

Symantec™ Gateway Security 300 Series Installation Guide

Supported models:

Models 320, 360, and 360R



Symantec™ Gateway Security 300 Series Installation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 1.0

February 12, 2004

Copyright notice

Copyright © 1998–2004 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Symantec, the Symantec logo, and Norton AntiVirus are U.S. registered trademarks of Symantec Corporation. LiveUpdate, LiveUpdate Administration Utility, Symantec AntiVirus, and Symantec Security Response are trademarks of Symantec Corporation.

Other brands and product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide

Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components that provide rapid response and up-to-the-minute information
- Upgrade insurance that delivers automatic software upgrade protection
- Content Updates for virus definitions and security signatures that ensure the highest level of protection
- Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages for those customers enrolled in the Platinum Support program
- Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our Web site for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

Licensing and registration

See “[Licensing](#)” on page 47.

Contacting Technical Support

Customers with a current maintenance agreement may contact the Technical Support group by phone or online at www.symantec.com/techsupp/.

Customers with Platinum support agreements may contact Platinum Technical Support by the Platinum Web site at www-secure.symantec.com/platinum/.

When contacting the Technical Support group, please have the following:

- Product release level
- Hardware information
- Available memory, disk space, NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description
- Error messages/log files
- Troubleshooting performed prior to contacting Symantec

- Recent software configuration changes and/or network changes

Customer Service

To contact Enterprise Customer Service online, go to www.symantec.com/techsupp/, select the appropriate Global Site for your country, then select the enterprise Continue link. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advice on Symantec's technical support options
- Nontechnical presales questions
- Missing or defective CD-ROMs or manuals

Contents

Chapter 1	Introducing the Symantec Gateway Security 300 Series	
	Intended audience	8
	Document structure	8
	Where to get more information	9
	Checking the components list	9
	Replacement CD-ROMs	10
Chapter 2	Installing the Symantec Gateway Security 300 Series appliance	
	Planning for installation	11
	Installing the appliance	12
	Connecting the appliance to the network	14
	Powering the appliance	14
	Configuring the appliance	15
Chapter 3	Running the Setup Wizard	
	About the Setup Wizard	17
	Understanding connection types	17
	DHCP	19
	DSL	20
	Static IP address	21
	Dial-up/ISDN	22
	Running the Setup Wizard	23
	Before you begin	24
	Starting the Setup Wizard	24
	Setting up Dialup/ISDN	25
	Configuring a DHCP connection	26
	Configuring a DSL connection	27
	Configuring a static IP address connection	27
	Completing the Setup Wizard	28
	Access the Security Gateway Management Interface (SGMI)	29

Appendix A	Developing a pre-installation security plan	
	About developing a security plan	31
	Defining your security policy	31
	Before writing your security plan	32
	Becoming security-conscious	33
	Educating users	33
	Involving the user community	34
	Filling out worksheets	34
	Defining your organization	34
	Site hardware information	37
	TCP/IP address	38
	Allowed TCP/IP services	40
	Web service information	42
	Access lists	42
	Defining your network architecture	45
Appendix B	Licensing	
	Session licensing for Symantec Gateway Security 300 Series	
	Client-to-Gateway VPN functions	47
	Additive session licenses	47
	SYMANTEC GATEWAY SECURITY APPLIANCE LICENSE AND WARRANTY AGREEMENT	48
Appendix C	Specifications and safety	
	Product specifications	53
	Safeguard instructions	55
	Product certifications	57
Appendix D	LEDs and DIP switches	
	About LEDs	59
	Interpreting the LEDs	60
	LiveUpdate LED status	61
	DIP switches	62
Appendix E	About troubleshooting	
	Accessing troubleshooting information	63
	Index	

Introducing the Symantec Gateway Security 300 Series

This chapter includes the following topics:

- [Intended audience](#)
- [Document structure](#)
- [Where to get more information](#)
- [Checking the components list](#)
- [Replacement CD-ROMs](#)

Symantec Gateway Security 300 Series appliances are Symantec's integrated security solution for the Remote Office/Branch Office (ROBO) and small office environments, with support for secure wireless LANs in any size office.

Symantec Gateway Security 300 Series provides integrated security by offering six security functions in the base product:

- Firewall
- IPsec Virtual Private Networks (VPNs) with hardware-assisted 3DES and AES encryption
- Intrusion detection
- Intrusion protection
- Static content filtering
- Antivirus policy enforcement (AVpe)

Intended audience

All these features are designed specifically for the small or remote office. These appliances are perfect for stand-alone environments or as a complement to Symantec Gateway Security 5400 Series appliances deployed at hub sites.

Symantec Gateway Security 300 Series models are wireless-capable. They have special wireless firmware and a CardBus slot that can accommodate an optional wireless network card consisting of an integrated 802.11b/g radio and antenna, to allow the highest possible integrated security for wireless LANs, when used with clients running the Symantec Client VPN software.

Intended audience

This manual is intended for system managers or administrators responsible for administering the Symantec Gateway Security 300 Series appliances.

Document structure

This manual is structured as follows:

Table 1-1 Document structure

Chapter	Title	Content
Chapter 2	Installing the Symantec Gateway Security 300 Series	Tells you how to do a stand-alone or rack mount install of the appliance.
Chapter 3	Running the Setup Wizard	Tells you how to run the Setup Wizard to configure the appliance.
Chapter 4	Verifying your installation	Lists procedures for checking that the appliance is installed and configured properly.
Appendix A	Developing a pre-installation plan	Lays out basic guidelines for developing an overall security plan and provides a checklist for assessing your security issues.
Appendix B	About licensing	Tells you how to obtain license files and lists GNU licenses.
Appendix C	About troubleshooting	Tells you where to find troubleshooting information.

