杨逢君 2010-01-14 发表

## S5800交换机SSL应用举例-HTTPS配置

一、 组网需求: 无特殊组网需求,只是通过HTTPS以实现对S5800交换机的Web管理。 二、 组网图: 无特殊组网。 三、 配置步骤: 这里使用微软Windows Server 2003作为证书服务器, S5800通过SCEP (Simple Cert ificate Enrollment Protocol,简单证书注册协议)申请并获取证书。 3.1 配置证书服务器 本节介绍Windows Server 2003 CA服务的安装与配置,以及SCEP插件的安装与配置 ,为此,请事先准备好Windows Server 2003系统安装盘,以及SCEP插件(可从微 软网站下载,名为cepsetup.exe)。 注意! 微软SCEP插件的运行依赖IIS服务, 请安装并运行IIS! 3.1.1 安装与配置Windows Server 2003 CA 1) 以管理员身份登录系统。或者,如果您装有 Active Directory,则以域管理员身份 登录到系统。 2) 单击"开始",指向"设置",然后单击"控制面板"。 3) 双击"添加/删除程序"并单击"添加/删除 Windows 组件"。 4) 在"Windows 组件向导"中,选中"Certificate Services (证书服务)"复选框,如下 图所示: Windows Components Wizard 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: 4.9 MB 🗹 📻 Accessories and Utilities Application Server 1.4 MB Certificate Services E-mail Services 1.1 MB 7.9 MB Description: Installs a certification authority (CA) to issue certificates for use with

Total disk space required:	4.9	MB	D	etails
Space available on disk:	12888.9	MB		

5) 单击"Stand-alone root CA(独立根 CA)"。(在没有安装域的情况下,不可选择" Enterprise root CA(企业根CA)"),如下图所示:

Type Select the type of CA you want to set up.
C Enterprise root CA
C Enterprise subordinate CA
<ul> <li>Stand-alone root CA</li> </ul>
C Stand-alone subordinate CA
Description of CA type The most trusted CA in a CA hierarchy.
To install an enterprise CA, Active Directory is required; you must also be a member of the Enterprise Admins group.
Use custom settings to generate the key pair and CA certificate

6) 键入证书颁发机构的名称和其他必要信息。注意! 在 CA 设置完成后这些信息都不 能改变,如果要修改只能先删除CA组件再重新安装!
这里取CA CN为CA,如下图所示:
提示:经验证,该名称中可以有空格和点等字符!

Common name for this I	ΓA.	
CA		
Distinguished name suf	fix	
Preview of distinguishe	d name:	
CN=CA		
	Expiration date:	
Validity period:	7/17/2013 7:28 PM	

7) 指定证书数据库、证书数据库日志和共享文件夹的存储位置,如下图所示:

Enter locations for the information.	Settings : certificate database, database log, ar	d configuration
<u>C</u> ertificate database:		
C:\WINDOWS\system	m32\CertLog	Br <u>o</u> wse
Certificate <u>d</u> atabase lo	og:	
C:\WINDOWS\system	m32\CertLog	Browse
Store continuation	n information in a snated folder	
IV Store configuration Shared folder:	n information in a shared folder	
I         Store configuration           Shared folder:         C:\CertConfig	n information in a shared rolder	Browse

8) 如果正在运行 WWW 发布服务,则您会遇到一条要求在安装之前停止此项服务的请求信息。单击"确定",如果出现提示,则键入证书服务安装文件的路径。9) 提示组件安装成功。

10) 运行CA服务, CA服务默认操作为挂起请求, 等待管理员手动颁发证书。为了方便, 请按以下三图所示操作(并按提示重启证书服务), 让证书服务器自动颁发证书。



