

Technical Guide

Remote VPN

Released: 2018-04-27 Doc Rev. No: R2

Copyright Notification

Edgecore Networks Corporation

[©] Copyright 2019 Edgecore Networks Corporation.

The information contained herein is subject to change without notice. This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered by Edgecore Networks Corporation. Edgecore Networks Corporation shall not be liable for technical or editorial errors or omissions contained herein.

Table of Contents

1.	Introduction	2
2.	Setup of Remote VPN - PPTP	
2.1	WLAN Controller Configuration	3
2.2	Remote Client Configuration	
3.	Setup of Remote VPN - IKEv2	15
3.1	WLAN Controller Configuration	15
3.2	Remote Client Configuration	21
4.	Conclusion	
5.	Remarks	

1. Introduction

Virtual private networks (VPNs) provide a way for secure connections to be established across the public network by tunneling the traffic. VPNs generally fall into two types—remote-access VPN and site-to-site VPN. Remote-access VPNs can be used to securely connect a host to a private network. For example, companies can allow staff to remotely access the file servers or other resources on the headquarters' intranet from an outside network using remote VPNs. With site-to-site VPNs, separate private networks could be joined for data sharing or other purposes. For example, private networks of different office branches of a company or even private networks of different companies can be joined.

In this technical guide, the Remote VPN feature on the controller is introduced, and guidance on how to setup and configure remote VPNs on the controller as well as on client devices is provided.

Technical Guide Remote VPN

2. Setup of Remote VPN - PPTP

2.1 WLAN Controller Configuration

Step 1.

Enter controller's IP address/domain name in browser and login as administrator.

LOGIN	
Username	
Password Log In	
Change password? English	

Figure 2-1-1. Controller's WMI Login Page

Step 2.

Create some accounts in the local database for remote VPN connections if local authentication is preferred. When other authentication methods are used, make sure accounts are created in the databases.

Go to **Users > Internal Authentication > Local > Local User List** to create local user accounts.

	SYSTEM	JSERS DEVICES	NETWORK	UTILITIES	STATUS
Groups	Main a Lisers a Internal Authent	ination a Local Authentication			
Authentication Servers		cauon / Local Admenication			
Internal Authentication	Server No. 1: Server 1 🔻				
Local					
On-Demand	Local Authenti	cation			
Guest					
One Time Password		Carteria			
External Authentication	Local User List	Conligure			
On-Demand Accounts	Account Roaming O	ut 🔍 Enable 🖲 D	isable		
Schedule	802.1X Authenticati	on 💿 Enable 🖲 D	isable		
Policies					
Blacklists			Annhy OC	maal	
Privilege Lists		L	W Apply	incer	
Additional Controls					

Figure 2-1-2. Create local user accounts

	SYSTEM		USER	S	DEVICES	NETWOR	к	UTILITIES	STATUS	
Groups	Main > Users > I	nternal Au	uthentication	> Local Authenti	ation > Local User Lis	t				
Authentication Servers										
Internal Authentication	Local U	ser	List							
Local										
On-Demand										
Guest	Add.	. Dele	te Backi	up List Uploa	d					Search
One Time Password				,						bearen
External Authentication		No	Status	Username	Password	MAC	Group	Activation	Expiration	Remark
On-Demand Accounts		1	Valid	1	1		Group 1			
Schedule			14-11-1		2					
Policies		2	Valid	2	2		Group 1			
Blacklists		3	Valid	3	3		Group 1			
Privilege Lists										
Additional Controls				(T	otal:3/10000) 🔤 Fire	st ⇔Prev Next⇒ L	.ast 🕬 Go to Pa	ge 1 ▼ (Page:1/1)	Rowp	oer Page: 10 ▼

After accounts are created, administrator can view the accounts' details in Local User List.

Figure 2-1-3. Local User List

Step 3.

Go to *Network > VPN > Remote VPN PPTP* and enable the function.

