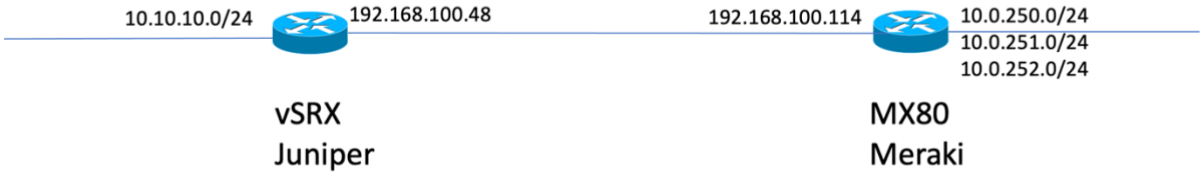
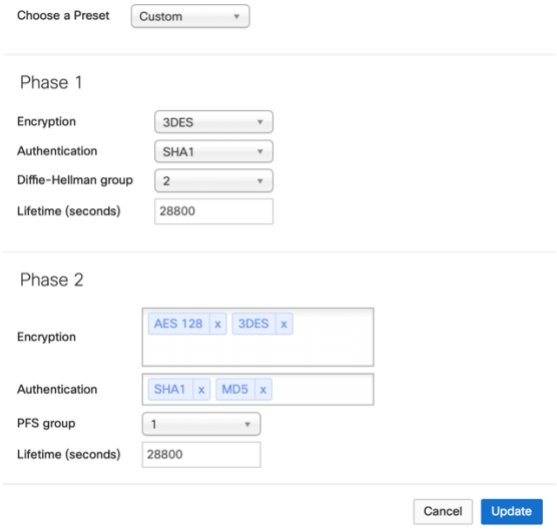
Meraki site to site VPN to Cisco IOS vSRX

1. Topology

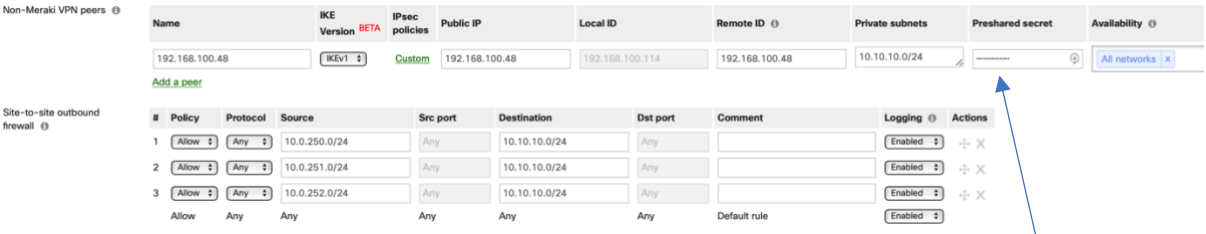


2. Configuration the Meraki MX80 Site to Site VPN

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



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:



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

3. Configuration on the Juniper SRX

ISAKMP / IKE Phase 1:

```
lab@vsrx1# show security ike
proposal isakmp-proposal {
    authentication-method pre-shared-keys;
```

```
    dh-group group2;
    authentication-algorithm sha1;
    encryption-algorithm 3des-cbc;
    lifetime-seconds 28800;
}
policy isakmp-policy {
    proposals isakmp-proposal;
    pre-shared-key ascii-text "$9$x4d7wgGUHm5FiktuB1hcwY2"; ## SECRET-DATA
}
gateway phase1-to-cisco {
    ike-policy isakmp-policy;
    address 192.168.100.114;
    external-interface ge-0/0/4.0;
    version v1-only;
```

IPset / Phase 2:

```
proposal ipsec-proposal {
    protocol esp;
    authentication-algorithm hmac-md5-96;
    encryption-algorithm aes-128-cbc;
    lifetime-seconds 28800;
}
policy ipsec-policy {
    perfect-forward-secrecy {
        keys group1;
    }
    proposals ipsec-proposal;
}
vpn phase2-to-cisco {
    bind-interface st0.0;
    ike {
        gateway phase1-to-cisco;
        ipsec-policy ipsec-policy;
```

Since this is a Routed VPN, make sure you create the proper routes:

```
lab@vsrx1# top show routing-options
static {
    route 10.0.251.0/24 next-hop st0.0;
    route 10.0.252.0/24 next-hop st0.0;
    route 10.0.250.0/24 next-hop st0.0;
```

I have applied the st0.0 interface to a zone “VPN”, and the Lo0.0 interface to a zone “dmz”, and of course created a security policy to allow traffic to flow from dmz → vpn.

