61203860G1-29.1B
January 2012

Configuration Guide

NAT Pools in AOS

This configuration guide will aid in the setup of static 1:1 network address translation (NAT) pools for ADTRAN Operating System (AOS) products. An overview of general concepts combined with detailed command descriptions for example networks provide step-by-step assistance for configuration. The troubleshooting section outlines proper use of **show** and **debug** commands to verify that static 1:1 NAT pools have been configured properly on the AOS product(s).

This guide consists of the following sections:

Static 1:1 NAT Pools Overview

Static 1:1 NAT allows connections initiated from a particular private Internet Protocol version 4 (IPv4) Address to always map to a particular public IPv4 address. For every private host that requires a 1:1 NAT mapping, there must be a corresponding NAT address on the public side. In previous versions of AOS, this was accomplished by using an exhaustive list of all address mappings. AOS version 17.4 and later provided support for using NAT pools that list ranges of local and global IPv4 addresses to create the 1:1 mappings.

Hardware and Software Requirements and Limitations

Introduced in AOS 17.4, support for static 1:1 NAT pools is available on AOS data products as outlined in the ADTRAN knowledge base article, article number 2272, *Product Feature Matrix*. This matrix is available online at http://kb.adtran.com.

Configuring NAT Pools in AOS

The following steps are required to implement NAT pools in AOS:

1. Access the CLI.
2. Enable security features.
3. Define the local and global network address ranges.
4. Create the NAT pool.
5. Create an access control policy (ACP) and apply it to the interface.

Step 1: Access the CLI

To access the command line interface (CLI) on your AOS unit, follow these steps:

1. Boot up the unit.
2. Telnet to the unit (**telnet** <*ipv4 address*>). For example:
   telnet 10.10.10.1

> NOTE *If during the unit's setup process you have changed the default IPv4 address (10.10.10.1), use the configured IPv4 address.*

3. Enter your user name and password at the prompt.

> NOTE *The AOS default user name is **admin** and the default password is **password**. If your product no longer has the default user name and password, contact your system administrator for the appropriate user name and password.*

4. Enable your unit by entering **enable** at the prompt as follows:
   >**enable**
5. If configured, enter your Enable mode password at the prompt.
6. Enter the unit's Global Configuration mode as follows:
   #**configure terminal**
   (config)#

Step 2: Enable Security Features

Enable the AOS security features using the **ip firewall** command. The firewall is disabled by default. Also, use the **ip firewall nat-preserve-source-port** command to ensure source port preservation is enabled. Unlike the firewall, source port preservation is enabled by default.

The following example enables AOS security features:

(config)#**ip firewall**

(config)#**ip firewall nat-preserve-source-port**

*The **ip firewall nat-preserve-source-port** command was introduced in AOS version 14.01.00 and is enabled by default. It is not visible in the **show running-config** command output. Instead, use the **show running-config verbose** command to view.*

Step 3: Define the Local and Global Network Address Ranges

Be sure to define and apply the IPv4 address (or range of addresses) you plan to use for the public interface, if you have not already done so. Use the **ip address** command issued at the appropriate interface configuration mode to define a primary IPv4 address. There can be only one primary address on the interface, but a secondary IPv4 address can be defined using the **secondary** keyword. A range of secondary IPv4 addresses can also be defined using the **ip address range** <*start ip address*> <*end ip address*> <*subnet mask*> **secondary** command.

For example, the following commands apply the IPv4 address 208.61.209.1 to the PPP 1 interface:

(config)#**interface ppp 1**

(config-ppp1)#**ip address 208.61.209.1 255.255.255.0**

In this example, the following commands apply the secondary IPv4 address range 208.61.209.2 to 208.62.209.254 to the PPP 1 interface:

(config)#**interface ppp 1**

(config-ppp1)#**ip address range 208.61.209.2 208.62.209.254 255.255.255.0 secondary**

