GRANDSTREAM
CONNECTING THE WORLD

Grandstream Networks, Inc.

VPN Guide

WireGuard® Site-to-Site Configuration Guide

Introduction

This guide provides step-by-step instructions to configure a WireGuard site-to-site VPN between two Grandstream GWN routers. It is intended for users looking to establish a secure VPN tunnel between two remote networks using the WireGuard protocol.

Device Series	Models Supported
GWN70x2 (Wireless Routers)	GWN7052, GWN7052F, GWN7062
GWN70xx (Wired Routers)	GWN7001, GWN7002, GWN7003
GCC6000 (Convergence Devices)	GCC6010W, GCC6010, GCC6011

WireGuard® supported devices

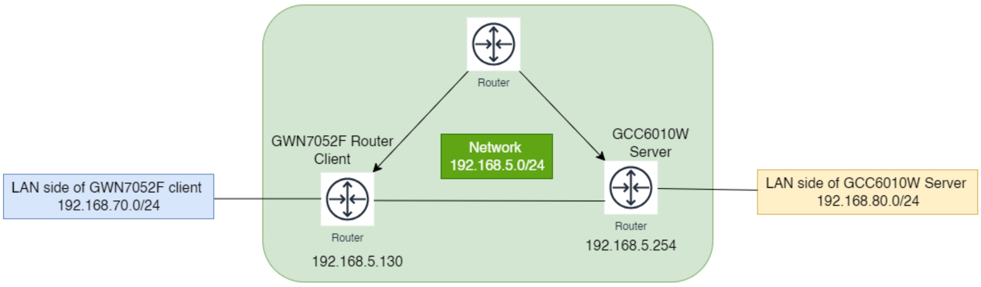
Prerequisites

- Two Grandstream GWN routers (e.g., GWN7052F and GCC6010W).
- Firmware on both routers should be up-to-date.
- Each site requires a public IP address or Dynamic DNS (DDNS) configured.

Lab Setup Overview

This lab setup involves two routers configured as follows:

- **Site A:** GWN7052F
  - LAN Subnet: 192.168.70.0/24
  - WireGuard IP: 10.0.0.2/24
- **Site B:** GCC6010W
  - LAN Subnet: 192.168.80.0/24
  - WireGuard IP: 10.0.0.1/24
- **Transit Network:** Internet (represented as 192.168.5.0/24 in the lab)



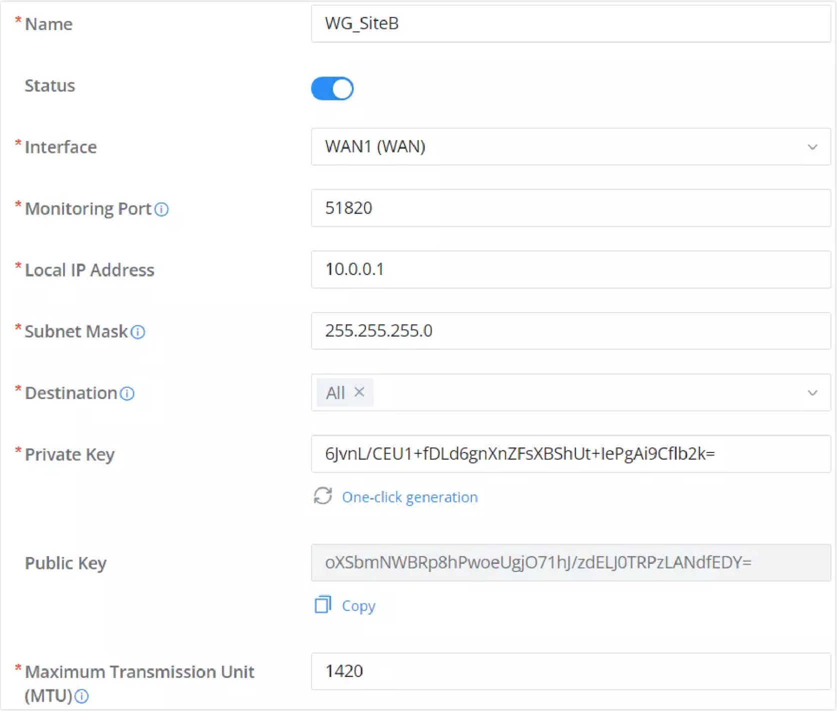
Network Topology

Step 1: Configuring WireGuard on Site B (GCC6010W)

