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

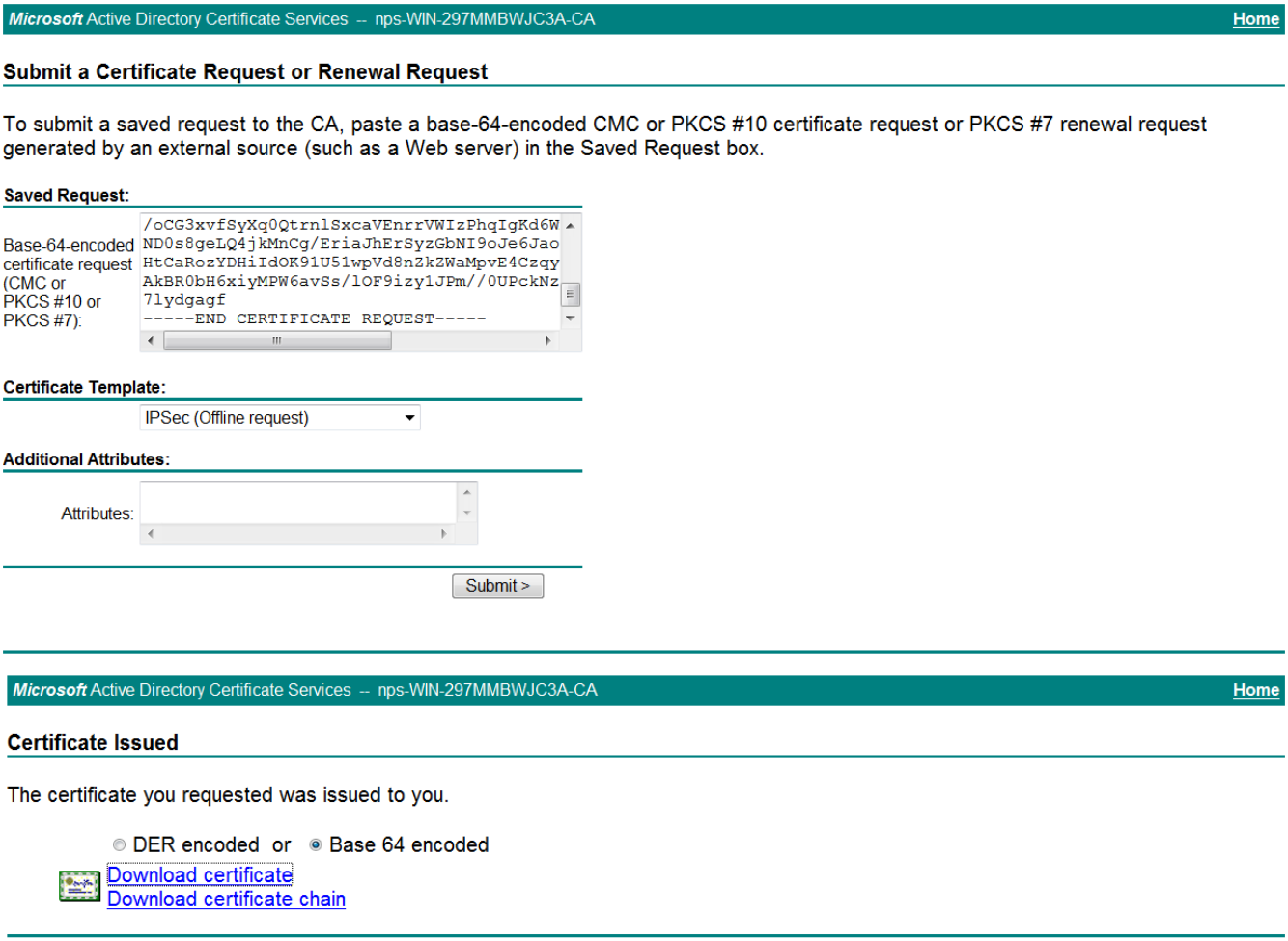
6. Generate self certificate on two IPSec VPN peer units:
   a. Name: DSR1/DSR2
   b. Subject(Fixed format in Red):
      C=TW, ST=Taiwan, L=Taipei, O=D-Link, OU=TSS2, CN=DSR_1 (for DSR-1)
      C=TW, ST=Taiwan, L=Taipei, O=D-Link, OU=TSS2, CN=DSR_2 (for DSR-2)
   c. Hash Algorithm : SHA1
   d. Signature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

