1. Login the OPNsense server

In this case, the OPNsense server IP is 60.208.44.205. If you have your own OpenVPN server, you can login your server with correct username and password.

In this case, we configure the OpenVPN server and the OpenVPN clients to achieve the function as the following picture:



2. Create authorities and certificates

2.1 Create a CA certificate.

System->Trust->Authorities

ZOPOsense' <						root@OPNsense.localdomain	٩
Lobby	System: Trust: A	uthorities					
E System 1	Name	Internal	Issuer	Certificates	Distinguished Name		4 💌
Configuration 9 Firmware	OpenVPN_CA	YES	self-signed	3	emailAddress=renchengcheng@usr.cn, ST=SD, O=USR, L=JN, CN=internal-ca, C=AD Valid From: Tue, 21 Mar 2023 2020:28-0800 Valid Until: Mon, 23 Jun 2025 2023:28-0800		/ ± ± 0
Gateways 4 High Availability 2	OpenVPN1_CA	YES	self-signed	0	emailAddress=rencheng@usr.cn, ST=SD, O=usr, L=JN, CN=internai-ca, C=CN Valid From: Wed, 22 Mar 2023 18:02:14 -0800 Valid Until: Tus. 24 Jan 2025 18:02:14 -0800		/
Routes Routes Total Settings 0	test	YES	self-signed	1	emailAddress=wangchenglong@usr.cn, ST=SD, O=test, L=jn, CN=test, C=AD Valid From: Wed, 22 Mar 2023 38:14:50 - 0800 Valid Until: Tus 24 Jun 2025 38:14:50 - 0800		
3 Authorities Certificates							

Edit authorities:

🖵 Lobby	System: Truct: Authoritics	
Reporting	System: Trust: Authorities	
🚍 System		
Access 🐸		
Configuration ${\mathfrak D}$	Descriptive name 1	OpenVPN-Test-CA
Firmware	@Wathod	
Gateways 🕈	2 Z	Create an internal Certificate Authority
High Availability 2	Internal Certificate Authority	
Routes 🗧		
Settings 🕫	e ney type	RSA -
Trust	Kev length (bits)	
Authorities		2048
Certificates	1 Digest Algorithm	SHA256 .
Revocation		017 200
Wizard 🌮	Difetime (days)	825
Log Files 🐵		
Diagnostics 🔯	Distinguished name	
📥 Interfaces	Country Code :	AD (Andorra)
✤ Firewall	2	
VPN	3 State or Province :	SD
Services		
🖋 Power	• City:	Jinan
Help	Organization :	
	Organization.	PUSR
	• Email Address :	liumeimei@u:r.cn
	1 Common Name :	internal-ca
	4	Save

2.2 Create Server Certificate

System->Trust->Certificates

	Lobby		Suchemu Truch Contificates			
	Reporting		system: Trust: Certificates			
-	System 1		Name	Issuer	Distinguished Name	4 🖬
	Access	9 9	Web GUI TLS certificate	self-signed	ST=Zuid-Holland, O=OPHisense self-signed web certificate, L=Hiddelhamis, CH=OPKisense.localdomain, C=NL Valid Form: Thu: 23 Eek 2023 021 (957 + 0800	0 4 4 5
	Firmware		CA: No, Server: Yes		Valid Until: Tue, 26 Mar 2024 02:19:57 +0800	
	High Availability	0	OpenVPN_Server_Cert	OpenVPN_CA	emailAddress=rencheng@usr.cn, ST=SD, Q=USR, L=JN, CN=Open/VPN_Server_Cert, C=AD Valid From: Tue, 21 Mar 2023 20:30:49 +0800	OpenVPN Server
	Routes	÷	CA: No, Server: Yes		Valid Until: Sun, 21 Apr 2024 20:30:49 +0800	
	Settings	00	• test	test	emailAddress=wangchenglong@usr.cn, ST=SD, O=test, L=jn, CN=test, C=AD	User Cert
	Trust 2 Authorities	•	CA: No, Server: No		Valid Prom: Wed, 22 Mar 2023 18:18:11 +0000 Valid Until: Mon, 22 Apr 2024 18:18:11 +0800	0 1 1 1
	Certificates 3		OpenVPN_Client1	OpenVPN_CA	emailAddress=rencheng@uss.cn, ST=SD, O=USR, L=JN, CN=OpenVPN_Clients, C=AD Valid From: Thu: 23 Mar 2023 20:55(23 +0800	User Cert
	Revocation		CA: No, Server: No		Valid Unbit: Tue, 23 Apr 2024 20:55:23 +0800	

1>Method: Select "Create an internal Certificate",

2>Enter the descriptive name of the certificate,

3>Certificates authority: Select the "OpenVPN-Test-CA" which is created in the Step 2.1,

4>Type: Server Certificate,

5>Enter the common name,

6>Click "Save".

