

Branches and Head Office

This type of connection allows you to combine the LANs of several SafeUTM servers.

Features of IPsec technology implementation in SafeUTM assume two roles of using SafeUTM:

- **Head office** - SafeUTM must have a public address on the Internet and accept connections from other SafeUTM (Branches), network equipment, or workstations (Remote Users).
 - **Branch office** - SafeUTM connects to the Head Office and, as a rule, does not have a public address on the Internet. But if the Branch has a public address, then any other device can also be connected to it.
-

Setting up Connection Between Branch and Head Office

Head offices and **Branches** are added on the tabs with the same names in the section **Services** -> **IPsec**.

- Before creating a connection between the Branch and the Head Office, make sure that the **time zone is correctly configured** on each of the connected parties. It is impossible to establish a connection without this.
- Before configuring IPsec, it should be taken into account that for it to work, no IP subnets involved in connections, including the networks of the Head Office and all Branches, should overlap and, moreover, coincide.
- Networks of local interfaces of the Head offices and Branches to which you want to give access, must be set statically.
- Before setting up the connection, you need to make sure that one of the servers has a public (white) IP address from the Internet provider. If it turns out that the Head Office does not have a public IP address, and the Branch has such an address, then the server roles for this connection should be reversed.
- When replacing/reissuing the root certificate in the **TLS Certificates** section, IPsec connections Head Office <-> Branch will stop working and they will need to be recreated.

Step 1. Creating a connection in a Branch

In order to create a connection on SafeUTM, which will act as a Branch, it is necessary to perform the following settings in the web interface of this UTM:

1. Open the section **Services -> IPsec -> Branch office** and click **Add** in the upper left corner of the screen.
2. Fill in the following fields:

- **Head office name** - maximum 42 characters.
- **Head office's external address** - the domain name or external IP address of the head office issued by the provider. If necessary, you can enter the **Head office's additional address**.
- **Branch office LANs** - the IP address of the Branch's subnet that will be available to users in the Head Office, in the IP address/mask format.

IPsec

Head office **Branch office** Devices

Head office name

Main office

Head office's external address

172.16.150.3

Head office's additional address

Branch office LANs

192.168.105.0/24

Networks that will be accessible from the head office.

Add LAN

Add head office

Cancel

- 3. After filling in the fields, click **Add head Office.**
- 4. Click on the edit icon next to the added Head Office.

IPsec

2

Head office

Branch office

Devices

+ Add

Title	Statuses	Operations
Main office (Not configured)		<div><div></div><div></div><div></div></div>



5. Copy the contents of the **Branch office settings** field. The contents need to be pasted when setting up the Head Office to which the connection is being made (see [step 2](#)).



Head office

Branch office

Devices

Branch office settings

eyJkZXBhcnRtZW50X2NzciI6ICItLS0tLUJFR0I
OIEUFUIRJRkIDQVRFIJFUVVFU1QtLS0tLVxu
TUIJQkt6Q0lwd0lCQURCZ01RNHdEQVIEVIFR
S0RBVkpaR1ZqYnpFTU1Bb0dBMVVFQ3d3RF
ZWUk5N
VUF3UGdZRFxuVIFRREREZHdjWx0WVhKNV
gyOW1abWxqWlY4eFgyTTRNVFZpTW1SalItW
TJOVFE0
WTJWaVIXTmxNMIpsTnpKaVxuTWpnNVltRXI
MbWx3YzJWak1Ga3dFd1lIS29aSXpqMENBU

The content must be sent to Head Office for further setup.

Head office name

Main office

Head office's external address

172.16.150.3

Head office's additional address

Branch office LANs

- 192.168.105.0/24

Networks that will be accessible from the head office.

Head office settings

You need to paste the data received from the head office to complete the setup.

Save

Cancel

Step 2. Creating a connection in the Head Office

In order to create a connection on SafeUTM which will act as the Head Office it is necessary to perform the following settings in the web interface of this UTM:

1. Open the section **Services -> IPsec -> Head Office** and click **Add**.
2. Fill in the following fields:

- **Branch office name** - maximum 42 characters.
- **Branch office settings** - paste the settings that you copied from the Branch after completing [step 1](#).



Head office

Branch office

Devices

Branch office name

Branch office

Branch office settings

FQXdJRFJ3QXdSQUlnY2FyUFxuZVN5MStjZVd
4Q25p
ZERQMTRMZnVPenhNaGxLK21xRGh3L3UvN
ERZQ0IHSUZtUUxGVlhsd3ZwNitSUXloYUNxO
FxuL0Zs
WnJoU3F0V01mY2E5Zm40aTdcbi0tLS0tRU5
EIENFUlRJRklDQVRFIjFUVVVFU1QtLS0tLVxuli
wg
ImRlcGFydG1lbnRfbmV0cyI6IFsiMTkyLjE2OC
4xMDUuMC8yNCJdfQ==

Data generated during branch office setup.

