### Технология NAT

NAT (Network Address Translation) – трансляция адресов, поз- воляющая скрывать адреса сети от узлов, находящихся за Cisco PIX. При прохождении пакетов через Cisco PIX внутренние адреса сети перед выходом с внешнего интерфейса транслируются в дру- гие адреса. NAT конфигурируется с помощью команд **nat** и **global**.

Когда исходящий пакет от узла, находящегося во внутренней зоне, попадает на Cisco PIX, на котором сконфигурирована система NAT, адрес источника пакета сравнивается с таблицей существую- щих трансляций. Если этого адреса источника нет в таблице, он транслируется в один из адресов пула и в таблице трансляций по- является новая запись для этого адреса источника. Пул выдаваемых адресов конфигурируется командой **global**. В результате этого происходит обновление таблицы трансляций, а пакет перенаправ- ляется дальше. По истечении определенного времени (значение по умолчанию равно трем часам) запись в таблице трансляций для ад- реса источника, не пославшего ни одного пакета, очищается и ад- рес, выданный из пула, освобождается для использования другими узлами внутренней зоны.

Задание правил трансляции адресов исходящих пакетов для одного либо нескольких узлов осуществляется с помощью команды **nat**.

Синтаксис команды можно представить следующим образом: **nat [(if\_name)] nat\_id address [netmask] [[tcp] tcp\_max\_conns [emb\_limit] [norandomseq]]] [udp**

**udp\_max\_conns]**, где:

* + - * if\_name – имя интерфейса, подключенного к сети, адреса ко- торой необходимо транслировать;
			* nat\_id – число от 1 до 65535, соответствующее номеру пула глобальных адресов, в которые будут транслироваться внутренние адреса;
			* address [netmask] – адрес, в который будет происходить трансляция;
			* tcp\_max\_conns – максимальное число одновременных со- единений, разрешенных узлам внутренней зоны. Соединения в со- стоянии бездействия закрываются автоматически по истечении таймаута, задаваемого командой **timeout conn**;
			* emb\_limit – максимальное число незавершенных (embryonic) соединений. К незавершенным соединениям относятся те, которые еще не были до конца установлены между источником и назначе- нием, например, при установке TCP-соединения между узлами;
			* norandomseq – устанавливает необходимость при каждом новом соединении генерировать случайный initial sequence number (ISN). Связано это с тем, что TCP/IP стек некоторых ОС использует предсказуемые ISN, а это дает возможность злоумышленнику вклиниться в чужую сессию;
			* udp\_max\_conns – максимальное число одновременных UDP-соединений, разрешенных каждому из узлов внутренней сети. UDP-соединения, находящиеся в состоянии бездействия, закрыва- ются автоматически по истечении таймаута, задаваемого командой **timeout conn**.

Пример настройки службы NAT:

# PIX(config)#nat (inside) 1 10.0.0.0

**255.255.255.0.**

## ВЫПОЛНИТЬ!

1. Настроить службу NAT на внутреннем интерфейсе межсетевого экрана.

В команде **nаt** параметром nat\_id (в примере – 1) указывает- ся номер пула глобальных адресов, которые можно сконфигуриро- вать командой **global**. Синтаксис:

# global [(if\_name)] nat\_id {mapped\_ip

**[-mapped\_ip] [netmask mapped\_mask]} | interface**, где:

* + if\_name – имя интерфейса, на котором необходимо исполь- зовать задаваемый пул глобальных адресов;
	+ mapped\_ip [-mapped\_ip] – один адрес либо диапазон адресов;
	+ netmask mapped\_mask – задание маски для пула адресов в случае, если используются подсети. Если диапазон адресов с задан- ной маской покрывает несколько подсетей, то адрес подсети и ши- роковещательный адрес подсети не выдаются для трансляции. Например, если задан диапазон адресов 192.168.0.20-192.168.0.140 и маска 255.255.255.128, то адрес второй подсети 192.168.0.128 и широковещательный адрес первой подсети 192.168.0.127 выдавать- ся не будут;
	+ interface – определяет использование PAT (Port Address Translation) на интерфейсе. Пример:

**PIX(config)#nat (inside) 1 10.0.0.0**

**255.255.255.0**

**PIX(config)#global (outside) 1 192.168.0.3-**

**192.168.0.100**

В этом примере сконфигурирован пул из 98 адресов (192.168.0.3-192.168.0.100) под номером 1, в которые будут транс- лироваться внутренние адреса узлов из сети 10.0.0.0 при прохожде- нии сетевых пакетов через межсетевой экран.

Выдача адресов осуществляется динамически, начиная с начала диапазона и до его конца. В примере первым выданным ад- ресом будет 192.168.0.3.

## ВЫПОЛНИТЬ!

1. Выполнить конфигурацию пула глобальных адресов для внутреннего интерфейса межсетевого экрана.

Командой **nat control** включается одноименный режим. При работе в этом режиме пакеты, идущие из внутреннего (inside) интерфейса на внешний (outside), должны иметь сконфигурирован- ное для них правило трансляции. То есть, каждый узел сети внут-

ренней зоны может обмениваться данными с узлами сети внешней зоны, если заданы правила трансляции для этих внутренних узлов. Если на Cisco PIX приходит пакет от внутреннего узла, для которо- го не сконфигурировано правило трансляции, то этот пакет им не обрабатывается.

Режим **nat control** является выключенным по умолчанию. По- этому Cisco PIX транслирует адрес источника пакета в любом слу- чае.

## ВЫПОЛНИТЬ!

1. Включить nat control режим и проверить возможность прохождения сетевых пакетов между интерфейсами устройства.
2. Выключить nat control режим.

Кроме команды **nat** существует команда **static**, с помощью которой осуществляется конфигурирование статической трансля- ции. Синтаксис команды:

# PIX(config)# static (real\_ifc, global\_ifc)

**{global\_ip | interface} {real\_ip [netmask mask]}**, где:

* + real\_ifc – интерфейс, на который приходят пакеты, подле- жащие трансляции;
	+ global\_ifc – интерфейс, с которого уходит для дальнейшей маршрутизации транслированный пакет;
	+ global\_ip – адрес, в который будет осуществляться трансля-

ция;

* real\_ip – адрес, который будет транслироваться. Пример:

# PIX(config)#static (inside,outside) 192.168.100.10 10.10.10.10 netmask

**255.255.255.255**

Все пакеты, приходящие на адрес 192.168.100.10 будут пере- даваться на узел с адресом 10.10.10.10.

## ВЫПОЛНИТЬ!

1. Сконфигурировать статическую трансляцию на внешнем интерфейсе межсетевого экрана.