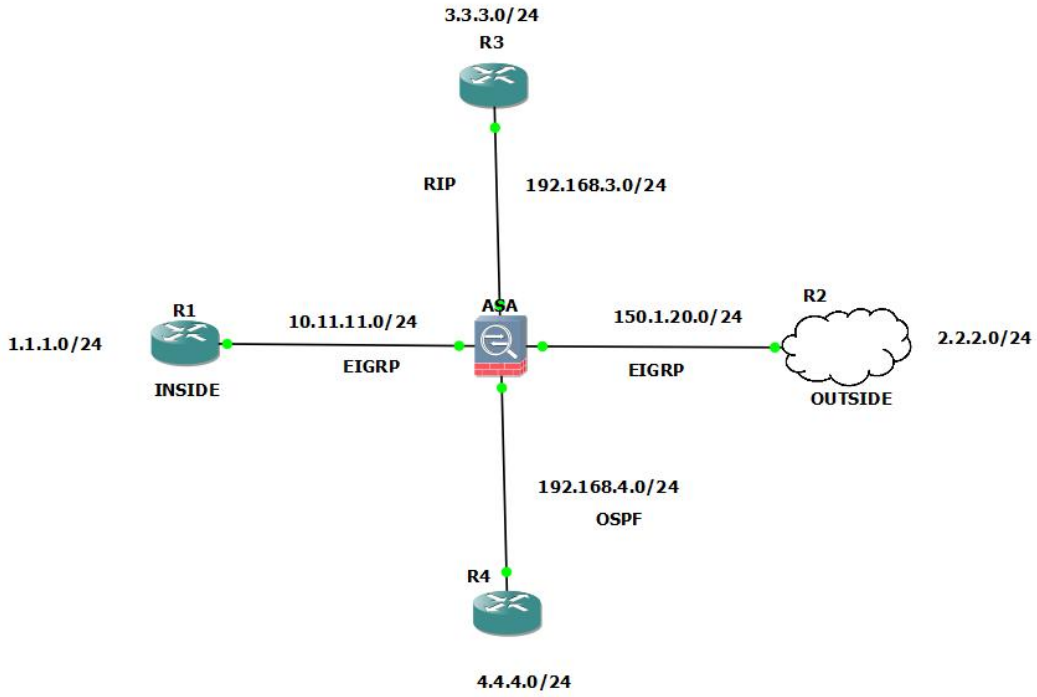
Firewall Routing and Redistribution



Initial configuration

On Firewall

en
Press enter when asked for password
Conf t
Int g0/0
Ip address 10.11.11.10 255.255.255.0
No shutdown
Security-level 100
Nameif Inside

Int g0/1
Ip address 150.1.20.10 255.255.255.0
No shutdown
Security-level 0
Nameif Outside

Int g0/2
Ip address 192.168.3.10 255.255.255.0
No shutdown
Security-level 50
Nameif DMZ-3

Int g0/3
Ip address 192.168.4.10 255.255.255.0
No shutdown
Security-level 50
Nameif DMZ-4

On routers

On R1

Int f 0/0
Ip add 10.11.11.1 255.255.255.0
No shut

Int lo0
Ip add 10.1.1.1 255.255.255.0

Similarly, do configurations on the other routers interfaces.

If we do not want the outside interface to ping, we can deny it, as attackers can send multiple pings so that the interface foes down.
icmp deny any Outside

Routing protocols

Configure all the protocols normally according to the topology.

