Joshua Lane IT419 11/11/2021

Use and Usefulness of Firewall Rules

Firewalls have more than just the purpose of keeping the bad guys out, they also keep legitimate users from deviating from their responsibilities. With the human layer being the weakest one, certain rules should be implemented to keep users from visiting risky sites/sites that have nothing to do with work or the use of that specific network. For instance, if you want clients outside your network to have access to your web server but deny access to other things such as file sharing and pinging; add rules to pfsense (your firewall) through the Graphic User Interface.

From the internal network (in our case from the Windows Web Server 2016), access your pfsense and log into the admin account via Chrome or some other browser. The goal is to use firewall rules in pfsense to limit access from the outside first, so we address the WAN (Wide Area Network) interface of the firewall rules. In the screenshot on the next page, I disabled a rule that allowed filesharing in the common file sharing ports in Windows (139 to 445) on the WAN interface of pfsense (the firewall). You can make a similar rule but make it a blocking rule and that will achieve the same result. Make sure it is at the top of the list of rules so that it is prioritized. The idea is to minimize privileges to the least amount needed to do the necessary tasks. This further secures the network. Go to Firewalls>Rules>Add rule. The protocol is TCP and applies to "any" client outside the private network, so that is the selection you make. Make sure to click "apply changes" after making each rule.

ARNING: The 'admin' account password is set to the default value. Change the password in the User Manager. irrewall / Rules / WAN te firewall rule configuration has been changed. te changes must be applied for them to take effect. Ioating WAN LAN WAN LAN VAN LAN V	he 'admin' account password is set to the default value. Change the password in the User Manager. / Rules / WAN	1.1/fi pf	REWALL	rules.php?if=ง SC Syst	wan em v Inte	erfaces -	Firew	rall - Services	✓ VPN ✓	Status 🕶	Diagnostic	:s ▼ Helį	•	
ire wall / Rules / WAN The forewall rule configuration has been changed. the changes must be applied for them to take effect.	/ Rule / WAN Image: Image	WA	RNING	3: The 'admin'	account passv	vord is set t	o the def	ault value. Change th	he password in the U	ser Manager.				
ere forewall rule configuration has been changed. te changes must be applied for them to take effect. VAN LAN Ules (Drag to Change Order) VISKAB IPV4 TCP * * 192.168.101.2 139.445 * none	twing the applied for them to take effect. WAN LAN APProtocol Source Port Destination Port Gateway Queue Schedule Description Actions Ports KB IPv4 TCP * * 192.168.101.2 139 · 445 * none Port Gateway Queue Schedule Description Actions Port Gateway Queue Schedule Description Actions Port Gateway Queue Schedule Description Actions Port 192.168.101.2 139 · 445 * none Port 192.168.101.2 80 (HTTP) * none Port 192.168.101.2 80 (HTTP) * none Port 192.168.101.1 443 (HTTPS) * none Port 192.168.101.2 80 (HTTP) * none Port 192.168.101.1 443 (HTTPS) * none Port 192.168.101.2 80 (HTTP) * none Port 192.168.101.1 443 (HTTPS)	Fi	rewa	all / Rule	s/WAN									≢ Ш 🗉 (
MAN LAN States Protocol Source Port Destination Port Gateway Queue Schedule Description Actions ✓ 0/15 KdB IPV4 TCP * * 192.168.101.2 139.445 * none ④ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	I'must be applied for them to take effect. WAN LAN Arg to Change Order) Tataes Protocol Source Port Destination Port Gateway Queue Schedule Description Actions 1/15 KIB IPv4 TCP * * 192.168.101.2 139 · 445 * none 0/0 B IPv4 TCP * * 192.168.101.2 80 (HTTP) * none 0/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * * * * 192.168.101.1 443 (HTTPS) * none 0/0 B IPv4 TCP * * * * * * * * * * * * * * * * * * *	Th	e firew:	all rule config	uration has bee	en changed.								
WAN LN States Protocol Source Port Gateway Queue Schedule Description Actions ✓ 0/15 Ki8 IPV4 TCP * * 192.168.101.2 139.445 * none	WAN LAN and to Cherry and to	Th	e chan	ges must be a	applied for ther	n to take eff	ect.							Apply Changes
Ulles (Drag to Charge Order) States Protocol Source Port Destination Port Gateway Queu Schedule Description Actions ✓ 0/15 KB IPv4 TCP * * 192.168.101.2 139 · 445 * none ✓ 0/0 B IPv4 TCP * * 192.168.101.2 80 (HTTP) * none ✓ 0/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none ✓ 0/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none ✓ 10/0 B IPv4 TCP * * * 192.168.101.1 443 (HTTPS) * none ✓ 10/0 B IPv4 TCP * * * 192.168.101.1 443 (HTTPS) * none ✓ 10/0 B IPv4 TCP * * * 192.168.101.1 443 (HTTPS) * none ✓ 10/0 B IPv4 TCP * * * 192.168.101.1 443 (HTTPS) * none ✓ 10/0 B IPv4 TCP * * * 192.168.101.1 443 (HTTPS) * none ✓ 10/0 B IPv4 TCP * * * 192.168.101.1 443 (HTTPS) * none ✓ 10/0 B IPv4 TCP * * * 192.168.101.1 443 (HTTPS) * none ✓ 10/0 B IPv4 TCP * * * 192.168.101.1 443 (HTTPS) * none ✓ 10/0 B IPv4 TCP * * * * 192.168.101.1 443 (HTTPS) * none ✓ 10/0 B IPv4 TCP * * * * 192.168.101.1 443 (HTTPS) * none ✓ 10/0 B IPv4 TCP * * * * * * * * * * * * * * * * * * *	age to Charry Part Gateway Queu Schedule Description Actions 0/15 KiB IPv4 TCP * * 192.168.101.2 139 - 445 * none ●	Fl	pating	WAN	LAN									
State Protool Source Port Destination Porton Gateway Queue Schedue Description Actional ● 0/15 KK8 IPV4 TCP 4 12 120.168.101.0 130.445 4 none - ●	Attes Pordol Source Port Destination Porton Schedule Description Actional 175 K80 IPV4 TCP * * 192-168.101.2 199-445 * none * * #<	Ru	ıles (I	Drag to Ch	ange Order)								
✓ 0/15 Ki8 IPv4 TCP * 192.168.101.2 139-445 * none .	1/75 K08 IPv4 TCP * 192.168.101.2 139-445 * none			States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 0 / 0 B IPv4 TCP * 192.168.101.2 80 (HTTP) * none	1/0 B IPv4 TCP * 192.168.101.2 80 (HTTP) * none		×	0 /15 KiB	IPv4 TCP	*	*	192.168.101.2	139 - 445	*	none			₺∥ ⊡⊡
✓ 0/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none ↓ ♪ ↓ ○ □ ↑ Add ↓ Add □ Delete □ Sove + Separate	J/0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none		~	0 /0 B	IPv4 TCP	*	*	192.168.101.2	80 (HTTP)	*	none			₺₡₽०₸
1 Add 1 Add 1 Delete Sove + Separat	1 Add 1 Add 🛅 Delete 🕞 Save + Separator		~	0 /0 B	IPv4 TCP	*	*	192.168.101.1	443 (HTTPS)	*	none			℄ℐ⅊Ω面
												1 Add	Add 🔟 Delete	Save + Separ
		6												

