20: Warpgate - Secure SSH Gateway

Warpgate is a secure SSH gateway (also called a "bastion host") that provides a web interface for managing SSH access to your server. Instead of connecting directly to your server, you connect through Warpgate, which adds an extra layer of security and makes it easier to manage who can access what.

For advanced features, API documentation, and technical details, see the official Warpgate documentation.

Why Warpgate?

- **Secure SSH gateway** - All SSH connections go through Warpgate
- **Web-based management** - Easy-to-use web interface for managing access
- **User access control** - Control who can access which servers
- **Session recording** - Keep track of SSH sessions for security
- **No direct server access** - Server SSH port can be closed, only Warpgate port open
- **Centralized access** - Manage all SSH access from one place
- **Better security** - Reduces attack surface by closing direct SSH access

Prerequisites

- **Docker running** (from Chapter 3)
- **Optional: Traefik installed** (from Chapter 4) for HTTPS access with a domain
- **Optional: Subdomain** (from Chapter 4.5), e.g., `warpgate.yourdomain.com`
- **Firewall access** - Ability to open port 2222 (SSH) and optionally close port 22

Note: Warpgate works great with Traefik and a domain name. Having a friendly URL like `warpgate.yourdomain.com` makes it easy to access the web management interface.

Step 1: Start Infinity Tools

```
sudo infinity-tools
```

Step 2: Install Warpgate

1. Go to □□ **APPLICATIONS**
2. Select **Warpgate**
3. Choose **Install Warpgate**

Using the Infinity Tools GUI

- Use **↑/↓** to move, **Enter** to select, **Esc** to go back
- Look for the **turquoise cursor** indicating the current selection
- Each screen shows a short description at the top explaining what's needed

Step 2.1: Choose SSL Mode

You'll see two options. Here's what each means:

- **Traefik (recommended)**
  - **What it is:** Uses your domain name with a trusted HTTPS certificate from Let's Encrypt
  - **What you need:** A subdomain (e.g., `warpgate.yourdomain.com`) pointing to your server (see Chapter 4.5)
  - **What you get:** Professional URL like `https://warpgate.yourdomain.com` with trusted SSL
  - **Pick this if:** You have a domain and want secure, easy access (recommended)
- **Standalone**
  - **What it is:** Uses HTTPS with a self-signed certificate and direct port access
  - **What you need:** Just a free port (default: 8888)
  - **What you get:** URL like `https://SERVER_IP:8888` with a warning you must accept once
  - **Pick this if:** You don't have a domain or prefer direct access

Simple rule of thumb: Use **Traefik** if you have a domain (recommended). Use **Standalone** if you don't have a domain.

Step 2.2: Domain Configuration (Traefik Mode)

If you chose Traefik, you'll be asked for your domain:

- **What it is:** The subdomain where Warpgate will be accessible
- **Example:** `warpgate.yourdomain.com`
- **Important:** DNS must already point to your server (see Chapter 4.5)

Step 2.3: Port Configuration (Standalone Mode)

If you chose Standalone, you'll be asked for a port:

- **Default:** 8888
- **What it is:** The port for the web interface
- **Note:** SSH port (2222) is always exposed directly

What Happens During Installation

- Warpgate container is created
- Data directory is set up
- Web interface becomes accessible
- SSH gateway starts on port 2222
- Interactive setup prompts for admin credentials

Step 3: Set Up Admin Account

After installation, Warpgate will run an interactive setup. You'll be prompted to create an admin account:

Admin Setup Prompts

1. **Admin username:** Choose a username for the admin account (e.g., `admin`)
2. **Admin password:** Choose a strong password (you'll use this to log into the web interface)
3. **Confirm password:** Enter the password again to confirm

⚠ **IMPORTANT:** Save these credentials immediately! You'll need them to access the web interface.

Step 4: Access Warpgate Web Interface

If Using Traefik

1. Wait 30-60 seconds for SSL certificate generation
2. Open `https://warpgate.yourdomain.com` in your browser

3. You'll see the Warpgate login page

If Using Standalone

1. Open `https://SERVER_IP:8888` in your browser
2. You'll see a security warning (normal for self-signed certificates)
3. Click "Advanced" → "Proceed to site" to continue
4. You'll see the Warpgate login page

Step 5: Login to Web Interface

1. Enter the admin username you created during setup
2. Enter the admin password you created during setup
3. Click "Login"
4. You'll see the Warpgate dashboard!

Step 6: Understanding Warpgate

Warpgate acts as a gateway (or "bastion") between you and your server:

How It Works

- **Before Warpgate:** You connect directly to your server via SSH (port 22)
- **With Warpgate:** You connect to Warpgate (port 2222), which then connects you to your server
- **Benefits:** All SSH access goes through Warpgate, making it easier to manage and secure

What You Can Do

- **Manage users** - Add users who can access servers through Warpgate
- **Control access** - Decide which users can access which servers
- **View sessions** - See who's connected and what they're doing
- **Record sessions** - Keep logs of SSH sessions for security
- **Manage targets** - Add servers that users can connect to

Step 7: Add Your First Target (Server)

Before users can connect, you need to add a "target" (the server they'll connect to):

