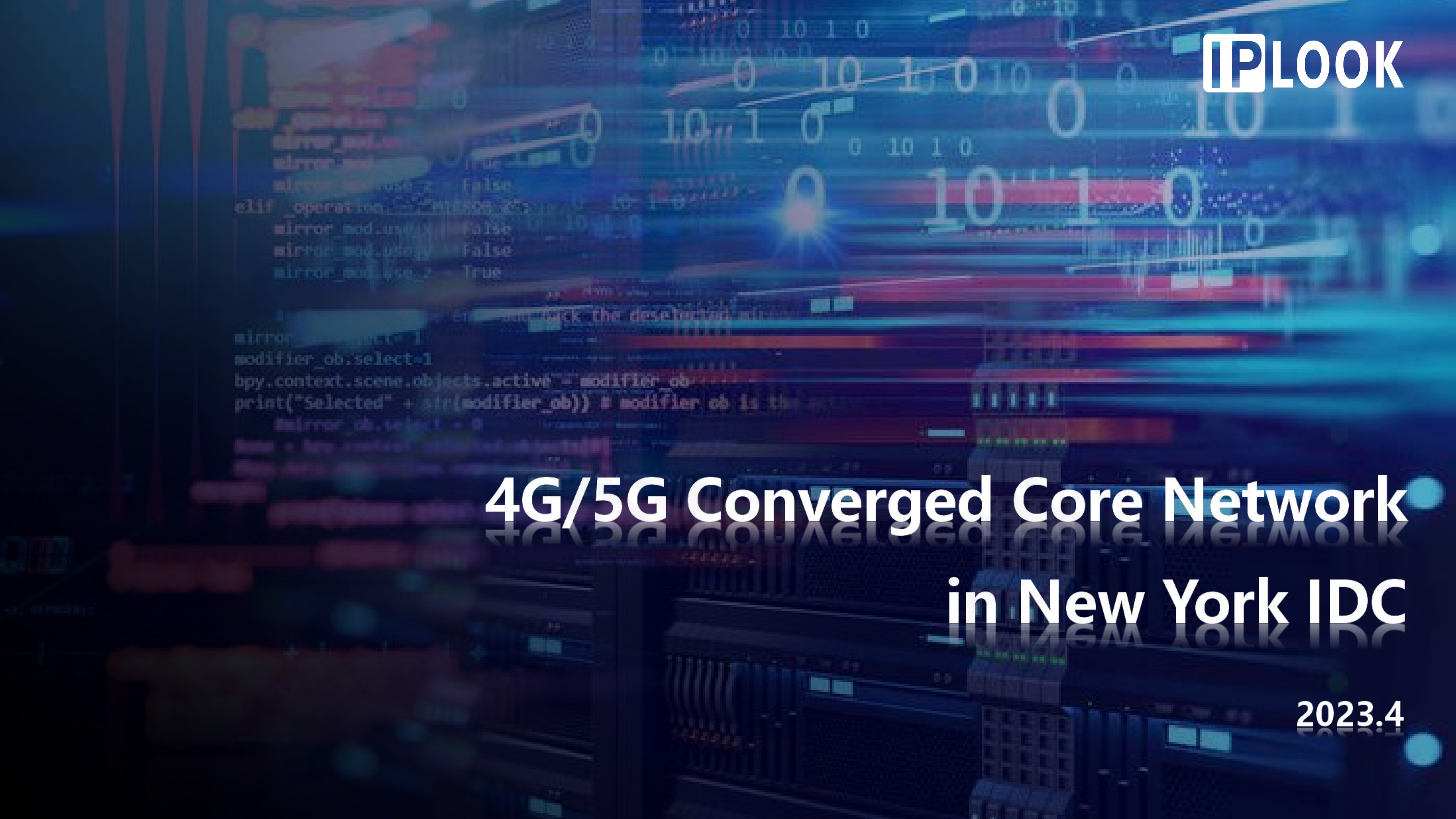


IPLOOK

4G/5G Converged Core Network in New York IDC

2023.4

01 Test Environment

02 Application

03 Precondition

04 Test Guidance

05 Expected Results

01

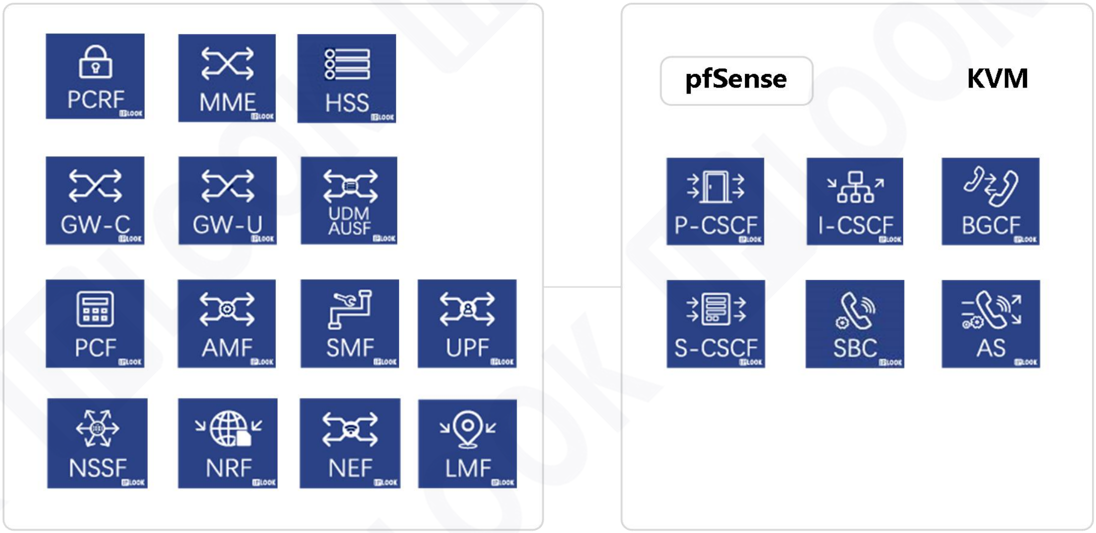
Test Environment

Test Environment

IPLOOK
www.iplook.com

IPLOOK's 4G/5G converged core network has been deployed on the server in New York IDC, and successfully connected with eNodeB/gNodeB based at IPLOOK R&D center, via IPSec tunnel.

Currently, the test environment has been well operated, achieving smooth and stable 4G/5G data services and VoNR/VoLTE call.



