D-Link

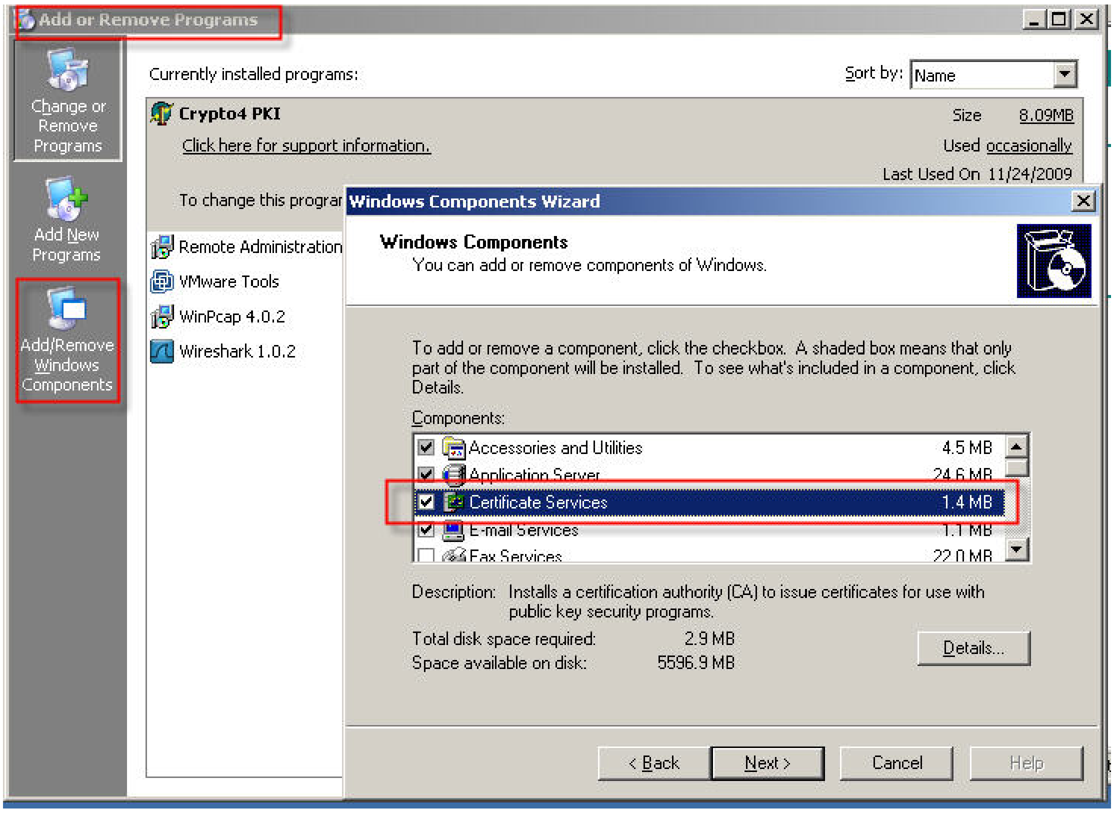
How To Use Windows CA Server For TLS_ALG

In this case, firewall can proxy https service while translates the “HTTPS” traffic to “HTTP_Server”. It means, http client established a http session with firewall, and get http information from a HTTP_Server which behind DFL firewall.

1. Topology:

HTTP_Server(192.168.1.2)---(192.168.1.1)DFL-Series(10.1.1.12)---(10.1.1.13)HTTP_client

2. Create CAs for firewall, now setup CA service.



Currently installed programs:

Size 8.09MB

Used occasionally

Last Used On 11/24/2009

To change this prograr

Windows Components

You can add or remove components of Windows.

To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.

Components:

☑ Accessories and Utilities 4.5 MB

☑ Application Server 24.6 MB

☑ Certificate Services 1.4 MB

☑ E-mail Services 1.1 MB

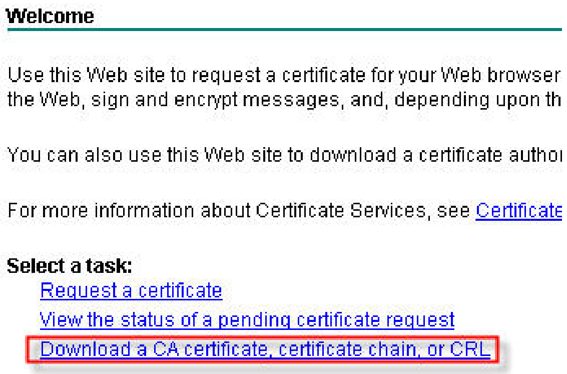
□ Fax Services 22.0 MB

Description: Installs a certification authority (CA) to issue certificates for use with public key security programs.

Total disk space required: 2.9 MB

Space available on disk: 5596.9 MB

3. Download Root CA, go to http://127.0.0.1/certsrv, and:



Welcome

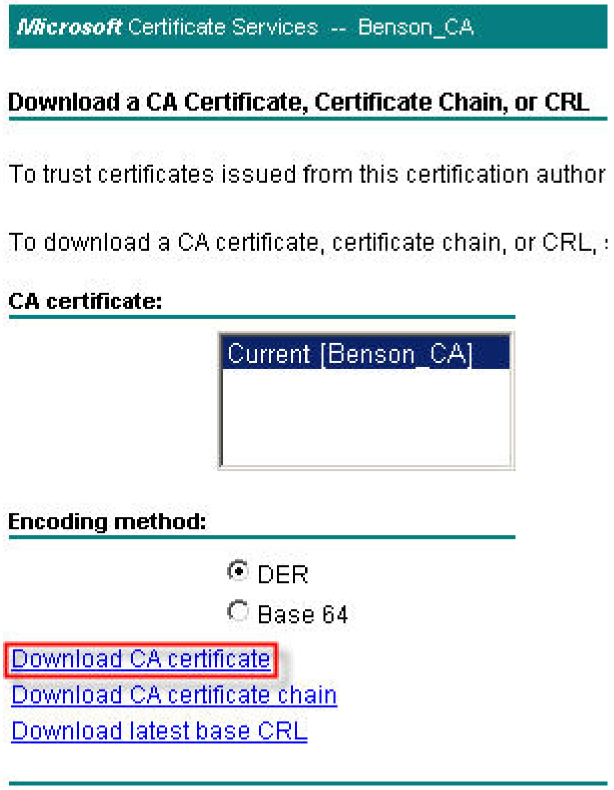
Use this Web site to request a certificate for your Web browser
the Web, sign and encrypt messages, and, depending upon th

You can also use this Web site to download a certificate authoi

For more information about Certificate Services, see Certificate

Select a task:

- Request a certificate
- View the status of a pending certificate request
- Download a CA certificate, certificate chain, or CRL



Microsoft Certificate Services -- Benson_CA

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification author

To download a CA certificate, certificate chain, or CRL, :

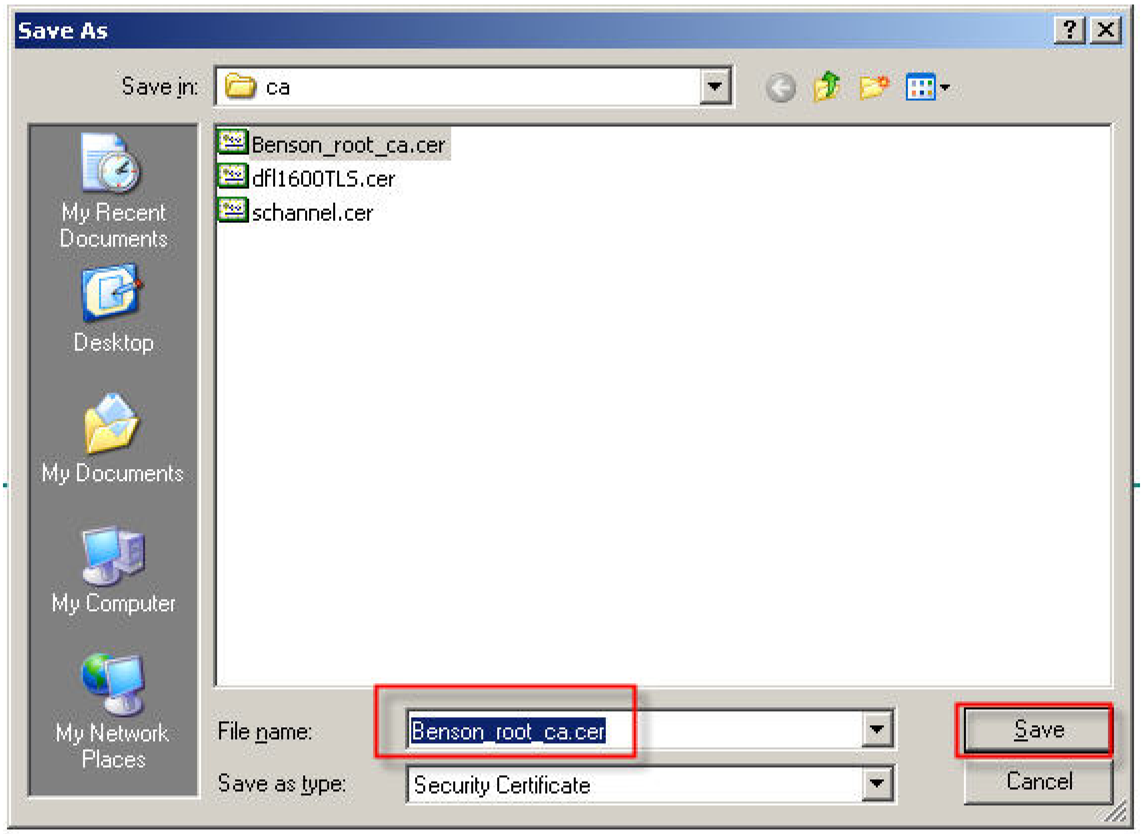
CA certificate:

Current [Benson_CA]

Encoding method:

● DER
○ Base 64

Download CA certificate
Download CA certificate chain
Download latest base CRL



Benson_root_ca.cer
dfl1600TLS.cer
schannel.cer

File name: Benson_root_ca.cer

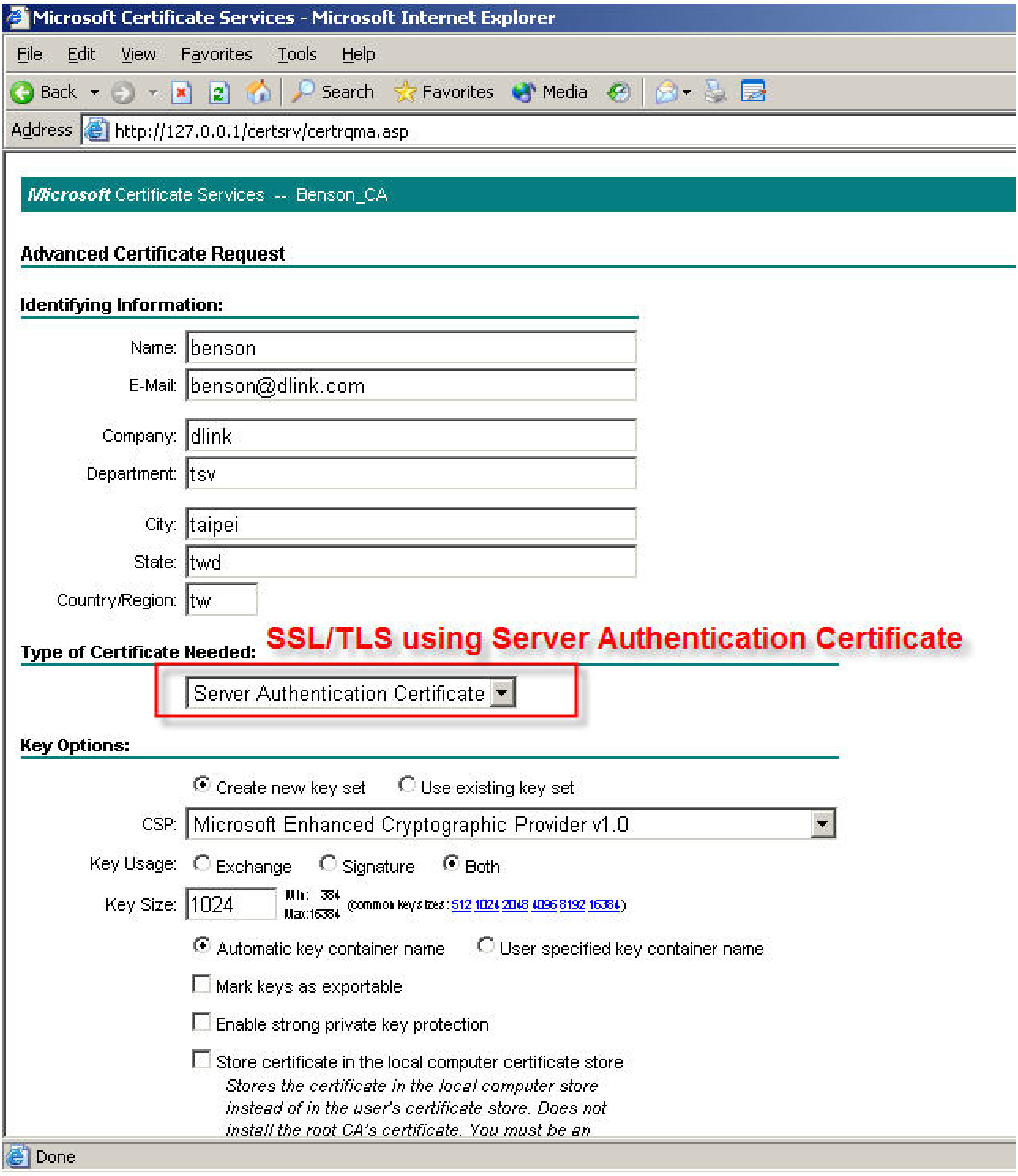
Save as type: Security Certificate

4. Request a CA for TLS_ALG.

   Request a certificate

   Or, submit an advanced certificate request.