Where to get more information

The Symantec Gateway Security 300 Series functionality is described in the following manuals:

- *Symantec™ Gateway Security 300 Series Installation Guide*
 The guide you are reading covers the physical installation of the appliance, the initial setup of the appliance and the Security Gateway Management Interface (SGMI).
- *Symantec™ Gateway Security 300 Series Administrator's Guide*
 This guide describes the SGMI. This guide covers topics related to the appliance and its related components, including: base components, access controls, secure tunnels, VPN policies, remote policies, and monitoring controls. It is provided in PDF format on the Symantec Gateway Security 300 Series software CD-ROM.

Checking the components list

After carefully unpacking the appliance, compare the actual kit contents with [Table 1-2](#) to ensure that you have received all ordered components.

Table 1-2 Components list

Part	Description
Appliance	A single stand-alone device.
Cables	<ul style="list-style-type: none"> ■ A power cord appropriate for the country in which the appliance will operate. ■ Network cable ■ Serial cable
Printed documentation	<i>Symantec Gateway Security 300 Series Quick Start Card</i>

Table 1-2 Components list (Continued)

Part	Description
Symantec Gateway Security 300 Series software CD-ROM	<p>AVpe</p> <ul style="list-style-type: none"> ■ AVpe client activation registration file <p>Documentation</p> <ul style="list-style-type: none"> ■ <i>Symantec Gateway Security 300 Series Administrator's Guide</i> (PDF) ■ <i>Symantec Gateway Security 300 Series Getting Started Guide</i> (PDF) ■ <i>Symantec Gateway Security 300 Series Installation Guide</i> (PDF) ■ <i>Symantec Gateway Security 300 Series Quick Start Card</i> (PDF) ■ <i>Symantec Gateway Security 300 Series Release Notes</i> (PDF) ■ Symantec Gateway Security 300 Series Help (JAR file) ■ Adobe Acrobat Reader <p>320</p> <ul style="list-style-type: none"> ■ Model 320 firmware <p>360</p> <ul style="list-style-type: none"> ■ Model 360 firmware <p>Tools</p> <ul style="list-style-type: none"> ■ FTP client software (Passive-mode, Microsoft Windows only)
Symantec Client VPN Version 8.0 CD-ROM	<p>Symantec Client VPN software</p> <p>The following documentation in PDF format:</p> <ul style="list-style-type: none"> ■ <i>Symantec Client VPN User's Guide</i> ■ <i>Symantec Client VPN Getting Started Cards</i> ■ <i>Symantec Client VPN Release Notes</i>

Replacement CD-ROMs

You may need to replace the media due to a defective or lost CD-ROM. If you need a replacement CD-ROM because it is defective, contact Customer Support.

If you require a new CD-ROM because you have lost it, contact your Sales Representative to purchase a new media kit.

Installing the Symantec Gateway Security 300 Series appliance

This chapter includes the following topics:

- [Planning for installation](#)
- [Installing the appliance](#)
- [Configuring the appliance](#)

This chapter contains information about preparing to install the Symantec Gateway Security 300 Series appliance, connecting it to the network, and turning on the power.

Planning for installation

Before you install your appliance, remove plastic cover sheet from the top of the appliance.

In preparation for installing your appliance, select an appropriate location for the appliance. The following guidelines help you select a location for the appliance:

- **Smooth and level surface**
Place the appliance on a smooth and level surface, such as the top of a computer table. Make sure that the area is clear of dust and debris.

- Plenty of air circulation
Ensure that there is adequate space (at least 1 inch) on all sides of the appliance to allow for air circulation to cool the machine. Never place objects or paper on top of the appliance.
- Proper power source
Install the appliance near a power source that is adequate and near enough the appliance that the power cord is not strained, stretched, or in danger of coming unplugged.
- Appliance and cables away from high-traffic areas
Install the appliance in an area that is out of the way of foot traffic.

Installing the appliance

This section describes the back panel of Symantec Gateway Security 300 Series models 320, 360, and 360R.

Figure 2-1 shows the back panel of model 320.

Figure 2-1 Model 320 back panel

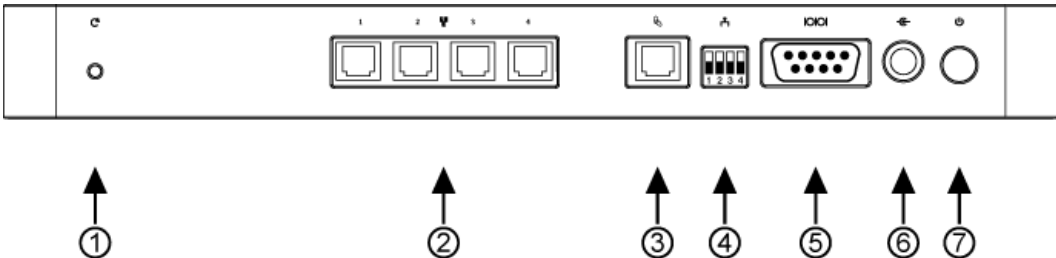


Figure 2-2 shows the back panel of models 360 and 360R.