Servers in New York IDC

02

Application

Application

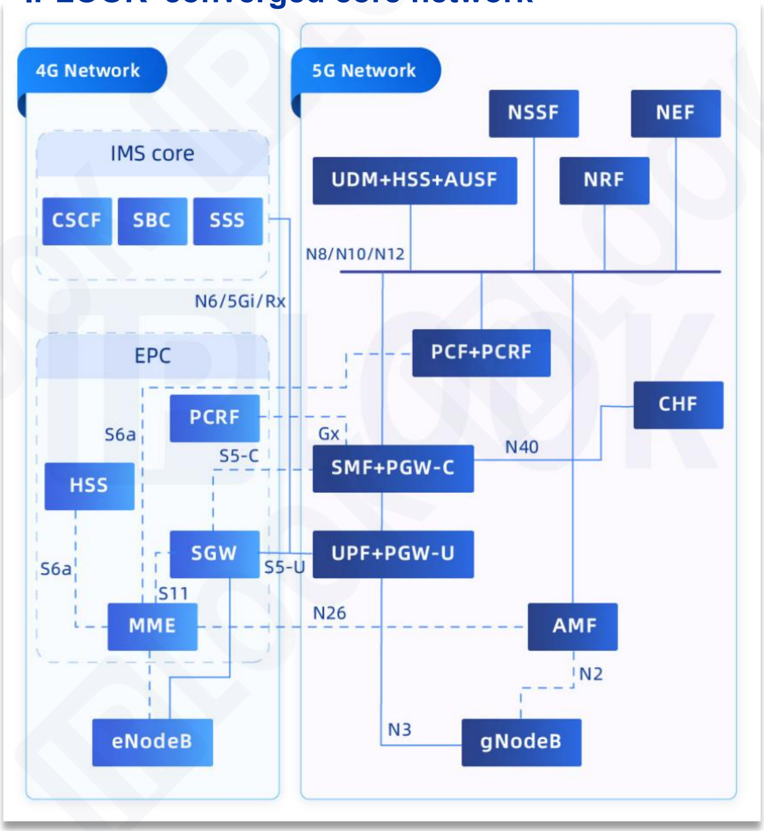
- The test environment is available for **worldwide potential customer**.

- Connect the base stations with IPLOOK's 4G/5G converged core network in New York IDC to **achieve data, VoLTE/VoNR tests**.

- **Verify the capability** of IPLOOK's mobile core network and the quality of network services.

- **Simple operation** to finish the test with IPLOOK's core network.

IPLOOK' converged core network

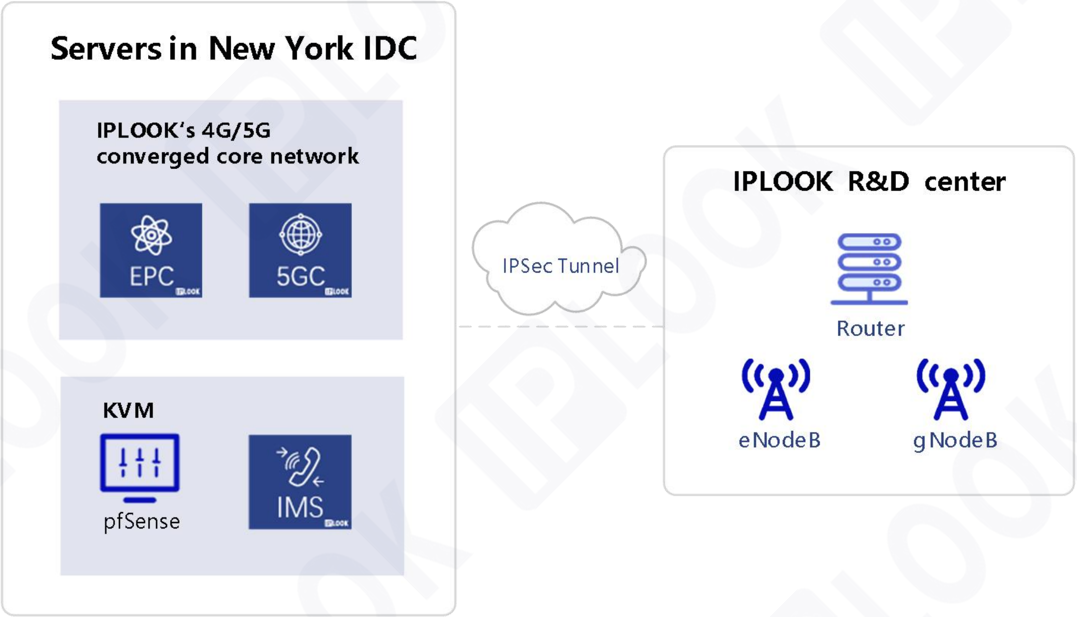


03

Precondition

Precondition

3.1 Network Topology



(For differentiation, here pfSense refers to the core network side where the IPSec tunnel is established, and the router refers to the base station side.)

Precondition

3.2 Parameters

With the set up (left side of the IPSec tunnel) of core network and pfSense server, customers need to prepare or confirm the following things for testing.

	Parameters	Note
1	IPSec-enabled router	Or install pfSense system on a server
2	eNodeB/gNodeB	
3	Public IP address	
4	Private IP address	For the IPSec tunnel of the base station side
5	Fixed IP address	On the base station side
6	SIM cards	Blank SIMs
7	Information for SIM card writing	IMSI/KI/OPC
8	PLMN	The one that the customers want to test
9	SMSC Number	For SMS service

04

Test Guidance

Test Guidance

*Note 1:

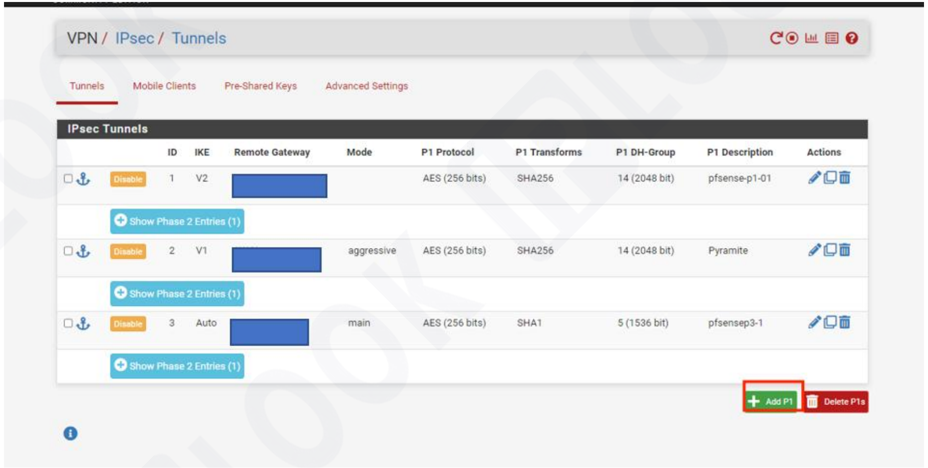
a. The following configurations are for reference only and should be configured flexibly according to the specific situation.

b. The following screenshots of the OAM interface are for reference only, as the OAM interface varies from different routers and base stations.