   Create and submit a request to this CA.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://127.0.0.1/certsrv/certrqma.asp
Microsoft Certificate Services -- Benson_CA
Done

Advanced Certificate Request

Identifying Information:

Name: benson
E-Mail: benson@dlink.com
Company: dlink
Department: tsv
City: taipei
State: twd
Country/Region: tw

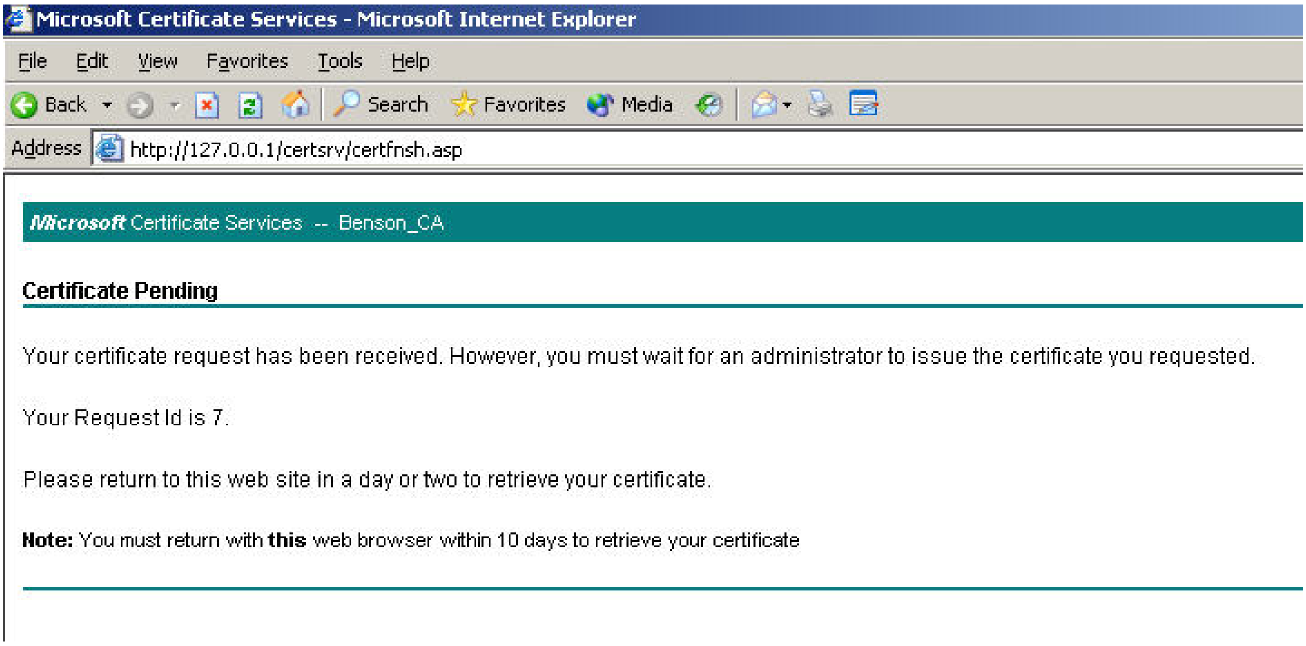
Type of Certificate Needed: Server Authentication Certificate

SSL/TLS using Server Authentication Certificate

Key Options:

● Create new key set ○ Use existing key set
CSP: Microsoft Enhanced Cryptographic Provider v1.0
Key Usage: ○ Exchange ○ Signature ● Both
Key Size: 1024 Min: 384 Max:16384 (common key sizes: 512 1024 2048 4096 8192 16384)
● Automatic key container name ○ User specified key container name
□ Mark keys as exportable
□ Enable strong private key protection
□ Store certificate in the local computer certificate store
Stores the certificate in the local computer store instead of in the user's certificate store. Does not install the root CA's certificate. You must be an

5. Now, CA is pending.


Microsoft Certificate Services - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address

http://127.0.0.1/certsrv/certfnsh.asp

Microsoft Certificate Services -- Benson_CA

Certificate Pending

Your certificate request has been received. However, you must wait for an administrator to issue the certificate you requested.

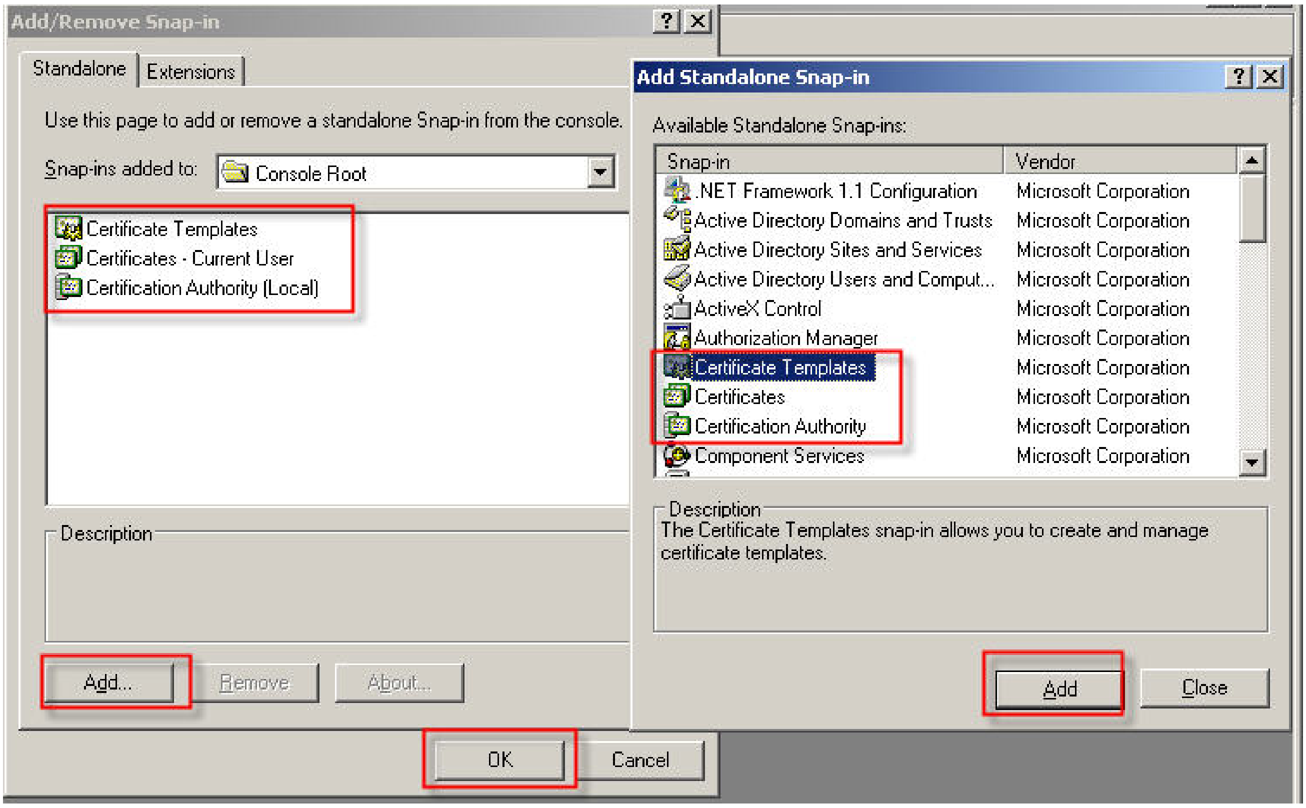
Your Request Id is 7.

Please return to this web site in a day or two to retrieve your certificate.

Note: You must return with **this** web browser within 10 days to retrieve your certificate

6. Go to MMC-> CA to issued this CA.

Start > mmc



Use this page to add or remove a standalone Snap-in from the console.

Snap-ins added to: Console Root

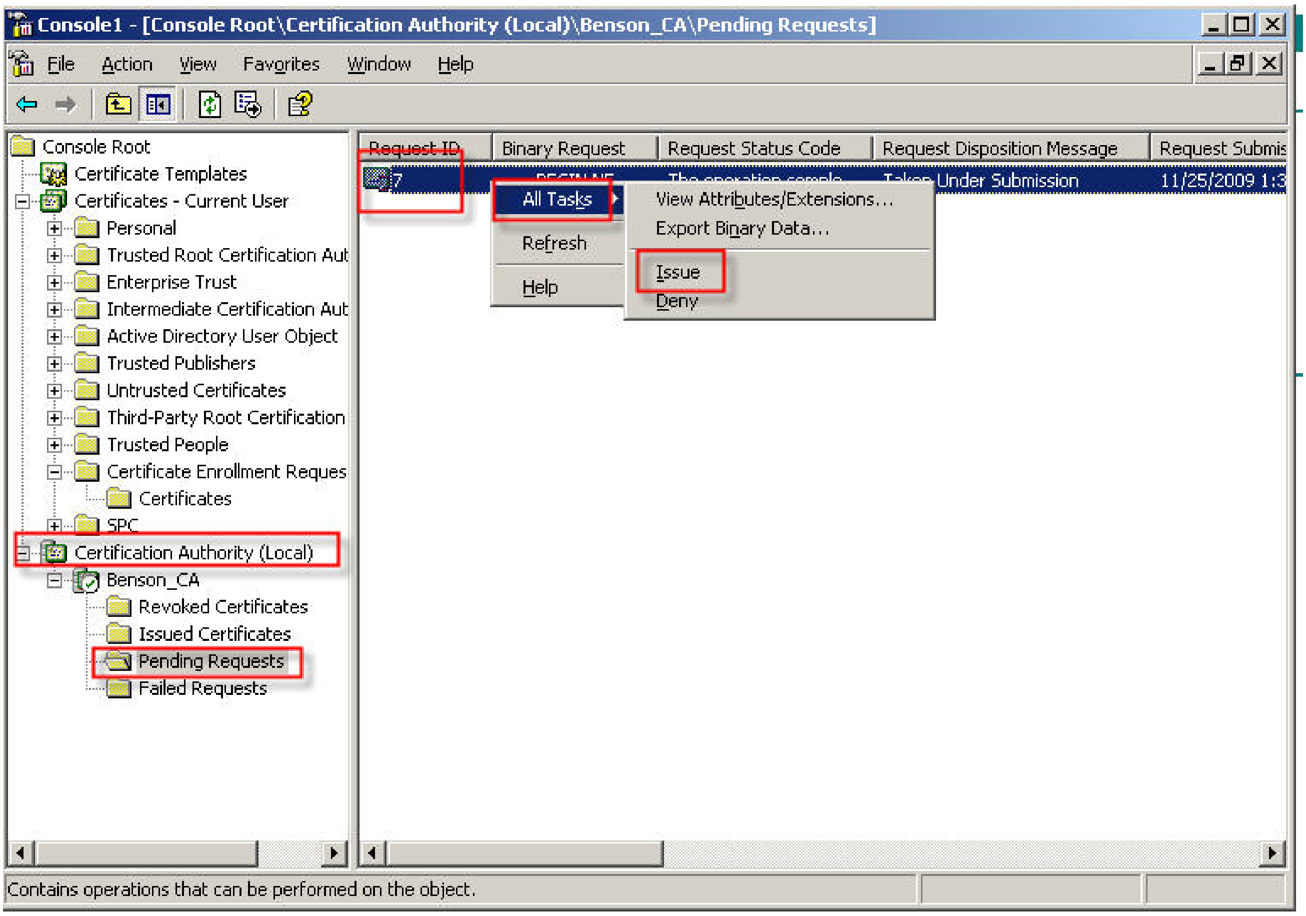
- Certificate Templates
- Certificates - Current User
- Certification Authority (Local)