Step 4: Create the NAT Pool

Static NAT pools define a local network range of addresses whose size must be equal to the global range. Source NAT will translate from the local range to the global range. Destination NAT will translate from the global range to the local range. The addresses do not have to start at the same offset. If this command is entered and the two ranges are not of the same size, an error message is displayed. Due to this requirement of equal local and global addresses, static NAT pools should only be used when the desired local address range is less than or equal to the amount of the available global addresses. For instance, if 15 global (public) addresses were available for NAT, then only 15 or fewer local (private) addresses could be used with a NAT pool. If there are many more local addresses than global, NAT with overloading (many-to-one NAT) should be used instead. If the command fails due to mismatched local and global address size, the pool will remain in its original state. If the pool was configured with an existing address range prior to issuing the failed command, that range will remain unchanged. If no address range was present, the pool will remain incomplete.

For more information on many-to-one NAT, refer to the Firewall Wizard video (article number 2185) available at http://kb.adtran.com.

Create a NAT pool. Keep in mind that the pool name is case-sensitive. There is no limit to the number of NAT pools that can be defined, except the amount of random access memory (RAM) available on your AOS unit. To create a NAT pool, enter the **ip nat pool** <*name*> **static** command.

For example, enter the following command to create a static NAT pool named **POOL1**:

(config)#**ip nat pool POOL1 static**

After applying the IPv4 address(es), the following command creates a static NAT pool and defines the local range from 10.1.1.1 to 10.1.1.254 and the global range as 208.61.209.1 to 208.61.209.254:

(config)#**ip nat pool POOL1 static**

(config-natpool)#**local 10.1.1.1 10.1.1.254 global 208.61.209.1 208.61.209.254**

In some situations, an address that falls within a range needs to be excluded. For example, if you are excluding 208.61.209.10 because it is the address used for many-to-one source NAT for other nonstatic NAT hosts. This can be accomplished by creating multiple pools. This configuration requires multiple ACP entries, but each can use the same access control list (ACL).

In the following example, the address 208.61.209.10 is excluded from the 1:1 NAT pool.

(config)#**ip nat pool POOL1 static**

(config-natpool)#**local 10.1.1.1 10.1.1.9 global 208.61.209.1 208.61.209.9**

(config)#**ip nat pool POOL2 static**

(config-natpool)#**local 10.1.1.11 10.1.1.254 global 208.61.209.11 208.61.209.254**

Step 5: Create an Access Control Policy (ACP) and Apply to the Interface.

ACPs are used to allow, discard, or manipulate (using NAT) data for each physical interface. Each ACP consists of a selector (i.e., an ACL) and an action (**allow**, **discard**, or **NAT**). The selector can be an undefined ACL, which will permit any traffic or an ACL that specifies particular traffic to permit. When packets are received on an interface, the configured ACPs are applied to determine whether the data is processed or discarded.

ACPs are order dependent. When a packet is evaluated, the matching engine begins with the first entry and progresses through the entries until it finds a match. The first entry that matches is executed. The policy class has an implicit discard at the end of the list. Typically, the most specific entries should be at the top and the most general at the bottom.

The following example configures the ACP **PRIVATE** using an undefined ACL that matches all traffic:

(config)#**ip policy-class PRIVATE**

(config-policy-class)#**nat source list MATCHALL pool POOL1 policy PUBLIC**

Next, apply the ACP to the interface. The following example assigns the access policy **PRIVATE** to the Ethernet 0/1 interface:

(config)#**interface ethernet 0/1**

(config-eth 0/1)#**ip access-policy PRIVATE**

Using ACLs

If the NAT pool does not retrict traffic enough, you will want to create ACLs. ACLs are used as packet selectors by ACPs. They must be assigned to an ACP in order to be active. ACLs are composed of an ordered list of entries. Each entry contains two parts: an action (**permit** or **deny**) and a packet pattern. A **permit** ACL is used to permit packets (meeting the specified pattern) to enter the router system. A **deny** ACL advances the AOS to the next ACP entry. AOS provides two types of ACLs: **standard** and **extended**. Standard ACLs allow source IPv4 address packet patterns only. Extended ACLs specify patterns using most fields in the IP header and the Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) header.

