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.

 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

VPN » IPSec VPN » Certificates » Self C	ertificate Requests		0 0
Trusted Certificates Active Self	Certificates Self Certificate Re	quests	
The Self Certificate Requests table displ	ays a list of all the certificate requ	ests made.	
Self Certificate Requests List			
Show 10 v entries [Right click on red	cord to get more options]		٩
Name 🗘	Status		⇔
DSR1	Active Self Certificate Uploaded		
Showing 1 to 1 of 1 entries		H	First I Previous 1 Next > Last >
New Self Certificate			
D-Link Unified Services Router - DSR-1000 Generate Self Certificate	Request	Logged in as: admin (ADMIN) L Serial: S34V000000002 Firm	Language: English [US] () Logout ware: 3.17B501C_WW
Name	DSR1		
VPN » Hash Algorithm	,=D-Link.QU=TSS2,CN=	DSR_1	Ø
Signature Key Length	SHAT	×	
Tr Application Type	2048	×	
The Se IP Address			
Self (Domain Name		Optional	
Show Empil Address		Optional	م
Nam		Optional	
DSR1			
Showi			IK a
Ne			Save

	-Link ied Services Router - DSR-1000	Logged in as: admin (ADMIN) Serial: QBAD000000001 Fin	Language: English [US] () Logout mware: 3.178501C_WW
	Generate Self Certificate Request		
	Name	DSR2	
	Subject	C=TW,ST=Taiwan,L=Taipei,O=	
VPN >	Hash Algorithm	SHA1 🗸	0
Т	Signature Key Length	2048 🗸	
_	Application Type	IPSec 🗸	
The Se	IP Address	Optional	
Self	Domain Name	Optional	
Show	Email Address	Optional	٩
Nam			\Leftrightarrow
DSR2			
Show			
Ne			Save

2. 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)

D-L Unified Se	ink ervices Router - D	SR-1000AC		Logged in a Serial:	as: admin (ADMIN) S34V000000002 Fin	Language: English [US] mware: 3.17B501C_WW Wizard System Searc	က် Logout ch ဇ
	🙆 Status	🛜 Wireless	💻 Network	යි VPN	🔒 Security	🍄 Maintenance	
VPN » IPSec	: VPN » Certificates	» Self Certificate Requ	lests				00
Trusted	Certificates Act	ive Self Certificates	Self Certificate Re	equests			
The Self Cer Self Certi	tificate Requests ta ficate Requests	ble displays a list of a List	ll the certificate requ	uests made.			
Show 10	✓ entries [Right cl	ick on record to get mo	re options]				٩
Name		🔂 Status					€
DSR1 Showing 1 to	1 of 1 entries	Active Self Cer	tificate Uploaded Select All Delete	Right Click	И	First J Previous 1 Nex	t 🔪 Last 刘
New Sel	f Certificate		E View				

Certificate Details					X
System Name Hash Algorithm Signature Algorithm Key length Data to supply to CA	C=TW,ST=Taiwan SHA1 RSA 2048 2HvK wmetkfo/YgYh2V	,L=Taipei,O=D-Lir	ik,OU=TSS2,CN=DSf	3_1	
	zi IOLHS62FtYxOdq nG DKfXOCqiqY8k22 xdq LaADBq7m3mFlc AGtg H4vxEPp6116DKL Op5 iriXyVruC64= END CERTI	Dw+JgINHhR7PwLt GeEgX3Wed1CXeU XspPzUSHjRIPTy55 WoEb3Kk401PP6 Copy Search Google fc Print	fQ512i7Sj/Ifg0rRHeE Okb/taLcm+2WqiEc ZX0aYcmYwMXLBnM mNci1yDT07uEaw2l or *BEGIN CERTIFI	ISNZaT/aW3W3/mWq x0D3dU+JLPowptlyL weXpEnp9oVLeVRvp whyEB1CY02CCP7oS	Ctrl+C Ctrl+P
D-Link Unified Services Router - DSR-10	uoo us 🖳 Network		egged in as: admin (Serial: QBAD000000 B Security	ADMIN) Language: Eng 2001 Firmware: 3.1785 Wizard S Maintenance	tish [US] () Logout 01C_WW /stem Search Q
VPN » IPSec VPN » Certificates » Se Trusted Certificates Active Se	If Certificate Requests O If Certificates Self Certifi	peration Succ	eeded		0 0
The Self Certificate Requests table di Self Certificate Requests List	splays a list of all the certific	cate requests mad	e.		
Show 10 v entries [Right click on	record to get more options]				٩
Name 🗘	Status				Θ
DSR2 Showing 1 to 1 of 1 entries New Self Certificate	Active Self Certificate Not Upload	ed Right Click	C Select All	First Previo	us 1 Next > Last >