						Jo	shua Lane
						1.	1/11/2021
🕌 Windows Server [Running] - Oracle VM	VirtualBox					1. _	
ile Machine View Input Devices H	elp						
< +							^
https://192.168.101.1/firewall_rules_edit.php?id	1=2						
	Set this option to disable this	rule without removing it from the l	ist.				
Interface	WAN		~				
	Choose the interface from wh	iich packets must come to match t	his rule.				
Address Family	IPv4 Select the Internet Protocol w	preion this rule applies to	~				
Destand		ersion this rule applies to.					
Protocol	Choose which IP protocol this	rule should match.	~				
Source							
Source	Invert match	any	~	So	urce Address	/	~
	Display Advanced	connection is typically random and	almost pover equal to th	a doctin	tion port. In most cases this	a actting must remain at	
	its default value, any .	connection is typically random and	annost never equal to a	ie destina		s setting must remain at	
Destination							
Destination	 Invert match 	Single host or alias	~	19	2.168.101.1	/	~
Destination Port Range	HTTPS (443)		HTTPS (443) 🗸				
	From	Custom T	D	Cus	tom		
	Specify the destination port o	r port range for this rule. The "To" f	ield may be left empty if	only filter	ing a single port.		_
Extra Options							
Log	 Log packets that are hand Hint: the firewall has limited left 	led by this rule ocal log space. Don't turn on loggin	a for everything. If doing	a lot of l	oqqinq, consider using a rer	note svslog server (see	
	the Status: System Logs: Sett	ings page).	J		- 3 3 3		
Description							
	A description may be entered log.	here for administrative reference.	A maximum of 52 chara	cters will	be used in the ruleset and d	isplayed in the firewall	
ver Manager							
	Sector Display Advanced						
Attride section.							
Tracking ID	1636492030						
		1004/04040/0/ IB+I)			Activate V	Vindows	×
					Go to Sotto		Right Ctrl 📰