7. Click View and copy the text as below:

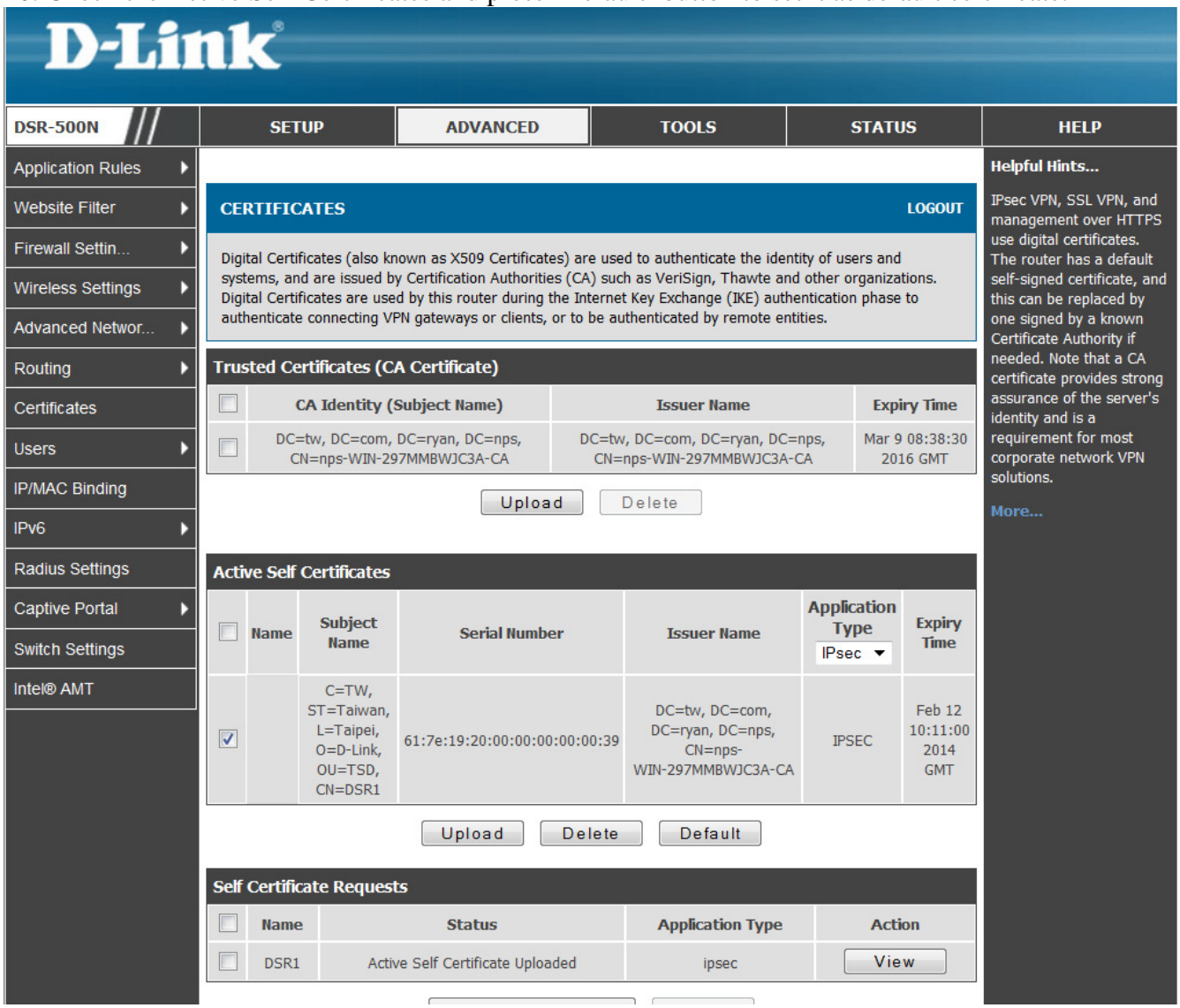
-----BEGIN CERTIFICATE REQUEST-----
MIICojCCAYoCAQAwXTELMAkGA1UEBhMCVFcxDzANBgNVBAgTBlRhaXdhbjEPMA0G
A1UEBxMGVGFpcGVpMQ8wDQYDVQQKEwZELUxpbmsxDDAKBgNVBAsTA1RTRDENMAsG
A1UEAxMERFNSMTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBANYIU/Rt
5CTbLsR2P9RJYiKdbrYa6VGq6p1REJrS4nsW7I4BjdeLiJ45CcGxurVTCgO06FWP
/rWTXH8I45CdKT8hhk73Lby0k0KN/UGFsmlo5f0YQb0DAK6SggKvuhaWPsgQoRVN
qOOTKjev2ToSR6XLxYmumPgQERr6aGwajiC2ffwlCZKWo8+7RI+5Xp/Ka+nRzdd0
bEeqiVwdhNbeP5vEWY7N70/L7JuX3FiDZvD+TxW1HU1IwW1NPcWShut2P5Z5UuMU
oyZ28n08QafhmycIGyizts2HlyxEpXS3/alOWJh1zSFKwi+YEMYsEmD0mz+dlMlL
frC/YrE7bAT9fDECAwEAAaAAMA0GCSqGSIb3DQEBBQUAA4IBAQAtwNGViHSD7SJa
Ze8e7N6UL6KOGVJM5PVLCghe4IOvRnPprbIHWsJ6epi6An137ZSkhy7mT3l/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

