## H3C SecPath L2TP IPsec VPN

# 簡易マニュアル(RADIUS 認証 CLI 編)

(iNode L2TP IPsec VPN client)

V1.4 2021/7/7

## 内容

1. テストトポロジ	3
2. L2TP IPsec VPN 設定パラメーター	4
2.1 基本設定	4
2.2 L2TP トンネル	4
2.3 IPsec パラメーター	4
2.4 IKE パラメーター	4
3. SecPathF1020 側の設定手順	5
手順1:SecPathの内部、外部インターフェースに IP アドレスを割り当てる	5
手順2. IPsec VPN の設定をする	5
VPN クライアントに割り当てられる IP アドレスプールの設定をする	5
VPN クライアントのログインユーザー、パスワードの設定をする	5
IPsec ポリシーの設定をする	6
L2TP の設定をする	7
IKE ポリシーの設定をする	7
IPsecトンネルキーの設定をする	8
手順 3. セキュリティゾーンとセキュリティポリシーを設定する	8
手順 4. RADIUS サーバーの設定をする	9
4. クライアント側の設定	10
5. 接続と切断	14
付録 1. iNode クライアントのインストール	16
iNode Management center のインストール。	16
iNode Client インストールパッケージの作成	19
iNode クライアントのインストール	23
付録 2. SecPathF1020 側の設定例	26



テスト環境では、RADIUSと Active Directory 連携によるユーザー認証を実施。 Active Directory のドメインは ad.rem-system.com としています。



この例は version 7.1.064, Release 9345P14 で実施しました。

**クライアントソフトウェア適応システム**: Windows7、8、Vista、10、XP、Windows Server 2003

# 2. L2TP IPsec VPN 設定パラメーター

#### 2.1 基本設定

パラメーター	設定値
LNS サーバー	192.168.30.1
代替 LNS サーバー	192.168.30.1
IPsec	Enable
認証モード	Pre-shared-key
認証キー	test
IPsec サーバー	LNS サーバーを使用

### 2.2 L2TP トンネル

パラメーター	設定値
認証モード	PAP
Hello パケット送信間隔	60 秒
L2TP ポート	1701

### 2.3 IPsec パラメーター

パラメーター	設定値
モード	トンネル
SA ライフタイム	3600 秒
ESPトランスフォーム	3DES(16 bit) / ESP-MD5
АН	MD5
PFS	なし
アドレス変換	NAT トラバーサル

### 2.4 IKE パラメーター

パラメーター	設定値
ネゴシエーションモード	Aggressive
認証アルゴリズム	SHA
暗号化アルゴリズム	DES-CBC
DH グループ	2
IKE ポート	500
SA ライフタイム	86400 秒
ローカルセキュリティゲートウェイ名	Inode
リモートセキュリティゲートウェイ名	Ins
keepalive パケット受信間隔	なし
keepalive パケット送信間隔	なし

## 3. SecPathF1020 側の設定手順

## 手順1:SecPathの内部、外部インターフェースに IP アドレス を割り当てる

#インターフェースの IP 設定 interface GigabitEthernet1/0/0 ip address 192.168.30.1/32 # interface GigabitEthernet1/0/1 ip address 192.168.20.1 24 #

### 手順2. IPsec VPN の設定をする

### VPN クライアントに割り当てられる IP アドレスプールの設定

### をする

#VPN クライアントへ割り当てる IP アドレスプールの設定 ip pool pool 192.168.10.11 192.168.10.253 ip pool pool gateway 192.168.10.1 # interface Virtual-Template1 ppp authentication-mode pap remote address pool pool ip address 192.168.10.1 255.255.255.0 #

## VPN クライアントのログインユーザー、パスワードの設定をす

## る

#ログインユーザー設定 local-user client class network password simple client service-type ppp authorization-attribute user-role network-operator