Description

Available Standalone Snap-ins:

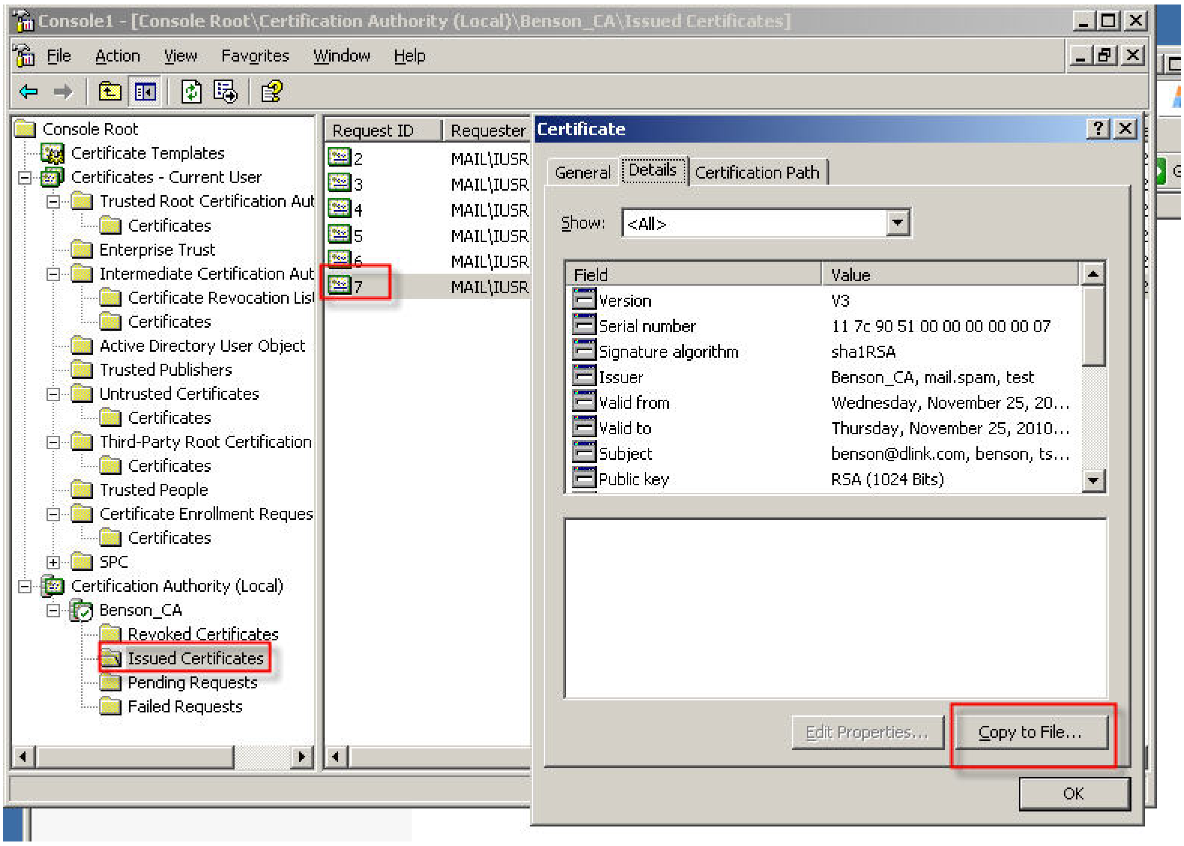
Snap-in	Vendor
.NET Framework 1.1 Configuration	Microsoft Corporation
Active Directory Domains and Trusts	Microsoft Corporation
Active Directory Sites and Services	Microsoft Corporation
Active Directory Users and Comput...	Microsoft Corporation
ActiveX Control	Microsoft Corporation
Authorization Manager	Microsoft Corporation
Certificate Templates	Microsoft Corporation
Certificates	Microsoft Corporation
Certification Authority	Microsoft Corporation
Component Services	Microsoft Corporation

Description
The Certificate Templates snap-in allows you to create and manage certificate templates.

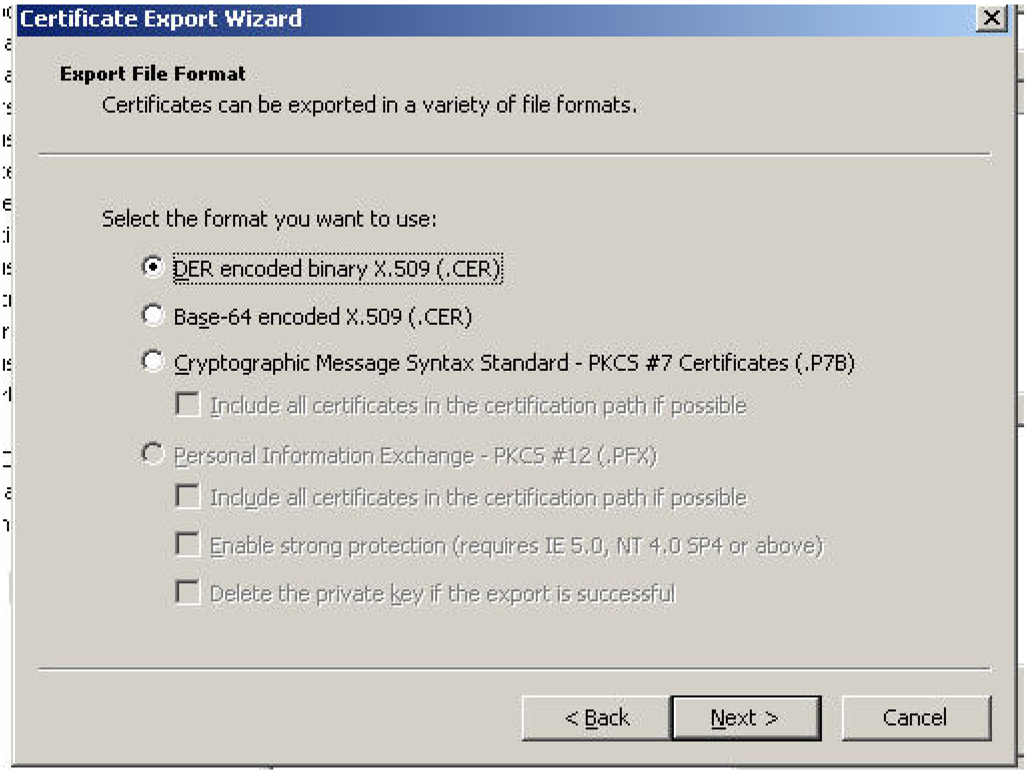

Console1 - [Console Root\Certification Authority (Local)\Benson_CA\Pending Requests]
File Action View Favorites Window Help
Console Root
Certificate Templates
Certificates - Current User
Personal
Trusted Root Certification Aut
Enterprise Trust
Intermediate Certification Aut
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification
Trusted People
Certificate Enrollment Reques
Certificates
SPC
Certification Authority (Local)
Benson_CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Request ID
Binary Request
Request Status Code
Request Disposition Message
Request Submis
7
Taken Under Submission
11/25/2009 1:3
All Tasks
Refresh
Help
View Attributes/Extensions...
Export Binary Data...
Issue
Deny

Contains operations that can be performed on the object.

7. Copy this CA.



Field	Value
Version	V3
Serial number	11 7c 90 51 00 00 00 00 00 07
Signature algorithm	sha1RSA
Issuer	Benson_CA, mail.spam, test
Valid from	Wednesday, November 25, 20...
Valid to	Thursday, November 25, 2010...
Subject	benson@dlink.com, benson, ts...
Public key	RSA (1024 Bits)



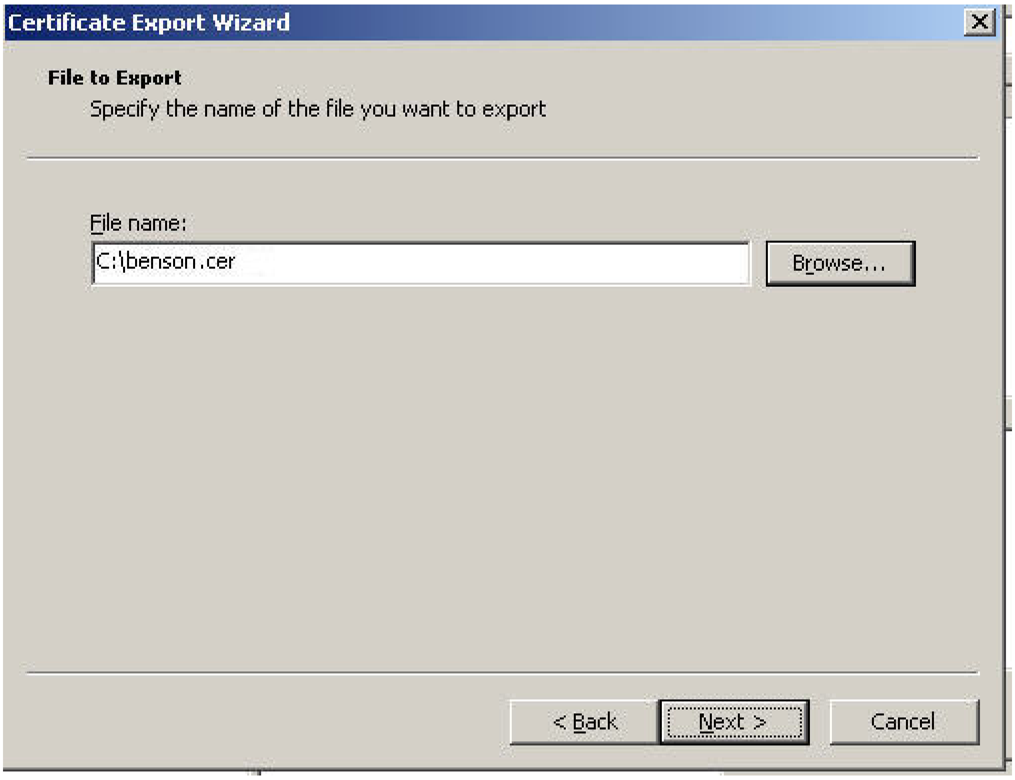
Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

- ● DER encoded binary X.509 (.CER)
- ○ Base-64 encoded X.509 (.CER)
- ○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
  - □ Include all certificates in the certification path if possible
- ○ Personal Information Exchange - PKCS #12 (.PFX)
  - □ Include all certificates in the certification path if possible
  - □ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)
  - □ Delete the private key if the export is successful



