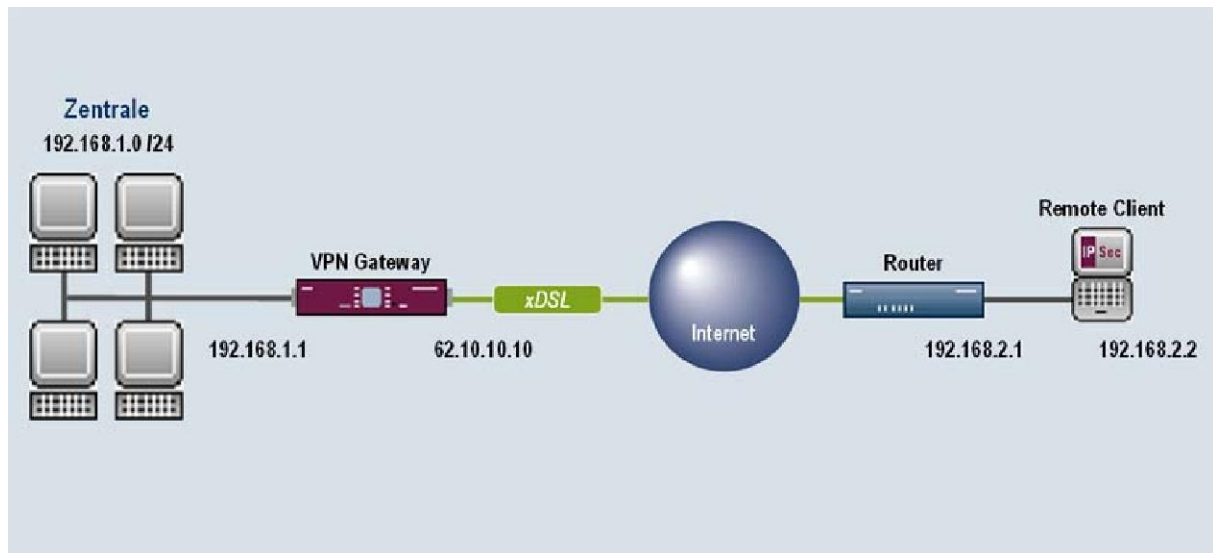


## 1. IPsec Verbindung zwischen Gateway und IPsec Client - Host



### 1.1 Einleitung

Im Folgenden wird die Konfiguration einer IPsec Verbindung zwischen einem Bintec IPsec Gateway und dem Bintec IPsec Client beschrieben. Der Client befindet sich hinter einem Router. Diese Anleitung zeigt die Konfiguration auf Release 7.1.4

Zur Konfiguration wird hierbei das Setup-Tool verwendet.

### 1.2 Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Grundkonfiguration des Gateways
- Für das IPsec Gateway ist ein Bootimage ab Version 7.1.4 zu verwenden.
- Die Konfiguration erfordert auf beiden Gateways einen funktionsfähigen Internetzugang
- Der Remote PC hängt hinter einem Router
- In der Zentrale brauchen Sie eine statische IP Adresse oder DynDNS für das Internet
- Auf dem Remote PC ist der installierte IPsec Client ab Version 1.0 build 78 erforderlich

### 1.3 Konfiguration

Die Anleitung konfiguriert die Zentrale und den Client. Es wird sowohl die Konfiguration mit NAT Traversal, als auch mit NAT Freigaben erläutert.

Um IPsec zu konfigurieren, müssen Sie im Folgenden Menü Einstellungen vornehmen:

Hauptmenü -> IPSEC

In dem Untermenü "Configure Peers" haben Sie die Möglichkeit mit "APPEND" Verbindungspartner für IPsec hinzuzufügen.

#### INFO

Bei der Erstkonfiguration von IPsec startet der Wizard. Den sollten Sie ausführen, um Default Parameter für IPsec zu generieren. Die Vorgehensweise beim Anlegen von Verbindungen ist jedoch beim Wizard und beim manuellen Konfigurieren fast identisch.