Certificate Details				x
System Name	C=T₩,ST=Taiwan,L	=Taipei,O=D-Link,OU=TSS2,CN=DSR_2		
Hash Algorithm	SHA1			
Signature Algorithm	RSA			
Key length	2048			
Data to supply to CA	VBLCBQUOTLQQUST GGFPXZMhZ1fbR02C W6oES0BQZ4KT5B2 rUei0L2cdAS0jhL W16LfBz8UfcOKm ZB8uDcS0rpQ= END CERTIFIC	Copy Copy Search Google for "BEGIN CERTIFICATE REQUEST"	Ctrl+C Ctrl+P	
	4	🚺 AdBlock — best ad blocker		۲.
		Inspect	Ctrl+Shift+I	

3. Go to windows server with URL "<u>http://<server ip>/certsrv</u>" to download a CA certificate. *Microsoft* Active Directory Certificate Services – tsd2test-root-CA

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.

Home

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

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

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:



Encoding method:

O DER Base 64

Install CA certificate
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL



全部顯示 ×

Hom

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 Microsoft Active Directory Certificate Services – tsd2test-root-CA

Microsoft Active Directory Certificate Services - tsd2test-root-CA

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:		
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	BEGIN CERTIFICATE REQUEST MITCpDCCAYwCAQAwXzELMAkGAJUEBhMCVF cxDzANBgNVBAgMB1RhaXdhbjEPMA0G A1UEBwwGVGFpcGVpMQ8wDQYDVQQKDAZELUxpbmsxDTALBgNVBAsMBFRTUzIXDjAM BgNVBAMMBURTU18xMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwyJK KiuQPR9jzF16bV8P/9ZKw9eVJ16FnUbcjD+AVvCGaRqfd+W+cYwHIMJNR9WJHaem +21XeHBuJp6zzGQb8TqqVJxH+c1P417q09UOCiVnvCY6F3muJ/iQ2QBa+DapxVA Geku0RrdYfshJgSFN71DvdJreGbi7vQ/PD1FGhSreZjN/PVaLfCSawI0gX9cMiof UVOCgrJftXGJSVJgsL+4LT8HWyJzJrbESO9+Mv003BfRiNMM0mZoSIHpjerIy1L9 ODN4LC1DiVeAVjzhaHdDixkaRwi1veD6mARBR0qzH01xea2voeLWKFVF80LMcd1m gsHm8qyPRN60pzzvwIDAQABoAAwDQYJKoZIhvcNAQEFBQADggEBABZgSpJz2HvK wme1kfo/YgVhzwfvP3VbJ9S1Y/PIuPiAC9JTjrrGQMRIGOwN5+vz02vK8X+cgwzi IOLHS6zFtYxOdqDw+JgINHhR7PwLfQ5I2i75j/Ifg0rRHeEsNzaT/aW3W3/mWgnG DKfXOCqiqY8k2ZGeEgX3WedICXeUOkb/taLcm+2WqiEcx0D3dU+JPowptJyLxdq LaADBq7m3mF1cXspPzUSHjRIPTySSZ0AYcmYwMXLBnMweXpEnp90VLeVRvpAGtg I4vxEPp61I6DKI+WqFb3Kk4p1RP6JmNci1vDTQ7uFaw2kbyrBi1CY02CCP7nS0p5 iriXyVruC64= END CERTIFICATE REQUEST	
Certificate Templ	ate.	
ocranoute rempi	IPSec (Offline request)	-
Additional Attribu	itee:	
Attributes:		
4	Submit >	-
Microsoft Active	Directory Certificate Services – tsd2test-root-CA	Home
Certificate Iss	ued	
The certificate	you requested was issued to you.	
	DER encoded or Sase 64 encoded vnload certificate vnload 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.