Test Guidance

4.1 IPSec Configuration on Core Network pfSense (Configured by IPLOOK)

1. Access to the pfSense management interface via the ip configured on the LAN port after the pfSense installation is completed.
2. Enter IPSec configuration tunnel under VPN option and click on Add P1.
3. The configuration can be done according to the diagram.



VPN / IPsec / Tunnels

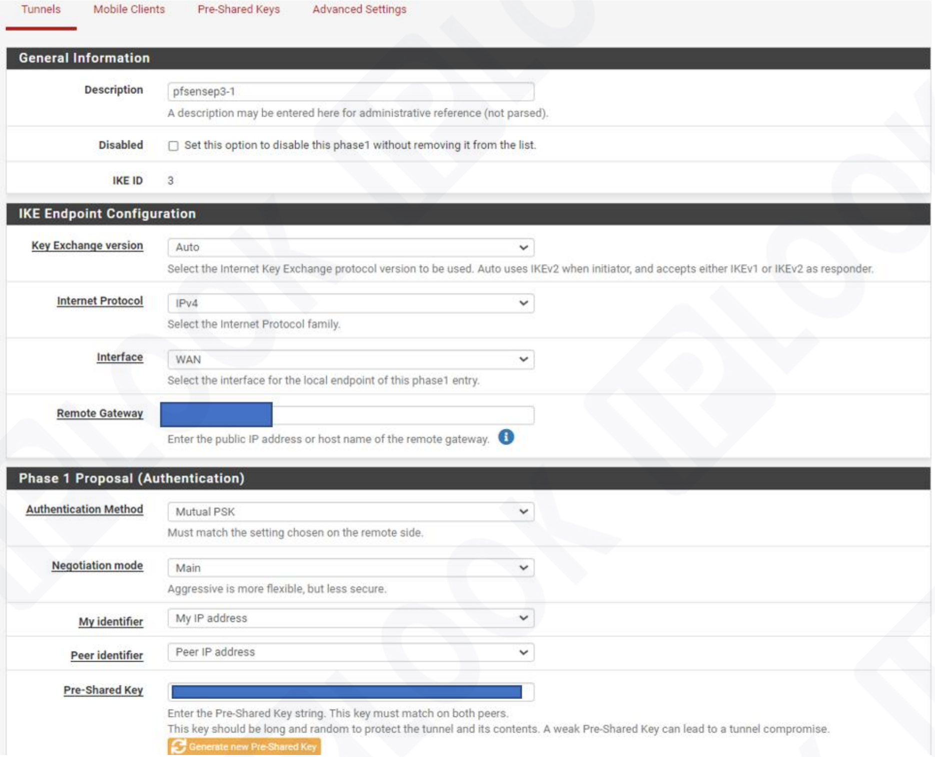
IPsec Tunnels

		ID	IKE	Remote Gateway	Mode	P1 Protocol	P1 Transforms	P1 DH-Group	P1 Description	Actions
□ ⚓	Disable	1	V2	[redacted]		AES (256 bits)	SHA256	14 (2048 bit)	pfsense-p1-01	✎ ❐ 🗑
	Show Phase 2 Entries (1)									
□ ⚓	Disable	2	V1	[redacted]	aggressive	AES (256 bits)	SHA256	14 (2048 bit)	Pyramite	✎ ❐ 🗑
	Show Phase 2 Entries (1)									
□ ⚓	Disable	3	Auto	[redacted]	main	AES (256 bits)	SHA1	5 (1536 bit)	pfsensep3-1	✎ ❐ 🗑
	Show Phase 2 Entries (1)									

Test Guidance

IPLOOK
www.iplook.com

4.1 IPSec Configuration on Core Network pfSense (Configured by IPLOOK)



General Information

Description: pfsensep3-1
A description may be entered here for administrative reference (not parsed).

Disabled: □ Set this option to disable this phase1 without removing it from the list.

IKE ID: 3

IKE Endpoint Configuration

Key Exchange version: Auto
Select the Internet Key Exchange protocol version to be used. Auto uses IKEv2 when initiator, and accepts either IKEv1 or IKEv2 as responder.

Internet Protocol: IPv4
Select the Internet Protocol family.

Interface: WAN
Select the interface for the local endpoint of this phase1 entry.

Remote Gateway: [redacted]
Enter the public IP address or host name of the remote gateway.

Phase 1 Proposal (Authentication)

Authentication Method: Mutual PSK
Must match the setting chosen on the remote side.

Negotiation mode: Main
Aggressive is more flexible, but less secure.

My identifier: My IP address

Peer identifier: Peer IP address

Pre-Shared Key: [redacted]
Enter the Pre-Shared Key string. This key must match on both peers.
This key should be long and random to protect the tunnel and its contents. A weak Pre-Shared Key can lead to a tunnel compromise.

