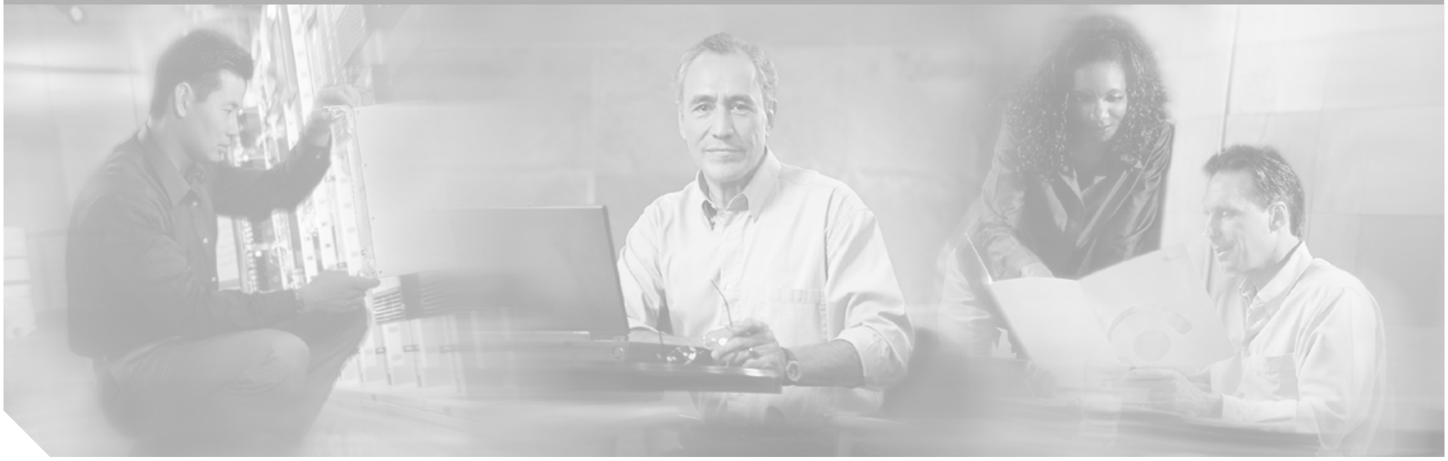


Catalyst 6500 Series Switch WebVPN Services Module Software Configuration Guide

Software Release 1.1
June 2005

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-7309-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

- Turn the television or radio antenna until the interference stops.

- Move the equipment to one side or the other of the television or radio.

- Move the equipment farther away from the television or radio.

- Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Catalyst 6500 Series Switch WebVPN Services Module Software Configuration Guide

Copyright Notices

Third-party software used under license accompanies the Cisco Web VPN Module Software release 1.1(1). One or more of the following notices may apply in connection with the license and use of such third-party software.

GNU General Public License

The Catalyst 6500 Series Web VPN Module contains software covered under the GNU Public License (listed below). If you would like to obtain the source for the modified GPL code in the SSL Services Module, please send a request to ssl_sw_req@Cisco.com.

License Text

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software—to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program," below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you."

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. END OF TERMS AND CONDITIONS.

CONTENTS

Preface

This preface describes who should read the *Catalyst 6500 Series Switch WebVPN Services Module Software Configuration Guide*, how it is organized, and its document conventions.

This publication does not contain the instructions to install the Catalyst 6500 series switch chassis. For information on installing the switch chassis, refer to the *Catalyst 6500 Series Switch Installation Guide*.

Audience

This publication is for experienced network administrators who are responsible for configuring and maintaining Catalyst 6500 series switches.

Organization

This publication is organized as follows:

Chapter	Title	Description
Chapter 1	Overview	Presents an overview of the Catalyst 6500 series switch WebVPN Services Module.
Chapter 2	Initial Configurations	Describes the initial configuration for the Catalyst 6500 series switch and the WebVPN Services Module, as well as password recovery procedures.
Chapter 3	Configuring the WebVPN Services Module	Describes how to configure the WebVPN Services Module.
Chapter 4	Setting Up WebVPN for the End User	Describes the configuration requirements and tasks for the end user's remote system.
Appendix A	Importing the Embedded Test Certificate	Describes how to import the embedded test certificate.

Chapter	Title	Description
Appendix B	Upgrading the Images	Contains information for upgrading the application and maintenance partitions, as well as installing the SSL VPN client (SVC) package.
Appendix C	Color Names and RGB Color Values	Shows the valid color values for entering the **title-color** *color* and **secondary-color** *color* commands in the WebVPN context

Conventions

This publication uses the following conventions:

Convention	Description
boldface font	Commands, command options, and keywords are in **boldface**.
italic font	Arguments for which you supply values are in *italics*.
[ ]	Elements in square brackets are optional.
{ x | y | z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
`screen` font	Terminal sessions and information the system displays are in `screen` font.
`boldface screen` font	Information you must enter is in **`boldface screen`** font.
italic screen font	Arguments for which you supply values are in *italic screen* font.
^	The symbol ^ represents the key labeled Control—for example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Nonprinting characters, such as passwords are in angle brackets.

Notes use the following conventions:

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Tips use the following conventions:

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.

Cautions use the following conventions:

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

For more detailed installation and configuration information, refer to the following publications:

- *Regulatory Compliance and Safety Information for the Catalyst 6500 Series Switches*
- *Catalyst 6500 Series WebVPN Module Installation and Verification Note*
- *Catalyst 6500 Series WebVPN Module Quick Start Guide*
- *Catalyst 6500 Series WebVPN Services Module Configuration Guide*
- *Catalyst 6500 Series Switch WebVPN Module Command Reference*
- *Catalyst 6500 Series Switch Installation Guide*
- *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*
- *Catalyst 6500 Series Switch Cisco IOS Command Reference*
- *Release Notes for Cisco IOS Release 12.2SX on the Catalyst 6500 and Cisco 7600 Supervisor Engine 720 and Supervisor Engine 2*
- For information about MIBs, refer to this URL:

  http://www.cisco.com/go/mibs

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/

Cisco Marketplace:

http://www.cisco.com/go/marketplace/

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:

  http://www.cisco.com/en/US/partner/ordering/

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

http://tools.cisco.com/RPF/register/register.do

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

  http://www.cisco.com/go/marketplace/

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

CHAPTER 1

Overview

This chapter provides an overview of the WebVPN Services Module, features, and modes of remote access, and has the following sections:

- Understanding WebVPN, page 1-1
- Modes of Remote Access, page 1-2

Understanding WebVPN

The WebVPN Services Module is a Layer 4-through-Layer 7 services module that you can install into the Catalyst 6500 series switch. WebVPN allows end users to establish a secure, remote-access VPN tunnel using a web browser. A software or hardware client is not required. WebVPN provides easy access to a broad range of web resources and web-enabled applications from almost any computer that can reach HTTPS Internet sites. WebVPN uses Secure Socket Layer Protocol and its successor, Transport Layer Security (SSL/TLS1) to provide a secure connection between remote end users and specific, supported internal resources that you configure at a central site. The WebVPN Services Module recognizes connections that need to be proxied, and the HTTP server interacts with the authentication subsystem to authenticate end users.

The network administrator provides access to WebVPN resources to end users on a group basis. End users have no direct access to resources on the internal network.

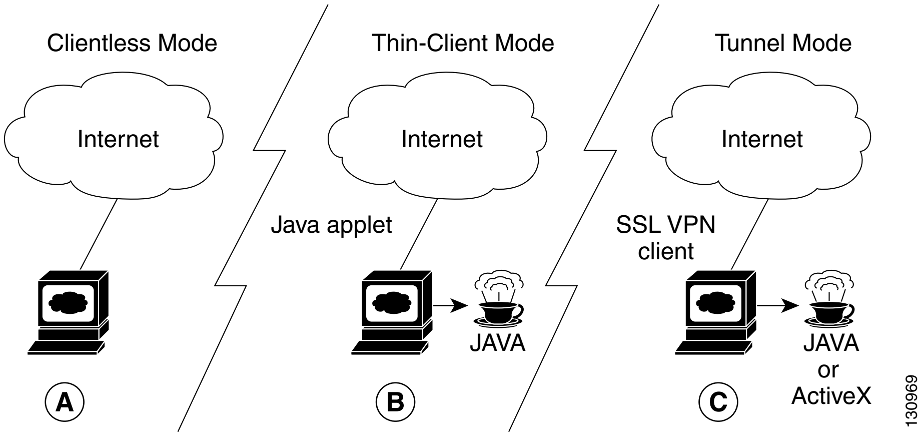
Connections on the WebVPN Services Module are very different from remote access IPsec connections. In a WebVPN connection, the WebVPN Services Module acts as a proxy between the end user's web browser and target web servers. When a WebVPN end user connects to an SSL-enabled web server, the WebVPN Services Module establishes a secure connection and validates the server's SSL certificate. The end user's browser never receives the presented certificate, so it cannot examine and validate the certificate.

Modes of Remote Access

End user login and authentication is done by the web browser to the secure gateway using an HTTP request. This process creates a session that is referenced by a cookie. After authentication, the end user is shown a portal page that allows access to the WebVPN networks. All requests sent by the browser include the authentication cookie. The portal page provides all the resources available on the internal networks. For example, the portal page could provide a link to allow the end user to download and install a thin-client Java applet (for TCP port forwarding) or a tunneling client.

Figure 1-1 shows an overview of the remote access modes.

Figure 1-1 Modes of Remote Access Overview



A	Clientless Mode	B	Thin-client Mode	C	Tunnel Mode
•	Browser-based (clientless)	•	TCP port forwarding	•	Works like “clientless” IPsec
•	Web-enabled applications, file sharing (CIFS), Outlook Web Access (OWA)	•	Uses Java Applet	•	Tunnel client loaded through Java or ActiveX (approximately 500 kB)
•	Gateway performs address or protocol conversion and content parsing and rewriting	•	Extends application support	•	Application agnostic—supports all IP-based applications
		•	Telnet, e-mail, SSH, Meeting Maker, Sametime	•	Scalable
		•	Static port-based applications	•	Administrator permission for installation

The three supported modes of remote access are described in the following sections:

- Clientless Mode, page 1-3
- Thin-Client Mode, page 1-3
- Tunnel Mode, page 1-4

Clientless Mode

In clientless mode, the end user accesses the internal or corporate network using the web browser on the client machine.

The following applications are supported in clientless mode:

- Web browsing (using HTTP and secure HTTP [HTTPS])—provides a URL box and a list of web server links in the portal page that allows the end user to browse the web.
- File sharing (using common Internet file system [CIFS])—provides a list of file server links in the portal page that allows the end user to do the following operations:
  - Browse a network (listing of domains)
  - Browse a domain (listing of servers)
  - Browse a server (listing of shares)
  - List the files in a share
  - Create a new file
  - Create a directory
  - Rename a directory
  - Update a file
  - Download a file
  - Remove a file
  - Rename a file
- Web-based e-mail, such as Microsoft Outlook Web Access (OWA) 2003 (using HTTP and HTTPS) with Web Distributed Authoring and Versioning (WebDAV) extensions—provides a link that allows the end user to connect to the Exchange server and read web-based e-mail.

Thin-Client Mode

Thin-client mode, also called TCP port forwarding, assumes that the client application uses TCP to connect to a well-known server and port.

In thin-client mode, the end user downloads a Java applet by clicking on the link provided on the portal page. The Java applet acts as a TCP proxy on the client machine for the services that you configure on the gateway.

The applications that are supported in thin-client mode are mainly e-mail-based (SMTP, POP3, and IMAP4) applications.

Note The TCP port forwarding proxy works only with the Sun 1.4 Java virtual machine (JVM) or later releases. The HTML will be specified to have the browser attempt to download the 1.4 JVM. The applet also checks for the particular version of the JVM and will refuse to run if it is not using a compatible version.

The Java applet initiates an HTTP request from the end user client to the WebVPN gateway. The name and port number of the internal Email server is included in the HTTP request (POST or CONNECT). The WebVPN gateway creates a TCP connection to that internal Email server and port.

The Java applet starts a new SSL connection for every client connection.

You should observe the following restrictions when using thin-client mode:

- The end user must allow the Java applet to download and install.
- You cannot use thin-client mode for applications such as FTP, where the ports are negotiated dynamically. You can use TCP port forwarding only with static ports.
- For applications to work seamlessly, you should give administrative privileges to end users. If you do not give administrative privileges to end users, then the end users must manually change the client program settings so that applications work properly.

Tunnel Mode

In a typical clientless remote access scenario, end users establish an SSL tunnel to move data to and from the internal networks at the application layer (for example, web and Email). In tunnel mode, end users use an SSL tunnel to move data at the network (IP) layer. Therefore, tunnel mode supports most IP-based applications. Tunnel mode supports many popular corporate applications (for example, Microsoft Outlook, Microsoft Exchange, Lotus Notes E-mail, and Telnet).

The tunnel connection is determined by the group policy configuration. The SSL VPN client (SVC) is downloaded and installed to the end user’s PC, and the tunnel connection is established when the end user logs into the WebVPN gateway.

By default, the SVC is removed from the client PC after the connection is closed. However, you have the option to keep the SVC installed on the client PC.

CHAPTER 2

Initial Configurations

This chapter describes how to initially configure the WebVPN Services Module and contains these sections:

- Using the CLI, page 2-1
- Initial Catalyst 6500 Series Switch Configuration, page 2-1
- Initial WebVPN Services Module Configuration, page 2-3
- Verifying the Initial Configuration, page 2-5
- Recovering a Lost Password, page 2-6

Using the CLI

The software interface for the WebVPN Services Module is the Cisco IOS CLI. To understand the Cisco IOS CLI and Cisco IOS command modes, refer to Chapter 2, "Command-Line Interfaces," in the *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*.

Unless your switch is located in a fully trusted environment, we recommend that you configure the WebVPN Services Module through a direct connection to the module's console port or through an encrypted session using Secure Shell (SSH). See the "Configuring Authentication for Administrators" section on page 2-5 for information on configuring SSH on the module.

Note The initial WebVPN Services Module configuration must be made through a direct connection to the console port on the module.

Initial Catalyst 6500 Series Switch Configuration

This section describes how to configure the following tasks on the Catalyst 6500 series switch:

- Configuring VLANs on the Switch, page 2-2
- Configuring a LAN Port for Layer 2 Switching, page 2-2
- Adding the WebVPN Services Module to the Corresponding VLAN, page 2-3

Configuring VLANs on the Switch

VLAN IDs must be the same for the switch and the module. Refer to the "Configuring VLANs" chapter in the *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide* for details.

Note The WebVPN software supports only the normal-range VLANs (2 through 1005). Limit the WebVPN Services Module configuration to the normal-range VLANs.

To configure VLANs on the switch, perform this task:

	Command	Purpose
Step 1	`Router# configure terminal`	Enters configuration mode, selecting the terminal option.
Step 2	`Router(config)# vlan vlan_ID`	Enters VLAN configuration mode and adds a VLAN. The valid range is 2 through 1001. **Note** Do not add an external VLAN.
Step 3	`Router(config-vlan)# end`	Updates the VLAN database and returns to privileged EXEC mode.

This example shows how to configure VLANs on the switch:

```
Router> enable
Router# configure terminal
Router(config)# vlan 100
VLAN 100 added:
     Name: VLAN100

Router(config-vlan)# end
```

Configuring a LAN Port for Layer 2 Switching

To configure a LAN port for Layer 2 switching, perform this task:

	Command	Purpose
Step 1	`Router(config)# interface type`[1] `mod/port`	Selects the LAN port to configure.
Step 2	`Router(config-if)# switchport`	Configures the LAN port for Layer 2 switching. **Note** You must enter the **switchport** command once without any keywords to configure the LAN port as a Layer 2 port before you can enter additional **switchport** commands with keywords.
Step 3	`Router(config-if)# switchport mode access`	Puts the LAN port into permanent nontrunking mode and negotiates to convert the link into a nontrunk link. The LAN port becomes a nontrunk port even if the neighboring LAN port does not agree to the change.

	Command	Purpose
Step 4	`Router(config-if)# switchport access vlan vlan_ID`	Configures the default VLAN, which is used if the interface stops trunking.
Step 5	`Router(config-if)# no shutdown`	Activates the interface.

1. *type* = **ethernet**, **fastethernet**, **gigabitethernet**, or **tengigabitethernet**

This example shows how to configure a LAN port for Layer 2 switching:

```
Router(config)# interface gigabitethernet 1/1
Router(config-if)# switchport
Router(config-if)# switchport mode access
Router(config-if)# switchport access vlan 100
Router(config-if)# no shutdown
Router(config-if)# exit
```

Adding the WebVPN Services Module to the Corresponding VLAN

To add the WebVPN Services Module to the corresponding VLAN, perform this task:

Command	Purpose
`Router (config)# webvpn module mod allowed-vlan vlan_ID`	Configures the VLANs allowed over the trunk to the WebVPN Services Module. **Note** One of the allowed VLANs must be the admin VLAN.

This example shows how to add a WebVPN Services Module that is installed in slot 3 to a specific VLAN:

```
Router>
Router> enable
Router# configure terminal
Router (config)# webvpn module 3 allowed-vlan 100
Router (config)# end
```

Initial WebVPN Services Module Configuration

Note You are required to make the following initial WebVPN Services Module configurations through a direct connection to the WebVPN Services Module console port. After the initial configurations, you can make an SSH or Telnet connection to the module to further configure the module.

The initial WebVPN Services Module configuration consists of the following tasks:

- Configuring Interfaces on the WebVPN Services Module, page 2-4
- Configuring the Default Route, page 2-4
- Configuring Authentication for Administrators, page 2-5

Configuring Interfaces on the WebVPN Services Module

Note The WebVPN0 interface is enabled by default and should not be shut down or otherwise configured.

To configure the WebVPN interface, perform this task:

	Command	Purpose
Step 1	webvpn(config)# **interfaces webvpn**<i>n</i> *interface-number.subinterface-number*	Selects a subinterface to configure.
Step 2	webvpn(config-subif)# **encap dot1q** *vlan_id*	Uses 802.1Q to send the Ethernet frames from the subinterface to the assigned *vlan-id* without any encapsulation.
Step 3	webvpn(config-subif)# **ip address** *ip-address ip-address-mask*	Configures an IP address on the subinterface.
Step 4	webvpn(config-subif)# **no shutdown**	Enables WebVPN access on the subinterface.

This example shows how to configure the WebVPN interface:

```
webvpn(config)# interface webvpn 0.1
webvpn(config-subif)# encap dot1q 100
webvpn(config-subif)# ip address 10.10.1.10
webvpn(config-subif)# no shutdown
webvpn(config-subif)# exit
webvpn(config)#
```

Configuring the Default Route

To configure the default route, perform this task:

Command	Purpose
webvpn(config)# **ip route** *prefix mask ip-address*	Configures a default route.

This example shows how to configure the default route:

```
webvpn(config)# ip route 0.0.0.0 0.0.0.0 10.10.10.100
webvpn(config)#
```

Configuring Authentication for Administrators

To configure authentication, authorization, and accounting (AAA), perform this task:

	Command	Purpose
Step 1	webvpn(config)# **username** *username* **secret** {**0** | **5**} *password*	Enables enhanced password security for the specified, unretrievable username.
Step 2	webvpn(config)# **enable password** *password*	Specifies a local enable password, if not already specified.
Step 3	webvpn(config)# **aaa new-model**	Enables authentication, authorization, and accounting (AAA).
Step 4	webvpn(config)# **aaa authentication login default local**	Specifies the module to use the local username database for authentication.
Step 5	webvpn(config)# **line vty** *line-number ending-line-number*	Identifies a range of lines for configuration and enters line configuration mode.
Step 6	webvpn(config-line)# **transport input** [**ssh** | **telnet** | **all**]	Configures the protocol used on the line.

This example shows how to configure AAA for the SSH connection to the WebVPN Services Module:

```
webvpn(config)# username admin secret admin-pass
webvpn(config)# enable password enable-pass
webvpn(config)# aaa new-model
webvpn(config)# aaa authentication login default local
webvpn(config)# line vty 0 4
webvpn(config-line)# transport input ssh
webvpn(config-line)# end
webvpn#
```

Verifying the Initial Configuration

This example shows how to verify that the VLAN information displayed matches the VLAN configuration:

```
Router# show webvpn mod 3 state
SSL-VPN module 3 data-port:2

Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: 2-1001
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:100
Vlans allowed and active in management domain: 6-8,10-13,17-18,24,30,80,170,172,255
Vlans in spanning tree forwarding state and not pruned:
   6-8,10-13,17-18,24,30,80,170,172,255
Allowed-vlan : 2-1001
```

Recovering a Lost Password

Note You must have access to the supervisor engine to perform the WebVPN Services Module password recovery procedures. To recover the enable password on the supervisor engine, refer to the software configuration guide for your software platform.

Note To run the password recovery script, the WebVPN Services Module must be in the application partition (AP).

Note The password recovery script is not compatible with WebVPN Services Module release 1.x.

Caution For security reasons, all private keys are unusable after password recovery.

To recover a lost password on the WebVPN Services Module, perform this task:

	Command	Purpose
Step 1	Router> **enable**	Initiates enable mode.
Step 2	Router# **copy tftp: pclc#**_mod_**-fs:**	Downloads the script to the specified module.
Step 3	webvpn# **copy system:startup-config nvram:running-config**	Saves the startup configuration into the running configuration.
Step 4	webvpn(config)# **enable password** _password_	Specifies a local enable password.
Step 5	webvpn(config)# **line vty** _starting-line-number ending-line-number_	Identifies a range of lines for configuration and enters line configuration mode.
Step 6	webvpn(config-line)# **login**	Enables password checking at login.
Step 7	webvpn(config-line)# **password** _password_	Specifies a password on the line.
Step 8	webvpn(config-line)# **end**	Exits line configuration mode.
Step 9	webvpn# **copy system:running-config nvram:startup-config**	Saves the configuration to the NVRAM.
Step 10	Router# **hw-module module** _mod_ **reset**	Resets the module.

The following example shows how to recover a lost password on the WebVPN Services Module installed in slot 4:

- From the supervisor engine, enter the following commands:

```
Router> enable
Password:
Router# copy tftp: pclc#4-fs:
Address or name of remote host []? 10.1.1.100
Source filename []? images/c6svc-webvpn-pwr.1-1-1.bin
Destination filename [images/c6svc-webvnp-pwr.1-1-1.bin]?
Accessing tftp://10.1.1.100/images/c6svc-webvpn-pwr.1-1-1.bin...
Loading images/c6svc-webvnp-pwr.1-1-1.bin from 10.1.1.100(via Vlan999): !
[OK - 435 bytes]

435 bytes copied in 0.092 secs (4728 bytes/sec)
2003 Nov 10 21:53:25 %SYS-3-SUP_ERRMSGFROMPC:MP upgrade/Password Recovery started.
2003 Nov 10 21:53:25 %SYS-3-SUP_ERRMSGFROMPC:Uncompress of the file succeeded.
Continuing upgrade/recovery.
2003 Nov 10 21:53:25 %SYS-3-SUP_ERRMSGFROMPC:This file appears to be a
PasswordRecovery image. Continuing.
2003 Nov 10 21:53:25 %SYS-3-SUP_ERRMSGFROMPC:Extraction of password recovery image
succeeded.
2003 Nov 10 21:53:25 %SYS-3-SUP_ERRMSGFROMPC:Continuing with password recovery.

2003 Nov 10 21:55:03 %SYS-3-SUP_ERRMSGFROMPC:System in password recovery mode.
2003 Nov 10 21:55:03 %SYS-3-SUP_ERRMSGFROMPC:Please recover configuration and reset
board.

Router#
```

- From the WebVPN Services Module console port, enter the following commands:

```
webvpn# copy system:startup-config nvram:running-config

webvpn(config)# enable password cisco
webvpn(config)# line vty 0 4
webvpn(config-line)# login
webvpn(config-line)# password cisco
webvpn(config-line)# end
webvpn# copy system:running-config nvram:startup-config
```

- From the supervisor engine, enter the following commands:

```
Router# hw-module module 4 reset
```

- From the WebVPN Services Module console port, import the keys from the backup or regenerate the keys.

  See the "Configuring Keys and Certificates" section on page 3-26 for information on generating keys and importing keys.

CHAPTER 3

Configuring the WebVPN Services Module

This chapter describes how to configure the WebVPN Services Module from the command-line interface (CLI) of the module:

Configuring Address Resolution

Each unique IP address can have an associated hostname. The Cisco IOS software maintains a cache of hostname-to-address mappings for use by the **connect**, **telnet**, and **ping** EXEC commands, and related Telnet support operations. This cache speeds the process of converting names to addresses.

IP defines a naming scheme that allows a device to be identified by its location in the IP. This is a hierarchical naming scheme that provides for *domains*. Domain names are pieced together with periods (.) as the delimiting characters. For example, Cisco is a commercial organization that the IP identifies by a *com* domain name, so its domain name is *cisco.com*. A specific device in this domain, the File Transfer Protocol (FTP) system, for example, is identified as *ftp.cisco.com*.

To keep track of domain names, IP has defined the concept of a *name server*, whose job is to hold a cache (or database) of names mapped to IP addresses. To map domain names to IP addresses, you must first identify the hostnames, then specify a name server, and enable the Domain Naming System (DNS), which is the global naming scheme of the Internet that uniquely identifies network devices.

These tasks are described in the following sections:

- Assigning Hostnames to IP Addresses, page 3-2
- Specifying the Domain Name, page 3-2
- Specifying a Name Server, page 3-3
- Enabling the DNS, page 3-3

A VPN routing and forwarding (VRF) instance consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine the information that goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a Provider Edge router.

To enable the VRF-aware DNS feature, configure the following in global configuration mode:

- A VRF routing table with the **ip vrf** *name* command
- At least one name server in the VRF with the **ip name-server vrf** *name* command.
- Domain lookup enabled with the **ip domain lookup** command.

Optionally, you can also configure a VRF specific default domain name or domain list with the **ip domain name vrf** *name* command or **ip domain list vrf** *name* command.

Assigning Hostnames to IP Addresses

The Cisco IOS software maintains a table of hostnames and their corresponding addresses, also called a hostname-to-address mapping. Higher-layer protocols such as Telnet use hostnames to identify network devices (hosts). The router and other network devices must be able to associate hostnames with IP addresses to communicate with other IP devices. Hostnames and IP addresses can be associated with one another through static or dynamic means.

Manually assigning hostnames to addresses is useful when dynamic mapping is not available.

To assign hostnames to addresses, perform this task in global configuration mode:

Command	Purpose
`Router(config)# ip host [vrf name] hostname [tcp-port-number] address1 [address2...address8]`	Statically associates hostnames with IP addresses. If a VRF name is specified, the name entry is created in the VRF specific cache. If the VRF specific name cache does not exist yet, it is dynamically created. Without a VRF name specified, the name entry is created in the global cache.

Specifying the Domain Name

You can specify a default domain name that the Cisco IOS software will use to complete domain name requests. You can specify either a single domain name or a list of domain names. Any IP hostname that does not contain a domain name will have the domain name that you specify appended to it before being added to the host table.

To specify a domain name or names, perform one of the following tasks in global configuration mode:

Command	Purpose
`Router(config)# ip domain name [vrf name] name`	Defines a default domain name that the Cisco IOS software uses to complete unqualified hostnames. If a VRF name is specified, the domain name is only used for name queries in the specified VRF.
`Router(config)# ip domain list [vrf name] name`	Defines a list of default domain names to complete unqualified hostnames. If a VRF name is specified, the domain names are only used for name queries in the specified VRF.

The following example establishes a domain list with several alternate domain names:

```
Router(config)# ip domain list csi.com
Router(config)# ip domain list telecomprog.edu
Router(config)# ip domain list merit.edu
```

Specifying a Name Server

To specify one or more hosts (up to six) that can function as a name server to supply name information for the DNS, perform the following task in global configuration mode:

Command	Purpose
`Router(config)# ip name-server [vrf name] server-address1 [server-address2... server-address6]`	Specifies one or more hosts that supply name information.

Enabling the DNS

If your network devices require connectivity with devices in networks for which you do not control name assignment, you can assign device names that uniquely identify your devices within the entire internetwork. The global naming scheme of the Internet, the DNS, accomplishes this task. This service is enabled by default.

To reenable DNS if it has been disabled, perform the following task in global configuration mode:

Command	Purpose
`Router(config)# ip domain lookup`	Enables DNS-based hostname-to-address translation.

A cache of hostname-to-address mappings is used by **connect**, **telnet**, **ping**, **trace**, **write net**, and **configure net** EXEC commands to speed the process of converting names to addresses. The commands used in this example specify the form of dynamic name lookup to be used. Static name lookup also can be configured.

The following example configures the hostname-to-address mapping process. IP DNS-based translation is specified, the addresses of the name servers are specified, and the default domain name is given.

```
Router(config)# ip domain lookup
Router(config)# ip name-server 131.108.1.111 131.108.1.2
Router(config)# ip domain name cisco.com
```

Configuring the Virtual Gateway

You define the virtual gateway using the **webvpn gateway** *gateway_name* command. The gateway is referenced in the WebVPN context.

To configure virtual gateway services, perform this task:

	Command	Purpose
Step 1	webvpn(config)# **webvpn gateway** *gateway_name*	Defines the name of the virtual gateway service. **Note** The *gateway_name* value is case sensitive.
Step 2	webvpn(config-webvpn-gateway)# **ip address** *ip_addr* [*mask_addr*][1] **port** *port* [**secondary**[2,3,4]]	Defines the virtual IP address and port number for which the WebVPN Services Module is the proxy. The default for *port* is 443. **Note** The **secondary** keyword is required if the virtual IP address is not on a network with a direct connection.
Step 3	webvpn(config-webvpn-gateway)# **http-redirect** [**port** *port*]	Specifies that the HTTP port (the default *port* is 80) is open and that any HTTP connections to the virtual gateway is directed to use secure HTTP (HTTPS).
Step 4	webvpn(config-webvpn-gateway)# **policy tcp** *tcp_policy_name*[5]	(Optional) Applies a TCP policy. See the "Configuring TCP Policy (Optional)" section on page 3-23 for TCP policy parameters. The TCP policy affects only client-side connections.
Step 5	webvpn(config-webvpn-gateway)# **policy ssl** *ssl_policy_name*[5]	(Optional) Applies an SSL policy. See the "Configuring SSL Policy (Optional)" section on page 3-21 for SSL policy parameters. The SSL policy affects only client-side connections.
Step 6	webvpn(config-webvpn-gateway)# **ssl trustpoint** *trustpoint_label*	Applies a trustpoint configuration to the WebVPN gateway[6]. You can import the test certificate embedded on the module; see Appendix B, "Importing the Embedded Test Certificate." **Note** The trustpoint defines the certificate authority server, the key parameters and key-generation methods, and the certificate enrollment methods for the WebVPN gateway. See the "Declaring the Trustpoint" section on page 3-29 for information on configuring the trustpoint.