For example, on the firewall,

router rip
version 2
no auto-summary
network 192.168.3.0
ex
router ospf 100
network 192.168.4.0 255.255.255.0 area 0

On R4,
router ospf 1
network 192.168.4.0 0.0.0.255 area 0
network 4.4.4.0 0.0.0.255 area 0

Routes on ASA:

```
ciscoasa# sh route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
Gateway of last resort is not set

D        1.1.1.0 255.255.255.0 [90/130816] via 10.11.11.1, 00:01:07, Inside
D        2.2.2.0 255.255.255.0 [90/130816] via 150.1.20.1, 00:01:07, Outside
R        3.3.3.0 255.255.255.0 [120/1] via 192.168.3.1, 00:00:26, DMZ-3
O        4.4.4.4 255.255.255.255 [110/11] via 192.168.4.1, 00:00:25, DMZ-4
C        10.11.11.0 255.255.255.0 is directly connected, Inside
L        10.11.11.10 255.255.255.255 is directly connected, Inside
C        150.1.20.0 255.255.255.0 is directly connected, Outside
L        150.1.20.10 255.255.255.255 is directly connected, Outside
C        192.168.3.0 255.255.255.0 is directly connected, DMZ-3
L        192.168.3.10 255.255.255.255 is directly connected, DMZ-3
C        192.168.4.0 255.255.255.0 is directly connected, DMZ-4
L        192.168.4.10 255.255.255.255 is directly connected, DMZ-4
```

Redistribution of routes

1. R1 should receive all loopback routes from R2, R3 and R4.
For this, redistribution should be done TO eigrp.
On ASA

Redistribute rip metric 100 10 50 50 1500
Redistribute ospf 100 metric 1 1 1 1 1

To see existing protocols:
Sh run router

Now we also need to redistribute routes from eigrp into rip and ospf:
On ASA
Router rip
Redistribute eigrp 100 metric 1
(Here metric is not important)

Router ospf 100
Redistribute eigrp 100 subnets
(means if something is classless, redistribute that also)

To check, since ping does not remian in connection table, let us see telnet
On R1
Telnet 4.4.4.4

```
R1#
R1#telnet 4.4.4.4
Trying 4.4.4.4 ... Open


Password required, but none set

[Connection to 4.4.4.4 closed by foreign host]
R1#
```

Works but let us make it work on R4 as well
On R4
Line vty 0 4
Password cisco
Login
Exit

2. R3 should receive routes from R4 as well and vice versa.
On ASA
router ospf 100
Redistribute rip subnets metric 21

We can see the route is present, since we redistributed from rip into ospf, routes should be present on the router running ospf which is R4 as we can see here.

```
R4#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/24 is subnetted, 1 subnets
O E2    1.1.1.0 [110/20] via 192.168.4.10, 00:11:07, FastEthernet0/0
     2.0.0.0/24 is subnetted, 1 subnets
O E2    2.2.2.0 [110/20] via 192.168.4.10, 00:11:07, FastEthernet0/0
     3.0.0.0/24 is subnetted, 1 subnets
O E2    3.3.3.0 [110/21] via 192.168.4.10, 00:03:17, FastEthernet0/0
     4.0.0.0/24 is subnetted, 1 subnets
C       4.4.4.0 is directly connected, Loopback0
C    192.168.4.0/24 is directly connected, FastEthernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
O E2    10.11.11.0 [110/20] via 192.168.4.10, 00:11:08, FastEthernet0/0
     150.1.0.0/24 is subnetted, 1 subnets
O E2    150.1.20.0 [110/20] via 192.168.4.10, 00:11:08, FastEthernet0/0
O E2 192.168.3.0/24 [110/21] via 192.168.4.10, 00:03:29, FastEthernet0/0
R4#
```

router rip
Redistribute ospf 100 metric 2
Now routes of R4 will be present in routes of R3