Create ACLs and policy classes to regulate traffic through the network. ACLs are created and used to select traffic that matches their criteria. Once traffic is selected, the actions specified in the ACP are applied to it. In the instances discussed in this document, the action is to NAT the traffic.

In cases where you have defined a static 1:1 NAT for every host on the network or you have created multiple pools to exclude certain addresses, then using a **MATCHALL** ACL is sufficient. In other instances, more specific traffic selectors are necessary, requiring more restrictive ACLs.

For example, the following ACL is matching traffic sourced from the 10.1.1.0 /28 network and destined to the 192.168.0.0 /16 network:

(config)#**ip access-list extended INSIDE**

(config-ext-nacl)#**permit ip 10.1.1.0 0.0.0.15 192.168.0.0 0.0.255.255**

When choosing an action from an ACP entry, the destination ACP is matched first, followed by the NAT pool, and finally the ACL. If all three match, the ACP entry's action (in this case NAT the traffic) is taken. If any one of the three criteria do not match, the next ACP entry is inspected. This process is repeated until there are no more entries. At that point, the implicit discard will drop the traffic.

The following example, configuration of the ACP **PRIVATE** enables NAT for traffic that matches the destination ACP named **PUBLIC**, the NAT pool named **POOL1**, and the ACL named **INSIDE**:

(config)#**ip policy-class PRIVATE**

(config-policy-class)#**nat source list INSIDE pool POOL1 policy PUBLIC**

Apply the ACP to an interface.

The following example assigns the access policy **PRIVATE** to the Ethernet 0/1 interface:

(config)#**interface ethernet 0/1**

(config-eth 0/1)#**ip access-policy PRIVATE**

Configuration Examples

This guide provides two example configurations using static 1:1 NAT pools in AOS along with a sample script.

Example 1: Static 1:1 NAT to Public Network on page 6

Example 2: Static 1:1 NAT to Arbitrary Network Addresses Over VPN on page 8

Example 1: Static 1:1 NAT to Public Network

In this example, a customer has purchased a /24 public block of IPv4 addresses from their Internet service provider (ISP) and wants to utilize the addresses to NAT hosts on the private network out to the Internet. Each private host will have their source address translated to the matching address in the public block from the NAT pool as depicted in the diagram below. The local area network (LAN) interface is **eth 0/1** and the wide area network (WAN) is a Metro Ethernet connection from the ISP (**eth 0/2**). Hosts on the private side will have their IPv4 address assigned by the AOS device via the configured Dynamic Host Configuration Protocol (DHCP) server pool. This will assign the hosts an IPv4 address, a default gateway, and a DNS server. These assigned private IPv4 addresses will be translated to the public IPv4 addresses with the configured NAT pool for Internet access.

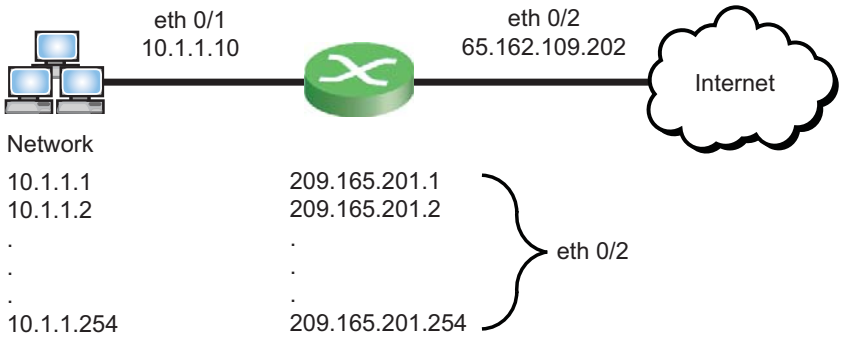

Figure 1. Static 1:1 NAT to Public Network

The following example configuration does not have a destination NAT entry in the **PUBLIC** ACP. This means that only traffic initiated from the **PRIVATE** ACP via source NAT will be allowed as returning traffic during the lifetime of the individual flows. If this is not desired, a destination NAT entry on the **PUBLIC** ACP can be added. This will indicate that you want to always allow traffic initiated from the public side. An example using a destination NAT entry is shown in Example 2.