To configure WireGuard on the GCC6010W router at Site B, follow these steps:

Step-by-Step Instructions for site B

1. Log in to the web interface of the GCC6010W router.
2. Navigate to **VPN** > **WireGuard** and click "**Add**" to create a new WireGuard instance.
3. Fill out the configuration fields as follows:



*Name	WG_SiteB
Status	●
*Interface	WAN1 (WAN)
*Monitoring Port ⓘ	51820
*Local IP Address	10.0.0.1
*Subnet Mask ⓘ	255.255.255.0
*Destination ⓘ	All ×
*Private Key	6JvnL/CEU1+fDLd6gnXnZFsXBShUt+IePgAi9Cflb2k= One-click generation
Public Key	oXSbmNWBRp8hPwoeUgjO71hJ/zdELJ0TRPzLANdfEDY= Copy
*Maximum Transmission Unit (MTU) ⓘ	1420

Configuring WireGuard on Site B

Field	Value	Description
Name	WG_SiteB	The name of the WireGuard interface.
Status	ON	Toggle ON the status to enable it.
Interface	WAN1	Select the WAN interface connected to the internet.
Monitoring Port	51820	Standard WireGuard port; can be customized.
Local IP Address	10.0.0.1/24	WireGuard IP address for this interface at Site B.
Subnet Mask	255.255.255.0	Subnet mask for the WireGuard network.
Destination	All	Allows routing to all networks.
Private Key	[Auto-Generated]	Automatically generated; keep it secure.
Public Key	[Auto-Generated]	Public Key changes whenever the Private Key changes. ***Note:*** *Copy and save the public key immediately after generating the private key, as this public key will be used for configuration on the other site (either Site A or Site B).*
MTU	1420	Maximum Transmission Unit; default is recommended.

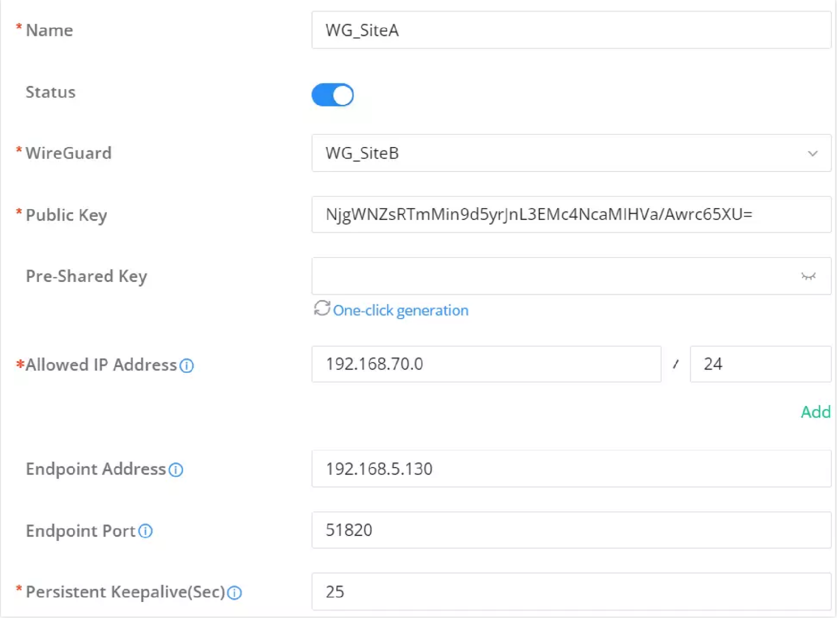
Configuring WireGuard on Site B

Once the fields are filled out, click "**Save**" to create the WireGuard interface.

Adding the Peer for Site A

Next, add the peer for Site A on the router at Site B:

1. Navigate to the **Peers** section and click "**Add**"
2. Fill out the peer fields as follows:



* Name	WG_SiteA
Status	●
* WireGuard	WG_SiteB
* Public Key	NjgWNZsRTmMin9d5yrJnL3EMc4NcaMIHVa/Awrc65XU=
Pre-Shared Key	
*Allowed IP Address	192.168.70.0 / 24
Endpoint Address	192.168.5.130
Endpoint Port	51820
* Persistent Keepalive(Sec)	25

