Руководство по pfSense 2.0. Часть 7

Часть 7 Трансляция сетевых адресов (NAT)

оглавление

В наиболее общем смысле, NAT (Network Address Translation) позволяет подключить несколько компьютеров к сети Интернет, используя единственный внешний IP адрес. pfSense реализуют данный функционал в базовом развёртывании, а кроме того имеет возможности более расширенного и сложного конфигурирования NAT необходимого в сетях с несколькими публичными IP адресами. NAT настраивается в двух направлениях - входящем и исходящем. Исходящий NAT определяет работу с трафиком исходящим из сети в сеть Интернет. Входящий NAT работает с трафиком входящим в вашу сеть из Интернет. Наиболее распространённый тип входящего NAT, и один из наиболее знакомых, называется форвардингом портов.

7.1. Конфигурация NAT по умолчанию.

В данном разделе описывается конфигурация NAT используемая в pfSense по умолчанию. Чаще всего подходящая конфигурация NAT генерируется автоматически. В некоторых средах вы можете захотеть изменить эту конфигурацию и pfSense позволяет сделать это в полном объёме посредством Web-интерфейса. Это выгодно отличает pfSense от прочих брандмауэров проекта Open Source.

7.1.1. Конфигурация исходящего NAT по умолчанию.

Конфигурация NAT по умолчанию, используемая в pfSense с интерфейсами LAN и WAN автоматически транслирует интернет трафик в WAN IP адреса. Когда настроены несколько WAN интерфейсов, трафик покидающий любой WAN интерфейс автоматически транслируется в адрес используемого WAN интерфейса. Статический порт автоматически настраивается для трафика IKE (часть IPSec) и SIP(VoIP). Статический порт более подробно будет рассмотрен в разделе 7.6, "Исходящий NAT".

7.1.2. Конфигурация по умолчанию для входящего NAT

По умолчанию, никакой трафик из Интернет внутрь не допускается. Если вам

www.thin.kiev.ua - Руководство по pfSense 2.0. Часть 7 Трансляция сетевых адресов (NAT)

Автор: 02.04.12 11:38 - Последнее обновление 02.04.12 14:42

требуется позволить трафику инициированному в Интернет попадать в вашу внутреннюю сеть, вы должны настроить форвардинг портов или 1:1 NAT. Эти возможности мы рассмотрим в следующих разделах.

7.2. Порт форвардинг (Port Forwards)

Порт-форвардинг (или если угодно перенаправление портов) позволяет вам открыть специфичный порт, диапазон портов или протокол для приватных адресов устройств в вашей сети. Название "port forward" было выбрано после бесчисленного числа жалоб. Однако этот термин не совсем верен, поскольку вы можете перенаправить GRE и ESP протоколы в дополнение к портам TCP и UDP. Наиболее часто это используется при хостинге серверов или использовании приложений, которые требуют входящего соединения из Интернет.

7.2.1. Риски использования форвардинга портов

В конфигурации по умолчанию, pfSense не позволяет любой трафик инициированный в Интернет. Это обеспечивает защиту от любого сканирования системы при поисках целей атаки. При включении форвардинга портов, pfSense позволяет любой трафик соответствующий правилу брандмауэра. Система не разбирается в типе пропускаемого пакета. Если он удовлетворяет правилу - он разрешён. В данном случае, вам придётся полагаться на систему безопасности конечного хоста.

7.2.2. Перенаправление портов и локальные сервисы

Порт-форвардинг может быть запущен относительно любой службы работающей локально на брандмауэре, например web интерфейсу, SSH и прочим запущенным сервисам. Например, это означает, что если вы позволили удалённый доступ с WAN используя HTTPS на порт TCP 443, если вы добавили перенаправление порта на WAN для TCP 443, то стандартный доступ к web интерфейсу работать не будет. Это не повлияет на доступ к другим интерфейсам.

7.2.3. Добавление перенаправления портов

Перенаправление портов управляется в меню Firewall -> NAT, на закладке Port Forward. Правила на этом экране управляются аналогично правилам брандмауэра (смотрите раздел 6.2. "Введение в экран правила брандмауэра").