Certificate Manag	gers Restrictions Auditing Security
General Policy	Module Exit Module Extensions Storage
Description of act	ive policy module
Name:	Windows default
Description	Constitues how to brandle contificate requests for
Description.	Enterprise and Stand-alone CAs
Version:	5.2.3790.1830
Copyright:	Microsoft Corporation. All rights reserved.
	Properties Select
	OK Cancel Apply
erties	21)
erties	2)2
equest Handling	212
perties equest Handling   The Windows defa	2
equest Handling   Fhe Windows defa cettificate requests	2 2 uit policy module controls how this CA should handle by default.
perties equest Handling   The Windows defa certificate requests	2 2
Derties equest Handling The Windows defa certificate requests Do the following wh	2 > ult policy module controls how this CA should handle by default. nen a certificate request is received:
Perties equest Handling   The Windows defa pertificate requests Do the following wh	2 > ult policy module controls how this CA should handle by default. nen a certificate request is received: cate request status to pending. The administrator must
equest Handling   fhe Windows defa certificate requests Do the following wh C Set the certific explicitly issue C Set when the set	It policy module controls how this CA should handle by default. Then a certificate request is received: cate request status to pending. The administrator must the certificate.
equest Handling   Ine Windows defa- certificate requests No the following wh explicitly issue Follow the set Otherwise, au	2 2 ult policy module controls how this CA should handle by default. nen a certificate request is received: cate request status to pending. The administrator must the certificate. titings in the certificate template, if applicable. tomatically issue the certificate.
C Set the set of the s	2 2 ult policy module controls how this CA should handle by default. nen a certificate request is received: cate request status to pending. The administrator must the certificate. titings in the certificate template, if applicable. tomatically issue the certificate.
Cherties equest Handling The Windows defa entificate requests Do the following wh Set the certific explicitly issue of Follow the set Otherwise, au	2 2 ult policy module controls how this CA should handle by default. nen a certificate request is received: cate request status to pending. The administrator must the certificate. titings in the certificate template, if applicable. tomatically issue the certificate.
equest Handling   The Windows defain retrificate requests Do the following which C Set the certific explicitly issue C Follow the set Otherwise, au	(2) a ult policy module controls how this CA should handle by default. nen a certificate request is received: cate request status to pending. The administrator must the certificate. titings in the certificate template, if applicable. tomatically issue the certificate.
equest Handling   Ene Windows defain certificate requests Do the following which C Set the certific explicitly issue C Follow the set D therwise, au	It policy module controls how this CA should handle by default.       nen a certificate request is received:       cate request status to pending. The administrator must the certificate.       titings in the certificate template, if applicable.
Cheves Handling Prevent Handling Prevention of the following where the following where the following where the following where the follow the set Cherewise, au Ditherwise, au Ditherwi	It policy module controls how this CA should handle by default.       nen a certificate request is received:       cate request status to pending. The administrator must the certificate.       titings in the certificate template, if applicable.
equest Handling   The Windows defa certificate requests Do the following wh C Set the certific explicitly issue C Follow the set Otherwise, au	It policy module controls how this CA should handle by default. Then a certificate request is received: cate request status to pending. The administrator must the certificate. tings in the certificate template, if applicable. tomatically issue the certificate.
Cheves Handling The Windows defails pertificate requests Do the following wh Set the certific explicitly issue Epollow the set Otherwise, au	Let policy module controls how this CA should handle by default. Then a certificate request is received: cate request status to pending. The administrator must the certificate. tings in the certificate template, if applicable. tomatically issue the certificate.
Che Windows defa equest Handling   The Windows defa entificate requests Do the following wf Set the certific explicitly issue Set the certific explicitly issue Epillow the set Otherwise, au	ult policy module controls how this CA should handle by default. even a certificate request is received: cate request status to pending. The administrator must the certificate. tings in the certificate template, if applicable. tomatically issue the certificate.
erties squest Handing   ihe Windows defa entificate requests to the following wh	ult policy module controls how this CA should handle by default. ene a certificate request is received: cate request status to pending. The administrator must the certificate. tings in the certificate template, if applicable. tomatically issue the certificate.

11) (可选) 修改IIS服务的属性:

打开[控制面板/管理工具]中的[Internet 信息服务(IIS)管理器],将[Default Web Site ( 默认网站)]属性中"Home Directory (主目录)"的Local path (本地路径)修改为证 书服务保存的路径。另外,为了避免与已有的服务冲突,建议修改默认网站的TCP端 口号为未使用的端口号,这里取8080。如以下三图所示:



Directory Security       HTTP Headers       Custom Errors       ASP.NET         The content for this resource should come from: <ul> <li></li></ul>	ory Security HTTP Headers Custom Errors ASP.NET e Performance ISAPI Filters Home Directory Documents intent for this resource should come from:	
The content for this resource should come from:	intent for this resource should come from:	
Image: A glored on this computer         C A glored costed on another computer         C A redirection to a LPL         Logial path:       C: WINDOWS [system 32] (CertSv       Brgwse         Strip source access       Image: Log yelds       Brgmove         Bead       Image: Default Application       Rgmove         Application nage:       Default Application       Rgmove         Strip point:       Obfault Web Site >       Configuration         Application point:       Obfault Web Site >       Configuration         Application point:       Offault Web Site >       Configuration         Application point:       Offault Web Site >       Configuration         Application pool:       Default AppPool       Urfoord         OK       Cancel       Apply       Help         Add: Web Site Properties       Custom Errors       ASP.NET         Description:       Oefault Web Site       Properties       Import:         P address:       (Influnassigned)       SSI, port:       Advanced         ICP port:       8000       SSI, port:       Importies         Orgonetion timeout:       120       seconds       Importies         Ve Inside logging       Acting log format:       Properties </td <td></td> <td></td>		
Image: Construction of SUCCE Star       Browsen         Stript source access       Image: Construction of SUCCE Star       Browsen         Stript source access       Image: Imag	A girectory located on this computer     A share located on another computer	
Logi path:       C: (WINDOWS)system32(CetSv       Brgwse         Script source access       Log yisks         Bread       Index this resource         Write       Index this resource         Directory browsing       Application name:       Default Application         Starting point:       Obfault Web Ste>       Configuration         Execute germissions:       Scripts only       Urload         Application pool:       Default Web Ste>       Configuration         Directory Security       HTTP Headers       Custom Errors       ASP.NET         Directory Security       HTTP Headers       Custom Errors       ASP.NET         Default Web Ste       Performance       ISAPI Filters       Home Directory       Documents         Web Ste       Performance       ISAPI Filters       Home Directory       Documents         UP port:       0001       SSL port:       Connections       Cognection timeout:       120 seconds         Very Enable HTTP Keep-Alves       Very Enable HTTP Keep-Alves       Very Enable HTTP Keep-Alves       Very Enable HTTP Keep-Alves         Very Enable HTTP Keep-Alves       Very Enable HTTP Keep-Alves       Very Help       4dyanced         21       Station SCEPE       Active log format:       Very Help       He	C A redirection to a URL	
Conje source access <ul> <li>Log yests</li> <li>Bead</li> <li>Index this resource</li> <li>Write</li> <li>Derectory browsing</li> <li>Application name:</li> <li>Default Application</li> <li>Regmove</li> </ul> Application name:         Default Application         Regmove           Starting point: <clefault site="" web="">         Configuration           Application point:         <clefault site="" web="">         Configuration           Application point:         <clefault site="" web="">         Configuration           Application pool:         Default Appleol         Indeed           OK         Cancel         Apply         Help           Mut Web Site Properties         2 ×         More Directory         Documents           Web Site Identification         Default Web Site         Performance         ISAPI Filters         Home Directory         Documents           UP port:         00801         SSL port:         Aglyanced         ICP port:         00801         SSL port:         Connections           Cognection timeout:         120         seconds         Enable HTTP Keep-Alves         Enable HTTP Keep-Alves         Enable HTTP Keep-Alves         Enable Ing file Format:         Properties         Prepoperties         2         g g</clefault></clefault></clefault>	ath: C:\WINDOWS\system32\CertSrv Brgwse	
Wite       Directory growsing         Application nage:       Default Application         Regnove       Configuration         Starting point: <clefault site="" web="">         Evecute germissions:       Scripts only         Application pool:       Default Application         Application pool:       Default Application         Application pool:       Default AppPool         OK       Cancel         Application pool:       Default AppPool         UNU Web Site Properties       2 ×         Directory Security       HTTP Headers       Custom Errors         Veb Site       Performance       ISAPI Filters         Paddress:       (All Unassigned)       Aglyanced         ICP port:       0000       SSL port:         Connections       I20 seconds       Enable HTTP Keep-Alives         Enable HTTP Keep-Alives       I20 seconds       I20 seconds         VW3C Extended Log File Format       Properties       Properties         VW3C Extended Log File Format       Properties       Properties         VW3C Extended Log File Format       Properties       Yes Start Agalaxiu bioSCEP Earter (Abjocepsetup.exe) , the point again a</clefault>	ipt source access	