Method	1 Create an internal Certificate -
Descriptive name	2 OpenVPN-Test-Sever-Cert
Internal Certificate	
Certificate authority	3 OpenVPN-Test-CA
6 Туре	4 Server Certificate -
🚯 Кеу Туре	RSA -
Key length (bits)	2048 -
0 Digest Algorithm	SHA256 -
O Lifetime (days)	397
Private key location	Save on this firewall 🔹
Distinguished name	
Ountry Code :	AD (Andorra)
• State or Province :	SD
Oity:	Jinan
Organization :	PUSR
• Email Address :	liumeimei@usr.cn
Ocommon Name :	5 OpenVPN-Test-Sever-Cert

2.3 Add users and create user certificates

System->Access->Users

2 C	PD <mark>sense</mark> <						root@OPNsense.localdomain	۹	
🖵 Lobby			System: Access: Users						
Report	ing		-,						
System Acce	1 ■_2		Username		Full name		Groups	4 🖬	
Use	3		CpenVPN_Client1					/ 0	
Gra Ser	ips Nrs		CpenVPN_Client2					/ 8	
Tes	ar		≜ root		System Administrator		admins	1	
Conf	guration	ອ 	≜ test					/ 1	
Gate	uays	1		System Administrator	& Disabled User	👗 Normal User			

1>Enter custom username,

2>Enter the password,

3>Confirm the password,

4>Check the "Click to create a user certificate",

5>Click "Save" button.

System: Access: Users	
Defined by	USER
1 Disabled	
Username	1 OpenVPN-Test-Client1
Password	2
	Confirmation)
6 Group Memberships	Not Member Of
	admins
• Certificate	Click to create a user certificate.
OTP seed	

After clicking the "Save" button, it will automatically redirect to a new page as following, in this page:

- 1> Method: Create an internal Certificate,
- 2> Certificates authority: Select the "OpenVPN-Test-CA" which is created in the Step 2.1,
- 3> The other parameters stay the default,
- 4> Click "Save" button.

System: Trust: Certificates	
Method	Create an internal Certificate
O Descriptive name	OpenVPN-Test-Client1
Internal Certificate	
Certificate authority	2 OpenVPN-Test-CA -
Ө Туре	Client Certificate 🔹
• Кеу Туре	RSA -

After saving the parameters, it will return to the user accessing page, and we can see the user certificate listed. Then we need to click "Save and go back".

Effective Privileges	Inherited from			Туре	Name	
() User Certificates	Name OpenVPN-Test-Client1 +	CA OpenVPN-Test-CA	Valid From Mon, 17 Apr 2023 20:21:49 +0800		Valid To Sat, 18 May 2024 20:21:49 +0800	* *
O API keys	key					
OTP seed	Generate new secret (160 bit)					
O Authorized keys	Paste an authorized keys file here.					,
IPsec Pre-Shared Key	Save Save and go back Canc	zel				

In this case, we need 2 users and certificates, and the second one can be added using the same steps.

2.4 Configure OpenVPN Server

VPN->OpenVPN->Servers->Use a wizard to setup a new server

Lobby		VPN: OpenV	PN: Servers			
■ System			Protocol / Port	Tunnel Network	Description	4
Firewall		•	UDP/1194	10.0.8.0/24		
VPN IPsec	•					
OpenVPN 2	•					
Clients						

1>Type of Server: Local User Access

Lobby	V	PN: OpenVPN: Servers: Authentication Type Selection
📥 Reporting		
System		
🛔 Interfaces		Select an Authentication Backend Type
👌 Firewall		Type of Server: Local User Access
VPN		
IPsec	a	If you are unsure, leave this set to "Local User Access".
OpenVPN	A	Next
Servers		
Clients		

2>Certificate Authority: "OpenVPN-Test-CA" created in Step 2.1

Lobby Reporting	VPN: OpenVPN: Servers: Certificate Authority Selection
≣ System	
👍 Interfaces	Choose a Certificate Authority (CA)
✤ Firewall	2 Certificate Authority: OpenVPN-Test-CA
VPN	
IPsec 🔒	Add new CA
OpenVPN	
Servers	Next
Clients	