*Note:

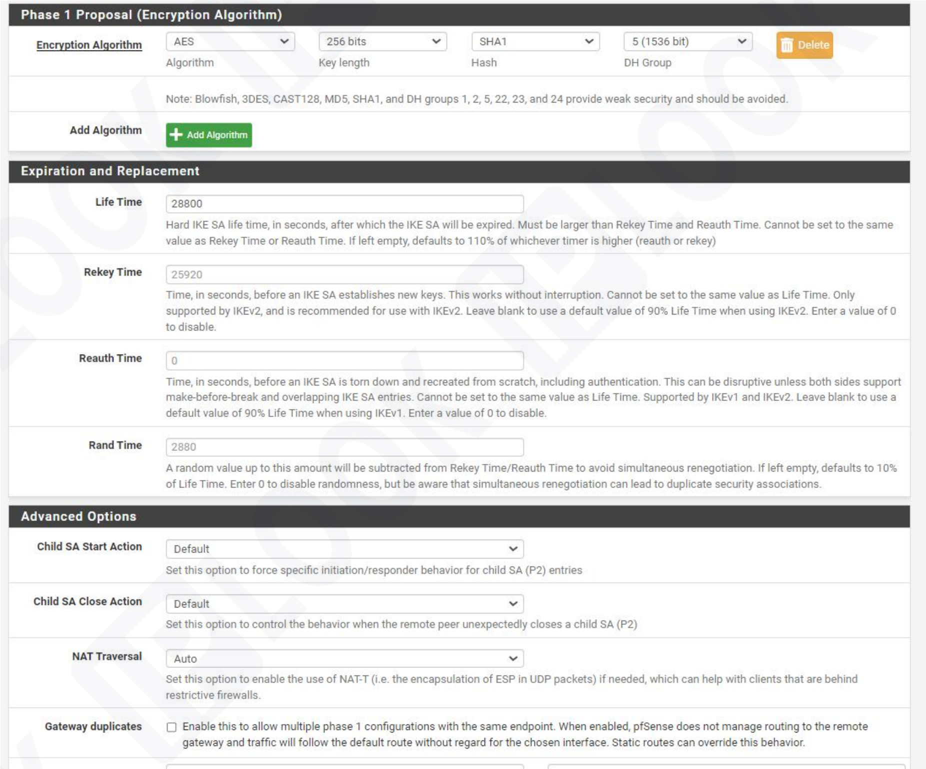
a. Remote Gateway fills in the public IP address of the WAN port on the router side.
b. The Authentication Method and Pre-Shared Key should correspond to the configuration on the router side.

Test Guidance

4.1 IPSec Configuration on Core Network pfSense (Configured by IPLOOK)

4. The overall configuration is shown in the right diagram.

*Note: Encryption Algorithm should correspond to the configuration on the router.



Phase 1 Proposal (Encryption Algorithm)

Encryption Algorithm: AES (Algorithm) | 256 bits (Key length) | SHA1 (Hash) | 5 (1536 bit) (DH Group) | Delete

Note: Blowfish, 3DES, CAST128, MD5, SHA1, and DH groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Add Algorithm: + Add Algorithm

Expiration and Replacement

Life Time: 28800

Hard IKE SA life time, in seconds, after which the IKE SA will be expired. Must be larger than Rekey Time and Reauth Time. Cannot be set to the same value as Rekey Time or Reauth Time. If left empty, defaults to 110% of whichever timer is higher (reauth or rekey)

Rekey Time: 25920

Time, in seconds, before an IKE SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Only supported by IKEv2, and is recommended for use with IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv2. Enter a value of 0 to disable.

Reauth Time: 0

Time, in seconds, before an IKE SA is torn down and recreated from scratch, including authentication. This can be disruptive unless both sides support make-before-break and overlapping IKE SA entries. Cannot be set to the same value as Life Time. Supported by IKEv1 and IKEv2. Leave blank to use a default value of 90% Life Time when using IKEv1. Enter a value of 0 to disable.

Rand Time: 2880

A random value up to this amount will be subtracted from Rekey Time/Reauth Time to avoid simultaneous renegotiation. If left empty, defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to duplicate security associations.

Advanced Options

Child SA Start Action: Default

Set this option to force specific initiation/responder behavior for child SA (P2) entries

Child SA Close Action: Default

Set this option to control the behavior when the remote peer unexpectedly closes a child SA (P2)

NAT Traversal: Auto

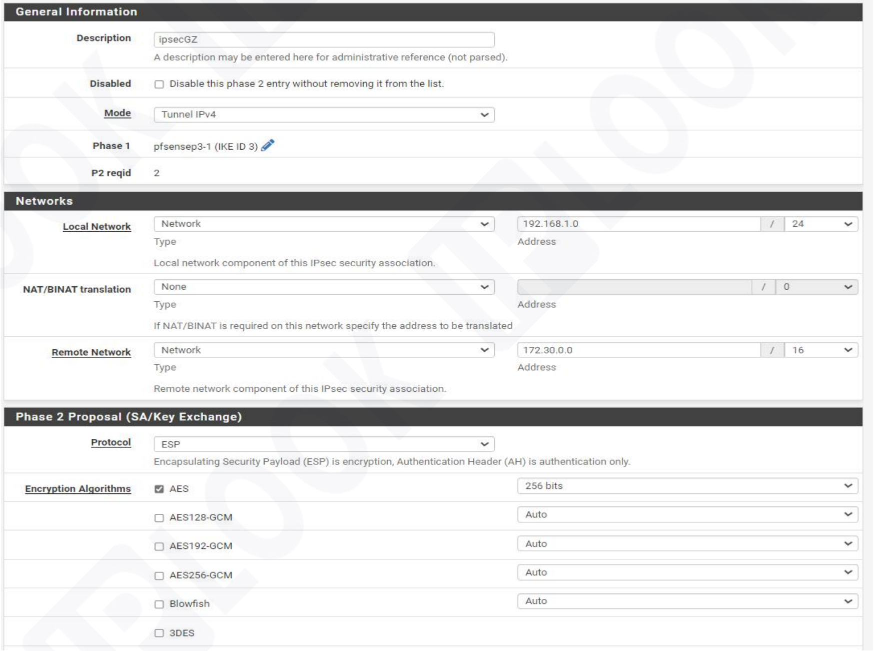
Set this option to enable the use of NAT-T (i.e. the encapsulation of ESP in UDP packets) if needed, which can help with clients that are behind restrictive firewalls.

Gateway duplicates: □ Enable this to allow multiple phase 1 configurations with the same endpoint. When enabled, pfSense does not manage routing to the remote gateway and traffic will follow the default route without regard for the chosen interface. Static routes can override this behavior.

Test Guidance

4.1 IPSec Configuration on Core Network pfSense (Configured by IPLOOK)

5. The overall configuration of Phase 2 is shown in the diagram on right.
6. Fill the subnet IP on the pfSense side in the Local Network.
7. Fill the subnet IP on the router side in the Remote Network.



General Information

Description: ipsecGZ
A description may be entered here for administrative reference (not parsed).

Disabled: □ Disable this phase 2 entry without removing it from the list.

Mode: Tunnel IPv4

Phase 1: pfsensep3-1 (IKE ID 3)

P2 reqid: 2

Networks

Local Network: Network (Type) — 192.168.1.0 / 24 (Address)
Local network component of this IPsec security association.