	Command	Purpose

Step 7	`webvpn(config-webvpn-gateway)#`
	`hostname` *`name`*
		(Optional) Specifies the hostname that is used in the URL and cookie mangling process. In the load-balancing configuration, the hostname specified is the virtual gateway IP address configured on the load-balancing device.

Step 8	`webvpn(config-webvpn-gateway)#`
	`inservice`
		Puts the gateway in service.

[1] Configure the mask address to specify a wildcard proxy service. You must enter the **secondary** keyword to configure a wildcard proxy service.

[2] When you enter the **secondary** keyword, the WebVPN Services Module does not respond to ARP requests of the virtual IP address.

[3] You can enter the **secondary** keyword when the WebVPN Services Module is used in a standalone configuration or when the WebVPN Services Module is used as a real server on a load balancer (like the CSM) configured in dispatch mode (MAC address rewrite).

[4] You can enter the **secondary** keyword if you configure multiple devices using the same virtual IP address. The virtual IP address can be any legal IP address and does not have to be in the VLAN (subnet) connected to the WebVPN Services Module.

[5] If you create a policy without specifying any parameters, the policy is created using the default values.

[6] If the key (modulus) size is other than 512, 768, 1024, 1536, or 2048, you will receive an error and the trustpoint configuration is not applied. Replace the key by generating a key (using the same *key_label*) and specifying a supported modulus size, then repeat Step 6.

Configuring End User Authentication

For more detailed information on configuring RADIUS, refer to the "Configuring RADIUS" chapter in the *Cisco IOS Security Configuration Guide, Release 12.2* at this URL

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/fsecsp/scfrad.htm

Table 3-1 shows information on the WebVPN RADIUS attribute-value pairs.

Note All WebVPN attributes (except for the standard IETF RADIUS attributes) start with **webvpn:** For example:

webvpn:urllist-name=cisco
webvpn:nbnslist-name=cifs
webvpn:default-domain=cisco.com

Table 3-1 WebVPN RADIUS Attribute-Value Pairs

Attribute	Type of Value	Values	Default
addr (Framed-IP-Address[1])	ipaddr	*IP_address*	
addr-pool	string	*name*	
banner	string		
default-domain	string		
dns-servers	ipaddr	*IP_address*	
dpd-client-timeout	integer (seconds)	0 (disabled)–3600	300
dpd-gateway-timeout	integer (seconds)	0 (disabled)–3600	300

Table 3-1 WebVPN RADIUS Attribute-Value Pairs (continued)

Attribute	Type of Value	Values	Default
file-access	integer	0 (disable) 1 (enable)	0
file-browse	integer	0 (disable) 1 (enable)	0
file-entry	integer	0 (disable) 1 (enable)	0
hide-urlbar	integer	0 (disable) 1 (enable)	0
home-page	string		
idletime (Idle-Timeout[1])	integer (seconds)	0–3600	2100
ie-proxy-exception	string	*DNS_name*	
	ipaddr	*IP_address*	
ie-proxy-server	ipaddr	*IP_address*	
inacl	integer	1–199, 1300–2699	
	string	*name*	
keep-svc-installed	integer	0 (disable) 1 (enable)	1
nbnslist-name	string	*name*	
netmask (Framed-IP-Netmask[1])	ipaddr	*IP_address_mask*	
port-forward-name	string	*name*	
primary-dns	ipaddr	*IP_address*	
rekey-interval	integer (seconds)	0–43200	21600
secondary-dns	ipaddr	*IP_address*	
split-dns	string		
split-exclude[2]	ipaddr ipaddr	*IP_address* *IP_address_mask*	
	word	local-lans	
split-include[2]	ipaddr ipaddr	*IP_address* *IP_address_mask*	
svc-enabled[3]	integer	0 (disable) 1 (enable)	0
svc-ie-proxy-policy	word	none, auto, bypass-local	
svc-required[3]	integer	0 (disable) 1 (enable)	0
timeout (Session-Timeout[1])	integer (seconds)	1–1209600	43200
urllist-name	string	*name*	
user-vpn-group	string	*name*	

Table 3-1 WebVPN RADIUS Attribute-Value Pairs (continued)

Attribute	Type of Value	Values	Default
wins-server-primary	ipaddr	*IP_address*	
wins-servers	ipaddr	*IP_address*	
wins-server-secondary	ipaddr	*IP_address*	

1. Standard IETF RADIUS attributes.
2. You can specify either split-include or split-exclude, but you cannot specify both options.
3. You can specify either svc-enable or svc-required, but you cannot specify both options.

Configuring the Virtual Context

You define the virtual context using the **webvpn context** command. The virtual context links the previously configured address resolution, gateway, and authentication configurations.

To configure clientless mode, configure the URL lists and the group policy. To access email using Outlook Web Access (OWA), configure the URL list to point to the Microsoft Exchange server (for example, **http://***ipaddr***/exchange**).

To configure thin-client mode, configure the list of ports to forward and the group policy.

To configure file sharing using the common Internet file system (CIFS), configure the NetBIOS name service (NBNS) list and server address and the group policy.

To configure virtual context, perform this task:

	Command	Purpose
Step 1	`webvpn(config)#` **`webvpn context`** `[`*`vpn-name`*`]`	Enters the WebVPN context subcommand mode. The optional VPN service name *vpn-name* is used to specify a WebVPN instance.
Step 2	`webvpn(config-webvpn-context)#` **`gateway`** *`gateway-name`* `{`**`virtual-host`** *`virtual-host-name`*`|`**`domain-name`** *`domain-name`*`}`	Specifies the corresponding virtual gateway instance configured on the secure gateway and the mapping methods (for example, IP address, URL, and domain name). The *gateway-name* parameter should match one of the virtual gateways configured on the system. The *domain-name* parameter is an ASCII string, which is used to specify a corporate-specific domain name (for example, cisco.com) for the virtual WebVPN instance.
Step 3	`webvpn(config-webvpn-context)#` **`nat-address`** *`start-address end-address`* **`netmask`** *`netmask`*	Specifies the NAT addresses to be used in opening a server connection. The addresses specified in the **nat-address** command must match one of the subnets configured on the WebVPN subinterfaces. **Note** This command is required for clientless mode and thin-client mode.

	Command	Purpose
Step 4	`webvpn(config-webvpn-context)#` **`url-list`** *`listname`*	Enters url submode and allows you to configure the list of URLs that display on the portal web page. See the "Configuring Clientless Mode" section on page 3-10 for information on configuring the URL entries.
Step 5	`webvpn(config-webvpn-context)#` **`port-forward`** *`listname`*	Enters port-fwd submode and allows you to configure the list of ports to which the end user has access. See the "Configuring Thin-Client Mode" section on page 3-14 for information on configuring port forwarding.
Step 6	`webvpn(config-webvpn-context)#` **`policy group`** *`default-policy-name`*	Enters the group submode and allows you to configure group policy settings. See the "Configuring Group Policy" section on page 3-20 for detailed information on configuring group policy settings, and see the "Configuring Tunnel Mode" section on page 3-17 for detailed information on configuring tunnel mode using group policy settings.
Step 7	`webvpn(config-webvpn-context)#` **`policy ssl`** *`policy-name`*	(Optional) Specifies the SSL policy that the SSL protocol uses. The SSL policy affects only server-side connections.
Step 8	`webvpn(config-webvpn-context)#` **`policy tcp`** *`policy-name`*	(Optional) Specifies the TCP policy that the TCP protocol uses. The TCP policy affects only server-side connections.
Step 9	`webvpn(config-webvpn-context)#` **`title`** *`string`*	Specifies the HTML title string in the browser title and on the title bar. The *string* is limited to 255 characters. The default *string* is "WebVPN Service."
Step 10	`webvpn(config-webvpn-context)#` **`login-message`** *`string`*	Specifies the text that prompts the end user to log in. The *string* is limited to 255 characters. The default *string* is "Please enter your username and password."
Step 11	`webvpn(config-webvpn-context)#` **`logout-message`** *`string`*	Specifies the text that prompts the end user to log out. The *string* is limited to 255 characters. The default *string* is "Goodbye."
Step 12	`webvpn(config-webvpn-context)#` **`logo`** `[`**`file`** *`filename`*`|`**`none`**`]`	Specifies the custom logo image that is displayed on the login and portal pages. The *filename* is a file that is uploaded by the administrator to the security gateway.
Step 13	`webvpn(config-webvpn-context)#` **`title-color`** *`color`*	Specifies the color of the title bars on the login, home, and file-access portal pages. The default color is purple. For information on valid color values, see Appendix D, "Color Names and RGB Color Values."

	Command	Purpose
Step 14	`webvpn(config-webvpn-context)# secondary-color color`	Specifies the color of the secondary title bars on the login, home, and file-access portal pages. The default color is purple. For information on valid color values, see Appendix D, "Color Names and RGB Color Values."
Step 15	`webvpn(config-webvpn-context)# text-color [black|white]`	Specifies the color of the text of the title bars on the portal page. The default value is **white**.
Step 16	`webvpn(config-webvpn-context)# secondary-text-color [black|white]`	Specifies the color of the text of the secondary bars on the portal page. The default value is **black**.
Step 17	`webvpn(config-webvpn-context)# username-prompt prompt`	Configures the initial WebVPN login username prompt. The maximum length of *prompt* is 16 characters. The default *prompt* is "Login:".
Step 18	`webvpn(config-webvpn-context)# password-prompt prompt`	Configures the initial WebVPN login password prompt. The maximum length of *prompt* is 16 characters. The default *prompt* is "Password:".
Step 19	`webvpn(config-webvpn-context)# aaa authentication [domain domain-name]|[list list-name]`	Configures the authentication parameters. Specify either the domain to be used for authentication or an authentication list.
Step 20	`webvpn(config-webvpn-context)# default-group-policy policy`	Specifies the default group-policy that the virtual WebVPN context instance uses. See the "Configuring Group Policy" section on page 3-20 for information on group policies.
Step 21	`webvpn(config-webvpn-context)# vrf-name vrf-name`	Specifies the VRF domain configured for the virtual WebVPN context.
Step 22	`webvpn(config-webvpn-context)# max-users number`	Specifies the maximum number of client connections that are allowed to be open for the given virtual WebVPN context (per VRF domain).
Step 23	`webvpn(config-webvpn-context)# nbns-list name`	Creates the NBNS list name and enters nbmslist submode. See the "Configuring File Sharing Using CIFS" section on page 3-11 for information on configuring file sharing.
Step 24	`webvpn(config-webvpn-context)# ssl authenticate verify {all|none}`	Configures the peer certificate verification behavior. This behavior applies to the SSL server certificate when the WebVPN Services Module tries to connect to an HTTPS server. • **all**—Verifies signature authenticity and revocation status based on the associated trustpoint configuration. This is the default setting. • **none**—Accepts any certificate that is in its validity period.

Configuring Clientless Mode

In clientless mode, you configure an end user portal page that displays all URLs displayed as hotlinks. The HTML interface visible to these WebVPN end users varies depending on the values that you set here. End users see a customized home page (portal page) that includes only those features that you enable.

The types of servers you configure here include web servers that provide the following resources:

- Internal websites
- e-mail servers for Outlook Web Access (OWA)

The portal page for end users who are not members of a group displays all servers that you configure here. If you do not configure any servers or URLs, no servers or URLs are displayed on the portal page, although end users can still access the servers by entering the URL from the toolbar.

To configure the URL lists, perform this task:

	Command	Purpose
Step 1	`webvpn(config-webvpn-context)#` **`url-list`** *`listname`*	Specifies a name for the URL list and enters url submode.
Step 2	`webvpn(config-webvpn-url)#` **`heading`** *`text`*	Specifies the heading text for the group of URLs. Enclose the *text* within quotation marks if the heading includes any spaces. You can specify only one heading per listname.
Step 3	`webvpn(config-webvpn-url)#` **`url-text`** *`text`* **`url-value`** *`url`*	Specifies the text that the end user sees for the link on his or her home page; the *text* must be unique within a given list name. Enclose the *text* within quotation marks if the text includes any spaces. The *url* parameter specifies the URL of the link. To use OWA for web-based email, append the URL with **/exchange** (this keyword requires authentication to an Exchange server). You can specify multiple URLs for a given list name.
Step 4	`webvpn(config-webvpn-url)#` **`exit`**	Exits url submode and returns to WebVPN context submode.

Specifying **no** removes the matching line from the configuration; the URL does not need to be included. Specifying just **no url-list** *listname* removes the given list from the configuration.

This example shows how to configure URL lists:

```
webvpn(config-webvpn-context)# url-list cisco
webvpn(config-webvpn-url)# url-text cisco url-value http://cisco.com
webvpn(config-webvpn-url)# url-text CNN url-value http://cnn.com
webvpn(config-webvpn-url)# url-text yahoo url-value http://yahoo.com
webvpn(config-webvpn-url)# url-text payroll url-value http://10.1.2.215/payroll
webvpn(config-webvpn-url)# url-text finance url-value https://finance.cisco.com
webvpn(config-webvpn-url)# url-text “OWA server” url-value http://mail.cisco.com/exchange
webvpn(config-webvpn-url)# exit
webvpn(config-webvpn-context)#
```

Configuring File Sharing Using CIFS

This section describe how to configure NetBIOS Name Service (NBNS) servers that the WebVPN Services Module queries to map a NetBIOS name to an IP address.

WebVPN requires NetBIOS to access or share files on remote systems. When you attempt a file-sharing connection to a Windows computer by using its computer name, the file server that you specify corresponds to a specific NetBIOS name that identifies a resource on the network.

To make NBNS operational, you must configure at least one NetBIOS server (host). You can configure up to three NBNS servers for redundancy. The first available server on the list acts as the backup if the active server fails.

To configure the NBNS server for file sharing, perform this task:

	Command	Purpose
Step 1	`webvpn(config-webvpn-context)# **nbns-list** *name*`	Creates an NBNS list name and enters nbmslist submode.
Step 2	`webvpn(config-webvpn-nbnslist)# **nbns-server** *ip_addr* [**master**] [**timeout** *timeout*][**retry** *retries*]`	Specifies a NetBIOS name service (NBNS) list and server address for common Internet file system (CIFS) name resolution. You can configure up to three servers. **Note** Supported only on Windows 2000 and Samba servers running on Linux. The *ip_addrs* specifies the primary domain controller (PDC) on a Windows network. The **master** keyword indicates that this is a master browser. Do not enter the **master** keyword if this a Windows Internet Naming Service (WINS) server. The *timeout* value specifies the initial time in seconds to wait for a response to an NBNS query before sending the query to the next server. The default *timeout* value is 2 seconds; the range is from 1 to 30. The *retries* value specifies the number of times to retry sending a NBNS query to the configured servers, in order. This value represents the number of times to cycle through the list of servers before returning an error. The default *retries* value is 2; the range is 0 to 10.
Step 3	`webvpn(config-webvpn-nbnslist)# **exit**`	Returns to context submode.
Step 4	`webvpn(config-webvpn-context)# **policy group** *policy-name*`	Specifies the group policy name and enters the group subcommand mode. See the "Configuring Group Policy" section on page 3-20 for additional information on configuring group policy settings.
Step 5	`webvpn(config-webvpn-group)# **nbns-list** *name*`	Specifies the previously defined NBNS list. **Note** Supported on Windows 2000 servers and Linux/UNIX.

	Command	Purpose
Step 6	`webvpn(config-webvpn-group)#` **`functions`** `{`**`file-access`** `|` **`file-browse`** `|` **`file-entry`**`}`	Specifies the following functions: **file-access**—Enables the end user to access the file servers that are listed on the home page. This keyword is disabled by default. Disabling **file-access** removes **file-browse** and **file-entry** configuration. **file-browse**—Enables the end user to browse file servers. This keyword is disabled by default. **Note** You must enable file access before you can enable file browse. **file-entry**—Enables the end user to enter file servers or shares directly. This keyword is disabled by default. **Note** You must enable file access before you can enable file entry.
Step 7	`webvpn(config-webvpn-group)#` **`exit`**	Returns to context submode.
Step 8	`webvpn(config-webvpn-context)#` **`default-group-policy`** *`name`*	Specifies the default group policy.
Step 9	`webvpn(config-webvpn-context)#` **`gateway`** *`gateway-name`* **`domain-name`** *`domain-name`*`}`	Specifies the corresponding virtual gateway instance configured on the secure gateway and the mapping methods. The *gateway-name* parameter should match one of the virtual gateways configured on the system. The *domain-name* parameter is a ASCII string, which is used to specify corporate-specific domain name (for example, cisco.com) for the virtual WebVPN instance.
Step 10	`webvpn(config-webvpn-context)#` **`inservice`**	Puts the context in service.

This example shows how to configure the context for file sharing:

```
webvpn(config)# webvpn context c1
webvpn(config-webvpn-context)# nbns-list list2
webvpn(config-webvpn-nbnslist)# nbns-server 10.1.1.2
webvpn(config-webvpn-nbnslist)# exit
webvpn(config-webvpn-context)# policy group p1
webvpn(config-webvpn-group)# nbns-list "list2"
webvpn(config-webvpn-group)# functions file-acsess
webvpn(config-webvpn-group)# functions file-browse
webvpn(config-webvpn-group)# functions file-entry
webvpn(config-webvpn-group)# exit
webvpn(config-webvpn-context)# default-group-policy p1
webvpn(config-webvpn-context)# gateway g1 domain example.com
webvpn(config-webvpn-context)# inservice
```

Configuring Thin-Client Mode

Thin-client mode, also called TCP port forwarding, provides access for remote end users to client and server applications that communicate over known, fixed TCP ports. Remote end users can use client applications that are installed on their local PC and securely access remote servers that support those applications.

Cisco has tested the following applications:

- Email—SMTP, POP3, IMAP4
- Virtual Network Computing (VNC)
- Windows Terminal Services
- Telnet
- SSH
- Perforce
- XDDTS
- Sametime Instant Messaging

Other TCP-based applications may also work, but Cisco has not tested them.

Thin-client mode requires installing Sun Microsystems Java Runtime Environment and configuring applications on the end user's PC. Both require administrator permissions. It is unlikely that end users will be able to use applications when they connect from public remote systems, such as Internet kiosks or web cafes.

Note When end users authenticate using digital certificates, the Java applet does not work. Java cannot access the web browser's keystore; therefore, Java cannot use the certificates that the browser used for end user authentication, and the application cannot start. Do not use digital certificates to authenticate WebVPN end users if you want the end users to be able to access applications.

You provide mapping information that the WebVPN Services Module adds to the Hosts file on an end user's PC as the application opens. This mapping information allows the PC to connect to the server at the central site that supports the desired application.

Port forwarding can work only if the applications on remote servers are uniquely identified and reachable either by hostname or by IP address and port. We recommend that you use hostnames. See the "Using Hostnames Versus IP Addresses" section on page 3-17 for usage guidelines.

Port forwarding entries are configured in port-fwd submode. Multiple entries may be specified for a given *listname*. The *listname* is provided to group the port forwarding entries into a list that can be applied to a username or group policy.

To configure thin-client mode by specifying port forwarding settings, perform this task:

	Command	Purpose
Step 1	webvpn(config-webvpn-context)# **port-forward** *listname*	Specifies a name for a list of forwarded ports and enters WebVPN port-fwd submode. The maximum length of the *listname* is 63 characters.
Step 2	webvpn(config-webvpn-port-fwd)# **local** *localport* **remote-server** *remoteserver* **remote-port** *remoteport* **description** *description*	Specifies global access to TCP-based applications for WebVPN end users. For the end user's PC, configure the local TCP port for the application as follows: • Specifies the *localport* parameter for the local port that is listened upon; a *localport* value may be used only once within a given list name. • Set the port in the range from 1024 to 65535 to avoid conflicts with existing services that may be on the end user's workstation. See the "Guidelines for Local Ports" section on page 3-16 for usage guidelines. For the server that the end user needs to access, configure the remote server and remote TCP port as follows: • Specify the *remoteserver* parameter as the hostname or IP address to connect to on the remote server. See the "Using Hostnames Versus IP Addresses" section on page 3-17 for usage guidelines. • Specify the *remoteport* parameter as the port to connect to on the remote server. The *description* parameter allows for an application name or short description to display on the end user applet window.
Step 3	webvpn(config-webvpn-port-fwd)# **exit**	Exits WebVPN port-fwd submode and returns to WebVPN context submode.

This example shows how to configure port forwarding:

```
webvpn(config-webvpn-context)# port-forward abc
webvpn(config-webvpn-port-fwd)# local-port 25 remote-server "mailman" remote-port 25
description "SMTP server"
webvpn(config-webvpn-port-fwd)# local-port 110 remote-server "pop3-ny" remote-port 110
description "POP3-server"
webvpn(config-webvpn-port-fwd)# local-port 143 remote-server "imap-ny" remote-port 143
description "IMAP server"
webvpn(config-webvpn-port-fwd)# exit
webvpn(config-webvpn-context)#
```

Guidelines for Local Ports

When the Java applet is downloaded to start port forwarding mode on end user systems that run on Windows 2000 or XP, the hosts file (located at C:\WINNT\system32\drivers\etc\hosts) is backed up as hosts.webvpn. The Java applet then adds a mapping in the hosts file for each port forwarding entry that you configured in the port forwarding list assigned to the end user.

For example, for the following configuration:

```
port-forward "cisco"
  local-port 25 remote-server "mailman" remote-port 25 description "smtp"
  local-port 23 remote-server "pc46" remote-port 23 description "telnet"
  local-port 110 remote-server "sjcd-2" remote-port 110 description "pop3"
```

the Java applet maps “mailman” to 127.0.0.2, “pc46” to 127.0.0.3, and “sjcd-2” to 127.0.0.4 in the client's host file. The Java applet then listens on the remote port for 127.0.0.2:25, 127.0.0.3:23 and 127.0.0.4:110 on the end user’s PC.

Because the mapping is done and the Java applet listens on the required ports, you do not need to change the client applications. For example, the client can still create a Telnet connection to host pc46 (**telnet pc46**), but the Telnet connection actually goes through the Java applet and is secure.

The above configuration assumes that there are no local servers running on ports 23, 25, and 110. But if the end user’s PC is running an application on any of the ports before the applet is downloaded (for example, a Telnet server running on the client PC listening on port 23), the applet then tries to run on 127.0.0.1:*local-port*. This situation creates two possible scenarios:

- When *local-port* is the same as *remote-port,* the Java applet listens on the local-port 127.0.0.1:23, as in the following example:

  ```
  local-port 23 remote-server "pc46" remote-port 23 description "telnet"
  ```

  Port forwarding fails since the port forwarding entry is unusable by the user.

- When *local-port* is different from *remote-port*, the Java applet listens on 127.0.0.1:1230. as in the following example:

  ```
  local-port 1230 remote-server "pc46" remote-port 23 description "telnet"
  ```

  Port forwarding succeeds as there aren’t any applications running in port 1230 in the client PC. In this scenario, if the end user wants to open a Telnet connection to host pc46, the end user has to enter **telnet 127.0.0.1 1230**. Whenever the Java applet listens on the local port, you need to modify the client application to communicate with 127.0.0.1:*local-port*.

The Java applet also listens on 127.0.0.1:*local-port* when you configure the remote-server’s IP address in the port forwarding entry instead of the hostname, as follows:

```
local-port 1230 remote-server 19.0.0.1 remote-port 23 description "telnet"
```

The above configuration results in the Java applet listening to 127.0.0.1:1230. If the end user wants to open a Telnet connection to 19.0.0.1, the user needs to enter **telnet 127.0.0.1:1230**.

See the “Using Hostnames Versus IP Addresses” section on page 3-17 for usage guidelines.

Note On end user systems that run on Linux, the Java applet always listens on 127.0.0.1:*local-port*. Therefore, you need to modify all client applications to connect to 127.0.0.1:*local-port*. No mapping occurs in the hosts file.

Using Hostnames Versus IP Addresses

When you use a hostname to identify a remote server, the Java applet modifies the hosts file (assuming that the operating system is Windows and you have administrative privileges on the PC) to create an entry for each application server. For example, when you configure your first port forwarding remote server with hostname *johndoew2ksrv*, the Java applet creates a backup copy of the original hosts file, and then modifies the hosts file to include a WebVPN entry that maps *johndoew2ksrv* to a loopback IP address of 127.0.0.2. If your second port forwarding entry is *NotesServer*, the Java applet adds an entry that maps *NotesServer* to 127.0.0.3 to the hosts file. These entries are then associated with the real remote application ports. Each entry is unique because the loopback address the Java applet assigns is unique.

When you use an IP address to identify the remote server, the Java applet does not back up or modify the hosts file. It assigns each server the loopback IP address of 127.0.0.1 and the TCP port that is configured as the local TCP port. Because the assigned IP address is always 127.0.0.1, each entry must have a unique local TCP port to differentiate applications.

You configure client applications to communicate to a server address. When you use the hostname and remote TCP port, addressing information for application servers is the same regardless of the end user's location. When you use an IP address and local TCP port, addressing information changes as the end user changes locations. You have to reconfigure client applications on end users' PCs.

Configuring Tunnel Mode

Note Before end users can download and install the SSL VPN client (SVC) to their PCs, you must first install the SVC package to the internal Flash device on the WebVPN Services Module. See the "Installing the SVC Package for Tunnel Mode" section on page C-6 for information on installing the SVC package.

Note You configure tunnel mode using group policy commands. Additional group policy commands are described in the "Configuring Group Policy" section on page 3-20.

This section shows how to configure tunnel mode by specifying an IP local address pool, a WebVPN context, and a WebVPN group policy.

In tunnel mode, the gateway supplies an SSL VPN client (SVC) IP address to each of the end users that are logged into the gateway. Enter the **ip local pool** command to configure the local IP address pool to supply the SVC IP addresses.

To configure tunnel mode, perform this task:

	Command	Purpose
Step 1	webvpn(config)# **ip local pool** *pool-name start-range end-range*	Specfies the IP address pool to be used by the WebVPN Service Module for supplying an IP address for each SVC. **Note** The IP address of the WebVPN subinterface should be in the same subnet as this IP address pool. See the "Configuring Interfaces on the WebVPN Services Module" section on page 2-4 to configure the WebVPN subinterface.
Step 2	webvpn(config)# **webvpn context** *vpn_name*	Specifies the WebVPN context to be used in the configuration.
Step 3	webvpn(config-webvpn-context)# **webvpn policy group** *policy-name*	Specifies the group policy name and enters the group subcommand mode.
Step 4	webvpn(config-webvpn-group)# **functions** {**svc-enabled** | **svc-required**}	Enables tunnel mode for this group policy. Tunnel mode is disabled by default. **svc-enabled**—Enables the user of the group to use tunnel mode. If the SVC fails to install on the end user's PC, the end user can continue to use clientless mode or thin-client mode. **svc-required**—Tunnel mode is required. If the SVC fails to install on the end user's PC, the end user cannot use other modes.
Step 5	webvpn(config-webvpn-group)# **svc dpd interval** {**client** | **gateway**} *timeout*	Specifies the dead peer detection (DPD) interval values for the gateway or the client, if tunnel-mode WebVPN is enabled for the user or group. The timeout parameter specifies the timeout value in seconds. The DPD timer is used to determine if a DPD packet needs to be sent to the peer. The DPD timer is reset every time a Cisco SSL Tunnel Protocol (CSTP) frame is received from the peer. When either the gateway or the client does not receive a DPD response, the default is disabled for gateway and client. Valid values for the DPD interval for client and gateway are 0 (disabled) to 3600 seconds.
Step 6	webvpn(config-webvpn-group)# **svc address-pool** *name*	Configures the local IP address pool to supply the SVC IP addresses.
Step 7	webvpn(config-webvpn-group)# **svc dns-server** {**primary** *ip_addr* | **secondary** *ip_addr*}	Specifies the primary and secondary DNS servers for web browsing. After the SVC is installed, the active web browser is deactivated and a new browser is launched. The DNS server information specified here is for the newly launched browser. Once the connection is closed, the previous DNS settings are reapplied.
Step 8	webvpn(config-webvpn-group)# **svc homepage** *url*	Specifies the URL of the web page that is displayed when the end user logs in. The *url* specifies the path of the URL. The maximum length for the URL is 255 characters. This setting is disabled by default.

	Command	Purpose
Step 9	`webvpn(config-webvpn-group)# svc wins-server {primary ip_addr | secondary ip_addr}`	Specifies the primary and secondary WINS servers.
Step 10	`webvpn(config-webvpn-group)# svc default-domain default-domain-name`	Specifies the default domain used for the group.
Step 11	`webvpn(config-webvpn-group)# svc keep-installed`	Specifies that the SVC remains installed on the end user client PC after the connection is closed. By keeping the SVC installed on the end user PC, the end user does not have to download the SVC again when a new connection is established. The **no** version of this command uninstalls the VPN client and removes the downloaded setup file after the tunnel is terminated.
Step 12	`webvpn(config-webvpn-group)# svc rekey [time interval] [method {new-tunnel | ssl}]`	Specifies when the VPN client rekeys the SSL tunnel and the rekey method used by the WebVPN client. Rekeying is disabled by default. If rekeying is enabled, the default method is **ssl**. Valid values for **time** *interval* are 0 to 43200 seconds; the default is 21600 (6 hours). The **method new-tunnel** keyword terminates the existing tunnel and requests a new tunnel. The **method ssl** keyword triggers the SVC to renegotioate SSL security parameters without terminating the existing tunnel.
Step 13	`webvpn(config-webvpn-group)# svc split [dns string]{[include ip-address netmask]|[exclude ip-address netmask|local-lans]}`	Specifies whether all traffic is tunneled to the private network (include) or if traffic destined for an external (nonprivate) network is sent directly to the external website (exclude). **Note** You can specify either the **include** or the **exclude** keyword; you cannot specify both keywords. You can specify up to 200 addresses for either the **include** or **exclude** keyword by entering the command multiple times. The **include** keyword allows you to specify the traffic that is tunneled; all other traffic is not tunneled through the internal network. The **exclude** keyword allows you to specify the traffic that is sent directly to an external website without being tunneled through the internal network; all other traffic is tunneled. The **exclude local-lans** keyword specifies that the end user's local LAN is excluded from being tunneled.