SYSTEM US	ERS DEVICES	NETWORK	UTILITIE	S STA	TUS
Remote VPN PF	РΤΡ				
Function Allocate IP Address fm WISPr Authentication Option	Enable Disable Activate SIP WAN I 172.29.0.1 Configure	nterface: WAN1			
	Auth Opt	ion Au	uth Database	Postfix	Enable
	Server	1	LOCAL	local	V
	Server	2	RADIUS	radius	
	Server	3	NTDOMAIN	ntdomain	
	Server Server	4	NTDOMAIN LDAP	ntdomain Idap	8 8
	Remote VPN PF Function Allocate IP Address fro WISPr Authentication Option	Remote VPN PPTP Function Enable Disable Activate SIP WAN II Allocate IP Address from VISPr Configure Authentication Options Auth Opt Server Server	Remote VPN PPTP Function Function Allocate IP Address from WISPr Configure Authentication Options Auth Option Auth Option Auth Server 1 Server 1 Server 2	Remote VPN PPTP Function Function Activate SIP WAN Interface: WAN1 Allocate IP Address from T72.29.0.1 WISPr Configure Authentication Options Auth Database Server 1 LOCAL Sever 2 PADULS	Function Enable Disable Activate SIP Akivate SIP WAN Interface: Allocate IP Address from 172.29.0.1 Interface: WISPr Configure Authentication Options Authentication Options Server 1 LOCAL local Server 2 PADIUS radius

Figure 2-1-4. Enable Remote VPN PPTP

Step 4.

Enter start IP address to be assigned to remote clients.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	ST	ATUS
NAT							
Monitor List	Remote VPI	N PPTP					
Walled Garden							
VPN	Function		Enable Disable				
Proxy Server	Tuncton						
Local DNS Records			Activate SIP WAN Inte	rface: WAN1			
Dynamic Routing	Allocate IP Ad	dress from	172.29.0.1				
DDNS	WISPr		Configure				
Client Mobility							
	Authentication	n Options					
			Auth Optior		Auth Database	Postfix	Enable
			Server 1		LOCAL	local	
			Server 2		RADIUS	radius	•
			Server 3		NTDOMAIN	ntdomain	•
			Server 4		LDAP	Idap	•
			Server 5		POP3	рор3	
	Demete VD						
	Remote VPI	N IKEV2					

Figure 2-1-5. Select start IP address for Remote VPN PPTP

Step 5.

Select authentication databases to be used for remote VPN connection.

	SYSTEM	USERS	DEVICES	NETWORK UTIL	ITIES ST	ATUS
NAT						
Monitor List	Remote VPN	PPTP				
Walled Garden						
/PN						
roxy Server	Function		🖲 Enable 🔍 Disable			
ocal DNS Records			Activate SIP WAN Interface	:: WAN1		
Dynamic Routing	Allocate IP Addr	ress from	172.29.0.1			
DNS	WISPr		Configure			
Client Mobility						
	Authentication	Options				
			Auth Option	Auth Database	Postfix	Enable
			Auth Option Server 1	Auth Database	Postfix	Enable 💌
			Auth Option Server 1 Server 2	Auth Database LOCAL RADIUS	Postfix local radius	Enable
			Auth Option Server 1 Server 2 Server 3	Auth Database LOCAL RADIUS NTDOMAIN	Postfix local radius ntdomain	Enable V V
			Auth Option Server 1 Server 2 Server 3 Server 4	Auth Database LOCAL RADIUS NTDOMAIN LDAP	Postfix local radius ntdomain ldap	Enable V V V
			Auth Option Server 1 Server 2 Server 3 Server 4 Server 5	Auth Database LOCAL RADIUS NTDOMAIN LDAP POP3	Postfix local radius ntdomain ldap pop3	Enable V V V

Figure 2-1-6. Select authentication databases for Remote VPN PPTP

Step 6.

Click *Apply* button at the bottom of the page and reboot the controller in order for the configuration to be effective.