Above we address what clients can have access to. We allow them to access the webserver through port 443 (a common HTTPS port) and we do the same with port 80 (for HTTP). The source will be "any" (as in any client) etc. Another good rule-of-thumb is to disable anything allowing pinging through the firewall. This helps stop unwanted traffic bogging down your network. The protocol to make a rule for blocking this is ICMP. I had a passing rule, so I simply disabled it, and pinging was unsuccessful afterwards. This is shown on the next page in two screenshots.

ARNING: The 'admin' account password is set to the default value. Change the password in the User Manager. ARNING: The 'admin' account password is set to the default value. Change the password in the User Manager. irrewall / Rules / WAN	WARNING: The 'admin' account p	assword is set to the defa	ult value. Change the p	assword in the User Mai	Diagnostics The pager	leip +	
ARRNING: The 'admin' account password is set to the default value. Change the password in the User Manager.	WARNING: The 'admin' account p	assword is set to the defa	ult value. Change the p	assword in the User Ma	nager		
iriewall / Rules / WAN the forewall rule configuration has been changed. the changes must be applied for them to take effect. WAN LAN Ules (Drag to Charge Order)	Firewall / Rules / WA	N			lagel.		
he frewall rule configuration has been changed. Loating WAN LAN Ules (Drag to Change Order) ✓ 2/840 B IPV4 TCP * * 102168.101.2 139 -445 * none		AIN .				幸 區	III
Interval Consignation has been changed. Image: Consignation has been changed. Ioating WAN LAN ules (Drag to Change Order) Image: Change of the model of the							
MAN LAN allosting Order) States Protocol Source Pot Destination Port Gateway Queue Schedule Description Actions 2 2/840 B IPV4 ICMP * * * none <td< td=""><td>The firewall rule configuration has The changes must be applied for</td><td>been changed. them to take effect.</td><td></td><td></td><td></td><td>Apply C</td><td>Changes</td></td<>	The firewall rule configuration has The changes must be applied for	been changed. them to take effect.				Apply C	Changes
Notice of the construction Construction Port Gateway Quoue Schedule Description Actions 2/840 B	Floating WAN LAN						
ulles (Drag to Change Order) States Protocol Source Port Destination Port Gateway Queue Schedule Description Actions ✓ 2 /840 B IPV4 ICMP * * * * none	Floating Wat Little						
Caters Protect Caters Protect Caters Protect Caters Caters <th>Rules (Drag to Change Or</th> <th>der) Source Port</th> <th>Destination</th> <th>Port Gat</th> <th>away Quaya Schedule</th> <th>Description Actions</th> <th>-</th>	Rules (Drag to Change Or	der) Source Port	Destination	Port Gat	away Quaya Schedule	Description Actions	-
anx 192168.101.2 139 - 445 none ●	2 /840 B IPv4 ICt	//P * *	*	* *	none	🕹 🖉 🖓 🖓 🖓	2 💼
✓ 0 / 0 B IPv4 TCP * 192.168.101.2 80 (HTTP) * none </td <td>any 0 /0 B IPv4 TC</td> <td>P * *</td> <td>192.168.101.2</td> <td>139 - 445 *</td> <td>none</td> <td></td> <td></td>	any 0 /0 B IPv4 TC	P * *	192.168.101.2	139 - 445 *	none		
✓ 0 /0 B IPv4 TCP * * 192.168.101.1 443 (HTTPS) * none ↓ Add ① Delete □ Save + Separator	○ 0/0B IPv4 TC	P * *	192.168.101.2	80 (HTTP) *	none	€ ₽ <i>₽</i> ₽©©	
1 Add 1 Add 1 Save + Separator	0 /0 B IPv4 TC	p * *	192.168.101.1	443 (HTTPS) *	none	₺∥©©	
•					1 Add	🖡 Add 🛅 Delete 🕞 Save 🕂	Separator
	0						

Next, you want to take care of your clients in your private network. You can blacklist (prohibit access to) certain sites, but professionals recommend whitelisting (allowing access to) to save time and effort. There will always be new sites for clients to abuse, access, etc. For this reason, it takes fewer rules to allow access to the necessary websites. For the following example, however, I will simply show how to prohibit access to certain sites/create a loopback feature that keeps clients from misusing the network. Say, for instance, I wanted to block access to girlsgeekout.org. First, I want to find the IP address of the website, I do this by using "nslookup girlsgeekout.org" in a command prompt window as shown below.



