บทที่ ๗ การบริหารจัดการเครือข่ายคอมพิวเตอร์

หลังจากที่เราได้ทำการตั้ง Firewall Policy สำหรับจัดการเครือข่ายคอมพิวเตอร์ และได้ เรียนรู้การตั้งค่าเครื่องลูกข่าย (เครื่องนักเรียน) เพื่อเชื่อมออกสู่อินเทอร์เน็ตในบทที่ ๕ และบทที่ ๖ มาแล้ว ในบทนี้จะกล่าวถึงการบริหารจัดการเครือข่ายคอมพิวเตอร์พื้นฐาน ซึ่งจะใช้สำหรับเครือข่าย คอมพิวเตอร์ในโรงเรียนของเราก็คือ

- ๑. บล็อก URL (Block URL)
- ๒. บล็อกไฟล์ (Block File)
- ๓. บล็อกไอพีแอดเดรส (Block IP Address)

บล็อก URL (Block URL)

หากเราต้องการบล็อกเว็บไซต์ที่เราไม่อยากให้นักเรียนเข้าใช้ เราสามารถใช้ TMG ๒๐๑๐ ทำ การบล็อกได้ตามต้องการ โดยมีวิธีการดังนี้

๑. เรียกโปรแกรม Forefront Threat Management Gateway ๒๐๑๐ โดยไปที่ Start -

> All Programs ->Microsoft Forefront TMG->Forefront TMG Management จะได้ตามรูป ๗.๑

🕮 Forefront I NG					- O ×
File Action Vew HHp					
🗢 🔿 🖄 🖬 📓 🖬 😫 😔	ې 🖻 🗟 🕑) 🖆 %]			
Microsoft ForeFord Threat Management Genefront IMs (WIN-RRBSESNILH Goshboard Monitaring	Forei	front Management	Gateway 2010		Firewall Policy Standard
Rewall Policy	All Firewall	olicy			Tooloox Tasks Heb
E Mai Polcy	Section		D Examples		
Intrusion Prevention System A Remote Access Policy (VPN)	Order +	Name	Acton	"rotocc +	Firewall Policy Tasks
J. Networking	🗉 Web Access Policy Group			🐑 Publish Exchange Web	
i oyeten i ogy S Reputs pdate Center i Troubi≾hooting	■ <u>1</u> 1	Blocked Web De	s 🚫 Deny	Щнтв Щнов	Clarit Access Clarit Access Ly Publich Mail Servers Publich Web Sites Ly Publich Non-Web Server Protocols Craste Access Public Configure VoIP Configure VoIP Configure Clerit Access
	E 💽 🤉	Alow access to	i 🧭 Alow	Щ нття Щ нття	Policy Editing Tasks
	💽 Last	Default rue	🚫 Deny		 Move Selected Rules Up Move Selected Rules Down
Done					

รูป ๗.๑

๒. ทางช่องซ้ายมือ ให้คลิกชวาที่ Firewall Policy -> New -> Access Rule ตามรูป ๗.๒

* 🔶 🖄 🖬 🛙		🕞 🍯 🗄	1 🕫 🔮 🎕 📘			
 Microsoft Forefront T Forefront TMG (// Cashboard Monitoring 	in eal Managemen YON-RRB365IVITLH	Fo	eat Management (Gateway 2010		Firewall Policy Standard
Wab Acces	Refresh	ri	all Policy			Tooloox Tasks Heb
E Mail Folicy	Export Firewall	Policy Policy	Name	Acton	instace +	Firewali Policy Tasks
Networking System Logs 8 Sep	New Al Tasks	•	Exchange Web Client A Mail Server Publishing F SharePoint Site Publish	.ccess Publishing Ru Lule ng Rule	12 HTTF	Publish Exchange Web Ciant Access
🥃 update Cer	чер Нер		Web Site Publishing Ru Non-Web Server Proto Access Rule	e al Publicing Role.	. HIT	Publick SharePoint Stres Publick SharePoint Stres Publick Web Stes Protectle Protocole
		F P 2	Alon access to a			Canfigure VoIP
		Last	Default rule	S Deny	йй нтт т III () т III () т III ()	Policy Editing Tasks

รูป ๗.๒

 ๓. ในช่อง Access rule name: ให้กรอกชื่อของ Access Rule โดยให้สื่อความหมายที่ สามารถเข้าใจได้ เช่น กรณีนี้เราต้องการสร้างกฎของการบล็อก URL เราก็ควรตั้งเป็น ดังนี้ Block_URL

	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: Block_URL	
11/1/1	To continue, click Next.	

รูป ๗.๓

๔. คลิกเลือกที่ O Deny หมายถึงไม่อนุญาต ตามรูป ๗.๔ จากนั้นให้กดปุ่ม Next

ew Access Rule Wizard	×
Rule Action Select how client requests for content from the specified destination are de if the conditions specified in the rule are met.	ealt with
Action to take when rule conditions are met:	
C Allow	
O Deny	
	- 100
< Back Next >	Cancel



๕. จะได้หน้าต่าง New Access Rule Wizard ปรากฏขึ้นมาในส่วนของ Protocols โดยที่ ช่อง This rule applies to: ให้เราเลือกเป็น All outbound traffic (หมายถึงช่องทาง การออกสู่เครือข่ายขาออกทั้งหมด) ตามรูป ๗.๕ จากนั้นคลิกที่ปุ่ม Next

v Access Rule Wizard	
Protocols Select the protocols this rule applies to.	\mathcal{H}
This rule applies to:	
All outbound traffic	
Protocols:	
	Add
	E dit
	Remove
	Ports
< Back	Next > Cancel

