# Fail Over IPSec Site-to-site VPN With Dual WAN Links and IP SLA on Cisco ASA

## 1. Overview:

In some environments of site-to-site IPSec VPN, it is required to guarantee the up time of the VPN connection. To serve this objective, we can use WAN redundancy links with IP SLA tracking to automatically switch over the VPN connection from one ISP to another ISP.

In this article will show how to configure site-to-site IPSec VPN on Cisco ASA firewalls IOS version 9.x over two WAN links with IP SLA tracking to have redundancy connection between two office locations.

## 2. Prerequisites:

To start this configuration, it is supposing that:

Download lab and Task from eve-nglab.com

Setup Ram in Platfrom: **At least 8GB**

ASA will ask password: Just **Enter**

Note: you will get that log:

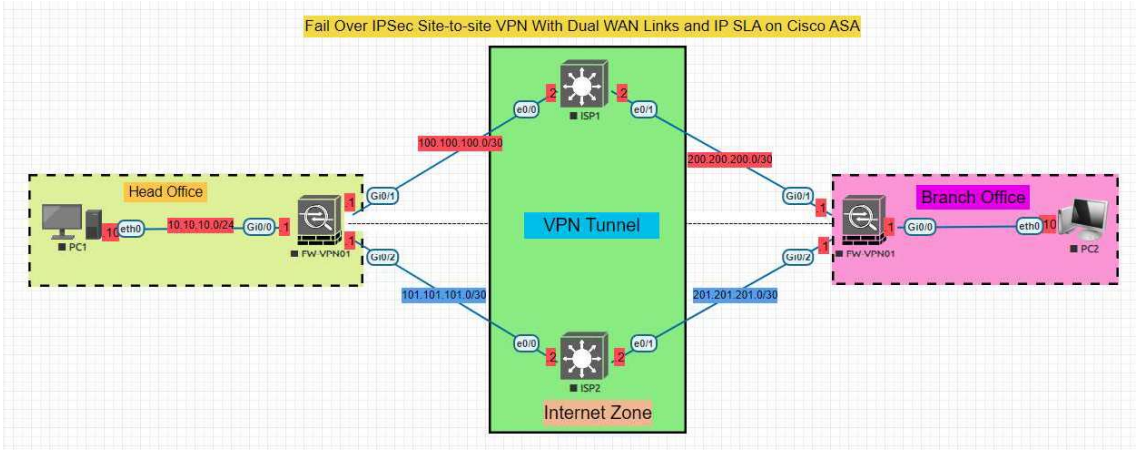
Warning: ASAv platform license state is Unlicensed.

Install ASAv platform license for full functionality.

=> **Just skip it, it will not impact to the lab**

## 3. Lab Scenario Setup:

To demonstrate configuring IPSec VPN site-to-site with IP SLA tracking the availability of WAN links on Cisco ASA firewall with IOS, we will set up a EVE-NGLab Platfrom as the following diagram.




There are two Cisco ASA firewall appliances. FW-VPN01 locates in Head Office and FW-VPN02 locates in Branch Office. There is two routers act as two different internet connection for dual WAN redundancy.

## 4. Configuration and Verification:

### 4.1 IP addressing:

On PC1

```
PC1> ip 10.10.10.10/24 10.10.10.1

Checking for duplicate address...

PC1 : 10.10.10.10 255.255.255.0 gateway 10.10.10.1


PC1> save

Saving startup configuration to startup.vpc

.  done
```

On PC2

```
PC2> ip 20.20.20.10/24 20.20.20.1

Checking for duplicate address...

PC1 : 20.20.20.10 255.255.255.0 gateway 20.20.20.1
```

```
PC2> save
Saving startup configuration to startup.vpc
.  done
```

**On FW-VPN01**

```
int g0/0
   no sh
   ip add 10.10.10.1 255.255.255.0
   security-level 100
   nameif inside
int g0/1
   no sh
   ip add 100.100.100.1 255.255.255.252
   security-level 0
   nameif outside-isp01
int g0/2
    no sh
    ip add 101.101.101.1 255.255.255.252
    security-level 0
    nameif outside-isp02
policy-map global_policy
   class inspection_default
      inspect icmp
      inspect icmp erro
```

**On Internet router of ISP1**

```
int E0/0
   no sh
   ip add 100.100.100.2 255.255.255.252
int E0/1
   no sh
   ip add 200.200.200.2 255.255.255.252
```

**On Internet router of ISP02**

```
int E0/0
    no sh
    ip add 101.101.101.2 255.255.255.252
int E0/1
    no sh
    ip add 201.201.201.2 255.255.255.252
```

**On FW-VPN02**

```
int g0/0
   no sh
   ip add 20.20.20.1 255.255.255.0
   nameif inside
int g0/1
   no sh
   ip add 200.200.200.1 255.255.255.252
```

```
   nameif outside-isp01
int g0/2
   no sh
   ip add 201.201.201.1 255.255.255.252
   nameif outside-isp02
policy-map global_policy
   class inspection_default
      inspect icmp
      inspect icmp erro
```

**4.2 Configure IP SLA Tracking And Default Route**

Apply the the following IP SLA tracking and default router configuration on **FW-VPN01**.

```
sla monitor 20
  type echo protocol ipIcmpEcho 100.100.100.2 interface outside-
isp01
  num-packets 3
  frequency 10
sla monitor schedule 20 life forever start-time now
track 1 rtr 20 reachability
route outside-isp01 0.0.0.0 0.0.0.0 100.100.100.2 track 1
route outside-isp02 0.0.0.0 0.0.0.0 101.101.101.2 2
```

Apply the the following IP SLA tracking and default router configuration on **FW-VPN02**.

```
sla monitor 20
   type echo protocol ipIcmpEcho 200.200.200.2 interface outside-
isp01
```

```
   num-packets 3

   frequency 10

sla monitor schedule 20 life forever start-time now

track 1 rtr 20 reachability

route outside-isp01 0.0.0.0 0.0.0.0 200.200.200.2 track 1

route outside-isp02 0.0.0.0 0.0.0.0 201.201.201.2 2
```

Now both FW-VPN01 and FW-VPN02 should be able to ping their public IP each other via ISP01 connection.

```
FW-VPN01# show route


Codes: C - connected, S - static, I - IGRP, 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, E - EGP

       i - IS-IS, 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 100.100.100.2 to network 0.0.0.0


C    100.100.100.0 255.255.255.252 is directly connected, outside-
isp01
```