

How To Setup IPSec VPN mit X509 Zertifikaten

[Voraussetzungen]

1. DSR-500N/1000N mit Firmware Version: v1.06B43 und höher

[Szenario]

(lan:192.168.10.1/24)DSR1(Wan:1.1.1.2)------(Wan:1.1.1.1)DSR2(lan:192.168.11.1/24)

[Schritte]

Stellen Sie bitte sicher, dass sich Server und Client in der korrekte, gleichen Zeitzone befinden.

Procedures:

1. Browse to http://<server_ip>/certsrv on server
2. Download a CA certificate
3. Select Base 64 encoded and download CA certificate
4. Save the trusted certificate file
5. Upload the trusted certificate file to DUT

D-Link

DSR-500N // SETUP ADVANCED TOOLS STATUS HELP

Application Rules ▶
Website Filter ▶
Firewall Settin... ▶
Wireless Settings ▶
Advanced Networ... ▶
Routing ▶
Certificates
Users ▶
IP/MAC Binding
IPv6 ▶
Radius Settings
Captive Portal ▶
Switch Settings
Intel® AMT

CERTIFICATES LOGOUT

Digital Certificates (also known as X509 Certificates) are used to authenticate the identity of users and systems, and are issued by Certification Authorities (CA) such as VeriSign, Thawte and other organizations. Digital Certificates are used by this router during the Internet Key Exchange (IKE) authentication phase to authenticate connecting VPN gateways or clients, or to be authenticated by remote entities.

Trusted Certificates (CA Certificate)

<input type="checkbox"/>	CA Identity (Subject Name)	Issuer Name	Expiry Time
<input type="checkbox"/>	DC=tw, DC=com, DC=ryan, DC=nps, CN=nps-WIN-297MMBWJC3A-CA	DC=tw, DC=com, DC=ryan, DC=nps, CN=nps-WIN-297MMBWJC3A-CA	Mar 9 08:38:30 2016 GMT

Upload Delete

Active Self Certificates

<input type="checkbox"/>	Name	Subject Name	Serial Number	Issuer Name	Application Type	Expiry Time
<input type="checkbox"/>					IPsec ▼	

Upload Delete Default

Self Certificate Requests

<input type="checkbox"/>	Name	Status	Application Type	Action
<input type="checkbox"/>				

New Self Certificate Delete

Helpful Hints...
IPsec VPN, SSL VPN, and management over HTTPS use digital certificates. The router has a default self-signed certificate, and this can be replaced by one signed by a known Certificate Authority if needed. Note that a CA certificate provides strong assurance of the server's identity and is a requirement for most corporate network VPN solutions.
More...

6. Generate self certificate on two IPsec VPN peer units:

- a. Name: DSR1/DSR2
- b. Subject(Fixed format in Red):
 C=TW, ST=Taiwan, L=Taipei, O=D-Link, OU=TSS2, CN=DSR_1 (for DSR-1)
 C=TW, ST=Taiwan, L=Taipei, O=D-Link, OU=TSS2, CN=DSR_2 (for DSR-2)
- c. Hash Algorithm : SHA1
- d. Signature Key Length: 2048
- e. Authentication Type: IPsec

7. Click View and copy the text as below:

-----BEGIN CERTIFICATE REQUEST-----

MIICojCCAYoCAQAwXTElMAkGA1UEBhMCVFcxDzANBgNVBAGTBIRhaXdhbjE
PMA0G

A1UEBxMGVGFpGpMQ8wDQYDVQQKEwZELUxpbnmsxDDAKBgNVBAsTA1RT
RDENMAcG

A1UEAxMERMFSMTCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBA
NYIU/Rt

5CTbLsR2P9RJYiKdbrYa6VGq6p1REJrS4nsW7I4BjdeLiJ45CcGxurVTCgO06FWP
/rWTXH8I45CdKT8hhk73Lby0k0KN/UGFsmlo5f0YQb0DAK6SggKvuhaWPsgQoRVN
qOoTKjev2ToSR6XLxYmumPgQERr6aGwajiC2ffwlcZKWo8+7RI+5Xp/Ka+nRzdd0
bEqiVwdhNbeP5vEWY7N70/L7JuX3FiDzVd+TxW1HU1IwW1NPcWShut2P5Z5UuM
U

oyZ28n08QafhmycIGyizts2HlyxEpXS3/alOWJh1zSFKwi+YEMYsEmD0mz+dIMIL
frC/YrE7bAT9fDECAwEAaAAMA0GCSqGSIb3DQEBAQUAA4IBAQAAtwNGViHS
D7SJa

Ze8e7N6UL6KOGVJM5PVLcghe4IOvRnPrbIHWsJ6epi6An137ZSkhy7mT3l/Ba9V
JDusUcwG/23dhpiKzBLlGzrEI4k9eiFkcYLwKlzWvxDJRyV9D3Xi/QN7wd1gYqZK
hOc9mni4E8kDfdYCe+2kgZQujjwLiwR3nmeuUzDoMadG22SvbhyQtGdEdomnLOFe
dXS3P3oIgX2ZsbBgVLGid1y6JbTiAlz1JqBN+jaIjy/xNdgjxGQT27lBe7YkGiDC
Njqx9vzHJu8yQzz7WJ4jjb/RMdtjIVe3QyoUsH9nq2cuihyElCs8TAdpxvew86hT
A4Ttix8T

-----END CERTIFICATE REQUEST-----

8. Paste above to the Certificate Server (http://<server_ip>/certsrv)

- a. Click Request a certificate
- b. Click Advanced certificate request
- c. Click Submit a certificate request by using a base-64....
- d. Paste the above copied text to the Saved Request screen, choose Certificate Template as IPsec (Offline request)(The template needs to create before requesting), then press Submit

e. Choose Base64 encoded and click 'Download certificate'

