บทที่ ๕ การกำหนด Firewall Policy

ผู้เขียนได้ทดลองทำการติดตั้ง TMG ๒๐๑๐ ตามบทที่ ๔ ซึ่งทำตามขั้นตอนและหน้าต่างที่ ปรากฏขึ้นมาโดยตลอด พบว่า Firewall Policy ที่ติดตั้งมากับระบบเมื่อจะทำการบริหารจัดการ เครือข่ายคอมพิวเตอร์เพื่อเชื่อมออกสู่อินเทอร์เน็ตพบว่าเป็นไปด้วยความยุ่งยาก ซึ่งไม่แน่ใจว่าเป็น เพราะการติดตั้งหรืออย่างไร แต่ผู้เขียนได้ทดลองทำถึง ๓ ครั้ง ก็พบว่าเป็นปัญหาเดิมๆ อยู่ จึงคิดว่า เราจะไม่สนใจ Firewall Policy ที่ติดตั้งมาตามบทที่ ๔ แต่ผู้เขียนจะกำหนด Firewall Policy ด้วย ตนเอง ซึ่งจะทำให้ผู้อ่านเข้าใจและรู้ที่มาที่ไปพร้อมกับเรียนรู้ไปในตัวอันจะทำให้เกิดความเข้าใจมาก ยิ่งขึ้น

โดยวิธีการตั้ง Firewall Policy ด้วยตนเอง ให้ทำดังนี้

๑. ขั้นแรกเราจะลบ Firewall Policy เดิมทิ้งเสียก่อน โดยให้เปิด Forefront TMG ให้เป็น ดังรูป ๕.๑ (นำเมาส์ไปคลิกที่ Firewall Policy ตรงช่องซ้ายมือ)

File Auton Vew Help) (E) 📑 😑 🤉	9 2° 40 D			
Nicrosoft Forefort Trraet Managene Discosoft Forefort Trraet Managene Dashbaard Monitoring Coshbaard Monitoring Coshbaard Monitoring Coshbaard Monitoring Coshbaard Monitoring Coshbaard Monitoring Coshbaard Monitoring	Fore Threat	front: t Management (Reliex	Sateway 2010		Firewall Policy Statulard / Teobox / Tesks / Heb
C-Mail Folicy	Search		P Examples		
Remote Access Policy (VPN)	Order	Name	Acton	Frotocc +	Firewall Policy Tasks
▲ Networking 日子 Sylinin 山口ge 8 Reports ジロ4dato Center 留作 Troubleshooting	• Web Acces	ss Policy Group Blacked Web Des	🚫 Deny	Qim	Publish Exchange Web Clini L Arress Publish Muß Servers Publish Muß Servers Publish Web Stess Publish Non-Web Server Protocols Cristic Access Rule Contigure VoIP Contigure VoIP
	⊒ 👅 2	Allow Web Acces	🥝 Alow		Policy Editing Tasks
	💽 Last	Defa il que	S In-ny	😫 Al Ti	Edill Selected Rule Delete Sciented Rules
· 1				▶	A. Move Selected Rilles Drown

รูป ๕.๑

๒. นำเมาส์ไปคลิกขวาที่ Allow Web Access... แล้วเลือก Delete เพื่อลบ Firewall Policy ที่ติดตั้งตามบทที่ ๔ ซึ่งจะได้ตามรูป ๕.๒ และเมื่อคลิกปุ่ม Delete ก็จะถาม ยืนยันว่าต้องการลบ Allow Web Access for All Users หรือไม่ ตามรูป ๕.๓ ก็ให้ คลิกปุ่ม Yes

• 🔶 🔟 🔝 🖬 😫 🕸		9 🖲 🎡 🔁 🧐 1	9 🔹 🖢 🤅	E 🖻 🔶	
Nicrosoft Forsfront Threat Manageme Forefront IMs (WLN-RRBSESNILH Cashboard Monitoring	Fore Threat	front Management G	ateway 2010	Ŭ.	Firewall Polic Standar
Rewall Policy	All firewall	Policy			Toolocx Tasks Tieb
C-Mai Folcy	Search	A	Examples		
Intrusion Prevention System Remote Access Policy (VPN)	Order	Name	Acton	Frotoce +	Firewall Policy Tasks
A Networking	Web Acces	s Policy Group		-	Publish Exchange Web
Logs & Reports	I 💽 1	Blocked Web Dec.	. 🚫 Deny	Properdes Delete	Cient Access Publish Mail Servers
Traubleshooting				Сору	Publish SharePoint Sites
				Ungroup	Publish Web Stes
				Export Selected Import to Select	Publish Non Web Server Protocols Create Access Rule
				Move Up Disable	Configure VoIP Configure Client Access
		Alow Web Acces	Alow	Configure HITP	
				1111 M	Policy Editing Tasks
	Pil and	Defedition	S Derm	DB MIT	Edit Constant D. In