Application settings         Application nagge:       Default Application         Regnove       Configuration         Starting point:       < CDefault Web Site>         Execute germissions:       Scripts only         Application pool:       Default AppPool         OK       Cancel         Application pool:       Default Web Site         Directory Security       HTTP Headers         Custom Errors       ASP.NET         Description:       Default Web Site         P address:       (All Unassigned)         ICP port:       8080         SSI, port:       Connections         Cognection timeout:       120 seconds         P enable HTTP Keep-Alives       Properties         Enable HTTP Keep-Alives       Properties         OK       Cancel       Apply         Help       22       Szks Fatele SCEP         cysk Tr stagel ArbubioSCEP Hather (Abjocepsetup.exe) , durtregint         pad	te	
Application nagge:       Default Application       Rgmove         Starting point: <default site="" web="">       Configuration         Application pool:       Default Web Site&gt;       Configuration         Application pool:       Default Application       Integration         OK       Cancel       Apply       Help         NMWeb Site Properties       Integration       Integration       Integration         Description:       Default Web Site       Performance       ISAPI Filters       Home Directory       Documents         ICP port:       90801       SSIL port:       Occornections       Cornections       Integration       Integration         Connections       IICP port:       90801       SSIL port:       Integration       Integration         Connections       IICP port:       90801       SSIL port:       Integration       Integration         Connections       IICP port:       90801       SSIL port:       Integration       Integration         Connections       IICP port:       IICP port:</default>	ectory growsing	
Starting port:          Execute germissions:       Scripts only         Applicatiog pool:       Default Web Site         OK       Cancel         Apply       Help	tion name: Default Application Remove	
Execute germissions: Scripts only Application pool: DefaultAppPool Catolog OK Cancel Apply Help MU Web Site Properties OX Directory Security HTTP Headers Custom Errors ASP.NET Web Site Performance ISAPI Fiters Home Directory Documents Web site identification Degraption: Default Web Site Performance ISAPI Fiters Home Directory Documents Web site identification Degraption: Default Web Site I CP port: 9080 SIL port: Connections Cognection timeout: 120 seconds F Enable HOTP (seep-Alves F Enable HOTP (seep-Alves Cost Cancel Apply Help Cornections Cognection timeout: Properties 2 ge ge Jan Elso EP ge To the Site Site State Site Site Site Site Site Site Site Si	g point: <default site="" web=""></default>	
Application pool:  PefaultAppPool  PefaultAppPool  CK Cancel Apply Help  CK Cancel Apply Help  CK Cancel Apply Help  Comments  Veb site identification  Degraption:  Default Web Site P address:  (Al Unassigned)  Adjvanced  Connections  Cognection timeout:  120 seconds  F Enable HITP Keep-Alves  F Enable HITP Keep-Alves  CK Cancel Apply Help  C CK Cancel Apply Help  2 安装与配置SCEP  cy装下载到本地的SCEP插件(名为cepsetup.exe),如下图例  P Add-On for Certificate Services Setup Wizard	e germissions: Scripts only	
OK       Cancel       Apply       Help         Nulk Web Site Properties       2 ×         Directory Security       HTTP Headers       Custom Errors       ASP.NET         Web Site       Performance       ISAPI Filters       Home Directory       Documents         Web site identification       Description:       Default Web Site       P advanced         ICP port:       0060       S8L port:       Advanced         ICP port:       0060       S8L port:       Connections         Cognection timeout:       120 seconds       Connections         Cognection timeout:       120 seconds       Connections         Cignection timeout:       120 seconds       Conenections	tiog pool: DefaultAppPool 💌 Unload	
OK       Cancel       Apply/       Help         Ault Web Site Properties       2 ×         Directory Security       HTTP Headers       Custom Errors       ASP.NET         Directory Security       HTTP Headers       Custom Errors       ASP.NET         Directory Security       HTTP Headers       Custom Errors       ASP.NET         Description:       Default Web Site       Image: Cost of the c		
Unit Web Site Properties       2×         Directory Security       HTTP Headers       Custom Errors       ASP.NET         Web Site       Performance       ISAPI Filters       Home Directory       Documents         Web site identification       Default Web Site       Performance       ISAPI Filters       Home Directory       Documents         Web site identification       Default Web Site       Performance       ISAPI Filters       Home Directory       Documents         Web site identification       Default Web Site       Performation       Advanced       ICP port:       90800       SSIL port:       ICP port:       ICP port:       120 seconds       ICP port:       ICP po	OK Cancel Apply Help	
ault Web Site Properties Directory Security HTTP Headers Custom Errors ASP.NET Directory Security HTTP Headers Custom Errors ASP.NET Web Site Performance ISAPI Filters Home Directory Documents Uperformance Site Performance Performance Site Performance Site Performance Site Performance Perform		
Directory Security HTTP Headers Custom Errors ASP.NET Web Site Performance ISAPI Filters Home Directory Documents Web site identification Degription: Default Web Site IP address: (Al Unassigned) ▲ Advanced ICP port: 9080 SSL port: Connections Cognection timeout: 120 seconds ICP Enable HTTP Keep-Alves ICE Enable HTTP Keep-Alves ICE Enable HTTP Keep-Alves ICE Enable HOgging Active log format: W3C Extended Log File Format ICE Properties 2. 安装与配置SCEP 安装下载到本地的SCEP插件(名为cepsetup.exe),如下图例	eb Site Properties	
