก Internet ไม่ได้	- ให้ไปที่ firewall policy ตรวจสอบว่	าปิดจริง
	H 気 む し む Microsoft Internet Security and Accelerat File Action Yew Help ← → ℃ 10 ② ● ● ● Microsoft Internet Security and Accele Microsoft Internet Security and Accele Microsoft Internet Security and Accele Microsoft Internet Security and Accele Microsoft Internet Security and Acceleration Set Standard Galoon O Click here to learn. Networks Addins General	ver VM v v - 5
	ถ้าต้องการเปิดให้ใช้ทำอย่างไร	
	1. ใช้ Network Template	
	2. สร้ำง Access Control Policy	
	Network Template	
	1. กิถิก Server Node > Configuration > n	etworks
	2. คลิกที่แท็บ Templates	
	3. ระบุชนิดของ Firewall	

	Tasks Templates Help
	Edge Frewall Connect your Internal network to the Internet and protect it from intruders.
	Connect your Internal network
	to the Internet, protect it from intruders, and publish services to the Internet from a Perimeter network.
	Front Firewall
	Use ISA Server as the mont line of defense in a back-to-back perimeter network configuration. Use this option when you have two firewalls between the protected Internal network and the Internet.
	4. ให้กลิกที่ Edge Firewall
	5. คลิกปุ่มNext
	$6 n\overline{n}$ Next \overline{n} $7 n\overline{s}$
	7 เลือก Unrestricted Internet Access. คลิกป่ม Next. คลิกป่ม Finish
	8 คลิกป่ม Apply. คลิก OK
	ทดสถาปโดยให้
	1. เปิด Browser ไปพิมพ์ URL <u>http://www.internet.com</u>
	2. ftp 202.55.44.101 ระบุชื่อ Anonymous แล้วเกาะ Enter 2 ครั้ง พิมพ์ I s
	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	1. ไปที่ Server Node > configuration > Networks > คลิกที่แท็บ Templates
Access	(ด้านซ้าย)
	2. คลิกที่ Edge Firewall, คลิกปุ่ม Next 3 ครั้ง แล้วเลือก Limited Web Access Only,

	คลิกปุ่ม Next แล้วคลิกปุ่ม Finish
	3. คลิกปุ่ม Apply, คลิกปุ่ม OK
	4. ตรวจสอบดใน Firewall Policy
	Web Access Only Properties
	General Action Rotocols From
	<u>I</u> his rule applies to:
	Selected protocols
	Protocols:
	FTP HTTP HTTPS
	ทดสอบสกข่าย
	1. ลองเปิด Browser ใช้ได้
	2 ให้ Telnet ไม่ได้
	2. ジェーマローマン 3. 1 3. 1 省 FTP 1 尚
	4 Ping ไม่ได้
กรณีที่ลูกข่ายออก	1. ตรวจสอบที่ Default Gateway ว่าระบุไปยังขา ISA Server หรือไม่
อินเทอร์เน็ต	2. ตรวจสอบหมายเลข IP ว่าตรงกับตามโครงสร้างระบบเครือข่ายหรือไม่
ถ้าต้องการใช้ Remote	1. ให้เปิด ISA Server Management
Desktop มาเข้าที่ ISA	2. คลิกขวาที่ Firewall Policy > Edit System Policy
Server ทำอย่างไร	3. ใปดูรายการ Remote Management > TerminalServer
	System Policy Editor ? × Configuration Groups Eeneral From Remote Management This rule applies to traffic from these sources: Microsoft Management Remote Management Computers Microsoft Error Repo Edt ICMP (Microsoft Error Repo Edt Windows Networking Microsoft Error Repo Microsoft Error Repo HTTP Connectivity viruation WUD'11 กลี้องที่จะใช้ Remote Management Computers ได้ต้องอยู่ในกลุ่ม Remote Management Computers ทำอย่างไร
	4. ให้ไปที่Tool box