### 1.3.1 Einstellungen im Menü IPSEC -> Configure Peers -> APPEND

#### 1.3.1a Configure Peer Parameter

```

VPN Access 25 Setup Tool                               BinTec Access Networks GmbH
[IPSEC][PEERS][ADD]: Configure Peer                    zentrale
-----
Description:      Client
Admin Status:    up           Oper Status:  down

Peer Address:
Peer IDs:        Client
Pre Shared Key:  bintec

IPSec Callback >
Peer specific Settings >

Virtual Interface: no
Traffic List Settings >

                                SAVE                       CANCEL
  
```

Folgende Felder sind hierbei relevant:

Feld	Bedeutung
Description	Geben Sie eine Beschreibung für die Verbindung an.
Peer Address	Die IP Adresse des IPsec Partners (Bleibt bei einer Client Einwahl frei)
Peer IDs	Hier tragen Sie eine Identifikation des Partners ein
Pre Shared Key	Das gemeinsame Passwort von beiden IPsec Partnern
Virtual Interface	Bestimmen Sie hier, ob Sie Traffic List oder Interface Routing konfigurieren.
Traffic List Settings	Hier konfigurieren Sie die Traffic List Einträge (Virtual Interface steht auf: no)

Gehen Sie folgendermassen vor, um die Einstellungen im Peer vorzunehmen:

- Benennen Sie den Eintrag **Client**
- Bei Peer Address geben Sie nichts an. Der Eintrag bleibt leer.
- Bei Peer IDs geben Sie **Client** an
- Im Pre Shared Key tragen Sie **bintec** als Passwort ein
- Virtual Interface steht auf: **no**

### 1.3.1b Traffic List Settings

- Gehen Sie in das Untermenü "Traffic List Settings -> APPEND" um die Traffic List zu bearbeiten. (Sollten Sie den Wizard benutzen, verlassen Sie das Menü mit **SAVE**, um die Traffic List Einträge zu erstellen)

```

VPN Access 25 Setup Tool                               BinTec Access Networks GmbH
[IPSEC][PEERS][EDIT][TRAFFIC][ADD]: Traffic Entry (Client)           zentrale
-----
Description:      Client
Protocol:         dont-verify
Local:
  Type: net      Ip: 192.168.1.0      / 24
Remote:
  Type: host    Ip: 10.10.10.10
Action:          protect
Profile          *autogenerated*      edit >
-----
                                SAVE                                CANCEL
-----
  
```

Folgende Felder sind hierbei relevant:

Feld	Bedeutung
Description	Geben Sie eine Beschreibung für den Eintrag an
Local IP	Geben Sie hier das lokale Netz mit zugehöriger Subnetmask (in BIT) an
Remote Type	Geben Sie hier an, ob der IPsec Partner ein Netz darstellt oder nur ein Host ist
Remote IP	Geben Sie hier eine virtuelle IP Adresse für den Client an

Gehen Sie folgendermassen vor um Ihren Eintrag zu konfigurieren:

- Als Beschreibung geben Sie **Client** an
- Unter Lokal IP tragen Sie **192.168.1.0** mit der Mask **24** ein
- Den Remote Type stellen Sie auf **host**
- Bei Remote IP tragen Sie **10.10.10.10** ein
- Speichern Sie mit **SAVE** ab
- Verlassen Sie alle weiteren Menüs mit **Save** oder **Exit**, bis Sie sich im IPsec Main Menü befinden.

### 1.3.1c IPsec Anpassungen

In folgendem Untermenü können Sie PHASE 1 Vorlagen verändern oder mit ADD hinzufügen:

IPSEC -> IKE (Phase 1) Defaults -> EDIT

VPN Access 25 Setup Tool [IPSEC] [PHASE1] [EDIT]	BinTec Access Networks GmbH zentrale
<pre> Description (Idx 1) : *autogenerated* Proposal           : 19 (Rijndael/MD5) Lifetime          : use default Group             : 2 (1024 bit MODP) Authentication Method : Pre Shared Keys Mode              : aggressiv Heartbeats        : none Block Time        : 0 Local ID          : Local Certificate : none CA Certificates   : Nat-Traversal     : enabled  View Proposals &gt; Edit Lifetimes &gt;           </pre>	
<input type="button" value="SAVE"/>	<input type="button" value="CANCEL"/>
Enter string, max length = 255 chars	

Folgende Felder sind hierbei relevant:

<b>Feld</b>	<b>Bedeutung</b>
Description	Geben Sie dem PHASE 1 Profil einen Namen
Proposal	Mit diesem Algorithmus wird die PHASE 1 verschlüsselt
Mode	Der Mode bestimmt die Methode des IKE Aufbaus
NAT Traversal	Schalten Sie auf enabled, wenn Ihr Client hinter einem Router hängt und Sie in dem Router keine NAT Freigaben konfigurieren können

Konfigurieren Sie die Vorlagen mit folgenden Parametern:

- Die Proposals verändern Sie auf: **19 (Rijndael/MD5)**
- Den Mode stellen Sie auf **aggressiv** da Sie mindestens eine dynamische IP Adresse haben
- NAT Traversal schalten Sie auf **enabled**, wenn Client und Router das unterstützen und Sie in dem Router, hinter dem der Client sitzt, keine NAT Freigaben machen können
- NAT Traversal schalten Sie auf **disabled**, wenn Client oder Router das nicht unterstützen und Sie in dem Router, hinter dem der Client sitzt, NAT Freigaben machen können

Im folgenden Menü können Sie die optional benötigten NAT Freigaben konfigurieren:

IP -> Network Address Translation -> requested from OUTSIDE -> ADD

```

VPN Access 25 Setup Tool                               BinTec Access Networks GmbH
[IP][NAT][EDIT][OUTSIDE][ADD]: NAT - sessions from OUTSIDE (Internet) zentrale

```

---

```

Service                user defined
Protocol               udp

Remote Address
Remote Mask

External Address
External Mask
External Port          specify           Port 500

Internal Address       192.168.2.2
Internal Mask          255.255.255.255
Internal Port          any

                                SAVE                                CANCEL

```

```

VPN Access 25 Setup Tool                               BinTec Access Networks GmbH
[IP][NAT][EDIT][OUTSIDE][ADD]: NAT - sessions from OUTSIDE (Internet) zentrale

```

---

```

Service                user defined
Protocol               esp

Remote Address
Remote Mask

External Address
External Mask
External Port          any

Internal Address       192.168.2.2
Internal Mask          255.255.255.255
Internal Port          any

                                SAVE                                CANCEL

```

**INFO**

Der Client unterstützt per default den NAT Traversal Mode. Die Bintec Software ab Version 7.1.4 hat in dem Phase 1 Profil, das der Wizard generiert, das Feature eingeschaltet. Somit brauchen Sie keine NAT Freigaben im Router zu konfigurieren und können über jeden Router eine IPsec Verbindung herstellen, auch wenn NAT eingeschaltet ist.

In folgendem Untermenü können Sie PHASE 2 Vorlagen verändern oder mit ADD hinzufügen:

IPSEC -> IPsec (Phase 2) Defaults -> EDIT

```

VPN Access 25 Setup Tool                               BinTec Access Networks GmbH
[IPSEC] [PHASE2] [EDIT]                               zentrale
-----
Description (Idx 1) :      *autogenerated*

Proposal              :      23 (ESP(Rijndael/MD5))
Lifetime             :      use default
Use PFS              :      none
Heartbeats          :      none
Propagate PMTU      :      no

View Proposals >
Edit Lifetimes >

                                SAVE                      CANCEL
-----
Enter string, max length = 255 chars
  
```

Folgende Felder sind hierbei relevant:

<b>Feld</b>	<b>Bedeutung</b>
Description	Geben Sie dem PHASE 2 Profil einen Namen
Proposal	Mit diesem Algorithmus wird die PHASE 2 verschlüsselt

Konfigurieren Sie die Vorlagen mit folgenden Parametern:

- Die Proposals verändern Sie auf: **23 (ESP(Rijndael/MD5))**

### 1.3.2 Einstellungen im Bintec IPsec Client

Nach der ersten Installation des Clients müssen Sie über den Secure Client Monitor Ihre Verbindung konfigurieren. Legen Sie für jede Verbindung ein Profil an. Der Wizard startet nach der Installation automatisch. Gehen Sie folgendermassen vor, um eine Verbindung zur Zentrale zu konfigurieren:

- Starten Sie den Wizard ggf. unter Konfiguration -> Profil-Einstellungen -> Neuer Eintrag

1.

Wählen Sie die Konfiguration einer IPsec Verbindung aus

**Verbindung zum Firmennetz über IPsec:**

Erstellt eine Verbindung zum Firmennetzwerk über ein virtuelles privates Netzwerk (VPN) abgesichert über IPsec.

