

How to establish IPsec VPN by using X509 certificate?

This document shows how to establish IPsec VPN between two DSR by using RSA signature.

[Topology]

PC1 --- (Lan)DSR-1000AC(Wan1) --- IPsec VPN --- (Wan1)DSR-1000/B1(Lan) --- PC2

Windows server

Note: Windows server only needs to publish certificate so no need to put in this topology.

[Firmware Version]

DSR-1000AC: 3.17B501C_WW

DSR-1000/B1: 3.17B501C_WW

[IP address]

DSR-1000AC:

Wan1: 192.168.11.91/24

Lan: 192.168.0.0/24

DSR-1000/B1:

Wan1: 192.168.11.195/24

Lan: 192.168.10.0/24

[Procedure]

Before start, please make sure "Certificate Authority" function has been installed on your windows server.

1. Access DSR webGUI and go to VPN»IPSec VPN»Certificates»Self Certificate Requests page to generate CSR with below content:
Name: DSR1/DSR2
Subject:
 C=TW, ST=Taiwan, L=Taipei, O=D-Link, OU=TSS2, CN=DSR_1 (on DSR-1000AC)
 C=TW, ST=Taiwan, L=Taipei, O=D-Link, OU=TSS2, CN=DSR_2 (on DSR-1000)
Hash Algorithm: SHA1
Signature Key Length: 2048
Authentication Type: IPsec

The Self Certificate Requests table displays a list of all the certificate requests made.

Self Certificate Requests List

Show 10 entries [Right click on record to get more options]