Adding a Target

1. In the web interface, go to **"Targets"** or **"Servers"**
2. Click **"Add Target"** or the **"+"** button
3. Enter target details:
   - **Name:** A friendly name (e.g., "My Server")
   - **Host:** The server's IP address or hostname (usually `localhost` or `127.0.0.1` for the same server)
   - **Port:** SSH port (usually `22`)
   - **Username:** The SSH username (e.g., your server username)
4. Click **"Save"** or **"Create"**

For Same-Server Access

If Warpgate is running on the same server you want to access:

- **Host:** `localhost` or `127.0.0.1`
- **Port:** `22` (or your server's SSH port)
- **Username:** Your server username

Step 8: Add Users

Now add users who can connect through Warpgate:

Adding a User

1. In the web interface, go to **"Users"**
2. Click **"Add User"** or the **"+"** button
3. Enter user details:
   - **Username:** A username for Warpgate (e.g., "john")
   - **Password:** A password for this user
   - **Email:** Optional email address
4. Click **"Save"** or **"Create"**

Granting Access

After creating a user, grant them access to targets:

1. Go to the user's profile
2. Find **"Access"** or **"Targets"** section
3. Select which targets this user can access

4. Save the changes

Step 9: Connect via SSH Through Warpgate

Now you can connect to your server through Warpgate:

SSH Connection

```
ssh -p 2222 warpgate-user@warpgate.yourdomain.com
```

Or if using standalone mode:

```
ssh -p 2222 warpgate-user@SERVER_IP
```

What Happens

1. You connect to Warpgate on port 2222
2. Warpgate asks for your Warpgate username and password
3. After authentication, Warpgate shows you available targets
4. You select which target (server) you want to connect to
5. Warpgate connects you to that server

First-Time Connection

On your first connection, you'll see:

1. Warpgate login prompt
2. Enter your Warpgate username and password
3. List of available targets
4. Select a target to connect
5. You're now connected to your server!

Step 10: Security Best Practices

Close Direct SSH Access

Once Warpgate is working, you can close direct SSH access to your server:

```
# Close port 22 (direct SSH)
sudo ufw delete allow 22/tcp

# Keep port 2222 open (Warpgate SSH)
sudo ufw allow 2222/tcp
```

⚠ **WARNING:** Only do this after testing Warpgate! Make sure you can connect through Warpgate before closing port 22.

Firewall Configuration

- **Open port 2222** - Required for Warpgate SSH access
- **Open port 80/443** - If using Traefik (for web interface)
- **Open port 8888** - If using standalone mode (for web interface)
- ⚠ **Close port 22** - After testing Warpgate (optional but recommended)

User Management

- **Use strong passwords** - For both admin and user accounts
- **Limit access** - Only grant access to targets users need
- **Regularly review users** - Remove users who no longer need access
- **Monitor sessions** - Check who's connecting and when

Troubleshooting

Can't Access Web Interface

- **Traefik mode:** Wait 30-60 seconds after installation for SSL certificate generation
- **Standalone mode:** Accept the self-signed certificate warning
- **Check container:** Run `docker ps | grep warpgate` to see if it's running
- **Check logs:** Run `docker logs warpgate` to see error messages

Can't Connect via SSH

- **Check firewall:** Make sure port 2222 is open: `sudo ufw status | grep 2222`
- **Check credentials:** Verify you're using the correct Warpgate username and password
- **Check target:** Make sure the target server is configured correctly
- **Check access:** Verify the user has access to the target

Forgot Admin Password

- You'll need to reinstall Warpgate with `--deleteall` flag
- This will wipe all data and let you create a new admin account
- Make sure to back up any important data first!

Target Connection Fails

- **Check target host:** Verify the host IP/name is correct
- **Check target port:** Verify the SSH port is correct (usually 22)
- **Check target credentials:** Verify the username is correct
- **Test direct connection:** Try connecting directly to the target to verify it's accessible

Where to Find Warpgate After Install

- On the finish screen, Infinity Tools prints the web interface URL
- You can also see it in ◫ **STATUS & HEALTH → STATUS**
- Check the installation directory: `/opt/speedbits/warpgate`
- Configuration file: `/opt/speedbits/warpgate/data/warpgate.yaml`
- Database: `/opt/speedbits/warpgate/data/db/`

Managing Warpgate

Adding More Users

Simply repeat Step 8 for each user you want to add. Each user can have access to different targets.

Adding More Targets

Add more servers by repeating Step 7. Users can then be granted access to these new targets.

Viewing Sessions

The web interface shows active SSH sessions, including who's connected and what they're doing.

Session Recording

Warpgate can record SSH sessions for security auditing. Check the settings in the web interface to enable this.

You're Ready!

Warpgate is now installed and ready to use! Remember:

- □□ Save your admin credentials securely
- □□ Connect via port 2222 (not port 22)
- □□ Add users and grant them access to targets
- □□ Close port 22 after testing (optional but recommended)
- □□ Monitor sessions in the web interface
- □□ Use strong passwords for all accounts

Next steps: Add your first target, create users, grant access, test SSH connection through Warpgate, and optionally close direct SSH access (port 22) for better security!

Revision #1
Created 17 November 2025 17:31:13 by bjoern
Updated 17 November 2025 17:31:30 by bjoern