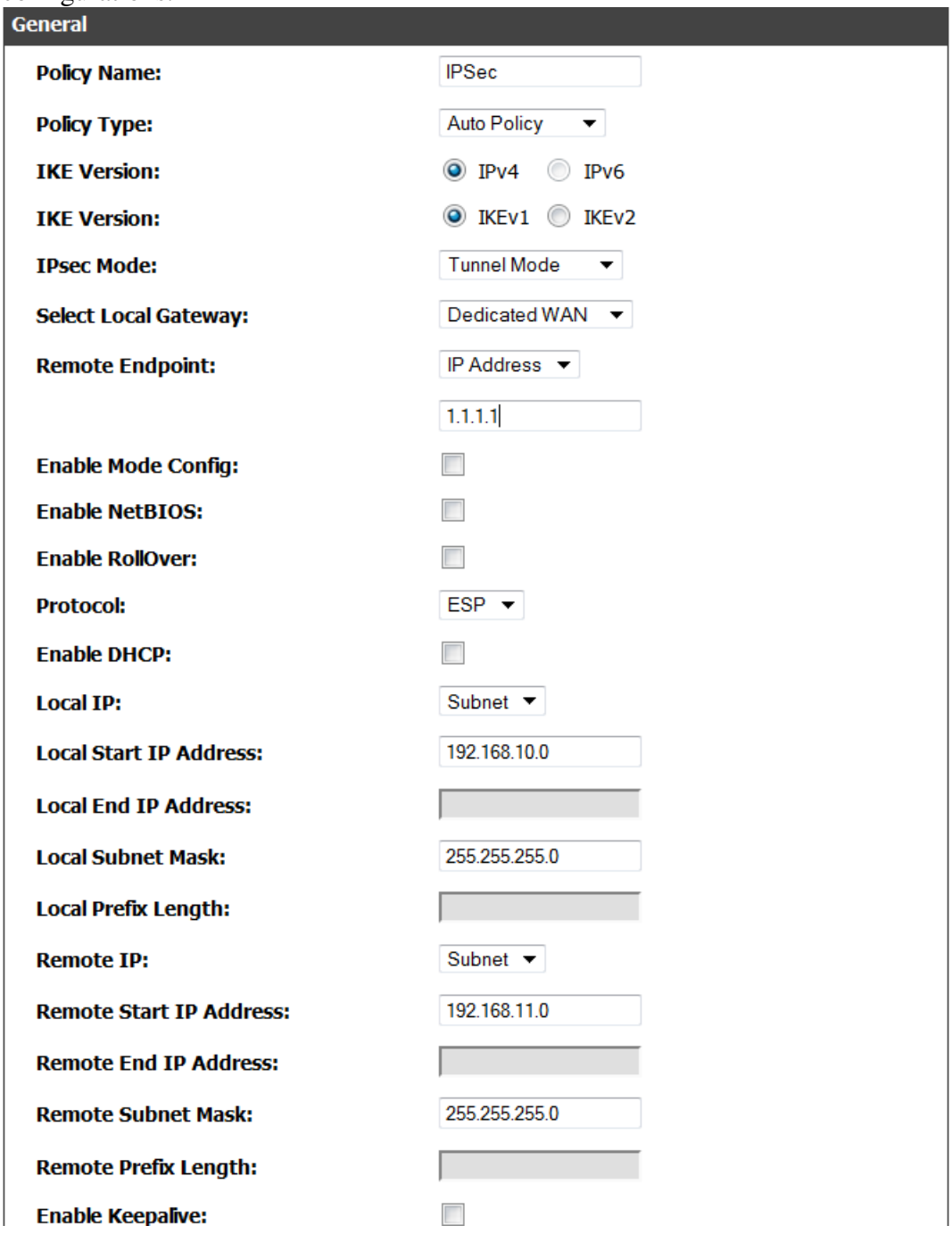
e. Choose Base64 encoded and click ‘Download certificate’