Для начала добавления перенаправления порта, нажмите кнопку [+] в верхней или нижней части списка, как показано на рисунке 7.1 "Добавление перенаправления порта".

rewal	: NAT:	Port Forward				
art Forwa	rd 1:1	Dutbound				1
	Proto	Ext. port range	NAT IP	Int. port range	Description	

Автор: 02.04.12 11:38 - Последнее обновление 02.04.12 14:42

Рисунок 7.1 "Добавление перенаправления порта"

Теперь, вы должны увидеть экран редактирования перенаправления порта, показанный на рисунке 7.2. "Пример перенаправления порта", с параметрами выбранными по умолчанию. Во-первых, выберите интерфейс (Interface), на котором будет находится перенаправляемый порт. В большинстве случаев это будет WAN, однако, если у вас есть интерфейс ОРТ, или если используется локальное перенаправление, это может быть другой интерфейс. Внешний адрес (External Address), в большинстве случаев, должен быть установлен в адрес интерфейса или доступный виртуальный IP (смотрите раздел 6.8. "Виртуальные IP"), если это локальное перенаправление. Протокол (Protocol) и диапазон внешних портов (External Port Range) должны быть установлены в соответствии с перенаправляемой службой. Например, для перенаправления VNC1 в должны установить протокол в значение TCP, а диапазон внешних портов в значение 5900. (Поскольку это стандартно перенаправляемый порт, он так же доступен в списке выпадающего меню выбираемых портов.) NAT IP должен быть установлен в локальный IP адрес, по которому перенаправляется данный порт, а локальный порт (Local Port) - в значение начала диапазона перенаправляемых портов. Если вы перенаправляете диапазон портов, скажем 19000-19100, вам необходимо указать локальную начальную точку, поскольку порты должны соответствовать по принципу "один к одному". Это поле позволяет открывать порт на внешней стороне, отличающийся от того на котором слушает внутренний хост, например, внешний порт 8888 может перенаправляться на локальный порт 80 внутреннего HTTP сервера. Поле Описание (Description), как и в других местах pfSense, доступно для внесение краткой информации о назначении создания перенаправления. Если вы не используете отказоустойчивый кластер CARP, пропустите опцию XML-RPC Sync. Если это не так, этот флаг будет препятствовать синхронизации данного правила с другими членами отказоустойчивого кластера (смотрите главу 20, "Избыточность брандмауэра/ Высокая доступность"), что обычно не желательно.

Последняя опция является очень важной. Если вы отметите Auto-add a firewall rule to permit traffic through this NAT rule (Добавлять правило брандмауэра автоматически, чтобы разрешить трафик через это правило NAT), то правило брандмауэра, для вас, будет создано автоматически, и это позволит трафику добраться до порта назначения. Как правило, лучше оставить эту опцию отмеченной, а позже, при необходимости, изменить правило брандмауэра.

Нажмите кнопку Save (Сохранить), по завершению конфигурирования, а затем Apply Changes (Применить изменения). На рисунке 7.2 "Пример перенаправления порта", показан пример экрана редактирования перенаправления порта, заполненный настройками для перенаправления VNC в локальную систему.

www.thin.kiev.ua - Руководство по pfSense 2.0. Часть 7 Трансляция сетевых адресов (NAT)

