### Cloudflare ZTNA for securing SSH access to endpoint devices

720 Manu Chacko July 2, 2024 Security Compliances, Tweaks & Configuration 721

### Setup Cloudflare ZTNA (Zero Trust Network Access) with Ezeelogin for securing SSH access

Cloudflare Tunnel can also route applications through a public hostname, allowing users to connect to an SSH server with Cloudflared access. This method requires Cloudflared to be installed on both the server and client machines, as well as an active zone on Cloudflare. The traffic is proxied over this connection.

The benefit of this method is that it provides a secure and reliable way to access Ezeelogin. By routing applications through a public hostname and using Cloudflare **Zero Trust Network Access**, you can enhance security by hiding your server's true IP address and exposing it through a secure Cloudflare Tunnel. This approach simplifies access, allowing users to connect to Ezeelogin from anywhere without the need for a VPN. Additionally, it improves reliability by leveraging Cloudflare's robust network, ensuring consistent and dependable access to your server. Centralized management of access and configurations is made easy through Cloudflare's dashboard, and the attack surface is reduced by minimizing the risk of direct attacks on your server using Cloudflare's security features.

User Desktop		Cloudflare Network		Ez	Ezeelogin Gateway Server				
Cloudflare Agent Daemon	HTTPS Cloudflare Access SSH	Cloudflare Edge Server	Cloudflare Tunnel	Cloudflared Tunnel Daemon	443 80 22 Jumpserver				

#### 1. Connect the server to Cloudflare

1. Login to <u>Cloudflare</u> dashboard. click on Zero Trust > Network > Tunnels

CLO	UDFLARE					Support 🔻 🖌	L -
←	Manuchacko@ezeel	•	Networks / Tunnels				
	Zero Trust overview		Tunnels				
O	Analytics	•	Tunnels establish a secure connection between Cloudflare's edge and your infrastructure.				
Ð	Gateway	•	Your tunnels showing 1 - 1				
÷	Access	•	Manage the configurations of your existing tunnels.				
<b>X</b>	Networks New	•	+ Create a tunnel		Search by tunnel name		
	Tunnels		Tunnel name	Routes	Status	Uptime	
L	Routes		Tunnel name 🎓 Connector type Connector ID Tunnel ID	Routes	Status	Uptime	-
222	Routes My Team	•	Tunnel name   Connector type Connector ID Tunnel ID  1 - 1 Items per page: 10	Routes	Status	Uptime < 1 of 1 page >	
æ	Routes	•		Routes	Status		
	Routes My Team			Routes	Status		
	Routes My Team Logs			Routes	Status		
	Routes My Team Logs			Routes	Status		

2. Click and Create tunnel and select Cloudflared connector, then click next

CLO	UDFLARE					Support 🔻	±	
←	ezeel	•	Create a tunnel					
	Zero Trust overview		Create a tunnel to connect HTTP web servers, safely to Cloudflare.	SSH servers, remote desktops, and other proto-	cols			
G	Analytics	•	E Learn more					
Ð	Gateway	-						
÷	Access	-	Select tunnel type / Name your tu	nnel / Install and run connectors / R	Route tunnel			
۶	Networks New							1
	Tunnels		Select your connector					
	Routes		-	t your resources to Cloudflare's global net	work.			1
222	My Team	•	Cloudflared	🕂 WARP 🛛 Beta				1
	Logs	-	Recommended	Linux distros only				1
鐐	Settings							
			Establishes a secure, outbound- only connection to Cloudflare for	Supports on-ramping and off- ramping traffic for site-to-site,				1
			user-to-network connectivity.	bidirectional, and mesh networking connectivity.				1
			🛤 Learn more	Learn more				1
								1
								1
								1
«	Collapse sidebar		Back			Nex	đ	