NAT/BINAT translation: None (Type) — / 0 (Address)
If NAT/BINAT is required on this network specify the address to be translated

Remote Network: Network (Type) — 172.30.0.0 / 16 (Address)
Remote network component of this IPsec security association.

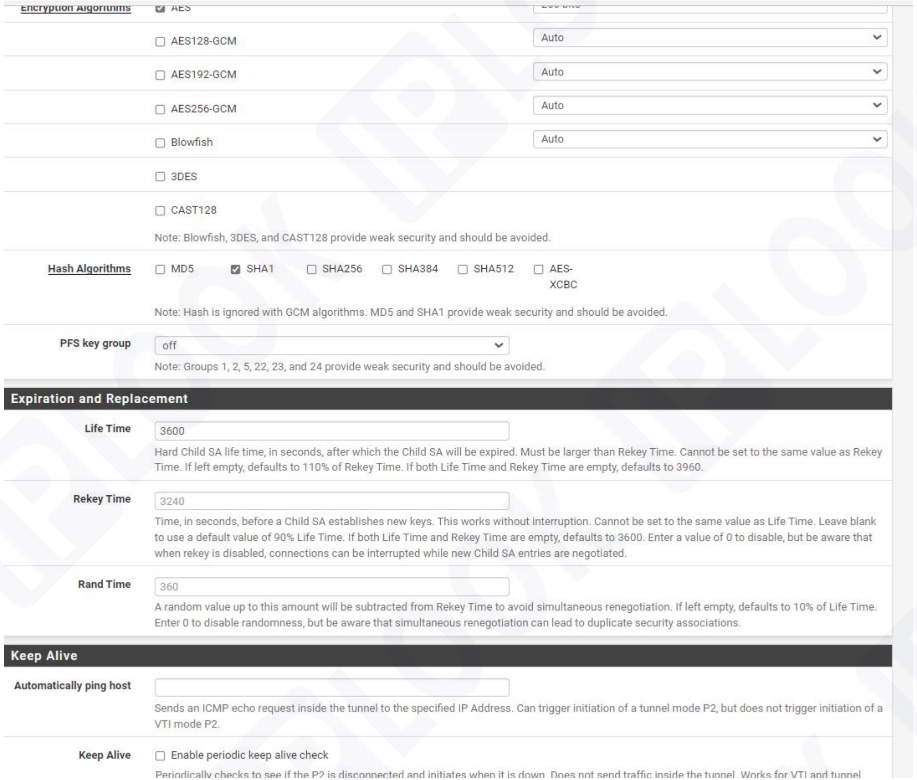
Phase 2 Proposal (SA/Key Exchange)

Protocol: ESP
Encapsulating Security Payload (ESP) is encryption, Authentication Header (AH) is authentication only.

Encryption Algorithms:
- ☑ AES — 256 bits
- □ AES128-GCM — Auto
- □ AES192-GCM — Auto
- □ AES256-GCM — Auto
- □ Blowfish — Auto
- □ 3DES

Test Guidance

4.1 IPSec Configuration on Core Network pfSense (Configured by IPLOOK)



Encryption Algorithms ☑ AES

☐ AES128-GCM — Auto

☐ AES192-GCM — Auto

☐ AES256-GCM — Auto

☐ Blowfish — Auto

☐ 3DES

☐ CAST128

Note: Blowfish, 3DES, and CAST128 provide weak security and should be avoided.

Hash Algorithms ☐ MD5 ☑ SHA1 ☐ SHA256 ☐ SHA384 ☐ SHA512 ☐ AES-XCBC

Note: Hash is ignored with GCM algorithms. MD5 and SHA1 provide weak security and should be avoided.

PFS key group: off

Note: Groups 1, 2, 5, 22, 23, and 24 provide weak security and should be avoided.

Expiration and Replacement

Life Time: 3600

Hard Child SA life time, in seconds, after which the Child SA will be expired. Must be larger than Rekey Time. Cannot be set to the same value as Rekey Time. If left empty, defaults to 110% of Rekey Time. If both Life Time and Rekey Time are empty, defaults to 3960.

Rekey Time: 3240

Time, in seconds, before a Child SA establishes new keys. This works without interruption. Cannot be set to the same value as Life Time. Leave blank to use a default value of 90% Life Time. If both Life Time and Rekey Time are empty, defaults to 3600. Enter a value of 0 to disable, but be aware that when rekey is disabled, connections can be interrupted while new Child SA entries are negotiated.

Rand Time: 360

A random value up to this amount will be subtracted from Rekey Time to avoid simultaneous renegotiation. If left empty, defaults to 10% of Life Time. Enter 0 to disable randomness, but be aware that simultaneous renegotiation can lead to duplicate security associations.

Keep Alive

Automatically ping host:

Sends an ICMP echo request inside the tunnel to the specified IP Address. Can trigger initiation of a tunnel mode P2, but does not trigger initiation of a VTI mode P2.

Keep Alive ☐ Enable periodic keep alive check

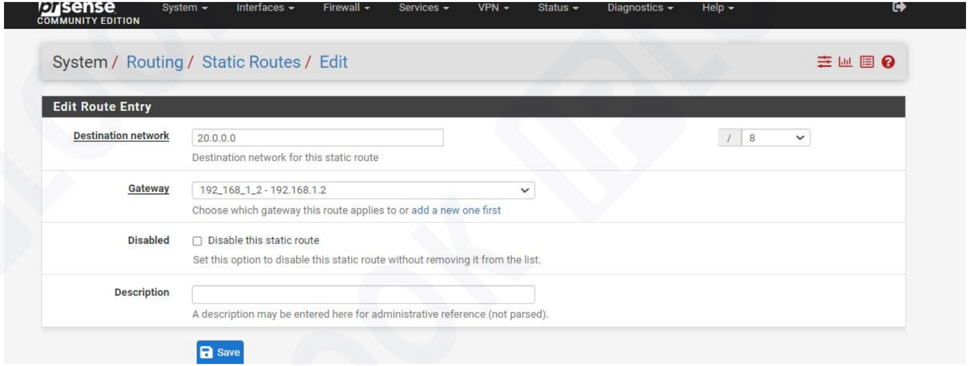
Periodically checks to see if the P2 is disconnected and initiates when it is down. Does not send traffic inside the tunnel. Works for VTI and tunnel

*Note: the configuration of Protocol, Encryption Algorithm, Hash Algorithm, and Life Time should be consistent on the both sides of IPSec .