Name	Status
DSR1	Active Self Certificate Uploaded

Showing 1 to 1 of 1 entries

First Previous 1 Next Last

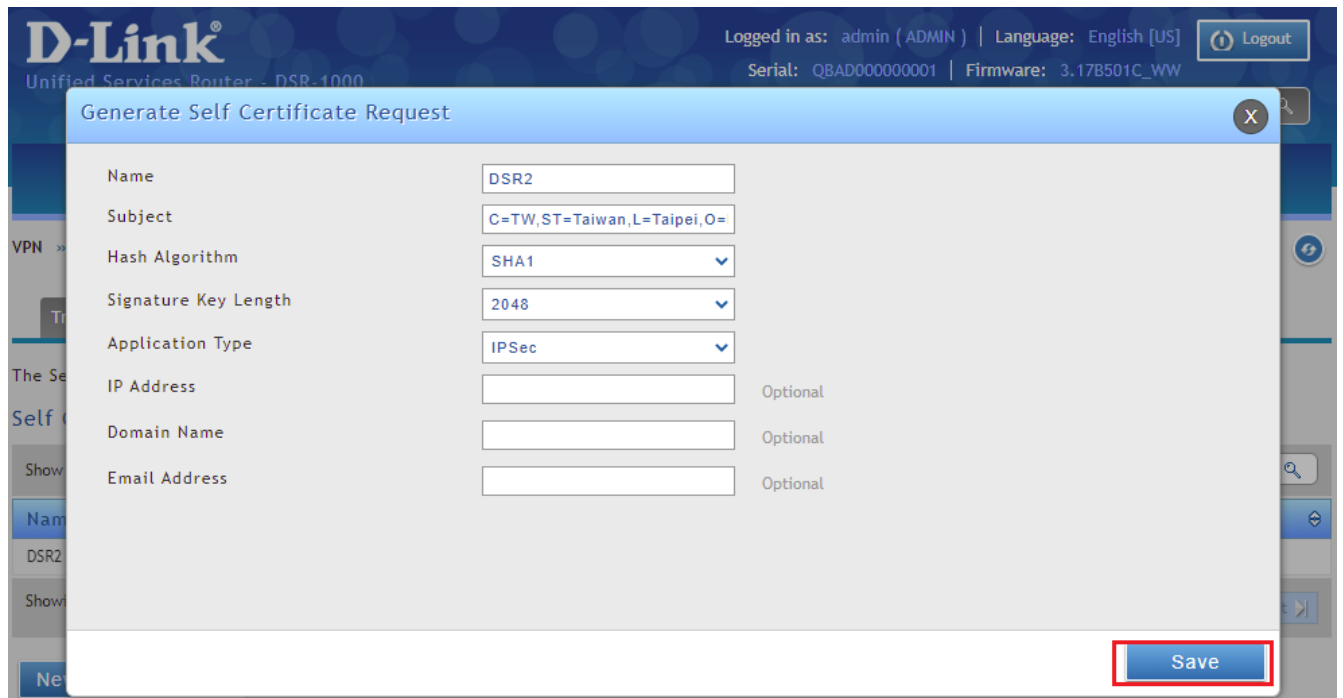
New Self Certificate



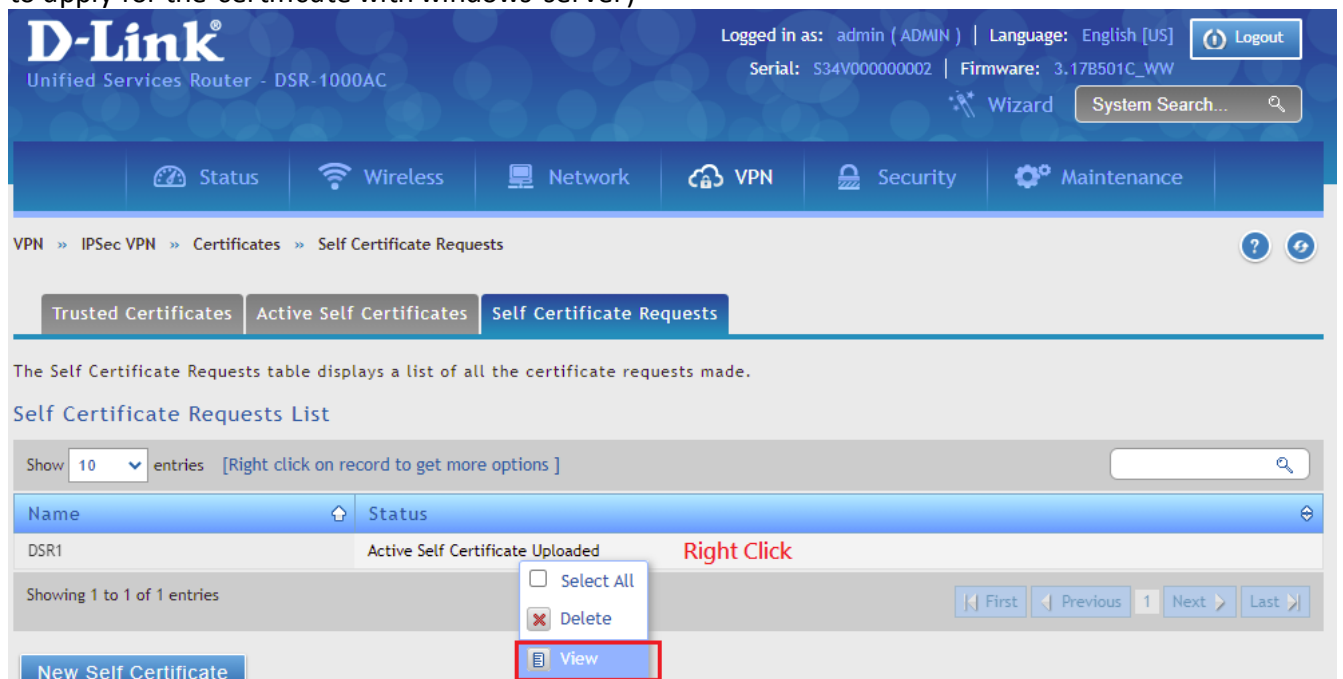
Generate Self Certificate Request

Name	<input type="text" value="DSR1"/>
Subject	<input type="text" value="CN=D-Link,OU=TSS2,CN=DSR_1"/>
Hash Algorithm	<input type="text" value="SHA1"/>
Signature Key Length	<input type="text" value="2048"/>
Application Type	<input type="text" value="IPSec"/>
IP Address	<input type="text"/> Optional
Domain Name	<input type="text"/> Optional
Email Address	<input type="text"/> Optional

Save



- Right click generated certificate View and copy the text as below: (We will need to use the text to apply for the certificate with windows server)



Certificate Details

System Name C=TW,ST=Taiwan,L=Taipei,O=D-Link,OU=TSS2,CN=DSR_1
Hash Algorithm SHA1
Signature Algorithm RSA
Key length 2048
Data to supply to CA

```
2HvK  
wme1kfo/YgYh2wfvP3VbJ9S1Y/PluPiAC9JTjrrGQMRIGOwN5+Vz02vK8X+cgw  
zi  
IOLHS6zFtYxOdqDw+JgINHhR7PwLfQ5I2i75//Ifg0rRHeEsNzaT/aW3W3/mWq  
nG  
DKfXOCqigY8k22GeEgX3Wed1CXeUOkb/taLcm+2WqiEcx0D3dU+JLPowptlyL  
xdq  
LaADBq7m3mFlcXspPzUSHjRIPTY5SZX0aYcmYwMXLbnMweXpEnp9oVLeVRvp  
AGtg  
H4vxEpp61I6DYLaWpEb3Kk4n4BP6ImNci4vDT0ZuEaw2khr8i1CY02CP7nS  
Op5  
iriXyVruC64=  
-----END CERT
```

