To replace the HTTP certification for DFL firewall

## [Topology]

PC-----(lan1)DFL

CA/DNS server--/

# 

PC IP address: 192.168.1.58 PC DNS address: 192.168.1.200

### 

## [Key points]

- 1. DFL needs to be installed a self-certification(including private and public key)
- 2. PC needs to be installed the CA-certification(Public key only) in the "Trusted certification authorities"
  - 1. Build up a windows CA server. (Brief installation)
    - a. Install DNS server
    - b. Issue the command of "dcpromo".
    - c. Install IIS
    - d. Install CA server
    - e. Create a CA template, name the template and allow its private key is exportable.

🙀 Certificate Templates	Template Display Name 🔺		Minimum Supp	oorted CAs	Version	Autoenrollment	
	Directory Email Replication		Windows Ser	ver 2003, En	115.0	Allowed	
	Domain Controller		Windows 200	0	4.1	Not allowed	
	Domain Controller Authentication		Windows Ser	ver 2003, En	110.0	Allowed	
	EFS Recovery Agent		Windows 200	0	6.1	Not allowed	
	Enrollment Agent		Windows 200	0	4.1	Not allowed	
	Enrollment Agent (Computer)		Windows 200	0	5.1	Not allowed	
	Exchange Enrollment Agent (Offline re	equest)	Windows 200	0	4.1	Not allowed	
	Exchange Signature Only		Windows 200	0	6.1	Not allowed	
	Exchange User		Windows 200	0	7.1	Not allowed	
	IPSec		Windows 200	0	8.1	Not allowed	
	IPSec (Offline request)		Windows 200	0	7.1	Not allowed	
	Key Recovery Agent		Windows Ser	ver 2003, En	105.0	Allowed	
	RAS and IAS Server		Windows Ser	ver 2003, En	101.0	Allowed	
	Root Certification Authority		Windows 200	0	5.1	Not allowed	
	Router (Offline request)		Windows 200	0	4.1	Not allowed	
	Smartcard Logon		Windows 200	0	6.1	Not allowed	
	Smartcard User		Windows 200	0	11.1	Not allowed	
	Subordinate Certification Authority		Windows 200	0	5.1	Not allowed	
	Trust List Signing		Windows 200	0	3.1	Not allowed	
	User		Windows 200	0	3.1	Not allowed	
	User Signature Only		Windows 200	0	4.1	Not allowed	
	💑 Web Server	Duplicate	Template	)	4.1	Not allowed	
	Workstation Authentication —			er 2003, En	101.0	Allowed	
	For-Web	All Tas <u>k</u> s	<u> </u>	er 2003, En	100.2	Not allowed	
		Propert	ies				
art 🛛 🚱 🥥 🛛	My Network Places 🛛 👸 Add or Remc	Help		Ma • 🖉 M	icrosoft Ce	rtifica 📔 🍓 🛃 🔮	11:21

For-Web Properties		? >			
Issuance Requirements General	Superseded Templates Request Handling	Extensions Security Subject Name			
Template display name: For-Web					
Minimum Supported CAs	Minimum Supported CAs: Windows Server 2003, Enterprise Edition				
Iemplate name: For-Web					
⊻alidity period:	<u>R</u> enewal period	×			
Publish certificate in Active Directory           Do not automatically reenroll if a duplicate certificate exists in Active Directory					
	ОК С	ancel <u>Apply</u>			

Issuance Require General	ements   Superseded Templates   Extensions   Security Request Handling   Subject Name			
<u>P</u> urpose:	Signature and encryption			
	Archive subject's encryption private key			
	Include symmetric algorithms allowed by the subject			
	Delete revoked or expired certificates (do not archive)			
Minimum keu siz	re: 1024 💌			
	1024			
Allow private	e key to be exported			
So the following when the subject is enrolled and when the private key associated with this certificate is used:     Enroll subject without requiring any user input				
Enroll subject     Prompt the u	this certificate is used: at without requiring any user input user during enrollment			
Enrol subject     Prompt the u     private key i	this certificate is used: at without requiring any user input user during enrollment user during enrollment and require user input when the is used			
<ul> <li>Enroll subject</li> <li>Prompt the c</li> <li>Prompt the c</li> <li>Prompt the c</li> <li>private key i</li> <li>To choose whic (CSPs) should b</li> </ul>	this certificate is used: at without requiring any user input user during enrollment gser during enrollment and require user input when the is used th cryptographic service providers re used, click CSPs.			
Enrol subject     Enrol subject     Prompt the <u>u</u> Prompt the <u>u</u> private key i     To choose whice     (CSPs) should b	this certificate is used: at without requiring any user input user during enrollment user during enrollment and require user input when the is used th cryptographic service providers is used, click CSPs. OK Cancel Apply			

