



ShareTech UTM Solution

Website
www.sharetech.com.tw/en-us

Sales Info
sales@sharetech.com.tw

Tech Support
help@sharetech.com.tw



ZTA VPN Site-to-Site

ZTA VPN's Site-to-Site mode allows two or more network locations to connect securely, forming a virtual private network. This mode is ideal for enterprises with multiple branches or remote offices that need to access internal resources reciprocally.

Basic Settings

Configure the [Server Connection Port](#), which is used for information exchange before the tunnel is established. The default port is 21820.

Basic Setting

Connection Port Enable	<input checked="" type="checkbox"/>
Connection Port	<input type="text" value="21820"/> (TCP)
Allow Interface	<input checked="" type="radio"/> ALL <input type="radio"/> User Define
Source IP Address Whitelist ?	<input type="text"/> ex. 192.168.1.1 192.168.2.0/24

tunnel mode

192.168.88.58



tunnel

10.0.0.1

10.0.0.2



Tunnel Mode can establish a point-to-point encrypted tunnel between two nodes, ensuring the security of data transmission.

- On the server side, select **VPN server** and use **tunnel mode**. Set the **Local IP Address** and **Tunnel Interface Address** according to the architecture, then generate a **Verification Code**. Other settings can be defined as needed. (The **Verification Code** has a fixed format; it is recommended to click "Change" to generate one.)
 - Tunnel Port:** Port used for data transmission and status detection. It does not have to be the same as the Client's **Tunnel Port**.
 - MTU:** Sets the maximum packet length.

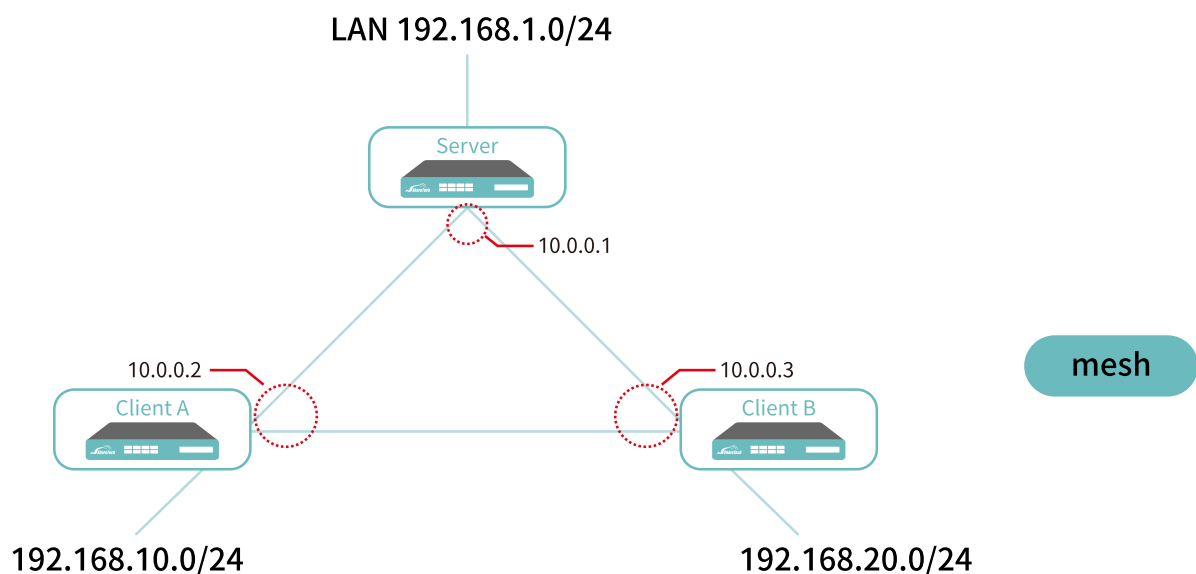
Add Server

Name	server (maximum 32 characters. Not have "{},)	
Enable	<input type="checkbox"/>	
VPN Mode	<input checked="" type="radio"/> Tunnel Mode <input type="radio"/> Mesh Mode	
Local IP Address	WAN1 (WAN1) ▾	192.168.88.58 ▾
Tunnel Interface Address	10.0.0.1 / 30	
Tunnel Port	60000 (1 ~ 65535)	
MTU	1500 (1400 ~ 1500)	
Verification Code	JlBQt47--9	<input type="button" value="Change"/>
Local Subnet	0.0.0.0/1,128.0.0.0/1	

- On the client side, select **VPN Client**. Enter the **Server Address** and **Local IP Address** according to the architecture. Fill in the **Verification Code** generated by the Server and the **Server Connection Port**. Other settings can be defined as needed.
 - Tunnel Port:** Port used for data transmission and status detection. It does not have to be the same as the Server's Tunnel Port.
 - MTU:** Sets the maximum packet length.