- Copy Ctrl+C
- Search Google for "-----BEGIN CERTIFICATE REQUEST-----..."
- Print... Ctrl+P
- Inspect Ctrl+Shift+I

D-Link
Unified Services Router - DSR-1000

Logged in as: admin (ADMIN) | Language: English [US] [Logout](#)
Serial: QBAD00000001 | Firmware: 3.17B501C_WW
[Wizard](#)

[Status](#) [Network](#) [VPN](#) [Security](#) [Maintenance](#)

VPN » IPsec VPN » Certificates » Self Certificate Requests

Operation Succeeded

[Trusted Certificates](#) [Active Self Certificates](#) [Self Certificate Requests](#)

The Self Certificate Requests table displays a list of all the certificate requests made.

Self Certificate Requests List

Show entries [\[Right click on record to get more options\]](#)

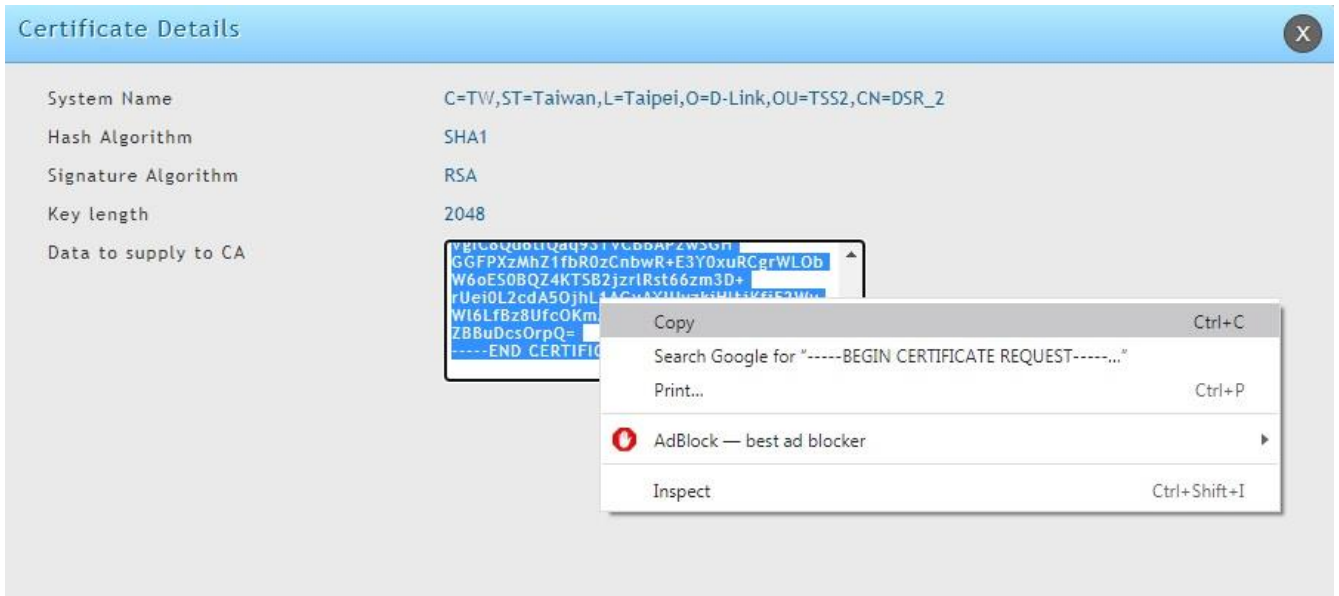
Name	Status
DSR2	Active Self Certificate Not Uploaded Right Click

Showing 1 to 1 of 1 entries

[New Self Certificate](#)

- Select All
- Delete
- View

[First](#) [Previous](#) 1 [Next](#) [Last](#)



3. Go to windows server with URL “ <http://<server ip>/certsrv>” to download a CA certificate.

Microsoft Active Directory Certificate Services — tsd2test-root-CA Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, [install this CA certificate](#).

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [tsd2test-root-CA(1)]
Previous [tsd2test-root-CA]

Encoding method:

DER
 Base 64

[Install CA certificate](#)

[Download CA certificate](#)

[Download CA certificate chain](#)

[Download latest base CRL](#)

[Download latest delta CRL](#)

 certnew.cer ^

全部顯示 ×

4. Apply for DSR IPsec certificate with the text which we saved at step 2.

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

[Request a certificate](#)

[View the status of a pending certificate request](#)

[Download a CA certificate, certificate chain, or CRL](#)

Request a Certificate

Select the certificate type:

[User Certificate](#)

Or, submit an [advanced certificate request](#).