	Command	Purpose
Step 14	webvpn(config-webvpn-group)# **svc msie-proxy** [**exception** *exception-string*]|[**server** {*ip-address*|*dns_name*}**:** *port*]|[**option** {**none** | **auto** | **bypass-local**}]	Specifies the Microsoft Internet Explorer (MSIE) browser proxy settings. **Note** This command is supported only with the MSIE browser. The **exception** keyword specifies a single DNS name or IP address for traffic that is not sent through a proxy. This keyword is disabled by default. The **server** keyword specifies an IP address or DNS name, optionally followed by a colon and port number, that is used by all the proxy setting in the browser (HTTP, Secure, FTP, Gopher) except Socks. This keyword is disabled by default. The **option none** keyword specifies that the browser does not use a proxy. This setting is the default. The **option auto** keyword specifies that the browser proxy settings are automatically detected. The **option bypass-local** keyword specifies that the local addresses bypass the proxy.
Step 15	webvpn(config-webvpn-group)# **filter tunnel** {*name* | *acl_list*}	Defines the name of the network-level access lists used for the group policy.

Configuring Policies

See the "Configuring the Virtual Gateway" section on page 3-4 for procedures for applying policies to a WebVPN gateway.

This section describes how to configure the following policies:

- Configuring Group Policy, page 3-20
- Configuring SSL Policy (Optional), page 3-21
- Configuring TCP Policy (Optional), page 3-23

Configuring Group Policy

Note Group policy commands that are specific to configuring tunnel mode are described in the "Configuring Tunnel Mode" section on page 3-17.

Note Some group policy commands apply to specific modes of remote access. See the notes below each command for specific mode information.

To configure various group policy parameters, perform this task:

	Command	Purpose

Step 1	`webvpn(config-webvpn-context)#`
	`webvpn policy group` *`policy-name`*
		Specifies the group policy name and enters the group subcommand mode.

Step 2	`webvpn(config-webvpn-group)#` **`banner`**
	`string`
		Specifies the banner string for the portal page. The *string* value may contain 7-bit ASCII values, HTML tags, and escape sequences. This string is presented to the end user after login.

Step 3	`webvpn(config-webvpn-group)`
	`hide-url-bar`
		Disables the URL bar on the portal page.
		Note This command applies only to clientless mode.

Step 4	`webvpn(config-webvpn-group)` **`timeout`**
	`{`**`idle`** *`time`* `|` **`session`** *`time`*`}`
		Specifies the end-user idle timeout value and maximum session timeout value for the user or group.
		The idle timeout specifies the end user inactivity. Valid values for idle timeout are from 0 (disabled) to 3600 seconds; the default value is 2100 seconds (35 minutes).
		The session timeout specifies the total session time, regardless of activity. Valid values for session timeout are from 1 to 1209600 seconds; the default value is 43200 seconds (12 hours).

Step 5	`webvpn(config-webvpn-group)#`
	`nbns-list` *`name`*
		Specifies the NBNS list for CIFS as defined in the context configuration.
		Supported only with Windows 2000 servers and Linux/UNIX.
		Note This command applies only to clientless mode.

Step 6	`webvpn(config-webvpn-group)#`
	`url-list` *`name`*
		Specifies the URL list as defined in the context configuration. Entering the command again overrides the previous setting. The default is to have no list specified.
		Note This command applies only to clientless mode.

Step 7	`webvpn(config-webvpn-group)#`
	`port-forward` *`name`*
		Specifies the port-forward list as defined in the context configuration. Entering the command again overrides the previous setting. The default is to have no list specified,
		Note This command applies only to thin-client mode.

Configuring SSL Policy (Optional)

The SSL policy template allows you to define parameters associated with the SSL stack.

One of the parameters you can configure is the SSL close-protocol behavior, which specifies that each of the SSL peers should send a close-notify alert and receive a close-notify alert before closing the connection properly. If the SSL connection is not closed properly, the session is removed so that the peers cannot use same SSL session ID in future SSL connections.

However, many SSL implementations do not follow the SSL close-protocol strictly (for example, an SSL peer sends a close-notify alert but does not wait for the close-notify alert from the remote SSL peer before closing the connection).

When an SSL peer initiates the close-connection sequence, the WebVPN Services Module strictly expects a close-notify alert message. If an SSL peer does not send a close-notify alert, the WebVPN Services Module removes the session from the session cache so that the same session ID cannot be used for future SSL connections.

When the WebVPN Services Module initiates the close connection sequence, you can configure the following close-protocol options:

- **strict**—The WebVPN Services Module sends a close-notify alert message to the SSL peer, and the WebVPN Services Module expects a close-notify alert message from the SSL peer. If the WebVPN Services Module does not receive a close-notify alert, SSL resumption is not allowed for that session.
- **none**—The WebVPN Services Module does not send a close-notify alert message to the SSL peer, and the WebVPN Services Module does not expect a close-notify alert message from the SSL peer. If the WebVPN Services Module receives a close-notify alert from the SSL peer, the WebVPN Services Module preserves the session information so that SSL resumption can be used for future SSL connections. However, if the WebVPN Services Module does not receive a close-notify alert from the SSL peer, SSL resumption is not allowed for that session.
- disabled (default)—The WebVPN Services Module sends a close-notify alert message to the SSL peer; however, the SSL peer does not expect a close-notify alert before removing the session. Whether SSL peer sends a close-notify alert or not, the session information is preserved allowing session resumption for future SSL connections.

If you do not associate an SSL policy with a particular proxy server, the proxy server enables all the supported cipher suites and protocol versions by default.

To define an SSL policy, perform this task:

	Command	Purpose
Step 1	`webvpn(config)#` **`webvpn policy ssl`** *`ssl_policy_name`*	Defines SSL policy templates.
Step 2	`webvpn(config-ssl-policy)#` **`cipher`** `{`**`rsa-with-rc4-128-md5`** `|` **`rsa-with-rc4-128-sha`** `|` **`rsa-with-des-cbc-sha`** `|` **`rsa-with-3des-ede-cbc-sha`** `|` **`others...`**`}`	Configures a list of cipher-suite names acceptable to the proxy server. The cipher-suite names follow the same convention as that of existing SSL stacks.
Step 3	`webvpn(config-ssl-policy)#` **`tls-rollback`** `[`**`current`** `|` **`any`**`]`	Specifies the version of the SLL protocol (SSL2.0, SSL3.0, TLS1.0) in the ClientHello message. TLS rollback is disabled by default. When you configure the **current** keyword, the SSL protocol version can be either the maximum supported version or the negotiated version. When you configure the **any** keyword, the SSL protocol version is not checked at all. **Note** By default, the WebVPN Services Module uses the maximum supported version. Enter this command if the client uses the negotiated version instead of the maximum supported version (as specified in the ClientHello message).
Step 4	`webvpn(config-ssl-policy)#` **`version`** `{`**`ssl3`** `|` **`tls1`** `|` **`all`**`}`	Defines the various protocol versions supported by the proxy server.

	Command	Purpose
Step 5	webvpn(config-ssl-policy)# **timeout handshake** *time*	Configures how long the module keeps the connection in handshake phase. The valid range is from 0 to 65535 seconds.
Step 6	webvpn(config-ssl-policy)# **close-protocol** {**strict** | **none**}	Configures the SSL close-protocol behavior. Close-protocol is disabled by default.
Step 7	webvpn(config-ssl-policy)# **session-cache**	Enables the session-caching feature. Session caching is enabled by default.
Step 8	webvpn(config-ssl-policy)# **timeout session** *timeout* [**absolute**[1]]	Configures the amount of time that an entry is kept in the session cache. The valid range is from 1 to 72000 seconds. **Note** The **absolute** keyword is required in order to configure session-cache size. **Note** The **absolute** keyword specifies that the session entry is kept in the session cache for the specified *timeout*. When the **absolute** keyword is specified, new incoming connections are rejected if there are no free entries available in the session cache.
Step 9	webvpn(config-ssl-policy)# **session-cache size** *size*	(Optional) Specifies the size of the session cache[1]. The valid range is from 1 to 262143 entries. **Note** Specify the session cache size when you enter the **absolute** keyword with the **timeout session** command. If this command is not entered or if no *size* is specified, the session cache size is the maximum size (262,144).

[1] When the **absolute** keyword is configured, the session entry is not reused until the configured session timeout expires. When **absolute** is configured, the number of session entries required is equal to (new_connection_rate * absolute_timeout). Depending on the timeout configuration and the new connection rate, the number of session entries might be very large. In this case, you can limit the number of session entries used by configuring the session-cache size.

Configuring TCP Policy (Optional)

The TCP policy template allows you to define parameters associated with the TCP stack.

To define an TCP policy template, perform this task:

	Command	Purpose
Step 1	webvpn(config)# **webvpn policy tcp** *tcp_policy_name*	Defines TCP policy templates. All defaults are assumed unless otherwise specified.
Step 2	webvpn(config-tcp-policy)# **mss** *max_segment_size*	Configures the maximum segment size (MSS), in bytes, that the connection will identify in the SYN packet that it generates. **Note** This command allows you to configure a different MSS for the client side and server side of the proxy server. The default is 1460 bytes. The valid range is from 256 to 2460 bytes[1].
Step 3	webvpn(config-tcp-policy)# **timeout syn** *time*	Configures the connection establishment timeout. The default is 75 seconds. The valid range is from 5 to 75 seconds.

	Command	Purpose
Step 4	`webvpn(config-tcp-policy)#` **`timeout reassembly`** *`time`*	Configures the amount of time, in seconds, before the reassembly queue is cleared. If the transaction is not complete within the specified time, the reassembly queue is cleared and the connection is dropped. The default is 60 seconds. The valid range is from 0 to 960 seconds (0 = disabled).
Step 5	`webvpn(config-tcp-policy)#` **`timeout inactivity`** *`time`*	Configures the amount of time, in seconds, that an established connection can be inactive. The default is 600 seconds. The valid range is from 0 to 960 seconds (0 = disabled).
Step 6	`webvpn(config-tcp-policy)#` **`timeout fin-wait`** *`time`*	Configures the FIN wait timeout in seconds. The default value is 600 seconds. The valid range is from 75 to 600 seconds.
Step 7	`webvpn(config-tcp-policy)#` **`buffer-share rx`** *`buffer_limit`*	Configures the maximum receive buffer share per connection in bytes. The default value is 32768 bytes. The valid range is from 8192 to 262144 bytes.
Step 8	`webvpn(config-tcp-policy)#` **`buffer-share tx`** *`buffer_limit`*	Configures the maximum transmit buffer share per connection in bytes. The default value is 32768 bytes. The valid range is from 8192 to 262144 bytes.
Step 9	`webvpn(config-tcp-policy)#` **`tos carryover`**	Forwards the type of service (ToS) value to all packets within a flow. **Note** If the policy is configured as a server TCP policy, the ToS value is sent from the server to the client. If the policy is configured as a virtual policy, the ToS value is sent from the client to the server. **Note** The ToS value needs to be learned before it can be propagated. For example, when a ToS value is configured to be propagated from the server to the client connection, the server connection must be established before the value is learned and propagated. Therefore, some of the initial packets will not carry the ToS value.
Step 10	`webvpn(config-tcp-policy)# [`**`no`**`]` **`nagle`**	Enables the Nagle algorithm. When you enable the **nagle** keyword, small amounts of data that are written by the application is queued into the connection-send queue, but is not sent until one of the following situations occurs: • There is data pending and an ACK arrives that acknowledges the data that was previously sent. • The application writes more data so that a full-sized segment is created and sent. When you disable the **nagle** keyword, queueing of data does not occur. All data that is written by the application is sent immediately. Nagle is enabled by default.

	Command	Purpose

Step 11	`webvpn(config-tcp-policy)#`
	`delayed-ack-threshold` *`packets`*
		Specifies the number of full-sized segments that must be received before a window-update ACK is sent. Valid values for *packets* are 1 to 10; the default value is 2.

Step 12	`webvpn(config-tcp-policy)#`
	`delay-ack-timeout` *`timer`*
		Specifies the amount of time before a window-update ACK is sent.
		If the number of full-sized segments (as specified in the **delayed-ack-threshold** command) is not received before this timer expires, then an ACK is sent acknowledging all data received up to this point, but the window is not updated. Valid values for *timer* are 50 to 500 milliseconds; the default value is 200.

[1] If fragmentation occurs, decrease the MSS value until there is no fragmentation.

Configuring Public Key Infrastructure

The WebVPN Services Module uses the SSL protocol to enable secure transactions of data through privacy, authentication, and data integrity; the protocol relies upon certificates, public keys, and private keys.

The certificates, which are similar to digital ID cards, verify the identity of the server to the clients and the clients to the server. The certificates, which are issued by certificate authorities, include the name of the entity to which the certificate was issued, the entity's public key, and the time stamps that indicate the certificate's expiration date.

Public and private keys are the ciphers that are used to encrypt and decrypt information. The public key is shared without any restrictions, but the private key is never shared. Each public-private key pair works together; data that is encrypted with the public key can only be decrypted with the corresponding private key.

Each WebVPN module supports up to 64 gateways. Each gateway acts as an HTTPS server. You must configure a pair of keys for each gateway in order to apply for a certificate for authentication.

We recommend that the certificates be stored in NVRAM so the module does not need to query the certificate authority at startup to obtain the certificates or to automatically enroll. See the "Saving Your Configuration" section on page 3-51 for more information.

When users try to access an HTTPS site through the gateway portal page, the WebVPN Services Module acts as an SSL client and needs to authenticate the certificate that it received from that site. The start time, end time, and the signature on the certificate are validated.

Note If you configure the **ssl authenticate verify none** command in the WebVPN context, the certificate is not verified.

A valid certificate may have been revoked if the key pair has been compromised. If revocation check is necessary, the WebVPN Services Module downloads the certificate revocation list (CRL) from the certificate authority and looks up the serial number of the certificate received.

The certificate can also be filtered by matching certain certificate attribute values with access control list (ACL) maps. Only authenticated certificates that are issued by trusted certificate authorities are accepted.

Note Only the certificate is authenticated, not the sender of the certificate. As part of the SSL handshake, the certificate sender is challenged for ownership of the private key that corresponds to the public key published in the certificate. If the challenge fails, the SSL handshake is aborted by the WebVPN Services Module.

These sections describe how to configure the public key infrastructure (PKI):

- Configuring Keys and Certificates, page 3-26
- Verifying Certificates and Trustpoints, page 3-50
- Saving Your Configuration, page 3-51
- Backing Up Keys and Certificates, page 3-53
- Monitoring and Maintaining Keys and Certificates, page 3-53
- Assigning a Certificate to a WebVPN Gateway and Context, page 3-54
- Renewing a Certificate, page 3-56
- Automatic Certificate Renewal and Enrollment, page 3-58

Configuring Keys and Certificates

You can configure keys and certificates using one of the following methods:

- If you are using Simple Certificate Enrollment Protocol (SCEP), configure the keys and certificates by doing the following:
  - Generate a key pair.
  - Declare the trustpoint.
  - Get the certificate authority certificate.
  - Send an enrollment request to a certificate authority on behalf of the SSL server.

  See the "Configuring the Trustpoint Using SCEP" section on page 3-27 for details.
- If you are not using SCEP, configure the keys and certificates using the manual certificate enrollment (TFTP and cut-and-paste) feature by doing the following:
  - Generate or import a key pair.
  - Declare the trustpoint.
  - Get the certificate authority certificate and enroll the trustpoint using TFTP or cut-and-paste to create a PKCS10 file.
  - Request the SSL server certificate offline using the PKCS10 package.
  - Import the SSL server certificate using TFTP or cut-and-paste.

  See the "Manual Certificate Enrollment" section on page 3-33 for details.
- If you are using an external PKI system, do the following:
  - Generate PKCS12 or PEM files.
  - Import this file to the module.

  See the "Importing and Exporting Key Pairs and Certificates" section on page 3-42 for details.

An external PKI system is a server or a PKI administration system that generates key pairs and enrolls for certificates from a certificate authority or a key and certificate archival system. The Public-Key Cryptography Standards (PKCS) specifies the transfer syntax for personal identity information, including the private keys and certificates. This information is packaged into an encrypted file. To open the encrypted file, you must know a pass phrase. The encryption key is derived from the pass phrase.

Note You do not need to configure a trustpoint before importing the PKCS12 or PEM files. If you import keys and certificates from PKCS12 or PEM files, the trustpoint is created automatically, if it does not already exist.

Configuring the Trustpoint Using SCEP

To configure a trustpoint using SCEP, complete the following tasks:

- Generating RSA Key Pairs, page 3-27
- Declaring the Trustpoint, page 3-29
- Obtaining the Certificate Authority Certificate, page 3-30
- Requesting a Certificate, page 3-31

Generating RSA Key Pairs

Note The first key pair generated enables SSH on the module. If you are using SSH, configure a key pair for SSH. See the "Configuring Authentication for Administrators" section on page 2-5.

RSA is the public key cryptographic system developed by Ron Rivest, Adi Shamir, and Leonard Aldeman. The RSA algorithm is widely used by certificate authorities and SSL servers to generate key pairs. Each certificate authority and each SSL server has its own RSA key pair. The SSL server sends its public key to the certificate authority when enrolling for a certificate. The SSL server uses the certificate to prove its identity to clients when setting up the SSL session.

The SSL server keeps the private key in a secure storage and sends only the public key to the certificate authority, which uses its private key to sign the certificate that contains the server's public key and other identifying information about the server.

Each certificate authority keeps the private key secret and uses the private key to sign certificates for its subordinate certificate authorities and SSL servers. The certificate authority has a certificate that contains its public key.

The certificate authorities form a hierarchy of one or more levels. The top-level certificate authority is called the root certificate authority. The lower level certificate authorities are called intermediate or subordinate certificate authorities. The root certificate authority has a self-signed certificate, and it signs the certificate for the next level subordinate certificate authority, which in turn signs the certificate for the next lower level certificate authority, and so on. The lowest level certificate authority signs the certificate for the SSL server.

Note The WebVPN Services Module supports up to eight levels of certificate authority (one root certificate authority and up to seven subordinate certificate authorities). For an example of a three-level (3-tier) enrollment, see the "Example of Three-Tier Certificate Authority Enrollment" section on page 3-32.

These certificates form a chain with the server certificate at the bottom and the root certificate authority's self-signed certificate at the top. Each signature is formed by using the private key of the issuing certificate authority to encrypt a hash digest of the certificate body. The signature is attached to the end of the certificate body to form the complete certificate.

When setting up an SSL session, the SSL server sends its certificate chain to the client. The client verifies the signature of each certificate up the chain by retrieving the public key from the next higher-level certificate to decrypt the signature attached to the certificate body. The decryption result is compared with the hash digest of the certificate body. Verification terminates when one of the certificate authority certificates in the chain matches one of the trusted certificate authority certificates stored in the client's own database.

If the top-level certificate authority certificate is reached in the chain, and there is no match of trusted self-signed certificates, the client may terminate the session or prompt the user to view the certificates and determine if they can be trusted.

After the SSL authenticates the server, it uses the public key from the server certificate to encrypt a secret and send it over to the server. The SSL server uses its private key to decrypt the secret. Both sides use the secret and two random numbers they exchanged to generate the key material required for the rest of the SSL session for data encryption, decryption, and integrity checking.

Note The WebVPN Services Module supports only general-purpose keys.

When you generate general-purpose keys, only one pair of RSA keys is generated. Named key pairs allow you to have multiple RSA key pairs, enabling the Cisco IOS software to maintain a different key pair for each identity certificate. We recommend that you specify a name for the key pairs.

Note The generated key pair resides in the system memory (RAM). Key pairs will be lost on power failure or module reset. You must enter the **copy system:running-config nvram:startup-config** command to save the running configuration, as well as save the key pairs to the private configuration file in the module NVRAM.

To generate RSA key pairs, perform this task:

Command	Purpose
webvpn(config)# **crypto key generate rsa general-keys label** *key-label* [**exportable**[1]] [**modulus** *size*]	Generates RSA key pairs.

[1] The **exportable** keyword specifies that the key is allowed to be exported. You can specify that a key is exportable during key generation. Once the key is generated as either exportable or not exportable, it cannot be modified for the life of the key.

Note When you generate RSA keys, you are prompted to enter a modulus length in bits. The WebVPN Services Module supports modulus lengths of 512, 768, 1024, 1536, and 2048 bits. Although you can specify 512 or 768, we recommend a minimum modulus length of 1024. A longer modulus takes longer to generate and takes longer to use, but it offers stronger security.

This example shows how to generate general-purpose RSA keys:

```
webvpn(config)# crypto key generate rsa general-keys label kp1 exportable

The name for the keys will be: kp1

Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024

Generating RSA keys.... [OK].
```

Note After you generate a key pair, you can test the SSL service by generating a self-signed certificate.

Declaring the Trustpoint

You should declare one trustpoint to be used by the WebVPN Services Module for each certificate.

To declare the trustpoint that your module uses and specify characteristics for the trustpoint, perform this task beginning in global configuration mode:

	Command	Purpose
Step 1	webvpn(config)# **crypto pki trustpoint** *trustpoint-label*[1]	Declares the trustpoint that your module should use. Enabling this command puts you in ca-trustpoint configuration mode.
Step 2	webvpn(ca-trustpoint)# **rsakeypair** *key-label*	Specifies which key pair to associate with the certificate.
Step 3	webvpn(ca-trustpoint)# **enrollment** [**mode ra**] [**retry** [**period** *minutes*] [**count** *count*]] **url** *url*	Specifies the enrollment parameters for your certificate authority.
Step 4	webvpn(ca-trustpoint)# **ip-address** *server_ip_addr*	(Optional) Specifies the IP address of the WebVPN gateway that will use this certificate[2].
Step 5	webvpn(ca-trustpoint)# **password** *password*	(Optional) Configures a challenge password.
Step 6	webvpn(ca-trustpoint)# **revocation-check** *method1* [*method2*[*method3*]]	(Optional) Specifies how to check the revocation status of a certificate. The available methods are as follows: • **crl**—Certificate checking is performed by a certificate revocation list (CRL). This behavior is the default. • **none**—Certificate checking is not required. • **ocsp**—Certificate checking is performed by an Online Certificate Status Protocol (OCSP) server. If a second and third method are specified, each method will be used only if the previous method returns an error, such as a server being down.

	Command	Purpose
Step 7	`webvpn(ca-trustpoint)#` **`subject-name`** *`line`*[3, 4]	(Optional) Configures the hostname of the WebVPN gateway[5].
Step 8	`webvpn(ca-trustpoint)#` **`exit`**	Exits ca-trustpoint configuration mode.

1. The *trustpoint-label* should match the *key-label* of the keys; however, this is not a requirement.
2. Some web browsers compare the IP address in the SSL server certificate with the IP address that might appear in the URL. If the IP addresses do not match, the browser may display a dialog box and ask the client to accept or reject this certificate.
3. For example, **subject-name CN=***server1.domain2.com*, where *server1* is the name of the SSL server that appears in the URL. The **subject-name** command uses the Lightweight Directory Access Protocol (LDAP) format.
4. Arguments specified in the subject name must be enclosed in quotation marks if they contain a comma. For example, **O="Cisco, Inc."**
5. Some browsers compare the CN field of the subject name in the SSL server certificate with the hostname that might appear in the URL. If the names do not match, the browser may display a dialog box and ask the client to accept or reject the certificate. Also, some browsers will reject the SSL session setup and silently close the session if the CN field is not defined in the certificate.

This example shows how to declare the trustpoint PROXY1 and verify connectivity:

```
webvpn(config)# crypto pki trustpoint PROXY1
webvpn(ca-trustpoint)# rsakeypair PROXY1
webvpn(ca-trustpoint)# enrollment url http://exampleCA.cisco.com
webvpn(ca-trustpoint)# revocation-check none
webvpn(ca-trustpoint)# subject-name C=US, ST=California, L=San Jose, O=Cisco, OU=Lab,
CN=host1.cisco.com
webvpn(ca-trustpoint)# end
webvpn# ping example.cisco.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 20.0.0.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
webvpn#
```

Obtaining the Certificate Authority Certificate

For each trustpoint, you must obtain a certificate that contains the public key of the certificate authority; multiple trustpoints can use the same certificate authority.

Note Contact the certificate authority to obtain the correct fingerprint of the certificate and verify the fingerprint displayed on the console.

To obtain the certificate that contains the public key of the certificate authority, perform this task in global configuration mode:

Command	Purpose
`webvpn(config)#` **`crypto pki authenticate`** *`trustpoint-label`*	Obtains the certificate that contains the public key of the certificate authority. Enter the same *trustpoint_label* that you entered when declaring the trustpoint.

This example shows how to obtain the certificate of the certificate authority:

```
webvpn(config)# crypto pki authenticate PROXY1
Certificate has the following attributes:
Fingerprint: A8D09689 74FB6587 02BFE0DC 2200B38A
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
webvpn(config)# end
webvpn#
```

Requesting a Certificate

You must obtain a signed certificate from the certificate authority for each trustpoint.

To request signed certificates from the certificate authority, perform this task in global configuration mode:

Command	Purpose
`webvpn(config)#` **crypto pki enroll** *trustpoint-label*[1]	Requests a certificate for the trustpoint.

[1] You have the option to create a challenge password that is not saved with the configuration. This password is required in the event that your certificate needs to be revoked, so you must remember this password.

Note If your module or switch reboots after you have entered the **pki enroll** command but before you have received the certificates, you must reenter the command and notify the certificate authority administrator.

This example shows how to request a certificate:

```
webvpn(config)# crypto pki enroll PROXY1
%
% Start certificate enrollment..

% The subject name in the certificate will be: C=US; ST=California; L=San Jose; O=Cisco;
OU=Lab; CN=host1.cisco.com
% The subject name in the certificate will be: host.cisco.com
% The serial number in the certificate will be: 00000000
% The IP address in the certificate is 10.0.0.1

% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificate' command will also show the fingerprint.
Fingerprint:  470DE382 65D8156B 0F84C2AF 4538B913

webvpn(config)# end
```

After you configure the trustpoint, see the "Verifying Certificates and Trustpoints" section on page 3-50 to verify the certificate and trustpoint information.

Example of Three-Tier Certificate Authority Enrollment

The WebVPN Services Module supports up to eight levels of certificate authority (one root certificate authority and up to seven subordinate certificate authorities).

The following example shows how to configure three levels of certificate authority:

- Generating the Keys

```
webvpn(config)# crypto key generate rsa general-keys label key1 exportable
The name for the keys will be:key1
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:1024
% Generating 1024 bit RSA keys ...[OK]
```

- Defining the Trustpoints

```
webvpn(config)# crypto pki trustpoint 3tier-root
webvpn(ca-trustpoint)# enrollment url tftp://10.1.1.1
webvpn(ca-trustpoint)#
webvpn(ca-trustpoint)# exit
webvpn(config)# crypto pki trustpoint 3tier-sub1
webvpn(ca-trustpoint)# enrollment url tftp://10.1.1.2
webvpn(ca-trustpoint)#
webvpn(ca-trustpoint)# exit
webvpn(config)# crypto pki trustpoint tp-proxy1
webvpn(ca-trustpoint)# enrollment url tftp://10.1.1.3
webvpn(ca-trustpoint)# serial-number
webvpn(ca-trustpoint)# password cisco
webvpn(ca-trustpoint)# subject CN=ste.cisco.com
webvpn(ca-trustpoint)# rsakeypair key1
webvpn(ca-trustpoint)# show
 enrollment url tftp://10.1.1.3
 serial-number
 password 7 02050D480809
 subject-name CN=ste.cisco.com
 rsakeypair key1
end

webvpn(ca-trustpoint)# exit
```

- Authenticating the Three Certificate Authorities (One Root And Two Subordinate Certificate Authorities)

```
webvpn(config)# crypto pki authenticate 3tier-root
Certificate has the following attributes:
Fingerprint:84E470A2 38176CB1 AA0476B9 C0B4F478
% Do you accept this certificate? [yes/no]:yes
Trustpoint CA certificate accepted.
webvpn(config)#
webvpn(config)# crypto pki authenticate 3tier-sub1
Certificate has the following attributes:
Fingerprint:FE89FB0D BF8450D7 9934C926 6C66708D
Certificate validated - Signed by existing trustpoint CA certificate.
Trustpoint CA certificate accepted.
webvpn(config)#
webvpn(config)# crypto pki authenticate tp-proxy1
Certificate has the following attributes:
Fingerprint:6E53911B E29AE44C ACE773E7 26A098C3
Certificate validated - Signed by existing trustpoint CA certificate.
Trustpoint CA certificate accepted.
```

- Enrolling with the Third Level Certificate Authority

```
webvpn(config)# crypto pki enroll tp-proxy1
%
% Start certificate enrollment ..

% The fully-qualified domain name in the certificate will be:ste.
% The subject name in the certificate will be:ste.
% The serial number in the certificate will be:B0FFF0C2
% Include an IP address in the subject name? [no]:
Request certificate from CA? [yes/no]:yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificate' command will also show the fingerprint.

webvpn(config)#    Fingerprint: 74390E57 26F89436 6FC52ABE 24E23CD9

webvpn(config)#
*Apr 18 05:10:20.963:%CRYPTO-6-CERTRET:Certificate received from Certificate Authority
```

Manual Certificate Enrollment

The Manual Certificate Enrollment (TFTP and cut-and-paste) feature allows you to generate a certificate request and accept certificate authority certificates as well as router certificates. These tasks are accomplished with a TFTP server or manual cut-and-paste operations. You may want to use TFTP or manual cut-and-paste enrollment in the following situations:

- Your certificate authority does not support Simple Certificate Enrollment Protocol (SCEP) (which is the most commonly used method for sending and receiving requests and certificates).
- A network connection between the router and certificate authority is not possible (which is how a router running Cisco IOS software obtains its certificate).

Configure the Manual Certificate Enrollment (TFTP and cut-and-paste) feature as described at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftmancrt.htm

Note If the certificate revocation list (CRL) fails to download because the CRL server is unreachable or the CRL download path does not exist, the certificate might fail to import. You should make sure all trustpoints that are linked to the import process are able to download the CRL. If the CRL path does not exist, or if the CRL server is unreachable, then you should enter the **revocation-check none** command for all trustpoints that are linked to the import process. Enter the **show crypto pki certificates** command to display information for all certificates, and obtain a list of associated trustpoints from the display of the certificate authority certificate. Enter the **revocation-check none** command for all these trustpoints.

For example, in a three-tier certificate authority hierarchy (root CA, subordinate CA1, and subordinate CA2), when you import the subordinate CA1 certificate, enter the **revocation-check none** command for all the trustpoints associated with root CA. Similarly, when you import the subordinate CA2 certificate, enter the **revocation-check none** command for all the trustpoints associated with root CA and subordinate CA1.