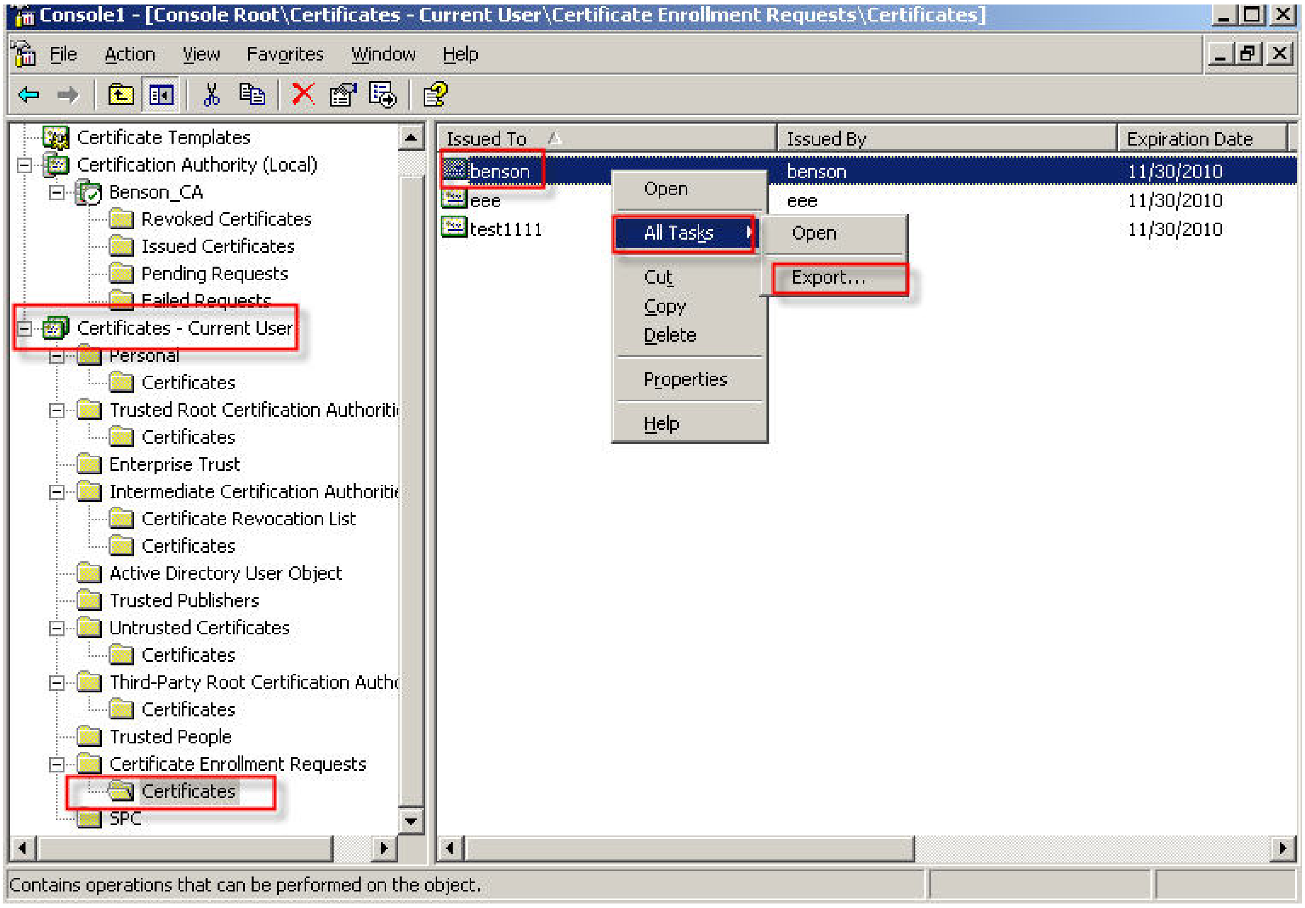
Certificate Export Wizard

File to Export

Specify the name of the file you want to export

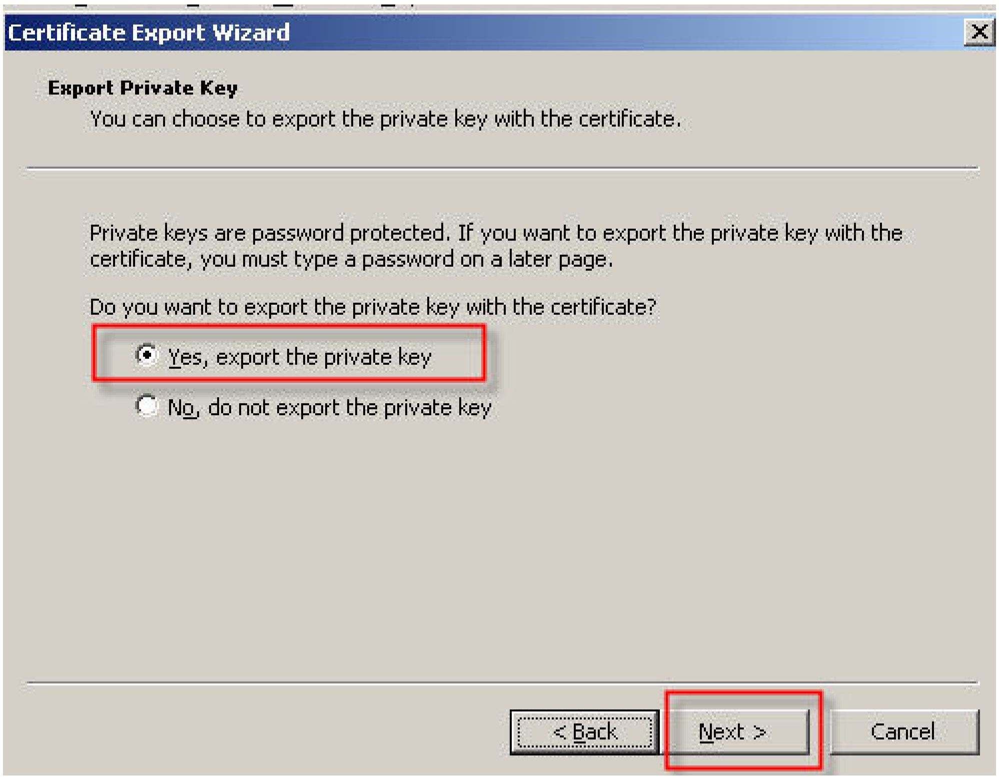
File name: C:\benson.cer

8. Download benson.pfx.


Console1 - [Console Root\Certificates - Current User\Certificate Enrollment Requests\Certificates]
File Action View Favorites Window Help
Certificate Templates
Certification Authority (Local)
Benson_CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificates - Current User
Personal
Certificates
Trusted Root Certification Authoriti
Certificates
Enterprise Trust
Intermediate Certification Authoritie
Certificate Revocation List
Certificates
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Certificates
Third-Party Root Certification Authc
Certificates
Trusted People
Certificate Enrollment Requests
Certificates
SPC
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Export...

Issued To	Issued By	Expiration Date
benson	benson	11/30/2010
eee	eee	11/30/2010
test1111		11/30/2010

Contains operations that can be performed on the object.


Certificate Export Wizard

Export Private Key

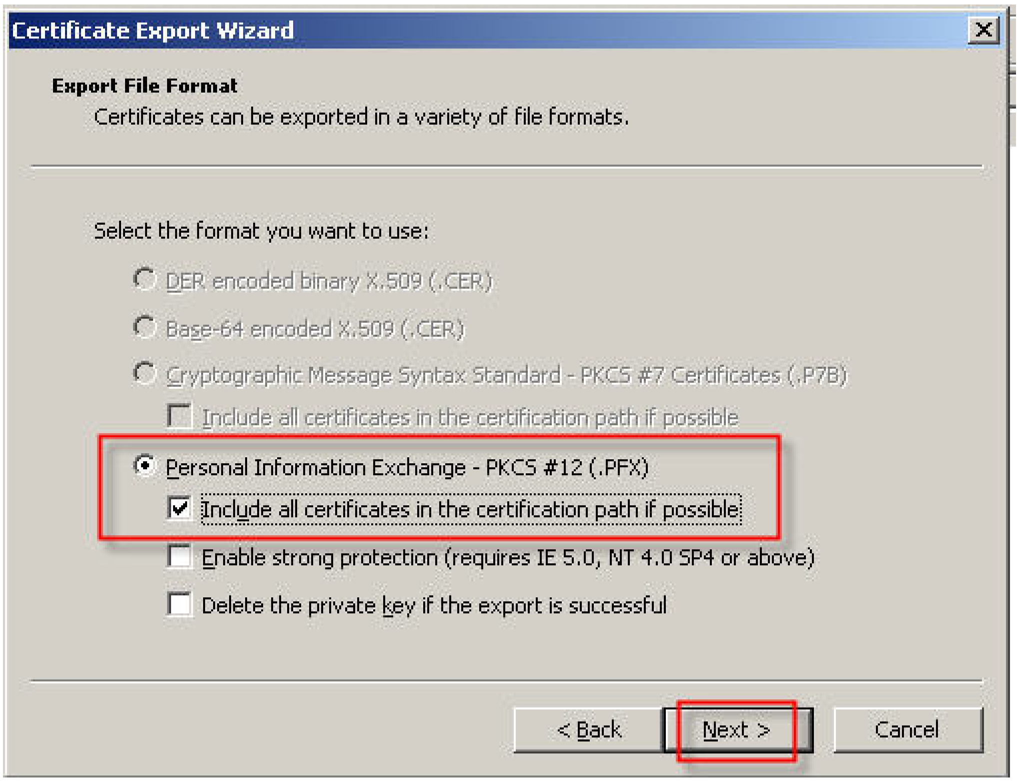
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

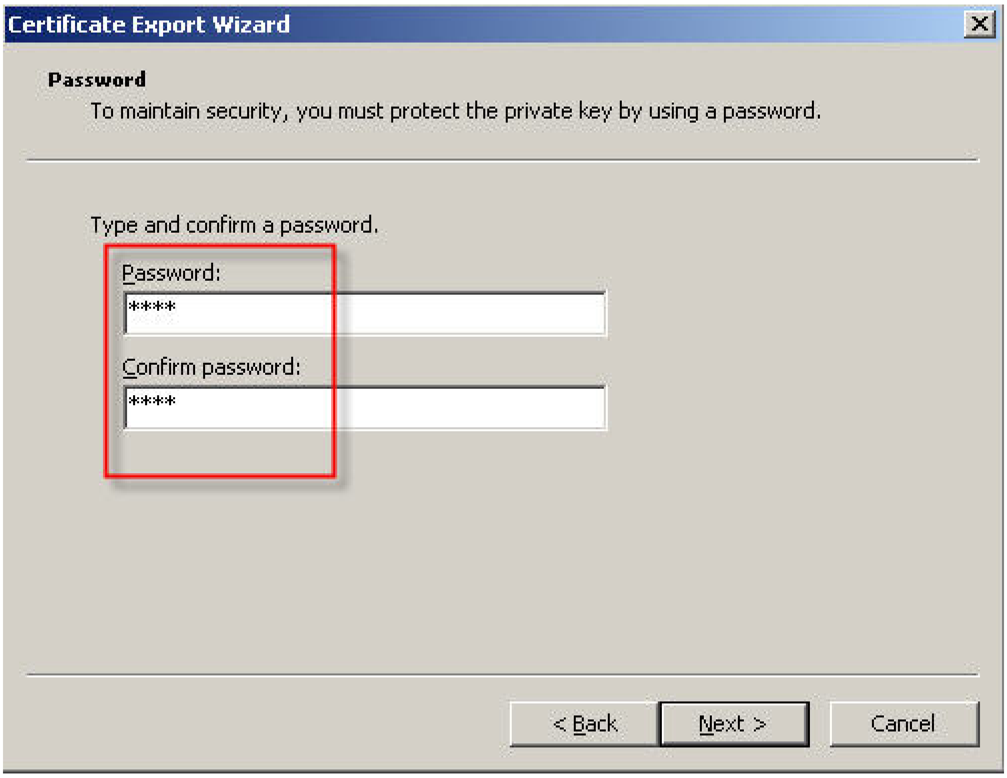
□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

☑ Include all certificates in the certification path if possible

□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

□ Delete the private key if the export is successful



Certificate Export Wizard

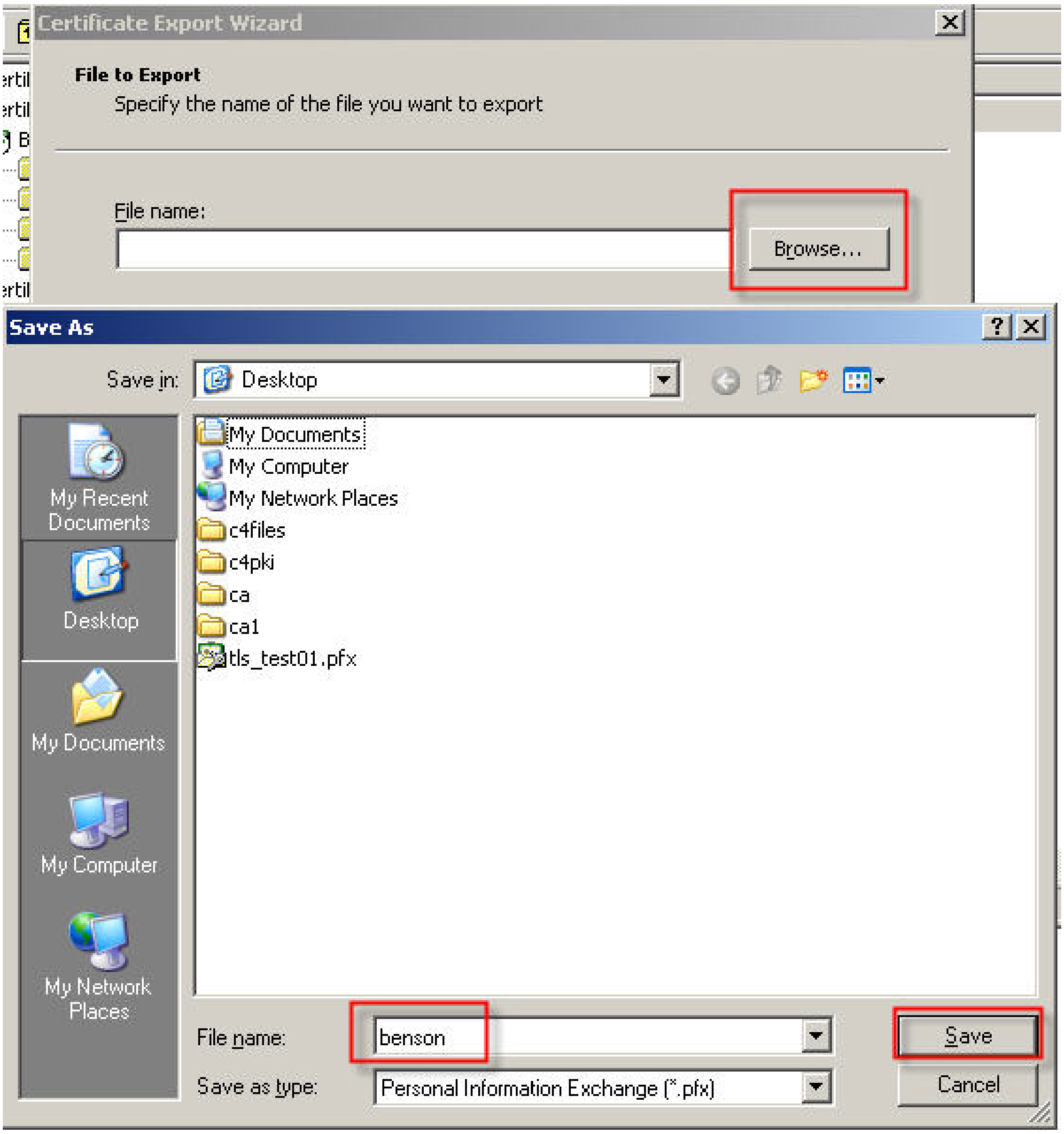
Password

To maintain security, you must protect the private key by using a password.