NAT Monitor List Walled Garden VeN
Monitor List Walled Garden
Walled Garden
VPN
Proxy Server Local Sites
Local DNS Records
Dynamic Routing Add Delete
DDNS Local Local Remote Rémote
Client Mobility No. Botto Vendor Vendor Tunnel Status
Remote Sites
Add Delete
No. Name IP Address Pre-shared Key
Apply Cancel

Figure 2-1-7. Apply the configuration

Technical Guide Remote VPN

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
Administrator Accounts	Main > Utilities > Resta	art					
Backup & Restore							
Certificates	Restart						
Network Utilities							
Restart	Restart the syst	em in Regular V Mo	de				
System Upgrade	_						
	Reason for Rest	art :					
	Perform	detailed filesystem cheo	k during booting				
	- Tenomin	actuated mesystem ener	and an ing booting				
				Apply C	Cancel		

Figure 2-1-8. Restart the controller for the new configuration to take effect

2.2 Remote Client Configuration

2.3 Windows 10 Configuration

Step 1.

On Window 10 device, search for VPN in search bar to open VPN configuration.



Figure 2-2-1-1. VPN Configuration on Windows10 Device

Step 2.

Select Add a VPN connection to create a new VPN connection.

Settings	-	×
I VPN		
VPN		
+ Add a VPN connection		
PPTP		
IKEv2		
Advanced Options		
Allow VPN over metered networks		
On On		

Figure 2-2-1-2. Add a new VPN connection

Step 3.

Fill in the VPN configuration details and save it.

VPN provider: Select Windows (built-in).

Connection name: It can be anything you prefer.

Server name or address: Enter your server address.

VPN type: Select Point to Point Protocol (PPTP).

Type of sign-in info: Select User name and password.

User name (optional): Enter your remote user account username. E.g. 1@local **Password (optional):** Enter your remote user account password.

Settings	-		×
Add a VPN connection			
VPN provider			
Windows (built-in) \sim			
Connection name			
РРТР			
Server name or address			
VPN type			
Point to Point Tunneling Protocol (PPTP) \sim			
Type of sign-in info			
User name and password			
User name (optional)			
	Save	Cance	

Figure 2-2-1-3. VPN PPTP Configuration Details

Step 4.

After saving the connection, it will be shown in the VPN connection list. Click on *Connect* for establishing the connection.

Settings	_	×
毯 VPN		
VPN		^
+ Add a VPN connection		
KEv2		
рртр		
Connect Advanced options Remove		

Figure 2-2-1-4. Establish VPN connection

Step 5.

After a while, it will connect and show "Connected" status.

Settings				_	×
戀 VPN					
VPN					
+ Add a VPN connection	on				
IKEv2					
Connected					
	Advanced options	Disconnect			
			•		

Figure 2-2-1-5. Establish VPN connection

2.4 iPhone Configuration

iPhone no longer supports VPN-PPTP option since iOS10.

2.5 Android Configuration

Step 1.

Go to **Settings > More connection settings > VPN**. Click on **ADD VPN** to create a new VPN connection.



Figure 2-2-2-1. Add a new VPN connection

Step 2.

Fill in the VPN configuration details and click SAVE to save it.

Name: It can be anything you prefer.

Type: Select PPTP.

Server address: Enter your server name.

PPP encryption: Enable the option.



Figure 2-2-2-2. Android VPN PPTP Configuration

Step 3.

After the VPN configuration is saved, it will be shown in the VPN page. Select the configuration for PPTP and tap it to establish VPN connection.

● ← 🗑 = O 🕻 = ► balle/s - uale/s ← VPN	≵ © ি র_রা97% ∎ 11:47 ADD VPN MORE
🔅 РРТР	۵

Figure 2-2-2-3. Establish VPN connection

Step 4.

Enter remote user account's username and password and click *CONNECT* to continue establishing VPN connection.



