Site-to-Site VPN Access with two 63xx Series Routers

6300-CX, 6310-DX, 6330-MX, and 6350-SR

Site-to-Site VPN Access with two 63xx Series Routers

Skill level: ***Expert*** (requires knowledge of IPSec tunnel setup)

Goal

To build an IPSec tunnel through the 63xx router's cellular WAN Internet connection to another 63xx, and use that IPSec tunnel to access endpoints inside a VPN.

Setup

For this setup, you will need two 63xx series routers. Both 63xx routers must be on firmware version 17.5.108.6 or higher. The 63xx series routers will need an active WAN Internet connection.

The main site's 63xx series router will need a publicly reachable IP address, so the remote 63xx series router can reach the IP and build a tunnel.

You will also need to decide on the IPSec credentials and settings needed to build a tunnel between the 63xx series routers.

If configuring a 6300-CX for Site-to-Site VPN Access, it must be in router mode.

Sample

The sample configuration below shows a 6300-CX building a tunnel to a 6350-SR through its cellular modem. The client laptop connected to the LAN Ethernet port of the 6300-CX can then use that IPSec tunnel to access any IP address in the 172.20.1.1/24 range behind the 6350-SR. Any traffic not destined for 172.20.1.1/24 will instead go through the cellular modem straight to the Internet.

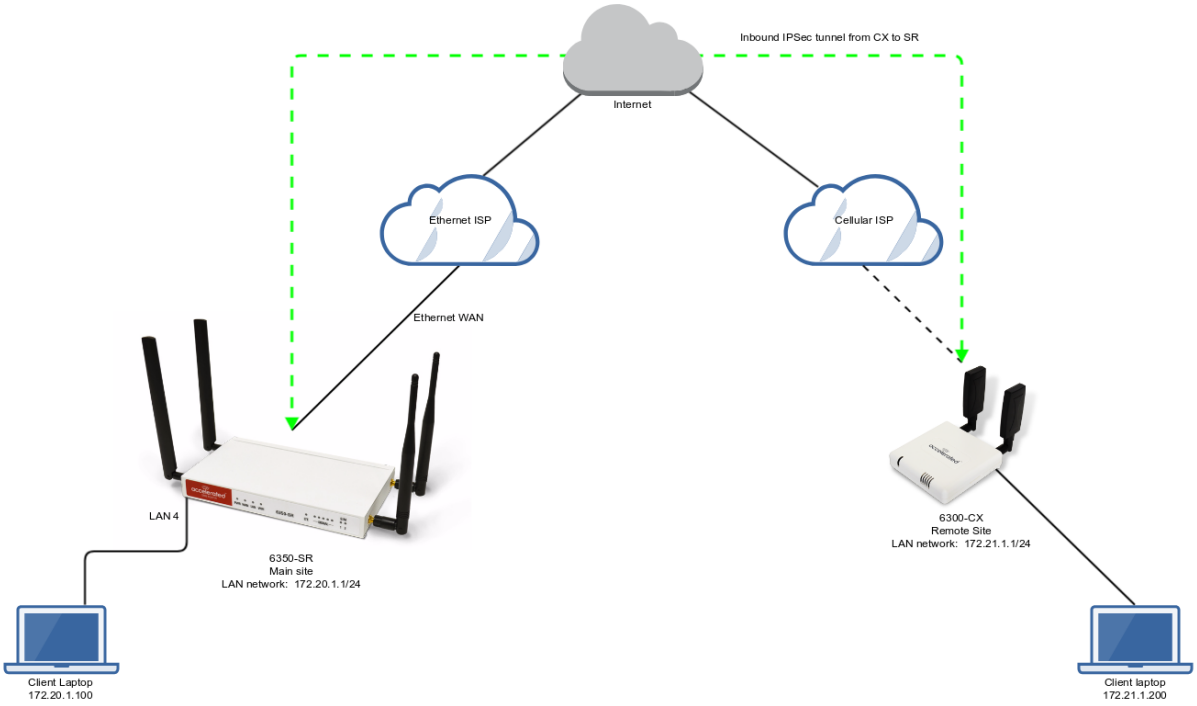
This tunnel will also allow the client laptop connected to the LAN 4 port of the 6350-SR to access any IP address in the 172.21.1.1/24 range behind the 6300-CX. Any traffic not destined for 172.20.1.1/24 will instead go through the Ethernet WAN of the 6350-SR straight to the Internet.