## IPsec ポリシーの設定をする

ipsec transform-set 1 esp encryption-algorithm 3des-cbc esp authentication-algorithm md5 # ipsec transform-set 2 encapsulation-mode transport esp encryption-algorithm aes-cbc-128 esp authentication-algorithm sha1 # ipsec transform-set 3 encapsulation-mode transport esp encryption-algorithm aes-cbc-256 esp authentication-algorithm sha1 # ipsec transform-set 4 encapsulation-mode transport esp encryption-algorithm des-cbc esp authentication-algorithm sha1 # ipsec transform-set 5 encapsulation-mode transport esp encryption-algorithm 3des-cbc esp authentication-algorithm sha1 # ipsec transform-set 6 encapsulation-mode transport esp encryption-algorithm aes-cbc-192 esp authentication-algorithm sha1 # #ipsec policy-template 1 1 transform-set 1 2 3 4 5 6 ike-profile 1 # ipsec policy 1 1 isakmp template 1 #

## L2TP の設定をする

#L2TP 設定 l2tp-group 1 mode Ins allow l2tp virtual-template 1 undo tunnel authentication # l2tp enable

## IKE ポリシーの設定をする

#IKE プロファイル ike profile 1 keychain 1 exchange-mode aggressive local-identity fqdn Ins match remote identity address 0.0.0.0 0.0.0.0 match remote identity fqdn inode proposal 1 2 3 4 5 6 #IKE プロポーザル ike proposal 1 dh group2 authentication-algorithm md5 # ike proposal 2 encryption-algorithm 3des-cbc dh group2 authentication-algorithm md5 # ike proposal 3 encryption-algorithm 3des-cbc dh group2 # ike proposal 4 encryption-algorithm aes-cbc-256 dh group2 # ike proposal 5 dh group2 # ike proposal 6

encryption-algorithm aes-cbc-192 dh group2

### IPsec トンネルキーの設定をする

#基本設定(認証モード、認証キー) ike keychain 1 pre-shared-key address 0.0.0.0 0.0.0.0 key simple test #

### 手順 3. セキュリティゾーンとセキュリティポリシーを設定する

#セキュリティゾーンのデフォルト設定 security-zone intra-zone default permit #セキュリティゾーンのインターフェース設定 security-zone name Trust import interface GigabitEthernet1/0/1 # security-zone name Untrust import interface Virtual-Template1 # security-zone name Management import interface GigabitEthernet1/0/0 #IP セキュリティポリシーの設定 security-policy ip rule 0 name 1 action pass rule 1 name 0 action pass counting enable source-zone Local source-zone Trust source-zone Untrust destination-zone Local destination-zone Trust destination-zone Untrust

#

## 手順 4. RADIUS サーバーの設定をする

#RADIUS 認証の設定

radius scheme user\_db

primary authentication 192.168.20.10 key simple test #

domain ad.rem-system.com

authentication ppp radius-scheme user\_db local authorization ppp radius-scheme user\_db local domain system

#

domain default enable ad.rem-system.com #

# 4. クライアント側の設定

① デスクトップの iNode Client のアイコンをダブルクリックします。



② Connect ボタンを右クリックして Properties が現れたら、Properties ボタンをクリックします。

中 ♥ - × iNode Intelligent Client	
L2TP IPsec VPN connection	
Username	
Password	
Save username 🗹 Save password	
Connect Prop	perties
• My scenario »	

#### ③基本設定

SecPath の外部 IP アドレスを入力し、IPsec、IPsec サーバーの設定を行います。

Y Properties	×
Basic Settings	
Connection Settings	
LNS Server: 192.168.30.1	
Second LNS: 192.168.30.1	
Clear ARP cache before authentication	
Upload version info	
Get username and password from smart card	
Get username and password from certificate	
Auto reconnect when forced offline	
Automatic authenticate at startup	
Unified Authentication	
Enable IPsec	
Authen-method: Pre-shared-Key 🔻	
Authenticator:	
Cert-Settings	
-IPsec Server	
Use LNS server	
O Specify IPsec server	
IPsec Server:	
Advanced	
OK Cance	ł

#### ④L2TP の設定を行います。

💦 Advanced Prop	erty				×
L2TP Settings	IPsec Settings	IKE Settings	Route	e Settings	
L2TP Protocol S	Settings				
Tunnel name:		vpn			
Authentication	mode:	PAP	•		
Interval for ser	nding Hello packet	s: 60		second	
L2TP port:		1701			
Use tunne	l authentication pa	ssword			
Tunnel auth	entication passwo	rd:			
Hide AVP					
			OK	(	Cancel