5. 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.

Home

VPN » IPSec VPN » Certifi	cates » Trusted Certificates]			00			
		Operation Succeeded	d					
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 v entries [R	ight click on record to get more	options]			٩			
CA Identity (Subject N	ame)	Suer Name	⇔	Expiry Date & Time	⇔			
DC=com, DC=tsd2test, CN=tsd	12test-root-CA	DC=com, DC=tsd2test, CN=tsd2test-ro	ot-CA	Jan 18 07:42:02 2039 GMT				
Showing 1 to 1 of 1 entries			KI F	First 🦪 Previous 1 Next	> Last >			
Upload New CA Certi	ficate							

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

D-L Unified Se	ink ervices Router - DSR-1000AC		Logged in a Serial:	as: admin (ADM S34V000000002	N) Language: Engli Firmware: 3.17850	ish [US] 🕜 Logout IC_WW stem Search ٩
	🙆 Status 🛜 Wireless	💻 Network	A VPN	<u> </u> Securi	ty 🗘 🍄 Mainte	enance
VPN » IPSec	VPN » Certificates » Active Self Certifica	tes				0 0
Trusted	Certificates Active Self Certificates	Self Certificate Re	equests			
This table lis IKE server va	sts the certificates issued to you by trust alidates this router using these certificate	ed Certification Autho es. For each certificat	orities (CAs), and a e, the following d	available for pro lata is displayed	esentation to remote 1:	IKE servers. The remote
Active Sel	f Certificates List					
Show 10	✓ entries [Right click on record to get mo	re options]			(٩
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 2023 GMT
Showing 1 to	1 of 1 entries				H First H Previou	s 1 Next > Last >
Upload N	New Self Certificate					

D-Link	9 uter - DSR-1000		2	Logged in as: admin Serial: QBAD0000	(ADMIN) Language: English [US] 00001 Firmware: 3.17B501C_WW Wizard System Se	Logout earch ۹
	🙆 Status	💻 Network	🚯 VPN	Security	O ^o Maintenance	
VPN » IPSec VPN » Cer Trusted Certificat	rtificates » Active Se	If Certificates	tificate Reques	ts		0 0

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	Show 10 v 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		K First Freviou	1	Next 👂 🛛 Last 刘
Upload	New Self Certificate				

7. 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						0		
Truste	d Certificates	Active Self Certifica	ates	Self Certificate Reque	sts			
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 Se	elf Certificat	es List						
Show 10	✓ entries [Ri	ght click on record to ge	t more	e options]		(٩	
Name 🔂	Subject Name	2	۲	Serial Number	Right Click 🛛 🕀	Issuer Name	⊖ Expiry ⊖ Time	
DSR1	C=TW, ST=Taiwan OU=TSS2, CN=DSR	, L=Taipei, O=D-Link, L_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 t	Showing 1 to 1 of 1 entries 1 Previous 1 Charles 1							
Upload	New Self Cert	ificate					X Delete	

D-Link Unified Services Roo	uter - DSR-1000		Logged in as: admin (ADMIN) Language: English [US] O Logout Serial: QBAD0000000001 Firmware: 3.17B501C_VVV Wizard System Search Q				
	🗥 Status	💻 Network	යි VPN	🔒 Security	OP Maintenance		
VPN » IPSec VPN » Cer	tificates » Active Se	lf Certificates			0 0		
Trusted Certificate	es Active Self Ce	rtificates Self Ceri	tificate Reques	ts			