Type and confirm a password.

Password: ****

Confirm password: ****



Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name:

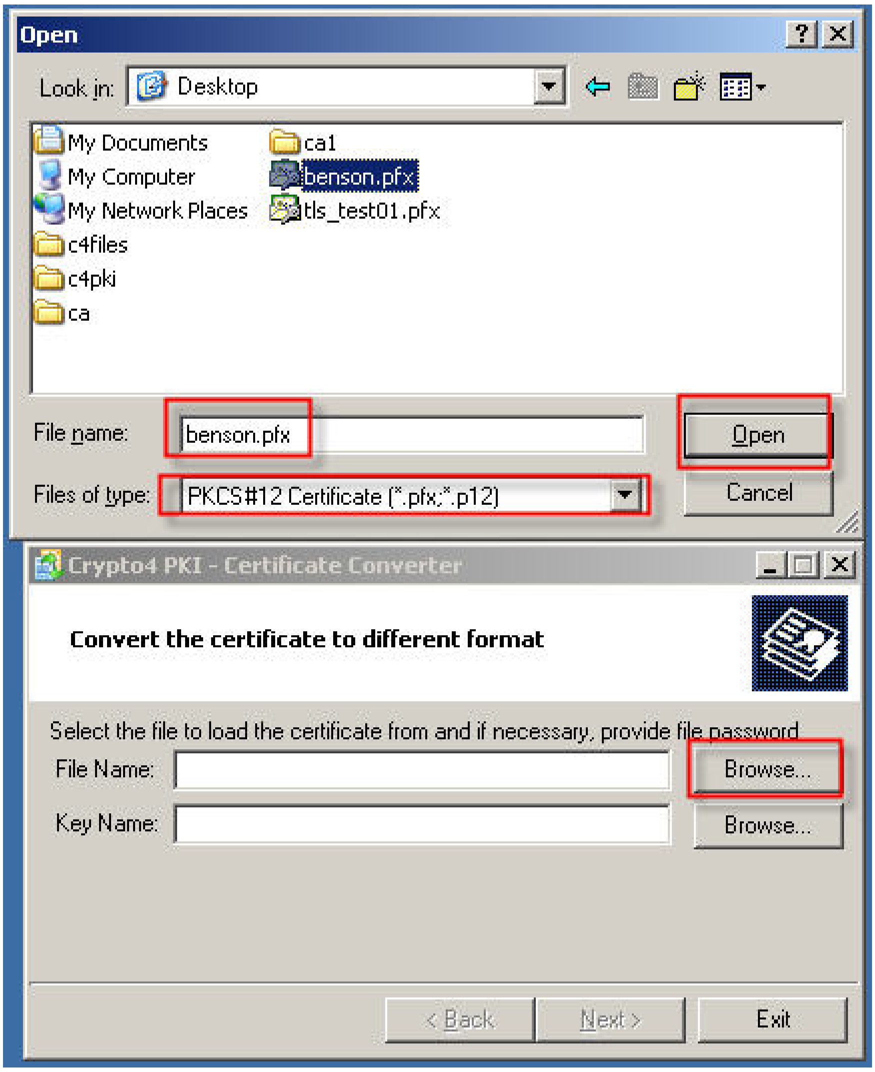
Save As

Save in: Desktop

File name: benson

Save as type: Personal Information Exchange (*.pfx)

9. User Crypto4 convert application to export benson.key(private key).



File name: benson.pfx

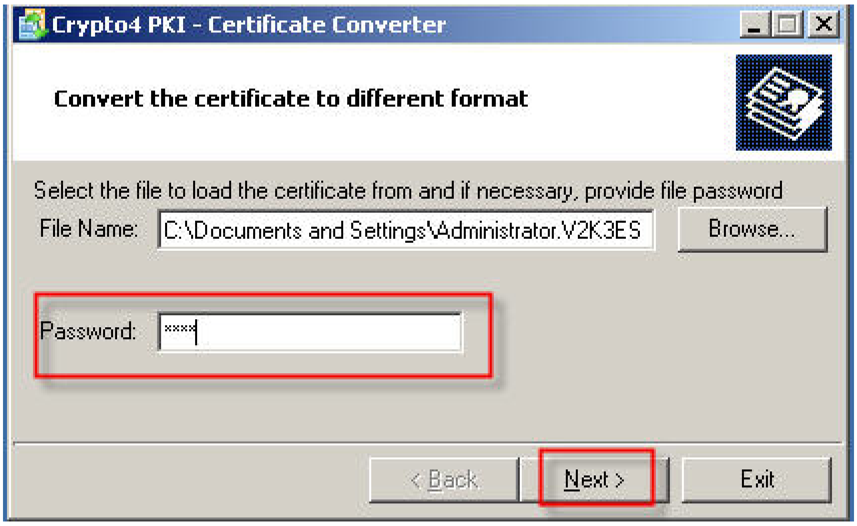
Files of type: PKCS#12 Certificate (*.pfx;*.p12)

Convert the certificate to different format

Select the file to load the certificate from and if necessary, provide file password

File Name:

Key Name:

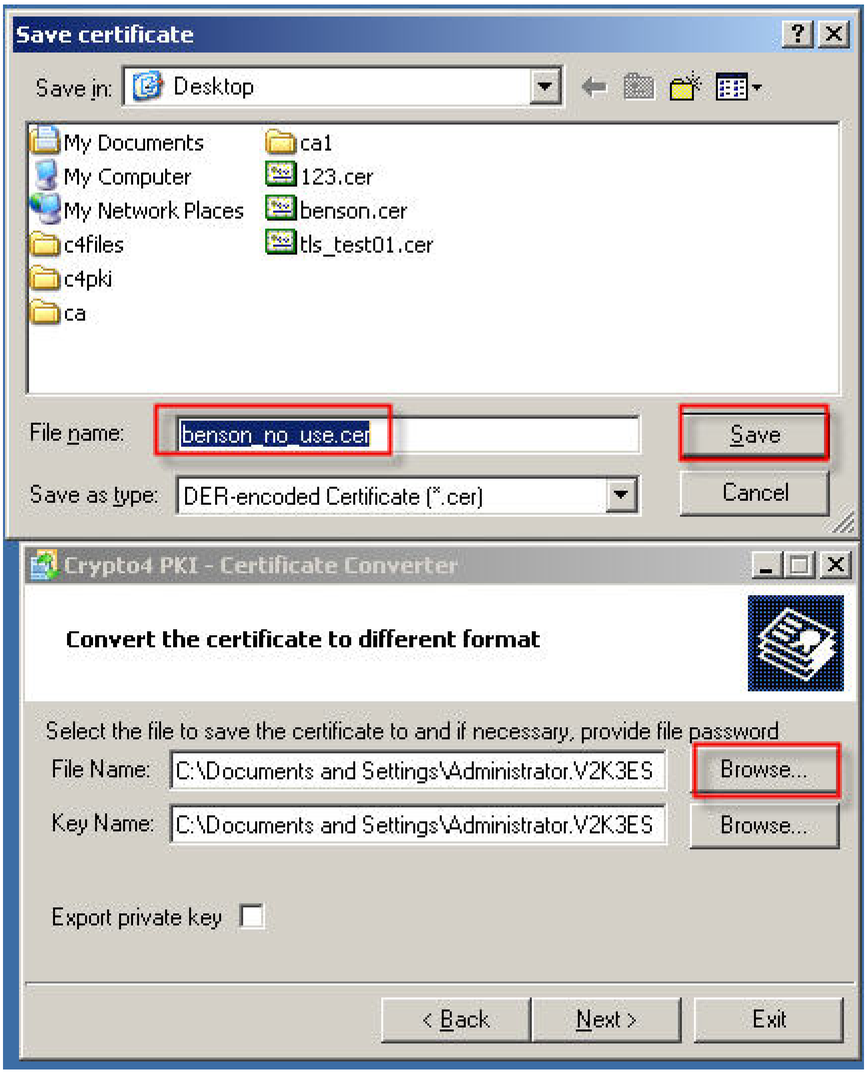


Convert the certificate to different format

Select the file to load the certificate from and if necessary, provide file password

File Name: C:\Documents and Settings\Administrator.V2K3ES

Password: ****



Save certificate

Save in: Desktop

File name: benson_no_use.cer

Save as type: DER-encoded Certificate (*.cer)

Crypto4 PKI - Certificate Converter

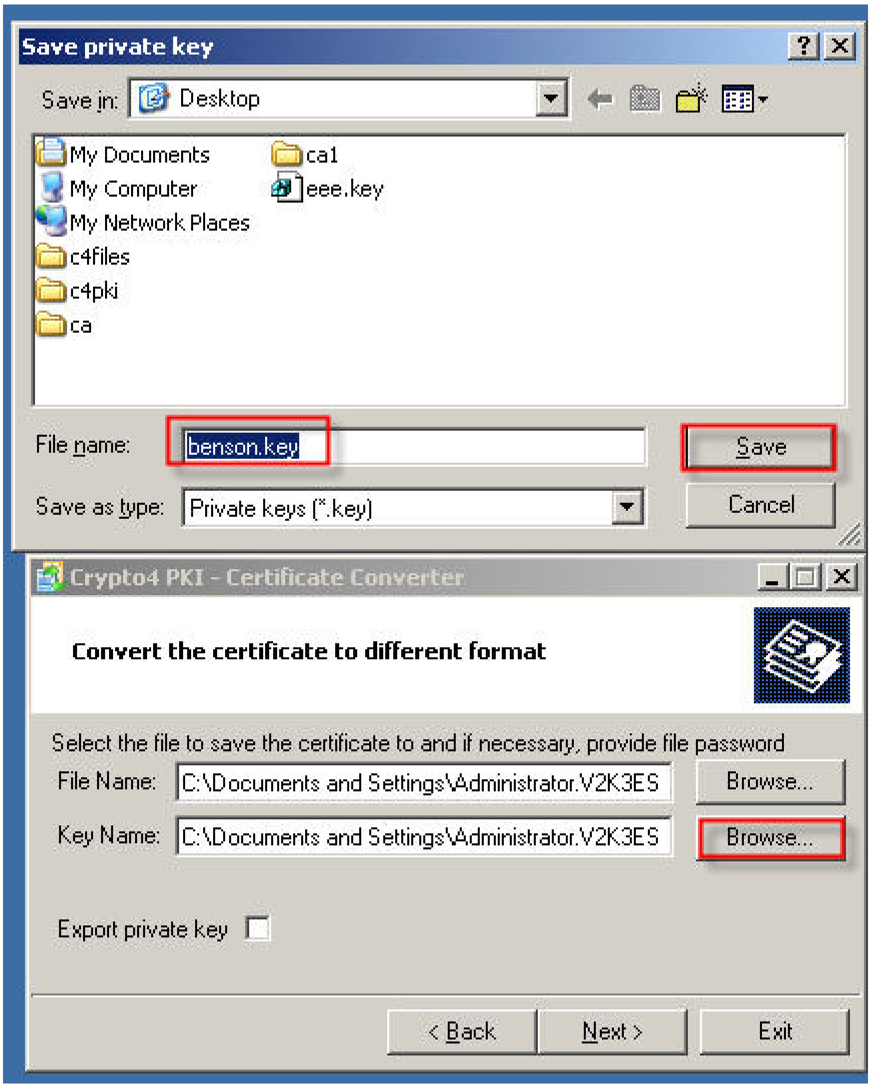
Convert the certificate to different format