	Internet
ถ้าต้องการบริหารงาน ISA	1. ติดตั้ง ISA server จากแผ่นซีดีรอมของ ISA Server 2006
Server จากลูกข่ายภายใน	2. แถ้วเรียก ISA Server Management ด้วยบุคคลที่มีสิทธิ์ในการบริหารงาน
ทำได้อย่างไร	
การติดตั้ง Microsoft	1. เข้าไปในแผ่นซีดีรอมของ ISA Server จะมีโฟลเดอร์ client
firewall Client	2. ดับเบิ้ลกลิกไฟล์ setup.exe ซึ่ง ISA Server จะมี Firewall client อยู่แล้ว
การกำหนดค่าควบคุมลูก	1. ไปที่ ISA Server Management > Server Node > Configuration > Networks >
ข่าย	Networks tab > ดับเบิ้ถกถิกที่ Internal

	Internal Properties
	Auto Discovery Firewall Client Web Proxy General Addresses Domains Web Browser Specify which servers or domains clients access directly, and how clients access the Internet if ISA Server is unavailable. These settings apply to all Web browsers using the specified utomatic configuration script from this ISA Server. Bypass proxy for Web servers in this network Directly access computers specified in the Domains tab Directly access computers specified in the Addresses tab เราสามารถที่จะปรับเปลี่ยนค่า Firewall Client, Web Proxy ส่วน SecureNAT ไม่ ต้องทำอะไรให้กำหนดเฉพาะ Default Gateway ผ่าน ISA Server เท่านั้น
การกำหนดบังคับให้ลูก	1. ไปที่ ISA Server Management > Server Node > Configuration > Networks >
ข่ายต้องลีอกออนก่อนผ่าน	Networks tab > ดับเบิ้ลกลิกที่ Internal
Internet	2. ¹ JİİLIŸİJ Web Proxy, nâniİİJİJ Authentication General Addresses Domains Web Browser Auto Discovery Frewall Clent Web Proxy ♥ Enable Web Proxy clent of the Server computer. ♥ Enable HTTP HTTP ort: 0000 SSL Enable SSL SSL port: 0444 Configure alowed authentication Configure alowed authentication Configure alowed authentication Configure alowed authentication Configure advanced propertie Advanced Ø Enable Servers for authentication: Select Dometry. Select RADIUS Servers for authentication: RADIUS Servers ØK Cancel ØK Cancel ØK Cancel
	3. กลิกที่ Require all users to authenticate
	 4. รายชื่อที่ใช้ถือกออนจะเป็นรายชื่อบนเครื่องที่ดำเนินการ (L3ISA01) Computer Management (UCOR) Exponen

	1. เปิด Browser ไปที่ Options > Internet Options
	2. คลิกที่แท็บ Connections > คลิกที่ LAN Settings
	2. กลิกิทีแบทับ Connections > กลิกิที LAN Settings Local Area Network (LAN) Settings Image: Configuration and override manual settings. To ensure the use of manual settings, disable automatic configuration. Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration. Image: Configuration and override manual settings. To ensure the use of manual settings, disable automatic configuration. Image: Configuration script Address Use a utomatic configuration script Address Image: Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections). Address: 192.168.0.99 Image: Construction of the use of
การเซต Automatic	1. จะใช้ร่วมกับ DHCP จะต้องแจกหมายเลข IP และค่า WPAD (Web Proxy
Discovery ปน ISA Server	Automatic Discovery) หมายเลข WPAD จะกำหนดโค้ด 252 และระบุ DNS ให้ไป หา WPAD.โดเมน 2 SecureNAT (Transparent)
กรณีที่ต้องการระบ	กำหนดที่ Advanced Settings ใส่ก่าเวลาที่เราต้องการเช่น 300 คือ 5 นาที
ระยะเวลารับรองของ Web Proxy	Internal Properties Advanced Settings Specify the number of allowed concurrent client connections. Number of connections: Unlimited Maximum: Connection timeout (seconds): OK Cancel Configure allowed authentication methods: Advanced
การพิจารณาเงื่อนไขใน Firewall Policy ปัญหาการที่ ISA Server ไม่สามารถติดต่อภายนอก ได้	จะพิจารณาจากบนลงล่าง หมายถึงถ้าระบุว่า Deny ด้านล่าง (เงื่อนไขใดไม่ถูกกำหนดจะหมายถึง Deny) 1. ให้ตรวจสอบที่ Firewall Policy ดูเงื่อนไข - Allow - Source > Destination - Protocols - Schedule, User, Contents 2. ไปตรวจสอบค่ากำหนดของ Networks > Internal
	ถ้ามีการระบุว่า authentication ใน Web Proxy ผู้ใช้ต้องเชื่อมต่อโคเมน หรือเถือก