### ⑤IPsec の設定を行います。

🔀 Advanced Prop	perty			×
L2TP Settings	IPsec Settings	IKE Settings	Route Settings	
-IPsec Security	Proposal Settings			
Encapsulatio	n mode:	Tunnel 💎		
SA lifetime:		3600	second	
Security proto	col:	ESP 🔻		
ESP authenti	cation algorithm:	MD5 🔹		
ESP encryptic	on algorithm:	3DES 🔹		
AH authentica	ation algorithm:	MD5 👻		
Use PFS				
PFS dh-gr	oup1 🔻			
Use NAT f	traversal			
			ОК	Cancel

⑥IKE の設定を行います。

🕺 Advanced Property	×
L2TP Settings IPsec Settings IKE Settings Route Settings	
IKE Security Proposal Settings	
Negotiation mode: Aggressive 🔻 ID type: name 👻	
Authentication algorithm: Encryption DES-CBC •	
Diffie-Hellman group identifier: Group2 ▼ IKE Port: 500	
ISAKMP-SA lifetime: 86400 second	
Local security gateway name: inode	
Remote security gateway name: Ins	
Send keepalive packets regularly	
Time interval: 0 second	
Receive keepalive packets	
Timeout time: 0 second	
OK Cance	er i

以上でクライアントの設定は完了しました。

# 5. 接続と切断

① デスクトップの iNode Client のアイコンをダブルクリックします。



 ② iNode Client のログイン画面が表示され、ユーザー名( client )とパスワード( client )を入 カします。

そして、 Connect ボタンをクリックします。



### ③ サーバーとの接続が完了しました。

	ection
Online user	client
Connection status	Connected
Security status	Not Checked
Connected at	2021-6-25 12:48:17
	i= '�
Psec VPN Authentication	↔ ≕ ×
IPsec VPN Authentication	÷ ≕ ×
IPsec VPN Authentication	E ••• ×

④ サーバーとの接続を切るには Disconnect ボタンをクリックします。

# 付録 1. iNode クライアントのインストール

## iNode Management center のインストール。

iNode Management Center - In	stallShield Wizard	$\times$
	Welcome to the InstallShield Wizard for iNode Management Center The InstallShield Wizard will install iNode Management Center on your computer. To continue, dick Next.	
① ライセンス規約に	< <u>B</u> ack <u>N</u> ext > Cancel 承諾	
iNode Management Center - In	stallShield Wizard	×
License Agreement Please read the following lice	nse agreement carefully.	
License Agreem	ent ,	`
Your use of this Software acceptance of the dauses o License Agreement with New	in installation, copy or other way shall be deemed as your f this License Agreement and your consent to execute this v H3C Technologies Co., Ltd. (hereinafter "H3C").	
1. Software Product (herein	after "The Software")	
The "Software" in this Ag	reement includes computer software and all or any parts of	-
<ul> <li>I accept the terms of the</li> <li>I do not accept the terms</li> </ul>	icense agreement Print Of the license agreement	
InstallShield		
	< Back Next > Cancel	

### ② インストール場所の設定

iNode Management Center - InstallShield Wiz	ard X
Choose Destination Location Select folder where setup will install files.	
Install iNode Management Center to C:¥Program Files (x86)¥iNode¥iNod	o: de Manager Change
TostallShield	
	< Back Next > Cancel
③ インストールの開始	
iNode Management Center - InstallShield Wiz	ard X
Ready to Install the Program The wizard is ready to begin installation.	
Click Install to begin the installation.	
If you want to review or change any of your exit the wizard.	installation settings, click Back. Click Cancel to
InstallShield	
	< Back Install Cancel