รูป ๗.๕

๖. จะได้หน้าต่าง Malware Inspection ตามรูป ๗.๖ ให้คลิกเลือก

 $oldsymbol{\Theta}$ Enable malware inspection for this rule

New Access Rule Wizard		×
Malware Inspection Select malware inspection settings.		H
• Enable malware inspection for this rule		
C Do not enable malware inspection for this	rule	
For malware inspection to be applie globally.	d to this rule, malwar	e inspection must be enabled
Help about malware inspection.		
	< Back	Next > Cancel

รูป ๗.๖

๗. เมื่อคลิกปุ่ม Next จะได้หน้าต่าง New Access Rule Wizard ปรากฏขึ้นมาภายใต้
 หน้าต่างเป็น Access Rule Sources ตามรูป ๗.๗

his rule applies to traffic	from these sources:		
			Add
			Edit
			Remove

รูป ๗.๗

 ๘. ให้คลิกปุ่ม Add... จะได้หน้าต่างย่อยชื่อ Add Network Entities ปรากฏขึ้นมาตาม รูป ๗.๘ ให้เลือก Internal ที่อยู่ภายใต้หมวด Networks





แล้วคลิก Add และ Close ตามลำดับจะได้ตามรูป ๗.๙

h <mark>is rule applies to traf</mark> fi	ic from these sources		
📥 Internal			Add
			Edit
			Remove
		-	

รูป ๗.๙

๙. จากนั้นตามรูป ๗.๙ ให้คลิกปุ่ม Next จะได้หน้าต่าง New Access Rule Wizard ภายใต้หน้าต่างคือ Access Rule Destination ตามรูป ๗.๑๐

Access Rule Wizard	
ccess Rule Destinations This rule will apply to traffic sent from the rule sourc in this page.	es to the destinations specified
nis rule applies to traffic sent to these destinations:	Add
	Edit
	Hemove.
<	Back Next > Cancel

รูป ๗.๑୦

๑๐.ให้คลิกปุ่ม Add... จะได้หน้าต่างย่อยชื่อ Add Network Entities ปรากฏขึ้นมาตามรูป ๗.๑๑ ให้เลือกหมวดหมู่ที่เราต้องการบล็อก ซึ่งเราจะบล็อกไว้ในหมวดไหนก็ได้ แต่ถ้าไม่ สื่อความหมาย ในอนาคตเราก็จะค้นหายาก



รูป ๗.๑๑

Access Rule Wizard	and the second	
Access Rule Destinations This rule will apply to traffic sent fro in this page.	om the rule sources to the	e destinations specified
This rule applies to traffic sent to these	destinations:	
Ceneral Entertainment		Add
		Edit
		Remove

๑๑.แล้วคลิก Add และ Close ตามลำดับ จะได้ตามรูป ๗.๑๒

รูป ๗.๑๒

๑๒.จากนั้นตามรูป ๗.๑๒ ให้คลิกปุ่ม Next จะได้หน้าต่าง New Access Rule Wizard ภายใต้หน้าต่างคือ User Sets ตามรูป ๗.๑๓ ซึ่งในช่อง This rule applies to requests from the following user sets: จะเป็น All Users (ถ้าไม่มีให้คลิก Add... แล้วเลือก All Users เข้าไป)

You can apply the rule to requests	s from all users. Or, you can limit access to
specific user sets.	
his rule applies to requests from the fo	ollowing user sets:
All Users	Add
	Edit
	Remove

รูป ๗.๑๓

๑๓.จากรูป ๗.๑๓ คลิกปุ่ม Next จะได้หน้าต่าง New Access Rule Wizard ภายใต้ หน้าต่างคือ Completing the New Access Rule Wizard ตามรูป ๗.๑๔

New Access Rule Wizard		×
411/	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: Block_URL Action: Allow Traffic: All outbound traffic Malware Inspection: Enabled	
981181	To close the wizard, click Finish.	
	< Back Finish Cancel	

รูป ๗.๑๔

ให้เราคลิกปุ่ม Finish เป็นอันเสร็จในส่วนของการตั้งกฎการบล็อกเว็บไซต์ แต่เราต้องมี การกำหนดว่าเว็บไซต์ใดบ้างที่ต้องการบล็อก

๑๔.เมื่อเราคลิกปุ่ม Finish ตามรูป ๗.๑๔ แล้วก็จะกลับมาที่หน้าต่าง Forefront TMG ตาม รูป ๗.๑๕ ให้เราคลิกขวาที่ General Entertainment เลือก Properties



รูป ๗.๑๕



๑๕.จะได้หน้าต่าง General Entertainment Properties ตามรูป ๗.๑๖

รูป ๗.๑๖

๑๖.ให้เลือกแท็บ URL Category Override จะปรากฏหน้าต่างตามรูป ๗.๑๗

General	URL Category Over	ride Cat	egory Que	ery		
URL ca overrid	tegories are predefin e its default.	ed. Add a	URL to a	different cate	egory to	
Filter b	y <mark>category:</mark>	Gen	eral Enter	tainment	<u>•</u>]
URL p	attern 🔺		Categor	у		I
	Add	Edit	in	Remove		
Pepert	Add	Edit	inn	Remove		
Report	Add	Edit	Service a	Remove s incorrectly o	ategorized	

รูป ๗.๑๗

๑๗.แล้วคลิก Add... จะได้หน้าต่างย่อย URL Category Override พิมพ์เว็บไซต์ที่ต้องการ จะบล็อกลงไปในช่องแรก เช่น www.facebook.com/* เป็นการบล็อกเว็บไซต์ Facebook โดยให้สังเกตด้วยว่าหลังเว็บไซต์จะต้องมีเครื่องหมาย /* ด้วย ตามรูป ๗.๑๘

oke category overnae	×
Override the default URL category for this URL pattern:	
www.facebook.com/*	
Example: www.contoso.com/*	
Move the URL pattern to this URL Category	/:]