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):

```
/oCG3xvfSyXq0Qtrn1SxcaVEnrrVWizPhqIgKd6W  
ND0s8geLQ4jkMnCG/EriaJhErSyzGbNI9oJe6Jao  
HtCaRozYDHiIdOK91U51wpVd8nZkzWampvE4Czgy  
AkBR0bh6xiyMPW6avSs/1OF9izy1JPm//0UPckNz  
7lydgagf  
-----END CERTIFICATE REQUEST-----
```

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](#)

9. Back to DUT, choose Authentication Type as IPsec, click Upload to upload the Certificate file

10. Check the Active Self Certificates and press 'Default' button to set it as default certificate.

D-Link

DSR-500N // SETUP ADVANCED TOOLS STATUS HELP

Application Rules ▶
Website Filter ▶
Firewall Sett... ▶
Wireless Settings ▶
Advanced Networ... ▶
Routing ▶
Certificates ▶
Users ▶
IP/MAC Binding ▶
IPv6 ▶
Radius Settings ▶
Captive Portal ▶
Switch Settings ▶
Intel® AMT

CERTIFICATES LOGOUT

Digital Certificates (also known as X509 Certificates) are used to authenticate the identity of users and systems, and are issued by Certification Authorities (CA) such as VeriSign, Thawte and other organizations. Digital Certificates are used by this router during the Internet Key Exchange (IKE) authentication phase to authenticate connecting VPN gateways or clients, or to be authenticated by remote entities.

Trusted Certificates (CA Certificate)

<input type="checkbox"/>	CA Identity (Subject Name)	Issuer Name	Expiry Time
<input type="checkbox"/>	DC=tw, DC=com, DC=ryan, DC=nps, CN=nps-WIN-297MMBWJC3A-CA	DC=tw, DC=com, DC=ryan, DC=nps, CN=nps-WIN-297MMBWJC3A-CA	Mar 9 08:38:30 2016 GMT

Upload Delete

Active Self Certificates

<input type="checkbox"/>	Name	Subject Name	Serial Number	Issuer Name	Application Type	Expiry Time
<input checked="" type="checkbox"/>		C=TW, ST=Taiwan, L=Taipei, O=D-Link, OU=TSD, CN=DSR1	61:7e:19:20:00:00:00:00:39	DC=tw, DC=com, DC=ryan, DC=nps, CN=nps-WIN-297MMBWJC3A-CA	IPSEC	Feb 12 10:11:00 2014 GMT

Upload Delete Default

Self Certificate Requests

<input type="checkbox"/>	Name	Status	Application Type	Action
<input type="checkbox"/>	DSR1	Active Self Certificate Uploaded	ipsec	View

Helpful Hints...
IPsec VPN, SSL VPN, and management over HTTPS use digital certificates. The router has a default self-signed certificate, and this can be replaced by one signed by a known Certificate Authority if needed. Note that a CA certificate provides strong assurance of the server's identity and is a requirement for most corporate network VPN solutions.
[More...](#)

11. Create an IPSec VPN policy on both peers. Set Local/Remote Identifier Type to DER ASN1 DN and enter local/remote IP address on Phase1, others just like normal IPsec configurations.

General	
Policy Name:	IPSec
Policy Type:	Auto Policy ▾
IKE Version:	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
IKE Version:	<input checked="" type="radio"/> IKEv1 <input type="radio"/> IKEv2
IPsec Mode:	Tunnel Mode ▾
Select Local Gateway:	Dedicated WAN ▾
Remote Endpoint:	IP Address ▾ 1.1.1.1
Enable Mode Config:	<input type="checkbox"/>
Enable NetBIOS:	<input type="checkbox"/>
Enable RollOver:	<input type="checkbox"/>
Protocol:	ESP ▾
Enable DHCP:	<input type="checkbox"/>
Local IP:	Subnet ▾
Local Start IP Address:	192.168.10.0
Local End IP Address:	
Local Subnet Mask:	255.255.255.0
Local Prefix Length:	
Remote IP:	Subnet ▾
Remote Start IP Address:	192.168.11.0
Remote End IP Address:	
Remote Subnet Mask:	255.255.255.0
Remote Prefix Length:	
Enable Keepalive:	<input type="checkbox"/>

Phase1(IKE SA Parameters)

Exchange Mode: Main ▼

Direction / Type: Both ▼

Nat Traversal:

On:

Off:

NAT Keep Alive Frequency (in seconds): 20

Local Identifier Type: DER ASN1 DN ▼

Local Identifier: 1.1.1.2

Remote Identifier Type: DER ASN1 DN ▼

Remote Identifier: 1.1.1.1

Encryption Algorithm:

Key length:

3DES:

AES-128:

AES-192:

AES-256:

BLOWFISH:

CAST128:

Authentication Algorithm:

MD5:

SHA-1:

SHA2-256:

SHA2-384:

SHA2-512:

Authentication Method: RSA-Signature ▼

Phase2-(Auto Policy Parameters)

SA Lifetime: ▾

Encryption Algorithm:

NONE:

DES:

3DES:

AES-128:

AES-192:

AES-256:

AES-CCM:

AES-GCM:

TWOFISH (128):

TWOFISH (192):

TWOFISH (256):

BLOWFISH:

CAST128:

Integrity Algorithm:

MD5:

SHA-1:

SHA2-224:

SHA2-256:

SHA2-384:

SHA2-512:

PFS Key Group: ▾

Follow those steps above, two DSR devices are now able to build IPsec VPN tunnel through X509.