Figure 2-2-2-4. Establish VPN connection

Step 5.

After the connection has been established successfully, it will show **Connected** for the connection.



Figure 2-2-2-5. Successful VPN connection

Technical Guide Remote VPN

3. Setup of Remote VPN - IKEv2

3.1 WLAN Controller Configuration

Step 1.

Enter the controller's IP address/domain name in browser and login as administrator.

	LOGIN		
User	name		
Pass	sword		
		Log In	
	000		
G F	hange password? orgot password?	English 🔻	

Figure 3-1-1. Controller's WMI Login Page

Step 2.

Create some accounts in the local database for remote VPN connections if local authentication is preferred. When other authentication methods are used, make sure accounts are created in the databases.

Go to **Users > Internal Authentication > Local > Local User List** to create local user accounts.

Groups Main > Users > Internal Authentication > Local Authentication Authentication Servers Server No. 1: Server 1 Local Server No. 1: Server 1 Local Authentication Local Authentication Green Come Password Local User List Condemand Accounts Configure Authentication Enable © Disable Schedule B02:1X Authentication Policles Blacklists Privilege Lists Additional Controls		SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
Authentication Servers Internal Authentication Incoal On-Demand Guest On-Demand Accounts Schedule Policies Blacklists Additional Controls	Groups	Main > Users > Internal Auth	nentication > Local >	Authentication			
Internal Authentication Server No. 1: Server 1 Local Cond Top Parand Guest Cocal Authentication One Time Password Local User List Cocal Local User List Configure Account Roaming Out Enable © Disable Schedule 802.1X Authentication Policies Blacklists Privilege Lists Additional Controls	Authentication Servers						
Local On-Demand Guest One Time Password One Time Password One Time Password One Time Password One Time Password Done Time Password Cocal User List Configure Account Roaming Out Enable © Disable 802.1X Authentication Enable © Disable Policel 802.1X Authentication Enable © Disable Enable © Disable Configure Account Roaming Out Enable © Disable Enable © Disable Configure Account Roaming Out Enable © Disable Configure Config	Internal Authentication	Server No. 1 : Server 1	•				
On-Demand Local Authentication Guest Image: Configure	Local						
Guest One Time Password External Authentication I.ocal User List On-Demand Accounts Account Roaming Out Schedule 802.1X Authentication Policies Blacklists Privilege Lists Additional Controls	On-Demand	Local Auther	ntication				
One Time Password Local User List External Authentication Account Roaming Out On-Demand Accounts Enable © Disable Schedule 802.1X Authentication Policies Blacklists Privilege Lists Additional Controls	Guest						
External Authentication Courd Set Est Compare On-Demand Accounts Account Roaming Out Enable ® Disable Schedule 802.1X Authentication Enable ® Disable Policies Privilege Lists Cancel Additional Controls Additional Controls Cancel	One Time Password	Local Licer List		Configure			
On-Demand Accounts Account Roaming Out Enable © Disable Schedule 802.1X Authentication Enable © Disable Policies Privilege Lists Cancel	External Authentication	Local Oser List		coningure			
Schedule 802.1X Authentication Enable Disable Policies Enable Disable Blacklists Privilege Lists Cancel Additional Controls Cancel Cancel	On-Demand Accounts	Account Roamin	g Out	Enable I Disable	2		
Policies Blacklists Privilege Lists Additional Controls	Schedule	802.1X Authentie	cation	🔍 Enable 🖲 Disable	2		
Blacklists Privilege Lists Additional Controls	Policies						
Privilege Lists Additional Controls	Blacklists				Apply	ancel	
Additional Controls	Privilege Lists			_			
	Additional Controls						