2.

Benennen Sie den Eintrag Zentrale



Name des Profils :

Zentrale

3.

Wählen Sie LAN (over IP) aus, da Sie sich hinter einem Router im Ethernet befinden



Verbindungsmedium :

- ISDN
- ISDN
- Modem
- LAN (over IP)
- xDSL (PPPoE)
- xDSL (AVM - PPP over CAPI)
- GPRS / UMTS
- PPTP

4.

Hier geben Sie die Gateway IP Adresse oder DynDNS Namen der Zentrale an



Gateway :

62.10.10.10

5.

Den IKE Modus setzen Sie auf Aggressive Mode, da Sie auf mindestens einer Seite dynamische IP Adressen haben



Exchange Modus :

Aggressive Mode

EPS-Gruppe :

Keine

Benutze IP-Kompression (LZS)

6.

Shared Secret ist der Preshared Key den Sie im Router hinterlegt haben. Bei Type wählen Sie FQDN aus und geben bei ID Ihre eigene Identifikation an, die der Router unter Peer IDs stehen hat (Client).



Pre-shared Key

Shared Secret :

\*\*\*\*\*

Shared Secret (Wiederholen) :

\*\*\*\*\*



Lokale Identität

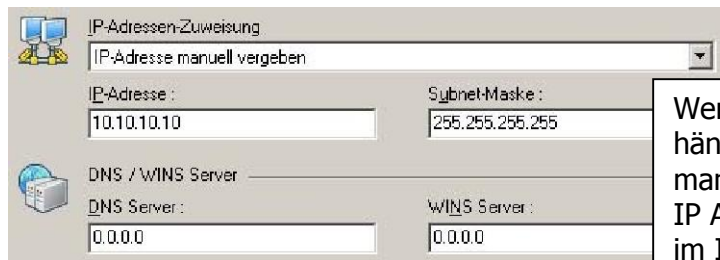
Type :

Fully Qualified Domain Name

ID :

Client

7.



IP-Adressen-Zuweisung  
 IP-Adresse manuell vergeben  
 IP-Adresse : 10.10.10.10 Subnet-Maske : 255.255.255.255  
 DNS / WINS Server  
 DNS Server : 0.0.0.0 WINS Server : 0.0.0.0

Wenn Sie hinter einem Internet Router hängen, wählen Sie „IP-Adresse manuell vergeben“ aus. Geben Sie bei IP Adresse eine virtuelle IP an, die Sie im IPsec Gateway in der Traffic List eingestellt haben (10.10.10.10). Unter DNS und WINS Server können Sie optional IP Adressen von Name Servern aus dem Zentralnetz eintragen

8.



Firewall  
 Stateful Inspection aktivieren : Aus

Optional können Sie die Stateful Inspection Firewall aktivieren. Belassen Sie den Eintrag anfangs auf AUS

Wenn Sie den Wizard ausgeführt haben müssen Sie die Verbindungs-Parameter noch anpassen. Gehen Sie wie folgt vor:

- Konfiguration -> Profil-Einstellungen -> Konfigurieren

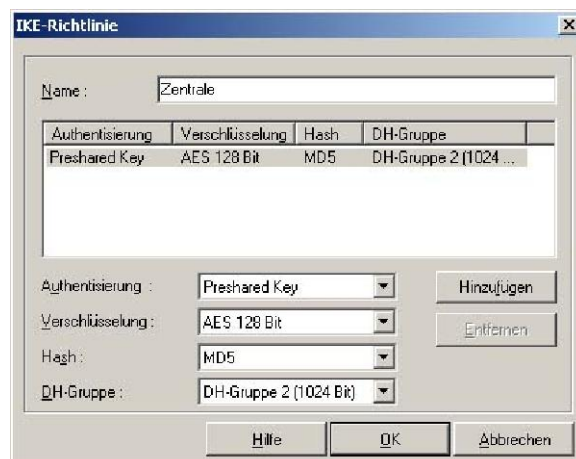
9.