Figure 2-2 Model 360 and 360R back panel

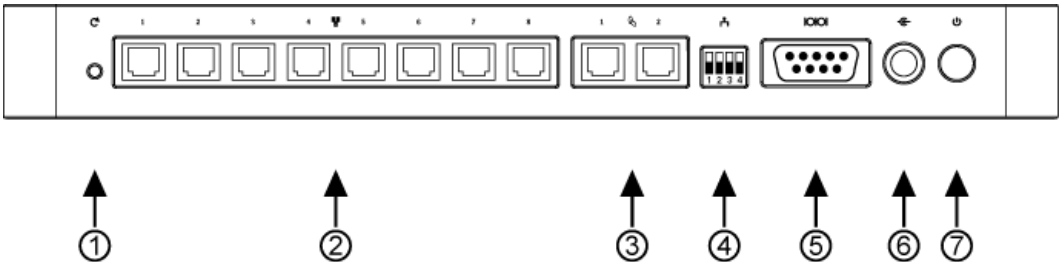









Table 2-1 describes the features and icons on the back panel of all the models.

Table 2-1 Symantec Gateway Security 300 Series back panel features

Location	Icon	Feature	Description
1		Restart	When you press this button, current connections and all client VPN tunnels are lost, all Gateway-to-Gateway VPN tunnels that were previously connected re-establish after the appliance restarts, and the initial hardware self-test is run. This button is recessed. Press it gently and quickly with a paper clip.
2		LAN ports	Model 320 has four Ethernet ports and models 360 and 360R have eight Ethernet ports to which you connect RJ-45 connectors from the nodes that the appliance protects.
3		WAN port	Model 320 has one Ethernet port and models 360 and 360R have two Ethernet ports to which you connect RJ-45 connectors from an outside network (such as an intranet) or the Internet.
4		DIP switches	The DIP switches are shown in the on (up) position. The default position is off (down). DIP switches provide additional functionality to the appliance. Generally, they are only used when performing tasks that involve manually updating the appliance.
5		Serial (modem) port	All the appliances have one serial port. If you use a modem and dial-up connection to provide Internet connectivity, you connect the modem to the serial port.
6		Power socket	Connect the power cord.
7		Power on/off	Turns the power supply to the appliance on or off.

Connecting the appliance to the network

You install the appliance by connecting it to your network with the LAN and WAN ports on the back panel of the appliance. Symantec Gateway Security 300 Series models 320, 360, and 360R have different numbers of LAN and WAN ports. [Table 2-2](#) briefly describes the appliance models and the LAN/WAN ports each has.

Table 2-2 Port distribution on models 320, 360, and 360R

Model	LAN ports	WAN ports
	Ethernet	Ethernet
320	4	1
360/360R	8	2

Generally, the WAN and serial ports provide connectivity to an outside network or the Internet, and the nodes that you are protecting connect to the LAN ports. See the *Symantec Gateway Security 300 Series Administrator's Guide* for more information.

Use the back panel location numbers from [Figure 2-1](#) when performing these steps.

To connect your appliance

- 1 In the WAN port (3) (WAN 1 on model 360 or 360R), plug in the RJ-45 connector from the outside network or your Internet connection.
- 2 For a dial-up Internet connection, connect the modem to the serial port (5). See the *Symantec Gateway Security 300 Series Administrator's Guide*. A serial modem cable is not included.
- 3 In one of the LAN ports (2), plug in the RJ-45 connector from a node that the appliance will protect.
The LAN ports are not ordered; you can plug any cable from a node into any of the LAN ports.
- 4 Repeat step 2 for up to four different nodes.

Powering the appliance

Use the back panel location numbers in [Figure 2-1](#) when you perform these instructions.

To connect the power cord to your appliance

- 1 Plug the power cord into the power socket on the back panel (6).
- 2 Connect the power cord from the appliance into an electrical outlet.
- 3 To turn on the appliance, press the power switch on the back panel (7).
The appliance power is functioning correctly if the LEDs illuminate.

Configuring the appliance

Once you have completed the physical installation of the appliance, you must log in and begin system configuration. The first time that you log in to the appliance, the Setup Wizard begins and guides you through an initial configuration. Proceed to [“Running the Setup Wizard”](#) on page 17.

Running the Setup Wizard

This chapter includes the following topics:

- [About the Setup Wizard](#)
- [Understanding connection types](#)
- [Dial-up/ISDN](#)
- [Running the Setup Wizard](#)
- [Access the Security Gateway Management Interface \(SGMI\)](#)

About the Setup Wizard

The Setup Wizard guides you through the steps required to connect your Symantec Gateway Security 300 Series WAN port (WAN 1 on models 360 and 360R) to the Internet, a corporate network, or any other external private or public network.

Understanding connection types

To connect the appliance to an outside or internal network, you must understand your connection type.

First, determine if you have a dial-up or broadband account. If you have a dial-up account, proceed to Dialup/ISDN. If you have a dedicated account, determine the connection type by reading the following table, and then proceed to the appropriate configuration section.

Typical dial-up accounts are analog (through a normal phone line connected to an external modem) and ISDN (through a special phone line). Typical broadband

accounts are broadband cable, DSL, T1/E1, or T3 connected to a terminal adaptor.

Note: Connect only RJ-45 cables to the WAN ports.

The following tables describe the supported connection types. The Connection type column is the option button you click on the Main Setup tab or in the Setup Wizard. The Services column is the types of accounts or protocols that are associated with the connection type. The Network termination types column lists the physical devices that a particular connection type typically uses to connect to the Internet or a network.

[Table 3-1](#) lists the supported dial-up connection types and ways you can identify them.

Table 3-1 Dial-up connection types

Connection type	Services	Network termination types
Analog or ISDN	Plain Old Telephone Service (POTS)	Analog dial-up modem
	Integrated Services Digital Network (ISDN)	Digital dial-up modem An ISDN modem is sometimes called a terminal adaptor.

If you have a broadband account, refer to [Table 3-2](#) to determine which connection type you have.