The ACL named **ADMIN** is used on the **PUBLIC** ACP to allow only incoming connections for router management on the IPv4 address 65.162.109.202. All other traffic coming into the router that was not in response to traffic initiated by the private side will be dropped by the firewall.

The following commands are entered to configure static 1:1 NAT pools for Example 1:

```
!
ip firewall
ip firewall nat-preserve-source-port
!
ip dhcp pool LAN
   network 10.1.1.0 255.255.255.0
   dns-server 4.2.2.2
   default-router 10.1.1.1
!
interface eth 0/1
   ip address 10.1.1.1 255.255.255.0
   ip access-policy PRIVATE
   no shutdown
!
interface eth 0/2
   ip address 65.162.109.202 255.255.255.252
   ip address range 208.61.209.1 208.61.209.254 255.255.255.0 secondary
   ip access-policy PUBLIC
   no shutdown
!
ip access-list standard MATCHALL
   permit any
!
ip access-list extended ADMIN
   remark allow administrative access for router
   permit ip any host 65.162.109.202
!
ip nat pool POOL1 static
   local 10.1.1.1 10.1.1.254 global 208.61.209.1 208.61.209.254
!
```



```
ip policy-class Private
   allow list MATCHALL self
   nat source list MATCHALL pool POOL1 policy PUBLIC
!
ip policy-class PUBLIC
   allow list ADMIN self
!
ip route 0.0.0.0 0.0.0.0 65.162.109.201
!
```

> NOTE
>
> *The **ip firewall nat-preserve-source-port** command was introduced in AOS version 14.01.00 and is enabled by default. It is not visible in the **show running-config** command output. It can be viewed in the output of the **show running-config verbose** command.*

Example 2: Static 1:1 NAT to Arbitrary Network Addresses Over VPN

This network configuration uses static 1:1 NAT to arbitrary network addresses and sends traffic over a virtual private network (VPN) tunnel. This is useful when several remote sites use the same LAN addressing scheme and need to distinguish remote traffic using a different arbitrary network at each site. The arbitrary network still needs to be known to the router since destination NAT will be used to allow traffic to be initiated to the LAN. This also allows routing protocols to advertise the network. It is easiest to add the network on a loopback interface.

Other private traffic not matching the NAT pool and ACL will be translated with many-to-one source NAT to the Ethernet 0/1 interface.

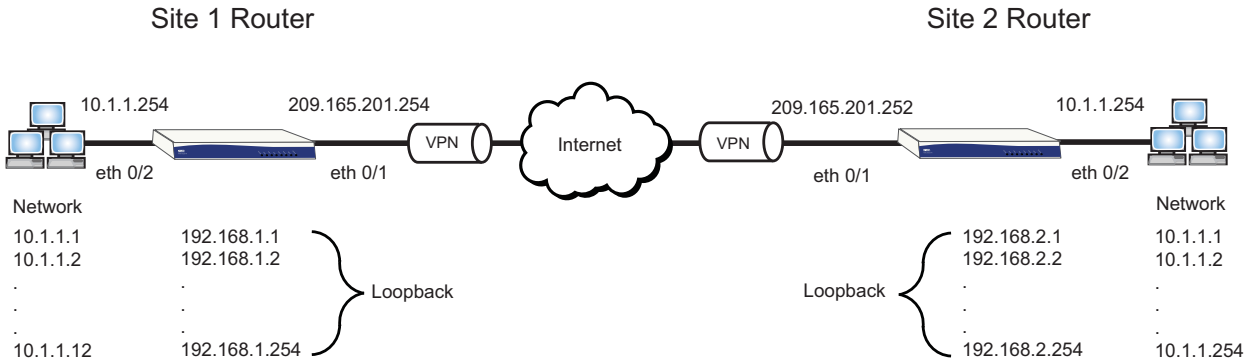

Figure 2. Static 1:1 NAT to Arbitrary Network Over VPN

In this example, two remote sites are connected via a main mode IPSec VPN tunnel using static WAN IPv4 addresses. Both sites have legacy networking equipment that forces them to use the 10.1.1.0 /24 subnet at each site. Hosts on the private side will have their IPv4 address assigned by the AOS device using the configured DHCP server pool. This will assign the hosts an IPv4 address, a default gateway, and a DNS server. Traffic that is destined for a remote 192.168.x.x address across the VPN tunnel will be translated