รูป ๗.๑๘

๑๘.ส่วนในช่องของ Move the URL pattern to this URL Category: จะเป็นการเลือก หมวดหมู่ ซึ่งเราเลือกมาจาก General Entertainment ก็จะเป็นตัวที่เราเลือกไว้ จากนั้นคลิกปุ่ม OK จะได้ตามรูป ๗.๑๙

ter by category.	General Entertainment	
JRL pattern 🔺	Category	

รูป ๗.๑๙ ได้ชื่อเว็บไซต์ที่ต้องการบล็อก

๑๙.ซึ่งถ้าเราจะเพิ่มเว็บไซต์ที่ต้องการบล็อกอีก ให้ทำตามขั้นตอนที่ ๑๗ ลงไปอีก เสร็จแล้ว ให้คลิกปุ่ม Apply แล้วตามด้วย OK

หลังจากนั้นอย่าลืม ให้คลิกปุ่ม Apply -> Apply -> OK ตามลำดับ จะได้ตามรูป ๗.๒๐

Forefront ING						- 0
File Action Vew Help						
🕨 🤣 📶 🚺 🖬 🖄 🔤 😫	* X 🏵 🕃 🖲	2 i @	🗳 🔹 🚺 🗉 🔍	t		
Nicrosoft Forefront Threat Managemei Nicrosoft Forefront TMk (WLH488558MILH Coshboard Montaning Microsoft Selfcy With Access Policy With Access Policy Government	Forefro Threat M	ont Ianagement	t Gateway 2010		Fire	wall Policy Staudary
	All Firewall Poli	ax \				
	Search		P Examples			
Intrusion Prevention System Second Access Policy (VPM)	Name	Acton	Fratacols	From / Listener	To	Conditi +
A Networking	licy Group					
Loce & Reports	Block UKL	S Deny	💐 NI Outbound .	. 👍 Internal	🚔 Ganeral Entar	🏝 All U
iagi Loge 8.∓eparte Grupha Conter ∰ Tris bleshooting	Blocked Web Des	🚫 Deny	ЧТТН 😡 гаттн 🥡	🕁 Internel	Anonymizors Buland Crimmal Activit. Grambiand Histe/Discrimi Millegal Dr. gs Malaous Clascene/Test Pitshirg Pronography 	ALU .
	Alow access to a	. 🕜 Alow		Je Internel	Sternal	🎦 All U
	Defaill de	O Det to	🔛 Almañ:	🕂 Al Networks /.	🛧 Al Networks C	🥭 all i

รูป ๗.๒๐

บล็อกไฟล์ (Block File)

หากเราต้องการบล็อกไฟล์ในกลุ่มต่างๆ เช่น ไฟล์เพลง (Audio) เราก็สามารถใช้ TMG ๒๐๑๐ ทำการบล็อกได้ตามต้องการ โดยมีวิธีการดังนี้

๑. เรียกโปรแกรม Forefront Threat Management Gateway ๒๐๑๐ หรือ TMG
 ๒๐๑๐ โดยไปที่ Start -> All Programs ->Microsoft Forefront TMG->Forefront
 TMG Management จะได้ตามรูป ๗.๒๑

Horefront ING					<u>- 0 ×</u>
File Action Vew Help					
🗢 🖈 🖄 📅 📓 🖬 🗟 🤄) 🕑 🍶 🔄 🥸) 🗠 % 🗋			
Microsoft Fore-Foret Transed Manageme Greefront IMS (WL4484836541LH Saahboard Monitaring Weth Access Policy	All Firewall P	front Management Ga Volicy	teway 2010		Firewall Policy Standard
E Mai Foicy	Searthan	م	Examples		
Tobusion Prevention System	Order +	Name	Acton	Protoce +	Firewali Policy Tasks
📥 Networking	E Web Acces	s Policy Group			Publish Exchange Web
i System i Jupkate Center i Jupkate Center i Troubi⊴hooting	1	Blocked Web Des.	🚫 Deny	Шнтв Юнтв (Clent Access Clent Access Clent Moil Servers Levelder Moil Servers Cleicht Web Sites Cleicht Web Sites Cleicht Web Sites Cleicht Non-Web Server Protocole Cleic Create Access Rule Cleic Create Access Cleic Cleic Access Cleic Acces Cleic Access Cleic Access Cleic
	E 💽 🤉	Alon access to al	Salow 🤡	аттн 🔛 аттн 💭	Policy Editing Tasks
	💽 Last	Default <mark>ru</mark> e	🚫 Deny	💹 NE LI	Move Selected Rules Up Move Selected Rules Down
· ·					-
Donc					

รูป ๗.๒๑

 ๒. ทางช่องซ้ายมือ ให้คลิกขวาที่ Firewall Policy -> New ->คลิกเลือก Access Rule ตามรูป ๗.๒๒

LINEA OR AND THE OTHER							- 0
ile Action Vew Help							
• 🕪 🖄 📅 🚺 🖬 🔄 🤆) 🕑 🍯	10 13	2 😤 🧕				
Microsoft Foraffont Threat Managemer Goodford IMs (WUNHRBSESNILH Coahboard Montoring Proved Parlies		Forefr Threat N	ont 4anagement	Gateway 2010		fire	svall Policy Stauclary
Revellation	1	cwall Pol	licy				
C-Mail Fr		P Examples					_
Intrusion Import Tirewell Pa	licy		Acton	Fratacols	From / Listener	Та	Conciti +
Activari System Jose Jose Jodate Trouble Help		Ficheng Mail Sar Shar Fic Web Sit	je Web Clier I Acc ver Publishing Rul in I Stie Publishing E Aublishing Rule, i Sterver Protocol Ruley,	ess Puhistung Rule C Rule Puhishing Rule	julitansi Julitanci	General Enter. Anonymizors Dobret Conin dl A Livi. Gambing Hotz/Gsorini. Hileyd Du ys Hotz/Gsorini. Hileyd Du ys Hotshing Prohing Prohing Prohing	Allo Allo Mio
	Alow ac	xess to al.	🥝 Alow		.a. Internal	🕘 External	🏝 ni u
	Defa It	ede.	O Denv	🕅 All Traffic	the Al Networks (.	🔄 Al Networks (🤷 All I 🖉