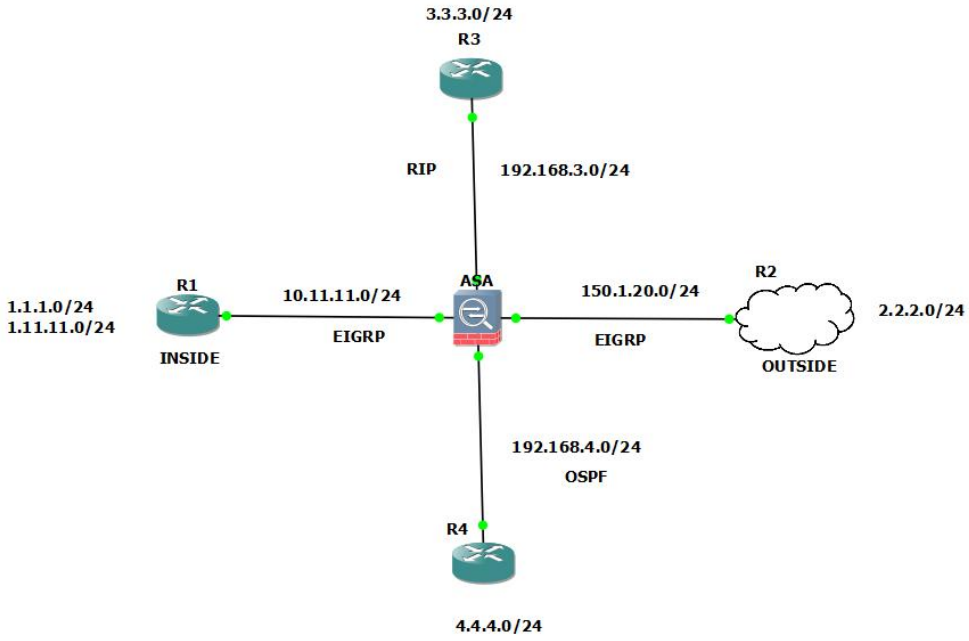
```
R3#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/24 is subnetted, 1 subnets
R       1.1.1.0 [120/1] via 192.168.3.10, 00:00:04, FastEthernet0/0
     2.0.0.0/24 is subnetted, 1 subnets
R       2.2.2.0 [120/1] via 192.168.3.10, 00:00:04, FastEthernet0/0
     3.0.0.0/24 is subnetted, 1 subnets
C       3.3.3.0 is directly connected, Loopback0
     4.0.0.0/32 is subnetted, 1 subnets
R       4.4.4.4 [120/2] via 192.168.3.10, 00:00:04, FastEthernet0/0
R    192.168.4.0/24 [120/1] via 192.168.3.10, 00:00:04, FastEthernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
R       10.11.11.0 [120/1] via 192.168.3.10, 00:00:05, FastEthernet0/0
     150.1.0.0/24 is subnetted, 1 subnets
R       150.1.20.0 [120/1] via 192.168.3.10, 00:00:05, FastEthernet0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
R3#
```

At this point everyone has all the loopbacks and routes.

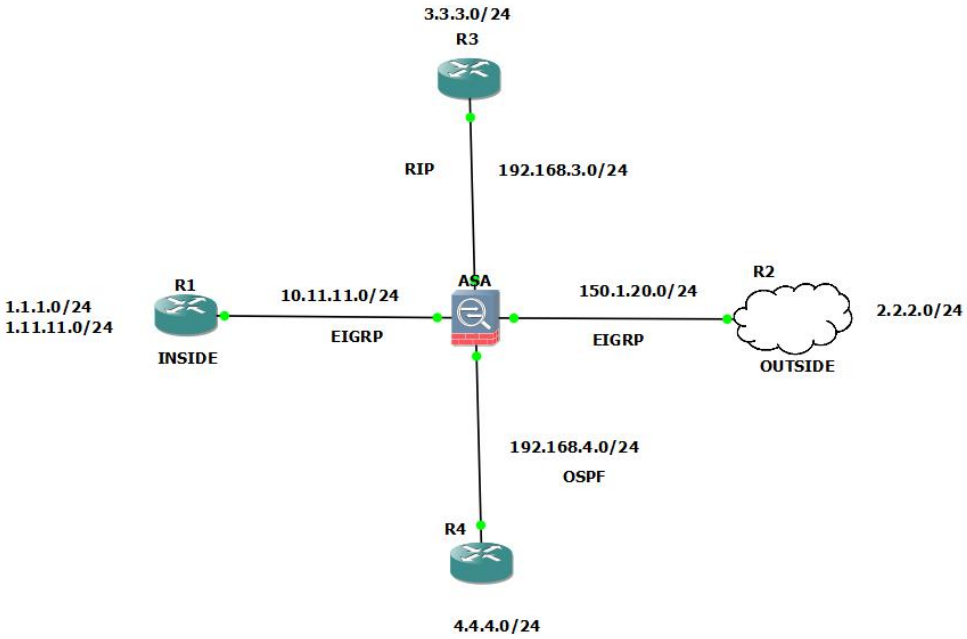
Now, say we have another loopback behind R1 but we do not want that to be redistributed.