Автор: 02.04.12 11:38 - Последнее обновление 02.04.12 14:42

Firewall: NAT: Por	t Forward: Edit							
Interface	WAN + Choose which interface this rule	applies to,						
External address	Interface address • If you want this rule to apply to need to define Virtual IP address	another IP address than the address of the interface chose as first). Note if you are redirecting connections on the UM	n above, select it here (you Liselect the "any" cotion.					
Protocol	TCP Choose which IP protocol this ru Hint: in most cases, you should:	e should match. pecify T2P here.						
External port range	from: VNC to: VNC	* * * * * * * *						
NAT IP	Specify the port or port range of Hint: you can leave the ito held	n the firewall's external address for this mapping. empty if you only want to map a single port						
Local port	Enter the internal IP address of e.g. 192.168.1.12	the server on which you want to map the ports.						
	Specify the port on the machine the range (the end port will be o Hint: this is usually identical to the	with the IP address entered above. In case of a port range alculated automatically). e "from" port above	specify the beginning port of					
Description	VNC to Sales Server You may enter a description her	e for your reference (not parsed).						
NO MILLION, SYITE	HINT: This prevents the rule	from automatically syncing to other CARP members lie to permit traffic through this NAT rule						
Port Forward 11	Ostbound	Ba FlinQitti an/	переналира	RIGCHUSPACEPSC HA	риюунун тёрден	attprateoriks	емых портов, и	
E Proto WAN TCP	5900 (VNC)	Int. pert range D 10.0.20.5 \$900 (1%C) \$	escription					
Interface	IAT: Port Forwa	rd: Edit			المالية المركلة للمحملة مراكبته فرحمتهم	רדוטיייעי ווייע	، محمد <u>1</u> ام دالم درم کر جمای با از سر	
	Choose whit Hint: in most) h interface this rule applies to. : cases, you'll want to use WAN here.						
External addre	ess any If you want need to defi	this rule to apply to another IP address than the a ne Virtual IP addresses first). Note if you are redir	iddress of the interface chosen a ecting connections on the LAN, s					
Protocol	TCP Choose whit	P protocol this rule should match.						
External port r	Hint: in most	Cases, you should specify <i>TCP</i> here.						
	to: HTT Specify the	P The firewall's external address	ss for this mapping.					
NAT IP	Hint: you ca	n leave the 10 Yield empty if you only want to map	a single port					
Local port	Enter the in e.g. 192.16	ernal IP address of the server on which you want 8.1.12	to map the ports.					
	Specify the the range (t Hint: this is	ort on the machine with the IP address entered a he end port will be calulated automatically). usually identical to the 'from' port above	bove. In case of a port range, s					
Description	Redirect H You may en	ITTP to Squid er a description here for your reference (not pars	ed).					
No XMLRPC Syni		orments the rule from automatically synch	a to other CARP members.					
Firewall: NAT:	: 1:1: Edit		John Law		والمحافظة المحافية والمحادث			
Interface	WAN Choose which interface Hint: in most cases, you	this rule applies to. Il want to uso WAN hore.						
External subnet	Enter the external (WA	/ 32 💌 i) subnet for the 1:1 mapping. You may map single IP addre	asses by specifying a /32 subret.					
Internal subnet	Enter the internal (LAN) internal subnet (they hi	subnet for the 1:1 mapping. The subnet size specified for the to be the same).	the external subnet also applies to the					
		here for the second of the second	A SHARE A SHARE A	ALLAN THIS	ACCONTRACTOR			_
Firewall: NAT:	1:1: Edit		2.2-311	······································	ومداجه فالمحارف المجامعة	,		T
Interface	Choose which interface Hint: in most cases, you	this rule applies to. Il want to use WAM here.						
External subnet	10.0.0.5 Enter the external (WA	/ 32 x I) subnet for the 1:1 napping. You may map single IP addre	sses by specifying a /32 subnet.					
Internal subnet	192.168.2.5 Enter the internal (LAN) internal subnet (they ha	subnet for the 1:1 mapping. The subnet size specified for t ve to be the same).	he external subnet also applies to the					
Bus	Tou nay entites of	here for a taxe (not pare 1).		A BARAROOTROTETE		IX OKIOI		т. 1
0	-1-1	a state a second division of		ورجار المحمد والمراجع والمراجع المراجع والمحم				
Website vis	ilor							
topdump								
NAT	> WAN							
Firewall rules								
	_							
Firewall	LAN							
topdump								
								1'
			-				1	Taxaa ay ahara
TCP		*	*	192.168.1.5	80 (HTTP)	*		NAT forv
	-							
-	1.4.1.1					1 - 20 - 68 - 8 C - 1 - 8		2
Netwo	ork Addr	ess Translatio	on					
Disabl	e NAT R	eflection	Disable	e the automatic cre	ation of NAT rea	tiroct rulo	e for access to you	r public ID
			from with	in your internal nets	works Note Ref	lection or	ly works on nort	forward to
			and does	not work for large r	anges > 500 no	ts.	in Horks on port	or waru ty
								<u>م</u>
د. مرجع بالدين الرغم ال	د از را از را از ا	مر عند الدين المراجع			and the second	Completion and the	r ochrywer profils	0
14-5	,	· [-] =-141*				-,	, , , , , , , , , , , , , , , , , , ,	

www.thin.kiev.ua - Руководство по pfSense 2.0. Часть 7 Трансляция сетевых адресов (NAT)

Автор: 02.04.12 11:38 - Последнее обновление 02.04.12 14:42