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

```

-----BEGIN CERTIFICATE REQUEST-----
MIICpDCCAYwCAQAwXzELMAkGA1UEBhMCVFcxDzANBgNVBAgMB1RhaXdhbjEPMA0G
A1UEBwwGVGFpcGpMQ8wDQYDVQQKDAZELUxpbmsxDALBgNVBAAsMBFRtUzIxZjAM
BGNVBAwMBURTU18xMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwwJK
KiUQPR9jzF16bV8P/9ZKw9eVJI6FnUbcjD+AVVCGaRqfd+W+cYwH1MJNR9WJHaem
+2lXeHBuJpGzzGQb8TqqvJxH+c1P4l7q09UOCiVnvCY6f+3muJ/iQ2QBa+0apxVA
Geku0RrdYfShJgSFN71DvdJreGbi7vQ/PD1fGhSreZjN/PVAlFC5awI0gX9cMi0f
UVOCgrJFtXGJ5VJgsL+4LT8FwhyZJrbES09+Plv003BfR1NVm0mZoSIHpjerIy1L9
ODN4LC1DiVeAVjzhaHdDixkaRwi1veD6m4RBR0qzH01xea2voeLWKFVf801Mcd1m
gsHm8qyPRN600FzzVwIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBABZgSpJz2HvK
yme1kFo/YgYh2wfvP3VbJ9S1Y/PiUPlAC9JtjnrGQMR1G0wN5+Vz02vK8X+cgwz1
IOLH56zfTyX0dqDw+JgINHHR7PwLFQ5I2i7Sj/Ifg0rRHeEsNzaT/aw3W3/mWqng
DKfXOCiqY8k22GeEgX3Wed1CXeU0kb/taLcm+2Wq1Ecx0D3dU+JLPowpt1yLxdq
LaADBq7m3mF1cXspPzUSHjR1PTy55ZX0aYcmYwMxLBnMweXpEnp9oVLeVRvpAGtg
H4vxEPp61I6DKI+WqFb3Kk4p1RP6JmNci1vDTQ7uFaw2kbyrB11CYO2CCP7nS0p5
irixyVruC64=
-----END CERTIFICATE REQUEST-----

```

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Certificate Template:
IPSec (Offline request) ▼


Additional Attributes:

Attributes:

Certificate Issued

The certificate you requested was issued to you.

DER encoded or
 Base 64 encoded


[Download certificate](#)

[Download certificate chain](#)

Note: Both DSR-1000AC and DSR-1000/B1 need to apply for the certificate, so please do this step twice for both devices.

- Go to DSR webGUI VPN»IPSec VPN»Certificates»Trusted Certificates page to upload the CA certificate file which we got at step3 on both devices.

VPN » IPsec VPN » Certificates » Trusted Certificates

Operation Succeeded

Trusted Certificates | Active Self Certificates | Self Certificate Requests

Trusted Certificates or CA certificates are used to verify the validity of certificates signed by them. When a certificate is generated, it is signed by a trusted organization or authority called the Certificate Authority. The table contains the certificates of each CA. When a remote VPN gateway or client presents a digital certificate, the authentication process verifies that the presented certificate is issued by one of the trusted authorities. The Trusted CA certificates are used in this authentication process.

Trusted Certificates (CA Certificate) List

Show 10 entries [Right click on record to get more options]

CA Identity (Subject Name)	Issuer Name	Expiry Date & Time
DC=com, DC=tsd2test, CN=tsd2test-root-CA	DC=com, DC=tsd2test, CN=tsd2test-root-CA	Jan 18 07:42:02 2039 GMT

Showing 1 to 1 of 1 entries

Upload New CA Certificate

- Go to VPN»IPsec VPN»Certificates»Active Self Certificates to upload assigned certificate which we got at step 4 on both devices.

D-Link
Unified Services Router - DSR-1000AC

Logged in as: admin (ADMIN) | Language: English [US] | Logout

Serial: S34V000000002 | Firmware: 3.17B501C_WW

Wizard | System Search...