รูป ๗.๒๒

๓. เมื่อคลิกเลือก Access Rule แล้วจะได้หน้าต่าง Welcome to the New Access Rule
 Wizard ขึ้นมา ในช่อง Access rule name: ให้กรอกชื่อของกฎ โดยให้สื่อความหมาย
 ที่เราเข้าใจ ในที่นี้เราต้องการบล็อกไฟล์ เราก็ควรตั้งเป็นชื่อ Block_File ตามรูป ๗.๒๓

New Access Rule Wizar	d.
	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: Block_File
	To continue, click Next.
/ // /////////////////////////////////	< Back Next > Cancel

รูป ๗.๒๓

๔. คลิกเลือกที่ O Deny หมายถึงไม่อนุญาต ตามรูป ๗.๒๔ จากนั้นให้คลิกปุ่ม Next



รูป ๗.๒๔

๕. จะได้หน้าต่าง New Access Rule Wizard ปรากฏขึ้นมา ภายใต้หน้าต่างคือ Protocols โดยที่ช่อง This rule applies to: ให้เราเลือกเป็น Selected Protocols ตามรูป ๗.๒๕

Select the protocols this rule appl	to.
his rule applies to:	
Selected protocols	
rotocols:	
	Ed
	Ren
	Por

รูป ๗.๒๕

 ๖. จากนั้นตามรูป ๗.๒๕ ให้คลิกปุ่ม Add... แล้วเลือก HTTP และ HTTPS ที่อยู่ภายใต้ หมวด Common Protocols เข้าไปตามรูป ๗.๒๖

New	• Edit Delete	
	Common Protocols DNS HTTPS HTTPS Server IMAPS Server IMAPS Server PING POP3 POP3 Server POP3S Server SMTP SMTP SMTP Server Telnet Telnet Server	
± [Infrastructure	

รูป ๗.๒๖

เมื่อคลิกปุ่ม Close ตามรูป ๗.๒๖ ก็จะได้ตามรูป ๗.๒๗

This rule applies to:	
Selected protocols	
Protocols:	
Щнттр	Add
ULHTTPS	Edit
	Remove
	Ports

รูป ๗.๒๗

๗. จากรูป ๗.๒๗ ให้คลิกปุ่ม Next จะได้หน้าต่าง New Access Rule Wizard ภายใต้ หน้าต่างคือ Access Rule Sources ตามรูป ๗.๒๘

w Access Rule Wizard		
Access Rule Sources This rule will apply to traffic origi	nating from the sources specified in this pa	age.
This rule applies to traffic from these	sources:	Add
		Edit
		Remove
	< Back Next >	Cancel

รูป ๗.๒๘

ให้คลิกปุ่ม Add... จะได้หน้าต่างย่อยชื่อ Add Network Entities ปรากฏขึ้นมาตามรูป ๗.๒๙ ให้เลือก Internal ที่อยู่ภายใต้หมวด Networks



รูป ๗.๒๙

หลังจากคลิกปุ่ม Close แล้วจะได้ตามรูป ๗.๓๐

Access Rule Wizard		
Access Rule Sources This rule will apply to traffic orig	ginating from the sources specified in this	page.
This rule applies to traffic from thes	e sources:	-
-linternal		Add
		Edit
		Remove
	< Back Next	> Cancel
	S DOGN I HEAT	

รูป ๗.๓๐

๘. จากนั้นตามรูป ๗.๓๐ ให้คลิกปุ่ม Next จะได้หน้าต่าง New Access Rule Wizard ภายใต้หน้าต่างคือ Access Rule Destinations ตามรูป ๗.๓๑

rule applies to traffic sent t	to these destinations:
	Add
	E dit
	Remov

รูป ๗.๓๑

ให้คลิกปุ่ม Add... จะได้หน้าต่างย่อยชื่อ Add Network Entities ปรากฏขึ้นมาตามรูป ๗.๓๒ ให้เราเลือก External ที่อยู่ภายใต้หมวด Networks

Networks External
External
- Internal
📥 Local Host
📥 Quarantined VPN Clients
VPN Clients
E 📴 Network Sets
Computers
🗄 🚞 Computer Sets
🗄 📴 Address Ranges
🚞 Subnets
🗄 🚞 Domain Name Sets
🗄 🚞 URL Categories
🗄 🚞 URL Category Sets
🗄 🧰 URL Sets

รูป ๗.๓๒

แล้วคลิกปุ่ม Add และคลิกปุ่ม Close ตามลำดับจะได้ตามรูป ๗.๓๓

This rule will apply to traffic sent from the rule	e sources to the destinations specified
in uns page.	51
nis rule applies to traffic sent to these destinatio	ns:
External	Add
	Edit
	Remove

รูป ๗.๓๓

๙. จากนั้นตามรูป ๗.๓๓ ให้คลิกปุ่ม Next จะได้หน้าต่าง New Access Rule Wizard ภายใต้หน้าต่างคือ User Sets ตามรูป ๗.๓๔ ซึ่งในช่อง This rule applies to requests from the following user sets: จะเป็น All Users (ถ้าไม่มีให้คลิก Add แล้วเลือก All Users เข้าไป)

		1923
Jser Sets You can apply the rule to requests specific user sets.	from all users. Or, you can limit access	to
his rule applies to requests from the fo	llowing user sets:	
All Users		Add
		E dit
		Remove

รูป ๗.๓๔

๑๐.จากรูป ๗.๓๔ คลิกปุ่ม Next จะได้หน้าต่าง New Access Rule Wizard ภายใต้ หน้าต่างคือ Completing the New Access Rule Wizard ตามรูป ๗.๓๕