Figure 3-1-2. Create local user accounts

	SYSTEM		USER	ts	DEVICES	NETWOR	к	UTILITIES	STATUS	
Groups	Main > Users > I	nternal A	uthenticatio	n > Local Authentic	ation > Local User Lis	t				
Authentication Servers										
Internal Authentication	Local U	ser	List							
Local										
On-Demand										
Guest	Add	. Dele	ete Back	up List Uploa	d					Search
One Time Password										
External Authentication		No	Status	Username	Password	MAC	Group	Activation	Expiration	Remark
On-Demand Accounts		1	Valid	1	1		Group 1			
Schedule		-	Male 4	2	2					
Policies	-	2	valid	2	2		Group I			
Blacklists		3	Valid	3	3		Group 1			
Privilege Lists										
Additional Controls				(10	otal:3/10000) Pering	st errev Nexte L	aster Go to Pa	ige I V (Page:1/1)	Kow p	er Page: 10

After accounts are created, administrator can view the accounts' details in Local User List.

Figure 3-1-3. Local User List

Step 3.

SYSTEM USERS DEVICES NETWORK UTILITIES STATUS Administrator Accounts Main > Utilities > Certificates Backup & Restore Certificate Management Certificates Network Utilities Restart Common Name Used by System Upgrade Cert Name System Certificate 🧳 Default Certificate WEB Server, Built-in RADIUS CN=gateway.example.com Internal Root CA 🥒 Internal Root CA N/A Internally Issued Certificate 🧳 N/A N/A Trusted Certificate Authorities (CA) N/A N/A

Go to Utilities > Certificates and edit System Certificate.

Figure 3-1-4. Edit System Certificate

Step 4.

Upload a valid certificate with its key and/or intermediate CA for the use of remote VPN IKEv2.

	SYSTEM USE	ERS DEVICES	NETWORK	UTILITIES STATUS
Administrator Accounts			Factory Default Cartificate	
Backup & Restore			Factory Default Certificate	
Certificates	Factory Default Certificate	CN=gateway.example.com	View	
Network Utilities				
Restart			Internally Issued Certificate	
System Upgrade	N/A	N/A	View Delete	
			Uploaded Certificate	
	N/A	N/A	View Delete	Upload Intermediate/Root CA Verify
	Upload System (Certificate Private Key Intermediate CA	Certificate Choose File No fil Choose File No fil Choose File No fil	e chosen e chosen e chosen	

Figure 3-1-5. Upload Certificate for Remote VPN IKEv2

Technical Guide Remote VPN

After uploading the certificate, administrator will be able to view it in the **System Certificate** page.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
General	Main > Utilities > Certificate	s > System Certificate	2				
WAN							
IPv6	System Cert	ificate					
LAN Ports							
High Availability	Cort Na	ma	Common Nama			Operation	
Service Zones	Cert Na		common Name			Operation	
Port Location Mapping				Factory Default Certificate			
PMS Interface	Factory Default Certi	ficate	CN=gateway.example.com	View			
				Internally Issued Certificate			
	N/A]	N/A	View Delete			
				Uploaded Certificate			
	upload1			View Delete	Upload Interme	diate/Root CA Verify	
						THE REPORT	
	Upload Syst	em Certifi	cate				
	Certificate		Choose File No file	chosen			

Figure 3-1-6. Uploaded Certificates Overview

Important: Make sure the server name matches certificate's CN and also the server name must be an existent domain name. Otherwise, Windows clients may fail to establish VPN connection with the controller.

Step 5.

Go to *Network > VPN > Remote VPN IKEv2* and enable the function.

	SYSTEM	USERS	DEVICES	ETWORK UTILITIE	s st	ATUS
NAT						
Monitor List	Remote VPN	IKEv2				
Walled Garden						
VPN	Eurotion		🖲 Epoble 🔘 Dicable			
Proxy Server	Tunction					
Local DNS Records	Allocate IP Addre	ss from	IP Address 172.16.0.1	* Subnet Mask 255.255.255.0 (/24) •	
Dynamic Routing	Certificate		UPLOAD 1			
DDNS	WISPr		Configure			
Client Mobility	Authentication C	ptions				
			Auth Option	Auth Database	Postfix	Enable
			Server 1	LOCAL	local	
			Server 2	RADIUS	radius	
			Server 2 Server 3	RADIUS	radius ntdomain	
			Server 2 Server 3 Server 4	RADIUS NTDOMAIN LDAP	radius ntdomain Idap	

Figure 3-1-7. Enable Remote VPN IKEv2

Step 6.