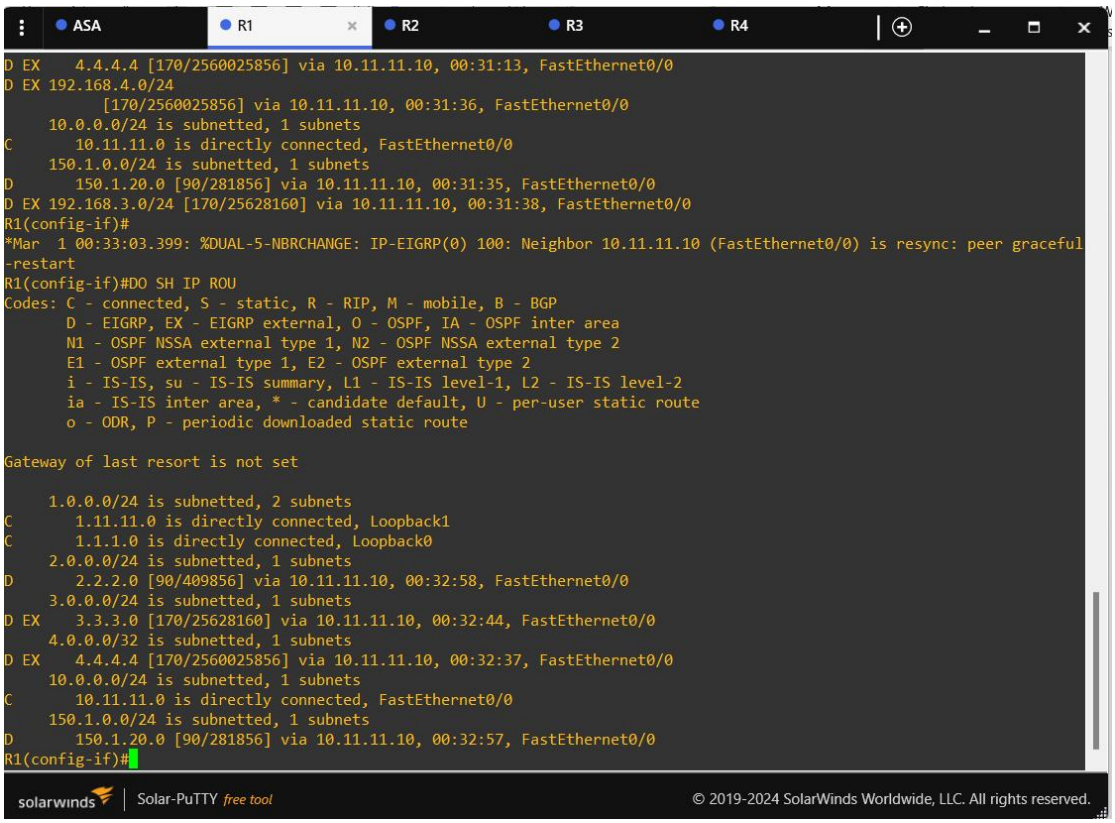
Let us make the loopback:
On R1
Int loopback 1
Ip address 1.11.11.11 255.255.255.0