รูป ๕.๒

Confirm Delete	X
	a dalate "Allow Wab Access for
All Users"?	Delete Allow Web Accessitor
Tes	110

ູລູປ ໕.๓

๓. จากรูป ๕.๓ เมื่อคลิกปุ่ม Yes แล้วจะได้ตามรูป ๕.๔

Forefront ING					_ [0) ×
File Action Vew Help						
💠 🔶 Ž 📅 🚺 🖬 🖄 🗳	ی ک ک	: 💖 🖬 🍇 🧕	• •			
Initrosoft Fordford Toreat Vanagenei Initrosoft Fordford Toreat Vanagenei Softboard Osahboard Monitaring Monitaring With Access Polev With Access Polev Softboard Folge	Morealt Forei Threat App	Management (y Discard	Sateway 2010 To save changer	s and update the cor	Firewall Poli Strinta Infguration, click Apply.	icy Ind
Remote Access Policy (VPN) Networking	Swarting		D Examples		Transie (199	1
System	Urder 🔺	Name	Acton	-rotoce +	Firewall Policy Tasks	
🥏 update Center 🔮 Trachleshaating	E Web Acces	s Policy Group Blocked Web De	a 🚫 Deny	анти Однии	 Publish Exchange Web Ciant Access Publish Mail Servers Publish SharePoint Sites Publish Web Sites 	_
				L	Publish Non-Web Server Protocols	
					Create Access Rule	
					Configure VoIP	
					Configure Client Access	
()	🕐 Last	Default rue	🚫 Deny	(TIA)	Policy Editing Tasks	

ູລູປ ໕.໔

๔. จากรูป ๕.๔ ให้คลิกปุ่ม Apply จะได้ตามรูป ๕.๕

Horefront ING		_ [] ×
File Action Vew Help		
🗢 🎓 🖄 🖬 🚺 🖬		
Introsoft Forefront Threat N Introsoft Forefront IMs (W.IN-RK) Toshbard Mondaring	Anagement Sessalut Threat Management Gateway 2010	Firewall Policy Standard
Prewall Policy	guration Change Description	× Acply.
C-Mail Folicy Typ Thruston Prev Remote Accee Networking	 a description for the applied changes. The description is displayed in the change tracking with nge description; 	
Logs & Report		Policy Tasks Exchange Web
	xport You can click Export to back up the entire configuration before applying the changes	Mail Servers SharePoint Sites
F	Do not show the promot again Apply Cance	Non-Web Server
		Configure VoIP Configure Client Access
<u> </u>	Last Defaultrue Obery (Jal)	Dicy Editing Tasks

ູລູປ ໕.໕

๙. คลิกปุ่ม Apply อีกที่ จะได้ตามรูป ๕.๖

Horefront ING		_ _ _ ×
(* *) 🖄 🖬 🚺 🖬		
Microsoft For effort Threet Manage Greffont IMs (WINHRBSSM Coshboard Monitoring	ILH Forefront: Threat Management Gateway 2010	Firewall Policy Standard
Web Access Pressing Co	nfouration Changes	k Apply.
Chall Foldy Fulluisin Preve Remote Accent Active Action Settern System S	The deciges were send to the Configuration Stange. Check configuration status to verify that changes were applied to all array memory.	OX Tasks Hep Policy Tasks Exchange Web Vccess Plad Servers ShorePoint Sites Web Sites Non-Web Server
		es Crede AccessRule Configure VoIP Configure Client Access
4	Lost Default rule ODeny QAIT	Policy Editing Tasks

รูป ๕.๖

แล้วคลิก OK จะได้ตามรูป ๕.๗



รูป ๕.๗

๖. จากรูป ๕.๗ คลิกขวาที่ Firewall Policy ที่อยู่ทางด้านซ้ายแล้วเลือกเมนู New ->
 Access Rule... ตามรูป ๕.๘