Table 3-2 Broadband connection types

Connection type	Services	Network termination types
DHCP	Broadband cable	Cable modem
	Digital Subscriber Line (DSL)	DSL modem with Ethernet cable
	Direct Ethernet connection	Ethernet Cable (usually an enclave network)
PPPoE	PPPoE	ADSL modem with Ethernet cable

Table 3-2 Broadband connection types (Continued)

Connection type	Services	Network termination types
Static IP (Static IP & DNS)	Broadband cable	Cable modem
	Digital Subscriber Line (DSL)	DSL modem
	T1	Channel Service Unit/Digital Service Unit (CSU/DSU)
	Direct Ethernet connection	Ethernet cable (usually an enclave network)
PPTP	PPTP	DSL modem with Ethernet cable

The following connection methods are supported by Symantec Gateway Security 300 Series:

- [DHCP](#)
- [DSL](#)
- [Static IP address](#)
- [Dial-up/ISDN](#)

DHCP

Dynamic Host Configuration Protocol (DHCP) automates the network configuration of computers. It enables a network with many clients to extract configuration information from a single server (DHCP server). In the case of a dedicated Internet account, the users are the clients extracting information from the ISP's DHCP server, and IP addresses are only assigned to connected accounts.

The account you have with your ISP may use DHCP to allocate IP addresses to you. Account types that frequently use DHCP are broadband cable and DSL. ISPs may authenticate broadband cable connections using the MAC address or physical address of your computer or gateway.

If you are using the security gateway on a pre-existing broadband cable connection, you can change the appliance to match the existing MAC address. If this is a new connection, you can obtain the physical address in the Setup Wizard for your ISP.

DSL

DSL ISPs provide Internet service by allocating IP addresses by DHCP, or they may assign your account a static IP address.

DSL ISPs use Point-to-Point Protocol over Ethernet (PPPoE) or Point-to-Point Tunneling Protocol (PPTP) technologies for user authentication of network connections.

Note: Point to Point Protocol over ATM (PPPoA) is not supported.

PPPoE

Point-to-Point Protocol over Ethernet (PPPoE) is used by many Asymmetrical Digital Subscriber Line (ASDL) providers. It is a specification for connecting many users on a network to the Internet through a single dedicated medium, such as a DSL account.

You can specify whether you connect or disconnect your PPPoE account manually or automatically. This is useful to verify connectivity.

You can configure the appliance to connect only when an Internet request is made from a user on the LAN (for example, browsing to a Web site) and disconnect when the connection is idle (unused). This feature is useful if your ISP charges on a per-usage time basis.

You can use multiple logins (if your ISP account allows multi-session PPPoE) to obtain additional IP addresses for the WAN. These are called PPPoE sessions. The login may be the same user name and password as the main session or may be different for each session, depending on your ISP. Up to five sessions or IP addresses are allowed for model 320 and up to three sessions for each WAN port on models 360 and 360R. LAN hosts are bound to a session on the Computers tab. See [“Configuring LAN IP settings”](#) on page 57.

Note: Multiple IP addresses on a WAN port are only supported for PPPoE connections.

By default, all settings are associated with Session 1. For multi-session PPPoE Accounts, configure each session individually. If you have multiple PPPoE accounts, assign each one to a different session in the SGMI.

Before configuring the WAN ports to use a PPPoE account, gather the following information:

- User name and password
All PPPoE accounts require user names and passwords. Get this information from your ISP before configuring PPPoE.
- Static IP address
You may have purchased or are assigned a static IP address for the PPPoE account.

PPTP

Point-to-Point-Tunneling Protocol (PPTP) is a protocol that enables a secure data transfer from a client to a server by creating a tunnel over a TCP/IP-based network. Symantec Gateway Security 300 Series appliances act as a PPTP access client (PAC) when you connect to a PPTP Network Server (PNS), generally with your ISP.

Some ADSL ISPs charge for connection time. The Symantec Gateway Security 300 Series reduces these costs by only connecting to your ISP when you use the Internet, and disconnecting when you are idle.

Before beginning PPTP configuration, gather the following information:

- PPTP server IP address
IP address of the PPTP server at the ISP.
- Static IP address
IP address assigned to your account.
- Account information
User name and password to log in to the account.

Static IP address

When you get an account with an ISP, you may have the option to purchase a static (permanent) IP address. This enables you to run a server, such as a Web or FTP server, because the address remains the same, all the time. Any type account (dial-up or broadband) can have a static IP address.

The appliance forwards any DNS lookup request to the specified DNS server for name resolution. The appliance supports up to three DNS servers. When you specify multiple DNS servers, they are used in sequence. For example, after the first server is used, the next request is forwarded to the second server and so on.

If you have a static IP address with your ISP or are using the appliance behind another security gateway device, select Static IP and DNS for your connection type. You can specify your static IP address and the IP addresses of the DNS servers you want to use for name resolution.

Before configuring the appliance to connect with your static IP account, gather the following information:

- Static IP, netmask, and default gateway addresses
Contact your ISP or IT department for this information.
- DNS addresses
You must specify the IP address for at least one, and up to three, DNS servers. Contact your ISP or IT department for this information. You do not need DNS IP address entries for dynamic Internet accounts or accounts where a DHCP server assigns the IP addresses.
If you have a static IP address with PPPoE, configure the appliance for PPPoE.
See “[PPPoE](#)” on page 20.

Dial-up/ISDN

There are two basic types of dial-up accounts: analog and ISDN. Analog uses a modem that connects to a regular telephone line (RJ-11 connector). ISDN is a digital dial-up account type that uses a special telephone line.

On the Symantec Gateway Security 300 Series appliance, you can use a dial-up account as your primary connection to the Internet, or as a backup to your dedicated account. In backup mode, the appliance automatically dials the ISP if the dedicated connection fails. The appliance re-engages the dedicated account when it is stable; usually 30 to 60 seconds.