Now this will be present in the routing table of ASA but we do not want it to be present on ASA so we will create ACL on ASA. We do not put this ACL on an interface because if we do that will be in data plane which means that the data coming from that course will be stopped, what we want to stop is routing traffic. The route will come in an eigrp packet(routing traffic) and not a data packet. Now if data traffic comes from that address, we will not have a route for that traffic so it will be dropped but if we have a default route, it will go through.
Access-list 10 deny 1.11.11.0 255.255.255.0
Access-list 10 permit any
Router eigrp 100
Distribute-list 10 in
In means the routes that are coming to ASA.
Now we can check that this route will not be present in ASA

3. Now we want that R3, R1 and R4 should not receive updates of links advertised in the routing table.



That means that in case of R3 for example, everyone should receive 3.3.3.0/24 but they should not receive 192.168.3.0/24
Now here we do not want others to receive certain routes so we will apply the redistribute list on the outside(outgoing).
On ASA
Access-list EIG-OUT deny 192.168.3.0 255.255.255.0
Access-list EIG-OUT deny 192.168.4.0 255.255.255.0
Access-list EIG-OUT permit any
Router eigrp 100
Distribute-list EIG-OUT out



We can see, now these routes are not present on R1.

The routing tables are now cleaner.
Let us do the same on R3
Access-list RIP-OUT deny 192.168.4.0 255.255.255.0
Access-list RIP-OUT deny 10.11.11.0 255.255.255.0
Access-list RIP-OUT deny 150.1.20.0 255.255.255.0
Access-list RIP-OUT permit any
Router rip
Distribute-list RIP-OUT out

It will take a long time for it to update on rip because it is slow.
To delete an access list in case of mistake:
clear configure access-list RIP-OUT

In the meantime to check if we did right, we can see the time of the routes on rip routing table, the ones we want to remove will be stuck on a time and will not be refreshed soon, other routes will be refreshed (00:00:0). It will update after some time.

```
Gateway of last resort is not set

     1.0.0.0/24 is subnetted, 1 subnets
R       1.1.1.0 [120/1] via 192.168.3.10, 00:00:24, FastEthernet0/0
     2.0.0.0/24 is subnetted, 1 subnets
R       2.2.2.0 [120/1] via 192.168.3.10, 00:00:24, FastEthernet0/0
     3.0.0.0/24 is subnetted, 1 subnets
C       3.3.3.0 is directly connected, Loopback0
     4.0.0.0/32 is subnetted, 1 subnets
R       4.4.4.4 [120/2] via 192.168.3.10, 00:00:24, FastEthernet0/0
R    192.168.4.0/24 [120/1] via 192.168.3.10, 00:01:49, FastEthernet0/0
     10.0.0.0/24 is subnetted, 1 subnets
R       10.11.11.0 [120/1] via 192.168.3.10, 00:01:50, FastEthernet0/0
     150.1.0.0/24 is subnetted, 1 subnets
R       150.1.20.0 [120/1] via 192.168.3.10, 00:01:50, FastEthernet0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
R3(config)#
```

Routes on R3 when updated:

```
R3(config)#do sh ip rou
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/24 is subnetted, 1 subnets
R       1.1.1.0 [120/1] via 192.168.3.10, 00:00:18, FastEthernet0/0
     2.0.0.0/24 is subnetted, 1 subnets
R       2.2.2.0 [120/1] via 192.168.3.10, 00:00:18, FastEthernet0/0
     3.0.0.0/24 is subnetted, 1 subnets
C       3.3.3.0 is directly connected, Loopback0
     4.0.0.0/32 is subnetted, 1 subnets
R       4.4.4.4 [120/2] via 192.168.3.10, 00:00:18, FastEthernet0/0
C    192.168.3.0/24 is directly connected, FastEthernet0/0
R3(config)#
```

Now for OSPF there are no distribute lists, only route maps.
For route maps we need to have ACLs:
On ASA

Access-list RM-Rip deny 192.168.3.0 255.255.255.0
Access-list RM-Rip permit any

Access-list RM-Eigrp deny 10.11.11.0 255.255.255.0
Access-list RM-Eigrp deny 150.1.20.0 255.255.255.0
Access-list RM-Eigrp permit any