Now we go to the LAN interface of pfsense, and we add a rule blocking that specific IP address

(216.92.30.104) as a destination. The source is set to "any", and the port is set to 80 since the

website is HTTP. This rule is shown on the next page.

Joshua Lane IT419 11/11/2021

🕌 Windows S	Gerver [Running] - Oracle VM	I VirtualBox —						
File Machine	View Input Devices H	Help						
× +			Â					
https://192.168.	101.1/firewall_rules_edit.php?if	if=lan&after=-1						
	Interface	LAN V						
		Choose the interface from which packets must come to match this rule.						
	Address Family	IPv4 V						
		Select the Internet Protocol version this rule applies to.						
	Protocol	TCP v						
		Choose which IP protocol this rule should match.						
	Source							
	Source	Invert match						
		Cisplay Advanced						
		The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at						
		its default value, any .						
	Destination							
	Destination	□ Invert match Single host or alias						
	Destination Port Range	HTTP (80) V						
		From Custom To Custom						
		Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.						
	Extra Options							
	Log	□ Log packets that are handled by this rule						
	Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see							
	the Status: System Logs: Settings page).							
	Description							
		A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall						
		iog.						
	Advanced Options	Ciplay Advanced						
		Save						
		pfSense is developed and maintained by Netgate. © ESF 2004 - 2021 View license.						
~		Activate Windows	~ ~					
		Go to Soliding and Solid and So	👌 🛃 Right Ctrl 🔡					

Hit save and apply changes (same as the rest of the rules).

Next, we look at blocking access to a popular site such as youtube.com. Here we want to use the domain override feature to simply show a "This site can't be reached" message to the client. First, you select "Services" from the pfsense GUI, then select DNS Resolver>General Settings>add domain override. The screenshot on the next page shows the domain override location.

Joshua Lane IT419 11/11/2021

Inter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the esolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'nas.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or somesite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records.	Host	Parent domain of host	IP to return for host	Description	Actions	
Domain Overrides Description Actions Demain for which the resolver's standard DNS lookup process should be overridden and a different (non-standard) lookup server should be queried instead. Non-standard, nvalid' and local domains, and subdomains, can also be entered, such as 'test', 'nas.home.arpa', 'mycompany.localdomain,' '1.168.192.in-addr.arpa', or 'somesite.com'. The IP address is reated as the authoritative lookup server for the domain (including all of its subdomains), and other lookup servers will not be queried. If there are multiple authoritative DNS servers valiable for a domain then make a separate entry for each, using the same domain name.	inter any indiv esolver. Stand somesite.com	idual hosts for which the resolver's standard lard and also non-standard names and paren '. Any lookup attempt for the host will autom	DNS lookup process should be overridden and a spe t domains can be entered, such as 'test', 'nas.home. atically return the given IP address, and the usual loc	ecific IPv4 or IPv6 address should a arpa', 'mycompany.localdomain', '1.1 okup server for the domain will not b	utomatically be returned by the 168.192.in-addr.arpa', or be queried for the host's records. Add	
Inter any domains for which the resolver's standard DNS lookup process should be overridden and a different (non-standard) lookup server should be queried instead. Non-standard, invalid' and local domains, and subdomains, can also be entered, such as 'test', 'nas.home.arpa', 'mycompany.localdomain, '1.168.192.in-addr.arpa', or 'somesite.com'. The IP address is reated as the authoritative lookup server for the domain (including all of its subdomains), and other lookup servers will not be queried. If there are multiple authoritative DNS servers wailable for a domain then make a separate entry for each, using the same domain name. Add	Domain O)verrides				
• Add	Domain	Lookup Server IP Address	\$	Description	Actions	
	Domain nter any doma nvalid' and loc reated as the a vailable for a	Lookup Server IP Address ains for which the resolver's standard DNS Ic cal domains, and aubdomains, can also be er authoritative lookup server for the domain (ir domain then make a separate entry for each	s where the owner of the owner of the owner of the owner of the owner owner owner owner owner owner owner owner where owner own where owner own owner owner own	Description non-standard) lookup server should scaldomain, '1.168.192.in-addr.arpa vers will not be queried. If there are	Actions d be queried instead. Non-standard, d, or 'somesite.com'. The IP address is multiple authoritative DNS servers	
	Domain Inter any doma nvalid' and loc reated as the a vailable for a	Lookup Server IP Address ains for which the resolver's standard DNS lo cal domains, and subdomains, can also be er authoritative lookup server for the domain (ir domain then make a separate entry for each	wokup process should be overridden and a different (tered, such as 'test', 'nas.home.arpa', 'mycompany.lc ncluding all of its subdomains), and other lookup ser using the same domain name.	Description non-standard) lookup server should ocaldomain, '1.168.192.in-addr.arpa vers will not be queried. If there are	Actions the queried instead. Non-standard, i', or 'somesite.com'. The IP address is multiple authoritative DNS servers Add	
	Domain nter any dom: nvalid' and loc reated as the a vailable for a 3	Lookup Server IP Address ains for which the resolver's standard DNS lo cal domains, and subdomains, can also be er authoritative lookup server for the domain (if domain then make a separate entry for each	s okup process should be overridden and a different (ntered, auch as 'test', 'nas.home.arpa', 'mycompany.lc ncluding all of its subdomains), and other lookup ser , using the same domain name. Its developed and maintained by Netgate. © ESF 200	Description non-standard) lookup server should ocaldomain, '1.168.192.in-addr.arpa vers will not be queried. If there are	Actions the queried instead. Non-standard, the or 'somesite.com'. The IP address is multiple authoritative DNS servers Add Add Add	