from a 10.1.1.0 /24 address to the corresponding 192.168.x.0 /24 address with the **nat source list INSIDE pool POOL1 policy PUBLIC** command**.** All other traffic will be translated to the public IPv4 address for Internet access with the **nat source list WIZARD-ICS interface eth 0/1 overload** command in the **PRIVATE** ACP.

The ACL named ADMIN is used on the **PUBLIC** ACP to only allow incoming connections for router management on the IPv4 address 209.165.201.254. Traffic coming in over the VPN tunnel will be allowed through and will be translated back to the proper 10.1.1.0 /24 address from the corresponding 192.168.x.0 /24 address using the **nat destination list OUTSIDE pool POOL1** command in the **PUBLIC** ACP.

The VPN selectors that are used in this setup specify 192.168.0.0 /16 to allow for other sites to be added in the future if needed. These configurations can be used as a template for additional sites by altering the applicable IPv4 addresses in the configurations.

Site 1 Configuration

```
!
ip firewall
ip firewall nat-preserve-source-port
!
ip dhcp pool LAN
   network 10.1.1.0 255.255.255.0
   dns-server 4.2.2.2
   default-router 10.1.1.254
!
ip crypto
!
crypto ike policy 100
   initiate main
   respond anymode
   local-id address 209.165.201.254
   peer 209.165.201.101
   attribute 1
      encryption 3des
      hash md5
      authentication pre-share
!
crypto ike remote-id address 209.165.201.101 preshared-key SHAREDSECRET ike-policy 100 crypto
map VPN 10 no-mode-config no-xauth
!
crypto ipsec transform-set esp-3des-esp-md5-hmac esp-3des esp-md5-hmac
   mode tunnel
!
```



```
crypto map VPN 10 ipsec-ike
   description VPN to Site 2
   match address VPN-10-vpn-selectors
   set peer 209.165.201.101
   set transform-set esp-3des-esp-md5-hmac
   ike-policy 100
!
interface loop 1
   ip address 192.168.1.1 255.255.255.0
   ip address range 192.168.1.2 192.168.1.254 255.255.255.0 secondary
   no shutdown
!
interface eth 0/1
   ip address 209.165.201.254 255.255.255.252
   ip access-policy PUBLIC
   crypto map VPN
   no shutdown
!
interface eth 0/2
   ip address 10.1.1.254 255.255.255.0
   ip access-policy PRIVATE
   no shutdown
!
ip access-list extended ADMIN
   remark allow administrative access to router
   permit ip any host 209.165.201.254
!
ip access-list standard WIZARD-ICS
   remark Internet Connection Sharing
   permit any
!
ip access-list extended INSIDE
   permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.255.255
!
ip access-list extended OUTSIDE
   permit ip 192.168.0.0 0.0.255.255 192.168.1.0 0.0.0.255
!
ip access-list extended SELF
   remark Traffic to NetVanta
   permit ip any any log
```



```
!
ip access-list extended VPN-10-vpn-selectors
   permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
!
!
ip nat pool POOL1 static
   local 10.1.1.1 10.1.1.254 global 192.168.1.1 192.168.1.254
!
ip policy-class PRIVATE
   allow list SELF self
   nat source list INSIDE pool POOL1 policy Public
   nat source list wizard-ics interface eth 0/1 overload
!
ip policy-class PUBLIC
   allow list ADMIN self
   nat destination list OUTSIDE pool POOL1
!
ip route 0.0.0.0 0.0.0.0 209.165.201.253
!
```