2055R	Completing the New Assess Date
	Wizard
	You have successfully completed the New Access Rule Wizard. The new Access Rule will have the following configuration:
	Name: Block_File Action: Deny Traffic: HTTP,HTTPS Source: Internal
XXXXXI -	To close the wizard, click Finish.
	< Back Finish Cancel

รูป ๗.๓๕

ให้เราคลิกปุ่ม Finish คลิกปุ่ม Apply -> Apply -> OK ตามลำดับ เป็นอันเสร็จในส่วน ของการตั้งกฎการบล็อกไฟล์ แต่เราต้องมีการกำหนดว่าไฟล์ใดบ้างที่ต้องการบล็อก

๑๑.เมื่อเราคลิกปุ่ม Apply -> Apply -> OK ตามลำดับ ตามรูป ๗.๓๕ แล้ว ก็จะกลับมาที่ หน้าต่าง Forefront TMG ตามรูป ๗.๓๖ ให้เราคลิกขวาที่กฎที่เราสร้างคือ Block_File เลือก Properties

File Action Vew Help		_				
🔶 🌧 🖄 📅 🚺 🖬 🔹 🖛	<u></u>) 🕘 📓 🕒	🖑 😤 💆 🗊 🗉	6 e e		
Nkrosoft Forefront Threat Managemer Je	Fore Threat	front [:] Managem	ent Gateway 2010		, r	irewall Policy Standard
Hirewall -dicy	All firemail	Policy				
F-Mail Policy	searchin		P Examples			
Intrusion Prevention System Dometry Access Delicy (UDb)	Orter +	Name	Action	Protocols	Fram / Listener	To 🔺
System	₹ 1	Block URL	O Deny Propertes	Al Outbound	i 🛻 Interna 👍 Interna	Cone Cone
	e શ 3	Blocked W -	Capy Ungroup	нття Флана ачала	🐣 Internal	Anon Bothe Crimic
			Export Selected Import to Selected			Hate,
			Move Down Move Up Disable			Dbsc thian Porne
-1	⊐ ' ? ']4	ólinw acces	s to al 🔊 Allow	Diterre	🐣 înterna	 a =vter ▼

รูป ๗.๓๖

๑๒.จะได้หน้าต่าง Block_File Properties ตามรูป ๗.๓๗

Schedule	1	Content Types	1	Malware In	spection
General	Action	Protocols	From	To	Usen
Name	:	Block_File			
Description (optional):					
Туре:		Access Rule			
Evaluation orde	er:	Rule 2 of 5			
🔽 Enable					

รูป ๗.๓๗

๑๓.ไปที่แท็บ Content Types เลือก Selected Content Types (with this option selected, the rule is applicable only to HTTP and HTTPS traffic) ตามรูป ๗.๓๘ เพราะถ้าเลือก All Content types หมายถึงไฟล์ต่างๆ ในช่อง Content types ทั่งหมด ดังนั้นเราจึงเลือกที่ Selected Content Types (with this option selected, the rule is applicable only to HTTP and HTTPS traffic) แทน เพราะจะได้ตามที่เราต้องการ





๑๔.จากรูป ๗.๓๘ คลิกปุ่ม New... เพื่อสร้าง Content Type ใหม่ ตามรูป ๗.๓๙

	ype sec	
Name:	Audio 1	
Description:		
Specify the file a	' and MIME types included in the content	type set.
vailable types:		
.mp3	•	Add
elected types:		
.mp3		Remove
or HTTP reques	sts. incomina content is identified by MI	ME type, When
or HTTP reques	sts, incoming content is identified by MI n is missing, or when FTP is used, conta ion)	ME type. When ent is identified b
or HTTP reques IIME informatio le type (extens	sts, incoming content is identified by MI n is missing, or when FTP is used, conte sion).	ME type. When ent is identified b
or HTTP reque: IIME informatio ile type (extens	sts, incoming content is identified by MI n is missing, or when FTP is used, contr sion).	ME type. When ent is identified t

รูป ๗.๓๙

ตั้งชื่อตามต้องการ เช่น Name: เป็น Audio1 *(เนื่องจากใน Content Type มี Audio อยู่แล้ว แต่เราจะทดลองบล็อกไฟล์ .mp๓ เท่านั้น)* แล้วใส่นามสกุลใน Available Types เป็น เช่น .mp๓ แล้วคลิก Add -> OK ตามลำดับ

๑๕.จากนั้นเลือก Audio1 ใน Content Types ที่เราสร้างขึ้นมาตามรูป ๗.๔๐ คลิกปุ่ม Apply -> OK ตามลำดับ





๑๖.ตามรูป ๗.๔๑ เพื่อให้มีผลตามที่เราต้องการ ต้องคลิกปุ่ม Apply -> Apply -> OK ตามลำดับ เป็นอันเสร็จสิ้นการบล็อกไฟล์

Forefront ING					_ [0]
File Action Vew Help					
	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	· • • • • • • • • • • • • • • • • • • •	2 8 8		
Incosoft Poremont Inneet Management Imagement Imagement	efront			1	irewall Polic
Coshboard Three	at Management Ga	teway 2010			Stautan
Hrewell Policy		To save change	ec and update the configur	aton, click Apply.	
E-Mail Folk y					
Intrusion Prevention System All cwa Bengte Access Daicy (VPN)	ill Policy				
	م	Examples			
System	Name	Action	Protocola	From / Listener	To *
Update Center Web Acc	ess Policy Group				
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	slock_URL	S Jeny	Al Outbound	🚣 Interna	(Genz
	slock Hiz	S Jeny	UTTES	Interna	i ⇒:ter_
ดลิญปุ่ม Apply	Blocked Web Des	S Deny	<u>ер</u> нтте	-#- îniema	Arite 1
(risirių Apply)			HITTPS		Bothe
\ ตรงนี /					Gant
					Llega
					Maici
					A Phien
4 I I I					- mine
fonc					