Enter start IP address to be assigned to remote clients.

	SYSTEM USERS	S DEVICES	NETWORK UTILIT	IES ST/	ATUS
NAT Monitor List	Remote VPN IKE	2			
Walled Garden VPN Proxy Server	Function	🖲 Enable 🔘 Disable			
Local DNS Records	Allocate IP Address from	IP Address 172.16.0.1	* Subnet Mask 255.255.255.0 (/2	24) 🔻	
Dynamic Routing	Certificate	UPLOAD 1			
DDNS	WISPr	Configure			
Client Mobility	Authentication Options				
		Auth Option	Auth Database	Postfix	Enable
		Server 1	LOCAL	local	
		Server 2	RADIUS	radius	
		Server 3	NTDOMAIN	ntdomain	
				latera -	
		Server 4	LDAP	idap	

Figure 3-1-8. Select start IP address for Remote VPN IKEv2

Step 7.

Select Certificate to be used for remote VPN connection.

	SYSTEM	USERS	DEVICES NE	TWORK UTILITI	ES ST.	ATUS
NAT						
Monitor List	Remote VI	PN IKEv2				
Walled Garden						
VPN	Euprtion		Feable Disable			
Proxy Server	rancion					
Local DNS Records	Allocate IP A	Address from	IP Address 172.16.0.1 *:	Subnet Mask 255.255.255.0 (/2-	4) 🔻	
Dynamic Routing	Certificate		UPLOAD 1 🔻			
DDNS	WISPr		Configure			
Client Mobility	Authenticat	ion Options				
			Auth Option	Auth Database	Postfix	Enable
			Server 1	LOCAL	local	
			Server 2	RADIUS	radius	
			Server 3	NTDOMAIN	ntdomain	
			Server 4	LDAP	Idap	

Figure 3-1-9. Select Certificate for Remote VPN IKEv2

Step 8.

Select authentication databases to be used for remote VPN connection.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
NAT Monitor List Walled Garden	Remote VPN	IKEv2				
VPN VPN Voxy Server Local DNS Records Dynamic Routing DDNS Client Mobility	Function Allocate IP Address Certificate WISPr Authentication Opt	from	Enable Disable IP Address 172.16.0.1 UPLOAD 1 Configure	* Subnet Mask 255.255	5.255.0 (/24)	
			Auth Optic	n Auth Datab	oase Postfix	c Enable
			Server 1	LOCAL	local	
			Server 2	RADIUS	radius	
			Server 3	NTDOMA	IN ntdoma	in 🛛
			Server 4	LDAP	Idap	
			Server 5	POP3	рор3	

Figure 3-1-10. Select authentication databases for Remote VPN IKEv2

Step 9.

Click *Apply* button at the bottom of the page and reboot the controller in order for the configuration to be effective.

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS
NAT						
Monitor List	Cito to Cit					
Walled Garden	5116-10-511	e v f N				
VPN						
Proxy Server	Local Sites					
Local DNS Records						
Dynamic Routing	-	Add Delete				
DDNS			Local Local	Remote	Remote	
Client Mobility		No. Ho	st/Subnet Interface	VPN Gateway	Host/Subnet	Tunnel Status
	Remote Site	S				
	A	Add Delete				
		No.	Name	IP Address	Pre-sł	nared Key
			01	Apply S Canc	el	

Figure 3-1-11. Apply the configuration

	SYSTEM	USERS	DEVICES	NETWORK	UTILITIES	STATUS	
Administrator Accounts	Main > Utilities > Resta	rt					
Backup & Restore							
Certificates	Restart						
Network Utilities							
Restart	Restart the syst	em in Regular V Moo	de				
System Upgrade			Les Martin Martin				
	Reason for Rest	art :					
	Perform	detailed filesystem chec	k during booting				
	0						
				Apply	Cancel		

Figure 3-1-12. Restart WHG for the new configuration to be effective

- 3.2 Remote Client Configuration
- 3.3 Windows 10 Configuration

Step 1.