[!NOTE] Setting the **Local IP Address** to "None" supports NAT traversal.

mesh mode



Tunnel Mode configuration is less convenient in multi-site scenarios and makes it difficult to achieve direct connections between any two sites. In contrast, **Mesh Mode** allows branch sites (Spokes) to establish tunnels

directly with each other without all traffic being forwarded through the headquarters (Hub), achieving more flexible interconnection between any two points.

1. On the server side, select **VPN server** and use **mesh mode**. Set the **Local IP Address** and **Tunnel Interface Address** according to the architecture. Other settings can be defined as needed. **Mesh mode** requires additionally specifying the local subnet that can connect to the remote ends.

Add Server

Name: mesh (maximum 32 characters. Not have "(),)

Enable:

VPN Mode: Tunnel Mode Mesh Mode

Local IP Address: WAN3 PPPOE (dppon2) 172.16.0.1

Tunnel Interface Address: 10.0.0.1 / 24

Tunnel Port: 60000 (1 ~ 65535)

MTU: 1500 (1400 ~ 1500)

Local Subnet: 192.168.1.0 / 24

Name	Verification Code	Client IP Address	Remote Subnet	More
client-A	hxx7v-j4#8 <input type="button" value="Change"/>	10.0.0.2 <input type="button" value="Add"/>	192.168.10.0 / 24 <input type="button" value="Add"/>	
client-B	2#5l=9fgks <input type="button" value="Change"/>	10.0.0.3 <input type="button" value="Add"/>	192.168.20.0 / 24 <input type="button" value="Add"/>	<input type="button" value="X"/>

2. Configure clients(remote networks); multiple clients can be added at once. Each client network must have a unique Verification Code, Client IP Address, and remote subnet.
3. On the client side, select **VPN Client**. Enter the **Server Address** and **Local IP Address** according to the architecture. Fill in the **Verification Code** generated by the Server and the **Server Connection Port**. Other settings can be defined as needed.

Client-A

Add Client

Name: client-A (maximum 32 characters. Not have "(),)

Enable:

Server Address: 172.16.0.1

Server Connection Port: 21820

Verification Code: hxx7v-j4#8

Local IP Address: None

Tunnel Port: 60000 (1 ~ 65535)

MTU: 1500 (1400 ~ 1500)

Client-B

Add Client

Name: client-B (maximum 32 characters. Not have "(),)

Enable:

Server Address: 172.16.0.1

Server Connection Port: 21820

Verification Code: 2#5l=9fgks

Local IP Address: None

Tunnel Port: 60000 (1 ~ 65535)

MTU: 1500 (1400 ~ 1500)

Connectivity

Mesh mode automatically generates routing tables for the specified internal networks on each mesh device. Therefore, you only need to configure the security policies.

For example: To allow 192.168.1.0/24 to connect to 192.168.10.0/24, set the policy as follows:

Server

Basic Setting

Policy Name	<input type="text"/>
Source Interface ?	LAN (LAN) <input type="checkbox"/> Multiple selections allowed
Assign Gateway	Default <input type="text"/>
Network Address Translation	Routing <input type="text"/>
Protocol	ALL <input type="text"/>
Source ?	IP Address 192.168.1.0/24 MAC Address <input type="text"/> Change to options
Destination ?	IP Address 192.168.10.0/24 Change to options
SRC Service Group	User Defined <input type="text"/> Port <input type="text"/>
DEST Service Group	User Defined <input type="text"/> Port <input type="text"/>
Action	Permit <input type="text"/>

Client-A

Basic Setting

Policy Name	<input type="text"/>
Source Interface ?	ZTA VPN S2S Client () <input type="checkbox"/> Multiple selections allowed
Assign Gateway	Default <input type="text"/>
Network Address Translation	Routing <input type="text"/>
Protocol	ALL <input type="text"/>
Source ?	IP Address 192.168.1.0/24 MAC Address <input type="text"/> Change to options
Destination ?	IP Address 192.168.10.0/24 Change to options
SRC Service Group	User Defined <input type="text"/> Port <input type="text"/>
DEST Service Group	User Defined <input type="text"/> Port <input type="text"/>
Action	Permit <input type="text"/>