	Enable Web Proxy Client บน Browser ระบบจะ Popup ให้มีการล็อกออน (ถ้า
	ไม่เช่นนั้นให้เอาออก)
	Authentication Servers
การกำหนดอนุญาตผู้ใช้	1. ISA Server ต้องเชื่อมต่อเข้ายังโดเมนของ AD (ไม่แนะนำ)
	2. ISA Server ระบุใช้ RADIUS Server แทน
การติดตั้ง Firewall Client	1. ในแผ่นซีดีรอมของ ISA Server จะมีโฟลเดอร์ Client
	2. ให้เลือกกำสั่ง Setup เพื่อติดตั้ง รองรับเฉพาะ Windows Platform
	 ระบบจะดึงค่ากำหนดจากเครื่องแม่ข่าย
	Internal Properties ア Auto Discovery Firewall Clent General Addresses Domains Web Browser IP address ranges included in this network: Start Address End Address 192.166.0.1 192.166.0.255 Edt Remove Add Private Add Private Add Range
	ผู้แขางผ่าม แก่ง และ เกิดผ่างการเกิด เพ
	4. Mathin Start > All Programs > Microsoft Firewall Client for ISA Server
	General Settings Web Browser
	Enable Microsoft Firewall Client for ISA Server ISA Server Selection Select how Firewall Client determines the ISA Server used for Internet access: Automatically detected ISA Server: (no ISA Server detected> Detect Now Manually specified ISA Server: L3ISA01 Test Server Default Settings Apply these Firewall Client settings as the default settings for services and users on this computer. Apply Default Settings Now OK Cancel Apply Help
	5. ไปที่แทบ Settings, เถือก Enable และระบุเครื่อง ISA Server
	6. ต้องการดึงก่าไช้ปุ่ม Apply Default Settings Now
การกำหนด Indirect	กรณีที่ ISA Server ไม่ต่ออินเทอร์เน็ตโดยตรง
connection	เช่น ที่ hqr มี ISA Server หลักอยู่ แล้วให้ที่สำนักฯติดต่อผ่าน ISA Server HQR > Province > Area > Group 178 areas 1999 ระหาวร
	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 ห์ถั๊ก (Master)
	Microsoft Internet Security & Networks Acceleration Server 2006 Standet Gradina
	() Click here to learn about the Eustomer Experience Improvement Program.
	Defout rule Properties 2 × I Edge Firewall General Action To Endging
	Process requests by: C Betrieving them directly from the specified destination
	Redrecting from to a specified upstream server Upstream proxy server: Settings
	Bokup route: Bokup route: Bokup route: Settings Bokup route: Settings D Name To D Anne To
	C Last Default rule 🔅 Al N C Regrecting them to a hosted site
	Port: 80 SSL Port: 443
	Cautomatic dal-up for the primary route Use automatic dal-up for the big/up route Use automatic dal-up for the big/up route
	Help about automatic datus connections
ရားရှိသူမှာ ICA ရောက္က	
ร้างสาย o	1. III Server Node > Configuration > Cache
1114 Lache Server	2. FIGTIFII IGN detine cache drive
	3. ระบุขนาดทเกบ เวเรงป Properties 7 x
	Cade brives
	3/35401
	Crive Type Del Space [Free Space] Cache Stee Crime State St
	Bisomum cache size (HD): 100 5et Enset
	Total dak space on NITFS drives (MB): 16370 Current total cade size (MB): 100
	OK Careel Arch
	เช่น 100 หมายถึง 100 MB
	ิดลิกปุ่ม S≞+
	น คลิกป่า Apply คลิก OK สองครั้ง
	ข้ออารระวังก้าแอซเซ็ม ระบบจะออก Internet ไม่ได้
	ให้หนับแกลียร์แคชเป็นระยะโดยไปที่ c\urdcache
	ลกข่ายที่ต้องการใช้ Cache Server
	ו. וווזטא ISA server אטאזבע Port מואזט Proxy ואט ושא Server Node > Configuration > Networks > Internal > Web Proxy tab
	ให้ระบพอร์ตที่ต้องการ เช่น 8080
	ถ้า ISA Server ต้องการให้ Authentication จะคลิกที่ป่ม Authentication แล้วเลือก
	วิธีการ (domain, radius, custom)
	2. ต้องระบ Internet Options ให้ใช้ Web Proxy มาที่เครื่อง ISA Server
	ถ้าขั้นตอนที่1 ระบ 8080 ตรงนี้ต้องระบ 8080 ด้วย