You must use an external modem for dial-up accounts. You connect the modem to the appliance through the serial port on the back of the appliance.

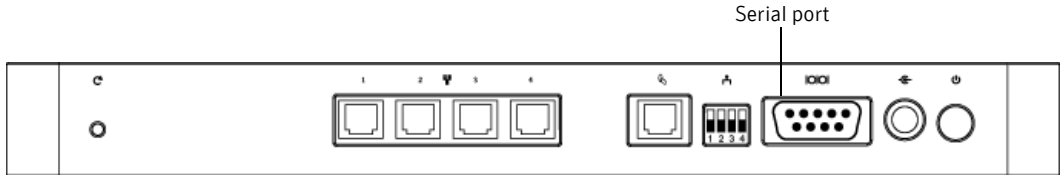
Note: Connect ISDN modems through the serial port on the back of the appliance.

You can configure a primary and a backup dial-up account. You can also connect or disconnect your account manually.

You may configure a backup dial-up account if your primary dedicated account fails. First, you must connect the modem to the appliance. Then, you use the SGMI to configure the dial-up account.

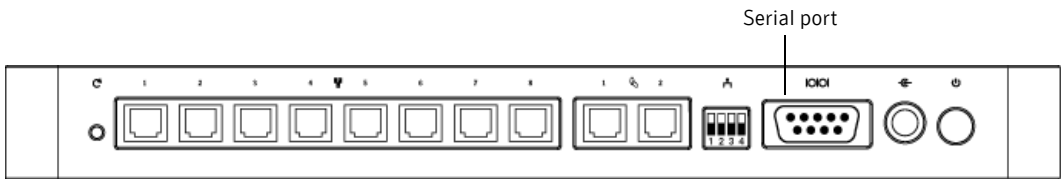
You must use an external modem to use a dial-up account. You connect it to the serial port on the rear panel of the appliance. [Figure 3-1](#) shows the serial port on the rear panel of the model 320 appliance.

Figure 3-1 Rear panel of Symantec Gateway Security model 320 appliance



[Figure 3-2](#) shows the serial port on the rear panel of the model 360 and 360R appliances.

Figure 3-2 Rear panel of Symantec Gateway Security model 360 and 360R appliances



Before configuring the appliance to use your dial-up account as either the primary or backup connection, gather the following information and equipment:

- Account information User name, which may be different from your account name, and associated password.
- Dial-up numbers Requires at least one, and up to three, telephone numbers.
- Static IP address Some ISPs assign static IP addresses to their accounts.
- Modem/cables An external modem and a serial cable to connect the modem to the serial port on the back of the appliance.
- Modem documentation You may need to consult your modem's documentation for modem command or model information.

Running the Setup Wizard

The Setup Wizard is run the first time the administrator browses to the appliance. You can also run it again to reconfigure the appliance by clicking

WAN/ISP in the left pane of the SGMI, and then clicking Main Setup in the right pane.

Using the SGMI, you can change any information you enter in the Setup Wizard, except the language. You can change the language by running the Setup Wizard again, and selecting a different language.

Before you begin

Before proceeding with the Setup Wizard, plug in the cable from your modem which is connected to the Internet or from your intranet into the WAN port (WAN 1 on models 360 and 360R) on the back of your appliance. After you plug in the appropriate cables, check that the Transmit LED is illuminated, restart your computer, and then begin the Setup Wizard.

If the WAN port is active (has an active Internet or intranet connection plugged in to it), the Setup Wizard guides you through configuring LiveUpdate and your administrator password. If the WAN port is not active, the Setup Wizard guides you through entering ISP-specific connection parameters.

LiveUpdate enables customers to keep their Symantec products up-to-date with the latest revision. You should run LiveUpdate as soon as your appliance is connected to the Internet. If new LiveUpdate packages are available, the appliance restarts after the package is downloaded and applied, but your configuration is preserved.

Note: You should configure the LiveUpdate service for automatic updates. This ensures that the appliance always provides the highest level of security available.

Starting the Setup Wizard

Configuring the appliance using the Setup Wizard consists of three parts: starting the Setup Wizard, configuring for your connection type, and then completing the Setup Wizard.

Note: If your connection type is DHCP and the appliance is connected to the WAN, when you start the Setup Wizard the appliance will automatically detect and configure DHCP for you.

To start the Setup Wizard

- 1 Install the appliance according to the instructions in [“Installing the Symantec Gateway Security 300 Series appliance”](#) on page 11.
- 2 Browse to the appliance IP address.
By default, the IP address is 192.168.0.1.
- 3 In the Symantec Gateway Security 300 Series panel, select a language.
When you select a language, it is the language in which the Setup Wizard proceeds, as well as the language which is used on the appliance.
- 4 Click **Next**.
- 5 In the Welcome to Symantec Gateway Security 300 Series Setup Wizard panel, click **Next**.
- 6 Proceed to the instructions for your connection type.
 - [“Setting up Dialup/ISDN”](#) on page 25.
 - [“Configuring a DHCP connection”](#) on page 26.
 - [“Configuring a DSL connection”](#) on page 27.
 - [“Configuring a static IP address connection”](#) on page 27.

Setting up Dialup/ISDN

The following procedures walk you through configuring a primary dial-up connection. For information on setting up a back-up dial-up account for connectivity, see *Symantec Gateway Security 300 Series Administrator’s Guide*.

Before performing these procedures, you must complete the tasks in [“To start the Setup Wizard”](#) on page 25.