For-Web Properties		? ×
General Request Handling Issuance Requirements Superseded Templates	S s   Exte	Subject Name
Group or user names:		
Administrator (TSD\Administrator)		
Authenticated Users		
Domain Admins (TSD\Domain Admins)		
Enterprise Admins (150 \Enterprise Admins)		
Ag	įd	<u>R</u> emove
Permissions for Administrator	Allow	Deny
Full Control		
Read		
Write		
Enroll		
Enroll Autoenroll	$\mathbf{\nabla}$	
Enroll Autoenroll	V V	
Enroll Autoenroll For special permissions or for advanced settings, click Advanced.		Advanced

f. Publish the CA template(For-Web) created at step "e".



- 2. To apply a self-certification and download the CA server's certification.
  - a. Connect to the web certificate service of CA server and request a certificate.

Address 🙆 http://srv4.tsd.local/certsrv/	💌 🔁 Go	Links
<i>Microsoft</i> Certificate Services summer	H	ome

### 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 Certificate Services, see 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

b. Go to "advanced certificate request"

Microsoft Certificate Services -- summer

### Request a Certificate

Select the certificate type: User Certificate

Or, submit an advanced certificate request

### <u>Home</u>

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.

Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

Micros	oft Certifi	cate Services summer	r		
Advan	iced Ce	rtificate Request			
Aurun					
Certifica	ate Temp	olate:			
		For-Web	•		
ldentifyi	ing Infor	mation For Offline Tem	plate:	This name must be the same	
	Name:	summer.tsd.local		must be able to resolution by	
	E-Mail:	summer@tsd.local		certification will be recognized as	
С	ompany:	d-link		non-trusted certification on client's browser.	
Dep	partment:	tsd			
	City:	taipei			
	State:	tw			
Country	//Region:	TW			
Key Opt	tions:				
			O Use existing key se	et	
	CSP:	Microsoft RSA SChanne	el Cryptographic Provider	•	
Ke	y Usage:	Exchange			
k	Key Size: 1024 Min: 1024 (common key sizes: <u>1024 2048 4096 8192 16384</u> )				
	Automatic key container name O User specified key container name				
	Mark keys as exportable				
		Export Reys to in	key protection		
		Store certificate in the	e local computer certifica	ate store	
		Stores the certificate	e in the local computer s	tore	
		instead of in the use install the root CA's	ers centificate store. Doe certificate. You must be	s not • an	
		administrator to gen machine_store	erate or use a key in the	local	
		indennike etere.			
Addition	nal Optio	ins:			
Request	t Format:	●CMC OPKCS	10		
Hash A	lgorithm:	SHA-1			
		Uniy used to sign reques	67.		
		Save request to a file			
А	ttributes:		×		
		1	Þ		
Friend	ly Name:				
				Submit >	
				Subline 2	

c. Export the self-certification.

Console Root	Issued To 🔺	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Tem.	
🖻 🐻 Certificates - Current User	🕮 Administrator	Administrator	7/27/2014	File Recovery	<none></none>			
🖻 ··· 🦲 Personal	🔤 summer	summer	8/5/2013	Server Authentication	<none></none>		For-Web	
Certificates	summer.tsd.local	summer	8/5/2013	Server Authentication	<nono></nono>		For-Web	
	E test	summer	8/4/2013	Server Authentication	Open		For-Web	
Enterprise Trust	I				All Tacks	Open		
Intermediate Certification Aut	1					Open		
🕀 📃 Active Directory User Object	1				Cut	Reques	st Certificate with	New Key
🕀 📄 Trusted Publishers	1				Conv	Reques	st Certificate with	Same Key
🕀 📄 Untrusted Certificates	1				Delete	Denew	Certificate with N	lew Key
Initial Party Root Certification	1				Delete	Denew	Cartificate with C	ama Kau
🗄 💼 Trusted People	1				Properties	Renew	Certificate with 5	allie Key
🖻 🔯 Certification Authority (Local)	1			-		Export		
E 😨 summer	1				Help			
				_				