Add branch office

Cancel

3. Click **Add branch office**.
4. Click the edit icon next to the added Branch.

IPsec

2

Head office

Branch office

Devices

+ Add

Title	Statuses	Operations
Branch office (Not configured)		<div><div></div><div></div><div></div></div>

5. Select the LANs of the Head Office and click **Save**.

Head office

Branch office

Devices

Branch office name

Branch office

Head office LANs

192.168.100.0/24

Networks that will be accessible from the branch office.

Add LAN

Branch office LANs


• 192.168.105.0/24

Networks that will be accessible from the head office.

Save

Cancel

6. Go back to editing the added Branch and copy the contents of the **Head office settings** field. The contents need to be added to the Branch settings (see [step 3](#)).

 **IPsec**

Head office Branch office Devices

Branch office name

Head office LANs

- 192.168.100.0/24

Networks that will be accessible from the branch office.



Branch office LANs

- 192.168.105.0/24

Networks that will be accessible from the head office.

Head office settings

eyJkZXBhc...ND
QVRXZ0F3SUJBZ0IVV2RVU3VicGZEBUkvRVh
wd2VwZEVrRWNjS0Fjd0NnWUlb1pJemowR
UF3SXdc
bkx6RVhNQIVHQTfVRUJSTU9NakF5TWpBNE
1qa3hNak01TVRNeEZEQVNCZ05WQkFNTUM
xVIVUUzFU
UVVaRIJFNVRcbk1CNFhEVEl5TURnek1ERTJN



Content must be sent to the branch office to complete the setup.

Save Cancel

Step 3. Final setup of the Branch

In order to complete the creation of a connection on SafeUTM which will act as a Branch it is necessary to perform the following settings in the web interface of this UTM:

1. Open section **Services -> IPsec -> Branch office**.
2. Select the desired head office and click **Edit**.
3. Insert into the **Head Office Settings** field the settings text received from the Head Office

during **step 2**.

IPsec

Head office

Branch office

Devices

Branch office settings

```
eyJkZXBhcnRtZW50X2NzciI6ICItLS0tLUJFR0I
OIENFUIRJRkIDQVRFIJFUVVFU1QtLS0tLVxu
TUIJQkt6Q0lwd0lCQURCZ01RNHdEQVIEVIFR
S0RBVkpaR1ZqYnpFTU1Bb0dBMVVFQ3d3RF
ZWUk5N
VUF3UGdZRFxuVIFRREREZHdjWx0WVhKNV
gyOW1abWxqWlY4eFgyTTRNVFZpTW1SalItW
TJOVFE0
WTJWaVlXTmxNMlpsTnpKaVxuTWpnNVltRXI
MbWx3YzJWak1Ga3dFd1lIS29aSXpqMENBU
```



The content must be sent to Head Office for further setup.

Head office name

Main office

Head office's external address

172.16.150.3

Head office's additional address

Branch office LANs

- 192.168.105.0/24

Networks that will be accessible from the head office.

Head office settings

```
k9pVjdTWnh3ajRPVm9NQW9HQ0NxR1NNND
ICQU1DQTBn
QU1FVUNcbklRRGFjTTNXbU1SWUNCd0pLcT
htN1I3am1HRIhjOTcvWlZ4OVdpdINERUZic1F
JZ09L
WWw4YzZoZVE5VHFkMWhcbnNzNUpkRnNy
ZE1LMFkvYkJoRmR3Y0FTV0paMD1cbi0tLS0
tRU5EIENF
UIRJRkIDQVRFLS0tLS1cbiJ9
|
```

You need to paste the data received from the head office to complete the setup.

Save

Cancel

4. Click **Save**.

5. Open section **Services -> IPsec -> Branch office** on UTM acting as a Branch and section **Services -> IPsec -> Head Office** on UTM acting as the Head Office and make sure that the connection to the Head Office is established. The confirmation **Established** should appear in a green frame.

IPsec

2

Head office

Branch office

Devices

+ Add

Title	Statuses	Operations
Main office	<div>Established</div> 172.16.150.3	<div></div> <div></div> <div></div>

Routing of additional networks located behind the router in the local UTM network through an IPsec tunnel.

In order to configure the routing of networks located behind the router in the local UTM network, it is necessary to create a route to an additional network via the router's IP on SafeUTM (UTM, router and target host will be on the same network).

- If SafeUTM is behind NAT, then in order to work with IPsec you need to forward ports 500 and 4500 UDP.
- When installing an IPsec tunnel between SafeUTM servers (Branch and Head Office), 256-bit AES encryption is always used, as it is common and very reliable.

Revision #5

Created 27 August 2022 14:02:06 by Val Redman

Updated 13 October 2022 15:30:45 by Val Redman