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		٩			
Name	Subject Name \varTheta	Serial Number	⇔	Issuer Name	$\Theta \begin{array}{c} Expiry \\ Time \end{array} \Theta$
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	Right Click	J Select All		1 Next > Last >
Upload	New Self Certificate		K Delete		

8. Add IPsec tunnel on DSR-1000AC.

D-Link Unified Services Router - DSR-1000AC								Log	ged in a Serial:	ns: admin S34V0000	(ADMIN) 100002 Fin	Language mware: 3 Wizard	: English [U .17B501C_W System	IS] (W Search	່ງ Logout າ Q	
	C	🛆 Status	🛜 Wi	reless	<u></u> 1	Netwo	ork	ഹ്ല v	'PN	@ 9	Security	Q °	Maintenar	ice		
VPN » IPSec VPN » Policies																
This page sh from this pa Note: Policy IPSec Pol	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.															
Show 10	✓ en	tries [Right)	lick on record	to get mor	re options]									(٩
Status	¢	Name		÷	Туре	÷	IPSec Mode	÷	Local	÷	Remote	⇔	Auth	÷	Encr	¢
						No c	lata availa	ble in tab	le							
Showing 0 to	o 0 of 0 e	entries										First	I Previous	Next	> Last	K
Add Nev	w IPSe	c Policy														

IP	Sec Policy Configuration				
G	eneral				*
	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		DSR-1000/B1 Wan IP	
	Enable Mode Config	OFF			
IP	Sec Policy Configuration				x)
	Enable Mode Config	OFF			-
	Enable NetBIOS	OFF			
	Enable RollOver	OFF			l.
	Protocol	ESP	~		
_	Enable DHCP	OFF			P
Г	Local IP	Subnet	~		
L	Local Start IP Address	192.168.0.0			
L	Local Subnet Mask	255.255.255.0			
L	Remote IP	Subnet	~		
	Remote Start IP Address	192.168.10.0			
L	Remote Subnet Mask	255.255.255.0			
	Enable Keepalive	OFF			-

IP:	Sec Policy Configuration						×
Р	hase1(IKE SA Parameters)						
	Exchange Mode		Main		~	✓	
	Direction / Type		Both		~	✓	
	Nat Traversal		ON III				
	NAT Keep Alive Frequency		20			Seconds	
	Local Identifier Type		DER ASN1 DN		~	~	
	Local Identifier		192.168.11.91			DSR-1000AC Wan IP	
	Remote Identifier Type		DER ASN1 DN		~	✓	
	Remote Identifier		192.168.11.195			DSR-1000/B1 Wan IP	
	Encryption Algorithm						
	DES		OFF	3DES		ON 111	
	AES-128	ON		AES-192		OFF	÷
IP	Sec Policy Configuration						×
	Encryption Algorithm						*
	DES		OFF	3DES		ON TH	
	AES-128	ON		AES-192		OFF	
	AES-256		OFF				
	BLOWFISH		OFF				
	CAST128		OFF				
	Authentication Algorithm						
	MD5		OFF	SHA-1		NO THE	
	SHA2-256		OFF	SHA2-384		OFF	
	SHA2-512		OFF				
[Authentication Method		RSA-Signature		~	<u>ন</u>	
	Diffie-Hellman (DH) Group		Group 2 (1024	bit)	~	~	

IPSec Policy Configuration				X
Diffie-Hellman (DH) Group	Group 2 (10)	24 bit) 🗸		*
SA-Lifetime	28800	[Range: 300 - 604800] Seconds		
Enable Dead Peer Detection	OFF			
Extended Authentication	None	~		
Phase2-(Auto Policy Parameters) SA Lifetime	3600	Seconds 🗸		
Encryption Algorithm				
DES	OFF	None	OFF	
3DES	ON III	AES-128	ON III	
AES-192	OFF	AES-256	OFF	
TWOFISH (128)	OFF	TWOFISH (192)	OFF	
TWOFISH (256)	OFF			
BLOWFISH	OFF			
CAST128	OFF			
Integrity Algorithm				
MD5	OFF	SHA-1	ON III	
SHA2-224	OFF	SHA2-256	OFF	
SHA2-384	OFF	SHA2-512	OFF	
PFS Key Group	OFF			
				-
				Save