รูป ๗.๔๑

บล็อกไอพีแอดเดรส (Block IP Address)

ผู้เขียนจะอธิบายหลักการให้ แต่เชื่อว่าในโรงเรียนคงไม่ได้ทำการบล็อกไอพีแอดเดรสกัน หรอก ซึ่งวิธีการมีดังนี้

๑. เรียกโปรแกรม Forefront Threat Management Gateway ๒๐๑๐ หรือ TMG
 ๒๐๑๐ โดยไปที่ Start -> All Programs ->Microsoft Forefront TMG->Forefront
 TMG Management จะได้ตามรูป ๗.๔๒

🕨 🅪 🖄 📅 🚺 🖬 🖄 🖾 u	₽ X ⊙ ⊙	ے 🕲 🖻 🍇 🕒	🍇 📴 🗉	E & 4		
Introsoft Forefront Threat Managemen Interfront IMs (WUN-RRBSESNILH Coshboard Monitoring	Fore	front Management Ga	teway 2010		r	irewall Policy Standard
Hrewall -clicy	All Firewall F	Policy				
F-Mai Polcy	search	P	Examples			
Intrusion Prevention System Demote Access Policy (VPM)	Order +	Name	Action	Protocols	Tram / I stener	To 🔺
Activating System Logs & Reports Jogs & Reports Jogs & Reports	Web Acces 1	s Policy Group Block URL Dlock_Tile	🚫 Deny	Al Outbound	👍 Interna	Cone
a constanty	C ? 3	Blocked Web Ces	🚫 Ceny	HTTPS HTTPS HTTPS	🐣 Interna	Anon Sothe Crimic Sant Hare, Elless Maini Obsc than
	∃ <mark>`8</mark>]4	álinu access to al	allow .	बगम् 💷		···

รูป ๗.๔๒

 ๒. ทางช่องซ้ายมือ ให้คลิกขวาที่ Firewall Policy -> New -> Access Rule ตามรูป ๗.๔๓



รูป ๗.๔๓

๓. ในช่อง Access rule name: ให้กรอกชื่อของ Access Rule ในที่นี้เราต้องการสร้างกฎ บล็อก IP Address ก็ตั้งเป็น Block_IP_Address ตามรูป ๗.๔๔

New Access Rule Wizard		×
411/ I	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: Block_IP_Address	
	To continue, click Next.	
	< Back Next > Canc	el

รูป ๗.๔๔

๙. คลิกเลือกที่ O Allow คืออนุญาตให้ใช้งานได้ (ถ้าไม่อนุญาตให้เลือก O Deny)
 ตามรูป ๗.๔๕ จากนั้นคลิกปุ่ม Next

Rule Action Select how client requests for content from if the conditions specified in the rule are m	n the specified de: et.	stination are dealt	with
Action to take when rule conditions are met:			
Allow			
C Deny			
	< Back	Next >	Cancel

รูป ๗.๔๕

๕. จะได้หน้าต่าง New Access Rule Wizard ปรากฏขึ้นมาในส่วนของ Protocols โดยที่ ช่อง This rule applies to: ให้เราเลือกเป็น Selected protocols ตามรูป ๗.๔๖

Protocols	100,000	
Select the protocols this rule applie	s to.	1
This rule applies to:		
Selected protocols		
Protocols:		
		Add
		E dit
		Remove
		0.722
		Ports
	<u> </u>	

รูป ๗.๔๖

๖. จากนั้นตามรูป ๗.๔๖ ให้คลิกปุ่ม Add... แล้วเลือก HTTP และ HTTPS ที่อยู่ภายใต้ หมวด Common Protocols ตามรูป ๗.๔๗



รูป ๗.๔๗

ನದ

เมื่อคลิกปุ่ม Close ตามรูป ๗.๔๗ ก็จะได้ตามรูป ๗.๔๘

Protocols Select the protocols this rule applies to.	 	ł
This rule applies to:		
Selected protocols		•
Protocols:		
HTTP		Add
M HIPS		Edit
		Remove
		Ports
	 	1



๗. จากรูป ๗.๔๘ ให้คลิกปุ่ม Next จะได้หน้าต่าง Malware Inspection ให้เลือก
 Enable malware inspection for the rule ตามรูป ๗.๔๙



รูป ๗.๔๙

จากรูป ๗.๔๙ ให้คลิกปุ่ม Next จะได้หน้าต่าง Access Rule Sources ตามรูป ๗.๕๐

Access Rule Wizaru				1.500
This rule will apply to traffic or	riginating from the	sources spec	ified in this pag	e. 🖒
				5.0
This rule applies to traffic from the	se sources:			
-				Add
				Eidit
				Remove
		< Back	Next >	Cance
		S DOCK	Next >	Lance



๙. ให้คลิกปุ่ม Add... จะได้หน้าต่างย่อยชื่อ Add Network Entities ปรากฏขึ้นมาตามรูป
 ๗.๕๑ ให้เลือก New -> Computer

26 DAVA 77 MA	
New - Edit Delete	
Network	
Network Set	
Computer	
Address Range	
Subnet s	
Computer Set	

รูป ๗.๕๑

๑๐.จะปรากฏหน้าต่าง ให้เรากำหนด IP Address ของเครื่องเพียงเครื่องเดียว หรือ IP Address เดียว ตามรูป ๗.๕๒ กำหนด Name: เป็น Admin Computer IP Address คือ ๑๙๒.๑๖๘.๑.๒๕๔ (แล้วแต่จะเลือกนะ)

omputer IP Address:	
192 . 168 . 1 . 25 ⁴	Browse
escription (optional):	

รูป ๗.๕๒

๑๑.และถ้าเราจะสร้างช่วงของ IP Address ที่จะอนุญาตให้เข้าใช้งานก็สามารถทำได้คือ จากรูป ๗.๕๐ คลิกปุ่ม Add จะปรากฏตามรูป ๗.๕๑ มา แต่ให้เราเลือกเป็น Address Range แทน ก็จะได้หน้าต่างเป็นตามรูป ๗.๕๓