Test Guidance

4.1 IPSec Configuration on Core Network pfSense (Configured by IPLOOK)

8. Add SGi interface of core network as a new gateway.
9. Static Routes: configure the core network address pool as the Destination Network and the S1 IP of the core network as the Gateway. (This configuration is required for internet access.)



System / Routing / Static Routes / Edit

Edit Route Entry

Destination network: 20.0.0.0 / 8
Destination network for this static route

Gateway: 192_168_1_2 - 192.168.1.2
Choose which gateway this route applies to or add a new one first

Disabled: □ Disable this static route
Set this option to disable this static route without removing it from the list.

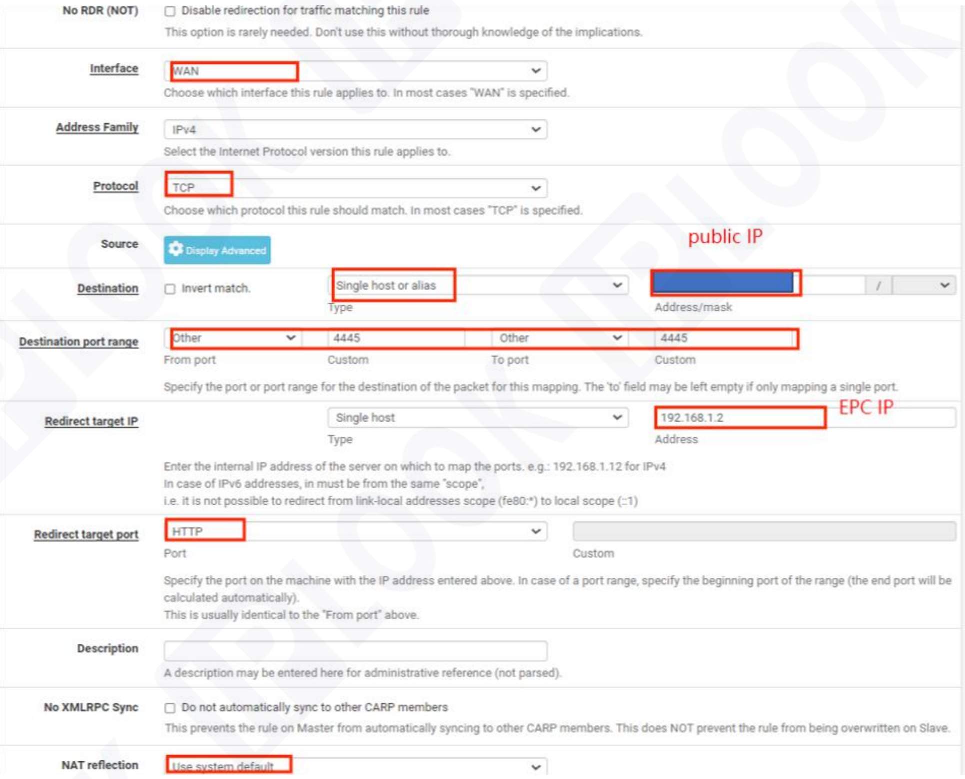
Description:
A description may be entered here for administrative reference (not parsed).

Save

Test Guidance

4.1 IPSec Configuration on Core Network pfSense (Configured by IPLOOK)

10. Remote access to the core gateway requires to configure port forwarding.



No RDR (NOT) □ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source Display Advanced

public IP

Destination □ Invert match. Single host or alias (Type) [redacted] / (Address/mask)

Destination port range Other (From port) 4445 (Custom) Other (To port) 4445 (Custom)
Specify the port or port range for the destination of the packet for this mapping. The 'to' field may be left empty if only mapping a single port.

Redirect target IP Single host (Type) 192.168.1.2 (Address) EPC IP
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, in must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Redirect target port HTTP (Port) (Custom)
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

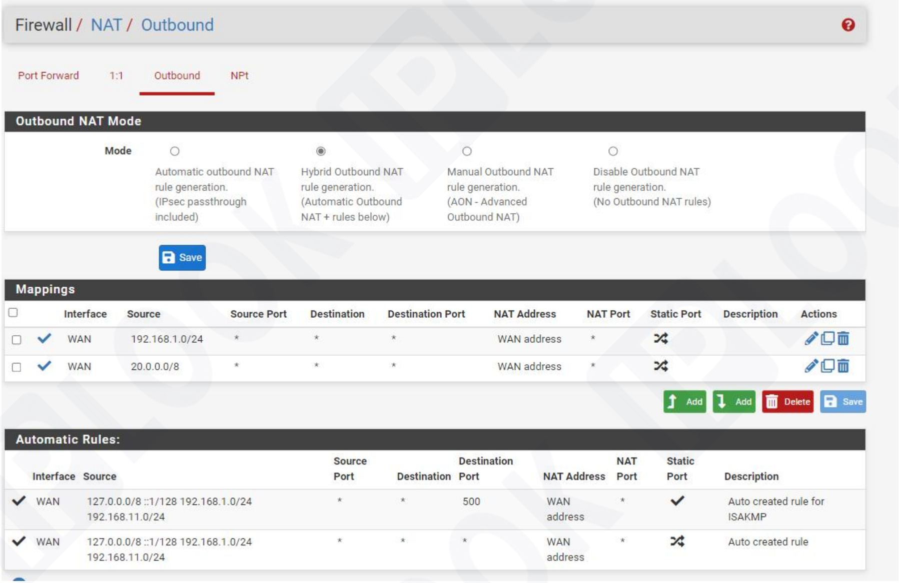
Description
A description may be entered here for administrative reference (not parsed).

No XMLRPC Sync □ Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule from being overwritten on Slave.