Route-map RM-Rip permit 10
Match ip address RM-Rip
Exit

Router ospf 100
Redistribute rip route-map RM-Rip subnets
Exit
Route-map RM-Eigrp permit 10
Match Ip address RM-Eigrp
Exit
Router ospf 100
Redistribute eigrp 100 subnets route-map RM-Eigrp
Exit

To check ACLs
Show run access-list
Or
Show access-list

Now, we can see it works,

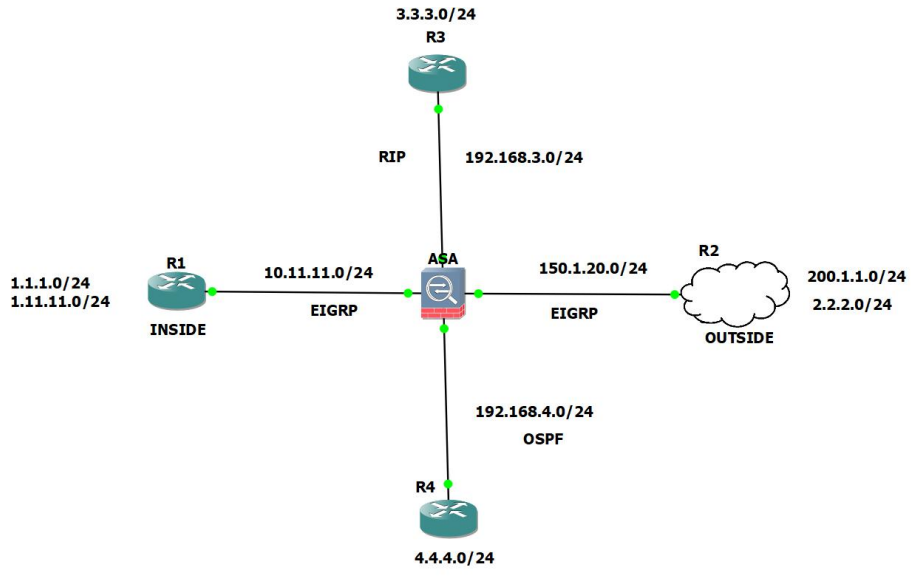
```
R4#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     1.0.0.0/24 is subnetted, 1 subnets
O E2    1.1.1.0 [110/20] via 192.168.4.10, 01:04:50, FastEthernet0/0
     2.0.0.0/24 is subnetted, 1 subnets
O E2    2.2.2.0 [110/20] via 192.168.4.10, 01:04:50, FastEthernet0/0
     3.0.0.0/24 is subnetted, 1 subnets
O E2    3.3.3.0 [110/21] via 192.168.4.10, 01:04:50, FastEthernet0/0
     4.0.0.0/24 is subnetted, 1 subnets
C       4.4.4.0 is directly connected, Loopback0
C    192.168.4.0/24 is directly connected, FastEthernet0/0
R4#
```

solarwinds | Solar-PuTTY *free tool* © 2019-2024 SolarWinds Worldwide, LLC. All rights reserved.

NAT



We first give a default route to the internet to ASA, ASA can reach the public address because it is directly connected to it, so let us give it a default route.

Route outside 0 0 150.1.20.1

The ping 150.1.20.1 will not work because we have not allowed icmp traffic to go outside during the configurations but this not show up in ACLs, so we have to check
Show run icmp
Here we will see that we have these commands

So write
Conf t
No icmp deny any Outside
The the ping will work.

Then we ping the internet:

We have a public address pool on the outside interface, and we need NAT.