Status | Wireless | Network | VPN | Security | Maintenance

VPN » IPsec VPN » Certificates » Active Self Certificates

Trusted Certificates | Active Self Certificates | Self Certificate Requests

This table lists the certificates issued to you by trusted Certification Authorities (CAs), and available for presentation to remote IKE servers. The remote IKE server validates this router using these certificates. For each certificate, the following data is displayed:

Active Self Certificates List

Show 10 entries [Right click on record to get more options]

Name	Subject Name	Serial Number	Issuer Name	Expiry Time
DSR1	C=TW, ST=Taiwan, L=Taipei, O=D-Link, OU=TSS2, CN=DSR_1	2c:00:00:00:11:54:ce:37:fb:98:e1:29:b1:00:01:00:00:11	DC=com, DC=tsd2test, CN=tsd2test-root-CA	Apr 15 03:02:10 2023 GMT

Showing 1 to 1 of 1 entries

Upload New Self Certificate

D-Link® Unified Services Router - DSR-1000

Logged in as: admin (ADMIN) | Language: English [US] | Logout

Serial: QBAD000000001 | Firmware: 3.17B501C_WW

Wizard | System Search...

Status | Network | VPN | Security | Maintenance

VPN » IPsec VPN » Certificates » Active Self Certificates

Trusted Certificates | Active Self Certificates | Self Certificate Requests

This table lists the certificates issued to you by trusted Certification Authorities (CAs), and available for presentation to remote IKE servers. The remote IKE server validates this router using these certificates. For each certificate, the following data is displayed:

Active Self Certificates List

Show 10 entries [Right click on record to get more options]

Name	Subject Name	Serial Number	Issuer Name	Expiry Time
DSR2	C=TW, ST=Taiwan, L=Taipei, O=D-Link, OU=TSS2, CN=DSR_2	2c:00:00:00:12:01:ca:b8:24:a6:68:e9:fc:00:01:00:00:00:12	DC=com, DC=tsd2test, CN=tsd2test-root-CA	Apr 15 03:03:44 2023 GMT

Showing 1 to 1 of 1 entries

First | Previous | 1 | Next | Last

Upload New Self Certificate

- In VPN»IPsec VPN»Certificates»Active Self Certificates, right click the certificate which we uploaded at step 6 with Default.

VPN » IPsec VPN » Certificates » Active Self Certificates

Trusted Certificates | Active Self Certificates | Self Certificate Requests

This table lists the certificates issued to you by trusted Certification Authorities (CAs), and available for presentation to remote IKE servers. The remote IKE server validates this router using these certificates. For each certificate, the following data is displayed:

Active Self Certificates List

Show 10 entries [Right click on record to get more options]

Name	Subject Name	Serial Number	Issuer Name	Expiry Time
DSR1	C=TW, ST=Taiwan, L=Taipei, O=D-Link, OU=TSS2, CN=DSR_1	2c:00:00:00:11:54:ce:37:fb:98:e1:29:b1:00:01:00:00:00:11	DC=com, DC=tsd2test, CN=tsd2test-root-CA	Apr 15 03:02:10

Showing 1 to 1 of 1 entries

First | Previous | 1 | Next | Last

Right Click

- Select All
- Default
- Delete

Upload New Self Certificate

D-Link
Unified Services Router - DSR-1000

Logged in as: admin (ADMIN) | Language: English [US] | Logout
 Serial: QBAD000000001 | Firmware: 3.17B501C_WW
 Wizard | System Search...

Status | Network | VPN | Security | Maintenance

VPN » IPsec VPN » Certificates » Active Self Certificates

Trusted Certificates | **Active Self Certificates** | Self Certificate Requests

This table lists the certificates issued to you by trusted Certification Authorities (CAs), and available for presentation to remote IKE servers. The remote IKE server validates this router using these certificates. For each certificate, the following data is displayed:

Active Self Certificates List

Show 10 entries [Right click on record to get more options]

Name	Subject Name	Serial Number	Issuer Name	Expiry Time
DSR2	C=TW, ST=Taiwan, L=Taipei, O=D-Link, OU=TSS2, CN=DSR_2	2c:00:00:00:12:01:ca:b8:24:a6:68:e9:fc:00:01:00:00:12	DC=com, DC=tsd2test, CN=tsd2test-root-CA	Apr 15 03:03:44 2023 GMT

Showing 1 to 1 of 1 entries

Right Click

- Select All
- Default**
- Delete

Upload New Self Certificate

8. Add IPsec tunnel on DSR-1000AC.

D-Link
Unified Services Router - DSR-1000AC

Logged in as: admin (ADMIN) | Language: English [US] | Logout
 Serial: S34V000000002 | Firmware: 3.17B501C_WW
 Wizard | System Search...

Status | Wireless | Network | VPN | Security | Maintenance

VPN » IPsec VPN » **Policies**

This page shows the list of configured IPsec VPN policies on the router. A user can also add, delete, edit, enable, disable and export IPsec VPN policies from this page.
 Note: Policy with '*' represents a Client Policy.

