Cisco ASA Cli

Static NAT (SNAT)

```
object network obj-192.168.1.100
host 192.168.1.100
nat (inside,outside) static 192.166.1.101 dns
```

PAT

> Allow outside connections targeting TCP port 80 to redirect to internal port 8080.

```
object network obj-192.166.1.101-srv_8080
host 192.166.1.101
nat (inside,outside) static 192.166.1.101 service tcp 8080 http
```

DNAT

In the example bellow, the subnet will be on a port channel named inside2 and will have a obj-group called net-local2

```
interface port-channel 150
nameif inside2
security-level 100
ip address 172.10.10.0 255.255.255.0
```

```
object-group network net-local2
network-object 172.10.10.0 255.255.255.0
```

after-auto Inserts the rule at the end of section.
You can translate all addresses on the source interface by specifying source dynamic any mapped_obj

```
nat (inside2,outside) after-auto source dynamic net-local2 interface dns
```

PAT connections will be visible in ***show xlate***

> fw1# show xlate
> TCP PAT from inside2:172.10.10.11/51995 to outside:199.199.199.100/51995 flags riD
> idle 0:05:37 timeout 0:00:30

For more advanced configs, refer to article below:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa-command-reference/I-R/cmdref2/n.html

Configuring Static PAT as a Twice NAT/Manual NAT

```
object network local-192.168.1.100
host 192.168.1.100

object network external-2.2.2.2
host 2.2.2.2

object service https
service tcp source eq https

object service tcp_8443
service tcp source eq 8443

nat (inside,outside) source static local-192.168.1.100 external-2.2.2.2 service tcp_8443 https
```

DHCP Server

```
dhcpd address 10.20.106.240-10.20.106.253 inside
dhcpd dns 8.8.8.8 8.8.4.4
dhcpd enable inside
```

ASDM

```
asdm image disk0:/asdm-X.bin
```

```
http server enable 8080
http <whitelist-ip> 255.255.255.0 OUTSIDE
```

```
username admin password PASSWORD privilege 15
```

```
https://<asa ip>:8080
```

Allow non-connected subnets

```
arp permit-nonconnected
```

The ASA ARP cache only contains entries from directly-connected subnets by default. You can enable the ARP cache to also include non-directly-connected subnets. We do not recommend enabling this feature unless you know the security risks. This feature could facilitate denial of service (DoS) attack against the ASA; a user on any interface could send out many ARP replies and overload the ASA ARP table with false entries.

You may want to use this feature if you use:

- Secondary subnets.
- Proxy ARP on adjacent routes for traffic forwarding.

Route LAN to remote subnet on physical port

```
interface GigabitEthernet1/8
 description remote
 no nameif
 no security-level
 no ip address

interface GigabitEthernet1/8.100
 description Public VLAN 100 remote
 vlan 100
 nameif remote
 no security-level
 ip address 192.168.1.2 255.255.255.0

object network local-net
 subnet 192.168.2.0 255.255.255.0

object network remote-net
 subnet 192.168.3.0 255.255.255.0

access-list inbound extended permit ip object local-net object remote-net
nat (inside,remote) source static local-net local-net destination static remote-net remote-net

route remote 192.168.3.0 255.255.255.0 192.168.1.1 1
```

> In this example you will be able to connect to "192.168.3.0/24" from your local "192.168.2.0/24" subnet using the 192.168.1.2 port, the remote port will be on the same vlan using the IP 192.168.1.1

Object Groups ASA

```
object-group service http-https tcp
port-object eq www
port-object eq https
```

```
object-group network webservers
network-object host 192.168.1.101
network-object host 192.168.1.102
```

```
network-object host 192.168.1.103
```

```
access-list OUTSIDE-IN extended permit tcp any object-group webservers object-group http-https
access-group OUTSIDE-IN in interface outside
```

packet-tracer

```
packet-tracer input inside icmp 192.168.1.100 8 0 8.8.8.8
packet-tracer input outside tcp 8.8.8.8 80 192.168.1.100 80
```

Backup/Restore

Create a Backup

```
copy running-config disk0:/backup-2017-00-00
```

Restore a backup

```
copy disk0:/backup-2017-08-18 startup-config
reload
```

Allow FTP passive ports

The firewall will block this data communication because it will start from a different source port (20 instead of 21). The purpose therefore of the inspect ftp command on the Cisco ASA is to listen for the initial Command FTP traffic (on port 21) and dynamically open a secondary Data connection between FTP server and client (from port 20). This will allow FTP communication to work. If you disable FTP inspection with the no inspect ftp command, outbound users can start connections only in passive mode, and all inbound FTP is disabled.

```
policy-map global_policy
 class inspection_default
  no inspect ftp
```

Mitigating attack traffic

DEFINE TRAFFIC

First of all we define which traffic the MPF policy will be applied to. In the example below we exclude the host 8.8.8.8 whilst inspecting all other traffic.

```
access-list mpf-policy-acl extended permit ip any any
```

CREATE CLASS-MAP

Next we assign the previously created access-list to a class-map.

```
class-map mpf-policy
match access-list mpf-policy-acl
```

CREATE POLICY-MAP

Then a policy-map is created and the necessary connection limits defined.

```
policy-map mpf-policy-map
class mpf-policy
set connection conn-max 9500
set connection embryonic-conn-max 5000
set connection per-client-embryonic-max 100
set connection per-client-max 300
```

Allow LAN management over VPN

```
management-access inside
nat (inside,any) source static obj-LANSUBNET obj-LANSUBNET destination static obj-VPNSUBNET obj-VPNSUBNET
route-lookup
http <VPNSUBNET> 255.255.255.0 inside
ssh <VPNSUBNET> 255.255.255.0 inside
```

Failover

To run on the Standby FW

```
failover active
```

Licensing Info

Different ASA models have different licensing options. To see what the limits of the active license, use the following:

```
sh version
```

Links

https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-command-reference-list.html

https://wiki.myhypervisor.ca/books/networking/page/cisco-asa-site-to-site

https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html

https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-configuration-examples-list.html

Revision #33
Created 29 June 2017 01:51:07 by Dave
Updated 13 February 2020 03:44:07 by Dave