Select the file to save the certificate to and if necessary, provide file password

File Name: C:\Documents and Settings\Administrator.V2K3ES

Key Name: C:\Documents and Settings\Administrator.V2K3ES

Export private key □



Save private key

Save in: Desktop

File name: benson.key

Save as type: Private keys (*.key)

Crypto4 PKI - Certificate Converter

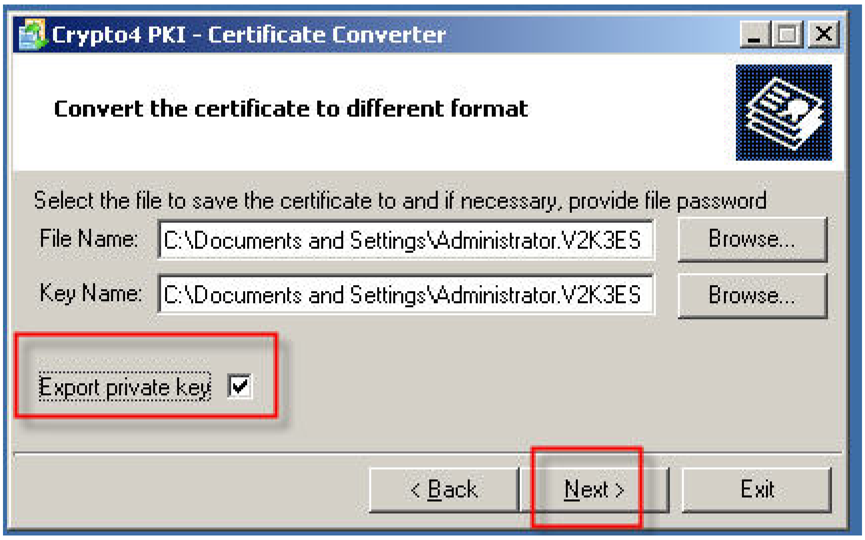
Convert the certificate to different format

Select the file to save the certificate to and if necessary, provide file password

File Name: C:\Documents and Settings\Administrator.V2K3ES

Key Name: C:\Documents and Settings\Administrator.V2K3ES

Export private key □



Crypto4 PKI - Certificate Converter

Convert the certificate to different format

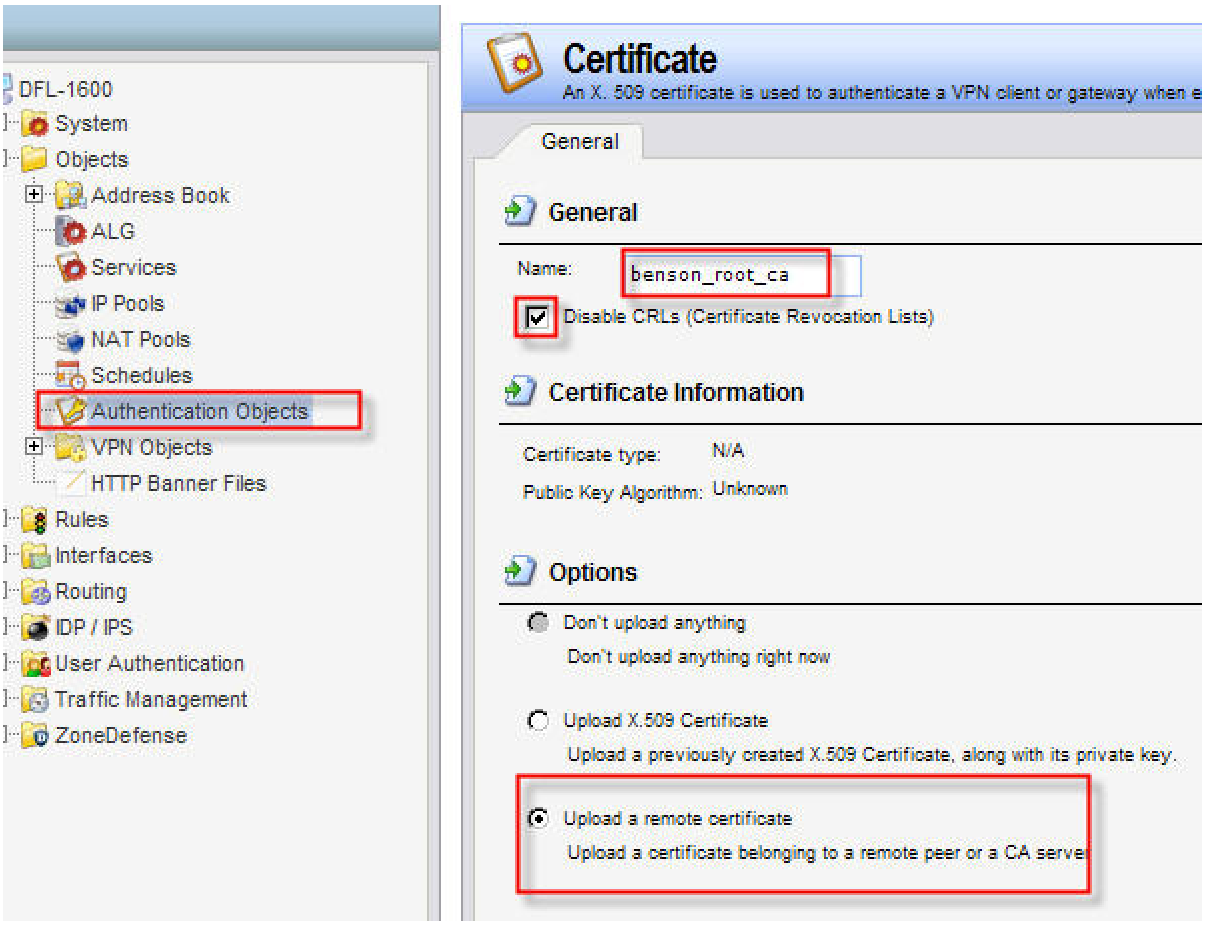
Select the file to save the certificate to and if necessary, provide file password

File Name: C:\Documents and Settings\Administrator.V2K3ES

Key Name: C:\Documents and Settings\Administrator.V2K3ES

Export private key ☑

10. Import Benson_root_ca.cer, benson.cert and benson.key into DFL



Certificate

An X. 509 certificate is used to authenticate a VPN client or gateway when e

General

General

Name: benson_root_ca

☑ Disable CRLs (Certificate Revocation Lists)

Certificate Information

Certificate type: N/A

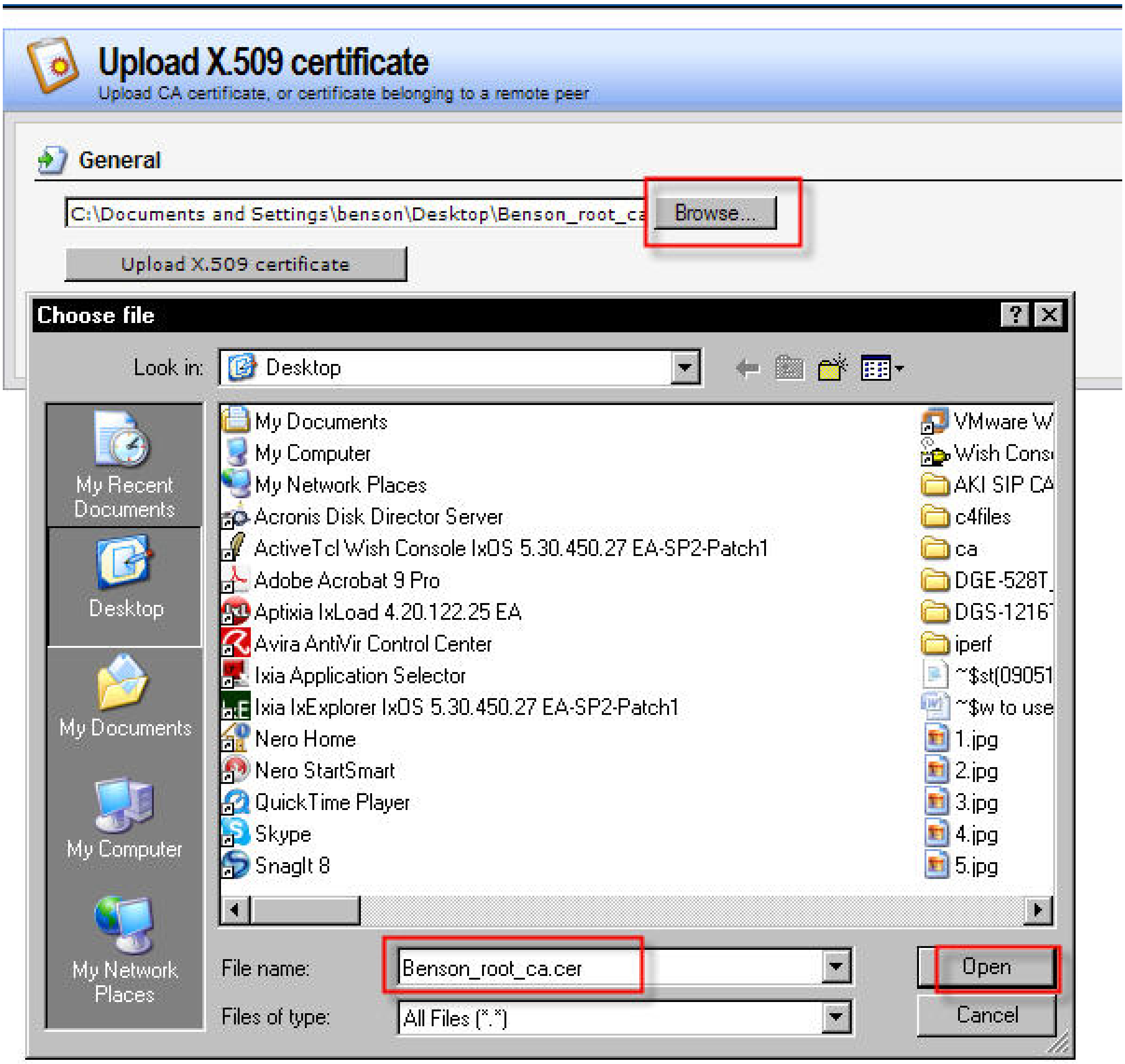
Public Key Algorithm: Unknown

Options

○ Don't upload anything
Don't upload anything right now

○ Upload X.509 Certificate
Upload a previously created X.509 Certificate, along with its private key.

● Upload a remote certificate
Upload a certificate belonging to a remote peer or a CA serve



Upload X.509 certificate

Upload CA certificate, or certificate belonging to a remote peer

General

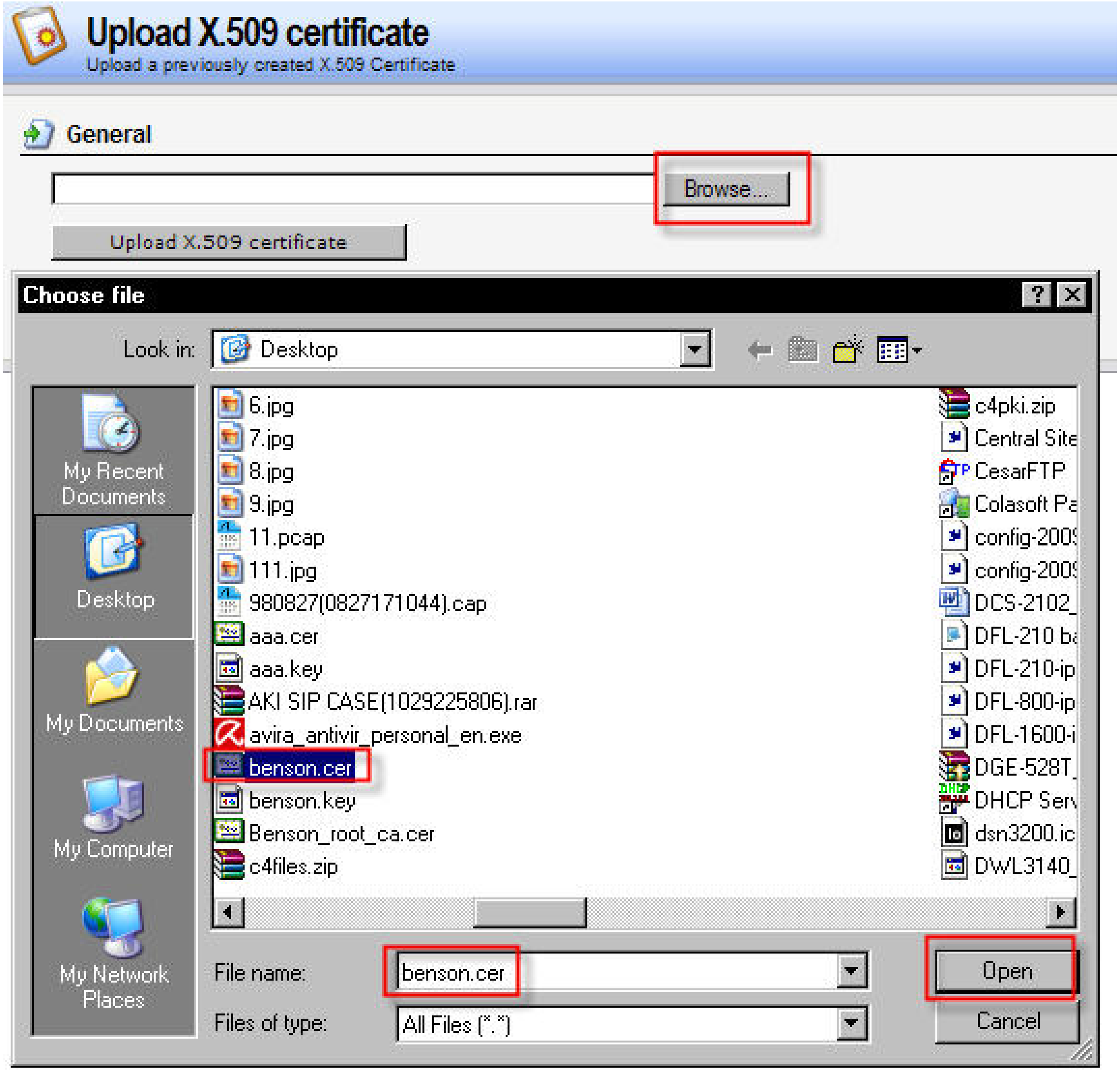
C:\Documents and Settings\benson\Desktop\Benson_root_ca