IPsec Policies List

Show 10 entries [Right click on record to get more options]

Status	Name	Backup Tunnel Name	Type	IPsec Mode	Local	Remote	Auth	Encr
No data available in table								

Showing 0 to 0 of 0 entries

Add New IPsec Policy

IPSec Policy Configuration

General

Policy Name	ToDSR1000B1
Policy Type	Auto Policy
IP Protocol Version	IPv4
IKE Version	IKEv1
L2TP Mode	None
IPSec Mode	Tunnel Mode
Select Local Gateway	Dedicated WAN
Remote Endpoint	IP Address
IP Address / FQDN	192.168.11.195
Enable Mode Config	<input type="checkbox"/> OFF

DSR-1000/B1 Wan IP

IPSec Policy Configuration

Enable Mode Config	<input type="checkbox"/> OFF
Enable NetBIOS	<input type="checkbox"/> OFF
Enable RollOver	<input type="checkbox"/> OFF
Protocol	ESP
Enable DHCP	<input type="checkbox"/> OFF
Local IP	Subnet
Local Start IP Address	192.168.0.0
Local Subnet Mask	255.255.255.0
Remote IP	Subnet
Remote Start IP Address	192.168.10.0
Remote Subnet Mask	255.255.255.0
Enable Keepalive	<input type="checkbox"/> OFF

IPSec Policy Configuration X

Phase1(IKE SA Parameters)

Exchange Mode	Main
Direction / Type	Both
Nat Traversal	<input checked="" type="checkbox"/>
NAT Keep Alive Frequency	20 Seconds
Local Identifier Type	DER ASN1 DN
Local Identifier	192.168.11.91
Remote Identifier Type	DER ASN1 DN
Remote Identifier	192.168.11.195

DSR-1000AC Wan IP
DSR-1000/B1 Wan IP

Encryption Algorithm

DES	<input type="checkbox"/> OFF	3DES	<input checked="" type="checkbox"/> ON
AES-128	<input checked="" type="checkbox"/> ON	AES-192	<input type="checkbox"/> OFF

IPSec Policy Configuration X

Encryption Algorithm

DES	<input type="checkbox"/> OFF	3DES	<input checked="" type="checkbox"/> ON
AES-128	<input checked="" type="checkbox"/> ON	AES-192	<input type="checkbox"/> OFF
AES-256	<input type="checkbox"/> OFF		
BLOWFISH	<input type="checkbox"/> OFF		
CAST128	<input type="checkbox"/> OFF		

Authentication Algorithm

MD5	<input type="checkbox"/> OFF	SHA-1	<input checked="" type="checkbox"/> ON
SHA2-256	<input type="checkbox"/> OFF	SHA2-384	<input type="checkbox"/> OFF
SHA2-512	<input type="checkbox"/> OFF		

Authentication Method	RSA-Signature
Diffie-Hellman (DH) Group	Group 2 (1024 bit)

IPSec Policy Configuration

Diffie-Hellman (DH) Group:

SA-Lifetime: [Range: 300 - 604800] Seconds

Enable Dead Peer Detection: OFF

Extended Authentication:

Phase2-(Auto Policy Parameters)

SA Lifetime:

Encryption Algorithm

DES	<input type="checkbox"/> OFF	None	<input type="checkbox"/> OFF
3DES	<input checked="" type="checkbox"/> ON	AES-128	<input checked="" type="checkbox"/> ON
AES-192	<input type="checkbox"/> OFF	AES-256	<input type="checkbox"/> OFF
TWOFISH (128)	<input type="checkbox"/> OFF	TWOFISH (192)	<input type="checkbox"/> OFF
TWOFISH (256)	<input type="checkbox"/> OFF		
BLOWFISH	<input type="checkbox"/> OFF		
CAST128	<input type="checkbox"/> OFF		

Integrity Algorithm

MD5	<input type="checkbox"/> OFF	SHA-1	<input checked="" type="checkbox"/> ON
SHA2-224	<input type="checkbox"/> OFF	SHA2-256	<input type="checkbox"/> OFF
SHA2-384	<input type="checkbox"/> OFF	SHA2-512	<input type="checkbox"/> OFF
PFS Key Group	<input type="checkbox"/> OFF		

Save

D-Link
Unified Services Router - DSR-1000AC

Logged in as: admin (ADMIN) | Language: English [US] [Logout](#)
Serial: S34V00000002 | Firmware: 3.17B501C_WW
Wizard

Status Wireless Network VPN Security Maintenance

VPN » IPsec VPN » Policies

Operation Succeeded

This page shows the list of configured IPsec VPN policies on the router. A user can also add, delete, edit, enable, disable and export IPsec VPN policies from this page.
Note: Policy with '*' represents a Client Policy.