Profil-Einstellungen Zentrale  
 Grundeinstellungen  
 Line Management  
 IPsec-Einstellungen  
 Identität  
 IP-Adressen-Zuweisung  
 VPN IP-Netze  
 Zertifikats-Überprüfung  
 Firewall-Einstellungen  
 IPsec-Einstellungen  
 Gateway : 62.10.10.10  
 Richtlinien  
 IKE-Richtlinie : Automatischer Modus  
 IPsec-Richtlinie : Automatischer Modus  
 Gültigkeit... Editor...  
 Erweiterte Optionen  
 Exch. mode : Aggressive Mode  
 EFS-Gruppe : None  
 IP-Kompression (LZS) verwenden  
 DPD (Dead Peer Detection) deaktivieren  
 Hilfe OK Abbrechen

In den IPsec Einstellungen müssen Sie im Editor die IKE und IPsec Richtlinien konfigurieren. Erstellen Sie unter Editor neue Einträge, die Sie im Anschluss in diesem Menü für die Verbindung auswählen

10.



IKE-Richtlinie  
 Name : Zentrale  

Authentisierung	Verschlüsselung	Hash	DH-Gruppe
Preshared Key	AES 128 Bit	MD5	DH-Gruppe 2 (1024 ...)

 Authentisierung : Preshared Key Hinzufügen  
 Verschlüsselung : AES 128 Bit Entfernen  
 Hash : MD5  
 DH-Gruppe : DH-Gruppe 2 (1024 Bit)  
 Hilfe OK Abbrechen

Benennen Sie den Eintrag Zentrale. Wählen Sie in der Reihenfolge aus:

- Preshared Key
- AES 128
- MD5
- DH-Gruppe2



## 11.



Benennen Sie den Eintrag Zentrale.  
Wählen Sie in der Reihenfolge aus:

- AES 128
- MD5

## 12.



Geben Sie unter VPN IP-Netze das  
Netzwerk der Zentrale an.  
(192.168.1.0)

## 1.4 Ergebnis

Sie haben eine IPsec Verbindung zwischen einem IPsec Gateway und einem Bintec IPsec Client konfiguriert. Der Client hat sich direkt ins Internet eingewählt und eine dynamische Adresse erhalten. Die Zentrale besitzt eine statische IP Adresse. Das Szenario ist wahlweise auch mit Angabe der DynDNS Adresse im Client für die Zentrale zu realisieren.

## 1.5 Kontrolle

Um die IPsec Verbindung zu testen, gehen Sie wie folgt beschrieben vor:

- Geben Sie an der Shell des Gateways folgendes ein: **ipsecGlobMaxSysLogLevel=debug**
- Danach starten Sie den Debug Modus mit : **debug all&**
- Verbinden Sie sich vom Client aus zur Zentrale
- Geben Sie einen Ping von Ihrer Eingabeaufforderung zum Remotenetz des Partners ab

```

C:\>ping 192.168.1.1

Ping wird ausgeführt für 192.168.1.1 mit 32 Bytes Daten:

Antwort von 192.168.1.1: Bytes=32 Zeit=1ms TTL=62
Antwort von 192.168.1.1: Bytes=32 Zeit=1ms TTL=62
Antwort von 192.168.1.1: Bytes=32 Zeit=1ms TTL=62
Antwort von 192.168.1.1: Bytes=32 Zeit=1ms TTL=62

Ping-Statistik für 192.168.1.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
    Ca. Zeitangaben in Millisek.:
    Minimum = 1ms, Maximum = 1ms, Mittelwert = 1ms

C:\>
  
