

Meraki site to site VPN to Cisco IOS CSR1000v

1. Topology



2. Configuration the Meraki MX80 Site to Site VPN

There are not a lot of IPsec options within the Dashboard for this, this is the IKEv1 configuration I used:

Choose a Preset

Phase 1

Encryption

Authentication

Diffie-Hellman group

Lifetime (seconds)

Phase 2

Encryption

Authentication

PFS group

Lifetime (seconds)

The other settings to allow internal networks 10.0.250.0/24, 10.0.251.0/24 and 10.0.252.0/24 towards 10.10.10.0/24 on the remote site, are:

Non-Meraki VPN peers

Name	IKE Version ^{BETA}	IPsec policies	Public IP	Local ID	Remote ID	Private subnets	Preshared secret	Availability
192.168.3.71	IKEv1	Custom	192.168.3.71	192.168.100.112	192.168.3.71	10.10.10.0/24	---	All networks

[Add a peer](#)

Site-to-site outbound firewall

#	Policy	Protocol	Source	Src port	Destination	Dst port	Comment	Logging	Actions	
1	Allow	Any	10.0.250.0/24	Any	10.10.10.0/24	Any		Enabled	+	X
2	Allow	Any	10.0.251.0/24	Any	10.10.10.0/24	Any		Enabled	+	X
3	Allow	Any	10.0.252.0/24	Any	10.10.10.0/24	Any		Enabled	+	X
	Allow	Any	Any	Any	Any	Any	Default rule	Enabled		

[Add a rule](#)

VERY ANNOYING on OsX: auto-password generation can alter your VPN password in the web-GUI!

3. Configuration on IOS

ISAKMP / IKE:

```
crypto isakmp policy 10  
encr 3des
```

Meraki site to site VPN to Cisco IOS CSR1000v

```
authentication pre-share
group 2
lifetime 28800
crypto isakmp key test123 address 192.168.100.114
```

IPset / Phase 2:

```
crypto ipsec transform-set MYSET esp-3des esp-sha-hmac
mode tunnel
!
!
!
crypto map to-mx 1 ipsec-isakmp
set peer 192.168.100.114
set transform-set MYSET
match address 110
```

The ACL 110:

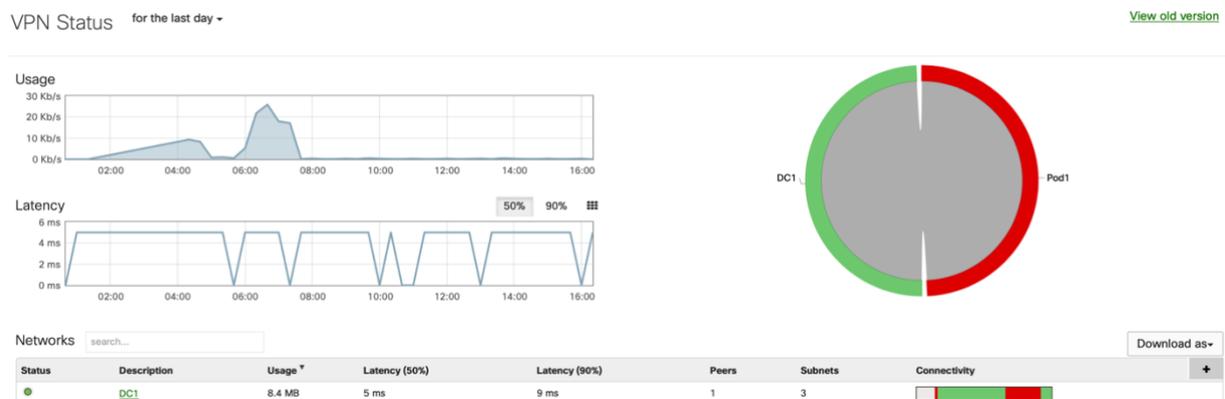
```
access-list 110 permit ip 10.10.10.0 0.0.0.255 10.0.250.0 0.0.0.255
access-list 110 permit ip 10.10.10.0 0.0.0.255 10.0.251.0 0.0.0.255
access-list 110 permit ip 10.10.10.0 0.0.0.255 10.0.252.0 0.0.0.255
```

And the application to the interface:

```
interface GigabitEthernet1
ip address 192.168.3.71 255.255.255.0
crypto map to-mx
```

4. Verification and monitoring

The dashboard could do with some more monitoring facilities. Under ORGANIZATION → MONITOR → VPN status, you can see this:



The red VPN “Pod1” was unavailable at the time, the DC1 is the one that is “up”.

