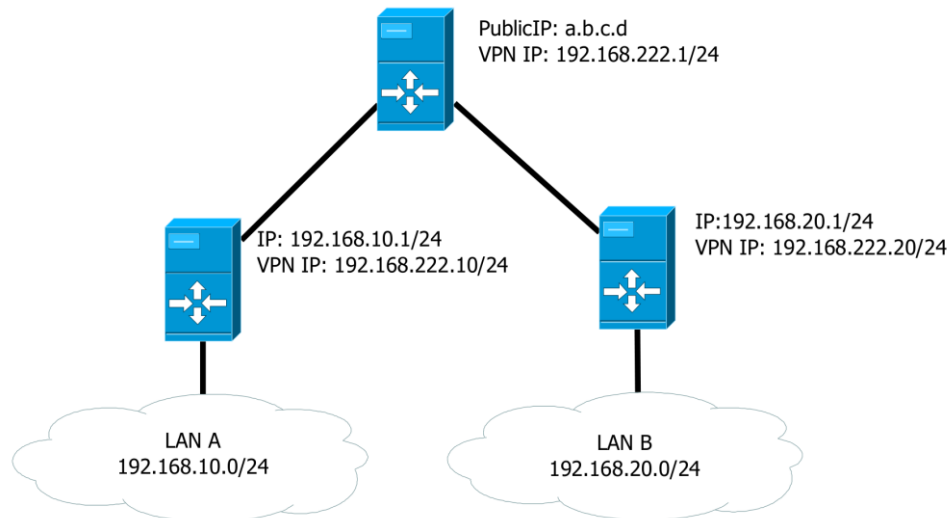


Wireguard



Node A

Interfaces » WG0

General Settings | Advanced Settings | Firewall Settings | Peers

Further information about WireGuard interfaces and peers at wireguard.com

Status: Device: wg0
Uptime: 38.2m 10s
RX: 482.45 KB (1583 Pkts.)
TX: 797.59 KB (2536 Pkts.)
IPv4: 192.168.222.10/24

Protocol: WireGuard VPN

Bring up on boot: ☒

Private Key:
Required: Base64-encoded private key for this interface.

Listen Port: random
Optional: UDP port used for outgoing and incoming packets.

IP Addresses: 192.168.222.10/24
Recommended: IP addresses of the WireGuard interface.

Dismiss Save

Interfaces » WG0

General Settings | Advanced Settings | Firewall Settings | Peers

Further information about WireGuard interfaces and peers at wireguard.com

Description:
Optional: Description of peer.

Public Key:
Required: Base64-encoded public key of peer.

Preshaed Key:
Optional: Base64-encoded preshaed key. Adds in an additional layer of symmetric-key cryptography for post-quantum resistance.

Allowed IPs: 192.168.10.0/24
192.168.222.10/32
192.168.222.1/32
192.168.222.20/32
192.168.20.0/24
Required: IP addresses and prefixes that this peer is allowed to use inside the tunnel. Usually the peer's tunnel IP addresses and the networks the peer routes through the tunnel.

Route Allowed IPs: ☐
Optional: Create routes for Allowed IPs for this peer.

Endpoint Host:
Optional: Host of peer. Names are resolved prior to bringing up the interface.

Endpoint Port:
Optional: Port of peer.

Persistent Keep Alive: 25
Optional: Seconds between keep alive messages. Default is 0 (disabled). Recommended value if this device is behind a NAT is 25.

Delete

allowed ips: 192.168.10.0/24, 192.168.222.10/32, 192.168.222.1/32, 192.168.222.20/32, 192.168.20.0/24

static route: 192.168.20.0/24 via 192.168.222.20 dev wg0

Node B

Interfaces » wg0

General Settings | Advanced Settings | Firewall Settings | Peers

Further information about WireGuard interfaces and peers at [wireguard.com](https://www.wireguard.com) Delete

Description

Public Key

Preshared Key

Allowed IPs

Route Allowed IPs ☐

Endpoint Host

Endpoint Port

Persistent Keep Alive

General Settings

Status Device: wg0
Uptime: 5h 15m 52s
RX: 785.86 KB (1895 Pkts.)
TX: 645.76 KB (2779 Pkts.)
IPv4: 192.168.222.20/24

Protocol WireGuard VPN

Bring up on boot ☒

Private Key

Listen Port

IP Addresses

Peers

Optional. Description of peer.

Optional. Base64-encoded public key of peer.

Optional. Base64-encoded preshared key. Adds in an additional layer of symmetric-key cryptography for post-quantum resistance.

Required. IP addresses and prefixes that this peer is allowed to use inside the tunnel. Usually the peer's tunnel IP addresses and the networks the peer routes through the tunnel.

Optional. Create routes for Allowed IPs for this peer.

Optional. Host of peer. Names are resolved prior to bringing up the interface.

Optional. Port of peer.

Optional. Seconds between keep alive messages. Default is 0 (disabled). Recommended value if this device is

Dismiss Save

allowed ips: 192.168.20.0/24, 192.168.222.20/32, 192.168.222.1/32, 192.168.222.10/32, 192.168.10.0/24

static route: 192.168.10.0/24 via 192.168.222.10 dev wg0

Server

```
~ # cat /etc/wireguard/wg0.conf
```

```
[Interface]
```

```
Address = 192.168.222.1/24
```

```
SaveConfig = true
```

```
PostUp = iptables -A FORWARD -i %i -j ACCEPT; iptables -A FORWARD -o  
%i -j ACCEPT; iptables -t nat -A POSTROUTING -o wg0 -j MASQUERADE
```

```
PostDown = iptables -D FORWARD -i %i -j ACCEPT; iptables -D FORWARD  
-o %i -j ACCEPT; iptables -t nat -D POSTROUTING -o wg0 -j MASQUERADE
```

```
ListenPort =
```

```
PrivateKey =
```

```
[Peer]
```

```
PublicKey =
```

```
AllowedIPs = 192.168.222.10/32, 192.168.10.0/24
```

```
[Peer]
```

```
PublicKey =
```

```
AllowedIPs = 192.168.222.20/32, 192.168.20.0/24
```