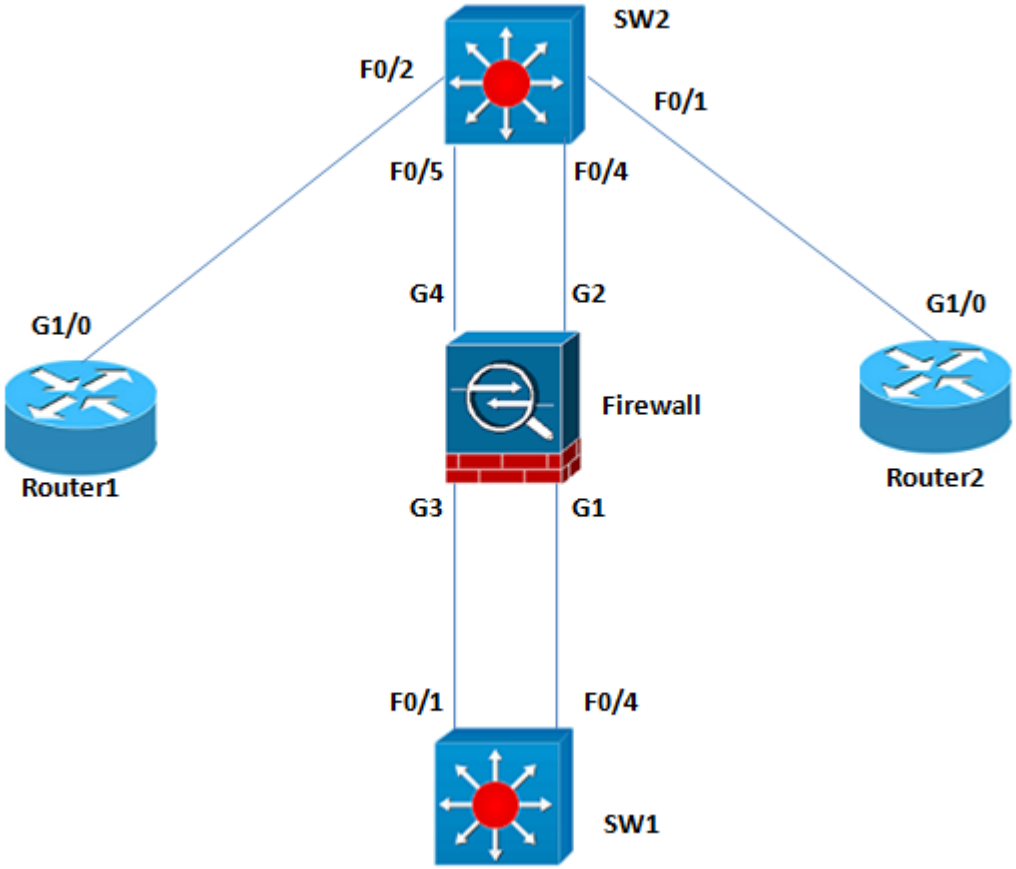
ASA Interface High Availability

Platform: https://racks.uninets.com
Lab Name: CCNP Security SENSS

Topology

ASA Interface High Availability



TASK

- Configure the above topology which meets the following requirements
- Configure ASA1 as follows

Hostname	Interface	Interface-mode	Nameif	Security-level	IP Address
ASA1	G1 and G3	Active-standby	inside	100	10.0.0.10/24
ASA1	G2 and G4	Active-Active	outside	0	20.0.0.10/24

- Allow no more than two interfaces in the bundle and load balance traffic on the ASA based layer3/layer4 information.
- Configure the IP addresses as per the topology with Router number in the last octet. For example: Router-1 IP address is 10.0.0.1/24
- Enable telnet on all routers, so it can be accessible directly into privilege level 15 without any authentication.
- All interfaces on SW1 are in vlan 10 and all interfaces on SW2 are in vlan 20.
- Router-1 should telnet to Router-2
- Use only static routing if required
- Do not use access-list for this task
- Unnecessary broadcasts are not allowed on any link and network should converge as fast as possible.

Explanation

ASA supports interface high availability and redundancy when operating in routed mode:

- In active-standby mode, where one interface is actively forwarding traffic and one interface is in standby mode; this is the redundancy feature.
- In active-active mode, where up to eight interfaces can be actively used for traffic forwarding, sharing the load; this is the ether channel feature.

A logical redundant interface is a pair of one active and one standby physical interface. When the active interface fails, the standby interface becomes active. From the perspective of the firewall applications, this event is completely transparent, because the interface pair is viewed as a single logical interface.

Notice that this method has a limitation; the detection of interface failure is based on simple physical monitoring. When the primary interface loses a carrier, it is declared as failed.

The logical redundant interface will take the MAC address of the first interface added to the group, because this will also become the active interface. This MAC address is not changed with the member interface failures, but changes when you swap the order of the physical interfaces added to the pair; optionally, a vMAC can be configured for the redundant interface. With redundant interfaces, the name if, security-level, and IP address configuration is done at the logical interface level. This feature is not pre-emptive; for example, if the initial active interface failed and the standby interface became active, when the initial active interface became up again, it would remain in standby state. The active interface can be changed at any time using the command redundant-interface.

redundant<nr> active-member <interface> .

Starting with code version 8.4(1), LACP/802.3ad support was added to the ASA; this is an enhancement to the redundant interface function, because all interfaces within a group (up to eight) can actively forward traffic. ASA supports both active and passive modes, where active initiates the LACP negotiation, and passive expects to receive LACP negotiations. Optionally, the ether channel can be configured in on mode, also known as static mode,

because there is no negotiation of the ether channel state between peers. The same restrictions as configuring ether channels on IOS code apply as well; all interfaces must be of same type and speed and use the same configuration. By default, ASA will load-balance the traffic across ether channel interfaces based on layer3 information. Optionally, layer2 andlayer4 can be taken into consideration, and this is configurable on a per-ether channel level. The logical port channel interface will take the MAC address of the lowest number interface from the group; optionally, a vMAC can be configured for the ether channel interface.