Your best bet for troubleshooting is the event – log:

Meraki site to site VPN to Cisco IOS CSR1000v

Event log

Client: Before: (PST)

Event type include: Event type ignore:

[Reset filters](#)

Download as ▾

Time (PST) ▼	Client	Event type	Details
Nov 4 00:25:10	Non-Meraki / Client	VPN negotiation	msg: IPsec-SA established: ESP/Tunnel 192.168.100.114[500]->192.168.3.71[500] spi=264230983(0xfbfd847)
Nov 4 00:25:10	Non-Meraki / Client	VPN negotiation	msg: IPsec-SA established: ESP/Tunnel 192.168.100.114[500]->192.168.3.71[500] spi=175804180(0xa7a8f14)
Nov 4 00:25:10	Non-Meraki / Client	VPN negotiation	msg: ISAKMP-SA established 192.168.100.114[500]-192.168.3.71[500] spi:3bc15e09d881d0bb:9343fd4c9aed9d24

On the IOS side, of course there are more facilities:

```
csr1000v1# show crypto isakmp sa
```

```
IPv4 Crypto ISAKMP SA
```

```
dst          src          state          conn-id status
192.168.100.114 192.168.3.71  QM_IDLE          1024 ACTIVE
```

```
csr1000v1# show crypto ipsec sa
```

```
interface: GigabitEthernet1
```

```
  Crypto map tag: to-mx, local addr 192.168.3.71
```

```
[...]
```

```
  local ident (addr/mask/prot/port): (10.10.10.0/255.255.255.0/0/0)
  remote ident (addr/mask/prot/port): (10.0.252.0/255.255.255.0/0/0)
  current_peer 192.168.100.114 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 169, #pkts encrypt: 169, #pkts digest: 169
    #pkts decaps: 200, #pkts decrypt: 200, #pkts verify: 200
```

And then there is “`debug crypto isakmp`” for the not so faint at heart, as it seems to be designed NOT to help you with any usable information.

And of course the proof is in the pudding:

```
csr1000v1# ping 10.0.251.11 source 10.10.10.10
Packet sent with a source address of 10.10.10.10
!!!!!!
```

5. Important notes

-This configuration was done using IKEv1, which is not available through NAT. ☹

The two devices here were simply routed. Be aware..

You are likely to need IKEv2.

-Using 3DES was of course not advisable for production environments, once you get the VPN to work you can increase the security on it.

-Was this a headache to setup?.. well.. IPsec usually is and despite that I got it to work before hanging myself, IPsec is NEVER cooperative. But it worked never the less.

-I did not get IKEv2 working yet from the MX to IOS. That could very well be my ignorance, but... since the Dashboard says that IKEv2 is in “Beta” (!), I think this is pretty strange. IKEv2 has been around for ages and is THE requirement to get IPsec working in a NAT environment. Strange. ☹

Meraki site to site VPN to Cisco IOS CSR1000v

The event-log displayed: msg: invalid flag 0x08, which apparently is indicative that there is an IKE version mismatch..

IKEv2 supported on MX appliances running firmware 15.12 or higher, so I did an upgrade to a Beta version on the MX.. ☹ ☹.

Screenshot of the Meraki firmware upgrade scheduling interface. The title is "Schedule firmware change". Below the title, it asks "When should this firmware be installed?" and includes a note: "Upgrade times may be staggered depending on the number of devices changing firmware." There are two radio button options: "Perform the upgrade now" (which is selected) and "Schedule the upgrade for:". Under the second option, there is a date field showing "11/04/2020" and a time field showing "11:00" with "(network local time)" next to it. At the bottom right, there are "Back" and "Next" buttons.

→ the upgrade will be scheduled “5 minutes from now”, in case you change your mind.

Screenshot of the Meraki upgrade confirmation window. The title is "5 minutes from now · Nov 4 at 10:38 AM CET". Below the title, it says "Scheduled by Pim Leemans on 10:33 AM CET". There is a section for "Upgrading to MX 15.39" with a note: "[Important Notice] This is a beta version for the next major MX release. Due to this, we recommend taking additional" and a "Read more" link. To the right, it says "1 MX network (1 security appliance)" and "DC1". At the bottom left, there is a "CANCEL" button, and at the bottom right, there is a "RESCHEDULE" button.

And after a few minutes:

Scheduled changes

Screenshot of the Meraki "Upgrading now" notification. It says "Upgrading now by Pim Leemans" and "DC1 to MX 15.39". There is a calendar icon to the right.

Note that DES is no longer supported in 15.x. ☹ ☹ ☹ That may sound “safer”.. but if you have to connect via an IPsec via to legacy endpoints, you are SCREWED!

Note: “The latest beta firmware is fully supported by our Support and Engineering teams. Older betas are supported with best effort; an upgrade to the latest beta will ensure full support.”

As I was waiting for the upgrade.. the message appeared: “Restricted from versions 15.0 and higher”.

This very cryptic message apparently means that the MX80 can NOT run version 15.0+. Hmm.. strange as the “Upgrading now” window still appears. Then that windows disappeared after a while as well.

So the end of the story is: Firmware <15.x which is still in Beta does NOT support IKEv2. And it seems.. like my MX80 never will. Boy this sucks.