Certificate Export Wizard		×			
	Welcome to the Certificate Expo Wizard         This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.         A certificate, which is issued by a certification authority a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area whe certificates are kept.         To continue, click Next.	rt , is 1 re			
11	< <u>B</u> ack Next > Ca	ncel			
Contificato Europet Wizard					
Private keys are password p certificate, you must type a Do you want to export the Yes, export the priv No, do not export t	protected. If you want to export the private key with the a password on a later page. private key with the certificate? vate key the private key				
	< <u>B</u> ack <u>N</u> ext > Car	ncel			
Certificate Export Wizard File to Export Specify the name of the file	tificate Export Wizard       X         File to Export       Specify the name of the file you want to export				
Eile name:	gs\Administrator\Desktop\personal-summ Browse				



Certificate Export Wizard		×
	Completing the Certificate E Wizard You have successfully completed the Certificate wizard. You have specified the following settings:	Export
	File Name Export Keys Include all certificates in the certification path File Format	C:\Doc Yes Yes Person
	< <u>B</u> ack Finish	Cancel

d. The self-certification exports from Microsoft windows will be the format of "PFX", we have to convert the file to the format of x.509 by the tool of "CryptTo4"



🚳 Crypto4 Pk	I - Certificate Converter		
Convert th	ne certificate to different format		
Select the file	to load the certificate from and if necessary, provide file password		
File Name: (	C:\Users\summer\Desktop\cert\personal-summer4 Browse		
Password:	сххм		
	< <u>B</u> ack <u>Next</u> > Exit		
🚳 Crypto4 PK	I - Certificate Converter		
Convert the certificate to different format			
Select the file t	o save the certificate to and if necessary, provide file password		
File Name: C	:\Users\summer\Desktop\cert\personal-4-public. Browse		
Key Name: C	:\Users\summer\Desktop\cert\personal-4-pri.key Browse		
Export private	key 🔽		
< <u>B</u> ack <u>N</u> ext > Exit			



e. Upload the self-certification to DFL.

An X. 509 certificate is used to authenticate a VPN client or gateway when establishing an IPsec tunnel.
General
🔊 General
Name: for-web4 Disable CRLs (Certificate Revocation Lists)
2 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 server



	-
	4

Network

🗟 lan1net

Interface

🔝 lan1

### 射 General

General

 $\gg$ 

**Remote Management Settings** 

Setup and configure methods and permissions for remote management of this system.

SSH Before Rules:		Enable SSH traffic to the security gateway regardless of configured IP Rules.
WebUI Before Rules:		Enable HTTP(S) traffic to the security gateway regardless of configured IP Rules.
WebUI Idle timeout:	900	Number of seconds of inactivity until the HTTP(S) session is closed.
Local Console Timeout:	900	Number of seconds of inactivity until the local console user is automatically logged out.
Validation Timeout:	30	Specifies the amount of seconds to wait for the administrator to log in before reverting to the previous configuration.
WebUI HTTP port:	80	Specifies the HTTP port for the web user interface.
WebUI HTTPS port:	443	Specifies the HTTP(S) port for the web user interface.
HTTPS Certificate:	for-web4 🗸	Specifies which certificate to use for HTTPS traffic. Only RSA certificates are supported.
NMP		

🌏 Home	🔀 Configuration	-
	Save and Activate	
UFL-2560G	View Changes	

f. On the DNS server, make sure the DNS resolution is work without problem.