3. Name your tunnel and save tunnel

CLO			Support 🔻 💄 💌
←	Manuchacko@ezeel	•	<u> Back to Tunnels</u>
	Zero Trust overview		Create a tunnel
O	Analytics	-	Create a tunnel to connect HTTP web servers, SSH servers, remote desktops, and other protocols safely to Cloudflare.
Ð	Gateway	•	Earn more
Ð	Access	•	
R	Networks New	•	Select tunnel type / Name your tunnel / Install and run connectors / Route tunnel
	Tunnels		
	Routes		
<u>.89</u> 2	My Team	-	Name your tunnel Use a descriptive name based on the network version want to connect. We recommend creating only one tunnel for each network.
	Logs	-	Tunnel name (Required)
鐐	Settings		Ezeelogin
			Back Save tunnel
«	Collapse sidebar		

4. Now you can install Cloudflared on your Ezeelogin server. Select the operating system of your server and copy the corresponding installation command as follows:

CLOUDFLARE	Support 🔻 🔺 🗶
← →	Configure
Zero Trust overview	Select tunnel type / Name your tunnel / Install and run connectors / Route tunnel
Analytics •	
🖶 Gateway 🔻	Choose your environment
left Access	Choose an operating system:
🕅 Networks New 🔺	
Tunnels	Copse an architecture:
Routes	64-bit 32-bit arm64-bit arm32-bit
ی My Team ۲	
🗉 Logs 🗸 👻	
8 Settings	Install and run a connector To connect your tunnel to Cloudflare, copy-paste one of the following commands into a terminal window. Remotely managed tunnels require that you install cloudflared 2022.03.04 or later.
	Store your token carefully. This command includes a sensitive token that allows the connector to run. Anyone with access to this token will be able to run the tunnel.
	If you don't have cloudflared installed on your machine: If you already have cloudflared installed on your machine:
	curl -Loutput cloudflared.deb       sudo cloudflared.deb         https://github.com/cloudflare/cloudflared/releases/latest/download/cloudflared       sudo cloudflared         ared-linux-amd64.deb &&       S         sudo cloudflared.deb &&       S         sudo cloudflared service install eyJhIjoiZj       S
Collapse sidebar	

5. After installation you can view the status as connected in the dashboard and click next

CLOUDFLARE		Support 💌
←	•	Install and run a connector
Zero Trust overvie	ew	To connect your tunnel to Cloudflare, copy-paste one of the following commands into a terminal window. Remotely managed tunnels require that you install cloudflared 2022.03.04 or later.
Analytics	-	Store your token carefully. This command includes a sensitive token that allows the connector to run. Anyone with access to this token will be
🗗 Gateway	•	U able to run the tunnel.
left Access	-	If you don't have cloudflared installed on your machine: If you already have cloudflared installed on
🕅 Networks New	*	curl -Loutput cloudflared.deb https://github.com/cloudflared/releases/latest/download/cloudfl sudo cloudflared
Tunnels		ared-linux-amd64.deb && S service install
Routes		sudo dpkg -i cloudflared.deb &&
28 My Team	•	sudo cloudflared service install eyJhIjoiZj
Logs	-	
Settings		View Frequently Asked Questions C
		Connector ID     Status     Virsion       6816890c-5c4c-4f20-a883-0187dee8281e     Connected     2024.6.1
Collapse sidebar		Back

6. Choose a **Domain** and specify any **subdomain**(eg: gateway). Select **HTTPS/HTTP** and enter the URL **127.0.0.1** or **localhost** 

You can select any domain that is already added in Cloudflare.