Adding the Peer for Site A

Field	Value	Description
Name	WG_SiteA	A descriptive name for the peer at Site A.
Status	ON	Toggle ON the status to enable it.
WireGuard	WG_SiteB	Select the WireGuard interface created earlier at Site B.
Public Key	[Public Key from Site A]	Enter the public key generated on the router at Site A.
Pre-Shared Key	Optional	A pre-shared key can be used for an additional layer of security. This key must be the same on both Site A and Site B. If you decide to use a pre-shared key, make sure to generate it and securely share it between the two sites.
Allowed IP Address	192.168.70.0/24	The subnet behind the router at Site A.
Endpoint Address	[Public IP/DDNS of Site A]	The public IP or DDNS of the router at Site A.
Endpoint Port	51820	The port WireGuard is listening on at Site A.
Persistent Keepalive	25	Default value to keep the connection alive.

Adding the Peer for Site A

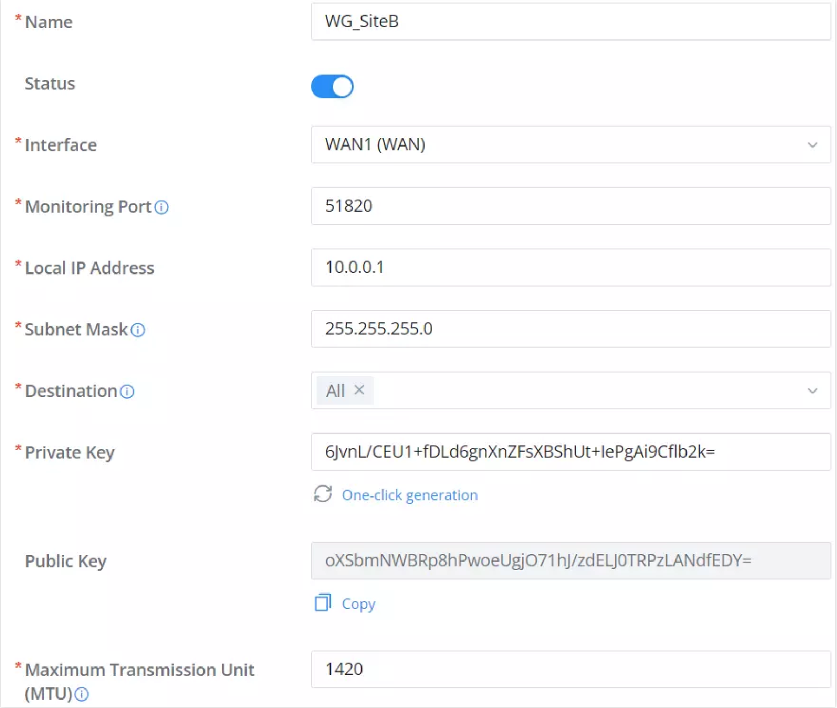
Click “**Save**” to store the peer configuration.

Step 2: Configuring WireGuard on Site A (GWN7052F)

To configure WireGuard on the GWN7052F router at Site A, follow these steps:

Step-by-Step Instructions for Site A

1. Log in to the web interface of the GWN7052F router.
2. Navigate to **VPN** > **WireGuard** and click “**Add**” to create a new WireGuard instance.
3. Fill out the configuration fields as follows:



*Name	WG_SiteB
Status	ON
*Interface	WAN1 (WAN)
*Monitoring Port	51820
*Local IP Address	10.0.0.1
*Subnet Mask	255.255.255.0
*Destination	All
*Private Key	6JvnL/CEU1+fDLd6gnXnZFsXBShUt+IePgAi9Cflb2k=
Public Key	oXSbmNWBRp8hPwoeUgjO71hJ/zdELJ0TRPzLANdfEDY=
*Maximum Transmission Unit (MTU)	1420

Configuring WireGuard on Site A

Field	Value	Description
Name	WG_SiteA	The name of the WireGuard interface.
Status	ON	Toggle ON the status to enable it.
Interface	WAN1	Select the WAN interface connected to the internet.
Monitoring Port	51820	Standard WireGuard port; can be customized.
Local IP Address	10.0.0.2/24	WireGuard IP address for this interface at Site A.
Subnet Mask	255.255.255.0	Subnet mask for the WireGuard network.
Destination	All	Allows routing to all networks.
Private Key	[Auto-Generated]	Automatically generated; keep it secure.
Public Key	[Auto-Generated]	Public Key changes whenever the Private Key changes. ***Note:*** *Copy and save the public key immediately after generating the private key, as this public key will be used for configuration on the other site (either Site A or Site B).*
MTU	1420	Maximum Transmission Unit; default is recommended.