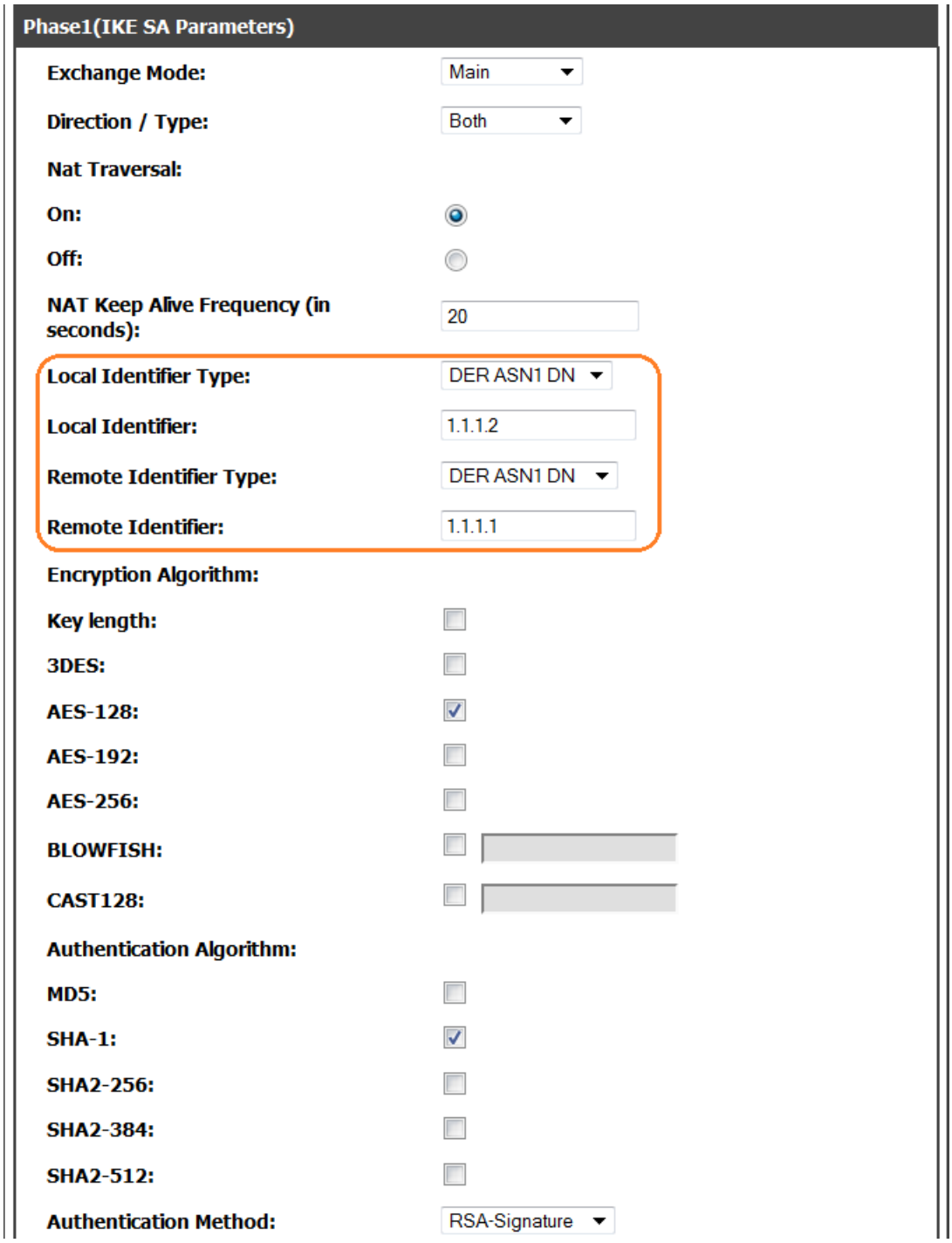


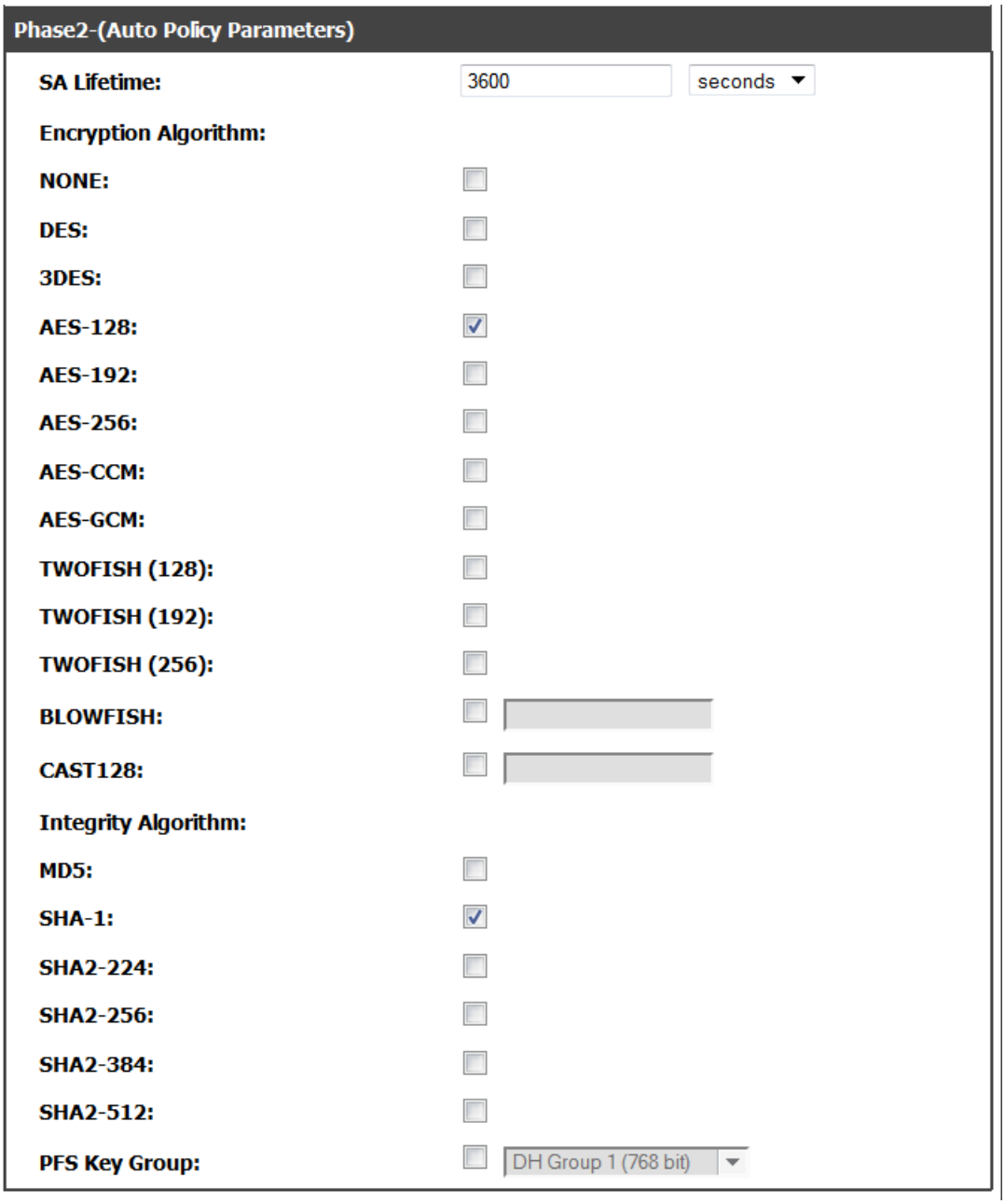
9. Back to DUT, choose Authentication Type as IPsec, click Upload to upload the Certificate file
10. Check the Active Self Certificates and press 'Default' button to set it as default certificate.



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.




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



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