Choose file

Look in: Desktop

File name: Benson_root_ca.cer

Files of type: All Files (*.*)



Upload X.509 certificate

Upload a previously created X.509 Certificate

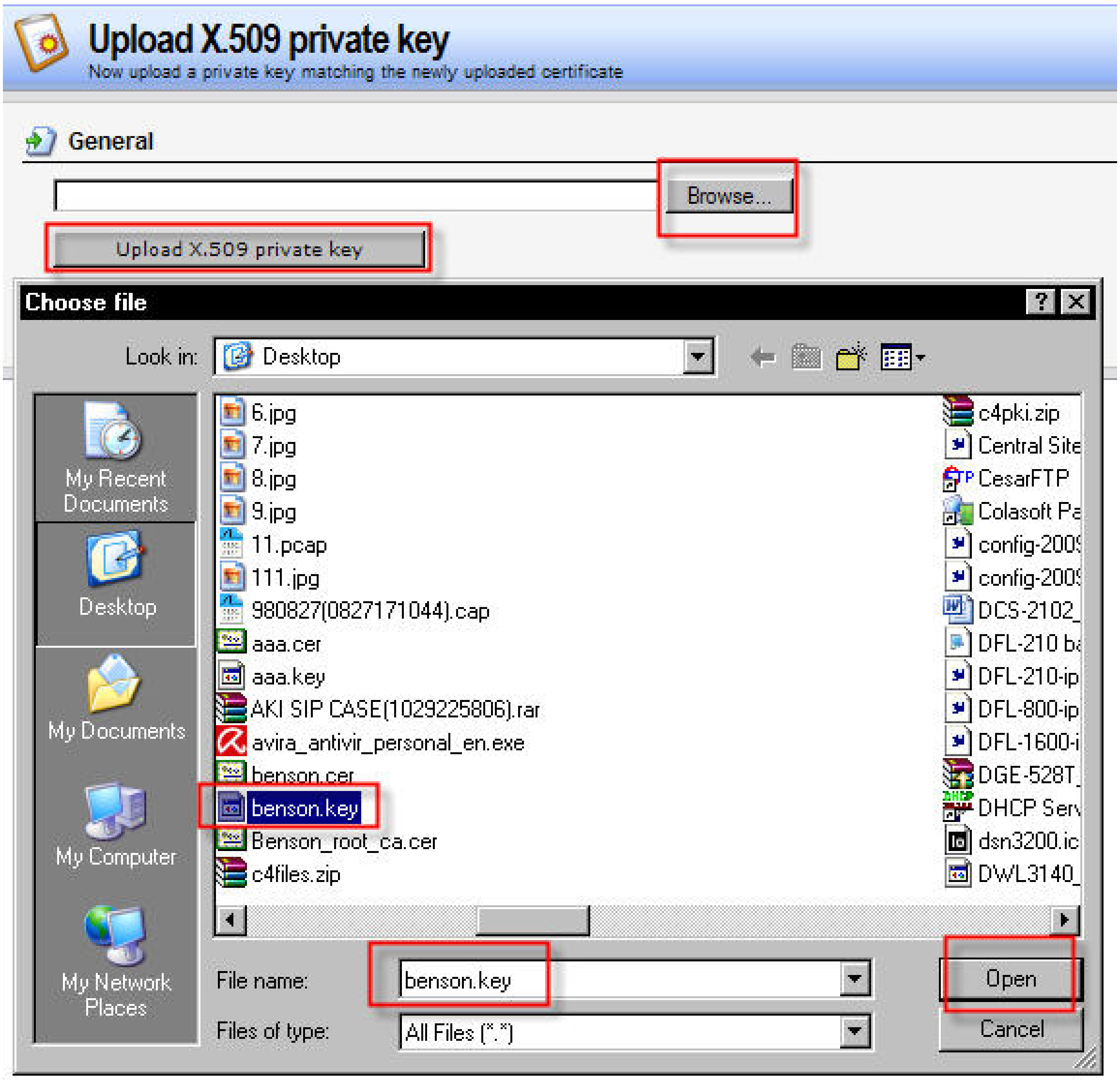
General

Choose file

Look in: Desktop

File name: benson.cer

Files of type: All Files (*.*)



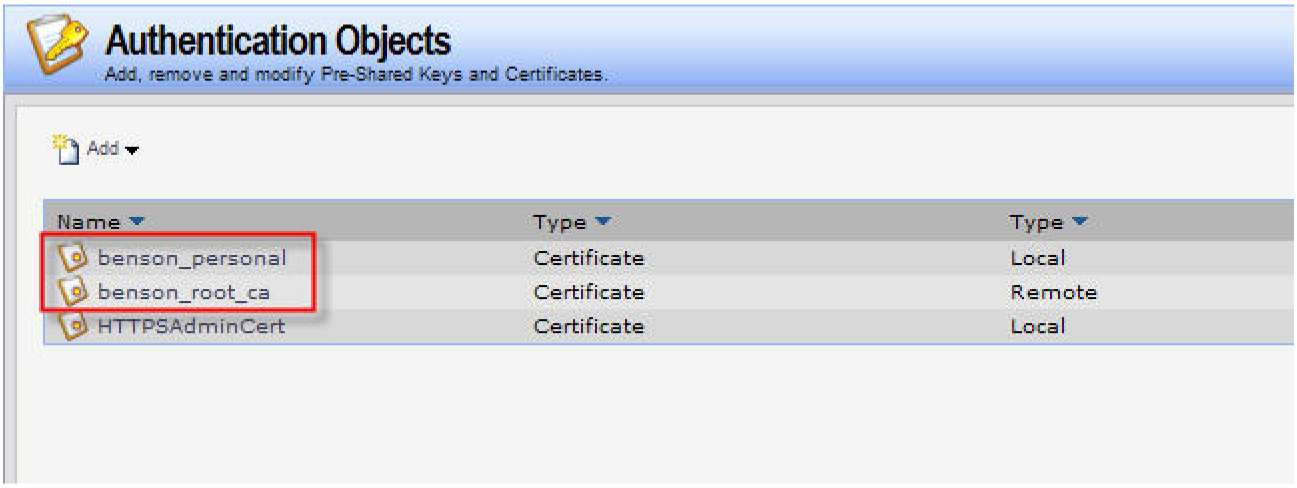
Upload X.509 private key

Now upload a private key matching the newly uploaded certificate

General

File name: benson.key

Files of type: All Files (*.*)

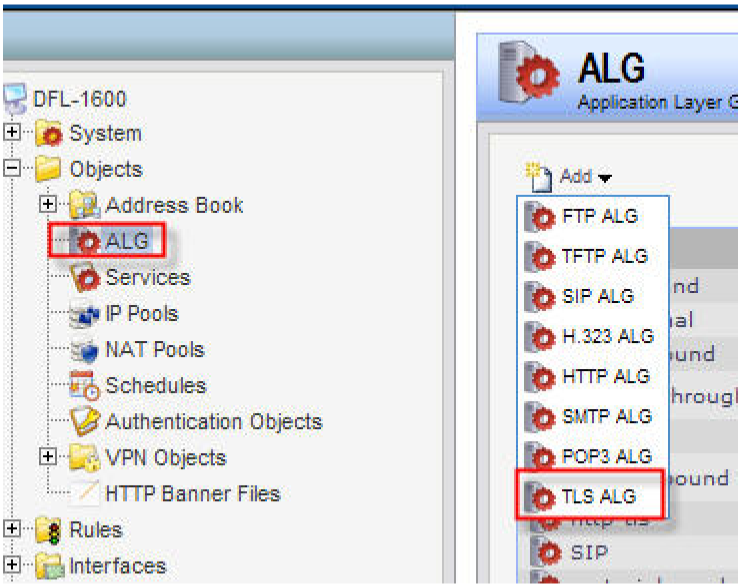


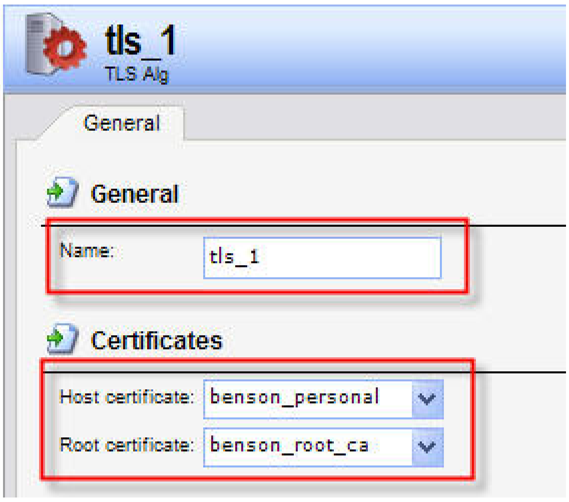
Authentication Objects

Add, remove and modify Pre-Shared Keys and Certificates.

Name	Type	Type
benson_personal	Certificate	Local
benson_root_ca	Certificate	Remote
HTTPSAdminCert	Certificate	Local