After you successfully import the certificate, you can restore the original CRL options on the trustpoints.

Example 1: Configuring Certificate Enrollment Using TFTP (One-Tier Certificate Authority)

1. Configure the trustpoint:

```
webvpn# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
webvpn(config)# crypto pki trustpoint tftp_example
webvpn(ca-trustpoint)# enrollment url tftp://10.1.1.2/win2k
webvpn(ca-trustpoint)# rsakeypair pair3
webvpn(ca-trustpoint)# exit
```

2. Request a certificate for the trustpoint:

```
webvpn(config)# crypto pki enroll tftp_example
% Start certificate enrollment ..

% The fully-qualified domain name in the certificate will be: ssl-proxy.cisco.com
% The subject name in the certificate will be: ssl-proxy.cisco.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 00000000
% Include an IP address in the subject name? [no]:
Send Certificate Request to tftp server? [yes/no]: yes
% Certificate request sent to TFTP Server
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificate' command will also show the fingerprint.
webvpn(config)#    Fingerprint:  D012D925 96F4B5C9 661FEC1E 207786B7
!!
```

3. Obtain the certificate that contains the public key of the certificate authority:

```
webvpn(config)# crypto pki auth tftp_example
Loading win2k.ca from 10.1.1.2 (via Ethernet0/0.168): !
[OK - 1436 bytes]

Certificate has the following attributes:
Fingerprint: 2732ED87 965F8FEB F89788D4 914B877D
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
webvpn(config)#
```

4. Import the server certificate:

```
webvpn(config)# crypto pki import tftp_example cert
% The fully-qualified domain name in the certificate will be: ssl-proxy.cisco.com
Retrieve Certificate from tftp server? [yes/no]: yes
% Request to retrieve Certificate queued

webvpn(config)#
Loading win2k.crt from 10.1.1.2 (via Ethernet0/0.168): !
[OK - 2112 bytes]

webvpn(config)#
*Apr 15 12:02:33.535: %CRYPTO-6-CERTRET: Certificate received from Certificate
Authority
webvpn(config)#
```

Example 2: Configuring Certificate Enrollment Using Cut-and-Paste (One-Tier Certificate Authority)

1. Generate the RSA key pair:

```
webvpn(config)# crypto key generate rsa general-keys label CSR-key exportable
The name for the keys will be:CSR-key
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:1024
% Generating 1024 bit RSA keys ...[OK]
```

2. Configure the trustpoints:

```
webvpn(config)# crypto pki trustpoint CSR-TP
webvpn(ca-trustpoint)# rsakeypair CSR-key
webvpn(ca-trustpoint)# serial
webvpn(ca-trustpoint)# subject-name CN=abc, OU=hss, O=cisco
webvpn(ca-trustpoint)# enrollment terminal
webvpn(ca-trustpoint)# exit
```

3. Request a certificate for the trustpoint:

```
webvpn(config)# crypto pki enroll CSR-TP
% Start certificate enrollment ..

% The subject name in the certificate will be:CN=abc, OU=hss, O=cisco
% The fully-qualified domain name in the certificate will be:ssl-proxy.cisco.com
% The subject name in the certificate will be:ssl-proxy.cisco.com
% The serial number in the certificate will be:B0FFF22E
% Include an IP address in the subject name? [no]:no
Display Certificate Request to terminal? [yes/no]:yes
```

```
Certificate Request follows:

MIIBwjCCASsCAQAwYTEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA2hzczEMMAoG
A1UEAxMDYWJjMTMwDwYDVQQFEwhCMEZGRjIyRTAgBgkqhkiG9w0BCQIWE3NzbC1w
cm94eS5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALt7O6tt
30lBVVK1qAE/agsuzIaa15YZft3bDb9t3pPncKh0ivBTgVKpJiLPWGZPjdbtejxQ
tYSF77R1pmhK0WSKPuu7fJPYr/Cbo80OUzkRAgMBAAGgITAfBgkqhkiG9w0BCQ4x
EjAQMA4GA1UdDwEB/wQEAwIFoDANBgkqhkiG9w0BAQQFAAOBgQC2GIX06/hihXHA
DA5sOpxgLsO1rMP8PF4bZDdlpWLVBSOrp4S1L7hH9P2NY9rgZAJhDTRfGGm179JY
GOtUuCyPYPkpb0S5VGTUrHvvUWekleKq2d91kfgbkRmJmHBaB2Ev5DNBcV11SIMX
RULG7oUafU6sxnDWqbMseToF4WrLPg==

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:no
```

4. Import the certificate authority certificate:

```
webvpn(config)# crypto pki authenticate CSR-TP

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIICxzCCAjCgAwIBAgIBADANBgkqhkiG9w0BAQQFADBSMQswCQYDVQQGEwJBVTET
MBEGA1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMYSW50ZXJuZXQgV2lkZ2l0cyBQ
dHkgTHRkMQswCQYDVQQDEwJjYTAeFw0wMzA2MjYyMjM4MDlaFw0wODEyMTYyMjM4
MDlaMFIxCzAJBgNVBAYTAkFVMRMwEQYDVQQIEwpTb21lLVN0YXRlMSEwHwYDVQQK
ExhJbnRlcm5ldCBXaWRnaXRzIFB0eSBMdGQxCzAJBgNVBAMTAmNhMIGfMA0GCSqG
SIb3DQEBAQUAA4GNADCBiQKBgQCcG9ObqOLmf0cASkF48jz8X7ZQxT1H68OQKNC3
ks95vkGbOAa/1/R4ACQ3s9iPkcGQVqi4Dv8/iNG/1mQo8HBwtR9VgG0l8IGBbuiZ
dlarYnQHUz6Bm/HzE1RXVOY/VmyPOVevYy8/cYhwx/xOE9BYQOyP15Chi8nhIS5F
+WWoHQIDAQABo4GsMIGpMB0GA1UdDgQWBBS4Y+/lSXKDrw5N5m/tgCzu/W81PDB6
BgNVHSMEczBxgBS4Y+/lSXKDrw5N5m/tgCzu/W81PKFWpFQwUjELMAkGA1UEBhMC
QVUxEzARBgNVBAgTClNvbWUtU3RhdGUxITAfBgNVBAoTGEludGVybmV0IFdpZGdp
dHMgUHR5IEx0ZDELMAkGA1UEAxMCY2GCAQAwDAYDVR0TBAUwAwEB/zANBgkqhkiG
9w0BAQQFAAOBgQB/rPdLFVuycbaJQucdFQG7kl/XBNI7aY3IL3Lkeumt/nXD+eCn
RpYE5WWY8X1Aizqnj4bqFdqPqYdD7Lg8viwqm2tQmU6zCsdaKhL1J7FCWbfs2+Z5
oNV2Vsqx0Ftnf8en/+HtyS2AdXHreThfgkXz3euXD0ISMFVKRy81o4EdzA==
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint:B8B35B00 095573D0 D3B8FA03 B6CA8934
% Do you accept this certificate? [yes/no]:yes
Trustpoint CA certificate accepted.
% Certificate successfully imported

webvpn(config)#
```

5. Import the server certificate (the server certificate is issued by the certificate authority whose certificate is imported in Step 4):

```
webvpn(config)# crypto pki import CSR-TP certificate
% The fully-qualified domain name in the certificate will be:ssl-proxy.cisco.com

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIB7TCCAVYCAQQwDQYJKoZIhvcNAQEEBQAwUjELMAkGA1UEBhMCQVUxEzARBgNV
BAgTClNvbWUtU3RhdGUxITAfBgNVBAoTGEludGVybmV0IFdpZGdpdHMgUHR5IEx0
ZDELMAkGA1UEAxMCY2EwHhcNMDMxMTIwMDAxMzE2WhcNMDQxMTE5MDAxMzE2WjAs
MQ4wDAYDVQQKEwVjaXNjbzEMMAoGA1UECxMDaHNzMQwwCgYDVQQDEwNhYmMwgZ8w
DQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALt7O6tt30lBVVK1qAE/agsuzIaa15YZ
```

```
ft3bDb9t3pPncKh0ivBTgVKpJiLPWGZPjdbtejxQksuSY589V+GMDrO9B4Sxn+5N
p2bQmd745NvI4gorNRvXcdjmE+/SzE+bBSBcKAwNtYSF77R1pmhK0WSKPuu7fJPY
r/Cbo80OUzkRAgMBAAEwDQYJKoZIhvcNAQEEBQADgYEAjqJ9378P6Gz69Ykplw06
Powp+2rbe2iFBrE1xE09BL6G6vzcBQgb5W4uwqxe7SIHrHsS0/7Be3zeJnlOseWx
/KVj7I02iPgrwUa9DLavwrTyaa0KtTpti/i5nIwTNh5xkp2bBJQikD4TEK7HAvXf
HQ9SyB3YZJk/Bjp6/eFHEfU=
-----END CERTIFICATE-----

% Router Certificate successfully imported

webvpn(config)#^Z
```

Example 3: Configuring Certificate Enrollment Using TFTP (Three-Tier Certificate Authority)

1. Generate the RSA key pair:

```
webvpn(config)# crypto key generate rsa general-keys label test-3tier exportable
The name for the keys will be:test-3tier
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:1024
% Generating 1024 bit RSA keys ...[OK]
```

2. Configure the trustpoint:

```
webvpn(config)# crypto pki trustpoint test-3tier
webvpn(ca-trustpoint)# serial-number
webvpn(ca-trustpoint)# password cisco
webvpn(ca-trustpoint)# subject CN=test-3tier, OU=hss, O=Cisco
webvpn(ca-trustpoint)# rsakeypair test-3tier
webvpn(ca-trustpoint)# enrollment url tftp://10.1.1.3/test-3tier
webvpn(ca-trustpoint)# exit
```

3. Generate the certificate signing request (CSR) and send it to the TFTP server:

```
webvpn(config)# crypto pki enroll test-3tier
%
% Start certificate enrollment ..

% The subject name in the certificate will be:CN=test-3tier, OU=hss, O=Cisco
% The fully-qualified domain name in the certificate will be:ssl-proxy.cisco.com
% The subject name in the certificate will be:ssl-proxy.cisco.com
% The serial number in the certificate will be:B0FFF22E
% Include an IP address in the subject name? [no]:
Send Certificate Request to tftp server? [yes/no]:yes
% Certificate request sent to TFTP Server
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificate' command will also show the fingerprint.

webvpn(config)# Fingerprint: 19B07392 319B2ACF F8FABE5C 52798971

webvpn(config)#
!!
```

4. Use the CSR to acquire the SSL certificate offline from the third-level certificate authority.

5. Authenticate the three certificate authorities (one root and two subordinate certificate authorities):

```
webvpn(config)# crypto pki trustpoint test-1tier
webvpn(ca-trustpoint)# enrollment url tftp://10.1.1.3/test-1tier
webvpn(ca-trustpoint)# revocation-check none
webvpn(ca-trustpoint)# exit
webvpn(config)# crypto pki authenticate test-1tier
Loading test-1tier.ca from 10.1.1.3 (via Ethernet0/0.172):!
[OK - 1046 bytes]

Certificate has the following attributes:
Fingerprint:AC6FC55E CC29E891 0DC3FAAA B4747C10
% Do you accept this certificate? [yes/no]:yes
Trustpoint CA certificate accepted.

webvpn(config)# crypto pki trustpoint test-2tier
webvpn(ca-trustpoint)# enrollment url tftp://10.1.1.3/test-2tier
webvpn(ca-trustpoint)# revocation-check none
webvpn(ca-trustpoint)# exit
webvpn(config)# crypto pki authenticate test-2tier
Loading test-2tier.ca from 10.1.1.3 (via Ethernet0/0.172):!
[OK - 1554 bytes]

Certificate has the following attributes:
Fingerprint:50A986F6 B471B82D E11B71FE 436A9BE6
Certificate validated - Signed by existing trustpoint CA certificate.
Trustpoint CA certificate accepted.

webvpn(config)# crypto pki authenticate test-3tier
Loading test-3tier.ca from 10.1.1.3 (via Ethernet0/0.172):!
[OK - 1545 bytes]

Certificate has the following attributes:
Fingerprint:2F2E44AC 609644FA 5B4B6B26 FDBFE569
Certificate validated - Signed by existing trustpoint CA certificate.
Trustpoint CA certificate accepted.
```

6. Import the server certificate:

```
webvpn(config)# crypto pki import test-3tier certificate
% The fully-qualified domain name in the certificate will be:ssl-proxy.cisco.com
Retrieve Certificate from tftp server? [yes/no]:yes
% Request to retrieve Certificate queued

webvpn(config)#
Loading test-3tier.crt from 10.1.1.3 (via Ethernet0/0.172):!
[OK - 1608 bytes]

webvpn(config)#
*Nov 25 21:52:36.299:%CRYPTO-6-CERTRET:Certificate received from Certificate Authority
webvpn(config)# ^Z
```

Example 4: Configuring Certificate Enrollment Using Cut-and-Paste (Three-Tier Certificate Authority)

1. Generate the RSA key pair:

```
webvpn(config)# crypto key generate rsa general-keys label tp-proxy1 exportable
The name for the keys will be:tp-proxy1
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:1024
% Generating 1024 bit RSA keys ...[OK]
```

2. Configure the trustpoint:

```
webvpn(config)# crypto pki trustpoint tp-proxy1
webvpn(ca-trustpoint)# enrollment ter
webvpn(ca-trustpoint)# rsakeypair tp-proxy1
webvpn(ca-trustpoint)# serial
webvpn(ca-trustpoint)# subject-name CN=test
webvpn(ca-trustpoint)# exit
```

3. Request a certificate for the trustpoint:

```
webvpn(config)# crypto pki enroll tp-proxy1
% Start certificate enrollment ..

% The subject name in the certificate will be:CN=test
% The fully-qualified domain name in the certificate will be:ssl-proxy.
% The subject name in the certificate will be:ssl-proxy.
% The serial number in the certificate will be:B0FFF14D
% Include an IP address in the subject name? [no]:no
Display Certificate Request to terminal? [yes/no]:yes
Certificate Request follows:

MIIBnDCCAQUCAQAwOzENMAsGA1UEAxMEdGVzdDEqMA8GA1UEBRMIQjBGRkYxNEQw
FwYJKoZIhvcNAQkCFgpzc2wtcHJveHkuMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCB
iQKBgQDFx1ol9IXoAx4fyUhaXH6s4p5t9soIZ1gvLtVX6Fp6zfuX47os5TGJH/IX
zV9B4e5Kv+wlMD0AvTh+/tvyAP3TMpCdpHYosd2VaTIgExpHf4M5Ruh8IebVKV25
rraIpNiS0PvPLFcrw4UfJVNpsc2XBxBhpT+FS9y67LqlhfSN4wIDAQABoCEwHwYJ
KoZIhvcNAQkOMRIwEDAOBgNVHQ8BAf8EBAMCBaAwDQYJKoZIhvcNAQEEBQADgYEA
kOIjd1KNJdKLMf33YELRd3MW/ujJIuiT1J8RYVbw1eE8JQf68TTdKiYqzQcoMgsp
ez3vSPxXFZ/c6naXdVyrTikTX3GZ1mu+UOvV6/Jaf5QcXa9tAi3fgyguV7jQMPjk
Qj2GrwhXjcqZGOMBh6Kq6s5UPsIDgrL036I42B6B3EQ=

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:no
```

4. Get the certificate request from Step 3 signed by a third-level certificate authority.

5. Define and import all certificate authorities (one root and two subordinate certificate authorities).

   a. Define two trustpoints for root certificate authority and subordinate 1 certificate authority.

Note The display in this procedure uses **tp-proxy1** to import the subordinate 2 certificate authority certificate.

```
webvpn(config)# crypto pki trustpoint 3tier-root
webvpn(ca-trustpoint)# enrollment terminal
webvpn(ca-trustpoint)# crl op
webvpn(ca-trustpoint)# exit
webvpn(config)# crypto pki trustpoint 3tier-sub1
webvpn(ca-trustpoint)# enrollment terminal
webvpn(ca-trustpoint)# crl op
webvpn(ca-trustpoint)# exit
```

   b. Import the root certificate authority certificate:

```
webvpn(config)# crypto pki authenticate 3tier-root

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIC1zCCAoGgAwIBAgIQadUxzU/i97hDmZRYJ1bBcDANBgkqhkiG9w0BAQUFADB1
```

```
MQswCQYDVQQGEwJVUzETMBEGA1UECBMKY2FsaWZvcm5pYTERMA8GA1UEBxMIc2Fu
IGpvc2UxDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwNoc3MxIDAeBgNVBAMTF3Np
bXBzb24tZGV2dGVzdC1yb290LUNBMB4XDTAzMTExMTIxNDgwMloXDTEzMTExMTIx
NTczOVowdTELMAkGA1UEBhMCVVMxEzARBgNVBAgTCmNhbGlmb3JuaWExETAPBgNV
BAcTCHNhbiBqb3NlMQ4wDAYDVQQKEwVjaXNjbzEMMAoGA1UECxMDaHNzMSAwHgYD
VQQDExdzaW1wc29uLWRldnRlc3Qtcm9vdC1DQTBcMA0GCSqGSIb3DQEBAQUAA0sA
MEgCQQCWEibAnUlVqQNUn0Wb94qnHi8FKjmVhibLHGRl6J+V7gHgzmF2MTz5WP5l
VQ2/1NVu0HjUORRdeCm1/raKJ/7ZAgMBAAGjgewwgekwCwYDVR0PBAQDAgHGMA8G
A1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFCYGLUBTKNd9EgUonHnoSvbHg0axMIGX
BgNVHR8EgY8wgYwwQ6BBoD+GPWh0dHA6Ly9jaXNjby1sOGo2b2hwbnIvQ2VydEVu
cm9sbC9zaW1wc29uLWRldnRlc3Qtcm9vdC1DQS5jcmwwRaBDoEGGP2ZpbGU6Ly9c
XGNpc2NvLWw4ajZvaHBuclxDZXJ0RW5yb2xsXHNpbXBzb24tZGV2dGVzdC1yb290
LUNBLmNybDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQUFAANBACBqe1wy
YjalelGZqLVu4bDVMFo6ELCV2AMBgi41K3ix+Z/03PJd7ct2BIAF4lktv9pCe6IO
EoBcmZteA+TQcKg=
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint:AC6FC55E CC29E891 0DC3FAAA B4747C10
% Do you accept this certificate? [yes/no]:yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

c. Import the subordinate 1 certificate authority certificate:

```
webvpn(config)# crypto pki authenticate 3tier-sub1

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIETzCCA/mgAwIBAgIKGj0cBwAAAAAADjANBgkqhkiG9w0BAQUFADB1MQswCQYD
VQQGEwJVUzETMBEGA1UECBMKY2FsaWZvcm5pYTERMA8GA1UEBxMIc2FuIGpvc2Ux
DjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwNoc3MxIDAeBgNVBAMTF3NpbXBzb24t
ZGV2dGVzdC1yb290LUNBMB4XDTAzMTExMzIyMDQyMVoXDTA0MTExMzIyMTQyMVow
dTELMAkGA1UEBhMCVVMxEzARBgNVBAgTCmNhbGlmb3JuaWExETAPBgNVBAcTCHNh
biBqb3NlMQ4wDAYDVQQKEwVjaXNjbzEMMAoGA1UECxMDaHNzMSAwHgYDVQQDExdz
aW1wc29uLWRldnRlc3Qtc3ViMS1jYTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDc
vV48nC2uukoSyGJ/GymCIEXZzMSzpbkYS7eWPaZYyiJDhCIKuUsMgFDRNfMQmUSA
rcWmPizFZc9PFumDa03vAgMBAAGjggJpMIICZTAQBgkrBgEEAYI3FQEEAwIBADAd
BgNVHQ4EFgQUWaaNN2U14BaBoU9mY+ncuHpP920wCwYDVR0PBAQDAgHGMA8GA1Ud
EwEB/wQFMAMBAf8wga4GA1UdIwSBpjCBo4AUJgYtQFMo130SBSiceehK9seDRrGh
eaR3MHUxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpjYWxpZm9ybmlhMREwDwYDVQQH
EwhzYW4gam9zZTEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA2hzczEgMB4GA1UE
AxMXc2ltcHNvbi1kZXZ0ZXN0LXJvb3QtQ0GCEGnVMc1P4ve4Q5mUWCdWwXAwgZcG
A1UdHwSBjzCBjDBDoEGgP4Y9aHR0cDovL2Npc2NvLWw4ajZvaHBuci9DZXJ0RW5y
b2xsL3NpbXBzb24tZGV2dGVzdC1yb290LUNBLmNybDBFoEOgQYY/ZmlsZTovL1xc
Y2lzY28tbDhqNm9ocG5yXENlcnRFbnJvbGxcc2ltcHNvbi1kZXZ0ZXN0LXJvb3Qt
Q0EuY3JsMIHIBggrBgEFBQcBAQSBuzCBuDBZBggrBgEFBQcwAoZNaHR0cDovL2Np
c2NvLWw4ajZvaHBuci9DZXJ0RW5yb2xsL2Npc2NvLWw4ajZvaHBucl9zaW1wc29u
LWRldnRlc3Qtcm9vdC1DQS5jcnQwWwYIKwYBBQUHMAKGT2ZpbGU6Ly9cXGNpc2Nv
LWw4ajZvaHBuclxDZXJ0RW5yb2xsXGNpc2NvLWw4ajZvaHBucl9zaW1wc29uLWRl
dnRlc3Qtcm9vdC1DQS5jcnQwDQYJKoZIhvcNAQEFBQADQQA6kAV3Jx/BOr2hlSp9
ER36ZkDJNIW93gNt2MkpcA07RmcrHln6q5RJ9WbvTxFnONdgpsag1EcOwn97XErH
Z2ow
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint:50A986F6 B471B82D E11B71FE 436A9BE6
Certificate validated - Signed by existing trustpoint CA certificate.
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

d. Import the subordinate 2 certificate authority certificate:

```
webvpn(config)# crypto pki authenticate tp-proxy1

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIESTCCA/OgAwIBAgIKHyiFxAAAAAAABjANBgkqhkiG9w0BAQUFADB1MQswCQYD
VQQGEwJVUzETMBEGA1UECBMKY2FsaWZvcm5pYTERMA8GA1UEBxMIc2FuIGpvc2Ux
DjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwNoc3MxIDAeBgNVBAMTF3NpbXBzb24t
ZGV2dGVzdC1zdWIxLWNhMB4XDTAzMTExMzIyMjI1MloXDTA0MTExMzIyMTQyMVow
dTELMAkGA1UEBhMCVVMxEzARBgNVBAgTCmNhbGlmb3JuaWExETAPBgNVBAcTCHNh
biBqb3NlMQ4wDAYDVQQKEwVjaXNjbzEMMAoGA1UECxMDaHNzMSAwHgYDVQQDExdz
aW1wc29uLWRldnRlc3Qtc3ViMi1jYTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQC7
ChZc0NYLBHf1sr/3Z4y6w5WoeioIpCOCSydhnbd5wnwuethoyStVt9lr6i61jWKl
d68Z8EoTg71daiV/WR/HAgMBAAGjggJjMIICXzAQBgkrBgEEAYI3FQEEAwIBADAd
BgNVHQ4EFgQU6FmJopqqzpbFMj6TaB2/wjlWlqEwCwYDVR0PBAQDAgHGMA8GA1Ud
EwEB/wQFMAMBAf8wgagGA1UdIwSBoDCBnYAUWaaNN2U14BaBoU9mY+ncuHpP922h
eaR3MHUxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpjYWxpZm9ybmlhMREwDwYDVQQH
EwhzYW4gam9zZTEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA2hzczEgMB4GA1UE
AxMXc2ltcHNvbi1kZXZ0ZXN0LXJvb3QtQ0GCCho9HAcAAAAAAA4wgZcGA1UdHwSB
jzCBjDBDoEGgP4Y9aHR0cDovL2Npc2NvLWcyNXVhNm80ZS9DZXJ0RW5yb2xsL3Np
bXBzb24tZGV2dGVzdC1zdWIxLWNhLmNybDBFoEOgQYY/ZmlsZTovL1xcY2lzY28t
ZzI1dWE2bzRlXENlcnRFbnJvbGxcc2ltcHNvbi1kZXZ0ZXN0LXN1YjEtY2EuY3Js
MIHIBggrBgEFBQcBAQSBuzCBuDBZBggrBgEFBQcwAoZNaHR0cDovL2Npc2NvLWcy
NXVhNm80ZS9DZXJ0RW5yb2xsL2Npc2NvLWcyNXVhNm80ZV9zaW1wc29uLWRldnRl
c3Qtc3ViMS1jYS5jcnQwWwYIKwYBBQUHMAKGT2ZpbGU6Ly9cXGNpc2NvLWcyNXVh
Nm80ZVxDZXJ0RW5yb2xsXGNpc2NvLWcyNXVhNm80ZV9zaW1wc29uLWRldnRlc3Qt
c3ViMS1jYS5jcnQwDQYJKoZIhvcNAQEFBQADQQCieB8rvVCqVF2cFw9/v51jGn7L
Q6pUGT3bMRbOrgQKytTz/Yx09156nYZHrvVuLzmzz5CriI2saVx+q1Tarwil
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint:2F2E44AC 609644FA 5B4B6B26 FDBFE569
Certificate validated - Signed by existing trustpoint CA certificate.
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

e. Import the server certificate:

```
webvpn(config)# crypto pki import tp-proxy1 certificate
% The fully-qualified domain name in the certificate will be:ssl-proxy.

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIENTCCA9+gAwIBAgIKLmibDwAAAAAACDANBgkqhkiG9w0BAQUFADB1MQswCQYD
VQQGEwJVUzETMBEGA1UECBMKY2FsaWZvcm5pYTERMA8GA1UEBxMIc2FuIGpvc2Ux
DjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwNoc3MxIDAeBgNVBAMTF3NpbXBzb24t
ZGV2dGVzdC1zdWIyLWNhMB4XDTAzMTExOTIzNDUzNVoXDTA0MTExMzIyMTQyMVow
PTERMA8GA1UEBRMIQjBGRkYxNEQxGTAXBgkqhkiG9w0BCQITCnNzbC1wcm94eS4x
DTALBgNVBAMTBHRlc3QwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMXHWiX0
hegDHh/JSFpcfqzinm32yghnWC8u1VfoWnrN+5fjuizlMYkf8hfNX0Hh7kq/7CUw
Af8EBAMCBaAwHQYDVR0OBBYEFCXlzcYHyo1PNbfubnivi8d2VO22MIGoBgNVHSME
gaAwgZ2AFOhZiaKaqs6WxTI+k2gdv8I5VpahoXmkdzB1MQswCQYDVQQGEwJVUzET
MBEGA1UECBMKY2FsaWZvcm5pYTERMA8GA1UEBxMIc2FuIGpvc2UxDjAMBgNVBAoT
BWNpc2NvMQwwCgYDVQQLEwNoc3MxIDAeBgNVBAMTF3NpbXBzb24tZGV2dGVzdC1z
dWIxLWNhggofKIXEAAAAAAAGMIGXBgNVHR8EgY8wgYwwQ6BBoD+GPWh0dHA6Ly9j
aXNjby1vam14Y25jenYvQ2VydEVucm9sbC9zaW1wc29uLWRldnRlc3Qtc3ViMi1j
YS5jcmwwRaBDoEGGP2ZpbGU6Ly9cXGNpc2NvLW9qbXhjbmN6dlxDZXJ0RW5yb2xs
XHNpbXBzb24tZGV2dGVzdC1zdWIyLWNhLmNybDCByAYIKwYBBQUHAQEEgbswgbgw
WQYIKwYBBQUHMAKGTWh0dHA6Ly9jaXNjby1vam14Y25jenYvQ2VydEVucm9sbC9j
```

```
aXNjby1vam14Y25jenZfc2ltcHNvbi1kZXZ0ZXN0LXN1YjItY2EuY3J0MFsGCCsG
AQUFBzAChk9maWxlOi8vXFxjaXNjby1vam14Y25jenZcQ2VydEVucm9sbFxjaXNj
by1vam14Y25jenZfc2ltcHNvbi1kZXZ0ZXN0LXN1YjItY2EuY3J0MA0GCSqGSIb3
DQEBBQUAA0EAtbxmUBOxZ/hcrCc3hY7pa6q/LmLonXSL8cjAbV2I7A5QGYaNi5k9
8FlEz1WOxW0J2C3/YsvIf4dYpsQWdKRJbQ==
-----END CERTIFICATE-----

% Router Certificate successfully imported

webvpn(config)#^Z
```

Importing and Exporting Key Pairs and Certificates

You can import and export key pairs and certificates using either the PKCS12 file format or privacy-enhanced mail (PEM) file format.

This section descrbies how to import or export key pairs and certificates:

- Importing and Exporting a PKCS12 File, page 3-43
- Importing and Exporting PEM Files, page 3-44

Note A test PKCS12 file (testssl.p12) is embedded in the WebVPN software on the WebVPN Services Module. You can install the file into Flash for testing purposes and for proof of concept. After the PKCS12 file is installed, you can import it to a trustpoint and then assign it to a WebVPN gateway configured for testing.

Note If the certificate revocation list (CRL) fails to download because the CRL server is unreachable or the CRL download path does not exist, the certificate might fail to import. You should make sure all trustpoints that are linked to the import process are able to download the CRL. If the CRL path does not exist, or if the CRL server is unreachable, then you should enter the **revocation-check none** command for all trustpoints that are linked to the import process. Enter the **show crypto pki certificates** command to display information for all certificates, and obtain a list of associated trustpoints from the display of the certificate authority certificate. Enter the **revocation-check none** command for all these trustpoints.

For example, in a three-tier certificate authority hierarchy (root CA, subordinate CA1, and subordinate CA2), when you import the subordinate CA1 certificate, enter the **revocation-check none** command for all the trustpoints associated with root CA. Similarly, when you import the subordinate CA2 certificate, enter the **revocation-check none** command for all the trustpoints associated with root CA and subordinate CA1.

After you successfully import the certificate, you can restore the original CRL options on the trustpoints.

Importing and Exporting a PKCS12 File

You can use an external PKI system to generate a PKCS12 file and then import this file to the WebVPN Services Module.

Note When creating a PKCS12 file, include the entire certificate chain, from the server certificate to the root certificate, and public and private keys. You can also generate a PKCS12 file from the WebVPN Services Module and export it.

Note If you are using SSH, we recommend using secure file transfer (SCP) when importing or exporting a PKCS12 file. SCP authenticates the host and encrypts the transfer session.

To import or export a PKCS12 file, perform this task:

Command	Purpose
webvpn(config)# **crypto pki** {**import** | **export**} *trustpoint_label* **pkcs12** {**scp:**| **ftp:**| **nvram:**| **rcp:**| **tftp:**} [*pkcs12_filename*[1]] *pass_phrase*[2]	Imports or exports a PKCS12 file. **Note** You do not need to configure a trustpoint before importing the PKCS12 file. Importing keys and certificates from a PKCS12 file creates the trustpoint automatically, if it does not already exist.

[1] If you do not specify the *pkcs12_filename* value, you will be prompted to accept the default filename (the default filename is the *trustpoint_label* value) or enter the filename. For **ftp:** or **tftp:**, include the full path in the *pkcs12_filename* value.

[2] You will receive an error if you enter the pass phrase incorrectly.

This example shows how to import a PKCS12 file using SCP:

```
webvpn(config)# crypto pki import TP2 pkcs12 scp: sky is blue
Address or name of remote host []? 10.1.1.1
Source username [ssl-proxy]? admin-1
Source filename [TP2]? /users/admin-1/pkcs12/TP2.p12

Password:password
Sending file modes:C0644 4379 TP2.p12
!
webvpn(config)#
*Aug 22 12:30:00.531:%CRYPTO-6-PKCS12IMPORT_SUCCESS:PKCS #12 Successfully Imported.
webvpn(config)#
```

This example shows how to export a PKCS12 file using SCP:

```
webvpn(config)# crypto pki export TP1 pkcs12 scp: sky is blue
Address or name of remote host []? 10.1.1.1
Destination username [ssl-proxy]? admin-1
Destination filename [TP1]? TP1.p12

Password:

Writing TP1.p12 Writing pkcs12 file to scp://admin-1@10.1.1.1/TP1.p12

Password:
!
CRYPTO_PKI:Exported PKCS12 file successfully.
webvpn(config)#
```

This example shows how to import a PKCS12 file using FTP:

```
webvpn(config)# crypto pki import TP2 pkcs12 ftp: sky is blue
Address or name of remote host []? 10.1.1.1
Source filename [TP2]? /admin-1/pkcs12/PK-1024
Loading /admin-1/pkcs12/PK-1024 !
[OK - 4339/4096 bytes]
webvpn(config)#
```

This example shows how to export a PKCS12 file using FTP:

```
webvpn(config)# crypto pki export TP1 pkcs12 ftp: sky is blue
Address or name of remote host []? 10.1.1.1
Destination filename [TP1]? /admin-1/pkcs12/PK-1024
Writing pkcs12 file to ftp://10.1.1.1//admin-1/pkcs12/PK-1024

Writing /admin-1/pkcs12/PK-1024 !!
CRYPTO_PKI:Exported PKCS12 file successfully.
webvpn(config)#
```

After you import the PKCS12 file, see the "Verifying Certificates and Trustpoints" section on page 3-50 to verify the certificate and trustpoint information.

Importing and Exporting PEM Files

Note The **crypto pki import pem** command imports only the private key (.prv), the server certificate (.crt), and the issuer certificate authority certificate (.ca). If you have more than one level of certificate authority in the certificate chain, you need to import the root and subordinate certificate authority certificates before this command is issued for authentication. Use cut-and-paste or TFTP to import the root and subordinate certificate authority certificates.

Note Imported key pairs cannot be exported.

Note If you are using SSH, we recommend using SCP when importing or exporting PEM files. SCP authenticates the host and encrypts the transfer session.

To import or export PEM files, perform one of these tasks:

Command	Purpose
webvpn(config)# **crypto pki import** *trustpoint_label* **pem** [**exportable**] {**terminal** | **url** {**scp:**| **ftp:**| **nvram:**| **rcp:**| **tftp:**} | **usage-keys**} *pass_phrase*[1,2]	Imports PEM files. **Note** You do not need to configure a trustpoint before importing the PEM files. Importing keys and certificates from PEM files creates the trustpoint automatically, if it does not already exist.
webvpn(config)# **crypto pki export** *trustpoint_label* **pem** {**terminal** | **url** {**scp:**| **ftp:**| **nvram:**| **rcp:**| **tftp:**} [**des** | **3des**] *pass_phrase*[1,2]	Exports PEM files. **Note** Only the key, the server certificate, and the issuer certificate authority of the server certificate are exported. All higher level certificate authorities need to be exported using cut-and-paste of TFTP.

[1] You will receive an error if you enter the pass phrase incorrectly.

[2] A pass phrase protects a PEM file that contains a private key. The PEM file is encrypted by DES or 3DES. The encryption key is derived from the pass phrase. A PEM file containing a certificate is not encrypted and is not protected by a pass phrase.

This example shows how to import PEM files using TFTP:

Note The TP5.ca, TP5.prv, and TP5.crt files should be present on the server.

```
webvpn(config)# crypto pki import TP5 pem url tftp://10.1.1.1/TP5 password
% Importing CA certificate...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.ca]?
Reading file from tftp://10.1.1.1/TP5.ca
Loading TP5.ca from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 1976 bytes]

% Importing private key PEM file...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.prv]?
Reading file from tftp://10.1.1.1/TP5.prv
Loading TP5.prv from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 963 bytes]

% Importing certificate PEM file...
Address or name of remote host [10.1.1.1]?
Destination filename [TP5.crt]?
Reading file from tftp://10.1.1.1/TP5.crt
Loading TP5.crt from 10.1.1.1 (via Ethernet0/0.168): !
[OK - 1692 bytes]
% PEM files import succeeded.
webvpn(config)#end
webvpn#
*Apr 11 15:11:29.901: %SYS-5-CONFIG_I: Configured from console by console
```

This example shows how to export PEM files using TFTP:

```
webvpn(config)# crypto pki export TP5 pem url tftp://10.1.1.1/tp99 3des password
% Exporting CA certificate...
Address or name of remote host [10.1.1.1]?
Destination filename [tp99.ca]?
% File 'tp99.ca' already exists.
% Do you really want to overwrite it? [yes/no]: yes
!Writing file to tftp://10.1.1.1/tp99.ca!
% Key name: key1
    Usage: General Purpose Key
% Exporting private key...
Address or name of remote host [10.1.1.1]?
Destination filename [tp99.prv]?
% File 'tp99.prv' already exists.
% Do you really want to overwrite it? [yes/no]: yes
!Writing file to tftp://10.1.1.1/tp99.prv!
% Exporting router certificate...
Address or name of remote host [10.1.1.1]?
Destination filename [tp99.crt]?
% File 'tp99.crt' already exists.
% Do you really want to overwrite it? [yes/no]: yes
!Writing file to tftp://10.1.1.1/tp99.crt!
webvpn(config)#
```

After you import the PEM files, see the “Verifying Certificates and Trustpoints” section on page 3-50 to verify the certificate and trustpoint information.

Example of Importing PEM Files for Three Levels of Certificate Authority

In this section, the root certificate authority certificate (Tier 1) and intermediate certificate authority certificate (Tier 2) are obtained using the cut-and-paste option of the offline enrollment. The intermediate certificate authority certificate (Tier 3), private keys, and router certificate are obtained by importing PEM files.

1. Use cut-and-paste to obtain the root certificate authority-tier 1 certificate:

```
webvpn(config)# crypto pki trustpoint 3tier-root
webvpn(ca-trustpoint)# enrollment terminal
webvpn(ca-trustpoint)# revocation-check none
webvpn(ca-trustpoint)# exit
webvpn(config)# crypto pki authenticate 3tier-root

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIC1zCCAoGgAwIBAgIQadUxzU/i97hDmZRYJ1bBcDANBgkqhkiG9w0BAQUFADB1
MQswCQYDVQQGEwJVUzETMBEGA1UECBMKY2FsaWZvcm5pYTERMA8GA1UEBxMIc2Fu
IGpvc2UxDjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwNoc3MxIDAeBgNVBAMTF3Np
bXBzb24tZGV2dGVzdC1yb290LUNBMB4XDTAzMTExMTIxNDgwMloXDTEzMTExMTIx
NTczOVowdTELMAkGA1UEBhMCVVMxEzARBgNVBAgTCmNhbGlmb3JuaWExETAPBgNV
BAcTCHNhbiBqb3NlMQ4wDAYDVQQKEwVjaXNjbzEMMAoGA1UECxMDaHNzMSAwHgYD
VQQDExdzaW1wc29uLWRldnRlc3Qtcm9vdC1DQTBcMA0GCSqGSIb3DQEBAQUAA0sA
MEgCQQCWEibAnUlVqQNUn0Wb94qnHi8FKjmVhibLHGRl6J+V7gHgzmF2MTz5WP5l
VQ2/1NVu0HjUORRdeCm1/raKJ/7ZAgMBAAGjgewwgekwCwYDVR0PBAQDAgHGMA8G
A1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFCYGLUBTKNd9EgUonHnoSvbHg0axMIGX
BgNVHR8EgY8wgYwwQ6BBoD+GPWh0dHA6Ly9jaXNjby1sOGo2b2hwbnIvQ2VydEVu
cm9sbC9zaW1wc29uLWRldnRlc3Qtcm9vdC1DQS5jcmwwRaBDoEGGP2ZpbGU6Ly9c
XGNpc2NvLWw4ajZvaHBuclxDZXJ0RW5yb2xsXHNpbXBzb24tZGV2dGVzdC1yb290
LUNBLmNybDAQBgkrBgEEAYI3FQEEAwIBADANBgkqhkiG9w0BAQUFAANBACBqe1wy
YjalelGZqLVu4bDVMFo6ELCV2AMBgi41K3ix+Z/03PJd7ct2BIAF4lktv9pCe6IO
```

```
EoBcmZteA+TQcKg=
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint:AC6FC55E CC29E891 0DC3FAAA B4747C10
% Do you accept this certificate? [yes/no]:yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

2. Use cut-and-paste to obtain the subordinate certificate authority 1 certificate:

```
webvpn(config)# crypto pki trustpoint 3tier-subca1
webvpn(ca-trustpoint)# enroll terminal
webvpn(ca-trustpoint)# revocation-check none
webvpn(ca-trustpoint)# exit
webvpn(config)# crypto pki authenticate 3tier-subca1

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIETzCCA/mgAwIBAgIKGj0cBwAAAAAADjANBgkqhkiG9w0BAQUFADB1MQswCQYD
VQQGEwJVUzETMBEGA1UECBMKY2FsaWZvcm5pYTERMA8GA1UEBxMIc2FuIGpvc2Ux
DjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwNoc3MxIDAeBgNVBAMTF3NpbXBzb24t
ZGV2dGVzdC1yb290LUNBMB4XDTAzMTExMzIyMDQyMVoXDTA0MTExMzIyMTQyMVow
dTELMAkGA1UEBhMCVVMxEzARBgNVBAgTCmNhbGlmb3JuaWExETAPBgNVBAcTCHNh
biBqb3NlMQ4wDAYDVQQKEwVjaXNjbzEMMAoGA1UECxMDaHNzMSAwHgYDVQQDExdz
aW1wc29uLWRldnRlc3Qtc3ViMS1jYTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDc
vV48nC2uukoSyGJ/GymCIEXZzMSzpbkYS7eWPaZYyiJDhCIKuUsMgFDRNfMQmUSA
rcWmPizFZc9PFumDa03vAgMBAAGjggJpMIICZTAQBgkrBgEEAYI3FQEEAwIBADAd
BgNVHQ4EFgQUWaaNN2U14BaBoU9mY+ncuHpP920wCwYDVR0PBAQDAgHGMA8GA1Ud
EwEB/wQFMAMBAf8wga4GA1UdIwSBpjCBo4AUJgYtQFMo130SBSiceehK9seDRrGh
eaR3MHUxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpjYWxpZm9ybmlhMREwDwYDVQQH
EwhzYW4gam9zZTEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA2hzczEgMB4GA1UE
AxMXc2ltcHNvbi1kZXZ0ZXN0LXJvb3QtQ0GCEGnVMc1P4ve4Q5mUWCdWwXAwgZcG
A1UdHwSBjzCBjDBDoEGgP4Y9aHR0cDovL2Npc2NvLWw4ajZvaHBuci9DZXJ0RW5y
b2xsL3NpbXBzb24tZGV2dGVzdC1yb290LUNBLmNybDBFoEOgQYY/ZmlsZTovL1xc
Y2lzY28tbDhqNm9ocG5yXENlcnRFbnJvbGxcc2ltcHNvbi1kZXZ0ZXN0LXJvb3Qt
Q0EuY3JsMIHIBggrBgEFBQcBAQSBuzCBuDBZBggrBgEFBQcwAoZNaHR0cDovL2Np
c2NvLWw4ajZvaHBuci9DZXJ0RW5yb2xsL2Npc2NvLWw4ajZvaHBucl9zaW1wc29u
LWRldnRlc3Qtcm9vdC1DQS5jcnQwWwYIKwYBBQUHMAKGT2ZpbGU6Ly9cXGNpc2Nv
LWw4ajZvaHBuclxDZXJ0RW5yb2xsXGNpc2NvLWw4ajZvaHBucl9zaW1wc29uLWRl
dnRlc3Qtcm9vdC1DQS5jcnQwDQYJKoZIhvcNAQEFBQADQQA6kAV3Jx/BOr2hlSp9
ER36ZkDJNIW93gNt2MkpcA07RmcrHln6q5RJ9WbvTxFnONdgpsag1EcOwn97XErH
Z2ow
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint:50A986F6 B471B82D E11B71FE 436A9BE6
Certificate validated - Signed by existing trustpoint CA certificate.
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

3. Import the subordinate certificate authority 2 certificate, the RSA key pair, and router certificate. The router certificate should be signed by the subordinate certificate authority 2.

```
webvpn(config)# crypto pki import tp-proxy1 pem terminal cisco
% Enter PEM-formatted CA certificate.
% End with a blank line or "quit" on a line by itself.
-----BEGIN CERTIFICATE-----
MIIESTCCA/OgAwIBAgIKHyiFxAAAAAAABjANBgkqhkiG9w0BAQUFADB1MQswCQYD
VQQGEwJVUzETMBEGA1UECBMKY2FsaWZvcm5pYTERMA8GA1UEBxMIc2FuIGpvc2Ux
DjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwNoc3MxIDAeBgNVBAMTF3NpbXBzb24t
ZGV2dGVzdC1zdWIxLWNhMB4XDTAzMTExMzIyMjI1MloXDTA0MTExMzIyMTQyMVow
```

```
dTELMAkGA1UEBhMCVVMxEzARBgNVBAgTCmNhbGlmb3JuaWExETAPBgNVBAcTCHNh
biBqb3NlMQ4wDAYDVQQKEwVjaXNjbzEMMAoGA1UECxMDaHNzMSAwHgYDVQQDExdz
aW1wc29uLWRldnRlc3Qtc3ViMi1jYTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQC7
ChZc0NYLBHf1sr/3Z4y6w5WoeioIpCOCSydhnbd5wnwuethoyStVt9lr6i61jWKl
d68Z8EoTg71daiV/WR/HAgMBAAGjggJjMIICXzAQBgkrBgEEAYI3FQEEAwIBADAd
BgNVHQ4EFgQU6FmJopqqzpbFMj6TaB2/wjlWlqEwCwYDVR0PBAQDAgHGMA8GA1Ud
EwEB/wQFMAMBAf8wgagGA1UdIwSBoDCBnYAUWaaNN2U14BaBoU9mY+ncuHpP922h
eaR3MHUxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpjYWxpZm9ybmlhMREwDwYDVQQH
EwhzYW4gam9zZTEOMAwGA1UEChMFY2lzY28xDDAKBgNVBAsTA2hzczEgMB4GA1UE
AxMXc2ltcHNvbi1kZXZ0ZXN0LXJvb3QtQ0GCCho9HAcAAAAAAA4wgZcGA1UdHwSB
jzCBjDBDoEGgP4Y9aHR0cDovL2Npc2NvLWcyNXVhNm80ZS9DZXJ0RW5yb2xsL3Np
bXBzb24tZGV2dGVzdC1zdWIxLWNhLmNybDBFoEOgQYY/ZmlsZTovL1xcY2lzY28t
ZzI1dWE2bzRlXENlcnRFbnJvbGxcc2ltcHNvbi1kZXZ0ZXN0LXN1YjEtY2EuY3Js
MIHIBggrBgEFBQcBAQSBuzCBuDBZBggrBgEFBQcwAoZNaHR0cDovL2Npc2NvLWcy
NXVhNm80ZS9DZXJ0RW5yb2xsL2Npc2NvLWcyNXVhNm80ZV9zaW1wc29uLWRldnRl
c3Qtc3ViMS1jYS5jcnQwWwYIKwYBBQUHMAKGT2ZpbGU6Ly9cXGNpc2NvLWcyNXVh
Nm80ZVxDZXJ0RW5yb2xsXGNpc2NvLWcyNXVhNm80ZV9zaW1wc29uLWRldnRlc3Qt
c3ViMS1jYS5jcnQwDQYJKoZIhvcNAQEFBQADQQCieB8rvVCqVF2cFw9/v51jGn7L
Q6pUGT3bMRbOrgQKytTz/Yx09156nYZHrvVuLzmzz5CriI2saVx+q1Tarwil
-----END CERTIFICATE-----

% Enter PEM-formatted encrypted private key.
% End with "quit" on a line by itself.
-----BEGIN RSA PRIVATE KEY-----
Proc-Type:4,ENCRYPTED
DEK-Info:DES-EDE3-CBC,F0D3269840071CF8

gQb9JMplIE5AEdhumLuBFWT53k+L/EGLhFfQn/roPlEOiIGEB6y3DeYNN/xZSiy3
JOHN0kh8Wjw3pshrdNVcoQj2X7BPI+YOipok40WOk5J/+dnRLwMjv+rl0tr+LcCk
nBdR8zIOkOJObULLUOXFBM7oB3Dsk4Y3FBv8EAR3AdQiZjevau4FIyQn+JfVZy+J
wctmvZnX0c0fevPsgID4dCPkeY6+I0DkxMyRiuyn+wIrJw1xVA2VIOrRJojBNlRu
6/APef8JwpfnNcgpcLYt/4Q+3Yjl9EfRLjgiL6eSRki/6K5lrV3eKbwOTyjvXq5h
G0Q6dtNEoIvOg1Vad0CXeL+TxJ4ySq4E63OxIHkclDBsusGoUGLoZ+OtaxApAZ+5
WbKqR+ND1LlPmS8/ZL9LMPhUh9eOqZJjJTe6NbxY7jeNHjAmpP7/WpB2f2kV/LZg
n2AV4GALBZtqXtreGiayZzXpEA5J00lbzRZWf9JHA1diz/unW00/GH9LvCqA9O15
YJGCrRMI9US7MWm8kIkiJqNgLtbPad5cOaieQe+Kncgcm18Hc7pfhDwXGG4RS40x
TSV/kIR4Gi7h8Lu71wZKTaWYHBPTUyTIpNsFUEdvItHXOSBw2LWNWzdYgpGoMT/t
ryuu0lAC9YdBalAxY0DaqqpuXKzxfiw5QDbqZWVq3qAxXfLAtTgu/gFCuFQvbBGl
87H1C+nOQUq2nkpMpHZLsl3V0w/2yqg+q6rUydANFF+a5vRaLgX/PGms92ZkZUdP
Z5qeKJmoURSlMYxDuhQDl93RYxXJxOYIYrCrI/QaBpIH6QvUH60wWA==
-----END RSA PRIVATE KEY-----
quit
% Enter PEM-formatted certificate.
% End with a blank line or "quit" on a line by itself.
-----BEGIN CERTIFICATE-----
MIIEXTCCBAegAwIBAgIKTJOcWgAAAAAACTANBgkqhkiG9w0BAQUFADB1MQswCQYD
VQQGEwJVUzETMBEGA1UECBMKY2FsaWZvcm5pYTERMA8GA1UEBxMIc2FuIGpvc2Ux
DjAMBgNVBAoTBWNpc2NvMQwwCgYDVQQLEwNoc3MxIDAeBgNVBAMTF3NpbXBzb24t
ZGV2dGVzdC1zdWIyLWNhMB4XDTAzMTEyNTIwMjExMFoXDTA0MTExMzIyMTQyMVow
PjERMA8GA1UEBRMIQjBGRkYyMkUxKTAnBgkqhkiG9w0BCQITGnNpbXBzb24tNjUw
OS1zdGUuY2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCkhRKm
38hSF7l0WXlYm8ixs2Hz/yjNw7tchtRPIp0qCTJKW00gzZpp8dqaNi3s2GVVWb+t
Cgsol0MZLIkyoj/9vT9MC7Zo3LOxYy9kD+6M9peUWMT4JLSD4Exzxsd87JpP1bo0
o8WhYjvMor/bL30sW8ly2RH2vppEMn9eLEN0vwIDAQABo4ICajCCAmYwCwYDVR0P
BAQDAgWgMB0GA1UdDgQWBBSx6uQ2sARlcjzhBSiMu7xeu1n6AjCBqAYDVR0jBIGg
MIGdgBToWYmimqrOlsUyPpNoHb/COVaWoaF5pHcwdTELMAkGA1UEBhMCVVMxEzAR
BgNVBAgTCmNhbGlmb3JuaWExETAPBgNVBAcTCHNhbiBqb3NlMQ4wDAYDVQQKEwVj
aXNjbzEMMAoGA1UECxMDaHNzMSAwHgYDVQQDExdzaW1wc29uLWRldnRlc3Qtc3Vi
MS1jYYIKHyiFxAAAAAAABjAoBgNVHREBAf8EHjAcghpzaW1wc29uLTY1MDktc3Rl
LmNpc2NvLmNvbTCBlwYDVR0fBIGPMIGMMEOgQaA/hj1odHRwOi8vY2lzY28tb2pt
eGNuY3p2L0NlcnRFbnJvbGwvc2ltcHNvbi1kZXZ0ZXN0LXN1YjItY2EuY3JsMEWg
Q6BBhj9maWxlOi8vXFxjaXNjby1vam14Y25jenZcQ2VydEVucm9sbFxzaW1wc29u
LWRldnRlc3Qtc3ViMi1jYS5jcmwwgcgGCCsGAQUFBwEBBIG7MIG4MFkGCCsGAQUF
BzAChk1odHRwOi8vY2lzY28tb2pteGNuY3p2L0NlcnRFbnJvbGwvY2lzY28tb2pt
```

```
eGNuY3p2X3NpbXBzb24tZGV2dGVzdC1zdWIyLWNhLmNydDBbBggrBgEFBQcwAoZP
ZmlsZTovL1xcY2lzY28tb2pteGNuY3p2XENlcnRFbnJvbGxcY2lzY28tb2pteGNu
Y3p2X3NpbXBzb24tZGV2dGVzdC1zdWIyLWNhLmNydDANBgkqhkiG9w0BAQUFAANB
ABFh7XeLwvfBtjAR+e5OaUH5KTGJDbeJppOmMFXnFakpgWop9Qg4cHRCQq7V0pAW
iA6VtJOmpYgEIVNTAzAAHR4=
-----END CERTIFICATE-----

% PEM files import succeeded.
webvpn(config)# ^Z
webvpn#
*Dec  4 18:11:49.850:%SYS-5-CONFIG_I:Configured from console by console
webvpn#
```

4. Display the certificate information (optional):

```
webvpn# show crypto pki certificates tp-proxy1
Certificate
  Status:Available
  Certificate Serial Number:04A0147B00000000010E
  Certificate Usage:General Purpose
  Issuer:
    CN = sub3ca
     C = US
Subject:
    Name:ssl-proxy.
    Serial Number:B0FFF0C2
    OID.1.2.840.113549.1.9.2 = ssl-proxy.
     OID.2.5.4.5 = B0FFF0C2
  CRL Distribution Point:
    http://sample.cisco.com/sub3ca.crl
  Validity Date:
    start date:18:04:09 UTC Jan 23 2003
    end   date:21:05:17 UTC Dec 12 2003
    renew date:00:00:00 UTC Apr 1 2003
  Associated Trustpoints:tp-proxy1

CA Certificate
  Status:Available
  Certificate Serial Number:6D1E6B0F000000000007
  Certificate Usage:Signature
  Issuer:
    CN = subtest
     C = US
Subject:
    CN = sub3ca
     C = US
CRL Distribution Point:
    http://sample.cisco.com/subtest.crl
  Validity Date:
    start date:22:22:52 UTC Mar 28 2003
    end   date:21:05:17 UTC Dec 12 2003
  Associated Trustpoints:tp-proxy1

webvpn# show crypto pki certificates 3tier-subca1
CA Certificate
  Status:Available
  Certificate Serial Number:29A47DEF0000000004E9
  Certificate Usage:Signature
  Issuer:
    CN = 6ebf9b3e-9a6d-4400-893c-dd85dcfe911b
     C = US
Subject:
    CN = subtest
     C = US
```

```
CRL Distribution Point:
    http://sample.cisco.com/6ebf9b3e-9a6d-4400-893c-dd85dcfe911b.crl
  Validity Date:
    start date:20:55:17 UTC Dec 12 2002
    end   date:21:05:17 UTC Dec 12 2003
  Associated Trustpoints:3tier-sub1

webvpn# show crypto pki certificates 3tier-root
CA Certificate
  Status:Available
  Certificate Serial Number:7FD5B209B5C2448C47F77F140625D265
  Certificate Usage:Signature
  Issuer:
    CN = 6ebf9b3e-9a6d-4400-893c-dd85dcfe911b
     C = US
Subject:
    CN = 6ebf9b3e-9a6d-4400-893c-dd85dcfe911b
     C = US
CRL Distribution Point:
    http://sample.cisco.com/6ebf9b3e-9a6d-4400-893c-dd85dcfe911b.crl
  Validity Date:
    start date:00:05:32 UTC Jun 13 2002
    end   date:00:11:58 UTC Jun 13 2004
  Associated Trustpoints:3tier-root
```

Verifying Certificates and Trustpoints

To verify information about your certificates and trustpoints, perform this task in EXEC mode:

	Command	Purpose
Step 1	`webvpn(ca-trustpoint)#` **`show crypto pki certificates`** [*`trustpoint_label`*]	Displays information about the certificates associated with the specified trustpoint, or all of your certificates, the certificates of the certificate authority, and registration authority certificates.
Step 2	`webvpn(ca-trustpoint)#` **`show crypto pki trustpoints`** [*`trustpoint_label`*]	Displays information about all trustpoints or the specified trustpoint.

Sharing Keys and Certificates

The WebVPN Services Module supports the sharing of the same key pair by multiple certificates. However, this is not a good practice because if one key pair is compromised, all the certificates must be revoked and replaced.

Because WebVPN gateways are added and removed at different times, the certificates also expire at different times. Some certificate authorities require you to refresh the key pair at the time of renewal. If certificates share one key pair, you need to renew the certificates at the same time. In general, it is easier to manage certificates if each certificate has its own key pair.

The WebVPN Services Module does not impose any restrictions on sharing certificates among multiple WebVPN gateways and multiple WebVPN Services Modules. The same trustpoint can be assigned to multiple WebVPN gateways.

From a business point of view, the certificate authority may impose restrictions (for example, on the number of servers in a server farm that can use the same certificate). There may be contractual or licensing agreements regarding certificate sharing. Consult with the certificate authority or the legal staff regarding business contractual aspects.

In practice, some web browsers compare the subject name of the server certificate with the hostname or the IP address that appears on the URL. If the subject name does not match the hostname or IP address, a dialog box appears, prompting the user to verify and accept the certificate. To avoid this step, limit the sharing of certificates based on the hostname or IP address.

Saving Your Configuration

Caution RSA key pairs are saved only to NVRAM. RSA keys are *not* saved with your configuration when you specify any other file system with the **copy system:running-config** *file_system***:** command.

Always remember to save your work when you make configuration changes.

To save your configuration to NVRAM, perform this task:

Command	Purpose
`webvpn# copy [/erase] system:running-config nvram:startup-config`	Saves the configuration, key pairs, and certificate to NVRAM. The key pairs are stored in the private configuration file, and each certificate is stored as a binary file in NVRAM. On bootup, the module will not need to query the certificate authority to obtain the certificates or to auto-enroll. **Note** For security reasons, we recommend that you enter the **/erase** option to erase the public and the private configuration files before updating the NVRAM. If you do not enter the **/erase** option, the key pairs from the old private configuration file may remain in the NVRAM. **Caution** When you enter the **/erase** option, both the current and the backup buffers in NVRAM are erased before the running configuration is saved into NVRAM. If a power failure or reboot occurs after the buffers are erased, but before the running configuration is saved, both configurations might be lost.

Note If you have a large number of files in NVRAM, this task may take up to 2 minutes to finish.

The automatic backup of the configuration to NVRAM feature automatically backs up the last saved configuration. If the current write process fails, the configuration is restored to the previous configuration automatically.

Verifying the Saved Configuration

To verify the saved configuration, perform this task:

	Command	Purpose
Step 1	`webvpn#` **`show startup-config`**	Displays the startup configuration.
Step 2	`webvpn#` **`directory nvram:`**	Displays the names and sizes of the files in NVRAM.

Note With the maximum number or WebVPN gateways and certificates configured, the output takes up to 7 minutes to display.

Erasing the Saved Configuration

To erase a saved configuration, perform one of these tasks:

Command	Purpose
`webvpn#` **`erase nvram:`**	Erases the startup configuration and the key pairs.
`webvpn#` **`erase /all nvram:`**	Erases the startup configuration, the key pairs, the certificates, and all other files from the NVRAM.

Note If you have a large number of files in NVRAM, this task may take up to 2 minutes to finish.

Caution If you erase the saved configuration, the automatic backup configuration in NVRAM is also erased.

Backing Up Keys and Certificates

If an event occurs that interrupts the process of saving the keys and certificates to NVRAM (for example, a power failure), you could lose the keys and certificates that are being saved. You can obtain public keys and certificates from the certificate authority. However, you cannot recover private keys.

If a secure server is available, back up key pairs and the associated certificate chain by exporting each trustpoint to a PKCS12 file. You can then import the PKCS12 files to recover the keys and certificates.

Security Guidelines

When backing up keys and certificates, observe the following guidelines:

- For each PKCS12, you must select a pass phrase that cannot be easily guessed and keep the pass phrase well protected. Do not store the PKCS12 file in clear form.
- The backup server must be secure. Allow only authorized personnel to access the backup server.
- When importing or exporting the PKCS12 file (in which you are required to enter a pass phrase), connect directly to the module console or use an SSH session.
- Use SCP for file transfer.

Monitoring and Maintaining Keys and Certificates

This section describes the following optional tasks:

- Deleting RSA Keys from the WebVPN Services Module, page 3-53
- Viewing Keys and Certificates, page 3-54
- Deleting Certificates from the Configuration, page 3-54

Deleting RSA Keys from the WebVPN Services Module

Caution Deleting the SSH key will disable SSH on the WebVPN Services Module. If you delete the SSH key, generate a new key. See the "Configuring Authentication for Administrators" section on page 2-5.

Under certain circumstances you might want to delete the RSA keys from a module. For example, if you believe the RSA keys were compromised in some way and should no longer be used, you should delete the keys.

To delete all RSA keys from the module, perform this task in global configuration mode:

Command	Purpose
`webvpn(config)#` **`crypto key zeroize rsa`** `[`*`key-label`*`]`	Deletes all RSA key pairs, or the specified key pair. **Caution** If a key is deleted, all certificates that are associated with the key are deleted.

After you delete the RSA keys from a module, complete these two additional tasks:

- Ask the certificate authority administrator to revoke the certificates for your module at the certificate authority; you must supply the challenge password that you created for that module with the **crypto pki enroll** command when you originally obtained the certificates.
- Manually remove the trustpoint from the configuration as described in the "Deleting Certificates from the Configuration" section on page 3-54.

Viewing Keys and Certificates

To view keys and certificates, perform one of these tasks:

Command	Purpose
`webvpn#` **`show crypto key mypubkey rsa`**	Displays RSA public keys for the module.
`webvpn#` **`show crypto pki certificates`** `[`*`trustpoint_label`*`]`	Displays information about the certificate, the certificate authority certificate, and any registration authority certificates.
`webvpn#` **`show running-config`** `[`**`brief`**`]`	Displays the public keys and the certificate chains. If the *brief* option is specified, the hex dump of each certificate is not displayed.

Deleting Certificates from the Configuration

The WebVPN Services Module saves its own certificates and the certificate of the certificate authority. You can delete certificates that are saved on the module.

To delete the certificate from the module configuration, perform this task in global configuration mode:

Command	Purpose
`webvpn(config)#` **`no crypto pki trustpoint`** *`trustpoint-label`*	Deletes the certificate.

Assigning a Certificate to a WebVPN Gateway and Context

When you enter the **ssl trustpoint** *trustpoint_label* subcommand (under the **webvpn gateway** *gateway_name* command), you assign a certificate to the specified WebVPN gateway. You can enter the **ssl trustpoint** subcommand multiple times for the gateway.

If the trustpoint label is modified, the gateway is momentarily taken out of service during the transition. Existing connections continue to use the old certificate until the connections are closed or cleared. New connections use the certificate from the new trustpoint, and the service is available again.

However, if the new trustpoint does not have a certificate yet, the operational status of the service remains down. New connections are not established until the new certificate is available. If the certificate is deleted by entering the **no ssl trustpoint** subcommand, the existing connections continue to use the certificate until the connections are closed or cleared. Although the certificate is obsolete, it is not removed from the WebVPN gateway until all connections are closed or cleared.

Note You can assign a generated self-signed certificate to a WebVPN gateway, but you cannot assign an imported self-signed certificate to a WebVPN gateway, because you cannot import the key pair of the certificate authority that signed the imported certificate.

This example shows how to assign a trustpoint to a gateway:

```
webvpn# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
webvpn(config)# webvpn gateway gw1
webvpn(config-webvpn-gateway)# ip address 10.1.1.2
webvpn(config-webvpn-gateway)# ssl trustpoint tp-1
webvpn(config-webvpn-gateway)# end
webvpn#
webvpn# show webvpn gateway gw1
Admin Status: up
Operation Status: up
IP: 10.1.1.2, port: 443
TCP Policy not configured
SSL Policy not configured
SSL Trustpoint: tp-1
  Certificate chain for new connections:
    Certificate:
       Key Label: tp-1, 1024-bit, not exportable
       Key Timestamp: 12:09:27 UTC Dec 25 2004
       Serial Number: 0FE5
    Root CA Certificate:
       Serial Number: 01
  rsa-general-purpose certificate
  Certificate chain complete

webvpn#
```

This example shows how to change a trustpoint for a WebVPN gateway:

Note The existing connections continue to use the old certificate until the connections are closed. The operational status of the service changes from up to down, and then up again. New connections use the new certificate.