Both the 6350-SR and 6300-CX will need to be configured with a new IPSec tunnel, using matching authentication settings, in order for the 6300-CX to build the tunnel to the 6350-SR. Sample configuration settings for both devices are listed below.

Additional 63xx series routers can build IPSec tunnels to this 6350-SR. Each 63xx series router will need a unique local address range (e.g. 172.21.2.1/24 or 172.21.100.1/24) so the various remote sites do not conflict with each other.

Also, the ***remote network*** and ***NAT*** settings of the main site's 6350-SR will need to be expanded to account for the additional ranges (e.g. 172.21.1.1/16).

NOTE: Be sure a value greater than 0 is specified for the local address ranges' fourth octet (i.e. X.X.X.1/24 is valid, X.X.X.0/24 is not).



6350-SR Sample Configuration

Open the configuration profile for the 6350-SR. Under ***IPSec***, create a new entry titled ***N6300*** (the name is arbitrary), and add your IPSec settings to the new entry. The following settings reflect the sample setup in the diagram above.

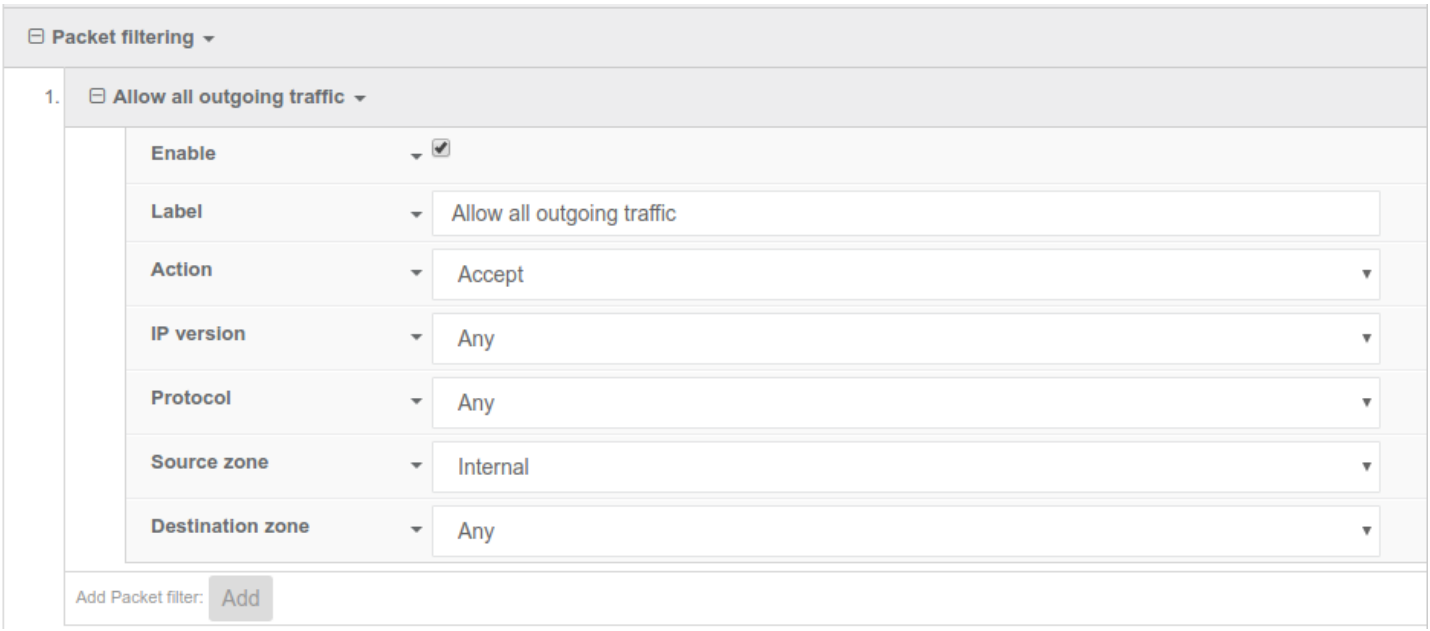
1. Enter in the PSK into the ***Pre-shared key***.
2. Change ***Local endpoint -> ID -> ID type*** to ***Raw***
3. Set the local ID in ***Local endpoint -> ID -> Raw ID Value***, e.g. *@nps*
4. Set ***Local endpoint -> type*** to ***Interface***,and set ***Local endpoint -> Interface*** to ***WAN***, or whichever interface you want to allow the inbound tunnel to connect through.
5. Change ***Remote endpoint -> ID -> ID type*** to ***Raw***
6. Set the remote ID in ***Remote endpoint -> ID -> Raw ID Value***, e.g. *@6300*.
7. Set the ***Remote endpoint -> Hostname*** to ***any***. This allows the 6300-CX to have any IP address. If you know the public IP address of the 6350-CX and wish to lock down the 6350-SR's settings so it only allows inbound tunnels from that IP, input the 6300-CX's public IP address here.
8. Set ***IKE -> Mode*** to ***Aggressive mode***.
9. Uncheck the ***IKE -> Initiate connection*** option.