การกำหนด Cache มี 3	1. กำหนดขนาดที่เกี่บ
ขั้นตอน	2. กำหนดเงื่อนไขที่เก็บ (Cache Role)
	- FTP, HTTP - TTL Min MAX (Casha) Size
	- Content type (Dynamic)
	 การทำ Active Cache ระบบจะทำการดาวน์โหลดเว็บมาเก็บไว้ก่อน
ต้องการบล็อกเว็บที่	1. เปิด ISA Server 2006 Management > Server Node > Firewall Policy
อาจารย์สุรชัยนิยมใช้	2. ด้านขวาจะมีแท็บ Toolbox
	 เมษายางานสายครามสา สายครามสายคร รายครามสายครา สายคร สายครามสายครายครามสายคราสายคราคราคราคราครายคราครายคราคราคราคราคราคราคราคราครา
กรณีที่เราต้องการ	เราด้องเลือก Deny จึงสามารถกำหนด Redirect ได้
Redirect Web site หรือ เงื่อนไขต่างๆ	Strachablock Properties Image: Schedule Content Types General Action Protocols From Action to take when the rule conditions are met: Image: Content Types Image: Content Types Image: Content take when the rule conditions are met: Image: Content Types Image: Content Types Image: Content take when the rule conditions are met: Image: Content Types Image: Content Types Image: Content take when the rule conditions are met: Image: Content take when the rule conditions are met: Image: Content take when the rule conditions are met: Image: Content take when the rule conditions are met: Image: Content take when the rule conditions are met: Image: Content take when the rule conditions are met: Image: Content take when the rule conditions are met: Image: Content take when the rule conditions are met: Image: Content take when the rule conditions are met: Image: Content take when the rule condition to take when the rule take when the rule take when the rule take when the rule condition to take when the rule take when
ต้องจำกัดแบนด์วิดช์	ในเวอร์ชั่น ISA server 2000
	แต่ในเวอร์ชั่น ISA server 2004, 2006 ไม่มี
	แนะนำให้ไปใช้ Hardware block (Juniper)

การกำหนด User	ISA Server สามารถระบุได้ 4 แบบ
	Nain Add Indupdate the configure Windows users and groups LDAP RADIUS SecurID Image: Configure
	 Windows users and groups ต้องนำเครื่องไปเชื่อมต่อกับ โคเมน
	- LDAP ต้องระบุเครื่อง LDAP Server ไว้ก่อน
	- RADIUS ต้องระบุเครื่อง RADIUS Server ไว้ก่อน (Windows ติดตั้ง IAS Server)
	 SecurID ต้องติดตั้งแอพพลิเกชั่น SecurID ลงในเกรื่อง
	วิธีการกำหนด
	1. ไปที่ Server Node > Firewall Policy > ด้านขวาจะมี Tools ให้เถือก User แล้วคลิก
	ขวาเลือกกำสั่ง New และระบุชื่อที่ต้องการ
	 ระบุชนิดของผู้ใช้ใส่ในรายการที่กำหนด
	การนำไปใช้
	1. ไปที่ Access Rule และระบุใช้แท็บ Users
	Web Access Only Properties
	General Action Protocols From To Users Schedule Content Types This rule applies to requests from the following user sets:
	All Users Add Edit Edit Edit
การควบคุมตารางเวลา	1. ไปที่ Server Node > Firewall Policy > Toolbox