```
webvpn# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
webvpn(config)# webvpn gateway gw1
webvpn(config-webvpn-gateway)# ssl trustpoint tp-2
webvpn(config-webvpn-gateway)# end
webvpn#
webvpn# show webvpn gateway gw1
Admin Status: up
Operation Status: up
IP: 10.1.1.2, port: 443
TCP Policy not configured
SSL Policy not configured
SSL Trustpoint: tp-2
  Certificate chain for new connections:
    Certificate:
       Key Label: tp-2, 1024-bit, not exportable
       Key Timestamp: 12:09:27 UTC Dec 25 2004
       Serial Number: 0FE5
    Root CA Certificate:
       Serial Number: 01
  rsa-general-purpose certificate
  Certificate chain complete
webvpn#
```

Renewing a Certificate

Some certificate authorities require you to generate a new key pair to renew a certificate, while other certificate authorities allow you to use the key pair of the expiring certificate to renew a certificate. Both cases are supported on the WebVPN Services Module.

The SSL server certificates usually expire in one or two years. Graceful rollover of certificates avoids sudden loss of services.

This example shows that gateway gw2 is assigned trustpoint t2:

```
webvpn# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
webvpn(config)# webvpn gateway gw2
webvpn(config-gateway)# ssl trustpoint t2
webvpn(config-gateway)# end
webvpn#

webvpn# show webvpn gateway gw2
Admin Status: up
Operation Status: up
IP: 2.100.100.202, port: 443
TCP Policy not configured
SSL Policy not configured
SSL Trustpoint: t2
  Certificate chain for new connections:
    Certificate:
       Key Label: k2, 1024-bit, not exportable
       Key Timestamp: 18:38:53 UTC Jan 24 2005
       Serial Number: 67A6
    Root CA Certificate:
       Serial Number: 01
  rsa-general-purpose certificate
  Certificate chain complete
```

This example shows that the key pair for trustpoint t2 is refreshed, and the old certificate is deleted from the Cisco IOS database. Graceful rollover starts automatically for gateway gw2.

```
webvpn# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
webvpn(config)# crypto key generate rsa general-keys label k2 exportable
% You already have RSA keys defined named k2.
% Do you really want to replace them? [yes/no]:yes
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]:1024
% Generating 1024 bit RSA keys ...[OK]
*May  7 17:47:10.718: %WEBVPN-6-PKI_CERT_ROLLOVER_BEGIN: The process of rolling over the
certificate without the sudden loss of services has begun for the proxy service: gw2,
trustpoint: t2
webvpn(config)#end
webvpn# show show webvpn gateway gw2
Admin Status:up
Operation Status:up
IP: 2.100.100.202, port: 443
TCP Policy not configured
SSL Policy not configured
SSL Trustpoint: t2
  Certificate chain in graceful rollover, being renewed:
    Certificate:
       Key Label:k2 1024-bit, exportable
       Key Timestamp: 17:47:10 UTC May 7 2005
       Serial Number:47AF
    Root CA Certificate:
      Serial Number:01
  rsa-general-purpose certificate
  Server certificate in graceful rollover
```

This example shows that existing and new connections use the old certificate until trustpoint t2 reenrolls. After trustpoint t2 reenrolls, new connections use the new certificate; existing connections continue to use the old certificate until the connections are closed.

```
webvpn# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
webvpn(config)# crypto pki enroll t2
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will be: CN=2.100.100.202
% The fully-qualified domain name will not be included in the certificate Request
certificate from CA? [yes/no]: y
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificate' command will also show the fingerprint.

CRYPTO_PKI:    Fingerprint:  36DC4511 CE0353DB A7194317 E2D10481

May  7 18:34:22.967: %PKI-6-CERTRET: Certificate received from Certificate Authority
May  7 18:34:24.195: %WEBVPN-6-PKI_SERVICE_CERT_INSTALL: Proxy: gw2, Trustpoint: t2, Key:
k2, Serial#: 47AF, Index: 4
May  7 18:34:24.203: %WEBVPN-6-PKI_CERT_ROLLOVER_END: The process of rolling over the
certificate without the sudden loss of services has ended for the proxy service: gw2,
trustpoint: t2
webvpn(config)# end

webvpn# show show webvpn gateway gw2
Admin Status: up
Operation Status: up
IP: 2.100.100.202, port: 443
TCP Policy not configured
SSL Policy not configured
SSL Trustpoint: t2
  Obsolete certificate chain for old connections:
    Certificate:
       Key Label: k2, 1024-bit, not exportable
       Key Timestamp: 18:38:53 UTC Jan 24 2005
       Serial Number: 67A6
    Root CA Certificate:
       Serial Number: 01
  Certificate chain for new connections:
    Certificate:
       Key Label: k2, 1024-bit, exportable
       Key Timestamp: 17:47:10 UTC May 7 2005
       Serial Number: 47AF
```

```
      Root CA Certificate:
         Serial Number: 01
    rsa-general-purpose certificate
    Certificate chain complete

May 7 18:34:44.191: %WEBVPN-6-PKI_SERVICE_CERT_DELETE: Proxy: gw2, Trustpoint: t2, Key:
k2, Serial#: 67A6, Index: 0
```

This example shows that the obsolete certificate is removed after all of the existing connections are closed.

```
webvpn# show show webvpn gateway gw2
IP: 2.100.100.202, port: 443
TCP Policy not configured
SSL Policy not configured
SSL Trustpoint: t2
  Certificate chain for new connections:
    Certificate:
       Key Label: k2, 1024-bit, exportable
       Key Timestamp: 17:47:10 UTC May 7 2005
       Serial Number: 47AF
    Root CA Certificate:
       Serial Number: 01
  rsa-general-purpose certificate
  Certificate chain complete
```

Automatic Certificate Renewal and Enrollment

When you configure automatic enrollment, the WebVPN Services Module automatically requests a certificate from the certificate authority that is using the parameters in the configuration.

You can configure the certificate to automatically renew after a specified percentage of the validity time has passed. For example, if the certificate is valid for 300 days, and you specify *renewal_percent* as 80, the certificate automatically renews after 240 days have passed since the start validity time of the certificate.

Note The certificate authority certificate needs to be in the database prior to auto enrollment or renewal. Authenticate the trustpoint prior to configuring automatic enrollment. Also, configure a SCEP enrollment URL for the trustpoint.

To enable automatic enrollment and renewal and to display timer information, perform this task:

	Command	Purpose
Step 1	`webvpn(config)#` **`crypto pki trustpoint`** *`trustpoint-label`*	Declares the trustpoint.
Step 2	`webvpn(ca-trustpoint)#` **`auto-enroll`** `{renewal_`*`percent`*`|`**`regenerate`**`}`	Enables automatic renewal and enrollment for the specified trustpoint. **Note** Valid values for *renewal_percent* are 0 (enroll within 1 minute) through 100. **Note** The **regenerate** keyword generates a new key for the certificate even if a named key already exists.
Step 3	`webvpn#` **`show crypto pki timers`**	Displays the time remaining before each timer expires.

This example shows how to enable auto enrollment and auto renewal:

```
webvpn# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
webvpn(config)# crypto pki trustpoint tk21
webvpn(ca-trustpoint)# auto-enroll 90
webvpn(ca-trustpoint)# end
webvpn# show crypto pki timers
PKI Timers
|          44.306
 |          44.306  RENEW tp-new
 |255d 5:28:32.348  RENEW tk21
webvpn#
```

APPENDIX A

Setting Up WebVPN for the End User

This appendix is for the system administrator who sets up WebVPN for end users. It summarizes configuration requirements and tasks for the end user's remote system. It also specifies information to communicate to end users to get them started using WebVPN.

Note Before you set up WebVPN for the end user, you should have already configured the WebVPN Services Module.

This appendix contains the following sections:

- Starting WebVPN, page A-1
- Usernames and Passwords, page A-2
- End User Interface, page A-3
- Using Other WebVPN Features, page A-14
- Security Tips, page A-16
- Application Access—Recovering from Hosts File Errors, page A-16

Starting WebVPN

The following are required to start WebVPN on an end user's remote system:

- Connection to the Internet—Any Internet connection is supported, including:
  - Home DSL, cable, or dial-ups
  - Public kiosks
  - Hotel hook-ups
  - Airport wireless nodes
  - Internet cafes

- WebVPN-supported browser—The following browsers have been verified for WebVPN. Other browsers might not fully support WebVPN features.

  On Microsoft Windows:

  - Internet Explorer 6.0 SP1 (SP2 required for Windows XP)
  - Netscape 7.2

  On Linux:

  - Netscape version 7.2
- Cookies enabled—Cookies must be enabled on the browser in order to access applications through port forwarding.
- Pop-ups enabled—Pop-ups should be enabled on the browser to allow the browser to display the floating WebVPN toolbar and timeout warnings. If pop-ups are blocked, change the browser setting and click the WebVPN floating toolbar icon on the in-page toolbar to display the floating toolbar.

  If pop-ups are disabled on the browser, WebVPN will not warn the end user before disconnecting due to an idle timeout or a maximum connect time.
- URL for WebVPN—An HTTPS address in the following form:

  https://*address*

  where *address* is the IP address or DNS hostname of an interface of the WebVPN module, such as https://10.89.192.163 or https://vpn.company.com.
- WebVPN username and password
- (Optional) Local printer—WebVPN does not support printing from a web browser to a network printer. Printing to a local printer is supported.

Usernames and Passwords

Table A-1 lists the type of usernames and passwords that WebVPN users might need to know.

Table A-1 Usernames and Passwords for WebVPN Users

Login Username/ Password Type	Purpose	Entered When
Computer	Access the computer	Starting the computer
Internet Provider	Access the Internet	Connecting to an Internet provider
WebVPN	Access the remote network	Starting WebVPN
File Server	Access the remote file server	Using the WebVPN file browsing feature to access a remote file server
Corporate Application Login	Access the firewall-protected internal server	Using the WebVPN web browsing feature to access an internal protected website
Mail Server	Access the remote mail server via WebVPN	Sending or receiving e-mail messages

End User Interface

An end user whose enterprise has configured WebVPN can access the enterprise network by launching a browser and connecting to the WebVPN gateway that is hosted by the enterprise network. The end user presents his or her credentials, authenticates, and sees the portal page (home page) of the enterprise site. The portal page displays those functionalities (for example, e-mail and web browsing) to which the end user has access on the basis of his or her credentials. If the end user has access to all functionalities of the WebVPN gateway, the home page provides links to all those functionalities.

Note The end user interface is primarily an HTML interface.

The following sections explain the end user interface in more detail:

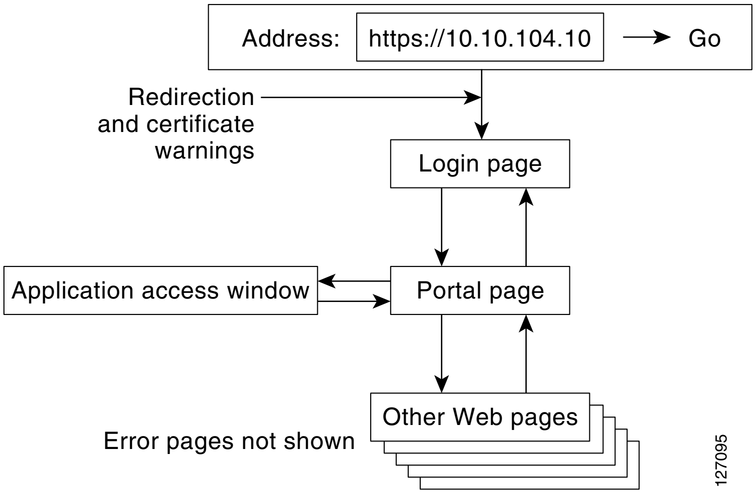
- Page Flow, page A-3
- Initial Connection, page A-4
- Login Page, page A-4
- Certificate Authentication, page A-5
- Logout Page, page A-5
- Portal Page, page A-7
- Remote Servers, page A-8
- DNS and Connection Errors, page A-9
- Session Timeout, page A-10
- TCP Port Forwarding and Application Access, page A-11

Page Flow

This section describes the page flow process (see Figure A-1) for a WebVPN session. When the end user enters the Hypertext Transfer Protocol Secure (HTTPS) URL (https://*address*) into his or her browser, the end user is then redirected to https://*address*/index.html, where the login page is located.

Note Depending on the configuration of the browser, this redirection may cause a warning in the browser of the end user indicating that he or she is being redirected to a secure connection.

Figure A-1 Page Flow



Initial Connection

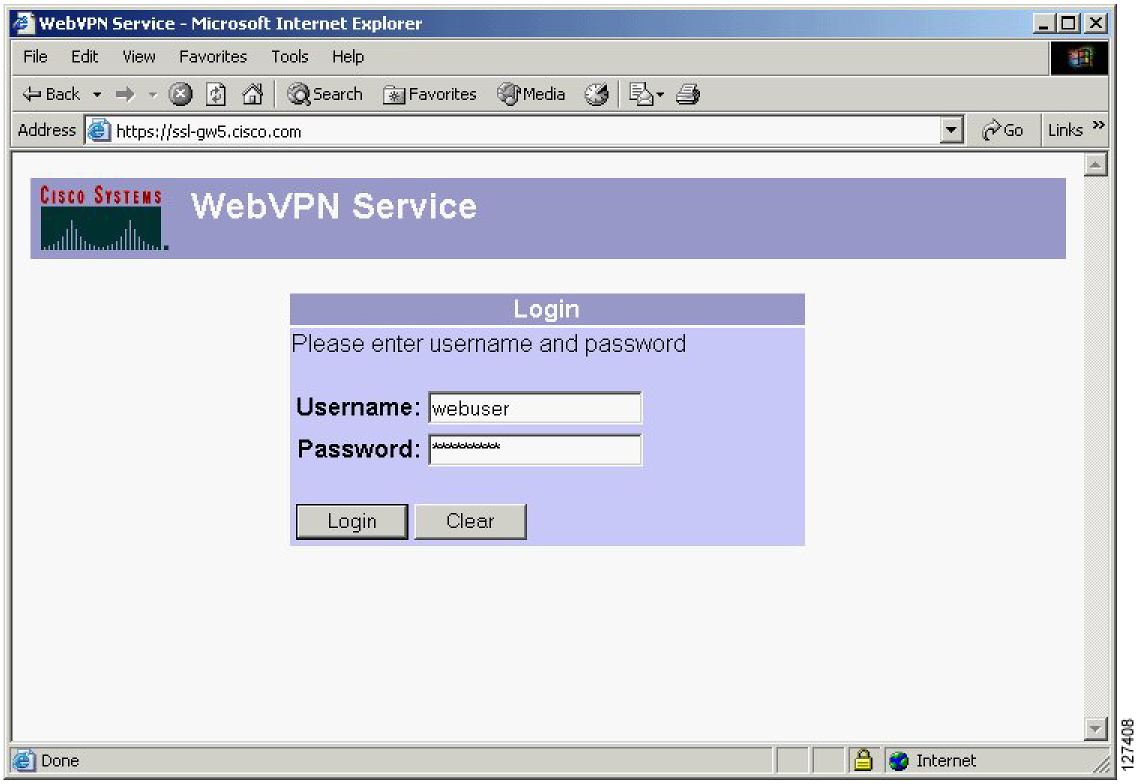
When the HTTPS connection is established, a warning about the SSL/TLS certificate may display. If the warning displays, the end user should install this certificate. If the warning does not display, then the system already has a certificate that the browser trusts.

The end user is then connected to the login page.

Login Page

The login page (see Figure A-2) prompts the end user to enter his or her username and password, which are entered into an HTML form. If an authentication failure occurs, the login page displays an error message.

Figure A-2 Default Login Page



WebVPN Service - Microsoft Internet Explorer

Address https://ssl-gw5.cisco.com

WebVPN Service

Login

Please enter username and password

Username: webuser

Password: *********

The login page has logos, titles, messages, and colors that may be customized by administrators.

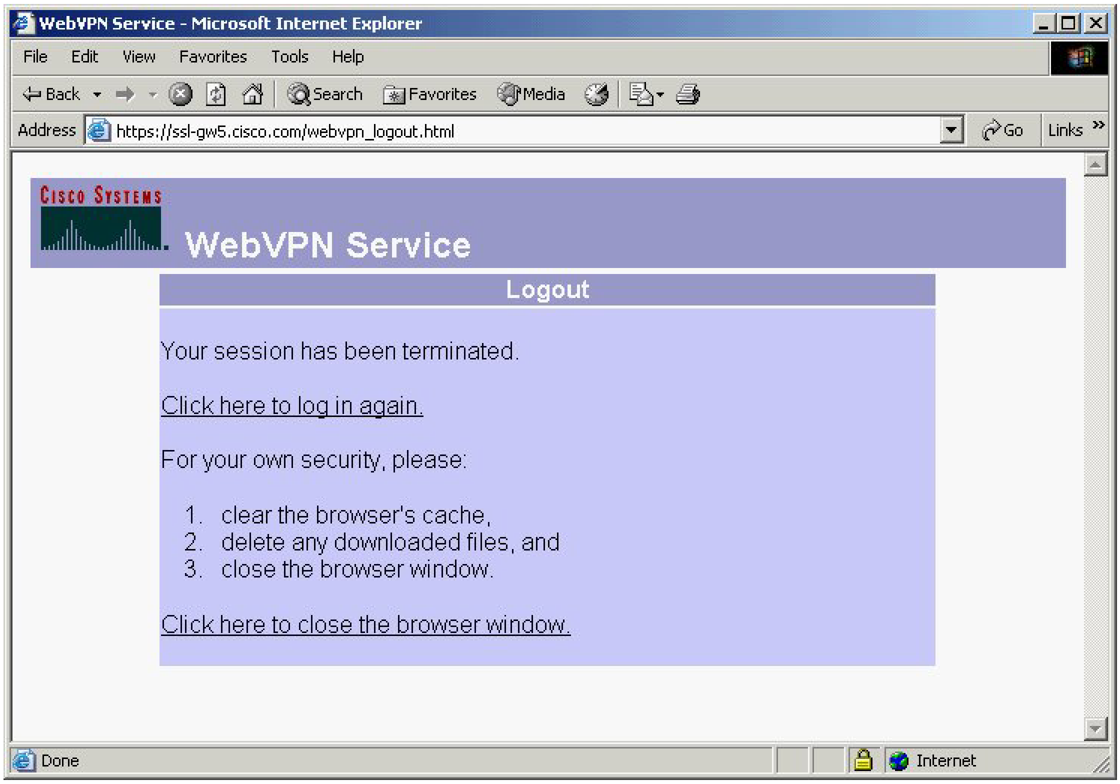
Certificate Authentication

Client certificate authentication is not supported. Only username and password authentication is supported.

Logout Page

The logout page (see Figure A-3) displays if the end user clicks the logout link, or if the session terminates because of an idle timeout or a maximum connection time.

Figure A-3 Logout Page


WebVPN Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://ssl-gw5.cisco.com/webvpn_logout.html
Go Links
Cisco Systems
Done
Internet
127409

WebVPN Service

Logout

Your session has been terminated.

Click here to log in again.

For your own security, please:

1. clear the browser's cache,
2. delete any downloaded files, and
3. close the browser window.

Click here to close the browser window.

Portal Page

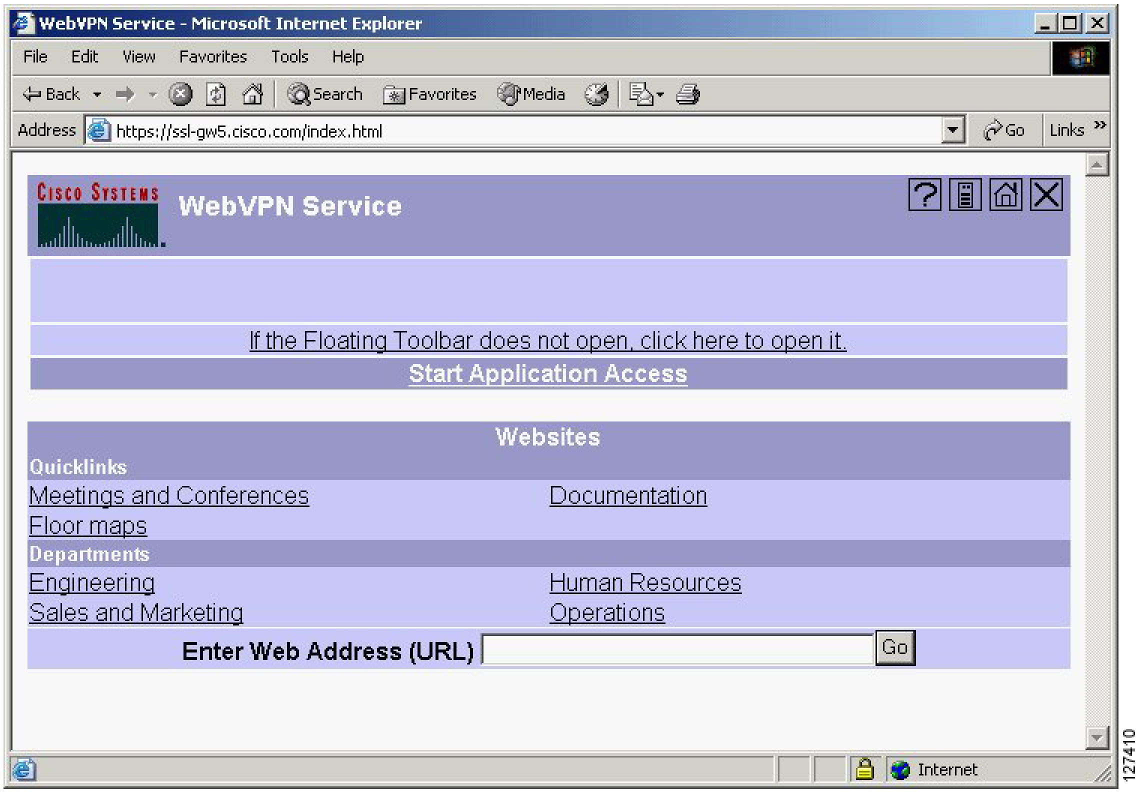
The portal page (see Figure A-4) is the main page for the WebVPN functionality. You can customize this page to contain the following:

- Custom logo (the default is the Cisco bridge logo
- Custom title (the default is "WebVPN Services")
- Custom banner (the default is an empty string)
- Custom colors (the default is a combination of white and purples)
- List of web server links (customizable)
- URL entry box (always present)
- Application access link (always present)
- Icon links for Help, Home (that is, the portal page), and Logout
- Link to the popup, floating toolbar

Items that you have not configured are not displayed on the portal page.

Note E-mail access is supported by thin-client mode, which is downloaded using the application access link.

Figure A-4 Portal Page



WebVPN Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Go
Links
Internet
127410

https://ssl-gw5.cisco.com/index.html

WebVPN Service

If the Floating Toolbar does not open, click here to open it.

Start Application Access

Websites

Quicklinks

Meetings and Conferences	Documentation
Floor maps	

Departments

Engineering	Human Resources
Sales and Marketing	Operations

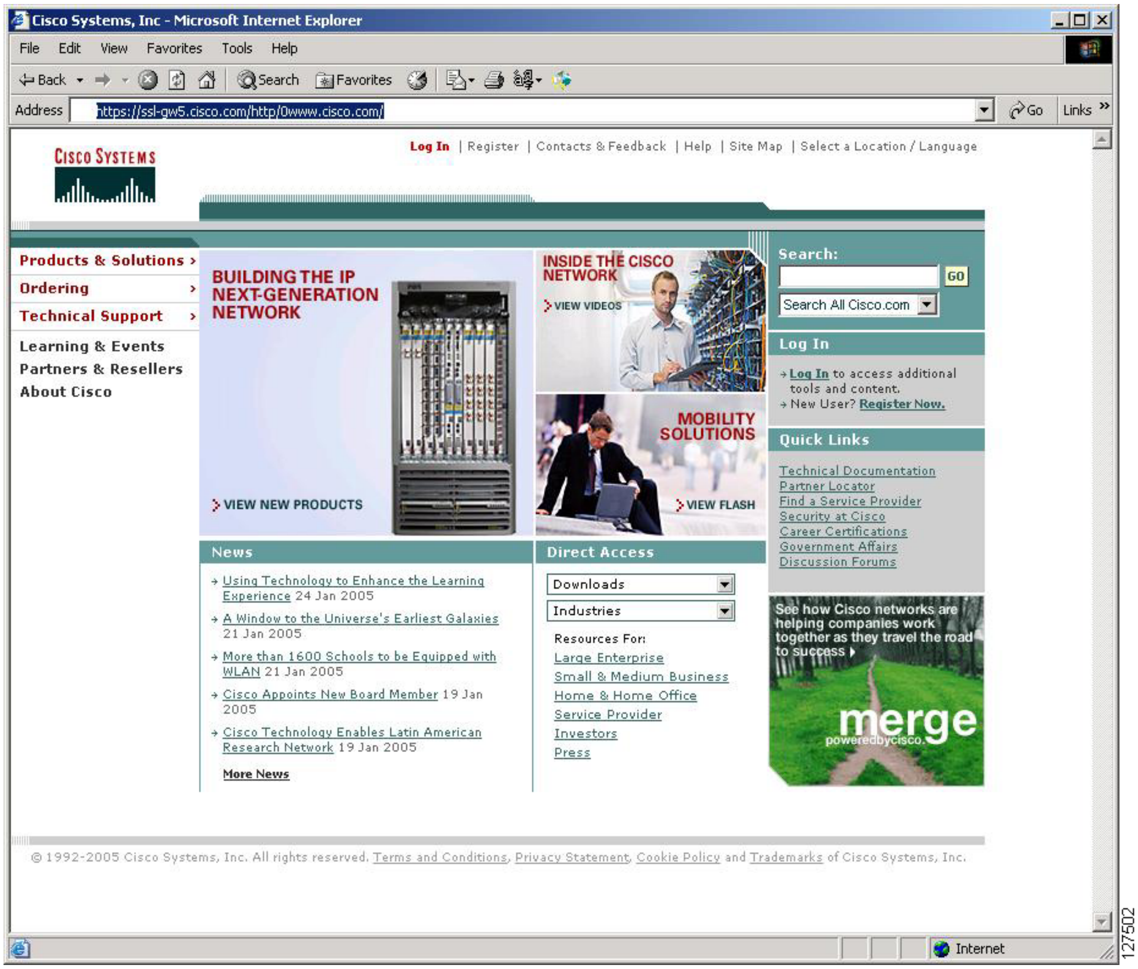
Enter Web Address (URL) Go

Remote Servers

An end user may enter an address or URL path of a website to which he or she wants to visit either in the text box on the portal page or in the text box on the floating toolbar. Pages from the remote server are displayed in the browser window. The end user can then browse to other links on the page.

Figure A-5 illustrates the portal page of a typical website. By clicking the home icon button on the floating toolbar (see Figure A-6), the end user can go back to the portal page.

Figure A-5 Website with a Toolbar



Address: https://ssl-gw5.cisco.com/http/0www.cisco.com/

Log In to access additional tools and content.
New User? Register Now.

- Using Technology to Enhance the Learning Experience 24 Jan 2005
- A Window to the Universe's Earliest Galaxies 21 Jan 2005
- More than 1600 Schools to be Equipped with WLAN 21 Jan 2005
- Cisco Appoints New Board Member 19 Jan 2005
- Cisco Technology Enables Latin American Research Network 19 Jan 2005

See how Cisco networks are helping companies work together as they travel the road to success

© 1992-2005 Cisco Systems, Inc. All rights reserved. Terms and Conditions, Privacy Statement, Cookie Policy and Trademarks of Cisco Systems, Inc.

WebVPN Floating Toolbar

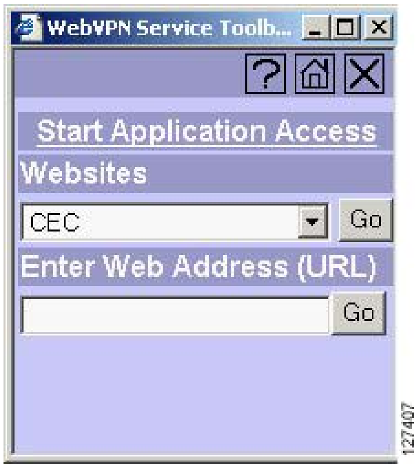
A floating toolbar (see Figure A-6) allows the end user to enter URLs, browse file locations, and choose preconfigured web connections without interfering with the main browser window.

The floating toolbar represents the WebVPN session. If the end user clicks the window's Close button, the WebVPN module prompts the end user to confirm that he or she wants to close the session.

Note Clicking the Home icon when viewing certain web pages, such as Hotmail.com and CNN.com, opens a new browser window because these sites rename the WebVPN browser window as part of how they function.

Tip To paste text into a text field, press Ctrl-V. Right-clicking is disabled in the WebVPN toolbar.

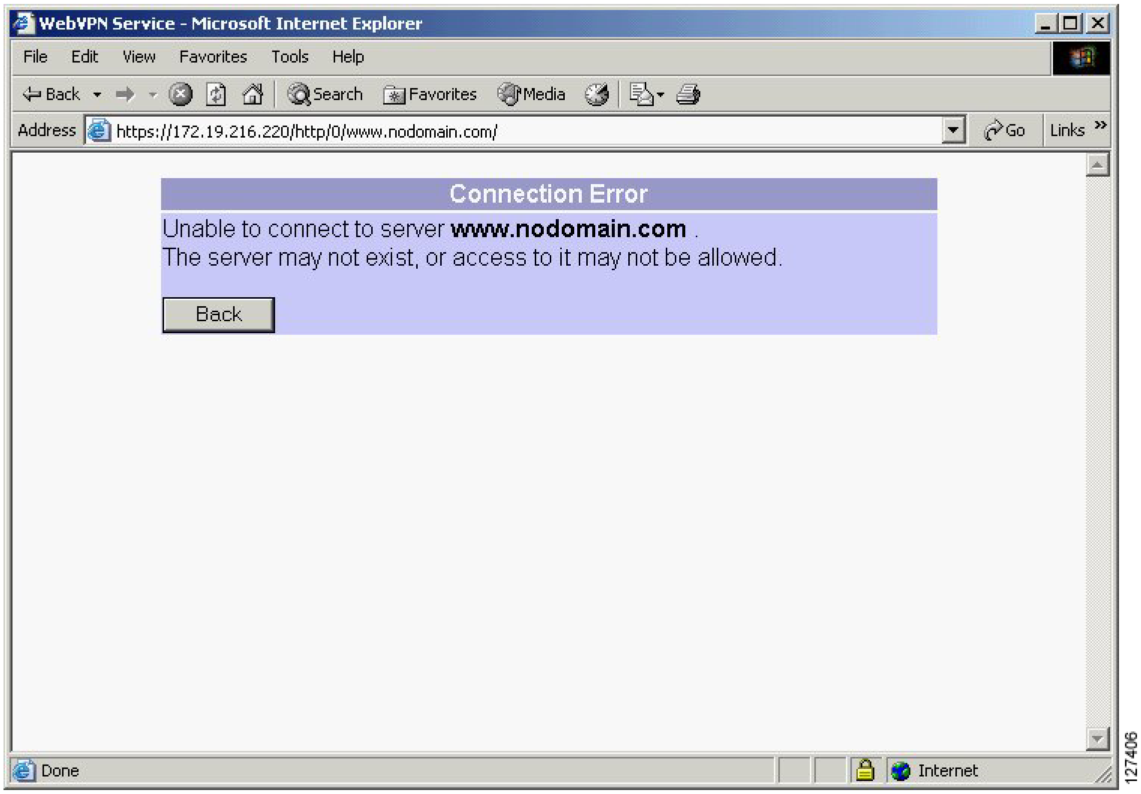
Figure A-6 Floating Toolbar



DNS and Connection Errors

If an end user specifies a remote server to which he or she cannot connect because of domain naming system (DNS) or other connection errors, an error displays (see Figure A-7). Because of TCP timeouts, it may take a while for connection errors to be returned to the end user.

Figure A-7 DNS Errors


WebVPN Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address https://172.19.216.220/http/0/www.nodomain.com/
Go Links
Done
Internet
127406

Connection Error

Unable to connect to server **www.nodomain.com** .
The server may not exist, or access to it may not be allowed.

Back

Session Timeout

End users receive a warning approximately 1 minute before the session expires due to inactivity, and they receive another warning when the session expires (see Figure A-8). The local time on the workstation is also displayed to indicate when the message was displayed.

The first message will be similar to the following:

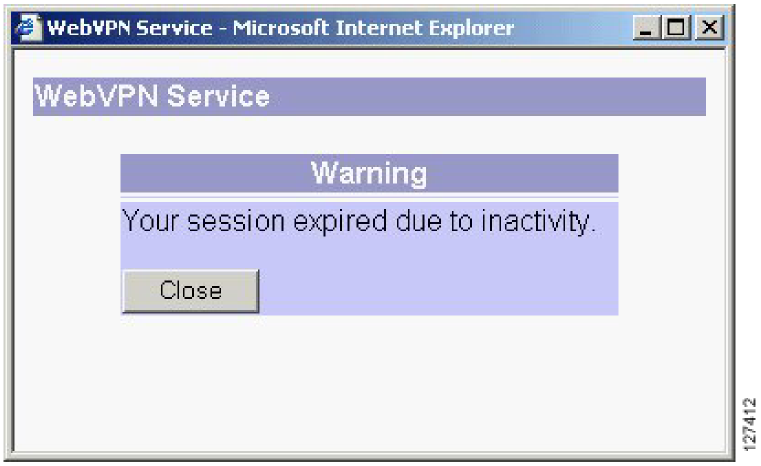
- "Your session will expire in *x* seconds due to inactivity. Click [Close] to reset the inactivity timer. (browser time and date)"

Clicking the [Close] button on the idle warning message resets the inactivity timer.

The last message, as shown below, displays when the time runs out (depending on whether the reason of the session termination is known):

- "Your session has expired due to inactivity."

Figure A-8 Session Inactivity or Timeout Window


WebVPN Service - Microsoft Internet Explorer

WebVPN Service

Warning

Your session expired due to inactivity.

TCP Port Forwarding and Application Access

Note This feature requires the Java 1.4 Java Virtual Machine (JVM) to properly support SSL connections.

Note Because this feature requires installing JRE and configuring the local clients, and because doing so requires administrator permissions on the local system, it is unlikely that end users will be able to use applications when they connect from public remote systems.

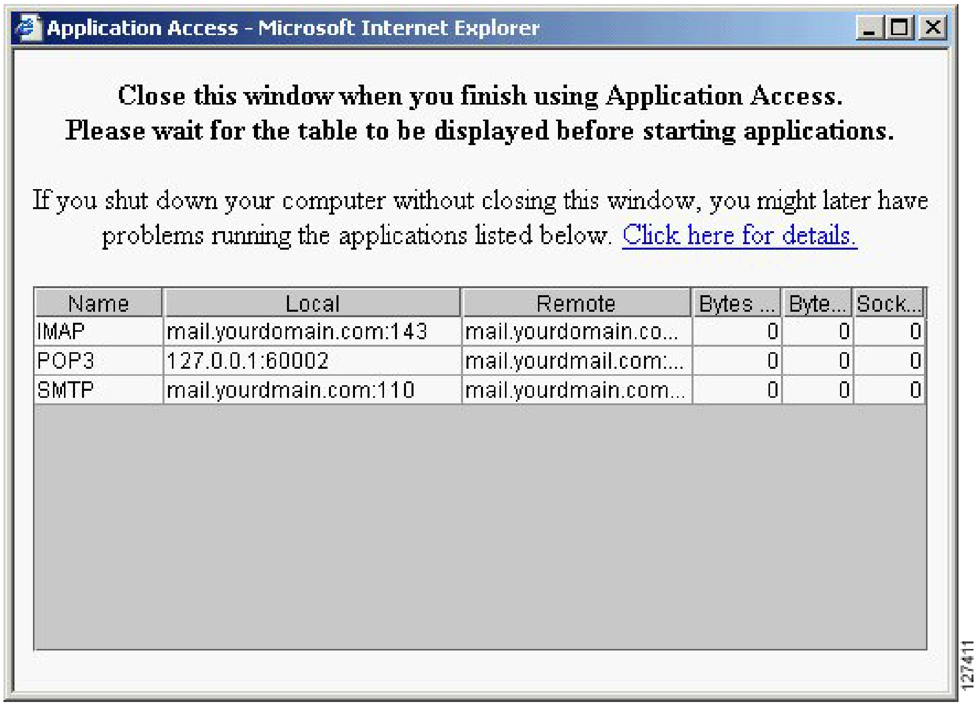
When the end user clicks the Application Access link, a new window is displayed. This window initiates the downloading of a port-forwarding applet. Another window is then displayed. This window asks the end user to verify the certificate with which this applet is signed. When the end user accepts the certificate, the applet starts running, and port-forwarding entries are displayed (see Figure A-9). The number of active connections and bytes that are sent and received is also listed on this window.

Note When end users launch Application Access, their system may display a dialog box regarding digital certificates, and this dialog box may appear behind other browser windows. If the end user's connection appears hung, tell the end user to minimize the browser windows to check for this dialog box.

You should have configured IP addresses, DNS names, and port numbers for the e-mail servers. The end user can then launch the e-mail client, which is configured to contact the above e-mail servers and send and receive e-mails. Point of Presence3 (POP3), Internet Message Access Protocol (IMAP), and Simple Mail Transfer Protocol (SMTP) protocols are supported.

The window attempts to close automatically if the end user is logged out using JavaScript. If the session terminated and a new port forwarding connection is established, the applet displays an error message.

Figure A-9 TCP Port Forwarding Page



**Close this window when you finish using Application Access.
Please wait for the table to be displayed before starting applications.**

If you shut down your computer without closing this window, you might later have problems running the applications listed below. Click here for details.

Name	Local	Remote	Bytes ...	Byte...	Sock...
IMAP	mail.yourdomain.com:143	mail.yourdomain.co...	0	0	0
POP3	127.0.0.1:60002	mail.yourdmail.com:...	0	0	0
SMTP	mail.yourdmain.com:110	mail.yourdmain.com...	0	0	0

Caution You should tell users to always close the Application Access window when they finish using applications by clicking the close icon. Failure to quit the window properly can cause Application Access or the applications to be disabled. See the "Application Access—Recovering from Hosts File Errors" section on page A-16 for details.

Table A-2 lists the requirements for Application Access (Port Forwarding) on an end user's remote system.

Table A-2 WebVPN Remote System Application Access Requirements

Remote System or End User Requirements	Specifications or Use Suggestions
Client applications installed	—
Cookies enabled on browser	—
Administrator privileges	End user must be local administrator on his or her PC.

Table A-2 WebVPN Remote System Application Access Requirements (continued)

Remote System or End User Requirements	Specifications or Use Suggestions
Sun Microsystems Java Runtime Environment (JRE) version 1.4 or later installed	WebVPN automatically checks for JRE whenever the end user starts Application Access. If it is necessary to install JRE, a pop-up window displays directing end users to a site where it is available.
Client applications configured, if necessary. **Note** The Microsoft Outlook client does not require this configuration step.	To configure the client application, use the server's locally mapped IP address and port number. To find this information, do the following: **1.** Start WebVPN on the remote system and click the Application Access link on the WebVPN home page. The Application Access window displays. **2.** In the Name column, find the name of the server that you want to use, and then identify its corresponding client IP address and port number (in the Local column). **3.** Use this IP address and port number to configure the client application. The configuration steps vary for each client application.
Windows XP SP2 patch	End users running Windows XP SP2 must install a patch from Microsoft that is available at the following address: http://support.microsoft.com/?kbid=884020 This problem is a known Microsoft issue.

Using Other WebVPN Features

Table A-3 lists the requirements for various WebVPN features.

Table A-3 WebVPN Remote System Configuration and End User Requirements

Task	Remote System or End User Requirements	Specifications or Use Suggestions
Web Browsing	Usernames and passwords for protected websites	Using WebVPN does not ensure that communication with every site is secure. See the "Security Tips" section on page A-16.
		The look and feel of web browsing with WebVPN might be different from what end users are accustomed to. For example, when using WebVPN, note the following: • The WebVPN title bar appears above each web page • You can access websites as follows: – Entering the URL in the Enter Web Address field on the WebVPN home page – Clicking on a preconfigured website link on the WebVPN home page – Clicking a link on a webpage accessed by one of the previous two methods Also, depending on how you configured a particular account, the following might have occured: • Some websites are blocked. • Only the websites that appear as links on the WebVPN home page are available.
Network Browsing and File Management	File permissions configured for shared remote access	Only shared folders and files are accessible through WebVPN.
	Server name and passwords for protected file servers	
	Domain, workgroup, and server names where folders and files reside	Users might not be familiar with how to locate their files through your organization's network.
	Note Do not interrupt the Copy File to Server command or navigate to a different screen while the copying is in progress. Interrupting the operation can cause an incomplete file to be saved on the server.	

Table A-3 WebVPN Remote System Configuration and End User Requirements (continued)

Task	Remote System or End User Requirements	Specifications or Use Suggestions
Using e-mail: Application Access	Fulfill requirements for Application Access (see the "TCP Port Forwarding and Application Access" section on page A-11)	To use e-mail, start Application Access from the WebVPN home page. The e-mail client is then available for use.
	Note If the end users are using an IMAP client and they lose their e-mail server connection or are unable to make a new connection, end users should close the IMAP application and restart WebVPN.	
	Other Mail Clients	Cisco has tested Microsoft Outlook Express versions 5.5 and 6.0. WebVPN should support other SMTPS, POP3S, or IMAP4S e-mail programs, such as Netscape Mail, Lotus Notes, and Eudora, but Cisco has not verified them.
Using e-mail: Web Access	Web-based e-mail product installed	Supported products are as follows: • Outlook Web Access (OWA) 5.5, 2000, and 2003 Netscape, Mozilla, and Internet Explorer are supported with OWA 5.5 and 2000. Internet Explorer 6.0 or higher is required with OWA 2003. Netscape and Mozilla are not supported with OWA 2003. • Lotus iNotes Other web-based e-mail products should also work, but Cisco has not verified them.
Using the WebVPN floating toolbar	Most platforms except for PocketPC	To paste text into a text field, press Ctrl-V. Right-clicking is disabled in the floating toolbar.
Using the Cisco SSL VPN Client (SVC)		To retrieve SVC log messages using the Windows Event Viewer, go to Program Files > Administrative Tools > Event Viewer in Windows.
Using Secure Desktop Manager	A Secure Desktop Manager-supported browser	On Microsoft Windows: • Internet Explorer version 6.0 • Netscape version 7.2 On Linux: • Netscape version 7.2
Using Cache Cleaner or Secure Desktop	A Cisco Secure Desktop-supported browser	Any browser supported for Secure Desktop Manager.

Security Tips

Advise end users always to log out from the WebVPN session when they are done. (To log out of WebVPN, click on the logout icon on the WebVPN toolbar or quit the browser.)

Advise end users that using WebVPN does not ensure that communication with every site is secure. WebVPN ensures the security of data transmission between the remote end user's PC or workstation and the WebVPN module on the corporate network. If the end user then accesses a non-HTTPS web resource (located on the Internet or on the internal network), the communication from the corporate WebVPN module to the destination web server is not secured.

Browser Caching and Security Implications

If end users use WebVPN through a public or shared Internet system, such as at an Internet cafe or kiosk, to ensure the security of their information after terminating or logging out of the WebVPN session, end users must delete all files that they saved on the PC during the WebVPN session. These files are not removed automatically upon disconnect.

Note WebVPN does not save the content of Web pages viewed during the session. However, for additional security, we recommend that end users also clear their browser's cache. Deleting content from a PC does not ensure that it cannot be recovered; keep this in mind when downloading sensitive data.

Application Access—Recovering from Hosts File Errors

It is very important to tell end users to close the Application Access window properly by clicking the close icon. If they do not close the window properly, the following could occur:

- The next time end users try to start Application Access, it might be disabled; they will receive a "Backup HOSTS File Found" error message
- The applications might be disabled or might malfunction even when the end user is running them locally

These errors can result from end users terminating the Application Access window in any improper way:

- The browser crashes while using Application Access
- A power outage or system shutdown occurs while using Application Access
- End users minimize the Application Access window and then shut down the computer with the window active (but minimized)

How WebVPN Uses the Hosts File

The hosts file on the end user system maps IP addresses to hostnames. When the end user starts Application Access, WebVPN modifies the hosts file by adding WebVPN-specific entries. When the end user stops Application Access by properly closing the Application Access window, WebVPN returns the hosts file to its original state. The hosts file goes through the following states:

- Before invoking Application Access, the hosts file is in its original state.
- When Application Access starts, WebVPN does the following:
    - **a.** Copies the hosts file to hosts.webvpn and creates a backup.
    - **b.** Edits the hosts file, inserting WebVPN-specific information.
- When Application Access stops, WebVPN does the following:
    - **a.** Copies the backup file to the hosts file, which restores the hosts file to its original state.
    - **b.** Deletes hosts.webvpn.
- After finishing Application Access, the hosts file is in its original state.

What Happens When the End User Stops Application Access Improperly

If the end user improperly terminates Application Access, the hosts file is left in a WebVPN-customized state. WebVPN checks for this possibility the next time that the end user starts Application Access by searching for a hosts.webvpn file. If WebVPN finds the file, the end user receives a "Backup HOSTS File Found" error message, and Application Access is temporarily disabled.

When end users shut down Application Access improperly, they leave the remote access client/server applications in a suspended state. If end users try to start these applications without using WebVPN, the applications might malfunction. End users might find that hosts that they normally connect to are unavailable. This situation could commonly occur if end users run applications remotely from home, fail to quit the Application Access window before shutting down the computer, and then try to run the applications later from the office.

What to Do

To reenable Application Access or malfunctioning applications, end users should do the following:

- If they canconnect to their remote access server, they should follow the steps in the "Reconfiguring the Hosts File Automatically Using WebVPN" section on page A-18.
- If they cannot connect to their remote access server from their current location or if they have made custom edits to the hosts file, they should follow the steps in the "Reconfiguring the Hosts File Manually" section on page A-18.

Reconfiguring the Hosts File Automatically Using WebVPN

If end users are able to connect to their remote access server, they should follow these steps to reconfigure the hosts file and reenable both Application Access and the applications:

Step 1 Start WebVPN and log in. The portal page opens.

Step 2 Click the Applications Access link. A "Backup HOSTS File Found" message displays.

Step 3 Choose one of the following options:

- Restore from backup—WebVPN forces a proper shutdown. WebVPN copies the hosts.webvpn backup file to the hosts file, restoring it to its original state, and then deletes hosts.webvpn. You then have to restart Application Access.
- Do nothing—Application Access does not start. You return to your remote access home page.
- Delete backup—WebVPN deletes the hosts.webvpn file, leaving the hosts file in its WebVPN-customized state. The original hosts file settings are lost. Then Application Access starts, using the WebVPN-customized hosts file as the new original. Choose this option only if you are unconcerned about losing hosts file settings. If you edited the hosts file after Application Access has shut down improperly, choose one of the other options, or edit the hosts file manually. (See the "Reconfiguring the Hosts File Manually" section on page A-18.)

Reconfiguring the Hosts File Manually

If end users are not able to connect to their remote access server from their current location, or if end users have customized the hosts file and do not want to lose their edits, they should follow these steps to reconfigure the hosts file and reenable both Application Access and the applications:

Step 1 Locate and edit your hosts file.

Step 2 Check if any lines contain the "added by WebVpnPortForward" string.

If any lines contain this string, your hosts file is WebVPN customized. If your hosts file is customized, it looks similar to the following example:

```
123.0.0.3 server1 # added by WebVpnPortForward
123.0.0.3 server1.example.com vpn3000.com # added by WebVpnPortForward
123.0.0.4 server2 # added by WebVpnPortForward
123.0.0.4 server2.example.com.vpn3000.com # added by WebVpnPortForward
123.0.0.5 server3 # added by WebVpnPortForward
123.0.0.5 server3.example.com vpn3000.com # added by WebVpnPortForward

# Copyright (c) 1993-1999 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
```

```
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

123.0.0.1       localhost
```

Step 3 Delete the lines that contain the "# added by WebVpnPortForward" string.

Step 4 Save and close the file.

Step 5 Start WebVPN and log in. Your home page appears.

Step 6 Click the Application Access link. The Application Access window appears. Application Access is now enabled.

APPENDIX B

Importing the Embedded Test Certificate

A test PKCS12 file (testssl.p12) is embedded in the WebVPN software on the module. You can install the file into the Flash memory for testing purposes and for proof of concept. After the PKCS12 file is installed, you can import it to a trustpoint, and then assign it to a WebVPN gateway that is configured for testing.

To install and import the test file, perform this task:

	Command	Purpose
Step 1	`webvpn#` **`test webvpn platform certificate install`**	Installs the test PKCS12 file to NVRAM.
Step 2	`webvpn#` **`configure terminal`**	Enters configuration mode, selecting the terminal option.
Step 3	`webvpn(config)#` **`crypto ca import`** *`trustpoint_label`* **`pkcs12 flash:testssl.p12`** *`passphrase`*	Imports the test PKCS12 file to the module. **Note** For the test certificate, the *passphrase* is **cisco**.
Step 4	`webvpn(config)#` **`ssl-proxy service`** *`test_service`*	Defines the name of the test proxy service.
Step 5	`webvpn(config-ssl-proxy)#` **`certificate rsa general-purpose trustpoint`** *`trustpoint_label`*	Applies a trustpoint configuration to the proxy server.
Step 6	`webvpn#` **`show ssl-proxy stats`** *`test_service`*	Displays test statistics information.

This example shows how to import the test PKCS12 file:

```
webvpn# test webvpn platform certificate install
% Opening file, please wait ...
% Writing, please wait ...
% Please use the following config command to import the file.
  "crypto ca import <trustpoint-name> pkcs12 flash:testssl.p12 cisco"
% Then you can assign the trustpoint to a WebVPN gateway for testing.

*May 5 20:15:57.831: %WEBVPN-6-PKI_TEST_CERT_INSTALL: Test key and certificate was
installed into Flash in a PKCS#12 file.
webvpn#
webvpn# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
webvpn(config)# crypto ca import test123 pkcs12 flash:testssl.p12 cisco
Source filename [testssl.p12]?
% You already have RSA keys named test123.
% If you replace them, all router certs issued using these keys
% will be removed.
% Do you really want to replace them? [yes/no]: yes
```

```
RYPTO_PKI: Imported PKCS12 file successfully.
webvpn(config)#
*May 5 20:16:25.883: %PKI-6-PKCS12IMPORT_SUCCESS: PKCS #12 Successfully Imported.
webvpn(config)# webvpn gateway test123
webvpn(config-webvpn-gateway)# ip address 2.100.100.77
webvpn(config-webvpn-gateway)# ssl trustpoint test123
*May 5 20:16:43.683: %WEBVPN-6-PKI_SERVICE_CERT_INSTALL: Proxy: test123, Trustpoint:
test123, Key: test123, Serial#: 01, Index: 10
*May 5 20:16:43.683: %WEBVPN-6-PKI_CA_CERT_INSTALL: Root, Subject Name:
cn=testca.cisco.com,ou=Security,o=Cisco Systems Inc,l=San Jose,st=California,c=US,
Serial#: 00, Index: 11
webvpn(config-webvpn-gateway)# inservice
webvpn(config-webvpn-gateway)# exit
webvpn(config)#
*May 5 20:16:46.159: %SSLVPN-5-UPDOWN: sslvpn gateway : test123 changed state to UP
webvpn# show webvpn gateway test123
Admin Status: up
Operation Status: up
IP: 2.100.100.77, port: 443
TCP Policy not configured
SSL Policy not configured
SSL Trustpoint: test123
  Certificate chain for new connections:
    Certificate:
       Key Label: test123, 1024-bit, not exportable
       Key Timestamp: 20:16:25 UTC May 5 2005
       Serial Number: 01
    Root CA Certificate:
       Serial Number: 00
  rsa-general-purpose certificate
  Certificate chain complete
webvpn#
```

Upgrading the Images

The compact Flash on the WebVPN Services Module has two bootable partitions: application partition (AP) and maintenance partition (MP). By default, the application partition boots every time. The application partition contains the binaries necessary to run the WebVPN image. The maintenance partition is booted if you need to upgrade the application partition.

You can upgrade both the application software and the maintenance software. However, you are not required to upgrade both images at the same time. Refer to the release notes for the WebVPN Services Module for the latest application partition and maintenance partition software versions.

The entire application and maintenance partitions are stored on the FTP or TFTP server. The images are downloaded and extracted to the application partition or maintenance partition depending on which image is being upgraded.

To upgrade the application partition, change the boot sequence to boot the module from the maintenance partition. To upgrade the maintenance partition, change the boot sequence to boot the module from the application partition. Set the boot sequence for the module using the supervisor engine CLI commands. The maintenance partition downloads and installs the application image. The supervisor engine must be executing the run-time image to provide network access to the maintenance partition.

Before starting the upgrade process, you will need to download the application partition image or maintenance partition image to the TFTP server.

A TFTP or FTP server is required to copy the images. The TFTP server should be connected to the switch, and the port connecting to the TFTP server should be included in any VLAN on the switch.

These sections describe how to upgrade the images:

- Upgrading the Application Software, page C-2
- Upgrading the Maintenance Software, page C-4
- Installing the SVC Package for Tunnel Mode, page C-6

Upgrading the Application Software

Note Do not reset the module until the image is upgraded. The total time to upgrade the image takes up to eight minutes.

To upgrade the application partition software, perform this task:

	Command	Purpose
Step 1	`Router# hw-module module mod reset cf:1`	Reboots the module from the maintenance partition. **Note** It is normal to see messages such as “Press Key” on the module console after entering this command.
Step 2	`Router# show module`	Displays that the maintenance partition for the module has booted.
Step 3	`Router# copy tftp: pclc#mod-fs:`	Downloads the image.
Step 4	`Router# hw-module module mod reset cf:4`	Resets and boots the module to the application partition. **Note** Do not reset the module until the “You can now reset the module” message is displayed on the console. Resetting the module before this message is displayed will cause the upgrade to fail.
Step 5	`Router# show module`	Displays that the application partition for the module has booted.

This example shows how to upgrade the application partition software:

```
Router# hw-module module 2 reset cf:1
Device BOOT variable for reset = <cf:1>
Warning: Device list is not verified.

Proceed with reload of module?[confirm]y
% reset issued for module 2
supervisor#
16:17:54: SP: The PC in slot 2 is shutting down. Please wait ...
16:18:15: SP: PC shutdown completed for module 2
*May 10 16:50:28.771: %C6KPWR-SP-4-DISABLED: power to module in slot 2 set off (Reset)
16:20:54: SP: OS_BOOT_STATUS(2) MP OS Boot Status: finished booting
*May 10 16:53:34.599: %DIAG-SP-6-RUN_MINIMUM: Module 2: Running Minimum Diagnostics...
*May 10 16:53:40.363: %DIAG-SP-6-DIAG_OK: Module 2: Passed Online Diagnostics
*May 10 16:53:40.759: %OIR-SP-6-INSCARD: Card inserted in slot 2, interfaces are now
online
```

```
Router# show module
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  1    2  Catalyst 6000 supervisor 2 (Active)    WS-X6K-S2U-MSFC2   SAD055006RZ
  2    2  SSL VPN Accelerator (MP)               WS-SVC-WEBVPN-K9

...<output truncated>...

Router# copy tftp: pclc#2-fs:

copy tftp pclc#2-fs:
Address or name of remote host []? 10.10.10.1
Source filename []? c6svc-webvpn-k9y9.1-1-1.bin
Destination filename [c6svc-webvpn-k9y9.1-1-1.bin]?
Accessing tftp://10.10.10.1/c6svc-webvpn-k9y9.1-1-1.bin...
Loading narenr/c6svc-webvpn-k9y9.1-1-1.bin from 10.10.10.1 (via Vlan6):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

...<output truncated>...

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 24944624 bytes]

24944624 bytes copied in 203.164 secs (122781 bytes/sec)
supervisor#
*May 10 17:01:40.323: %SVCLC-SP-5-STRRECVD: mod 2: <Application upgrade has started>
*May 10 17:01:40.323: %SVCLC-SP-5-STRRECVD: mod 2: <Do not reset the module till upgrade
completes!!>
*May 10 17:07:01.423: %SVCLC-SP-5-STRRECVD: mod 2: <Application upgrade has succeeded>
*May 10 17:07:01.423: %SVCLC-SP-5-STRRECVD: mod 2: <You can now reset the module>

Router# hw-module module 2 reset cf:4
Device BOOT variable for reset = <cf:4>
Warning: Device list is not verified.