NAT reflection Use system default

Test Guidance

4.1 IPSec Configuration on Core Network pfSense (Configured by IPLOOK)



Firewall / NAT / Outbound

Port Forward | 1:1 | Outbound | NPt

Outbound NAT Mode

Mode
- ○ Automatic outbound NAT rule generation. (IPsec passthrough included)
- ● Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
- ○ Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
- ○ Disable Outbound NAT rule generation. (No Outbound NAT rules)

Save

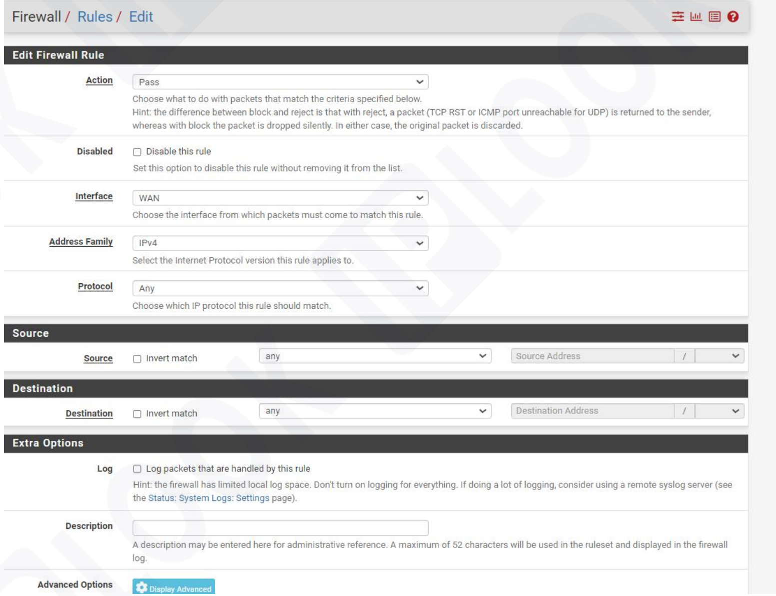
Mappings

□		Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
□	✓	WAN	192.168.1.0/24	*	*	*	WAN address	*	⤮		
□	✓	WAN	20.0.0.0/8	*	*	*	WAN address	*	⤮		

Add | Add | Delete | Save

Automatic Rules:

	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✓	WAN	127.0.0.0/8 ::1/128 192.168.1.0/24 192.168.11.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP
✓	WAN	127.0.0.0/8 ::1/128 192.168.1.0/24 192.168.11.0/24	*	*	*	WAN address	*	⤮	Auto created rule



Firewall / Rules / Edit

Edit Firewall Rule

Action: Pass
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled: □ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface: WAN
Choose the interface from which packets must come to match this rule.

Address Family: IPv4
Select the Internet Protocol version this rule applies to.

Protocol: Any
Choose which IP protocol this rule should match.

Source

Source: □ Invert match | any | Source Address | /

Destination

Destination: □ Invert match | any | Destination Address | /

Extra Options

Log: □ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).

Description:
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

Advanced Options: Display Advanced

*Note: The outbound and interface policy rules under the firewall need to be set up for release.

Test Guidance

*Note 2:

Due to the different brands and models of routers and base stations, the configuration names may be slightly different, but the parameters to be configured are basically the same. The IPSec configuration can be flexibly changed according to the parameters supported by the router, as long as the configurations on both sides of the IPSec are consistent.

The key configurations are listed below.

Test Guidance

4.2 Router Configuration for IPSec to Interface with pfSense

- Configured Router Brand/ Model: TP-LINK/ TL-R479GP-AC
- Key Configurations on the Router:

1. Enter the router management interface, then choose the IPSec management interface under the VPN option to add an IPSec entry;
2. Fill in the public IP address of the pfSense's WAN port in the peer gateway;
3. Bind the WAN port where the public IP address used by the router is located;
4. Fill in the subnet where the local router's LAN port is connected to the base station in the local subnet range;
5. Fill in the subnet 192.168.1.0/24 of the core network in the peer subnet;
6. The pre-shared key needs to correspond to the pre-shared key on the pfSense connected to the core network.
7. Note that the basic settings of the bound WAN port in the IPSec settings are correct.

Test Guidance

4.3 Base Station Configuration to Connect to the Router and Core Network

- Key Configurations on the Base Station:

1. Configure the subnet corresponding to the LAN port of the router in the base station;
2. The router's LAN port is the default gateway of the base station, which is in the same network segment as the base station IP.
3. Configure s1 IP of core network as service gateway, port 36412 (in 4G application scenario)
4. Configure PLMN, corresponding to the core network PLMN configuration.
5. Complete the configuration and confirm that the base station and router can ping successfully.

Test Guidance

4.4 4G/5G Data, VoLTE and VoNR Test on Mobile Phone/CPE

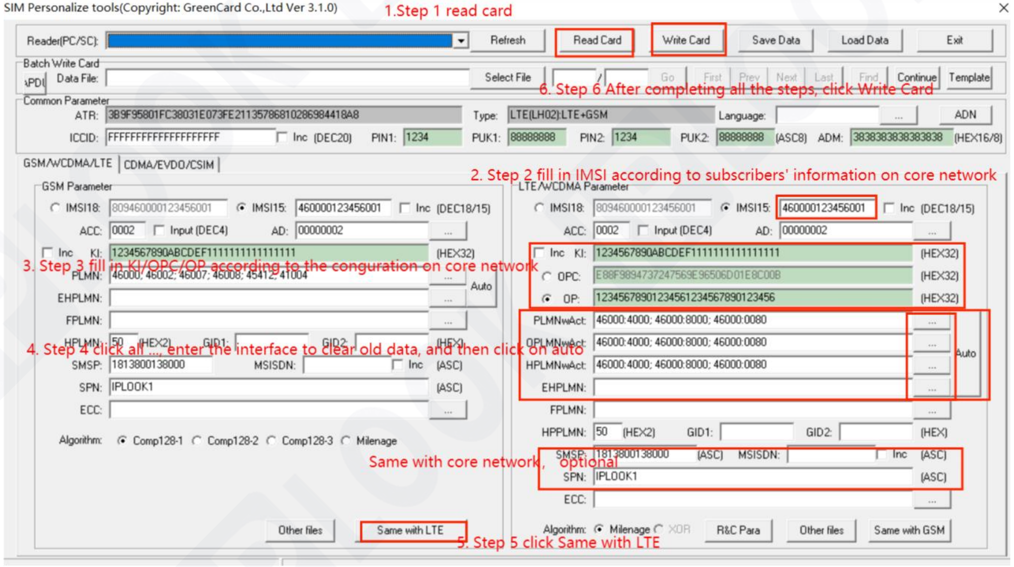
1. Write SIM cards according to the information on the core network.

*Note:

a. IMSI/KI/OPC need to be provided for core network for provisioning.

b. SMSC Number needs to be confirmed with customers for SMS service.

c. This interface will be different due to the different types of card writing tool. The above are the necessary modification items.