D-L Unified Se	ink ervices Router - D!	SR-1000AC		Logged in a Serial:	as: admin (ADMIN) S34V000000002 Fin	Language: English [US] mware: 3.178501C_WW Wizard System Search	ن) Logout ۱ ۹
	🕜 Status	🛜 Wireless	💻 Network	🚯 VPN	盈 Security	ᅌ Maintenance	
VPN » IPSec	VPN » Policies						80
			Operatio	on 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	Policie	s List

Show 10		٩							
Status G	Name ⊖	Backup Tunnel ⊖ Name	Туре	IPSec Mode ⊖	Local Ə	Remote ⊖	Auth	Encr \varTheta	
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-Lir Unified Service	tk es Router - DSR	-1000		Lo <u>s</u>	Logged in as: admin (ADMIN) Language: English [US] O Logout Serial: QBAD000000001 Firmware: 3.178501C_WW Wizard System Search Q					
	🙆 St	atus	Network	ക	VPN	盈 Security	🍄 Maintenar	nce		
VPN » IPSec VPN This page shows th from this page. Note: Policy with IPSec Policies	» Policies me list of configure (**' represents a C List	red IPsec VPN lient Policy.	policies on the	router. A	user can als	o add, delete, e	dit, enable, disable a	and export IPsed	? 🥑	
Show 10 🗸 er	ntries [Right click	on record to ge	et more options]						٩	
Status 📀	Name Ə	Backup Tunnel Name	⊖ Ө	⊖ M	Sec ode ⊖	Local 🖯	Remote Ə	Auth Θ	Encr Θ	

No data available in table

|| First || Previous | Next > | Last >|

Showing 0 to 0 of 0 entries

Add New IPSec Policy

IPSec Policy Configuration			×
General			(
Policy Name	ToDSR100DAC		
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	192.168.11.91	DSP 1000AC Wap IP	
Enable Mode Config	OFF	DSR-1000AC Wallin	
F 11 N 10105			
IPSec Policy Configuration			×
Enable Mode Config	OFF		
Enable NetBIOS	OFF		
Enable RollOver	OFF		
Protocol	ESP	~	
Enable DHCP	OFF		
Local IP	Subnet	~	
Local Start IP Address	192.168.10.0		
Local Subnet Mask	255.255.255.0		
Remote IP	Subnet	~	
Remote Start IP Address	192.168.0.0		
Remote Subnet Mask	255.255.255.0		
Enable Keepalive	OFF		

IPSec Policy Configuration				x
Phase1(IKE SA Parameters)				^
Exchange Mode	Main	~		
Direction / Type	Both	~		
Nat Traversal	ON III			
NAT Keep Alive Frequency	20		Seconds	
Local Identifier Type	DER ASN1 DN	~		
Local Identifier	192.168.11.195		DSR-1000/B1 Wan IP	
Remote Identifier Type	DER ASN1 DN	~		
Remote Identifier	192.168.11.91		DSR-1000AC Wan IP	
Encryption Algorithm	-			
DES	OFF	3DES	ON	
AES-128	N	AES-192	OFF	-
IPSec Policy Configuration				x
Encryption Algorithm				*
DES	OFF	3DES	ON THE	
AES-128		AES-192	OFF	
AES-256	OFF			
BLOWFISH	OFF			
CAST128	OFF			
Authentication Algorithm				
MD5	OFF	SHA-1	ON III	
SHA2-256	OFF	SHA2-384	OFF	
SHA2-512	OFF			
Authentication Method	RSA-Signature	~		
Diffie-Hellman (DH) Group	Group 2 (1024 b	oit) 🗸		÷