3>Certificate: "OpenVPN-Server-Test-Cert" created in Step 2.2

 Lobby Reporting 	V	/PN: OpenVPN: Servers: Server Certificate Selection
🗮 System		Choose a Server Cartificate
A Interfaces		
🚯 Firewall		3 Certificate: OpenVPN.Test.Sever-Cert -
VPN		
IPsec	a	Add new Certificate
OpenVPN	a	
Servers		Next
Clients		

4>Tunnel Settings->IPv4 Tunnel Network: 10.0.20.0/24

Tunnel Settings		
	IPvit Tunnel Network: 10.0.20.0/24	
	This is the IP-4 virtual network used for private communications between this server and client hosts expressed using CIDR (eg. 10.0.8.0/24). The first network address will be assigned to tremaining network addresses can optionally be assigned to connecting clients. (see Address Pool)	ne server virtual interface. The
	IPv6 Tunnel Network:	

5>Tunnel Settings->Inter-Client Communication

Tips: The other parameters in "Server Setup" page can stay default.

Compression:	No Preference -
	Compress tunnel packets using the LZO algorithm. Adaptive compression will dynamically disable compression for a period of time if OpenVPN detects that the data in the packets is not being compressed efficiently.
Type-of-Service:	Set the TOS IP header value of tunnel packets to match the encapsulated packet value.
5 Inter-Client Communication:	Allow communication between clients connected to this server.
Duplicate Connections:	Allow multiple concurrent connections from clients using the same Common Name. This is not generally recommended, but may be needed for some scenarios.

6>Firewall and OpenVPN rules need be enabled in this case.

	Lobby	1/5	NI: On an VONI: Samuran Einmunit Dula Canfingunation
	Reporting	VP	N: OpenVPN: Servers: Firewall Rule Configuration
	System		
÷	Interfaces		Firewall Rule Configuration
69	Firewall		
0	VPN		Firewall Bules control what network traffic is permitted. You must add rules to allow traffic to the Open/PN server's IP and port, as wells as allowing traffic from connected clients through the tunnel. These rules can be automatically added here, or configured manually after completing the tunnel. These rules can be automatically added here, or configured manually after completing the tunnel.
	IPsec	•	
	OpenVPN	•	Iramic trom cuents to server
	Servers		Firewall Rules: 🖬 Add a rule to permit traffic from clients on the Internet to the OpenIPN server process.
	Clients		Tooffic from clients through VPN 6
	Client Specific Overrides		
	Client Export		OpenVPN rule: 🖬 Add a rule to allow all traffic from connected clients to pass across the VPN tunnel.
	Connection Status		
	Log File		

7>Click "Finished" button, the servers are listed. "UDP / 1195" is the server we added.

😐 Lobby	VDN: OnenV	DN: Comiero								
🕍 Reporting	VPN: Openv	/N: UpenVPN: Servers								
I System		Protocol / Doct	Turned Mekande	Description						
A Interfaces		Protocol/Port	runnes network	Description						
49 Firewall	•	UDP/1194	10.0.8.0/24		/ 2 0					
VPN		UDP / 1195	10.0.20.0/24		/ = 0					
IPsec 🔒										

2.6 Configure the OpenVPN client and subnet

VPN->OpenVPN->Client Specific Overrides

ZOPO <mark>sense'</mark> <						root@OPNsense.localdomain
므 Lobby			N. Client Specific Overwider			
📥 Reporting	`	VPN: OpenvP	N: Client Specific Overrides			
I System						
📥 Interfaces			Common Name	Tunnel Network	Description	4 🖬 ∗ 🗉
6 Firewall			OpenVPN_Client1			< / i C
© VPN 1			OpenVPN_Client2			< / B C
IPsec	A					
OpenVPN 2	e					
Servers						
Clients						
Client Specific Overrides 3						
Client Export						
Connection Status						

1>Servers: Select "1195 / UDP" added in chapter 2.4,

2>Common name: This name should be kept consistent with the first username in chapter 2.3,

3>IPv4 Local Network: 192.168.33.0/24, the second router's LAN IP,

4> IPv4 Remote Network: 192.168.32.0/24, the first router's LAN IP,

5>Click "Save".