#### ④ iNode Management Center インストールの完了

## iNode Client インストールパッケージの作成

① iNode Management Center の起動



② L2TPの iNode Client をインストールします。

Network Access Component で、L2TP IPsec VPN のみにチェックをいれて、 Finish をクリックします。

🔀 iNode Management Center		– 🗆 🗙
File(F) View(V) Language(L) Help(H)		
🍳 🕞 💐 🔜 🕐 🥝		
E	Client Customization	
Client Customization	Please select the default configu	ration for the customization
Customization History		~
	Network Access Components iNode client supports various ne	twork access methods.
L2TP IPsec VPN Config File	Components Licensed	Description
💫 Configuration	802.1X Yes     Portal Yes	Support standard and extended 802.1X protocols Support Portal protocols
Client Quick Deploy	SSL VPN Yes	Support SSL VPN protocols
	L2TP IPsec VPN Yes	Support L2TP IPsec VPN protocols
	Function Components iNode client supports the following	ng function components.
	Components Licensed	Description
	EAD Yes	Endpoint admission defense. Only the policy-compli.
	New Smart C Yes	Reads the username and password for network ac
	Old Smart Ca Yes	Reads the username and password for network ac.
	<	>
	Click Advanced to custom advance	d details.
	Click Finish to finish current custom	ization.
		Advanced Finish

 インストールされるパッケージに名前を付け、Client Scenario Information を Default Scenario, Use existing Scenario にチェックして OK をクリックします。

Finish Client Customization			
Supplementary Information			
It is recommended to specify the supplementary information (such as "HR V1.0") to help you distinguish between configuration files.			
L2TP IPsec VPN			
Client Scenario Information			
Scenario Settings			
Default Scenario Provides a connection for each selected access component.			
Use Existing Scenario Preferably uses the existing scenario on the endpoint.			
Update and Installation Options			
Customized client setup is used to install iNode client on PCs which have no iNode client installed or upgrade previous clients to current version.			
Generate customized client setup program			
Silent installation A silent installation runs without any user interaction or displaying any dialog boxes.			
MSI MSI can only be installed as notified by the Windows AD domain			
Customized client upgrade package, which must be deployed on the server which is corresponding to the client, is used to upgrade previous clients to current version automatically.			
Generate customized dient upgrade package			
The lightweight client upgrade package is stored on the UAM server with which the client communicates to upgrade the client of a specific version to the current version.			
Generate VPN gateway iNode setup package			
OK Cancel			

 ④ L2TP IPsec VPN Client のインストールパッケージが作成できましたので、Exit をクリック します。



⑤ Client Customization Result ウインドウが表示されますので、Find Target をクリックして、iNode Clilent のインストールプログラムの場所を確認します。

Client Cust	omization Result	$\times$
Custo create	mization succeeded with an extra customized client setup program	
<b>R</b>	Click Find Target to view the new customized client setup program.	
Fir	nd Target	
	Exit	

⑥ iNode Clilent のインストールプログラムの場所です。

C:\Program Files(x86)\iNode\iNode Manager\Setup

🔜    💆 🔜 🗢    Setup			-	o x
ファイル ホーム 共有 表示				~ 🕐
← → × ↑ - Vrogram Files (x86) →	iNode > iNode Manager > Setup	✓ ひ	upの検索	
> 🧋 クイック アクセス	名前	更新日時	種類	サイズ
✓ 🛄 デスクトップ	iNodeSetup7.3 (E0548).exe	2021/06/26 11:18	アプリケーション	36,844 K
> 🦲 OneDrive - New H3C Group				
> 🦱 OneDrive - Personal				
> 🤱 m koshiro				
> 💻 PC				
> 🐂 ライブラリ				
> 👝 MicroSD (E:)				
> 💱 お気に入り(F:)				
> 💣 ネットワーク				
› 📴 コントロール パネル				
🛯 ごみ箱	٢			>
1 個の項目				

⑦ 上記 Client Customization Result ウインドウで、Exit をクリックします。

⑧ iNode Management Center は File(F)メニューから Exit して終了します。



## iNode クライアントのインストール

#### ① iNodeSetup7.3(E05048).exe をダブルクリックして起動します。

iNode Intelligent Client - InstallShield Wizard		
	Welcome to the InstallShield Wizard for iNode Intelligent Client The Installshield(R) Wizard will install iNode Intelligent client on your computer. To continue, click Next.	
	< Back Next > Cancel	