Console1 - [Console Root\DNS\SRV4\Forward Lookup Zones\tsd.local]					
📸 Eile Action View Favorites Window Help					
Console Root	Name	Туре	Data		
Certificate Templates	🔁 _msdcs				
🕀 👹 Certificates - Current Use					
⊕  ⊕	🗀 _tcp				
⊡-, A DNS					
E-SRV4	DomainDnsZones				
	ForestDnsZones				
Porward Lookup 2	🗒 (same as parent folder)	Start of Authority (SOA)	[22], srv4.tsd.local., hostm		
	🗒 (same as parent folder)	Name Server (NS)	srv4.tsd.local.		
+ The test.com	🗐 (same as parent folder)	Host (A)	192.168.1.200		
tsd.local	🗒 dfl	Host (A)	192.168.1.1		
	Srv4	Host (A)	192.168.1.200		
⊕ 🛄 _sites	summer	Host (A)	192.168.1.1		
🕀 🕀 庄 😥					
主 🛄 _udp					
🗄 🛄 DomainDr					
🕂 🖃 ForestDn					

g. PC downloads CA server's certification, and install it into "trusted root certification authorities".







Certificate	
General Details Certification Path	
Certificate Information	
This certificate is intended for the following purpose(s): • All issuance policies • All application policies	
Issued to: summer	
Valid from 04/ 08/ 2011 to 04/ 08/ 2016	
Install Certificate Issuer Statement	
ОК	
Certificate Import Wizard	
Welcome to the Certificate Imp Wizard	ort
This wizard helps you copy certificates, certificate lists, and certificate revocation lists from your disk certificate store.	trust to a
A certificate, which is issued by a certification aut a confirmation of your identity and contains inform used to protect data or to establish secure netwo	hority nation rk

connections. A	certificate	store is	the system	area where
certificates are	e kept.			

x

is

To continue, click Next.

 < Back	Next >	Cancel

Certificate Import Wizard
Certificate Store Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for the certificate.
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store Certificate store:
Trusted Root Certification Authorities Browse
Learn more about <u>certificate stores</u>
< Back Next > Cancel

h. Now, double check the DNS settings of PC is set correctly, then connect to DFL via domain name (summer.tsd.local).

🧀 Authentication Required - Windows Internet Explorer					
O ⊂  Phttps://summer.tsd.local		🔒 🗟 😽 🗙			
File Edit View Favorites Tools H	l <mark>p</mark>				
🖕 Favorites 🛛 👍 🙋 Get More Add-ons 🔻 🔊 Lanner eRMA 🞇 News.com.au Top stories 🏈 Suggested Sites 🔻 🔊 POSITION=MIDDLE1 🛂 Google 🖉 Free Hotmail					
🗄 👻 🚼 Google	D-Link Firewall 2.27.03 🏀 Microsoft Certificate Servi 🏈 Authentication Required 🗙	👌 🔻 🔊			

Authentication Required		
Please enter	your username and password.	
Username:		
Password:		
Language:	English 💌	
	Login	
Supported v Firefox 3+, C Chrome 4+.	<b>/eb browsers:</b> )pera 10.5+, Safari 3+, Internet Explorer 7+ an	nd

Authentication Required - Windows Internet Explorer	Complete and the Dig was high characteristics
https://summer.tsd.local/	
File Edit View Favorites Tools 📥elp	
🖕 Favorites 🛛 👍 🔊 Get More Add-ons 🔻 🖉 Lanner eRMA 🎆 News.com.au Top stor	ries 🏈 Suggested Sites 👻 🔊 POSITION=MIDDLE1 🔧 Google 🍃 Free Hotmail
🔠 🔹 🛃 Google 😈 D-Link Firewall 2.27.03 🏼 🏈 Microsoft Cer	tificate Servi 🏈 Authentication Required 🗴 👌 🔻
Certificate         General       Details       Certification Path         Image: Certificate Information         This certificate is intended for the following purpose(s):         • Ensures the identity of a remote computer         Need to be identical, otherwise the certification will be treated as non-trust.         Issued to:       summer.tsd.local         Issued by:       summer         Valid from       05/       08/       2011         Issuer Statement         Learn more about certificates	Authentication Required         Please enter your username and password.         Username:         Password:         Language:       English         Login         Duported web browsers:         Firefox 3+, Opera 10.5+, Safari 3+, Internet Explorer 7+ and Chrome 4+.

End of document.

Author: Summer Chang. 2011/08/05