

Networking

- [Azure to Ubiquiti IPsec](#)
- [Ubiquiti - USG disable NAT](#)
- [tcpdump](#)

Azure to Ubiquiti IPsec

Connecting Azure to on-premises.

After you've created your Azure Virtual Network Gateway log in to your router.

```
set vpn ipsec auto-firewall-nat-exclude enable

set vpn ipsec esp-group FOO0 lifetime 3600
set vpn ipsec esp-group FOO0 pfs disable
set vpn ipsec esp-group FOO0 proposal 1 encryption aes256
set vpn ipsec esp-group FOO0 proposal 1 hash sha1

set vpn ipsec ike-group FOO0 key-exchange ikev2
set vpn ipsec ike-group FOO0 lifetime 3600

! REPLACE "1" IF YOU ALREADY HAVE A PROPOSAL USING THIS IDENTIFIER
set vpn ipsec ike-group FOO0 proposal 1 dh-group 2
set vpn ipsec ike-group FOO0 proposal 1 encryption aes256
set vpn ipsec ike-group FOO0 proposal 1 hash sha1

set vpn ipsec site-to-site peer 22.24.48.131 authentication mode pre-shared-secret
set vpn ipsec site-to-site peer 22.24.48.131 authentication pre-shared-secret SXYHVuH5p4vySL3eeKHEut64m
set vpn ipsec site-to-site peer 22.24.48.131 connection-type respond
set vpn ipsec site-to-site peer 22.24.48.131 description IPsecAzure
set vpn ipsec site-to-site peer 22.24.48.131 ike-group FOO0
set vpn ipsec site-to-site peer 22.24.48.131 local-address 17.15.138.22

!REPLACE "vti0" BY ANOTHER VTI INTERFACE ID IF THIS ONE IS ALREADY USED BY YOUR UBIQUITI DEVICE
set vpn ipsec site-to-site peer 22.24.48.131 vti bind vti0
set vpn ipsec site-to-site peer 22.24.48.131 vti esp-group FOO0
set interfaces vti vti0
set protocols static interface-route 192.168.0.0/22 next-hop-interface vti0

set firewall options mss-clamp interface-type vti
set firewall options mss-clamp mss 1350
```

set system offload ipsec enable

Ubiquiti - USG disable NAT

1. **ssh <adminusername>@<IP of USG LAN>**
2. type **'configure'**
3. type **'show service nat'** #you should see rule 6001, 6002, 6003 by default
4. type **'set service nat rule 6001 disable'** #disables corporate network NAT
5. type **'set service nat rule 6002 disable'** #disables remote user network NAT
6. type **'set service nat rule 6003 disable'** #disables guest network NAT
7. type **'compare'** #just to see if you did things right
8. type **'commit'**
9. type **'save'**
10. type **'mca-ctrl -t dump-cfg > config.gateway.json'**
11. copy this file over to your Unifi controller,
.'scp config.gateway.json root@<controller_IP>:/usr/lib/unifi/data/sites/{ {site folder} }/config.gateway.json'

tcpdump

One-Liners: tcpdump

Helpful tcpdump commands.

Add -v to -vvvv to see from some to a lot of information.

General networking

Get CDP or LLDP information.

```
tcpdump -i enp132s0f0 -v -s 1500 -c 1 '(ether[12:2]=0x88cc or ether[20:2]=0x2000)'
```

Watch DHCP traffic

```
tcpdump -i enp1s0f0 port 67 or port 68 -e -n -vv
```

Show VLAN tags

```
tcpdump -i enp1s0f0 -e vlan -nn
```

Watch for 1 host

```
tcpdump -vvvv -n dst host 10.200.200.13 or src host 10.200.200.13
```