#### ② ライセンス規約を承認します。

iNode Intelligent Client - InstallShield Wizard	×
License Agreement Please read the following license agreement carefully.	
License Agreement	^
Your use of this Software in installation, copy or other way shall be deemed as your acceptance of the clauses of this License Agreement and your consent to execute this License Agreement with New H3C Technologies Co., Ltd. (hereinafter "H3C").	
1. Software Product (hereinafter "The Software")	
The "Software" in this Agreement includes computer software and all or any parts of	~
I accept the terms of the license agreement     Print     I do not accept the terms of the license agreement	
InstallShield	el

# ③ iNode Client のインストールされる場所を確認して、Next をクリックします。 C:\Program Files(x86)\iNode\iNode Client

iNode Intell	igent Client - InstallShield Wizard			×
Choose D Select fo	Destination Location older where setup will install files.			Z
	Install iNode Intelligent Client to: C:¥Program Files (x86)¥iNode¥iNode	: Client		Change
InstallShield ·		< Back	Next >	Cancel

### ④ Install ボタンをクリックしてインストールを始めます。

iNode Intelligent Client - InstallShield Wizard	×
<b>Ready to Install the Program</b> The wizard is ready to begin installation.	
Click Install to begin the installation.	
If you want to review or change any of your installation settings, click exit the wizard.	Back. Click Cancel to
Instalibnield	tall Cancel

#### ⑤ インストールが完了しました。



補足:デスクトップには iNode Clientを起動するためのアイコンが作成されます。



Finishをクリックして、Windowsを再起動後、クライアントを開始します。 クライアントの設定は、前記「4. クライアント側の設定」をご覧ください。

## 付録 2. SecPathF1020 側の設定例

```
#
version 7.1.064, Release 9345P14
#
sysname H3C
#
context Admin id 1
#
irf mac-address persistent timer
irf auto-update enable
undo irf link-delay
irf member 1 priority 1
#
ip pool l2tp1 192.168.10.11 192.168.10.253
#
password-recovery enable
#
vlan 1
#
controller Cellular1/0/0
#
interface Virtual-Template1
ppp authentication-mode pap
remote address pool l2tp1
ip address 192.168.10.1 255.255.255.0
#
interface NULL0
#
interface GigabitEthernet1/0/0
port link-mode route
ip address 192.168.30.1 255.255.255.0
nat outbound 3000
ipsec apply policy 1
#
interface GigabitEthernet1/0/1
port link-mode route
ip address 192.168.20.1 255.255.255.0
#
interface GigabitEthernet1/0/2
port link-mode route
#
```

interface GigabitEthernet1/0/3 port link-mode route # interface GigabitEthernet1/0/4 port link-mode route # interface GigabitEthernet1/0/5 port link-mode route # interface GigabitEthernet1/0/6 port link-mode route # interface GigabitEthernet1/0/7 port link-mode route # interface GigabitEthernet1/0/8 port link-mode route # interface GigabitEthernet1/0/9 port link-mode route # interface GigabitEthernet1/0/10 port link-mode route # interface GigabitEthernet1/0/11 port link-mode route # interface GigabitEthernet1/0/12 port link-mode route # interface GigabitEthernet1/0/13 port link-mode route # interface GigabitEthernet1/0/14 port link-mode route # interface GigabitEthernet1/0/15 port link-mode route # interface GigabitEthernet1/0/16 port link-mode route # interface GigabitEthernet1/0/17

port link-mode route # interface GigabitEthernet1/0/18 port link-mode route # interface GigabitEthernet1/0/19 port link-mode route # interface GigabitEthernet1/0/20 port link-mode route # interface GigabitEthernet1/0/21 port link-mode route # interface GigabitEthernet1/0/22 port link-mode route # interface GigabitEthernet1/0/23 port link-mode route # security-zone intra-zone default permit # security-zone name Local # security-zone name Trust import interface GigabitEthernet1/0/1 # security-zone name DMZ # security-zone name Untrust import interface Virtual-Template1 # security-zone name Management import interface GigabitEthernet1/0/0 # scheduler logfile size 16 # line class aux user-role network-operator # line class console authentication-mode scheme user-role network-admin