1. Dynamic NAT

Step 1:
Specify the pool that will be used to go outside the network
On routers, we defined the pool as:
Ip nat pool ABC 150.1.20.10 150.1.20.254
On firewall, here is how we define the pool
Outside = Interface
10 = any number which will be the id of the nat pool

Global (Outside) 10 150.1.20.10-150.1.20.254 netmask 255.255.255.0

Now we have new nat syntax
Define the source (internal) network that needs to be translated
object network OBJ_INSIDE
subnet 10.11.11.0 255.255.255.0

Define the NAT pool (public IP range)
object network OBJ_NAT_POOL
range 150.1.20.11 150.1.20.254

The NAT pool cannot contain the address of the outside interface so we exclude 150.1.20.10.

Step 2:
Use the nat command to specify the internal addresses to be natted and also bind it to the global pool.
Nat (inside) 10 10.11.11.0 255.255.255.0

This means whatever is coming from “inside” interface with the address of “10.11.11.0 255.255.255.0” nat it to whatever is present in “10”. it will go inside 10, and see whatever address is free and that will be given.

The modern syntax is:
Apply NAT: Translate internal to public IPs when going outside

nat (inside,outside) 10 source dynamic OBJ_INSIDE OBJ_NAT_POOL

10 is the number, source is syntax, dynamic is the type of nat, then we have address to be translated and then the nat pool.

To check:
On R2:
Line vty 0 4
Password cisco
login
exit
`

To see objects:
Show run objects
To see nat:
Show nat
To see if it hit any translations:
Show xlate

So telnet was not working, after much troubleshooting I found out that on 200.1.1.0 which is internet, eigrp was not enabled, so r1 had no route to their, so I set up eigrp and then I set up a default route to the internet on r1.
On R1:
Telnet 200.1.1.1

```
R1#telnet 200.1.1.1
Trying 200.1.1.1 ... Open


User Access Verification

Password:
```

The moment you enable NAT, R1(the inside) is stopped access to other interfaces that are not a part of nat. That means R1 will not be able to telnet to R3, This is only because of security purposes, had it been a router, it would work.
R1 will not be able to telnet to outside because of the above reason.
R3 will not be able to telnet to outside as well, but because of a different reason: remember the EIG-OUT acl, we redistributed that into eigrp, that means the network 192.168.1.3 will be denied, that essentially means it will not be distributed that means other routers will not have that network, it means that telnet is denied because outside interface does not have a route back to r3- means the telnet will be going out but it will not be coming back in.
To see if what ACL is being hit:

show access-list | include hitcnt

Write the command in which you are facing problem and then write the hitcount command again and see if any ACL has increased.

This means that for two interfaces to talk to each other, they need to have a rule (does not have to be a NAT connection, just a rule)if NAT is present on any interface.
We are natting from inside which means my inside interface is not allowed to go anywhere else.
Say for example, we now bind R4 to Outside, R4 will then not be able to talk to R3.

Let us allow inside interface to talk to others even though nat exists

Same-security-traffic permit inter-interface

2. Identity NAT

We want to bind R3 to R1. We will bind inside to DMZ3 but we do not change the source.
Access-list will bind the traffic going from R1 to R3
Access-list IN-DMZ3 permit ip 10.11.11.0 255.255.255.0 192.168.3.0 255.255.255.0
Access-list IN-DMZ3 permit ip 1.1.1.0 255.255.255.0 192.168.3.0 255.255.255.0
Access-list IN-DMZ3 permit ip 1.1.1.0 255.255.255.0 3.3.3.0 255.255.255.0
Access-list IN-DMZ3 permit ip 10.11.11.0 255.255.255.0 3.3.3.0 255.255.255.0

nat(inside) 0 access-list In-DMZ3

New syntax:
nat (inside,DMZ3) source static any any match access-list IN-DMZ3

Through this project, we successfully implemented routing protocols, route redistribution, and NAT configurations to enable controlled communication between different network segments. By leveraging access control lists, redistribution filters, and security policies, we ensured efficient routing while maintaining security boundaries. The implementation of NAT, both dynamic and identity-based, allowed for selective address translation, enabling internal devices to access external networks while restricting unauthorized access. This configuration provides a strong foundation for understanding firewall policies, inter-VLAN communication, and network security best practices.