	tha Users
	<u>concent types</u>
	<u>S</u> chedules
	New Edit Delete
	hal TEST schedule
	two managements and the second s
	Work hours
	2. คลิกที่แถบ Schedules
	3. คลิกปุ่ม New ใส่ชื่อ และช่วงเวลาที่ต้องการ
	การนำไปใช้
	1. ให้เข้าไปใน Access Rule, แท็บ Schedule
	 แล้วเลือกรายการที่ได้สร้างในตอนต้น
การกำหนดควบคุมเนื้อหา	ISA Server ใด้มีการเซตไว้ให้เรียบร้อยแล้ว Content type
	ถ้าต้องการเพิ่มทำได้โดย
	1. ไปที่ Server Node > Firewall Policy > Toolbox
	2. แถบ Content Types > คลิกปุ่ม New
	3. ระบุชื่อกฎ
	New Content Type Set
	Name: Image
	Description:
	Specify the file and MIME types included in the content type set.
	Available types:
	iji Add
	application/hta application/smil
	,jjj ,p7c
	 ระบุชื่อไฟล์ และนามสกุลไฟล์ที่ต้องการบล็อก
	การนำไปใช้
	1. ให้เข้าไปใน Access Rule, แท็บ Content type
	 แล้วเลือกรายการที่ได้สร้างในตอนต้น
การตรวจสอบกิจกรรม	1. ไปที่ Server Node > Monitor
ของผู้ใช้ ISA Server	2. คลิกที่แท็บ Logging

	(1) Elick here to learn about the Customer Experience Improvement Program.
	Conditionard y Alerts y Services y Reports y Connectivity Verifiers y Longling Tasks (Help) Filter By Condition Value
	Log Record Type Equals Firewall or Web P Logging Tasks
	Clerk IP Equals 192.168.0.101
	Configure Proval Loging
	Log Time Destination IP Destination Port Protocol Action Rule Configure Web Procy Logging S(4/2551 11:59:13 202.55.44.101 S3 DNS Denied Connection Default rule Configure Veb Procy Logging Configure Veb Procy Loggi
	5/4/2551 11:59:14 202:55:44.101 53 DNS Denied Connection Default rule Import Filter Definitions
	5/4/2551 11:59:15 202.55.44.101 53 DNS Deried Connection Default rule
	S/4/2551 11:59:21 202:55.44.101 53 DNS Denied Connection Default rule
	5(4)2551 11:59:29 192.168.0.255 137 NetRiss Name Ser Denied Connection Qui Copy Al Results to Cloboard
	5/4/2551 11:59:31 192.168.0.255 137 NgBios Name Ser Denied Connection
	5/4/2551 12:00:19 202:55:44:101 0 PING Initiated Connection Web Access C
	3. ด้านซ้ายจะมี Start query เราคลิกที่กำสั่งนี้
	จะพบว่ากิจกรรมทั้งหมดจะถูกแสดงผล
	4. ถ้าต้องการระบุเฉพาะเงื่อนไขที่ด้องการให้ไปกลิกที่ Edit filter
	Show only entries that match these conditions:
	Filter By Condition Value
	Log Record Type Equals Firewall or Web Proxy Filter Log Time Live
	Client IP Equals 192.168.0.101
	Define the criteria used to filter the data:
	Theorem Constitution Union
	Client IP Founds 192 . 168 . 0 . 101
	Remove Update Add To List
	Start Query Cancel
	ระบุ Filter by เช่น client IP เลือกเงือนไขว่า Equals และค่า Value เช่น
	192.168.0.101 คลกปุ่มStart query จะพบวาเง่อน ไขจะกำหนดไห้แสดงผลเฉพาะ
-	ราชการทระบุ
การป้องกันการจู่โจมจาก	Additional Security Policy
ภายนอก	Enable Intrusion Detection and DNS Attack Detection 🛛 🙀 Configure Flood Mitigation Settings
	Configure IP Protection
	- IDS & DNS Attack การโจมตีระบบจากผู้บุกรุก
	- Flood การยิงเครื่องให้ล่ม
	- IP Protection การป้องกันโหลดของเครื่อง
	1. ISA server Management > Server Node > Configuration > General >
	Additional Security Policy
	ถ้าหนดป้องอันอารออโอนตีอาออาซนออ
	104.0 - จะสี่มหัดจระ VDN 0
ทาวบองกนการดกพง	ISA Server 1530151115 VPN Server