Configuration

SW1:

```
Spanning-tree mode rstp
!
 Vtp mode transparent
 Vlan 10
!
 Interface range Fa0/1 , Fa0/4
 Switchport mode access
 Switchport access vlan 10
 Spanning-tree portfast
```

```
!
 Interface Fa0/2
 Switchport mode access
 Switchport access vlan 10
 Spanning-tree portfast
!
```

SW2:

```
!
 Spanning-tree mode rstp
!
 Vtp mode transparent
 Vlan20
!
 Interface Fa0/1
 Switchport mode access
 Switchportaccess vlan 20
 Spanning-tree portfast

!

 Interface range fa0/4 , fa0/5
 Channel-group 1 mode on
 No shutdown
!
 Interface port-channel 1
 Switchport mode access
 Switchport access vlan 20
!
```

Router1:

```
interface GigabitEthernet1/0
 Ip address 10.0.0.1 255.255.255.0
!
 linevty 0 4
 privilege level 15
 no login
!
 ip route 20.0.0.0 255.255.255.0 10.0.0.10
!
```

Router2:

```
interface GigabitEthernet1/0
 ip address 20.0.0.2 255.255.255.0
!
 linevty 0 4
 privilege level 15
 no login
!
 ip route 10.0.0.0 255.255.255.0 20.0.0.10
!
```

Firewall:

```
Interface GigabitEthernet1
nonameif
no security-level
noip address
!
interface GigabitEthernet2
channel-group 1 mode on
nonameif
no security-level
noip address
!
interface GigabitEthernet3
nonameif
no security-level
noip address
!
interface GigabitEthernet4
channel-group 1 mode on
nonameif
no security-level
noip address
!
interface GigabitEthernet5
shutdown
nonameif
no security-level
noip address
!
interface Redundant1
member-interface GigabitEthernet1
member-interface GigabitEthernet3
nameif inside
security-level 100
ip address 10.0.0.10 255.255.255.0
!
interface Port-channel1
lacp max-bundle 2
port-channel load-balance src-dst-ip-port
nameif outside
security-level 0
ip address 20.0.0.10 255.255.255.0!
!
```

Verification

Check nameif and IP addressing on Firewall

```
ASA1# sh nameif
Interface                  Name                       Security
Port-channel1              outside                      0
Redundant1                 inside                     100
ASA1# sh ip add
ASA1# sh ip address
System IP Addresses:
Interface                  Name                       IP address      Subnet mask
Method
Port-channel1              outside                    20.0.0.10       255.255.255.0
manual
Redundant1                 inside                     10.0.0.10       255.255.255.0
manual
Current IP Addresses:
Interface                  Name                       IP address      Subnet mask
Method
Port-channel1              outside                    20.0.0.10       255.255.255.0
manual
Redundant1                 inside                     10.0.0.10       255.255.255.0
manual
```

Check redundant, ether-channel and ether-channel load-balancing configurations on Firewall

```
ASA1# sh interface redundant 1 | be Redundancy
  Redundancy Information:
        Member GigabitEthernet1(Active), GigabitEthernet3
        Last switchover at 14:26:08 UTC Jul 26 2014
ASA1# sh port
ASA1# sh port-channel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        U - in use      N - not in use, no aggregation/nameif
        M - not in use, no aggregation due to minimum links not met
        w - waiting to be aggregated
Number of channel-groups in use: 1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(U)              -      Gi2(P)   Gi4(P)
ASA1# sh port-channel 1 load-balance
EtherChannel Load-Balancing Configuration:
        src-dst-ip-port

EtherChannel Load-Balancing Addresses UsedPer-Protocol:
Non-IP: Source XOR Destination MAC address
  IPv4: Source XOR Destination IP address and TCP/UDP (layer-4) port number
  IPv6: Source XOR Destination IP address and TCP/UDP (layer-4) port number
ASA1# sh port-channel 1 br
Ports: 2   Maxports = 16
Port-channels: 1 Max Port-channels = 48
Protocol: ON
Minimum Links: 1
Load balance: src-dst-ip-port
```

Check connectivity with the redundant interface and check that the assigned MAC is the one of the active interface, the one first attached in the group:

```
Router1#ping 10.0.0.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/13/20 ms
```

```
Router1#sh iparp
Protocol  Address        Age (min)  Hardware Addr   Type   Interface
Internet  10.0.0.10             56   00ab.381d.c501  ARPA   GigabitEthernet1/0
Internet  10.0.0.1               -   ca0b.10bc.001c  ARPA   GigabitEthernet1/0
Router1#
```

```
ASA1# shint g1 | in MAC

     MAC address 00ab.381d.c501, MTU not set

ASA1# shint g3 | in MAC

     MAC address 00ab.381d.c503, MTU not set
```

Verify connectivity with the ether-channel interface and that the assigned MAC is the one from the lowest interface in the group:

```
Router2#ping 20.0.0.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/33/56 ms
Router2#sh iparp
Protocol  Address        Age (min)  Hardware Addr   Type   Interface
Internet  20.0.0.2               -   ca0c.10bc.001c  ARPA   GigabitEthernet1/0
Internet  20.0.0.10             54   00ab.381d.c502  ARPA   GigabitEthernet1/0
```

```
ASA1# shint g2 | in MAC
     MAC address 00ab.381d.c502, MTU 1500
ASA1# shint g4 | in MAC
     MAC address 00ab.381d.c504, MTU 1500
ASA1#
```