To set up a dial-up or ISDN

- 1 Run the Setup Wizard.
See [“Starting the Setup Wizard”](#) on page 24.
- 2 In the Connection Settings panel, click **Dialup/ISDN**.
In the Dialup or ISDN Connection panel, under User account information and dialup numbers, do the following:

UserName	Type the account user name.
Password	Type the account password.
Verify Password	Retype the account password.
Dial-up Telephone 1	Type the dial-up telephone number.

Dial-up Telephone 2 Optionally, type a backup dial-up telephone number.

Dial-up Telephone 3 Optionally, type a backup dial-up telephone number.

- 3 Under ISP-provided static IP address, in the IP address text boxes, type the static IP address, if you have one.
 Under Modem Settings, do the following:

Model Select the model of your modem.

Line Speed Select the speed at which you want to connect.

Dial Type Select the dial type.

Redial String Type a redial string.

Initialization String Type an initialization string.
 If you select a modem type other than Other, the initialization string is provided. If you select Other, you must type an initializationstring.

Line Type Select the type of telephone line.

Dial String Type a dial string.

Idle Time Out Type the amount of time, in minutes, after which the connection is closed if idle.

- 4 Click **Next**.
- 5 Skip to [“To complete the Setup Wizard”](#) on page 28.

Configuring a DHCP connection

Before performing these procedures, you must complete the tasks in [“To start the Setup Wizard”](#) on page 25.

Note: If your connection type is DHCP and the appliance is connected to the WAN, when you start the Setup Wizard the appliance will automatically detect and configure DHCP for you.

To configure a DHCP connection

- 1 Begin the Setup Wizard.
 See [“Starting the Setup Wizard”](#) on page 24.
- 2 In the Connection Settings panel, click **DHCP**.

- 3 In the Broadband Cable Connection panel, in the Computer or gateway MAC address text boxes, type the physical address.
Change this value only if required by your ISP.
- 4 Click **Next**.
- 5 Skip to [“To complete the Setup Wizard”](#) on page 28.

Configuring a DSL connection

Before performing these procedures, you must complete the tasks in [“To start the Setup Wizard”](#) on page 25.

To configure a DSL connection

- 1 Run the Setup Wizard.
See [“Starting the Setup Wizard”](#) on page 24.
- 2 In the Connection Settings panel, click **DSL**.
- 3 In the Broadband ADSL/SDSL Connection Authentication panel, select the user authentication service.
- 4 If you selected PPPoE, in the Broadband ADSL/SDSL Connection with PPPoE panel, do the following:

User Name	Type the account user name.
Password	Type the account password.
Verify Password	Retype the account password.
Connect on Demand	If you want to establish the connection on an as-needed basis, check this check box.
Idle Time Out	Type the time, in minutes, after which the connection closes if idle.
Static IP address	Type the static IP address.

- 5 Click **Next**.
- 6 Skip to [“To complete the Setup Wizard”](#) on page 28.

Configuring a static IP address connection

Before performing these procedures, you must complete the tasks in [“To start the Setup Wizard”](#) on page 25.

To configure a static IP address connection

- 1 Run the Setup Wizard.
See [“Starting the Setup Wizard”](#) on page 24.
- 2 In the Connection Settings panel, click **Static IP**.
- 3 In the Broadband connection using a Static IP panel, do the following:

IP Address	Type the static IP address.
Network Mask	Type the net mask.
Default Gateway	Type the IP address of the default gateway.
DNS 1	Type the IP address of the first Domain Name Service (DNS) servers used to translate addresses.
DNS 2	Optionally, type the IP addresses of an additional DNS server used to translate addresses.
DNS 3	Optionally, type the IP addresses of an additional DNS server used to translate addresses.

- 4 Click **Next**.
- 5 Skip to [“To complete the Setup Wizard”](#) on page 28.

Completing the Setup Wizard

Before performing these procedures, you must complete the tasks in [“To start the Setup Wizard”](#) on page 25 and the procedures that are specific to the type of connection you have.

To complete the Setup Wizard

- 1 In the System Information panel, do the following:

Gateway Host Name	Type the name of the gateway host. You can leave the default value, or change it if required by your ISP or leave it blank.
Registered Internet Domain Name	Optionally, type the domain name.
Administrator Password	Type the administrator account password. The administrator user name is always admin.
Verify Administrator	Retype the administrator account password.

Gateway Host Name	Type the name of the gateway host. You can leave the default value, or change it if required by your ISP or leave it blank.
Enable	If you do not want to permit PING requests, under Block ICMP Requests, click this option button.

2 Click **Next**.

3 In the LiveUpdate Settings panel, do the following:

Run LiveUpdate	To run LiveUpdate after the Setup Wizard is complete, check this check box.
Enable Scheduler	To run Scheduler, check this check box.
LiveUpdate Server	Type the server address.
Frequency	Select the frequency with which LiveUpdate checks for updates.
Preferred Time (UTC)	Type the time of day which you want LiveUpdate to check for updates. The time is based on a 24-hour clock. The format is HH:MM, where HH is hour and MM and minutes. For example, to run the Live Update at 5:30 p. m., type 17:30.

4 Click **Next**.

5 In the Confirmation panel, review the settings.

6 Do one of the following:

- To make changes, click **Back**.
- To save the settings and restart the appliance, click **Apply Settings**. It takes a few minutes for the appliance to apply the settings and restart.

Access the Security Gateway Management Interface (SGMI)

Once you have completed the Setup Wizard, you can configure the other features of the appliance using the SGMI.

You should configure your browser to check for newer versions of stored pages every visit to the page before accessing the SGMI.

To access the SGMI

- ◆ Browse to 192.168.0.1 (the IP address of the appliance).
This is the default IP address of the appliance. Once you have logged in to the SGMI, you can change the IP address.
The administration user name is always admin. The SGMI login is case-sensitive.