Site 2 Configuration

```
!
ip firewall
ip firewall nat-preserve-source-port
!
ip dhcp pool LAN
   network 10.1.1.0 255.255.255.0
   dns-server 4.2.2.2
   default-router 10.1.1.254
!
ip crypto
!
crypto ike policy 100
   initiate main
   respond anymode
   local-id address 209.165.201.101
   peer 209.165.201.254
   attribute 1
      encryption 3des
```



```
      hash md5
      authentication pre-share
!
crypto ike remote-id address 209.165.201.254 preshared-key SHAREDSECRET ike-policy 100 crypto
map VPN 10 no-mode-config no-xauth
!
crypto ipsec transform-set esp-3des-esp-md5-hmac esp-3des esp-md5-hmac
   mode tunnel
!
crypto map VPN 10 ipsec-ike
   description VPN to Site 1
   match address VPN-10-vpn-selectors
   set peer 209.165.201.254
   set transform-set esp-3des-esp-md5-hmac
   ike-policy 100
!
interface loop 1
   ip address 192.168.2.1 255.255.255.0
   ip address range 192.168.2.2 192.168.2.254 255.255.255.0 secondary
   no shutdown
!
interface eth 0/1
   ip address 209.165.201.101 255.255.255.252
   ip access-policy PUBLIC
   crypto map VPN
   no shutdown
!
!
interface eth 0/2
   ip address 10.1.1.254 255.255.255.0
   ip access-policy PRIVATE
   no shutdown
!
ip access-list extended ADMIN
   remark allow administrative access to router
   permit ip any host 209.165.201.101
!
ip access-list standard WIZARD-ICS
   remark Internet Connection Sharing
   permit any
```



```
!
ip access-list extended INSIDE
   permit ip 10.1.1.0 0.0.0.255 192.168.0.0 0.0.255.255
!
ip access-list extended OUTSIDE
   permit ip 192.168.0.0 0.0.255.255 192.168.2.0 0.0.0.255
!
ip access-list extended SELF
   remark Traffic to NetVanta
   permit ip any any log
!
ip access-list extended VPN-10-vpn-selectors
   permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255
!
!
ip nat pool POOL1 static
   local 10.1.1.1 10.1.1.254 global 192.168.2.1 192.168.2.254
!
ip policy-class PRIVATE
   allow list SELF self
   nat source list INSIDE pool POOL1 policy PUBLIC
   nat source list WIZARD-ICS interface eth 0/1 overload
!
ip policy-class PUBLIC
   allow list ADMIN self
   nat destination list OUTSIDE pool POOL1
!
ip route 0.0.0.0 0.0.0.0 209.165.201.102
!
```

*The **ip firewall nat-preserve-source-port** command was introduced in AOS version 14.01.00 and is enabled by default. It is not visible in the **show running-config** command output. It can be viewed in the output of the **show running-config verbose** command.*

Command Summary

The following table describes commands for configuring NAT pools on an AOS product.

Table 1. NAT Pools Configuration Command Summary

Step	Command	Description
Step 1	(config)#**ip firewall**	Enable the IPv4 firewall functionality in AOS.
Step 2	(config-interface)#**ip address** <*ipv4 address*> <*subnet mask*> [**secondary**]	Defines a primary IPv4 address for the specified interface. Using the **secondary** keyword defines a secondary IPv4 address for the specified interface.
	(config-interface)#**ip address range** <*start ipv4 address*> <*end ipv4 address*> <*subnet mask*> **secondary**	Defines a range of secondary IPv4 addresses for the specified interface.
Step 3	(config)#**ip nat pool** <*name*> [**static**]	Creates a NAT pool and enters the NAT pool configuration command set. At this time, only a static type can be created by using the keyword **static**.
	(config-natpool)#**local** <*start ipv4 address*> <*end ipv4 address*> **global** <*start ipv4 address*> <*end ipv4 address*>	Defines a local network range of IPv4 addresses to match the global range. Source NAT will translate from the local range to the global range and destination NAT will translate from the global range to the local range.
Step 4	(config-policy-class)#**nat destination list** <*name*> **pool** <*name*> [**no-alg**]	Translates the destination IPv4 address to an address within the specified pool of addresses, translating a global address to a local association. The **no-alg** keyword indicates the packet is allowed through the firewall without being processed by the application-level gateways (ALG).
	(config-policy-class)#**nat source list** <*name*> **pool** <*name*> [**no-alg**] [**policy** <*name*>]	Translate the source IPv4 address to an address within the specified pool of addresses, translating a local address to a global address. The **no-alg** keyword indicates the packet is allowed through the firewall without being processed by the application-level gateways (ALG).