VPN: OpenVPN: Client Specific Overrides					
General information					
() Disabled					
() Servers	1 (1195 / UDP) -				
() Common name	2 OpenVPN-Test-Client1				
() Description					
Connection blocking					
Tunnel Settings					
1 IPv4 Tunnel Network					
1Pv6 Tunnel Network					
1 IPv4 Local Network	3 192.168.33.0/24				
19 IPv6 Local Network					
1 IPv4 Remote Network	4 192.168.32.0/24				
19 IPv6 Remote Network					

In this case, we need 2 clients, and the second one can be added using the same steps.

1>Servers: Select "1195 / UDP" added in chapter 2.4,

2>Common name: This name should be kept consistent with the second username in chapter 2.3,

3>IPv4 Local Network: 192.168.32.0/24, the first router's LAN IP,

4> IPv4 Remote Network: 192.168.33.0/24, the second router's LAN IP,

5>Click "Save".

General information	
() Disabled	
0 Servers	1 (1195 / UDP) -
0 Common name	2 OpenVPN-Test-Client2
Description	
Ocnnection blocking	
Tunnel Settings	
0 IPv4 Tunnel Network	
0 IPv6 Tunnel Network	
0 IPv4 Local Network	3 192.168.32.0/24
() IPv6 Local Network	
() IPv4 Remote Network	4 192.168.33.0/24
IPv6 Remote Network	

2.7 Export the OpenVPN client package

VPN->OpenVPN->Client Export

1> Remote Access Server: Server UDP:1195,

2>Download the package of Client1,

3> Download the package of Client2.

ZOPOsense <					root@OPNsense.localdomain	Q	
😐 Lobby		VDN OF HIVDN Climat Free est					
📥 Reporting		VPN: OpenVPN: Client Export					
I System							
🚠 Interfaces		Remote Access Server	1				
Firewall			Server UDP:1195				
VPN		Export type					
IPsec	•		Clear Al				
OpenVPN	-	Hostname	60 200 44 205				
Servers			0.20074.200				
Client Specific Overrides		() Port	1195				
Client Export		() Use random local port					
Connection Status		() Validate server subject					
Log File		O Windows Certificate System Store	0				
Services		O Disable password save					
🗲 Power		Custom config					
C Help			h				
		Accounts / certificates					
		Certificate		Linked user(s)			
		(none) Exclude certificate from export					۵
		Open/VPN-Test-Sever-Cert				2	۵
		OpenVPN-Test-Client1		OpenVPN-Test-Client1			۵
		OpenVPN-Test-Client2		OpenVPN-Test-Client2		3	۵

The downloaded file.

📕 🗹 📕 🗢 openvpn					-	
File Home Share View						~ 🕐
\leftarrow \rightarrow \checkmark \uparrow] \blacktriangleright openvpn				5 V		م
🛨 Quick access	Name	Date modified	Туре	Size		
Desisten	openvpn_OpenVPN_Test_Client1.ovpn	4/18/2023 4:38 PM	OVPN File	6 KB		
Desktop x	openvpn_OpenVPN_Test_Client2.ovpn	4/18/2023 4:38 PM	OVPN File	6 KB		
Documents	*					

3. Configure router's parameters

3.1 Configure the first router as OpenVPN Client1 1>Change LAN IP to 192.168.32.1

tus	Interface Ove	erview		
ervices	Network	Status		Actions
VPN Network Interfaces	الله الله الله الله الله الله الله الله	W Uptime: 0h 5m 5 (mac) (mac) (m	54s D4:AD:20:4F:FD:E3 559 Pkts.) 72 Pkts.) U24	🥔 Connect 🗐 Edit
SIM Card Network Switch	WAN Et	MAC-Address: RX: 0.00 B (0 Pkt h1 TX: 0.00 B (0 Pkt)E:2D:88:72:A1:CB s.) s.)	🖉 Connect 📝 Edit
Wifi DHCP Hostnames	WAN_ 알 eth	WIRED Uptime: 0h 5m 4 MAC-Address: MAC-Address: RX: 1.59 MB (33) TX: 796.98 KB (2) IPv4: 192.168.88 IPv4: 192.168.88	43s 54:AD:20:4F:FD:E1 35 Pkts.) 554 Pkts.) .234/24	🦉 Connect 🛛 🛃 Edit
twork	G	ieneral Setup		
erfaces			-7	
1 Card		Status	ور br-lan	Uptime: 0h 7m 16s MAC-Address: D4:AD:20:4F:FD:E3
work Switch				RX : 1.08 MB (4550 Pkts.) TX : 2.69 MB (4440 Pkts.)
				1 V 11 152 100 111724
		Destand	Statia address	
mes		Protocol	Static address	Ť
Routes		IPv4 address	192.168.32.1	
ostics		IPv4 netmask	255.255.255.0	~
1	1	Ise custom DNS servers	8.8.8.8	×
N/LAN Port			114.114.114.114	2