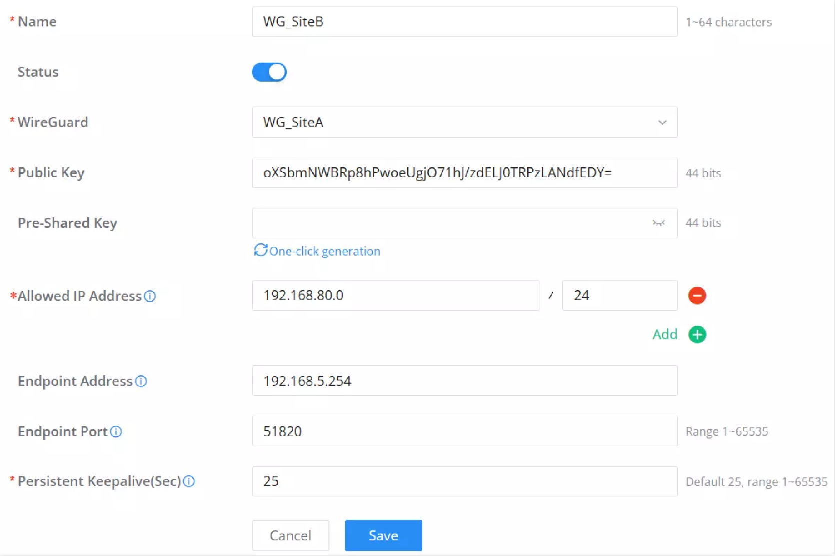
Configuring WireGuard on Site A

Once the fields are filled out, click “**Save**” to create the WireGuard interface.

Adding the Peer for Site B

Next, add the peer for Site B on the router at Site A:

1. Navigate to the **Peers** section and click “**Add**”
2. Fill out the peer fields as follows:



* Name	WG_SiteB	1~64 characters
Status	ON	
* WireGuard	WG_SiteA	
* Public Key	oXSbmNWBRp8hPwoeUgjO71hJ/zdELJ0TRPzLANdfEDY=	44 bits
Pre-Shared Key		44 bits
*Allowed IP Address	192.168.80.0 / 24	
Endpoint Address	192.168.5.254	
Endpoint Port	51820	Range 1~65535
* Persistent Keepalive(Sec)	25	Default 25, range 1~65535

Adding the Peer for Site B

Field	Value	Description
Name	WG_SiteB	A descriptive name for the peer at Site B.
Status	ON	Toggle ON the status to enable it.
WireGuard	WG_SiteA	Select the WireGuard interface created earlier at Site A.
Public Key	[Public Key from Site B]	Enter the public key generated on the router at Site B.
Pre-Shared Key	Optional	A pre-shared key can be used for an additional layer of security. This key must be the same on both Site A and Site B. If you decide to use a pre-shared key, make sure to generate it and securely share it between the two sites.
Allowed IP Address	192.168.80.0/24	The subnet behind the router at Site B.
Endpoint Address	[Public IP/DDNS of Site B]	The public IP or DDNS of the router at Site B.
Endpoint Port	51820	The port WireGuard is listening on at Site B.
Persistent Keepalive	25	Default value to keep the connection alive.

Adding the Peer for Site B

Click "**Save**" to store the peer configuration.

Step 3: Testing the VPN Connection

After configuring both Site A and Site B, it's important to test the VPN connection to ensure everything is working properly.

Testing the Connection

1. Turn on the WireGuard interfaces on both Site A and Site B.
2. Use the **ping** command to test connectivity between devices on the two networks (e.g., ping from a device in `192.168.70.0/24` to a device in `192.168.80.0/24`).

Troubleshooting Tips

- Check the WireGuard interface status on both routers to ensure the tunnel is active.
- Ensure that firewall rules on both routers allow traffic through the WireGuard interface.
- Verify that the correct public keys are entered on both Site A and Site B.

- Check logs on both routers for any errors related to the WireGuard tunnel.

Conclusion

By following this guide, you should now have a fully operational WireGuard site-to-site VPN between your GWN7052F and GCC6010W routers at Site A and Site B. This secure connection allows you to route traffic between the two networks seamlessly and securely over the internet.

If you encounter any issues or need further assistance, please refer to our support resources or contact our technical support team.