Web Site       Performance       ISAPI Filters       Home Directory       Documents         Web site identification	ory Security HTTP Headers Custom Errors ASP.NET	
Web site identification         Description:       Default Web Site         IP address:       (All Unassigned)         ICP port:       8080         SSL port:       Connections         Cognection timeout:       120         seconds       Image: Cognection timeout:         IP Enable HTTP Keep-Alves         Image: Cognection timeout:       120         Seconds       Image: Cognection timeout:         IP Enable HTTP Keep-Alves       Image: Cognection timeout:         Image: Cognection timeout:       120         Seconds       Image: Cognection timeout:         Image: Cognection timeout:       120         Image: Cognection timeout:       Image: Cognection timeout:         Image: Cognection timeout:	e Performance ISAPI Filters Home Directory Documents	
Corpection:       □ Cell aux Web Sx8e         IP address:       (All Unassigned)         ICP port:       80800         SSL port:       Connections         Connections       120 seconds         IP Enable HTTP Keep-Alives       IP operties         IP Enable HTTP Keep-Alives       IP operties         IP Enable HTTP Keep-Alives       IP operties         IP Enable logging       Active log format:         W3C Extended Log File Format       IP operties         IP operties       OK         Cancel       Apply         Help       4dd-0n for Certificate Services Setup Wizard	te identification	
ICP port: 9000 SSL port: Connections Cognection timeout: 120 seconds ✓ Enable HTTP Keep-Alives ✓ Enable logging Active log format: W3C Extended Log File Format Properties W3C Extended Log File Format Properties 2 安装与配置SCEP 安装下载到本地的SCEP插件(名为cepsetup.exe),如下图例	dress: (All Unassigned)	
Connections Cognection timeout: 120 seconds ✓ Enable HTTP (sep-Alives ✓ Enable Idgging Active log format: W3C Extended Log File Format Properties W3C Extended Log File Format Properties Cot Cancel Apply Help 2. 安装与配置SCEP 安装下载到本地的SCEP插件(名为cepsetup.exe),如下图例 P Add-On for Certificate Services Setup Wizard	ort: 8080 SSL port:	
Cornections Cognection timeout: 120 seconds ✓ Enable HTTP Keep-Alives ✓ Concell Apply Help ✓ Help ✓ Help ✓ Help ✓ Enable HTTP Keep-Alives ✓ Enabl		
Active log format: W3C Extended Log File Format Properties OK Cancel Apply Help 2 安装与配置SCEP 安装下载到本地的SCEP插件(名为cepsetup.exe),如下图例 P Add-On for Certificate Services Setup Wizard	vable HTTP Keep-Alives	
W3C Extended Log File Format Properties OK Cancel Apply Help 2 安装与配置SCEP 安装下载到本地的SCEP插件(名为cepsetup.exe),如下图府 P Add-On for Certificate Services Setup Wizard	ive log format:	
OK Cancel <u>Apply</u> Help .2 安装与配置SCEP 安装下载到本地的SCEP插件(名为cepsetup.exe),如下图月 P Add-On for Certificate Services Setup Wizard	3C Extended Log File Format  Properties	
OK Cancel Apply Help .2 安装与配置SCEP 安装下载到本地的SCEP插件(名为cepsetup.exe),如下图所 P Add-On for Certificate Services Setup Wizard		
OK Cancel Apply Help .2 安装与配置SCEP 安装下载到本地的SCEP插件(名为cepsetup.exe),如下图例 P Add-On for Certificate Services Setup Wizard		
OK Cancel <u>Apply</u> Help .2 安装与配置SCEP 安装下载到本地的SCEP插件(名为cepsetup.exe),如下图例 P Add-On for Certificate Services Setup Wizard		
.2 安装与配置SCEP 安装下载到本地的SCEP插件(名为cepsetup.exe),如下图例 P Add-On for Certificate Services Setup Wizard	OK Cancel Apply Help	
.2 安装与配置SCEP 安装下载到本地的SCEP插件(名为cepsetup.exe),如下图所 P Add-On for Certificate Services Setup Wizard		
安装下载到本地的SCEP插件(名为cepsetup.exe),如下图用 P Add-On for Certificate Services Setup Wizard		=====
P Add-On for Certificate Services Setup Wizard	卜载到本地的SCEP插件(名为cepsetup.exe),如下图	到 <b>外</b> 7
	On for Certificate Services Setup Wizard	2
Welcome to the SCEP Add-On for	Welcome to the SCEP Add-On for	
Certificate Services Setup Wizard	Certificate Services Setup Wizard	
This salue assessment will include the Graph Castificate	This sale is a supervise will include the Simple Contificate	
Enrollment Protocol (SCEP) Add-On for Certificate	Enrolment Protocol (SCEP) Add On for Cartificate	
Dervices.	Christians Protocol (SCEP) Add-On for Cerdificate	
Microsoft Windows Server 2003 family Certification	Services.	
when negotiating an IPSec session.	Services. Network routers use SCEP to request certificates from a Microsoft Windows Server 2003 family Certification Autorosoft Windows Server 2003 family Certification	
	Services. Network routers use SCEP to request certificates from a Microsoft Windows Server 2003 family Certification Authority (CA). The router can then use the certificate when negotiating an IPSec session.	
To Continue, Click Next.	Services. Network routers use SCEP to request certificates from a Microsoft Windows Server 2003 family Certification Authority (CA). The router can then use the certificate when negotiating an IPSec session.	
	Services. Network routers use SCEP to request certificates from a Microsoft Windows Server 2003 family Certification Authority (CA). The router can then use the certificate when negotiating an IPSec session. To Continue, Click Next.	
	Services. Network routers use SCEP to request certificates from a Microsoft Windows Server 2003 family Certification Authority (CA). The router can then use the certificate when negotiating an IPSec session. To Continue, Click Next.	
< Back Next > Cancel	Services. Network routers use SCEP to request certificates from a Microsoft Windows Server 2003 family Certification Authority (CA). The router can then use the certificate when negotiating an IPSec session. To Continue, Click Next.	