Troubleshooting

After configuring NAT pools, **show** commands can be used to assist in troubleshooting and verifying your configuration. The following are sample output displayed from issuing the **show ip access-lists**, **show ip policy-sessions**, **show ip policy-stats**, and **show running-config ip nat pool** commands. If traffic is not being translated as expected, verify that the traffic is matching the proper ACP entries, the ranges in the specified pool(s), and the specified ACLs.

Show Command Sample Output

The following sample output are provided to enhance your understanding of the information provided for each **show** command.

```
#show ip access-lists
Extended IP access list INSIDE
  permit ip 10.1.1.0 0.0.0.15 192.168.0.0 0.0.255.255   (3567 matches)
Extended IP access list OUTSIDE
  permit ip 192.168.0.0 0.0.255.255 192.168.1.0 0.0.0.15   (1 matches)
Extended IP access list VPN_Selectors
  permit ip 192.168.0.0 0.0.255.255 192.168.0.0 0.0.255.255     (3568 matches)
```

```
#show ip policy-sessions
Src Vrf (if not default), Src policy class:
Protocol (TTL) [in crypto map] -> [out crypto map] Dest VRF, Dest policy-class
  Src IP Address  Src Port Dest IP Address Dst Port NAT IP Address    NAT Port
  --------------- -------- --------------- -------- ---------------- --------

Policy class "Private":
tcp (579) -> Public
  10.10.20.9      3481     67.195.187.192  5050     s 208.61.209.1   3481
tcp (586) -> Public
  10.10.20.9      3490     98.137.130.66   443      s 208.61.209.1   3490
tcp (28800) -> self
  10.10.20.9      2176     192.168.0.25    23
udp (60) -> Public
  10.10.20.9      2233     208.61.208.253  2233     s 208.61.209.1   1057
udp (39) -> Public
  192.168.2.4     4500     66.0.238.250    4500     s 208.61.209.1   4500
udp (39) -> Public
  192.168.2.4     4500     208.61.208.235  4500     s 208.61.209.1   1061
tcp (544) -> Public
  192.168.5.3     61064    69.63.180.44    80       s 208.61.209.1   61064

Policy class "Public":
tcp (600) -> Private
  67.58.88.6      1027     208.61.209.1    47624    d 192.168.5.5    47624

Policy class "self":
icmp (46) -> Private
  192.168.5.1     2        192.168.5.5     2
icmp (46) -> Private
  192.168.5.1     1        192.168.5.61    1

Policy class "default":
```

Source NAT flows are identified by “s” and display the port number used for translation.

Destination NAT flows are identified by “d” and display the port number used for translation.

```
#show ip policy-stats
Current sessions: 0
Maximum sessions: 82200

Policy-class "PRIVATE":
  0 current sessions (27400 max)
  Entry 1 - nat source list INSIDE pool POOL1 policy PUBLIC
      583757 in bytes, 193950 out bytes, 3567 hits

  Entry 2 - nat source list MATCHALL interface ppp 1 overload
      3954 in bytes, 58312 out bytes, 36 hits
```



```
Policy-class "PUBLIC":
0 current sessions (27400 max)
  Entry 1 - nat destination list OUTSIDE pool POOL1
      512 in bytes, 512 out bytes, 1 hits

#show running-config ip nat pool
Building configuration...
!
ip nat pool POOL1 static
  local 10.1.1.1 10.1.1.12 global 192.168.1.1 192.168.1.12
!
end
```