On a Window 10 device, search for VPN in search bar to open VPN configuration.



Figure 3-2-1-1. VPN Configuration on Windows 10 Device

Step 2.

Select Add a VPN connection to create a new VPN connection.

Settings	-	×
☺ VPN		
VPN		
+ Add a VPN connection		
о РРТР РРТР		
KEv2		
Advanced Options		
Allow VPN over metered networks		
On On		

Figure 3-2-1-2. Add a new VPN connection

Step 3.

Fill in the VPN configuration details and save it.

VPN provider: Select Windows (built-in).

Connection name: It can be anything you prefer.

Server name or address: Enter your server name.

VPN type: Select IKEv2.

Type of sign-in info: Select User name and password.

User name (optional): Enter your remote user account username. E.g. 1@local **Password (optional):** Enter your remote user account password.

Settings			—		×
Add a VPN connection					
VPN provider					
Windows (built-in)	×				
	-				
INEV2					
Server name or address					
Aurofilenersy					
VPN type					
IKEv2	~ I				
Type of sian-in info					
User name and password	~				
		Save		Cancel	
		Juve		Curreer	

Figure 3-2-1-3. VPN IKEv2 Configuration Details

Important: Make sure the server name matches certificate's CN and also the server name must be an existent domain name. Otherwise, Windows clients may fail to establish VPN connection with the controller.

Step 4.

After saving the connection, it will be shown in the VPN connection list. Click on *Connect* for establishing the connection.

_		\times
		^
	-	- 0

Figure 3-2-1-4. Establish VPN connection

Step 5.

After a while, it will connect and show *Connected* status.

Settings	-	\times
VPN		
VPN		
+ Add a VPN connection		
KEv2		
Connected		
Advanced options Disconnect		

Figure 3-2-1-5. Successful VPN Connection

3.4 iPhone Configuration

Step 1.

On an iPhone, go to **Settings > General > VPN**. Click on **Add VPN Configuration** to create a new VPN connection.

11:34			11 4G 🖼	5:4	41	1 4G	5:41	 4G	5:41		11 4G 🔳
2,287	Thursday				Settings		Settings Gen	eral	Ceneral	VPN	
	19			\otimes	General	>	Destrictions	0.65			
Mail	Calendar	Photos	Camera	AA	Display & Brightness	>	Restrictions	UI >	Add VPN Conf	iguration	
	11 12 1 2 9 3 8 7 5 5			*	Wallpaper	>	Date & Time	>			
Maps	Clock	Weather	Home	((())	Sounds & Haptics	>	Keyboard	>			
	ww		X		Siri & Search	>	Language & Region	>			
Notes	Stocks	Reminders	App Store	(Ŀ)	Face ID & Passcode	>	Dictionary	\geq			
				SOS	Emergency SOS	>					
				⊐≻	Battery		iTunes Wi-Fi Sync	>	⇒		
	IBOOKS		svanet		Privacy	>	VPN	Not Connected >			
		Children of	Sept. Said				Device Management	MONSTAR LAB, INC. >			
Videos -	Settings	-		A	iTunes & App Store	>					
			and the second		Wallet & Apple Pay	>	Regulatory	>			
		and the second s									
				?	Accounts & Passwords	>	Reset	>			
	-				Mail	>	Shut Down				
			50		Contacts	>					
Concession of the local division of the loca		and the second			Calandar	>			-		-

Figure 3-2-2-1. Add a new VPN connection

Step 2.