		2 30				
-orefrant IMS Cashboar	d (WIN-KKBSESNICH	F	orefront preat Management	: Gateway 2010		Firewall Polic Standar
Wab Acce	Refrean	F	wall Policy			Tooloox Tasks Hele
C-Mail Foi	Export Firewal Poin Import Firewal Point	/ /	Name	Acton	- retecola	Firewali Policy Tasks
Networkin System Logs & Re	New Al Tasks	•	Exchange Web Client A Mail Server Publishing P SharePoint Site Publish	acess Publishing Rule rule ng Rule	нтр	Publish Exchange Web Cient Access Mail Servers
ᡒ update O 🕎 Troublesh	Нер		Web Site Publishing Ru Non-Web Server Proto Access Rule	e col Publishing Rule	gennes	Publish SharePoint Sites
		-				Protocola Protocola
	97					👷 Configure VoTP 🎥 Configure Client Access
		💽 Las	st Defaultrue	🚫 Deny	🛄 All Traff	Roliny Edition Lacks

ູລູປ ໕.໔

๗. เมื่อคลิกเลือก Access Rule... จะได้ตามรูป ๕.๙



ູລູປ ໕.๙

 ๘. ในช่อง Access rule name: ให้พิมพ์ Policy ที่ต้องการและสื่อความหมาย เช่น Allow access to all web sites (แปลตามภาษาผู้เขียนก็คืออนุญาตให้เชื่อมต่อเว็บไซต์ได้) ตามรูป ๕.๑๐ แล้วคลิกปุ่ม Next

Welcome to the New Access Rule Wizard
This wizard helps you create a new access rule. Access rules define the action that is taken, and the protocols that may be used, when specified clients from one network attempt to access specific destinations or content on another network.
Access rule name: Allow access to all web sites
To continue, click Next.

รูป ๕.๑๐

๙. จะได้ตามรูป ๕.๑๑ ให้คลิกเลือกช่อง 🖸 Allow (อนุญาต) แล้วคลิกปุ่ม Next



รูป ๕.๑๑

๑๐.จะได้หน้าต่าง Protocols ตามรูป ๕.๑๒ ซึ่งในช่อง This rule applies to: ให้เลือกเป็น Selected protocols

v Access Rule Wizard		100.00
Protocols Select the protocols this rule applies to.		\mathbb{H}
This rule applies to:		
Selected protocols Protocols:		
		Add
		Edit
		Remove
		Ports
	< Back	Next > Cancel

รูป ๕.๑๒

๑๑.จากนั้นคลิกปุ่ม Add... จะได้หน้าต่างย่อยชื่อ Add Protocols ให้เลือก Add เข้าไป ดังนี้คือ HTTP และ HTTPS ซึ่งอยู่ภายใต้หมวด Web ตามรูป ๕.๑๓





๑๒.เมื่อคลิก Add เข้าไปทั้ง ๒ ตัวแล้ว ให้คลิกที่ปุ่ม Close จะได้ตามรูป ๕.๑๔

Protocols Select the protocols this rule applies to.	ł
This rule applies to:	
Selected protocols	
Protocols:	
<u>Щ</u> нттр	Add
MI HTTPS	Edit
	Remove
	Ports
< Back	Next > Cancel

รูป ๕.๑๔

๑๓.คลิกปุ่ม Next ต่อไปจะได้หน้าต่าง Malware Inspection ตามรูป ๕.๑๕ ให้คลิกเลือก 💿 Enable malware inspection for this rule

Access Rule Wizar	ď			
Malware Inspection	1			
Select malware ins	spection settings.			11
Enable malware instant	spection for this rul	e		
C Do not enable mai	ware inspection for	this rule		
For malware globally.	inspection to be a	pplied to this rule, i	malware inspection	must be enabled
elp about malware insp	ection.			
		< Back	Next >	Cancel

รูป ๕.๑๕

๑๔.คลิกปุ่ม Next ต่อไปจะได้หน้าต่าง Access Rule Sources ตามรูป ๕.๑๖

This rule applie	s to traffic from the	ese sources:		
				Add
				Edit
				Remove
			-	

รูป ๕.๑๖

๑๕.ให้คลิกปุ่ม Add... จะได้หน้าต่างย่อย Add Network Entities ตามรูป ๕.๑๗ เพื่อเลือก เครือข่ายต้นทาง ให้เลือก Internal ซึ่งอยู่ภายใต้หมวด Networks แล้วคลิก Add และ Close ตามลำดับ