Name:	Student_Group	
Specify the range of	FIP addresses:	
Start Address:	192 . 168 . 1 . 101	
End Address:	192 . 168 . 1 . 200	
Description (optional):		



เราอาจกำหนด	Name:	เป็น	Student_Group
Start	Address:	เป็น	තේම.බ්ටය්.බ.ටෙබ
End	Address:	เป็น	୦୦୭.ଇଟଡ.୭୭

๑๒.เมื่อคลิก OK แล้ว ก็จะปรากฏหน้าต่าง New Access Rule Wizard ภายใต้หน้าต่าง คือ Access Rule Sources ตามรูป ๗.๕๔

and the second sec			
		[Add
			Edit
			Remove

รูป ๗.๕๔

๑๓.จากรูป ๗.๕๔ ให้คลิก Add... จะปรากฏหน้าต่างย่อยตามรูป ๗.๕๕ ให้เราเลือก Admin ที่อยู่ภายใต้หมวด Computers และ Student_group ที่อยู่ภายใต้หมวด Address Ranges เข้าไป

ic thorn	endues:	
New 🔻	Edit Delete	
H 📄	Networks	
+ 🚞	Network Sets	
0	Computers	
	📇 admin	
🗄 🚞	Computer Sets	
0	Address Ranges	
	Anywhere (IPv6)	
	💐 Student_Group	
	Subnets	

๑๔.คลิก Add และ Close ตามลำดับจะได้ตามรูป ๗.๕๖

ccess Rule Sources		
This rule will apply to traffic originati	ng from the sources specified in th	iis page.
his rule applies to traffic from these sou	irces:	- Add
admin		Edit
		Remove
		1

รูป ๗.๕๖

๑๕.จากรูป ๗.๕๖ คลิกปุ่ม Next จะได้หน้าต่าง New Access Rule Wizard ภายใต้ หน้าต่างคือ Access Rule Destinations ตามรูป ๗.๕๗

This rule will apply to traffic in this page.	ent from the rule sources to the destinations specified
This rule applies to traffic sent to	hese destinations:
	Add
	Edit
	Remove

รูป ๗.๕๗

๑๖.ให้คลิกปุ่ม Add... จะได้หน้าต่างย่อยชื่อ Add Network Entities ปรากฏขึ้นมาตามรูป ๗.๕๘ ให้เลือก External ที่อยู่ภายใต้หมวด Networks

 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 	w + 1	Edit Delete
 External Internal Local Host Quarantined VPN Clients VPN Clients VPN Clients Network Sets Computers Computer Sets Address Ranges Subnets Domain Name Sets URL Categories URL Category Sets 		Networks
 Internal Local Host Quarantined VPN Clients VPN Clients VPN Clients Network Sets Computers Computer Sets Address Ranges Subnets Domain Name Sets URL Categories URL Category Sets 	(🜒 External
 Local Host Quarantined VPN Clients VPN Clients Network Sets Computers Computer Sets Address Ranges Subnets Domain Name Sets URL Categories URL Category Sets 	-	📥 Internal
 Quarantined VPN Clients VPN Clients Network Sets Computers Computer Sets Address Ranges Subnets Domain Name Sets URL Categories URL Category Sets 	-	👍 Local Host
 VPN Clients Network Sets Computers Computer Sets Address Ranges Subnets Domain Name Sets URL Categories URL Category Sets 	-	Quarantined VPN Clients
Network Sets Computers Computer Sets Address Ranges Subnets Domain Name Sets URL Categories URL Category Sets	- 6	VPN Clients
Computers Computer Sets Address Ranges Subnets Domain Name Sets URL Categories URL Category Sets		Network Sets
Computer Sets Address Ranges Subnets Domain Name Sets URL Categories URL Category Sets		Computers
Address Ranges Subnets Domain Name Sets URL Categories URL Category Sets		Computer Sets
Subnets Domain Name Sets URL Categories URL Category Sets		Address Ranges
 Domain Name Sets URL Categories URL Category Sets 	- :	Subnets
URL Categories URL Category Sets		Domain Name Sets
URL Category Sets		JRL Categories
		JRL Category Sets
URL Sets		JRL Sets

รูป ๗.๕๘

๑๗.เมื่อคลิกปุ่ม Close จะได้หน้าต่างตามรูป ๗.๕๙

in this page.	
is rule applies to traffic sent to these destinati	ns:
) External	Add
	Edit
	Remove

รูป ๗.๕๙

ด๘.หลังจากนั้นคลิกปุ่ม Next จะได้หน้าต่าง New Access Rule Wizard ภายใต้หน้าต่าง คือ User Sets ตามรูป ๗.๖๐

er Sets You can apply the rule to requisive specific user sets.	uests from all users. Or, you can limit access to	
s rule applies to requests from t	the following user sets:	
All Users	Ac	ld
	Ec	lit
	Re	nove
	10 A A A A A A A A A A A A A A A A A A A	

รูป ๗.๖๐

ซึ่งในช่อง This rule applies to requests from the following user sets: จะเป็น All Users (ถ้าไม่มีให้คลิก Add... แล้วเลือก All Users เข้าไป)

ด๙.จากรูป ๗.๖๐ ให้คลิก Next จะได้หน้าต่าง New Access Rule Wizard ภายใต้ หน้าต่างคือ Completing the New Access Rule Wizard ตามรูป ๗.๖๑

New Access Rule Wizard	×
4117	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: Block_IP_Address Action: Allow Traffic: HTTP,HTTPS Malware Inspection: Enabled
980881	To close the wizard, click Finish.
	< Back Finish Cancel