IPsec Policies List

Show 10 entries [Right click on record to get more options]

Status	Name	Backup Tunnel Name	Type	IPsec Mode	Local	Remote	Auth	Encr
Enabled	ToDSR1000B1	None	Auto Policy	Tunnel Mode	192.168.0.0/255.255.255.0	192.168.10.0/255.255.255.0	SHA1	3DES AES-128

Showing 1 to 1 of 1 entries

[Add New IPsec Policy](#)

9. Add IPsec tunnel on DSR-1000/B1.

D-Link
Unified Services Router - DSR-1000

Logged in as: admin (ADMIN) | Language: English [US] [Logout](#)
Serial: QBAD00000001 | Firmware: 3.17B501C_WW
Wizard

Status Network VPN Security Maintenance

VPN » IPsec VPN » Policies

This page shows the list of configured IPsec VPN policies on the router. A user can also add, delete, edit, enable, disable and export IPsec VPN policies from this page.
Note: Policy with '*' represents a Client Policy.

IPsec Policies List

Show 10 entries [Right click on record to get more options]

Status	Name	Backup Tunnel Name	Type	IPsec Mode	Local	Remote	Auth	Encr
No data available in table								

Showing 0 to 0 of 0 entries

[Add New IPsec Policy](#)

IPSec Policy Configuration X

General

Policy Name	<input type="text" value="ToDSR1000AC"/>
Policy Type	<input type="text" value="Auto Policy"/>
IP Protocol Version	<input type="text" value="IPv4"/>
IKE Version	<input type="text" value="IKEv1"/>
L2TP Mode	<input type="text" value="None"/>
IPSec Mode	<input type="text" value="Tunnel Mode"/>
Select Local Gateway	<input type="text" value="Dedicated WAN"/>
Remote Endpoint	<input type="text" value="IP Address"/>
IP Address / FQDN	<input type="text" value="192.168.11.91"/> DSR-1000AC Wan IP
Enable Mode Config	<input type="checkbox"/> OFF

IPSec Policy Configuration X

Enable Mode Config	<input type="checkbox"/> OFF
Enable NetBIOS	<input type="checkbox"/> OFF
Enable RollOver	<input type="checkbox"/> OFF
Protocol	<input type="text" value="ESP"/>
Enable DHCP	<input type="checkbox"/> OFF
Local IP	<input type="text" value="Subnet"/>
Local Start IP Address	<input type="text" value="192.168.10.0"/>
Local Subnet Mask	<input type="text" value="255.255.255.0"/>
Remote IP	<input type="text" value="Subnet"/>
Remote Start IP Address	<input type="text" value="192.168.0.0"/>
Remote Subnet Mask	<input type="text" value="255.255.255.0"/>
Enable Keepalive	<input type="checkbox"/> OFF

IPSec Policy Configuration

Phase1(IKE SA Parameters)

Exchange Mode

Direction / Type

Nat Traversal

NAT Keep Alive Frequency Seconds

Local Identifier Type

Local Identifier

Remote Identifier Type

Remote Identifier

DSR-1000/B1 Wan IP

DSR-1000AC Wan IP

Encryption Algorithm

DES OFF 3DES ON

AES-128 ON AES-192 OFF

IPSec Policy Configuration

Encryption Algorithm

DES OFF 3DES ON

AES-128 ON AES-192 OFF

AES-256 OFF

BLOWFISH OFF

CAST128 OFF

Authentication Algorithm

MD5 OFF SHA-1 ON

SHA2-256 OFF SHA2-384 OFF

SHA2-512 OFF

Authentication Method

Diffie-Hellman (DH) Group

IPSec Policy Configuration

Diffie-Hellman (DH) Group:

SA-Lifetime: [Range: 300 - 604800] Seconds

Enable Dead Peer Detection: OFF

Extended Authentication:

Phase2-(Auto Policy Parameters)

SA Lifetime:

Encryption Algorithm

DES	<input type="checkbox"/> OFF	None	<input type="checkbox"/> OFF
3DES	<input checked="" type="checkbox"/> ON	AES-128	<input checked="" type="checkbox"/> ON
AES-192	<input type="checkbox"/> OFF	AES-256	<input type="checkbox"/> OFF
TWOFISH (128)	<input type="checkbox"/> OFF	TWOFISH (192)	<input type="checkbox"/> OFF
TWOFISH (256)	<input type="checkbox"/> OFF		
BLOWFISH	<input type="checkbox"/> OFF		
CAST128	<input type="checkbox"/> OFF		

Integrity Algorithm

MD5	<input type="checkbox"/> OFF	SHA-1	<input checked="" type="checkbox"/> ON
SHA2-224	<input type="checkbox"/> OFF	SHA2-256	<input type="checkbox"/> OFF
SHA2-384	<input type="checkbox"/> OFF	SHA2-512	<input type="checkbox"/> OFF
PFS Key Group	<input type="checkbox"/> OFF		

Save

D-Link
Unified Services Router - DSR-1000

Logged in as: admin (ADMIN) | Language: English [US] | Logout
 Serial: QBAD00000001 | Firmware: 3.17B501C_WW
 Wizard | System Search...