2>Modify the OpenVPN parameter,

> Status	En	nhanced OpenVPN desig	n allows 3 OpenVPN (Clients and 1 OpenVPN Server			
> Services	O	penVPN Configurati	ion				
V VPN	Na	ame	Туре	Description	Enable	Status	
РРТР L2TP	СЦ	JENT_1	CLIENT		OFF ¥	Disconnected	Modify
IPSec	cu	JENT_2	CLIENT		OFF ¥	Disconnected	Modify
GRE	сц	JENT_3	CLIENT		OFF 🛩	Disconnected	Modify
Certificate Management	SEF	RVER_1	SERVER		OFF 🛩	Disconnected	Modify
VPN Status							
> Network					Save & Apply		

3>OpenVPN Config File: choose the "client1.ovpn" file downloaded in Chapter 2.7,

4>User name: The entered name of the OpenVPN-Test-Client1 in Chapter2.3,

5>Password: The password of the OpenVPN-Test-Client1 in Chapter 2.3,

6>Click "Save & Apply" button.

	1 Enable ON V	^
0511 00003	Description	
> Status	2 Enable OpenVPN Config	
> Services	from file	1
VPN	3 OpenVPN Config File Choose File openvpn_OpeClient1.ovpn	
РРТР	4 User name OpenVPN-Test-Client1	
L2TP	Username used for authentication to the VPN server. It is needed when Authentication Turo contains Username Communication	
IPSec	Autrenucauon type contains osername/rassword.	
GRE	 Password Password used for authentication to the VPN server. It is needed when 	
OpenVPN	Authentication Type contains Username/Password.	

7>The OpenVPN connection is connected, and more details of the connection can be check in VPN status page.

031-00003	OpenVPN	OpenVPN Configuration							
> Status	Enhanced C	penVPN design	allows 3 OpenVPN	Clients and 1 C	penVPN Server				
> Services	OpenVPN	Configuratio	on						
V VPN	Name	Туре	Description	Enable	Status				
PPTP L2TP	CLIENT_1	CLIENT		on ~	Connected	🛃 Modify			
IPSec	CLIENT_2	CLIENT		OFF∽	Disconnected	🛛 Modify			
VPN									
РРТР	VPN								
L2TP	VPN Status								
IPSec									
GRE	Туре:	Open\	/PN_CLIENT_1						
OpenVPN	IP Addres	ss: 10.0.2	0.10						
Certificate Manager	Netmasl	<: 255.25	5.255.255						
VPN Status	Gateway	/: 10.0.2	0.9						
Network	Connected	Time: 13m,9	s						

8>Check the routes of router1.

â								
USR-G806s	Routes							
	Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
✓ Status	0.0.0.0	172.16.10.1	0.0.0.0	UG	0	0	0	eth0.2
Overview	0.0.0.0	172.16.10.1	0.0.0.0	UG	5	0	0	eth0.2
> Services	10.0.20.0	10.0.20.9	255.255.255.0	UG	0	0	0	tun_CLIENT_1
> VPN	10.0.20.9	0.0.0.0	255.255.255.255	UH	0	0	0	tun_CLIENT_1
Network	172.16.10.0	0.0.0.0	255.255.254.0	U	5	0	0	eth0.2
> Firewall	192.168.32.0	0.0.0.0	255.255.255.0	U	0	0	0	br-lan
> WAN/LAN Port	192.168.33.0	10.0.20.9	255.255.255.0	UG	0	0	0	tun_CLIENT_1

3.2 Configure the second router as OpenVPN Client2

1>The LAN IP of the second router is 192.168.33.1

USR-G806	Status	Image: Specific State Uptime: Sh 54m 54s br-lan MAC-Address: D4:AD:20:5F:55:14 RX: 6.68 MB (34377 Pkts.) TX: 38.56 MB (40765 Pkts.) TX: 38.56 MB (40765 Pkts.) IPv4: 192.168.33.1/24
> Services		
> VPN	Protocol	Static address 🗸
✓ Network	IPv4 address	192.168.33.1
Interfaces	IPv4 netmask	255.255.255.0 🗸
CINA Cand	,	