CLOUDFLARE		Support 🔻 💄
← Manuchacko@ezeel →	Route Traffic	
Zero Trust overview	Select tunnel type / Name your tunnel / Install and run connectors / Route tunnel	
Analytics •	🔅 Route traffic by adding a public hostname or a private network to your tunnel. You can always add more hostnames or networks at a later time.	
🖶 Gateway 🔹	Protect your resource by adding an Access policy under <u>Access &gt; Applications &gt; Self-hosted</u> .	
🕅 Networks New 🔺	Public Hostnames Private Networks	
Tunnels		
Routes		
📽 My Team 🔹	Add public hostname for Ezeelogin Public hostname	
Logs	Subdomain Domain (Required) Path	
🚯 Settings	gateway   Cloudweg.com  (optional) path	
	Service	
	Type (Required) URL (Required)	
	HTTPS V 127.0.0.1	
	For example, https://localhost.8001	
	Additional application settings	
Collapse sidebar	Back	Save tunnel

You can view the tunnel in the Tunnels dashboard after saving it.

CLO	UDFLARE							Support 🔻	*
~		•	Networks / Tunnels						
	Zero Trust overview		Tunnels						
G	Analytics	•	Tunnels establish a secure con	nection between Cloudflare's edge and your	infrastructure.		/		
÷	Gateway	•	Your tunnels Showing	1 - 1					
÷	Access	•	Manage the configurations of						
8	Networks New	•	+ Create a tunnel			२ Search by	tunnel name		
	Tunnels		Tunnel Connector type	Connector ID	Tunnel ID	Routes	Status	Uptime	
	Routes		name 个						
<u>898</u>	My Team	•	Ezeelogin cloudflared	<u>6816890c-5c4c-4f20-a883-0187dee8281e</u> び	fa53f8be-bcb8-48e6-a450-3efaf9212773	gateway.	HEALTHY	37 minutes	:
	Logs	•	1 - 1   Items per page: 10					< 1 of 1 pag	/e >
ŝ	Settings								

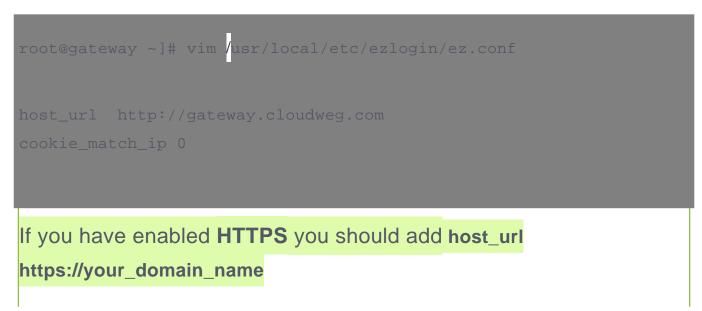
You can view the **subdomain** created from the **dashboard** > **configure** >**public hostname** 

Support 👻 🔺 💌

←	Manuchacko@ezeel	•	Networks / Tunne	els						
	Zero Trust overview		Tunnel	s						
G	Analytics	•	Tunnels establ	lish a secure conn	ection between Cloudflare's edge and y	our infrastructure.				
Ð	Gateway	•	Your tunr	nels Showing 1	- 1					
Ð	Access	-		-	our existing tunnels.					
<b>X</b>	Networks New	•	+ Create a tur	nnel			Search by	tunnel name		
	Tunnels		Tunnel	Connector type	Connector ID	Tunnel ID	Poutes	Status	Uptim	e
	Routes		name 个							
<u>200</u>	My Team	•	Ezeelogin	cloudflared	6816890c-5c4c-4f20-a883-0187dee8281e	fa53f8be-bcb8-48e6-a450-3efaf9212	gateway.o	HEALTH	43 min	nutes 🚺
=	Logs	•	1 - 1 Items per	page: 10					<	Configure
鐐	Settings									Delete

CLO	UDFLARE					Support	• ±•
←	Manuchacko@ezeel	•	- Back to tunnels				
	Zero Trust overview		Ezeelogin				
ው	Analytics	•	Overview Public Hostname Private Network				
Ð	Gateway	•					
-	Access	-	Public hostnames				
Ħ	Networks New	-	+ Add a public hostname				
	Tunnels		Public hostname	Path	Service	Origin configurations	Menu
	Routes		1 gateway.cloudweg.com	*	https://127.0.0.1	0	:
<u>208</u>	My Team	•					
	Logs	•	Catch-all rule: http_status:404 Edit				
鐐	Settings						