Next, set the domain entry to youtube.com, the IP address to 127.0.0.1, hit save and apply

changes. This is shown below.

	- Interfaces - Firewall - Services - VPN - Status - Diagnostics - Help -	
WARNING: The 'admin' acco	ount password is set to the default value. Change the password in the User Manager.	
Services / DNS R	esolver / General Settings / Edit Domain Override 🛛 C 💿 🛱 🔟 🗐 😧	
Domains to Override	with Custom Lookup Servers	1
Domain	youtube.com Domain whose lookups will be directed to a user-specified DNS lookup server.	
IP Address	127.0.0.1 IPv4 or IPv6 address of the authoritative DNS server for this domain. e.g.: 192.168.100.100 To use a non-default port for communication, append an @' with the port number.	
TLS Queries	 Use SSL/TLS for DNS Queries forwarded to this server When set, queries to all DNS servers for this domain will be sent using SSL/TLS on the default port of 853. 	
TLS Hostname	An optional TLS hostname used to verify the server certificate when performing TLS Queries.	
Description	block youtube by routing to loop back A description may be entered here for administrative reference (not parsed).	
	This page is used to specify domains for which the resolver's standard DNS lookup process will be overridden, and the resolver will query a different (non-standard) lookup server instead. It is possible to enter 'non-standard', 'invalid' and 'local' domains such as 'test', 'nas.home.arpa', 'mycompany.localdomain', or '1.168.192.in-addr.arpa', as well as usual publicly resolvable domains such as 'test', 'ndo', or 'google.co.uk'. The IP address entered will be treated as the IP address of an authoritative lookup server for the domain (including all of its subdomains), and other lookup servers will not be queried.	
	Save	

Joshua Lane IT419 11/11/2021 Once this is implemented, you can test it by trying to access youtube.com from inside the

network. This is shown below.

🗊 pfSense.home.arpa - Firewall: Rui 🗙 📀 www.youtube.com 🗙 🕇		, - • ×	
- → C () youtube.com		* 🔮 🗄	
			Smillia.
	Γ ¹		
	This site can't be reached		
	Check if there is a typo in www.youtube.com.		
	If spelling is correct, try running Windows Network Diagnostics.		
	DNS_PROBE_FINISHED_INXDOMAIN		
	Reload		
# P @ 🤌 🛤 💺 💽		~ 도 4.8 ,	1:24 PM

In these ways, you can block access to risky sites or sites you simply do not want your clients

accessing. This provides a more productive and safe work environment.