```

Jetzt sollten Sie folgende Meldungen erhalten:

```

zentrale:>
zentrale:> ipsecGlobMaxSysLogLevel=debug
ipsecGlobMaxSysLogLevel( rw):          debug
zentrale:> debug all&
02:25:58 DEBUG/IPSEC: IKE_INVALID_COOKIE: 19700105022558:   Source addr:0.0.0.0
  Destination addr:62.151.213.165
02:25:58 DEBUG/IPSEC: IKE_INVALID_COOKIE: 19700105022558:   Source addr:0.0.0.0
  Destination addr:62.151.213.165
02:25:58 DEBUG/IPSEC: P1: peer 0 () sa 1 (R): new ip 62.10.10.10 <- ip 62.151.21
3.165
02:25:58 INFO/IPSEC: P1: peer 0 () sa 1 (R): Vendor ID: 62.151.213.165:500 (No I
d) is 'draft-ietf-ipsra-isakmp-xauth-06'
02:25:58 INFO/IPSEC: P1: peer 0 () sa 1 (R): Vendor ID: 62.151.213.165:500 (No I
d) is 'draft-ietf-ipsec-nat-t-ike-03'
02:25:58 INFO/IPSEC: P1: peer 0 () sa 1 (R): Vendor ID: 62.151.213.165:500 (No I
d) is 'draft-ietf-ipsec-nat-t-ike-02'
02:25:58 INFO/IPSEC: P1: peer 0 () sa 1 (R): Vendor ID: 62.151.213.165:500 (No I
d) is 'draft-ietf-ipsec-nat-t-ike-00'
02:25:58 INFO/IPSEC: P1: peer 0 () sa 1 (R): Vendor ID: 62.151.213.165:500 (No I
d) is 'draft-ietf-ipsec-dpd-00.txt'
02:25:58 INFO/IPSEC: P1: peer 0 () sa 1 (R): Vendor ID: 62.151.213.165:500 (No I
d) is 'cbled48b6d68269bb411b61a07bce24f'
02:25:58 DEBUG/IPSEC: P1: peer 1 (client) sa 1 (R): identified ip 62.10.10.10 <-
ip 62.15.213.65
02:25:58 DEBUG/IPSEC: P1: peer 1 (client) sa 1 (R): notify id ipv4(any:0,[0..3]=
62.10.10.10) <- id fqdn(any:0,[0..5]=Client) (unencrypted): Initial contact
notification proto 1 spi(16) = [62257e0b d10f904c : 3beelcce 1d524fde]
02:25:58 INFO/IPSEC: P1: peer 1 (client) sa 1 (R): done id ipv4(any:0,[0..3]=62.
10.10.10) <- id fqdn(any:0,[0..5]=Client) AG[62257e0b d10f904c : 3beelcce 1d524f
de]
02:25:58 INFO/IPSEC: P2: peer 1 (client) traf 2 bundle 1 (R): created 192.168.1.
0/192.168.1.0:0 < any > 10.10.10.10/10.10.10.10:0 rekeyed 0
02:25:58 DEBUG/IPSEC: P2: peer 1 (client) traf 2 bundle 1 (R): SA 1 established
ESP[03554571] in[0] Mode tunnel enc rijndael-cbc(16) auth md5(16)
02:25:58 DEBUG/IPSEC: P2: peer 1 (client) traf 2 bundle 1 (R): SA 2 established
ESP[2b0c42ed] out[0] Mode tunnel enc rijndael-cbc(16) auth md5(16)
02:25:58 INFO/IPSEC: Activate Bundle 1 (Peer 1 Traffic 2)
02:25:58 INFO/IPSEC: P2: peer 1 (client) traf 2 bundle 1 (R): established (62.1
10.10.10<->62.151.213.165) with 2 SAs life 28800 Sec/0 Kb rekey 25920 Sec/0 Kb H
b both
02:25:58 DEBUG/INET: NAT: new outgoing session on ifc 100 prot 50 62.10.10.10:0/
62.10.10.10:0 -> 62.151.213.165:0
zentrale:>
  
```

## 1.6 Konfigurationsschritte im IPSEC Menü im Überblick

----- Configure Peer -----		
Feld	Menü	Wert
Description	Configure Peers > APPEND	Client
Peer IDs	Configure Peers > APPEND	Client
Pre Shared Key	Configure Peers > APPEND	bintec
----- Traffic List -----		
Feld	Menü	Wert
Description	Configure Peers > Traffic List Settings > APPEND	Client
Local IP	Configure Peers > Traffic List Settings > APPEND	192.168.1.0 /24
Remote Type	Configure Peers > Traffic List Settings > APPEND	host
Remote IP	Configure Peers > Traffic List Settings > APPEND	10.10.10.10
----- Phase 1 -----		
Feld	Menü	Wert
Proposal	IKE (Phase 1) Defaults > edit > ADD	19 (Rijndael/MD5)
Mode	IKE (Phase 1) Defaults > edit > ADD	aggressiv
----- Phase 2 -----		
Feld	Menü	Wert
Proposal	IPsec (Phase 2) Defaults > edit > ADD	23 (ESP(Rijndael/MD5))