	crosoft Internet Security and Accelerat 🖉 👩 ISAServer
Eile	Action View Help
\$	
	Iicrosoft Internet Security and Accele Internet Security & Internet Security & Acceleration Server 2006 Standard Edition
	Wirtual Private Networks (VPN) Origuration
	Cache Remote Sites
	General Configure VPN C This page helps you define a private network (VPN) conne
	Configure Address As:
	1. ใปที่ Server Node > Virtual Private Networks (VPN)
	2. กลิกที่ Configure Address Assignment
	Virtual Private Networks (VPN) Properties
	Access Networks Address Assignment Authentication RADIUS
	Select the IP address assignment method:
	Start Address End Address Add 192.168.1.101 192.168.1.150 Edit Remove Edit
	3. ระบุช่วงหมายเลข IP ซึ่งต้องไม่ตรงกับ Internal, คลิก OK
	VPN Clients Properties
	General Groups Protocols User Mapping
	Enable VPN client access
	Maximum number of VPN clients allowed:
	20
	จะการแก่ Enable VPIN Clients, เอ็มูขาน มน VPIN Clients ที่เขอ ระการสารระดูการสารร การระดูการสารระดูการสารระดูการสารระดูการสารระดูการสารระดูการสารระดูการสารระดูการสารระดูการสารระดูการสารระดูการสารร สารระดูการสารระดูการสารระดูการสารระดูการสารระดูการสารระดูการสารระดูการสารระดูการสารระดูการสารรรถารสารระดูการสารร
	D. IL II Specify Windows Users
	 คลิกระบุกลุ่มที่ต้องการ (เราต้องไส่สมาชิกในกลุ่มให้เรียบร้อยก่อน) PN Clients Properties General Groups Protocols User Mapping
	Select the domain groups for which remote access is allowed:
	Namespace Iroup Uomain Add Windows VPN L3ISA01 Eemove
การ	ทคสอบที่ลูกข่าย (อินเทอร์เน็ต)

	1. เปิด Network Connection
	2. เถื่อก Create a new connection, กลิกปุ่ม Next
	 3. เลือก Connect to the network at my workplace, คลิกปุ่ม Next Connect to the Internet Connect to the Internet so you can browse the Web and read email. Connect to the network at my workplace Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location. Set up an advanced connection Connect to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.
	4. เถือก 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 คืออะไว	โดยทั่วไป ISA Server จะกำหนด Access Role 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)
	เราต้องกิดก่อนว่า
	1. IP ภายในอยู่ที่ไหน
	2. ต้องการผ่านพอร์ตอะไร
การเข้าดูล็อก	1. เครื่องภายนอก(อินเทอร์เน็ต)เข้ามาดูเว็บภายในพบว่าในล็อกของ Web Server ขึ้น
	รายการ IP ของ ISA Server ขาในเท่านั้น ทำอย่างไร
	ตอบ ให้เปิดดูล็อกของ ISA Server ประกอบ