#### 7. Append below lines in /usr/local/etc/ezlogin/ez.conf



## Now you can access Ezeelogin GUI via Cloudflare Zero Trust Network Access

Access Ezeelogin GUI with the **subdomain** created <u>https://gateway.cloudflare.com</u>

← → C (S https://gateway.cloudweg.com/ezlogin		Ď	Paused :
🔗 Ezeelogin			
Usemame			
Password			
Login	1		19 m .
and the second			
			· · · ·
Logged IP: 192 168 1.6			Pawered by ezeelogin.com

Accessing Ezeelogin Shell via Cloudflare Zero Trust Network Access

1. Add a Public Hostnames from dashboard > configure > public hostname > Add

a Public Hostnames

CLO	UDFLARE					Support	• ± •
←	Manuchacko@ezeel	•	<u> Back to tunnels</u>				
	Zero Trust overview		Ezeelogin				
G	Analytics	•	Overview Public Hostname Private Network				
Ð	Gateway	-					
Ð	Access	•	Public hostnames				
ø	Networks New	•	+ Add a public hostname				
	Tunnels		Public hostname	Path	Service	Origin configurations	Menu
	Routes		1 gateway.cloudweg.com	*	https://127.0.0.1	0	:
<u>208</u>	My Team	•	2 ezsh.cloudweg.com	*	ssh://127.0.0.1	0	:
	Logs	•					
<b>1</b> 93	Settings		Catch-all rule: http_status:404 Edit				
«	Collapse sidebar						

Choose a domain from the drop-down menu and specify any subdomain (for example,ezsh.cloudweg.com).

For Service, select **SSH**, enter **127.0.0.1** and click **save** hostname.

CLO								
←	Manuchacko@ezeel	۲	Public Hostname Page					
	Zero Trust overview		Add public hostname for Ezeelogin			I		
G	Analytics	•	Public hostname Subdomain Domain (Recuire Path					
Ð	Gateway	•						
Ð	Access	•						
K	Networks New	•	Service Type (Required) URL (Required)					
	Tunnels							
	Routes		SSH VIII 127.0.0.1 For example, https://localhost.8001					
200	My Team	•						
	Logs	•						
<b>1</b> 93	Settings		Additional application settings					
			×					
*	Collapse sidebar			Save hostna	ime	×		

# ??2. Connect as a Ezeelogin user from your Terminal via cloudflare Zero Trust Network Access

- 1. <u>Cloudflared on the client machine.</u>
- 2. Add the following to your SSH configuration file on your machine ~/.ssh/config:

Input the following values; replacing **ezsh.cloudweg.com** with the hostname you created. Edit **vim** ~/.ssh/config

Host ezsh.cloudweg.com

ProxyCommand /usr/local/bin/cloudflared access ssh --hostname %h

The cloudflared path may be different depending on your OS and package manager. For example, if you installed cloudflared on macOS with Homebrew, the path is /opt/homebrew/bin/cloudflared

 You can now test the connection by running a command to acess Ezeelogin shell via zero trust network access(ZTNA).
 Replace ezsh.cloudweg.com with the hostname you created.

ssh <	ezeelogin_	username>@ezsh	.cloudweg.com
-------	------------	----------------	---------------

	👌 Ez: Groups	×	👃 root@secgw: ~	x   +	~		-	>
	*Linux	aws						
	Production Servers							
	Windows All servers	aws List of	f all accessible	servers				
	ALL SEIVERS	Lise		Servers				
	GROUPS [Normal / ]							
C	Start typing name to	a locat/	a ESC: Close co	anch El/+ Holr	EU/I: Evit			

Online URL: <u>https://www.ezeelogin.com/kb/article/cloudflare-ztna-for-securing-ssh-access-to-endpoint-devices-720.html</u>