For more information about configuring the appliance, see *Symantec Gateway Security 300 Series Administrator's Guide*.

Developing a pre-installation security plan

This chapter includes the following topics:

- [About developing a security plan](#)
- [Defining your security policy](#)
- [Educating users](#)
- [Filling out worksheets](#)

About developing a security plan

This appendix provides basic guidelines for developing an overall security plan. Developing a security plan is your first step in your installation process and helps you collect the information needed to install Symantec Gateway Security 300 Series.

The process of developing a security plan consists of three basic steps:

- Defining your security policy
- Educating your users
- Filling out worksheets

Defining your security policy

Before configuring your security gateway, you must understand exactly what network resources and services you want to protect. It is crucial to have a carefully designed network security policy to guard the valuable resources and information of your organization.

Ideally, you should capture your security policy in a document that describes your organization's network security needs and concerns. Creating this document is the first step in building an effective overall network security system and must be done prior to installation.

Your security plan details your security plan policy implementation. Based on the security concerns and trade-offs of your overall policy, your security plan should contain a set of tasks. One of these tasks consists of establishing procedures and rules for access to resources located on your network. These resources include:

- Host computers and servers
- Workstations
- Connection devices (gateways, routers, bridges, and repeaters)
- Terminal servers and remote access servers
- Networking and applications software
- Information in files and databases

The Symantec Gateway Security 300 Series firewall is the main tool for enforcing security, allowing you to define a security policy that allows or denies access to specific resources throughout your network.

Before writing your security plan

Before you write rules to implement your plan using the *Symantec Gateway Security 300 Series Administrator's Guide*, answer the following questions:

- How many points of entry exist into your network?
 - A security gateway defends a single point of entry. Every point of entry should be protected by a security gateway.
 - A Virtual Private Network (VPN) server also defends a single point of entry. You must decide what access the VPN server is going to provide for resources that exist behind the security gateway.
- What types of services do you want to allow for internal users?
- To what hosts, subnets, and users do you want to allow these services?
- What external users will you allow to access your network? Which hosts or subnets will you allow them to access? During what hours? For what period of time?
- Do you intend to implement a service network, often called a De-militarized zone (DMZ)?
- What types of services do you want to allow for external users?

- What type of authentication will you require for external users? (Symantec recommends strong authentication for any access from public networks.)
- If you are implementing VPN tunnels between any internal and external hosts, what types of traffic will be allowed over these tunnels?
- Will you place your Web server inside or outside of your protected network?

Becoming security-conscious

Developing and implementing a security plan for the security gateway you are implementing should be only one part of your overall security policy. The security gateway offers the best protection against uninvited entry into your network. However, the security gateway cannot guard against entry by people who pirate passwords, any more than a sophisticated lock can stop a thief in possession of the right key.

Formulate goals

Take the time to formulate the specific goals of your security plan. Identify the resources you are protecting and all possible threats. Protecting your resources from unauthorized external users maybe only one of your goals. You may also need to limit internal access to certain systems to specific users and groups, within specific time periods. You will need to define these users and groups for the firewall and how to configure special services to be passed through these systems. *Symantec Gateway Security 300 Series Administrator's Guide* explains how to define users and user groups.

Review issues

Review your organization's specific issues in detail before you configure the server. Your network's security depends on planning sound policies, implementing them carefully, and verifying that they work as intended.

Educating users

Your overall site policy involves a numbers of tasks. Of these, user education is paramount. Publish your company's security policy. Make sure your users are informed of the determination of would-be invaders and the sophistication of available password guessing programs. Make sure they understand how common security breaches are and how costly they can be. These facts alone dictate that users should be encouraged to select passwords that are difficult to crack and to change passwords regularly.

Involving the user community

When developing the details of your security plan, you should solicit the input of group managers or leaders on what services they require, for what users, and so on. Explain to users the need for network security to protect private information, intellectual property, and your business plans.

Notifying affected users

Before implementing policies, notify the user community of your proposed policies. Doing so in advance can prevent unnecessary frustration on the part of your users.

For instance, if you plan to pass all email through a dedicated server, or if external users will be disallowed from accessing certain systems by Telnet, consider passing these changes along before implementation. Consulting users prior to implementation may save you the time needed to fine-tune those policies later.

Taking a pro-active stance

Again, keep in mind that configuring a set of authorization rules on the security gateway is just one piece of your overall security plan. To be effective, this plan should also include:

- Physical security of key systems (especially the security gateway)
- Security risk training for users
- Guidelines on passwords
- Proprietary information policies
- Network planning

Filling out worksheets

Use the following set of policy planning worksheets to aid in the planning process. Use these worksheets to help implement the specific tasks of your security plan and to assist you during the installation process.

Defining your organization

Begin by defining your organization. Here is where you explore your existing security policy, if any; notate who will be assigned as administrators; types of authentication; and how your administrators will be contacted.

7 Use [Table A-1](#) to list all persons involved in administering the system.

Table A-1 Administrator names

Name	Email	Phone	Pager

8 Are organization computer resources accessible by remote dial-in?

_____ Yes _____ No

9 Are organization computer resources accessible by network?

_____ Yes _____ No

10 What communications servers are used?

11 Do you plan to manage the security gateway remotely?

_____ Yes _____ No

12 Do you have other Symantec security gateways on your network now?

_____ Yes _____ No

13 If Yes, what product and version? _____

14 Do you have other third-party firewalls on your network now?

_____ Yes _____ No

15 If Yes, what brand and version? _____

16 Have you created network diagram?

_____ Yes

_____ No

Site hardware information

Before you begin the installation process, collect some basic hardware information such as product serial numbers, type and quantity of interface cards, server memory, and number and type of computers that compose your network.