# line class usb user-role network-admin # line class vty user-role network-operator # line aux 0 user-role network-admin # line con 0 user-role network-admin # line vty 0 63 authentication-mode scheme user-role network-admin # ssh server enable # arp ip-conflict log prompt # radius scheme user\_db primary authentication 192.168.20.10 key simple test # domain ad.rem-system.com authentication ppp radius-scheme user\_db local authorization ppp radius-scheme user\_db local # domain system # domain default enable ad.rem-system.com # role name level-0 description Predefined level-0 role # role name level-1 description Predefined level-1 role # role name level-2 description Predefined level-2 role # role name level-3 description Predefined level-3 role

# role name level-4 description Predefined level-4 role # role name level-5 description Predefined level-5 role # role name level-6 description Predefined level-6 role # role name level-7 description Predefined level-7 role # role name level-8 description Predefined level-8 role # role name level-9 description Predefined level-9 role # role name level-10 description Predefined level-10 role # role name level-11 description Predefined level-11 role # role name level-12 description Predefined level-12 role # role name level-13 description Predefined level-13 role # role name level-14 description Predefined level-14 role # user-group system # local-user admin class manage password hash \$h\$6\$UbIhNnPevyKUwfpm\$LqR3+yg1IjNct39MkOR0H0iQXLkYB3jMqM4vbAeoXOhbabI IFnjJPEGR00YiYA1Sz4LiY3FmEdru2fOLMb1shQ== service-type ssh terminal https authorization-attribute user-role level-3 authorization-attribute user-role network-admin

authorization-attribute user-role network-operator # local-user client class network password cipher \$c\$3\$bUwUitzleC0IGT/e2EZdVgyMcNcWD3QwxQ== service-type ppp authorization-attribute user-role network-operator # session statistics enable # ipsec logging negotiation enable # ipsec transform-set 1 esp encryption-algorithm 3des-cbc esp authentication-algorithm md5 # ipsec transform-set 2 encapsulation-mode transport esp encryption-algorithm aes-cbc-128 esp authentication-algorithm sha1 # ipsec transform-set 3 encapsulation-mode transport esp encryption-algorithm aes-cbc-256 esp authentication-algorithm sha1 # ipsec transform-set 4 encapsulation-mode transport esp encryption-algorithm des-cbc esp authentication-algorithm sha1 # ipsec transform-set 5 encapsulation-mode transport esp encryption-algorithm 3des-cbc esp authentication-algorithm sha1 # ipsec transform-set 6 encapsulation-mode transport esp encryption-algorithm aes-cbc-192 esp authentication-algorithm sha1 # ipsec policy-template 1 1 transform-set 1 2 3 4 5 6 local-address 192,168,30,1

```
ike-profile 1
#
ipsec policy 1 1 isakmp template 1
#
l2tp-group 1 mode lns
allow l2tp virtual-template 1
undo tunnel authentication
#
l2tp enable
#
ike logging negotiation enable
#
ike profile 1
keychain 1
exchange-mode aggressive
local-identity fqdn Ins
match remote identity address 0.0.0.0 0.0.0.0
match remote identity fqdn inode
match local address GigabitEthernet1/0/0
proposal 1 2 3 4 5 6
#
ike proposal 1
dh group2
authentication-algorithm md5
#
ike proposal 2
encryption-algorithm 3des-cbc
dh group2
authentication-algorithm md5
#
ike proposal 3
encryption-algorithm 3des-cbc
dh group2
#
ike proposal 4
encryption-algorithm aes-cbc-256
dh group2
#
ike proposal 5
dh group2
#
ike proposal 6
encryption-algorithm aes-cbc-192
```

```
dh group2
#
ike keychain 1
match local address GigabitEthernet1/0/0
pre-shared-key address 0.0.0.0 0.0.0.0 key cipher
$c$3$ZS5ysc5WxbGXqQ4HAqHMVJPEYd83fKs=
#
ip https enable
webui log enable
#
loadbalance isp file flash:/lbispinfo_v1.5.tp
#
security-policy ip
rule 0 name 1
 action pass
rule 1 name 0
 action pass
 counting enable
 source-zone Local
 source-zone Trust
 source-zone Untrust
 destination-zone Local
 destination-zone Trust
 destination-zone Untrust
```

```
#
```