11. Add a TLS_ALG.





General

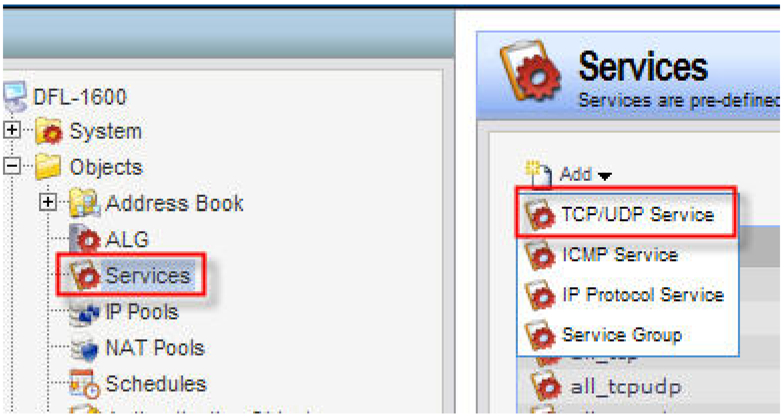
Name: tls_1

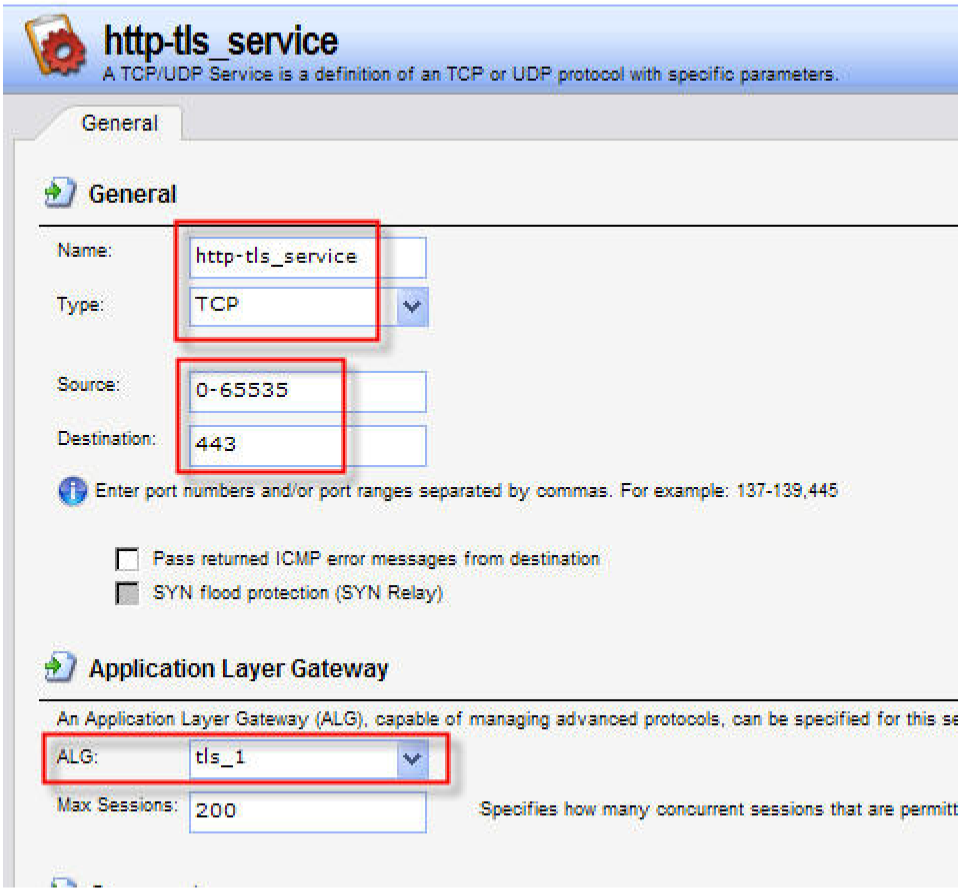
Certificates

Host certificate: benson_personal

Root certificate: benson_root_ca

12. Add a TLS Service.





http-tls_service

A TCP/UDP Service is a definition of an TCP or UDP protocol with specific parameters.

General

Name: http-tls_service

Type: TCP

Source: 0-65535

Destination: 443

Enter port numbers and/or port ranges separated by commas. For example: 137-139,445

□ Pass returned ICMP error messages from destination

□ SYN flood protection (SYN Relay)

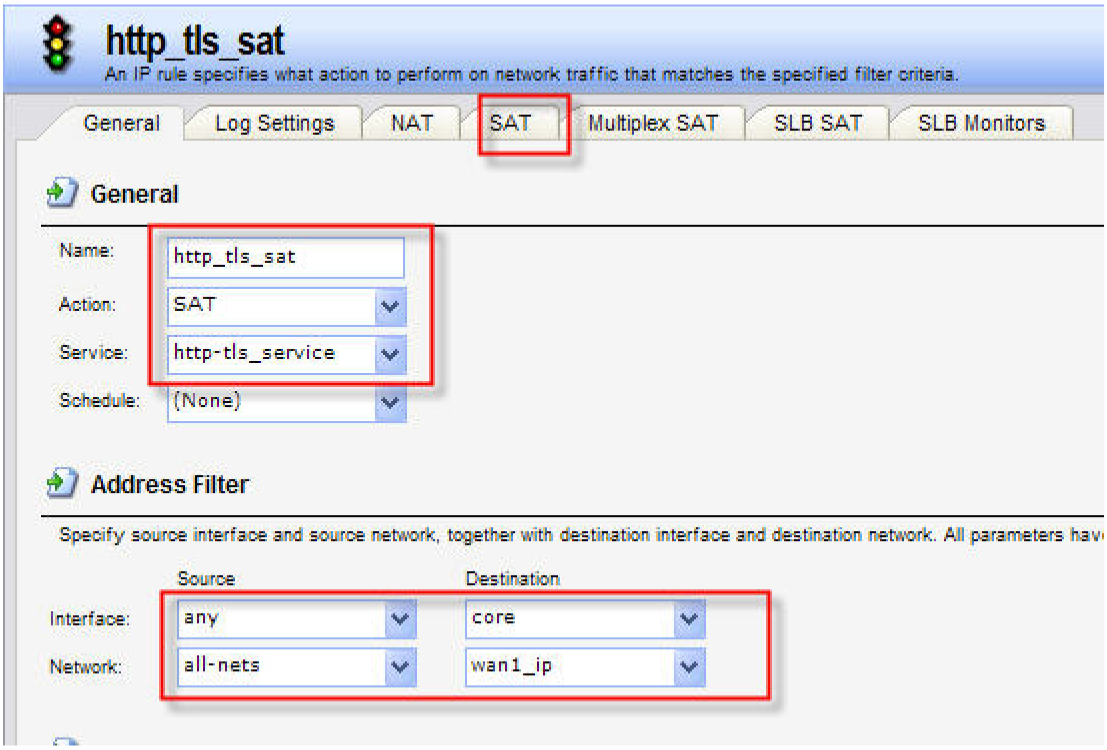
Application Layer Gateway

An Application Layer Gateway (ALG), capable of managing advanced protocols, can be specified for this se

ALG: tls_1

Max Sessions: 200 Specifies how many concurrent sessions that are permitt

13. Add SAT/ALLOW IP-Rules.



http_tls_sat

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General

Name: http_tls_sat

Action: SAT

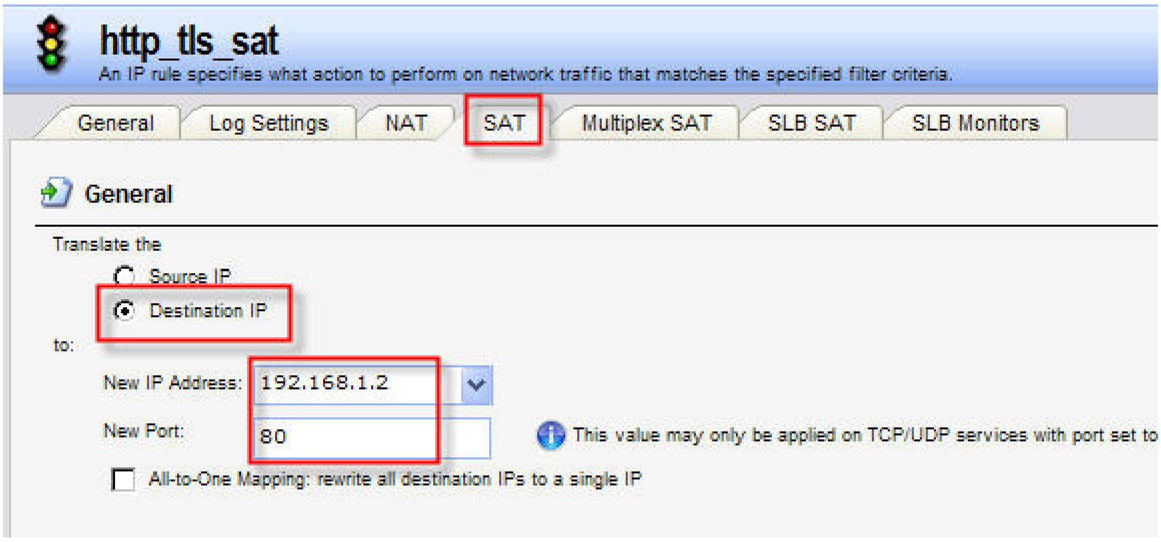
Service: http-tls_service

Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters hav

	Source	Destination
Interface:	any	core
Network:	all-nets	wan1_ip



http_tls_sat

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General

Translate the

○ Source IP

● Destination IP

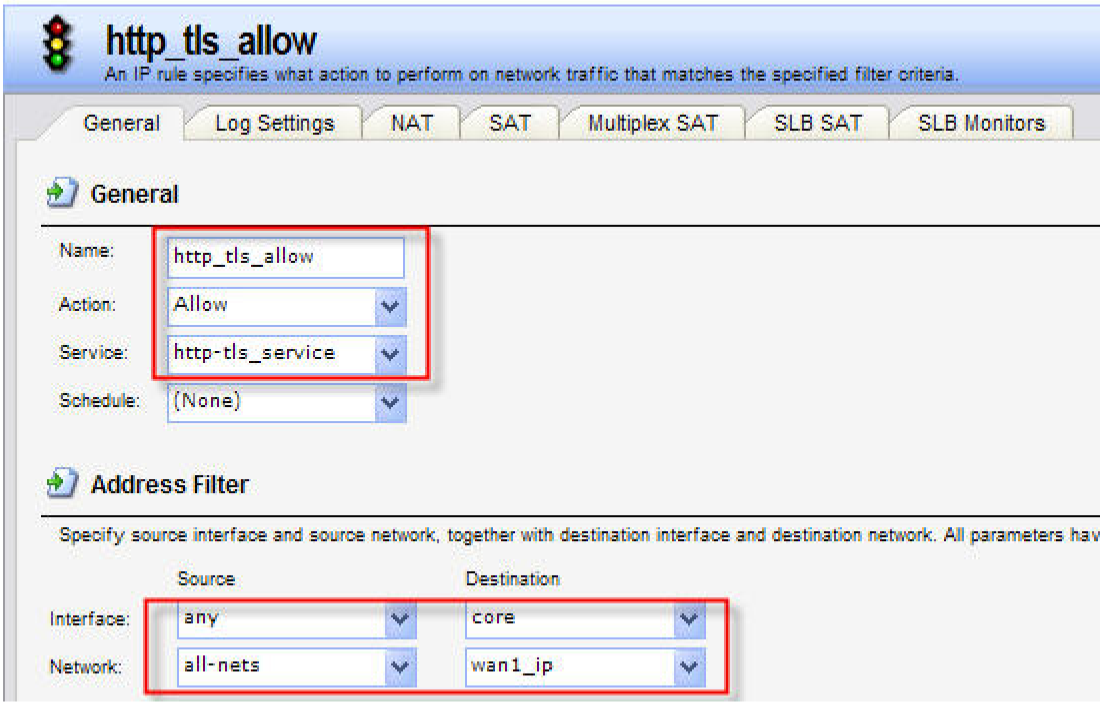
to:

New IP Address: 192.168.1.2

New Port: 80

This value may only be applied on TCP/UDP services with port set to

☐ All-to-One Mapping: rewrite all destination IPs to a single IP



http_tls_allow

An IP rule specifies what action to perform on network traffic that matches the specified filter criteria.

General

Name: http_tls_allow

Action: Allow

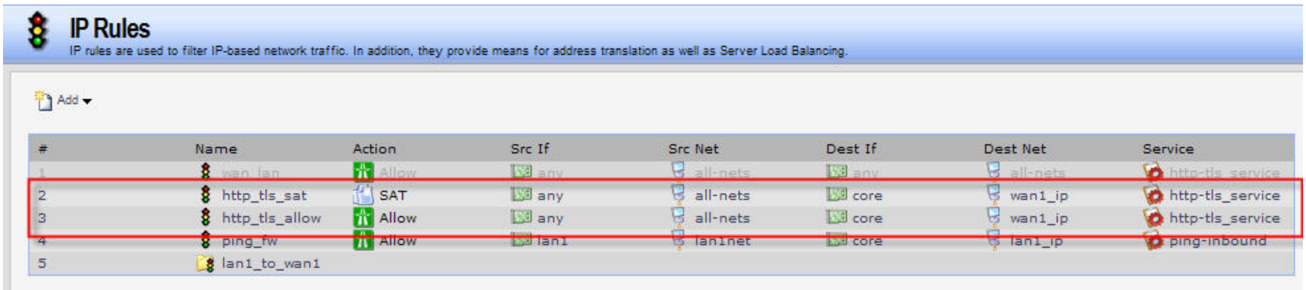
Service: http-tls_service

Schedule: (None)

Address Filter

Specify source interface and source network, together with destination interface and destination network. All parameters hav

	Source	Destination
Interface:	any	core
Network:	all-nets	wan1_ip



IP Rules

IP rules are used to filter IP-based network traffic. In addition, they provide means for address translation as well as Server Load Balancing.

#	Name	Action	Src If	Src Net	Dest If	Dest Net	Service
1	wan_lan	Allow	any	all-nets	any	all-nets	http-tls_service
2	http_tls_sat	SAT	any	all-nets	core	wan1_ip	http-tls_service
3	http_tls_allow	Allow	any	all-nets	core	wan1_ip	http-tls_service
4	ping_fw	Allow	lan1	lan1net	core	lan1_ip	ping-inbound
5	lan1_to_wan1						

14. Use HTTP_Client to connects https://10.1.1.12, if cusses, you can see HTTP_Server web information.