Vew +	Edit Delete	
🗆 🗁	Networks	
	External	
	📥 Internal	
	📥 Local Host	
	duarantined VPN Clients	
	VPN Clients	
+ 🚞	Network Sets	
	Computers	
+ 🚞	Computer Sets	
H 🚞	Address Ranges	
	Subnets	

๑๖.เมื่อเลือกเครือข่ายต้นทางแล้ว จะได้ตามรูป ๕.๑๘ ซึ่งในช่อง This rule applies to traffic from these sources: จะเป็น Internal

ccess Rule Sources		
This rule will apply to traffic originating	from the sources specified in this page.	
his rule applies to traffic from these source		
	Ad	id
	Ed	lit
	Ren	nove

รูป ๕.๑๘

ด๗.จากรูป ๕.๑๘ ให้คลิกปุ่ม Next จะได้หน้าต่าง Access Rule Destination (เครือข่าย ปลายทาง) ตามรูป ๕.๑๙

nis rule applies to traf	fic sent to these des	tinations:	
12			Add
			Edit
			Remove

รูป ๕.๑๙

๑๘.ให้คลิกปุ่ม Add... จะได้หน้าต่างย่อย Add Network Entities ตามรูป ๕.๒๐ เพื่อเลือก เครือข่ายปลายทาง ให้เลือก External ซึ่งอยู่ภายใต้หมวด Networks แล้วคลิก Add และ Close ตามลำดับ

w	Edit Delete
1	Networks
	External
	📥 Internal
	📥 Local Host
	- Quarantined VPN Clients
	VPN Clients
	Network Sets
	Computers
	Computer Sets
	Address Ranges
	Subnets
	Domain Name Sets
	URL Categories
	URL Category Sets
	URL Sets

รูป ๕.๒๐

๑๙.เมื่อเลือกเครือข่ายปลายทางแล้ว จะได้ตามรูป ๕.๒๑ ซึ่งในช่อง This rule applies to traffic sent to these destination: จะเป็น External

This rule will apply to traffic sent from the rule in this page.	sources to the destinations specified
nis rule applies to traffic sent to these destination External	Add
	Edit
	Remove

รูป ๕.๒๑

๒๐.คลิก Next จะได้หน้าต่าง User Sets ตามรูป ๕.๒๒ ซึ่งก็มีค่า All Users ให้มาแล้ว (ถ้า ไม่มีก็ให้คลิก Add... แล้วเลือก All Users)

Access Rule Wizard		
User Sets You can apply the rule to rea specific user sets.	quests from all users. Or, you can limit acce	ss to
This rule applies to requests from	the following user sets:	Add
		Edit.
		henove
		Consul

รูป ๕.๒๒

๒๑.เมื่อคลิก Next จะได้หน้าต่าง Completing the New Access Rule Wizard ตามรูป

	Completing the New Access Rule Wizard
	You have successfully completed the New Access Rule Wizard. The new Access Rule will have the following configuration:
	Name: Allow access to all web sites Action: Allow Traffic: HTTP,HTTPS Malware Inspection: Enabled
KKKK I –	To close the wizard, click Finish.

รูป ๕.๒๓

๒๒.ให้คลิก Finish จะได้ตามรูป ๕.๒๔

டீ. ©ள

File Action Vew Help					
🎋 🏓 Ž 📅 📓 🖬 😫 🍋	🚰 🗙 🏵 🤇	😍 🗗 🔬 💽 📀	🚰 🎪] 🖂	8	
Nou wolf Far of ar LT in set Mainsgemei Torefront IMs (WIN480555MILH Coohboard Manchainy Manchainy Freewell Policy Cooh Folgy Cooh	Korstr Forefront Threat Management Gateway 2010 Apply Discard To save charges and update the cor Old Eleveral Rollor				Firewall Polic Standar figuraton, dick Apply.
Remote Access Policy (VPN) Notworking Josten Josten Josten Josten Josten Josten Josten Josten Traublashooting	Scarof Order A	Name Blacked Web Dea	Acton	Arctocc •	Firewall Policy Tacks
	E 💽 2	Allow access to a	🥝 Alow	рания С ните ППТ	🚰 Configure Client Access
1	🕐 Lost	Default rule	🚫 Dепу	NIT _	Policy Editing Tasks