2) 选择"Use the local system account (使用本地系统帐号)",如下图所示:

Innlica	tion Identity Antions
Cho Cerl	user the application identity that IIS should use for running the SCEP Add-on for tificate Services
	☞ [Use the local system account]
	C Use a service account
	For more information on configuring a service account, see the SCEP Add-On Help file.

3) 因H3C设备目前尚不支持SCEP Challenge, 请一定要去掉下图中"Require SCEP Challenge Phrase to Enroll"选项。

icates to
n the Microsoft authenticate
he
tificate
Cancel
Cancer

4)为SCEP登记RA(Registration Authority,注册机构)证书:输入RA信息,这里取 RA名为RA,如下图所示:

提示:SCEP插件充当RA角色,S5800交换机作为证书申请者,通过SCEP向CA申请 证书,因此下文中S5800配置证书申请的注册受理机构时,类型一定要选RA而不是C A!

Name:	RA				
Email:	RA@abc.com				
<u>C</u> ompany:	A				
Department:	Research				
City:	В				
State:	C	c	ountry/Region:	US	
	Advanced Enrollm	ent Options			
he SCEP Add-On ne	eds a special certificate	(RA Certificate) tha	t allows it to mak	e request to	
ne CA on behair or t	ne router.				

5) 提示SCEP插件安装成功,请记下下图的URL信息,下文中S5800配置注册服务器 URL时要与之对应一致。

注意:此处ca实质为host:port,本案例中Windows Server 2003服务器IP为5.5.5.1,因此S5800配置注册服务器URL需为<u>http://5.5.5.1:8080/certsrv/mscep/mscep.dll</u>。

SCEP Add-On for Certificate Services Setup Wizard	×
Setup Successful. URL to use for SCEP enrollment is http://ca/certsrv/mscep/mscep.dll.	
(OK)	
6) 查看CA服务, 这时应该可以看到有两个证书已颁发给RA (即SCEP	插件)。
3.2 配置HTTPS服务器	
因证书具有时效性,请事先正确配置S5800时钟与时区!如果全网部署	了NTP服务器