Fill in the VPN configuration details and click **Done** to save it.

Type: Select *IKEv2*.

Description: It can be anything you prefer.

Server: Enter your server name.

Remote ID: Enter your server name.

Local ID: Leave empty.

User Authentication: Select username.

Username: Enter your remote user account username. E.g. 1@local **Password:** Enter your remote user account password. **Proxy:** Select *Off*.

5:43		11 4G
Cancel	IKEv2	
Туре		IKEv2
Description	IKEv2	
Server	{Your VPN Server N	lame}
Remote ID	{Your VPN Server N	lame}
Local ID		
AUTHENTICAT	ION	
User Auther	ntication	Username >
Username	1@local	
Password	•	
PROXY		

Figure 3-2-2-2. iPhone VPN IKEv2 Configuration

Step 3.

After the VPN configuration is saved, it will be shown in the VPN page. Select the configuration for IKEv2 and tap the Status slider to establish VPN connection.

11:35	ti 4G 🐲
〈 General	VPN
VPN CONFIGURATIO	ONS
Status	Not Connected
 IKEv2 Unknown 	(j)
Add VPN Config	guration

Figure 3-2-2-3. Establish VPN connection

Step 4.

After the connection has been established successfully, it will show **Connected** on the Status field.

5:45	•••• 4G
≺ General	PN
Status	
✓ IKEv2 Unknown	(j)
Add VPN Configuratio	n

Figure 3-2-2-4. Successful VPN Connection

3.5 Android Configuration

EWS controller currently only supports EAP-only authentication in IKEv2 but not other types of authentication, such as IKEv2 PSK or IKEv2 RSA. However, built-in VPN function on Android devices only supports IKEv2 PSK or IKEv2 RSA; therefore, it is required to use a third-party VPN APP that supports EAP-IKEv2 to establish VPN IKEv2 connection with the controller. In this guide, we use strongSwan APP as an example, but another APP that has the same feature can also be used.

Step 1.

Open strongSwan APP and click **ADD VPN PROFILE** to create a new VPN configuration.



Figure 3-2-3-1. Add a new VPN connection

Step 2.

Fill in the VPN configuration details and click **SAVE** to save it.

Server: Enter your server name.

VPN Type: Select IKEv2 EAP (Username/Password).

Username: Enter your remote user account username. E.g. 1@local **Password (Optional):** Enter your remote user account password.

CA certificate: Tick Select automatically.

Profile name (optional): Leave empty.

💩 🖬 🚰 🎯 🗋 🖬 📂	■∰© ଢ⊭ ≉©?, // 97%∎11			
0:0kb/s 0:0kb/s ← Add VPN profile	SAVE	CANCEL		
	SATE	CANCEL		
Server				
VPN Type				
IKEv2 EAP (Username/Pas	sword)	-		
Username				
1@local				
Password (optional)				
•				
CA certificate				
Select automatically				
Profile name (optional)				
Defaults to "remote.4ipnet.com"				
Show advanced settings				

Figure 3-2-3-2. Android VPN IKEv2 Configuration

Step 3.

After the VPN configuration is saved, it will be shown in the strongSwan APP. Tap the configuration to establish VPN connection.



Figure 3-2-3-3. Establish VPN connection

Step 4.

After the connection has been established successfully, it will show *Connected* on the Status field in strongSwan APP. Additionally, it will also show *Connected* for the VPN connection in Android's VPN page.



Figure 3-2-3-4. Successful VPN Connection

4. Conclusion

Some end users would like to access company network when they are outside of office or traveling so that they can access the file servers or have their internet traffic go through company network.

Remote VPN can be built using the EWS controller. Furthermore, any Local Accounts can remotely access the network resource under some certain wireless LAN environment, such as workplace, school, SMB, etc. That is, any employees could experience the wireless LAN of the certain application without any restriction.

5. Remarks

For more information, please contact your local Systems Integrator, or contact support@4ipnet.com for support.