4. Verification and monitoring

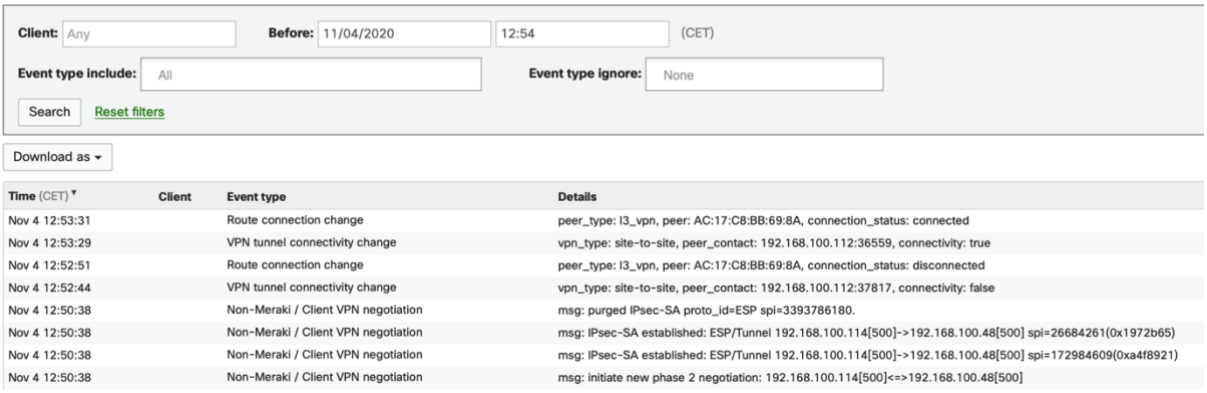
The dashboard could do with some more monitoring facilities. Under ORGANIZATION → MONITOR → VPN status, you can see this:

Meraki site to site VPN to Cisco IOS vSRX

The DC1 VPN is the one that is “up” and used.

Your best bet for troubleshooting within the dashboard is the event – log:

Event log



Time (CET)	Client	Event type	Details
Nov 4 12:53:31		Route connection change	peer_type: l3_vpn, peer: AC:17:C8:BB:69:8A, connection_status: connected
Nov 4 12:53:29		VPN tunnel connectivity change	vpn_type: site-to-site, peer_contact: 192.168.100.112:36559, connectivity: true
Nov 4 12:52:51		Route connection change	peer_type: l3_vpn, peer: AC:17:C8:BB:69:8A, connection_status: disconnected
Nov 4 12:52:44		VPN tunnel connectivity change	vpn_type: site-to-site, peer_contact: 192.168.100.112:37817, connectivity: false
Nov 4 12:50:38		Non-Meraki / Client VPN negotiation	msg: purged IPsec-SA proto_id=ESP spi=3393786180.
Nov 4 12:50:38		Non-Meraki / Client VPN negotiation	msg: IPsec-SA established: ESP/Tunnel 192.168.100.114[500]->192.168.100.48[500] spi=26684261(0x1972b65)
Nov 4 12:50:38		Non-Meraki / Client VPN negotiation	msg: IPsec-SA established: ESP/Tunnel 192.168.100.114[500]->192.168.100.48[500] spi=172984609(0xa4f8921)
Nov 4 12:50:38		Non-Meraki / Client VPN negotiation	msg: initiate new phase 2 negotiation: 192.168.100.114[500]<=>192.168.100.48[500]

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

```
lab@vsrx1# run show security ike security-associations
Index   State  Initiator cookie  Responder cookie  Mode Remote Address
51983   UP     781c05902f635326  579c4ddeae5d69fd  Main 192.168.100.114

lab@vsrx1# run show security ipsec security-associations
  Total active tunnels: 1
  ID    Algorithm               SPI      Life:sec/kb  Mon lsys    Port   Gateway
  <131073 ESP:aes-cbc-128/md5 9c1e8848   27254/unlim - root        500    192.168.100.114
  >131073 ESP:aes-cbc-128/md5 48713e     27254/unlim - root        500    192.168.100.114
```

And of course the proof is in the pudding:

```
vsrx1# ping 10.0.251.11 source 10.10.10.10
Packet sent with a source address of 10.10.10.10
!!!!!
```

And on the SRX you can create logfiles full of useless messages. (well.. some of them are usefu but it usually looks like a needle in a haystack)

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 is 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?..
With all the debugging possibilities on the SRX.. it was doable.

6. IKEv2 and an IPsec tunnel

After I was able to borrow a very recent MX67, I upgraded to the Beta firmware 15.39 which supports IKEv2.

I had no luck with IKEv2 so far however. Sigh..