,则强烈推荐配置S5800和证书服务器(Windows Server 2003) 以及用户的浏览器 与NTP服务器同步! 3.2.1 配置PKI并申请证书 1) 配置PKI实体 #配置实体名称为aaa,通用名为S5800。 [S5800] pki entity aaa [S5800-pki-entity-aaa] common-name S5800 2) 配置PKI域 #创建并进入PKI域ssl。 [S5800] pki domain ssl #配置可信任的CA名称为RA,与SCEP插件配置中RA名保持一致。 [S5800-pki-domain-ssl] ca identifier RA #配置注册服务器URL,与SCEP插件配置保持一致。 [S5800-pki-domain-ssl] certificate request url http://5.5.5.1:8080/certsrv/mscep/mscep.dll #配置证书申请的注册受理机构类型为RA。 [S5800-pki-domain-ssl] certificate request from ra #关联PKI实体名aaa。 [S5800-pki-domain-ssl] certificate request entity aaa 3) 用RSA算法生成本地密钥对 [S5800] public-key local create rsa The range of public key size is (512 ~ 2048). NOTES: If the key modulus is greater than 512, It will take a few minutes. Press CTRL+C to abort. Input the bits of the modulus[default = 1024]: Generating Keys... +...++...++...++...++...++...++...++...++...++...++...++...++...++...++...++ +.++++++ 4) 获取CA证书 [S5800] pki retrieval-certificate ca domain ssl Retrieving CA/RA certificates. Please wait a while..... The trusted CA's finger print is: MD5 fingerprint:9C7A 2FBA 9230 2BF5 F27D 5391 DCF7 9912 SHA1 fingerprint:189A CC85 F030 F866 51B1 9DD7 6DA9 65BA 5B05 2596 Is the finger print correct?(Y/N):y Saving CA/RA certificates chain, please wait a moment..... CA certificates retrieval success. 5) 获取本地证书 [S5800] pki request-certificate domain ssl Certificate is being requested, please wait..... [S5800] Enrolling the local certificate, please wait a while..... Certificate request Successfully! Saving the local certificate to device..... Done! 3.2.2 配置SSL服务器端策略 #创建一个名为myssl的SSL服务器端策略。 [S5800] ssl server-policy myssl #配置SSL服务器端策略使用的PKI域名为ssl。 [S5800-ssl-server-policy-myssl] pki-domain ssl # (可选) 配置服务器端需要验证客户端, 这时客户端也需要申请并安装客户端证书。 [S5800-ssl-server-policy-myssl] client-verify enable 3.2.3 配置HTTPS服务 # 配置指定HTTPS服务器的SSL策略为myssl。 [S5800] ip https ssl-server-policy myssl # 使能HTTPS服务。

[S5800] ip https enable 3.2.4 创建Web网管帐号 # 创建本地帐号以实现Web网管,用户名为abc,密码为123 (明文),服务类型一定 要指定为telnet, 权限级别为3 (最高)。 [S5800] local-user abc [S5800-luser-abc] password simple 123 [S5800-luser-abc] service-type telnet level 3 配置HTTPS浏览器 3.3 本案例中,使用微软IE6作为浏览器。经验证IE7, IE8以及苹果Safari 4也可以配合。 至于其它厂家浏览器或不同版本,本人尚未测试。 1) 运行IE, 地址栏输入证书服务器地址为 <u>http://5.5.5.1:8080/certsrv</u>, 如下图所示: Alicrosoft Certificate Services - Windows Internet Explorer • + × . G - ttp://5.5.5.1:8080/certsrv/ Ele Edit Yew Favorites Iools Help 😭 🎯 🍘 Microsoft Certificate Services Microsoft Certificate Services - CA server Welcome Use this Web site to request a certificate for your Web browser, e-mail client, or other progra can verify your identity to people you communicate with over the Web, sign and encrypt mess 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 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 2) 选择"Request a certificate", 接着指定证书类型为"Web Browser Certificate", 如

下图所示:

	5. 5. 1:0000/certsrv/certrq	is. asp				
e <u>E</u> dit <u>V</u> iew F <u>a</u> vorit	es <u>I</u> ools <u>H</u> elp					
🔗 🄏 Microsoft Certi	ficate Services					
icrosoft Certificate Se	nvices CA server					
equest a Certifica	te					
elect the certificate	type:					
Web Browser Cer	tificate					
E-Mail Protection	Certificate					
, submit an advance	ced certificate request.					
			_			
榆λ证书中 <del>读</del> 3	医信自 加下网际=	÷.				
刑八匹口中旧官		١٧.				
icrosoft Certificate Ser	vices - Windows Internet Ex	plorer				
+ 10 http://5.1	5. 5. 1 :8080/certsrv/certrqb	i.asp?type=0			-	
e Edit View Favorite	es <u>T</u> ools <u>H</u> elp					
A	Nanta Candana	1 1				
📯 🖉 Microsoft Certif	icace services					
Microsoft Certif	icake services					
Crosoft Certificate Se	rvices – CA server					
Microsoft Certificate Se	nices – CA server ficate - Identifying Info	ormation	_	_		
97 @Microsoft Certificate Se eb Browser Certifi	nices - CA server	ormation				
© @ Microsoft Certificate Se eb Browser Certificate Se complete your cert	Nices – CA server ficate - Identifying Info	ormation	ion in the	following	boxes.	
© € Microsoft Certificate Se eb Browser Certificate Se complete your cert Name:	nices - CA server ficate - Identifying Info tificate, type the reques Admin	ormation	ion in the	following	boxes.	
Morosoft Certificate Se     icrosoft Certificate Se     eb Browser Certif     complete your cer     Name:         E-Mail:	Nices - CA server ficate - Identifying Infe tificate, type the reques [Admin [Admin@abc.com	ormation sted informat	ion in the	following	boxes.	
Microsoft Certificate Se     eb Browser Certif      complete your cert     Name:     E-Mail:     Company:	Nices – CA server ficate - Identifying Info tificate, type the reques Admin Admin@abc.com	ormation sted informat	ion in the	following	boxes.	
Morosoft Certificate Se     eb Browser Certif      complete your cert     Name:     E-Mail:     Company:     Department:	nices – CA server ficate - Identifying Info tificate, type the reques Admin Admin@abc.com A Research	ormation sted informat	ion in the	following	boxes.	
Microsoft Certificate Se eb Browser Certifi o complete your cert Name: E-Mail: Company: Department: City:	Accession of the server	ormation sted informat	ion in the	following	boxes.	
Microsoft Certificate Se eb Browser Certificate complete your cert Name: E-Mail: Company: Department: City: State:	Nices – CA server ficate - Identifying Info tificate, type the reques Admin Admin@abc.com A Research B C	ormation sted informat	ion in the	following	boxes.	
Microsoft Certificate Se eb Browser Certif complete your cert Name: E-Mail: Company: Department: City: State: Country/Region:	Nices – CA server ficate - Identifying Info tificate, type the reques Admin Admin@abc.com A Research B C CN	ormation sted informat	ion in the	following	boxes.	
Microsoft Certificate Se eb Browser Certif complete your cert Name: E-Mail: Company: Department: City: State: Country/Region: re Ontions >>	Nices – CA server Nices – CA server ficate - Identifying Info tificate, type the reques Admin Admin@abc.com A Research B C CN	ormation	ion in the	following	boxes.	
Microsoft Certificate Se eb Browser Certif complete your cert Name: E-Mail: Company: Department: City: State: Country/Region: re Options >>	Nices - CA server ficate - Identifying Info tificate, type the reques Admin Admin@abc.com A Research B C CN	ormation	ion in the	following	boxes.	
Microsoft Certificate Se eb Browser Certifi o complete your cert Name: E-Mail: Company: Department: City: State: Country/Region: re Options >>	Nices - CA server ficate - Identifying Info tificate, type the reques Admin Admin@abc.com A Research B C CN	ormation	ion in the	following	boxes.	

A Microsoft Certificate Services - Windows Internet Explorer	
🚱 🕤 🔻 🖉 http://5.5.5.1:8080/certsrw/certfnsh. asp	
Ele Edit View Favorites Iools Help	
😪 🐼 🌈 Microsoft Certificate Services	
Microsoft Certificate Services - CA server	
Certificate Issued	
The certificate you requested was issued to you	
Install this certificate	
5)	
Options (Internet选项),继而选择 Content (内容) > Certificates (证书)加以	查看
o	
3.4 验证	
1)运行IE,地址栏输入S5800地址为 https://1.1.1.1,应该会弹出web网管登录对	话框
, 输入用户名abc和密码123登录。如下图所示:	
Web user login	
User Name abc	
Password •••	
Login	
四	
1) 田证书目有时効性 证书服务器 (Windows Server 2003) HTTPS服务器	\$58
	000
2) WINDOWS Server 2003 CA服务配直,推存使用自动测反证节束略,或首为于。	上甲
3) SCEP为Cisco提议,目前状态为Internet Draft,而H3C设备尚不支持SCEP C	nalle
nge,因此在配置微软SCEP插件时一定要去掉SCEP Challenge选项;	
4) S5800通过SCEP申请证书,微软SCEP插件充当RA,因此S5800配置证书申	清的

5)因HTTPS服务要涉及H3C设备后台Apache服务器与用户浏览器的相互兼容,请使用H3C验证过的浏览器实施基于HTTPS的Web网管。