10. Set *IKE -> Phase 1 Proposals* and *IKE -> Phase 2 Proposals*. In this example, both proposals are set to 3DES, SHA1, MODP1024.
11. Under **NAT**, add a destination that corresponds to the local address range of the *remote* device. (In this example, it'd be 172.21.1.1/24.)

Under *Policies*, click *Add* to create a new policy, and enter the following settings:

1. Set *Policy -> Local network -> Type* to *Custom network.*
2. Set *Policy -> Local network -> Custom network* to the IPv4 network you wish to have on the LAN side of the 6300-CX. In the sample, this is 172.20.1.1/24
3. Set *Policy -> Remote network* to the IPv4 network you wish to access through the tunnel. (In the sample, this is 172.21.1.1/24)

Under *Firewall*, click *Packet Filtering* to ensure *Allow all outgoing traffic* item exists and enabled.



6300-CX Sample Configuration

Open the configuration profile for the 6350-SR. Under ***IPSec***, create a new entry titled ***NPS*** (the name is arbitrary), and add your IPSec settings to the new entry. The following settings reflect the sample setup in the diagram above.

1. Enter in the PSK into the ***Pre-shared key***.
2. Change ***Local endpoint -> ID -> ID type*** to ***Raw***
3. Set the local ID in ***Local endpoint -> ID -> Raw ID Value***, e.g. *@6300.*
4. *(optional)* Set ***Local endpoint -> type*** to ***Interface***,and set ***Local endpoint -> Interface*** to ***Modem.*** This configures the 63xx-series router to only build the tunnel through the cellular modem WAN interface. Leaving ***Local endpoint -> type*** to ***Interface*** as ***Default route*** will allow the tunnel to be built through any available WAN interface.
5. Change ***Remote endpoint -> ID -> ID type*** to ***Raw***
6. Set the remote ID in ***Remote endpoint -> ID -> Raw ID Value***, e.g. *@nps*.
7. Set the ***Remote endpoint -> Hostname*** to the public IP address of the 6350-SR's WAN Ethernet.
8. Set ***IKE -> Mode*** to ***Aggressive mode***.
9. Set ***IKE -> Phase 1 Proposals*** and ***IKE -> Phase 2 Proposals*** to match the IKE settings required by the 6350-SR. In this example, both proposals are set to 3DES, SHA1, MODP1024.

Under ***Policies***, click ***Add*** to create a new policy, and enter the following settings:

1. Set ***Policy -> Local network -> Type*** to ***Custom network.***
2. Set ***Policy -> Local network -> Custom network*** to the IPv4 network you wish to have on the LAN side of the 6300-CX. In the sample, this is 172.21.1.0/24
3. Set ***Policy -> Remote network*** to the IPv4 network you wish to access through the tunnel. In the sample, this is 172.20.1.0/24