2>OpenVPN Config File: choose the "client2.ovpn" file downloaded in Chapter 2.7,

3>User name: The entered name of the OpenVPN-Test-Client2 in Chapter2.3,

4>Password: The password of the OpenVPN-Test-Client2 in Chapter 2.3,

USR-G806	Configuration
	1 Enable ON ~
> Status > Services	Description The maximum length is 50 Bytes.
VPN	2 Enable OpenVPN Config On Off
PPTP	from file
L2TP	3 OpenVPN Config File Choose File openvpn_OpeClient2.ovpr
IPSec	4 User name OpenVPN-Test-Client2
GRE	Username used for authentication to the VPN server. It is needed when Authentication Type contains Username/Password.
OpenVPN	
Certificate Manager	5 Password exercise a contract of the VPN server. It is needed when
×	Authentication Type contains Username/Password.

5>Click "Save & Apply" button,

6>The OpenVPN connection is connected, and more details of the connection can be check in VPN status page.

VPN
PPTP
L2TP
IPSec
GRE
OpenVPN
Certificate Manag
VPN Status
> Network

7> Check the routes of router2.

Communication Expert of Industrial IOT						В	еH	onest, Do
USR-G806	Routes							
	Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
✓ Status	0.0.0.0	172.16.10.1	0.0.0.0	UG	0	0	0	eth0.2
Overview	0.0.0.0	172.16.10.1	0.0.0.0	UG	5	0	0	eth0.2
> Services	10.0.20.0	10.0.20.5	255.255.255.0	UG	0	0	0	tun_CLIENT_1
> VPN	10.0.20.5	0.0.0.0	255.255.255.255	UH	0	0	0	tun_CLIENT_1
> Network	172.16.10.0	0.0.0.0	255.255.254.0	U	5	0	0	eth0.2
> WAN/LAN Port	192.168.32.0	10.0.20.5	255.255.255.0	UG	0	0	0	tun_CLIENT_1
> Firewall	192.168.33.0	0.0.0.0	255.255.255.0	U	0	0	0	br-lan

4. Inter-subnet connectivity testing

In this case, the IP of PC1 is192.168.32.182, and the IP of PC2(phone) is192.168.33.170.

Administrator: C:\Windows\system32\cmd.exe		×
Connection-specific DNS Suffix . : lan Link-local IPv6 Address : fe80::c7d1:c:124c:cf62%22 IPv4 Address : 192.168.32.182 1 Subnet Mask : 255.255.255.0 Default Gateway : 192.168.32.1		^
Ethernet adapter 以太网:		
Connection-specific DNS Suffix . : Link-local IPv6 Address : fe80::2cff:fa3c:6311:3405%23 IPv4 Address : 172.16.10.31 Subnet Mask : 255.255.254.0 Default Gateway : 172.16.10.1		
C:\Users\Administrator>ping 192.168.33.170 2		
Pinging 192.168.33.170 with 32 bytes of data: Reply from 192.168.33.170: bytes=32 time=19ms TTL=62 Reply from 192.168.33.170: bytes=32 time=38ms TTL=62 Reply from 192.168.33.170: bytes=32 time=25ms TTL=62 Reply from 192.168.33.170: bytes=32 time=38ms TTL=62		
Ping statistics for 192.168.33.170: Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round trip times in milli-seconds: Minimum = 19ms, Maximum = 38ms, Average = 30ms		
C:\Users\Administrator>		~

▲ App Store	下午 5:29	🕑 🖉 97% 🚮
〈 返回	Ping	启动

服务器

192.168.32.182

添加到服务器列表

输出信息:



PING 192.168.32.182 (192.168.32.182): 56 data bytes

64 bytes from 192.168.32.182: icmp_seq=0 ttl=32 time=76.731 ms

64 bytes from 192.168.32.182: icmp_seq=1 ttl=32 time=45.212 ms

64 bytes from 192.168.32.182: icmp_seq=2 ttl=32 time=223.148 ms

64 bytes from 192.168.32.182: icmp_seq=3 ttl=32 time=80.995 ms

--- 192.168.32.182 ping statistics ---4 packets transmitted, 4 received, 0.00% packet loss round-trip min / avg / max = 45.212 / 106.522 / 223.148 ms