Status | Network | VPN | Security | Maintenance

VPN » IPsec VPN » Policies

Operation Succeeded

This page shows the list of configured IPsec VPN policies on the router. A user can also add, delete, edit, enable, disable and export IPsec VPN policies from this page.
 Note: Policy with '*' represents a Client Policy.

IPSec Policies List

Show 10 entries [Right click on record to get more options]

Status	Name	Backup Tunnel Name	Type	IPSec Mode	Local	Remote	Auth	Encr
Enabled	ToDSR1000AC	None	Auto Policy	Tunnel Mode	192.168.10.0/255.255.255.0	192.168.0.0/255.255.255.0	SHA1	3DES AES-128

Showing 1 to 1 of 1 entries

First | Previous | 1 | Next | Last

[Add New IPsec Policy](#)

10. Go to Maintenance»Administration»Date and Time page to make sure both device time is the same.

D-Link
Unified Services Router - DSR-1000AC

Logged in as: admin (ADMIN) | Language: English [US] | Logout
 Serial: S34V000000002 | Firmware: 3.17B501C_WW
 Wizard | System Search...

Status | Wireless | Network | VPN | Security | Maintenance

Maintenance » Administration » Date and Time

This page allows us to set the date, time and NTP servers. Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock time in a network of computers. Accurate time across a network is important for many reasons.

Date and Time

Current Device Time: Thu Apr 15 11:54:56 GMT+0800 2021

Time Zone: (GMT+08:00) Taipei

Daylight Saving: OFF

NTP Servers: ON

NTP Server Type: Default Custom

Time to re-synchronize: 120 [Default: 120, Range: 5 - 1440] Minutes

[Save](#) [Cancel](#)

D-Link
Unified Services Router - DSR-1000

Logged in as: admin (ADMIN) | Language: English [US] [Logout](#)

Serial: QBAD000000001 | Firmware: 3.17B501C_VW

[Wizard](#)

[Status](#) [Network](#) [VPN](#) [Security](#) [Maintenance](#)

Maintenance » Administration » Date and Time

This page allows us to set the date, time and NTP servers. Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock time in a network of computers. Accurate time across a network is important for many reasons.

Date and Time

Current Device Time: Thu Apr 15 11:49:53 GMT+0800 2021

Time Zone: (GMT+08:00) Taipei

Daylight Saving: OFF

NTP Servers: ON

NTP Server Type: Default Custom

Time to re-synchronize: 120 [Default: 120, Range: 5 - 1440] Minutes

[Save](#) [Cancel](#)

[Result]

We can see tunnel can be established when we go to Status»Network Information»Active VPNs»IPsec SAs page to establish IPsec.

Status » Network Information » Active VPNs » IPsec SAs

[IPsec SAs](#) [PPTP VPN Connections](#) [Open VPN Connections](#) [L2TP VPN Connections](#) [GRE Tunnel Status](#)

This page lists current established IPsec Security Associations.

Active IPsec SAs List

Show 10 entries [Right click on record to get more options]

Policy Name	Endpoint	tx (KB)	tx (Packets)	State
ToDSR1000B1	192.168.11.195	0.00	0	IPsec SA Established

Showing 1 to 1 of 1 entries

[First](#) [Previous](#) 1 [Next](#) [Last](#)

Able to ping to DSR-1000/B1 lan from DSR-1000AC lan.

```
CA. Command Prompt
Wireless LAN adapter Wi-Fi:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . : dlink.com.tw
Ethernet adapter Ethernet:
    Connection-specific DNS Suffix . . :
    IPv4 Address. . . . . : 192.168.0.100
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.0.1
Tunnel adapter isatap.<2680B981-7831-4B48-9B3F-D1C081CF6724>:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . :
Tunnel adapter Teredo Tunneling Pseudo-Interface:
    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . :
C:\Users\jason>ping 192.168.10.106
Pinging 192.168.10.106 with 32 bytes of data:
Reply from 192.168.10.106: bytes=32 time=1ms TTL=126
Reply from 192.168.10.106: bytes=32 time=2ms TTL=126
Reply from 192.168.10.106: bytes=32 time=2ms TTL=126
Reply from 192.168.10.106: bytes=32 time=2ms TTL=126
Ping statistics for 192.168.10.106:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 2ms, Average = 1ms
```