Proceed with reload of module?[confirm]y
% reset issued for module 2
16:38:34: SP: The PC in slot 2 is shutting down. Please wait ...
16:38:57: SP: PC shutdown completed for module 2
*May 10 17:11:10.065: %C6KPWR-SP-4-DISABLED: power to module in slot 2 set off (Reset)
16:39:50: SP: OS_BOOT_STATUS(2) AP OS Boot Status: finished booting
*May 10 17:13:18.119: %DIAG-SP-6-RUN_MINIMUM: Module 2: Running Minimum Diagnostics...
*May 10 17:13:18.863: %DIAG-SP-6-DIAG_OK: Module 2: Passed Online Diagnostics
*May 10 17:13:19.195: %OIR-SP-6-INSCARD: Card inserted in slot 2, interfaces are now
online

Router# show module

Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  1    2  Catalyst 6000 supervisor 2 (Active)    WS-X6K-S2U-MSFC2   SAD055006RZ
  2    2  SSL VPN Accelerator                    WS-SVC-WEBVPN-K9

...<output truncated>...
```

Upgrading the Maintenance Software

Note Do not reset the module until the image is upgraded. The total time to upgrade the image takes up to 8 minutes.

To upgrade the maintenance partition software, perform this task:

	Command	Purpose
Step 1	`Router#` **`hw-module module`** *`mod`* **`reset cf:4`**	Reboots the module from the application partition.
Step 2	`Router#` **`show module`**	Displays that the application partition for the module has booted.
Step 3	`Router#` **`copy tftp: pclc#`***`mod`***`-fs:`**	Downloads the image.
Step 4	`Router#` **`hw-module module`** *`mod`* **`reset cf:1`**	Resets the module in the maintenance partition. **Note** Do not reset the module until the “Upgrade of MP was successful. You can now boot MP” message is displayed on the console. Resetting the module before this message is displayed will cause the upgrade to fail.
Step 5	`Router#` **`show module`**	Displays that the maintenance partition for the module has booted.

This example shows how to upgrade the maintenance partition software:

```
Router# hw module 2 reset cf:4
Device BOOT variable for reset = <cf:4>
Warning: Device list is not verified.

Proceed with reload of module?[confirm]y
% reset issued for module 2
16:43:51: SP: The PC in slot 2 is shutting down. Please wait ...
16:44:12: SP: PC shutdown completed for module 2
*May 10 17:16:25.271: %C6KPWR-SP-4-DISABLED: power to module in slot 2 set off (Reset)
16:45:05: SP: OS_BOOT_STATUS(2) AP OS Boot Status: finished booting
*May 10 17:18:33.363: %DIAG-SP-6-RUN_MINIMUM: Module 2: Running Minimum Diagnostics...
*May 10 17:18:34.103: %DIAG-SP-6-DIAG_OK: Module 2: Passed Online Diagnostics
*May 10 17:18:34.439: %OIR-SP-6-INSCARD: Card inserted in slot 2, interfaces are now
online

Router# show module

Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  1    2  Catalyst 6000 supervisor 2 (Active)    WS-X6K-S2U-MSFC2   SAD055006RZ
  2    2  SSL VPN Accelerator                    WS-SVC-WEBVPN-K9

...<output truncated>...
```

```
Router# copy tftp: pclc#2-fs:
Address or name of remote host []? 10.10.10.1
Source filename []? mp.3-3-1.bin.gz
Destination filename [mp.3-3-1.bin.gz]?
Accessing tftp://10.10.10.1/mp.3-3-1.bin.gz...
Loading mp.3-3-1.bin.gz from 10.10.10.1 (via Vlan6):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!

...<output truncated>...

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 12342623 bytes]

12342623 bytes copied in 99.908 secs (123540 bytes/sec)
*May 10 17:21:05.423: %SVCLC-SP-5-STRRECVD: mod 2: <MP upgrade/Password Recovery started.>
*May 10 17:21:05.991: %SVCLC-SP-5-STRRECVD: mod 2: <Uncompress of the file succeeded.
Continuing upgrade/recovery.>
*May 10 17:21:06.015: %SVCLC-SP-5-STRRECVD: mod 2: <This file appears to be a MP upgrade.
Continuing upgrade.>
*May 10 17:21:06.039: %SVCLC-SP-5-STRRECVD: mod 2: <Install of the MBR succeeded .
Continuing upgrade.>
*May 10 17:21:06.115: %SVCLC-SP-5-STRRECVD: mod 2: <Install of GRUB succeeded. Continuing
upgrade.>
*May 10 17:22:02.295: %SVCLC-SP-5-STRRECVD: mod 2: <Copying of MP succeeded. Continuing
upgrade.>
*May 10 17:22:02.311: %SVCLC-SP-5-STRRECVD: mod 2: <fsck of MP partition succeeded.>
*May 10 17:22:02.343: %SVCLC-SP-5-STRRECVD: mod 2: <Upgrade of MP was successful. You can
now boot MP.>
Router#
Router# hw mod 2 reset cf:1
Device BOOT variable for reset = <cf:1>
Warning: Device list is not verified.

Proceed with reload of module?[confirm]y
% reset issued for module 2
17:02:03: SP: The PC in slot 2 is shutting down. Please wait ...
17:02:23: SP: PC shutdown completed for module 2
*May 10 17:34:36.399: %C6KPWR-SP-4-DISABLED: power to module in slot 2 set off (Reset)
17:05:02: SP: OS_BOOT_STATUS(2) MP OS Boot Status: finished booting
*May 10 17:37:42.223: %DIAG-SP-6-RUN_MINIMUM: Module 2: Running Minimum Diagnostics...
*May 10 17:37:48.007: %DIAG-SP-6-DIAG_OK: Module 2: Passed Online Diagnostics
*May 10 17:37:48.303: %OIR-SP-6-INSCARD: Card inserted in slot 2, interfaces are now
online
Router#
Router# show module
Mod Ports Card Type                              Model              Serial No.
--- ----- -------------------------------------- ------------------ -----------
  1    2  Catalyst 6000 supervisor 2 (Active)    WS-X6K-S2U-MSFC2   SAD055006RZ
  2    2  SSL VPN Accelerator (MP)               WS-SVC-WEBVPN-K9

...<output truncated>...
```

Installing the SVC Package for Tunnel Mode

Before end users can download and install the SSL VPN client (SVC) to their PC, you must first install the SVC package to the Flash: device on the WebVPN Services Module.

To install the SVC package, perform this task:

	Command	Purpose
Step 1	`webvpn#` **`copy tftp: flash:/webvpn`**	Copies the SVC package to the Flash: device on the WebVPN Services Module. **Note** At the "Destination filename" prompt, rename the source filename to **svc.pkg**.
Step 2	`webvpn#` **`dir flash:/webvpn`**	Displays the contents of the Flash: device on the WebVPN Services Module. Confirm that the **svc.pkg** file is installed.
Step 3	`Router#` **`hw module`** *`mod`* **`reset cf:4`**	Reboots the WebVPN Services Module. **Note** When the WebVPN Services Module comes up, the SVC package stored in the Flash: device is extracted and stored in the cache file system. The WebVPN Services Module is now ready to service download requests sent from end users.
Step 4	`webvpn#` **`show webvpn install status svc`**	Displays the status of the installed SVC package.

This example shows how to install the SVC package:

- To download and install the SVC package, enter the following commands at the WebVPN Services Module CLI:

```
webvpn# copy tftp: flash:/webvpn
Address or name of remote host [10.1.1.1]?
Source filename []? <username>/sslclient-win-1.0.0.pkg
Destination filename [sslclient-win-1.0.0.pkg]? svc.pkg
%Warning:There is a file already existing with this name
Do you want to over write? [confirm] y
Accessing tftp://10.1.1.1/sslclient-win-1.0.0.pkg.zip...
Loading sslclient-win-1.0.0.pkg.zip from 10.1.1.1
(via WebVPN0.1): !!O!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 300265 bytes]
300265 bytes copied in 8.032 secs (37384 bytes/sec)
webvpn#
webvpn# dir flash:/webvpn
Directory of flash:/webvpn/
4 -rwx 300265 Apr 26 2005 00:41:16 +00:00 svc.pkg
16386048 bytes total (16072704 bytes free)
```

- To reboot the WebVPN Services Module, enter the following commands at the supervisor engine CLI:

```
Router# hw module 6 reset cf:4
Device BOOT variable for reset = <empty>
Warning:Device list is not verified.
Proceed with reload of module? [confirm]y
% reset issued for module 6
Router#
02:36:57:SP:The PC in slot 6 is shutting down. Please wait ...
02:37:17:SP:PC shutdown completed for module 6
02:37:17:%C6KPWR-SP-4-DISABLED:power to module in slot 6 set off (Reset)
1w0d:SP:OS_BOOT_STATUS(6) AP OS Boot Status:finished booting
1w0d:%OIR-SP-6-INSCARD:Card inserted in slot 6, interfaces are now online
```

- To display the status of the SVC package, enter the following command at the WebVPN Services Module CLI:

```
webvpn# show webvpn install status svc
SSLVPN Package SSL-VPN-Client version installed:
CISCO STC win2k+ 1.0.0
1,0,0
Tue 03/08/2005 15:31:20.43
```

APPENDIX D

Color Names and RGB Color Values

Table D-1 shows the valid values for *color* when entering the **title-color** *color* and **secondary-color** *color* commands in the WebVPN context. The default color is purple.

The value can be the name of the color that is recognized in HTML (no spaces between words or characters) or a comma-separated red, green, blue (RGB) value. The value is limited to 32 characters.

Note All browsers support the RGB value; however, not all browsers support the color name. If you enter a color name and do not get the expected results, use the RGB value for the color.

The following examples show different ways to configure the title color:

- `webvpn(config-webvpn-context)# title-color darkseagreen`
- `webvpn(config-webvpn-context)# title-color 143,188,143`

Table D-1 Color Names and RGB Values

Color Name	R	G	B
AliceBlue	240	248	255
AntiqueWhite	250	235	215
AntiqueWhite1	255	239	219
AntiqueWhite2	238	223	204
AntiqueWhite3	205	192	176
AntiqueWhite4	139	131	120
Aquamarine	127	255	212
Aquamarine1	127	255	212
Aquamarine2	118	238	198
Aquamarine3	102	205	170
Aquamarine4	69	139	116
Azure	240	255	255
Azure1	240	255	255
Azure2	224	238	238
Azure3	193	205	205
Azure4	131	139	139

Table D-1 Color Names and RGB Values (continued)

Color Name	R	G	B
Beige	245	245	220
Bisque	255	228	196
Bisque1	255	228	196
Bisque2	238	213	183
Bisque3	205	183	158
Bisque4	139	125	107
Black	0	0	0
BlanchedAlmond	255	235	205
Blue	0	0	255
Blue1	0	0	255
Blue2	0	0	238
Blue3	0	0	205
Blue4	0	0	139
BlueViolet	138	43	226
Brown	165	42	42
Brown1	255	64	64
Brown2	238	59	59
Brown3	205	51	51
Brown4	139	35	35
Burlywood	222	184	135
Burlywood1	255	211	155
Burlywood2	238	197	145
Burlywood3	205	170	125
Burlywood4	139	115	85
CadetBlue	95	158	160
CadetBlue1	152	245	255
CadetBlue2	142	229	238
CadetBlue3	122	197	205
CadetBlue4	83	134	139
Chartreuse	127	255	0
Chartreuse1	127	255	0
Chartreuse2	118	238	0
Chartreuse3	102	205	0
Chartreuse4	69	139	0
Chocolate	210	105	30
Chocolate1	255	127	36

Table D-1 Color Names and RGB Values (continued)

Color Name	R	G	B
Chocolate2	238	118	33
Chocolate3	205	102	29
Chocolate4	139	69	19
Coral	255	127	80
Coral1	255	114	86
Coral2	238	106	80
Coral3	205	91	69
Coral4	139	62	47
CornflowerBlue	100	149	237
Cornsilk	255	248	220
Cornsilk1	255	248	220
Cornsilk2	238	232	205
Cornsilk3	205	200	177
Cornsilk4	139	136	120
Cyan	0	255	255
Cyan1	0	255	255
Cyan2	0	238	238
Cyan3	0	205	205
Cyan4	0	139	139
DarkBlue	0	0	139
DarkCyan	0	139	139
DarkGoldenrod	184	134	11
DarkGoldenrod1	255	185	15
DarkGoldenrod2	238	173	14
DarkGoldenrod3	205	149	12
DarkGoldenrod4	139	101	8
DarkGray	169	169	169
DarkGreen	0	100	0
DarkKhaki	189	183	107
DarkMagenta	139	0	139
DarkOliveGreen	85	107	47
DarkOliveGreen1	202	255	112
DarkOliveGreen2	188	238	104
DarkOliveGreen3	162	205	90
DarkOliveGreen4	110	139	61
DarkOrange	255	140	0

Table D-1 Color Names and RGB Values (continued)

Color Name	R	G	B
DarkOrange1	255	127	0
DarkOrange2	238	118	0
DarkOrange3	205	102	0
DarkOrange4	139	69	0
DarkOrchid	153	50	204
DarkOrchid1	191	62	255
DarkOrchid2	178	58	238
DarkOrchid3	154	50	205
DarkOrchid4	104	34	139
DarkRed	139	0	0
DarkSalmon	233	150	122
DarkSeaGreen	143	188	143
DarkSeaGreen1	193	255	193
DarkSeaGreen2	180	238	180
DarkSeaGreen3	155	205	155
DarkSeaGreen4	105	139	105
DarkSlateBlue	72	61	139
DarkSlateGray	47	79	79
DarkSlateGray1	151	255	255
DarkSlateGray2	141	238	238
DarkSlateGray3	121	205	205
DarkSlateGray4	82	139	139
DarkTurquoise	0	206	209
DarkViolet	148	0	211
DeepPink	255	20	147
DeepPink1	255	20	147
DeepPink2	238	18	137
DeepPink3	205	16	118
DeepPink4	139	10	80
DeepSkyBlue	0	191	255
DeepSkyBlue1	0	191	255
DeepSkyBlue2	0	178	238
DeepSkyBlue3	0	154	205
DeepSkyBlue4	0	104	139
DimGrey	105	105	105
DodgerBlue	30	144	255

Table D-1 Color Names and RGB Values (continued)

Color Name	R	G	B
DodgerBlue1	30	144	255
DodgerBlue2	28	134	238
DodgerBlue3	24	116	205
DodgerBlue4	16	78	139
Firebrick	178	34	34
Firebrick1	255	48	48
Firebrick2	238	44	44
Firebrick3	205	38	38
Firebrick4	139	26	26
FloralWhite	255	250	240
ForestGreen	34	139	34
Gainsboro	220	220	220
GhostWhite	248	248	255
Gold	255	215	0
Gold1	255	215	0
Gold2	238	201	0
Gold3	205	173	0
Gold4	139	117	0
Goldenrod	218	165	32
Goldenrod1	255	193	37
Goldenrod2	238	180	34
Goldenrod3	205	155	29
Goldenrod4	139	105	20
Gray0	0	0	0
Gray1	3	3	3
Gray10	26	26	26
Gray100	255	255	255
Gray11	28	28	28
Gray12	31	31	31
Gray13	33	33	33
Gray14	36	36	36
Gray15	38	38	38
Gray16	41	41	41
Gray17	43	43	43
Gray18	46	46	46
Gray19	48	48	48

Table D-1 Color Names and RGB Values (continued)

Color Name	R	G	B
Gray2	5	5	5
Gray20	51	51	51
Gray21	54	54	54
Gray22	56	56	56
Gray23	59	59	59
Gray24	61	61	61
Gray25	64	64	64
Gray26	66	66	66
Gray27	69	69	69
Gray28	71	71	71
Gray29	74	74	74
Gray3	8	8	8
Gray30	77	77	77
Gray31	79	79	79
Gray32	82	82	82
Gray33	84	84	84
Gray34	87	87	87
Gray35	89	89	89
Gray36	92	92	92
Gray37	94	94	94
Gray38	97	97	97
Gray39	99	99	99
Gray4	10	10	10
Gray40	102	102	102
Gray41	105	105	105
Gray42	107	107	107
Gray43	110	110	110
Gray44	112	112	112
Gray45	115	115	115
Gray46	117	117	117
Gray47	120	120	120
Gray48	122	122	122
Gray49	125	125	125
Gray5	13	13	13
Gray50	127	127	127
Gray51	130	130	130

Table D-1 Color Names and RGB Values (continued)

Color Name	R	G	B
Gray52	133	133	133
Gray53	135	135	135
Gray54	138	138	138
Gray55	140	140	140
Gray56	143	143	143
Gray57	145	145	145
Gray58	148	148	148
Gray59	150	150	150
Gray6	15	15	15
Gray60	153	153	153
Gray61	156	156	156
Gray62	158	158	158
Gray63	161	161	161
Gray64	163	163	163
Gray65	166	166	166
Gray66	168	168	168
Gray67	171	171	171
Gray68	173	173	173
Gray69	176	176	176
Gray7	18	18	18
Gray70	179	179	179
Gray71	181	181	181
Gray72	184	184	184
Gray73	186	186	186
Gray74	189	189	189
Gray75	191	191	191
Gray76	194	194	194
Gray77	196	196	196
Gray78	199	199	199
Gray79	201	201	201
Gray8	20	20	20
Gray80	204	204	204
Gray81	207	207	207
Gray82	209	209	209
Gray83	212	212	212
Gray84	214	214	214

Table D-1 Color Names and RGB Values (continued)

Color Name	R	G	B
Gray85	217	217	217
Gray86	219	219	219
Gray87	222	222	222
Gray88	224	224	224
Gray89	227	227	227
Gray9	23	23	23
Gray90	229	229	229
Gray91	232	232	232
Gray92	235	235	235
Gray93	237	237	237
Gray94	240	240	240
Gray95	242	242	242
Gray96	245	245	245
Gray97	247	247	247
Gray98	250	250	250
Gray99	252	252	252
Green	0	255	0
Green1	0	255	0
Green2	0	238	0
Green3	0	205	0
Green4	0	139	0
GreenYellow	173	255	47
Grey	190	190	190
Grey0	0	0	0
Grey1	3	3	3
Grey10	26	26	26
Grey100	255	255	255
Grey11	28	28	28
Grey12	31	31	31
Grey13	33	33	33
Grey14	36	36	36
Grey15	38	38	38
Grey16	41	41	41
Grey17	43	43	43
Grey18	46	46	46
Grey19	48	48	48

Table D-1 Color Names and RGB Values (continued)

Color Name	R	G	B
Grey2	5	5	5
Grey20	51	51	51
Grey21	54	54	54
Grey22	56	56	56
Grey23	59	59	59
Grey24	61	61	61
Grey25	64	64	64
Grey26	66	66	66
Grey27	69	69	69
Grey28	71	71	71
Grey29	74	74	74
Grey3	8	8	8
Grey30	77	77	77
Grey31	79	79	79
Grey32	82	82	82
Grey33	84	84	84
Grey34	87	87	87
Grey35	89	89	89
Grey36	92	92	92
Grey37	94	94	94
Grey38	97	97	97
Grey39	99	99	99
Grey4	10	10	10
Grey40	102	102	102
Grey41	105	105	105
Grey42	107	107	107
Grey43	110	110	110
Grey44	112	112	112
Grey45	115	115	115
Grey46	117	117	117
Grey47	120	120	120
Grey48	122	122	122
Grey49	125	125	125
Grey5	13	13	13
Grey50	127	127	127
Grey51	130	130	130

Table D-1 Color Names and RGB Values (continued)

Color Name	R	G	B
Grey52	133	133	133
Grey53	135	135	135
Grey54	138	138	138
Grey55	140	140	140
Grey56	143	143	143
Grey57	145	145	145
Grey58	148	148	148
Grey59	150	150	150
Grey6	15	15	15
Grey60	153	153	153
Grey61	156	156	156
Grey62	158	158	158
Grey63	161	161	161
Grey64	163	163	163
Grey65	166	166	166
Grey66	168	168	168
Grey67	171	171	171
Grey68	173	173	173
Grey69	176	176	176
Grey7	18	18	18
Grey70	179	179	179
Grey71	181	181	181
Grey72	184	184	184
Grey73	186	186	186
Grey74	189	189	189
Grey75	191	191	191
Grey76	194	194	194
Grey77	196	196	196
Grey78	199	199	199
Grey79	201	201	201
Grey8	20	20	20
Grey80	204	204	204
Grey81	207	207	207
Grey82	209	209	209
Grey83	212	212	212
Grey84	214	214	214

Table D-1 Color Names and RGB Values (continued)

Color Name	R	G	B
Grey85	217	217	217
Grey86	219	219	219
Grey87	222	222	222
Grey88	224	224	224
Grey89	227	227	227
Grey9	23	23	23
Grey90	229	229	229
Grey91	232	232	232
Grey92	235	235	235
Grey93	237	237	237
Grey94	240	240	240
Grey95	242	242	242
Grey96	245	245	245
Grey97	247	247	247
Grey98	250	250	250
Grey99	252	252	252
Honeydew	240	255	240
Honeydew1	240	255	240
Honeydew2	224	238	224
Honeydew3	193	205	193
Honeydew4	131	139	131
HotPink	255	105	180
HotPink1	255	110	180
HotPink2	238	106	167
HotPink3	205	96	144
HotPink4	139	58	98
IndianRed	205	92	92
IndianRed1	255	106	106
IndianRed2	238	99	99
IndianRed3	205	85	85
IndianRed4	139	58	58
Ivory	255	255	240
Ivory1	255	255	240
Ivory2	238	238	224
Ivory3	205	205	193
Ivory4	139	139	131

Table D-1 Color Names and RGB Values (continued)

Color Name	R	G	B
Khaki	240	230	140
Khaki1	255	246	143
Khaki2	238	230	133
Khaki3	205	198	115
Khaki4	139	134	78
Lavender	230	230	250
LavenderBlush	255	240	245
LavenderBlush1	255	240	245
LavenderBlush2	238	224	229
LavenderBlush3	205	193	197
LavenderBlush4	139	131	134
LawnGreen	124	252	0
LemonChiffon	255	250	205
LemonChiffon1	255	250	205
LemonChiffon2	238	233	191
LemonChiffon3	205	201	165
LemonChiffon4	139	137	112
LightBlue	173	216	230
LightBlue1	191	239	255
LightBlue2	178	223	238
LightBlue3	154	192	205
LightBlue4	104	131	139
LightCoral	240	128	128
LightCyan	224	255	255
LightCyan1	224	255	255
LightCyan2	209	238	238
LightCyan3	180	205	205
LightCyan4	122	139	139
LightGoldenrod	238	221	130
LightGoldenrod1	255	236	139
LightGoldenrod2	238	220	130
LightGoldenrod3	205	190	112
LightGoldenrod4	139	129	76
LightGoldenrodYellow	250	250	210
LightGreen	144	238	144
LightGrey	211	211	211

Table D-1 Color Names and RGB Values (continued)

Color Name	R	G	B
LightPink	255	182	193
LightPink1	255	174	185
LightPink2	238	162	173
LightPink3	205	140	149
LightPink4	139	95	101
LightSalmon	255	160	122
LightSalmon1	255	160	122
LightSalmon2	238	149	114
LightSalmon3	205	129	98
LightSalmon4	139	87	66
LightSeaGreen	32	178	170
LightSkyBlue	135	206	250
LightSkyBlue1	176	226	255
LightSkyBlue2	164	211	238
LightSkyBlue3	141	182	205
LightSkyBlue4	96	123	139
LightSlateBlue	132	112	255
LightSlateGray	119	136	153
LightSteelBlue	176	196	222
LightSteelBlue1	202	225	255
LightSteelBlue2	188	210	238
LightSteelBlue3	162	181	205
LightSteelBlue4	110	123	139
LightYellow	255	255	224
LightYellow1	255	255	224
LightYellow2	238	238	209
LightYellow3	205	205	180
LightYellow4	139	139	122
LimeGreen	50	205	50
Linen	250	240	230
Magenta	255	0	255
Magenta1	255	0	255
Magenta2	238	0	238
Magenta3	205	0	205
Magenta4	139	0	139
Maroon	176	48	96

Table D-1 Color Names and RGB Values (continued)

Color Name	R	G	B
Maroon1	255	52	179
Maroon2	238	48	167
Maroon3	205	41	144
Maroon4	139	28	98
MediumAquamarine	102	205	170
MediumBlue	0	0	205
MediumOrchid	186	85	211
MediumOrchid1	224	102	255
MediumOrchid2	209	95	238
MediumOrchid3	180	82	205
MediumOrchid4	122	55	139
MediumPurple	147	112	219
MediumPurple1	171	130	255
MediumPurple2	159	121	238
MediumPurple3	137	104	205
MediumPurple4	93	71	139
MediumSeaGreen	60	179	113
MediumSlateBlue	123	104	238
MediumSpringGreen	0	250	154
MediumTurquoise	72	209	204
MediumVioletRed	199	21	133
MidnightBlue	25	25	112
MintCream	245	255	250
MistyRose	255	228	225
MistyRose1	255	228	225
MistyRose2	238	213	210
MistyRose3	205	183	181
MistyRose4	139	125	123
Moccasin	255	228	181
NavajoWhite	255	222	173
NavajoWhite1	255	222	173
NavajoWhite2	238	207	161
NavajoWhite3	205	179	139
NavajoWhite4	139	121	94
Navy	0	0	128
NavyBlue	0	0	128

Table D-1 Color Names and RGB Values (continued)

Color Name	R	G	B
OldLace	253	245	230
OliveDrab	107	142	35
OliveDrab1	192	255	62
OliveDrab2	179	238	58
OliveDrab3	154	205	50
OliveDrab4	105	139	34
Orange	255	165	0
Orange1	255	165	0
Orange2	238	154	0
Orange3	205	133	0
Orange4	139	90	0
OrangeRed	255	69	0
OrangeRed1	255	69	0
OrangeRed2	238	64	0
OrangeRed3	205	55	0
OrangeRed4	139	37	0
Orchid	218	112	214
Orchid1	255	131	250
Orchid2	238	122	233
Orchid3	205	105	201
Orchid4	139	71	137
PaleGoldenrod	238	232	170
PaleGreen	152	251	152
PaleGreen1	154	255	154
PaleGreen2	144	238	144
PaleGreen3	124	205	124
PaleGreen4	84	139	84
PaleTurquoise	175	238	238
PaleTurquoise1	187	255	255
PaleTurquoise2	174	238	238
PaleTurquoise3	150	205	205
PaleTurquoise4	102	139	139
PaleVioletRed	219	112	147
PaleVioletRed1	255	130	171
PaleVioletRed2	238	121	159
PaleVioletRed3	205	104	137

Table D-1 Color Names and RGB Values (continued)

Color Name	R	G	B
PaleVioletRed4	139	71	93
PapayaWhip	255	239	213
PeachPuff	255	218	185
PeachPuff1	255	218	185
PeachPuff2	238	203	173
PeachPuff3	205	175	149
PeachPuff4	139	119	101
Peru	205	133	63
Pink	255	192	203
Pink1	255	181	197
Pink2	238	169	184
Pink3	205	145	158
Pink4	139	99	108
Plum	221	160	221
Plum1	255	187	255
Plum2	238	174	238
Plum3	205	150	205
Plum4	139	102	139
PowderBlue	176	224	230
Purple	160	32	240
Purple1	155	48	255
Purple2	145	44	238
Purple3	125	38	205
Purple4	85	26	139
Red	255	0	0
Red1	255	0	0
Red2	238	0	0
Red3	205	0	0
Red4	139	0	0
RosyBrown	188	143	143
RosyBrown1	255	193	193
RosyBrown2	238	180	180
RosyBrown3	205	155	155
RosyBrown4	139	105	105
RoyalBlue	65	105	225
RoyalBlue1	72	118	255

Table D-1 Color Names and RGB Values (continued)

Color Name	R	G	B
RoyalBlue2	67	110	238
RoyalBlue3	58	95	205
RoyalBlue4	39	64	139
SaddleBrown	139	69	19
Salmon	250	128	114
Salmon1	255	140	105
Salmon2	238	130	98
Salmon3	205	112	84
Salmon4	139	76	57
SandyBrown	244	164	96
SeaGreen	46	139	87
SeaGreen1	84	255	159
SeaGreen2	78	238	148
SeaGreen3	67	205	128
SeaGreen4	46	139	87
Seashell	255	245	238
Seashell1	255	245	238
Seashell2	238	229	222
Seashell3	205	197	191
Seashell4	139	134	130
Sienna	160	82	45
Sienna1	255	130	71
Sienna2	238	121	66
Sienna3	205	104	57
Sienna4	139	71	38
SkyBlue	135	206	235
SkyBlue1	135	206	255
SkyBlue2	126	192	238
SkyBlue3	108	166	205
SkyBlue4	74	112	139
SlateBlue	106	90	205
SlateBlue1	131	111	255
SlateBlue2	122	103	238
SlateBlue3	105	89	205
SlateBlue4	71	60	139
SlateGray	112	128	144

Table D-1 Color Names and RGB Values (continued)

Color Name	R	G	B
SlateGray1	198	226	255
SlateGray2	185	211	238
SlateGray3	159	182	205
SlateGray4	108	123	139
Snow	255	250	250
Snow1	255	250	250
Snow2	238	233	233
Snow3	205	201	201
Snow4	139	137	137
SpringGreen	0	255	127
SpringGreen1	0	255	127
SpringGreen2	0	238	118
SpringGreen3	0	205	102
SpringGreen4	0	139	69
SteelBlue	70	130	180
SteelBlue1	99	184	255
SteelBlue2	92	172	238
SteelBlue3	79	148	205
SteelBlue4	54	100	139
Tan	210	180	140
Tan1	255	165	79
Tan2	238	154	73
Tan3	205	133	63
Tan4	139	90	43
Thistle	216	191	216
Thistle1	255	225	255
Thistle2	238	210	238
Thistle3	205	181	205
Thistle4	139	123	139
Tomato	255	99	71
Tomato1	255	99	71
Tomato2	238	92	66
Tomato3	205	79	57
Tomato4	139	54	38
Turquoise	64	224	208
Turquoise1	0	245	255

Table D-1 Color Names and RGB Values (continued)

Color Name	R	G	B
Turquoise2	0	229	238
Turquoise3	0	197	205
Turquoise4	0	134	139
Violet	238	130	238
VioletRed	208	32	144
VioletRed1	255	62	150
VioletRed2	238	58	140
VioletRed3	205	50	120
VioletRed4	139	34	82
Wheat	245	222	179
Wheat1	255	231	186
Wheat2	238	216	174
Wheat3	205	186	150
Wheat4	139	126	102
White	255	255	255
WhiteSmoke	245	245	245
Yellow	255	255	0
Yellow1	255	255	0
Yellow2	238	238	0
Yellow3	205	205	0
Yellow4	139	139	0
YellowGreen	154	205	50

INDEX