รูป ๗.๖๑

ให้เราคลิกปุ่ม Finish คลิก Apply -> Apply -> OK ตามลำดับ

๒๐.ซึ่งการบล็อกไอพีแอดเดรส แบบนี้ก็จะทำให้ IP Address ดังกล่าวสามารถใช้งาน อินเทอร์เน็ตได้ในช่วงไอพีที่กำหนด คือ ๑๙๒.๑๖๘.๑๐๑ ถึง ๑๙๒.๑๖๘.๑.๒๐๐ แต่ ถ้าเราไม่ต้องการให้ IP ช่วงดังกล่าวไม่สามารถใช้งานอินเทอร์เน็ตได้ สามารถทำได้โดย คลิกไม่อนุญาต ๋ Deny ตามรูป ๗.๔๕ หรือทำได้โดยการคลิกขวามี่ Firewall Policy ตรง Block_IP_Address แล้วเลือก Deny ตามรูป ๗.๖๒ ก็ได้

	~ @ @			v u				
Nicrosoft ForeFont Threat Managemer Index of ForeFont TMS (WUN-RRBSESNILH E Dashboard Montening	Forefront Threat Management Gateway 2010					Firewall Polic Staudar		
Hrewall Policy	All Firewall Policy							
F-Mail Policy	Searchin	P	Examples					
Intrusion Prevention System Demote Access Paicy (VPM)	Order +	Name	Action	Protocols	Tram / I stener	To 🔺		
iiii System iiiii Loge & k-eports iiiii Loge & Conter iiiii Trachik-handirg	₹ 1 ⊔ ₹ 2 ⊟ ₹ 3	Block URL Diock_JP_Address Block_File	S Deny Allow Allow Allow Allow Deny	Al Outbound	-Julinternal Studient_Group -Juliental	Conc Cotter Exter		
	L 💽 1	Blocked Web Des	S Deny	NUTTES	a∰a Interna	Anon Bohre Crimin Gamb Gamb Gamb Gamb Gamb Gamb Obsc Obsc Obsc		

รูป ๗.๖๒

จากนั้นคลิกปุ่ม Apply -> Apply -> OK ตามลำดับ

จากที่กล่าวถึงการบล็อกมา ๓ แบบ ถ้าเราต้องการลบกฎที่เราสร้างขึ้นมา ก็สามารถทำได้ โดยการคลิกขวาในกฎที่เราไม่ต้องการแล้วเลือก Delete เช่นตัวอย่างตามรูป ๗.๖๓

The second of the second secon	100						
Microsoft Forefront Threat Managemen Horefront IMS (WUN-RRBSESNILH Coshboard Monderine	Fore	front t Management Ga	teway 201	0	r	irewall Po Stand	lic) Ian
Rewell Policy	All Firewall	Policy					
😇 C-Mail Folicy	Search	0	Examples				
Thusion Prevention System	Order +	Name	Action	Protocols	Tran / Ustener	To	1
- Networking	= Web Acces	s Policy Group					
System	7 1	slock_ukt	🚫 Jeny	🔣 All Outbound .	🚣 Interna	(aena	e
Update Center Troubleshooting	n 📝 2	Block IP Address	S Deny	Properties	📕 admin 🌉 Student_Grou	🌒 Exte	
	⊟ 📝 3	Slock_SI-	S Seny	Deele	-&- Internal	🌒 =xle	4
				Сору	1.4.1.1		10000
	🖃 🏋 4	slocked Web Des	🚫 Jeny	Ungroup	🚢 Interna	nor	'n
				Export Seecled Import to Selected		Crimi	ii L
				Move Down Move Up		Cilege Main	e. i

รูป ๗.๖๓ ระบบจะถามยืนยันให้คลิกปุ่ม Yes ต่อด้วยคลิก Apply -> Apply -> OK ตามลำดับ

ซึ่งเมื่อเราทำการบริหารจัดการโดยการบล็อก

- ๑. บล็อก URL (Block URL)
- ๒. บล็อกไฟล์ (Block File)
- ๓. บล็อกไอพีแอดเดรส (Block IP Address)

แล้ว Firewall Policy ทั้ง ๓ อย่าง ต้องอยู่ลำดับก่อน Firewall Policy ที่เราตั้งเพื่อบริหารจัดการ เครือข่ายคอมพิวเตอร์ออกสู่อินเทอร์เน็ต (กฎชื่อ Allow Access to all web sites) ในบทที่ ๕ ด้วย ตามรูป ๗.๖๔

File Arlian View Help								
Microsoft Forefront Threat Managener Forefront Threat Managener Forefront Thus (NUD+RRES65\TLH Dashboard Monitoring	Fore Threa	front t Management Ga	Firewall Polic Standari					
Crewell Poicy	All Firewall Policy							
E-Mai Policy	Scordh	Q	Examples					
Intrusion Prevention System Remote Access Policy (VPN)	Crder 🔶	Name	Acton	Protocols	From / Listener	То		
	🖻 Web Acces	🖻 Web Access Policy Group						
E System Logs & Reports Collector To directioning	7 1	Bod: URL	🚫 Deny	Al Outbound	👍 Internal	Ceneral		
	U 🍸 2	Dock_P_Address	O Deny	TTTES	admin	le Externa		
	8 💽 3	Bock_Fle	O Deciy	भागम श्वागम 💭	-à-Internal	🍯 Estern.		
	⊟ <mark>(≬</mark>] 4	Allow access to al	. 🥝 Alon	атн Sum June L	👍 Internal	Stern:		
	💽 Loot	Default rule	🚫 Deny	👰 Al Traffic	🚖, Al Networks (🚖, Al Net		



เมื่อใช้เครื่องลูกข่ายเข้าสู่อินเทอร์เน็ตโดยทดลองเข้าไปยัง www.facebook.com จะพบว่า ไม่สามารถเข้าสู่เว็บไซต์ดังกล่าวได้ ตามรูป ๗.๖๕