SIM Personalize tools(Copyright: GreenCard Co.,Ltd Ver 3.1.0)

1.Step 1 read card

2. Step 2 fill in IMSI according to subscribers' information on core network

3. Step 3 fill in KI/OPC/OP according to the conguration on core network

4. Step 4 click all ..., enter the interface to clear old data, and then click on auto

5. Step 5 click Same with LTE

6. Step 6 After completing all the steps, click Write Card

Same with core network, optional

Reader(PC/SC):

Batch Write Card

Data File:

Common Parameter

ATR: 3B9F95801FC38031E073FE21135786810286984418A8

Type: LTE(LH02):LTE+GSM

Language:

ICCID: FFFFFFFFFFFFFFFFFFFF □ Inc (DEC20)

PIN1: 1234 PUK1: 88888888 PIN2: 1234 PUK2: 88888888 (ASC8) ADM: 3838383838383838 (HEX16/8)

GSM/WCDMA/LTE | CDMA/EVDO/CSIM

GSM Parameter

○ IMSI18: 809460000123456001 ● IMSI15: 460000123456001 □ Inc (DEC18/15)

ACC: 0002 □ Input (DEC4) AD: 00000002

□ Inc KI: 1234567890ABCDEF1111111111111111 (HEX32)

PLMN: 46000; 46002; 46007; 46008; 45412; 41004

EHPLMN:

FPLMN:

HPLMN: 50 (HEX2) GID1: GID2: (HEX)

SMSP: 1813800138000 MSISDN: □ Inc (ASC)

SPN: IPLOOK1 (ASC)

ECC:

Algorithm: ● Comp128-1 ○ Comp128-2 ○ Comp128-3 ○ Milenage

LTE/WCDMA Parameter

○ IMSI18: 809460000123456001 ● IMSI15: 460000123456001 □ Inc (DEC18/15)

ACC: 0002 □ Input (DEC4) AD: 00000002

□ Inc KI: 1234567890ABCDEF1111111111111111 (HEX32)

○ OPC: E88F9894737247569E96506D01E8C008 (HEX32)

● OP: 12345678901234561234567890123456 (HEX32)

PLMNwAct: 46000:4000; 46000:8000; 46000:0080

OPLMNwAct: 46000:4000; 46000:8000; 46000:0080

HPLMNwAct: 46000:4000; 46000:8000; 46000:0080

EHPLMN:

FPLMN:

HPPLMN: 50 (HEX2) GID1: GID2: (HEX)

SMSP: 1813800138000 (ASC) MSISDN: □ Inc (ASC)

SPN: IPLOOK1 (ASC)

ECC:

Algorithm: ● Milenage ○ XOR

Test Guidance

4.4 4G/5G Data, VoLTE and VoNR Tests on Mobile Phone/CPE

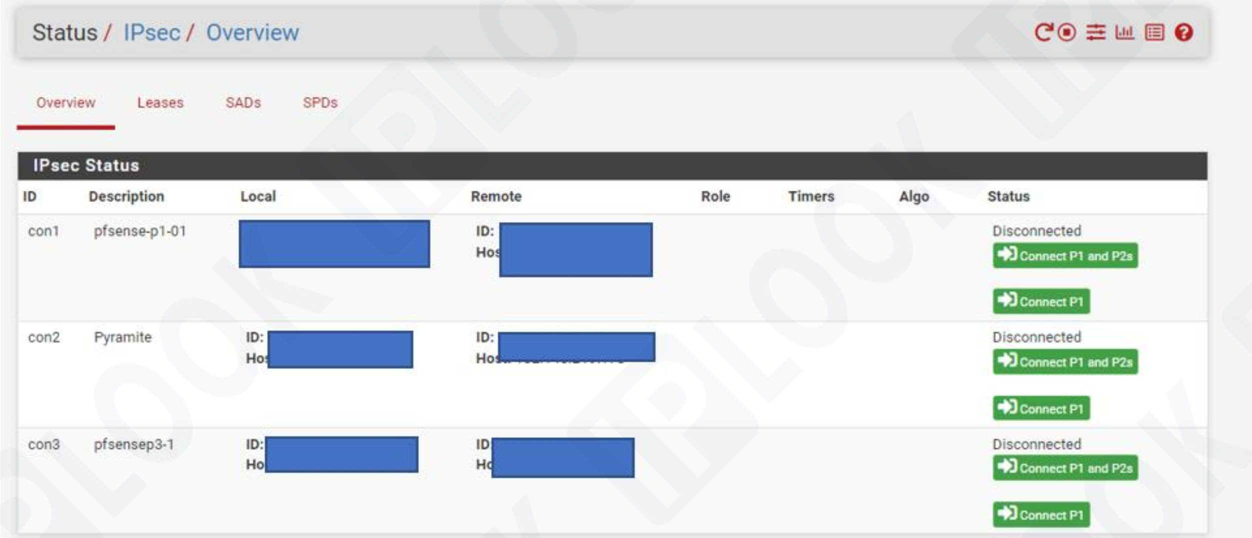
2. Insert the written SIM card into the mobile phone, and then register after opening and closing airplane mode.
3. See a signal and HD logo in the upper column of the mobile phone, which means the mobile phone is attached and registered successfully.
4. Use the number on the core network to conduct a call test between two mobile phones. After getting through, click to transfer video to conduct a video test.
5. Test the speed with a speed test app or website.

05

Expected Results

Expected Results

1. IPSec tunnels have been completed, shown as follows.



Status / IPsec / Overview

Overview Leases SADs SPDs

IPsec Status

ID	Description	Local	Remote	Role	Timers	Algo	Status
con1	pfsense-p1-01	[redacted]	ID: Hos [redacted]				Disconnected Connect P1 and P2s Connect P1
con2	Pyramite	ID: Hos [redacted]	ID: Hos [redacted]				Disconnected Connect P1 and P2s Connect P1
con3	pfsensep3-1	ID: Ho [redacted]	ID Ho [redacted]				Disconnected Connect P1 and P2s Connect P1

2. Customers’ eNodeB/gNodeB can connect with IPLOOK’s 4G/5G converged core network.
3. Mobile phone/CPE can attach and register successfully.
4. Mobile phone/CPE are able to access to the internet.
5. Mobile phone/CPE can achieve smooth VoLTE/ VoNR calls and SMS services.

THANK YOU

in IPLOOK Technologies

f IPLOOK Technologies

☎ +8602028906963

IPLOOK Technologies

✉ sales@iplook.com

www.iplook.com