ર્રુની હૅ.७હ

๒๓.จากรูป ๕.๒๔ ให้คลิกปุ่ม Apply จะได้ตามรูป ๕.๒๕

Horefront ING		_ [] ×
He Albon Vev Hap		
Nicrosoft Forefort Threat Manageme Jicrosoft Forefort Threat Manageme Jorefront IMs (WUN-RRBSESMILE Dashboard Monitoring Recentl Action	Forefront Threat Management Gateway 2020	Firewall Policy Standard
Wtb Access Configuration	Change Description vize for the appied changes. The description is displayed in the change tracking with plions:	y.
System	You, can dick Export to back up the entire contiguration	Policy Tasks Exchange Web Access Mail Servers
T Do not sh	before applying the changes w this promot again Apply Cance	Web Sites Web Sites Non-Web Server No
	2 Alon sccess to a @Alon UIITT	Configure VoIP Configure Client Access
۲ <u>ه</u>	Last Defaultrue ODeny Walling	Dicy Editing Tasks

รูป ๕.๒๕

๒๔.ให้คลิกปุ่ม Apply จะได้ตามรูป ๕.๒๖

🕮 Forefront 1 HG	_ D ×
File Action Vew Help	
🗢 🔶 💼 📓 🗃	
Marcadoff Pareff at IT real Mainingement Greefmont IMs (WILHARDSSMILH Goodford Maintering) Municiping Magnetization	Firewall Policy Standard
Wab Access PC Saving Configuration Changes	k Apply.
Chair Folder Tota Same Force And Folder The decays were seven to the Configuration Statege, the k Configuration States to verify that changes were applied to all array members.	OK Tasks Heb
C update Center Troublishootin Existing clent connections will be resvaluated according to the new configuration. Client connections and matching the newly enforced put	Exchange Web Vocess Mail Servero ShorePoint Sites Web Sites
More about <u>Soley enforcement</u>	Non-Web Server
= 📢 2 Alow access to a 🖉 Alow 👔	HIII Credit Access R de Configure VoIP Canfigure Client Access
👔 Last Default rue 🚫 Deny 🥹	All Tire Policy Editing Tasks
	Edit Seected Rule

รูป ๕.๒๖

๒๕.เสร็จแล้วให้คลิกปุ่ม OK จะได้ตามรูป ๕.๒๗

• 🔶 🗾 🔟 🖬						
Nkrosoft Forefront Threat Managemer Forefront IMS (WIN-488565MILH Cashboard Monitoring	Forefront Threat Management Gateway 2010				Firewall Policy Stemlard	
Rrewall Policy						
C-Mai Foicy	Search	9	Examples			
Intrusion Prevention System	Order +	Name	Acton	Frotoce +	Firewall Policy Tasks	
Networking System System Lodate Center Trai bleshooting	∃ 1	Blocked Web Des	🚫 Deny	Шнтв	Publish Exchange Web Circl Acress Publish Mail Servers Publish Mail Servers Publish MarkSates Publish Non-Web Server Protocols Contic AccessRule @ Contic, AccessRule	
	E 💽 2	Allow access to a	. 🥝 Alow	СС НТВ ОДНГВ	Configure Client Access	
	💽 Last	Default rule	🚫 Deny	😡 Alth	Policy Editing Tasks	
1 1		1			X Delete Sciected Rules	

รูป ๕.๒๗

เมื่อมาถึงตอนนี้ เราได้สร้าง Policy บน TMG ๒๐๑๐ สำหรับการเชื่อมออกสู่อินเทอร์เน็ต เสร็จเรียบร้อยแล้ว เครื่องเซิร์ฟเวอร์ของเราก็สามารถนำมาบริหารจัดการเครือข่ายในโรงเรียนได้แล้ว ดังนั้นตอนนี้เครื่องเซิร์ฟเวอร์ของเราก็เป็นพร็อกซี่ (Proxy) แล้ว เครื่องลูกข่ายที่จะออกสู่ อินเทอร์เน็ต เราสามารถใช้เครื่องเซิร์ฟเวอร์นี้บริหารจัดการเครือข่ายในโรงเรียนได้

ในบทต่อไปจะเป็นการจัดการกับเครื่องลุกข่ายในการจะออกสู่อินเทอร์เน็ต และการบริหาร จัดการเบื้องต้น