IPSec Policy Configuration				X
Diffie-Hellman (DH) Group	Group 2 (10	24 bit) 🗸		*
SA-Lifetime	28800	[Range: 300 - 604800] Seconds		
Enable Dead Peer Detection	OFF			
Extended Authentication	None	~		
Phase2-(Auto Policy Parameters)				
SA Lifetime	3600	Seconds 🗸		
Encryption Algorithm				
DES	OFF	None	OFF	
3DES		AES-128	ON	
AES-192	OFF	AES-256	OFF	
TWOFISH (128)	OFF	TWOFISH (192)	OFF	
TWOFISH (256)	OFF			+
BLOWFISH	OFF			
CAST128	OFF			
Integrity Algorithm				
MD5	OFF	SHA-1	ON	
SHA2-224	OFF	SHA2-256	OFF	
SHA2-384	OFF	SHA2-512	OFF	
PFS Key Group	OFF			
				T
				Save

D-Link Unified Services Router - DSR-1000 Logged in as: admin (ADMIN) Language: English [US] Serial: QBAD000000001 Firmware: 3.178501C_WW Wizard System Search							ک Logout rch ۹			
		孢 Status	💻 Ne	twork 🤇	S VPN	Security	/ 🗘 Mainte	enance		
VPN » IPSec VF	PN » Policies	(00
				Оре	eration Suc	ceeded				
This page show from this page. Note: Policy wi	s the list of c ith '*' represe	configured IPs nts a Client P	ec VPN policie Policy.	es on the route	er. A user can	also add, delete	, edit, enable, disał	ole and expo	rt IPse	c VPN policies
Show 10	es List entries [Rig	ht click on rec	ord to get more	e options]				C		٩
Status N	lame ⊖	Backup Tunnel ⊖ Name	Туре	IPSec Mode ⊖	Local	÷	Remote	⊖ Au	th ⊖	Encr ⊖
Enabled T	oDSR1000AC	None	Auto Policy	Tunnel Mode	192.168.10.0/	255.255.255.0	192.168.0.0/255.255.2	55.0 SH	A1	3DES AES-128
Showing 1 to 1 o	of 1 entries						First	Previous	1 Ne	xt 🔀 🛛 Last 💥

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

D-Link Jnified Services Router - DS	Logged in Seria	Logged in as: admin (ADMIN) Language: English [US] Logout Serial: S34V000000002 Firmware: 3.17B501C_WW Wizard System Search Q				
🝘 Status	🛜 Wireless 📃	Network 🚯 VPN	Security	Maintenance		
ntenance » Administration » I	Date and Time				?	
page allows us to set the dat	e, time and NTP servers. Netwark is imp	vork Time Protocol (NTP) is ortant for many reasons.	a protocol that is used	to synchronize computer cl	lock time	
te and Time						
Current Device Time	Thu Apr 15	11:54:56 GMT+0800 2021				
Time Zone	(GMT+08:0	0) Taipei 🗸 🗸				
Daylight Saving	OFF					
NTP Servers	ON					
NTP Server Type	Default	O Custom				
Time to re-synchronize	120	[Default: 120, Range: 5 - 14	40] 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 »		0 0					
IPsec SAs PPTP VPN Con	nections Open VPN Co	onnections L2TP V	PN Connections GRE Tu	nnel Status			
This page lists current establis	ned IPsec Security Associa	tions.					
Active IPSec SAs List							
Show 10 v entries [Right click on record to get more options]					٩		
Policy Name	Endpoint	⊖ tx (KB)	⊖ tx (Packets)	⊖ State	⇔		
ToDSR1000B1	192.168.11.195	0.00	0	IPsec SA	IPsec SA Established		
Showing 1 to 1 of 1 entries				🔣 First 🔄 Pre	vious 1 Next > Last >]		

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

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 . :			5
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			0