Per far funzionare una VPN IPSEC l2l tra Ubiquiti e Fortigate

- il **Fortigate** ha bisogno di:

1. setup VPN
    - oltre alle cose “ovvie” o solite, SERVE lasciare VUOTO il campo *local ID*
2. FIREWALL POLICY da/per interfaccia del tunnel sulla SUA “MADRE” (dove arriva il pacchetto, interfaccia IP)
    - sono in pratica le acl che vengono “scambiate” per far funzionare il tunnel
3. le normali *firewall policy* del traffico che ti interessa
4. le rotte statiche per indirizzare il traffico che interessa
5. è più comodo usare un *address group* che raccoglie i vari address delle sottoreti
    - ATTENZIONE! Per poter selezionare gli address nei tunnel, ho dovuto creare gli oggetti da lì, quelli creati normalmente **non** appaiono nell'elenco!
6. ho creato un address group unico “per tunnelizzare tutto sulle VPN” da usare per tutti

- Lato **Ubiquiti** permette un solo prefix per tunnel, per cui anche lato Fortigate ho messo più phase 2

Test in gennaio 2023 avevano dato circa **150-160 Mb con 3des-sha1**, e circa 40 Mb con aes256-sha256.

Da notare che per ITIS è stato necessario abbassare l'MTU del tunnel sul Fortigate dall'auto-calcolato 1420 a 1418, supponiamo sia per il fatto di aver usato VLAN TAGGED per la LAN. Da notare anche che gli AP in modalità campus (ci risulta facciano un GRE per WLAN) avevano problemi, messi in RAP (un unico? ipsec) tutto ok. I sintomi sia per LAN che AP erano navigazione a singhiozzo! Alcuni siti si raggiungevano altri no!

- template lato Ubiquiti:

```
vpn {
    ipsec {
        allow-access-to-local-interface disable
        auto-firewall-nat-exclude disable
        disable-uniqreqids
        esp-group mioesp {
            compression disable
            lifetime 1800
            mode tunnel
            pfs dh-group19
            proposal 1 {
                encryption aes256
                hash sha256
            }
        }
        ike-group mioike {
            dead-peer-detection {
                action restart
                interval 30
```

```
                timeout 60
            }
            ikev2-reauth no
            key-exchange ikev1
            lifetime 28800
            proposal 1 {
                dh-group 19
                encryption aes256
                hash sha256
            }
        }
        ipsec-interfaces {
            interface eth0
        }
        nat-traversal disable
        site-to-site {
            peer 172.30.150.13 {
                authentication {
                    mode pre-shared-secret
                    pre-shared-secret ****************
                }
                connection-type initiate
                default-esp-group mioesp
                ike-group mioike
                ikev2-reauth inherit
                local-address 172.30.150.14
                tunnel 1 {
                    allow-nat-networks disable
                    allow-public-networks enable
                    esp-group mioesp
                    local {
                        prefix 192.168.200.0/24
                    }
                    remote {
                        prefix 0.0.0.0/0
                    }
                }
            }
        }
    }
}
```

Una volta sugli Ubiquiti serviva il “comando segreto” *ip rule delete prio 220* da mettere in rc.local (o qualcosa altro) per farlo sopravvivere ai riavvii adesso pare non servire più.