To collect hardware information for your site

1 Type the Symantec System ID of the appliance:

2 Select type and quantity of network interface cards.

_____ Ethernet qty: _____

_____ GigE qty: _____

_____ FastEthernet qty: _____

_____ Appliance Ethernet qty: _____

_____ ATM qty: _____

_____ Other: (type) _____ qty: _____

Before installation, ensure the host network connections are configured and tested properly. Verify that you can PING the network interfaces of the server from clients on the same network.

3 Type the number of host computers of each type that compose your network.

_____ UNIX

_____ Windows

_____ Other: (type) _____

4 List the number of operating system types in your network.

5 What kind of Internet connection do you have? What speed?

- 6 Type the name of your Internet Service Provider (ISP):

- 7 Does your site have, or plan to have, more than one Internet access point?
_____ Yes _____ No
- 8 Are there any other Internet connections besides the firewall (such as modems connected to workstations)?
_____ Yes _____ No
- 9 Will you be using Symantec Client VPN?
_____ Yes _____ No

TCP/IP address

It is important to think about the TCP/IP requirements for your site. This includes information about running Domain Name Services (DNS), types and names of domains on your network, and making a list of protocols used at your site.

To collect TCP/IP address information

- 1 Do you currently run Domain Name Services (DNS) on your network?
_____ Yes _____ No
- 2 What type of DNS is in use at your site?
_____ Single domain _____ Multiple domains
_____ Subdomains
- 3 What type of name service do you provide?
_____ Primary name services _____ Secondary name services
- 4 List the DNS supported by this site:

5 Do you have an internal name server?

_____ Yes _____ No

6 Do you have someone at your site who is knowledgeable about, and comfortable working with, DNS and how to configure it properly?

_____ Yes _____ No

7 Check the address types being used at your site:

_____ Registered IP address _____ Private IP address (RFC 1918)
_____ Unregistered IP address

Your connection to the Internet must have at least one public network address. Symantec is not responsible for acquiring or registering public IP addresses. The internal (behind the firewall) addresses do not have to be legal or registered. Symantec strongly recommends that you use private, RFC 1918-compliant addresses internally.

8 List the address ranges you currently use in your network.

9 List the protocols you use in your network.

10 Will you be using network news services (NNTP protocol)?

_____ Yes _____ No

11 If yes, and you have your own internal NNTP server, type its IP address and the address of the server that will be supplying you with news feeds.

_____ Internal server: _____

_____ External news server: _____

Allowed TCP/IP services

Use the following tables to define all the allowed TCP/IP services in your network.

To define allowed TCP/IP services

- 1 Use [Table A-2](#) and check the access type (if any) you will allow for the following services:

Table A-2 Allowed TCP/IP access type

Access group	DNS	FTP	HTTP	HTTPS	SMTP	POP3	RADIUS Auth	Telnet	IPsec	PPTP	LiveUpdate	SESA
All users (Everyone)												
Computer Group 1												
Computer Group 2												
Computer Group 3												
Computer Group 4												
No access												

- 2 Use [Table A-3](#) to list the names of any special services you wish to pass through the firewall.

Table A-3 Special services names

Service name	Service port number	Service type (UDP/TCP)	Server name

Table A-3 Special services names

Service name	Service port number	Service type (UDP/TCP)	Server name

3 Use [Table A-4](#) to list your TCP/IP services.

Table A-4 TCP/IP services

	Group	Authentication
FTP		
Telnet		
HTTP		
Other		

Over time, you will likely refine these permissions. You should make periodic updates to this list.

- 4 Do you need transparent inbound access from the outside Internet's gateway?

Yes _____

No _____

Web service information

Use the following section to define information about your Web services.

To define your Web services

- 1 Will you be using a Web server?

_____ Yes

_____ No

- 2 If yes, select the location of the Web server:

_____ Internal to the Symantec Gateway Security 300 Series

_____ External to the Symantec Gateway Security 300 Series

- 3 Notate the Web server name and IP address:

Name: _____ Address: _____

- 4 Will you be using an external caching/proxy server? If yes, notate the server name and IP address.

_____ Yes

_____ No

Proxy server name: _____ Address: _____

Access lists

List those entities and users to which you plan to write rules to allow access through the Symantec Gateway Security 300 Series security gateway.

Table A-8 Denied Web sites (Continued)

Web site name	URL	comments

Defining your network architecture

In the following section, list all of the entities that comprise your network. Show all routers and computers systems that will be directly affected by, or connected to, the firewall and its directly connected networks. Label each network component with its IP address and network mask.

Use [Table A-9](#) to create a list of all internal servers. Your external network consists of at least the Symantec Gateway Security 300 Series host and a router.

Table A-9 Internal network servers

	DNS name services	Mail server	Web server	Other server
Service				
Host name				
IP address				
Subnet mask				

Use [Table A-10](#) to list your host system addresses.

Table A-10 Host internal and external IP addresses

Host	Internal/external IP addresses

Use [Table A-11](#) to list your router IP addresses.

Table A-11 Router IP addresses

Router	IP addresses

Your external network can also include external servers, such as an external Web server. Use [Table A-12](#) to list all external network servers.

Table A-12 External network servers

	DNS name services	Mail server	Web server	Other server
Service				
Host name				
IP address				
Subnet mask				

Licensing

This chapter includes the following topics:

- [Session licensing for Symantec Gateway Security 300 Series Client-to-Gateway VPN functions](#)
- [SYMANTEC GATEWAY SECURITY APPLIANCE LICENSE AND WARRANTY AGREEMENT](#)

Session licensing for Symantec Gateway Security 300 Series Client-to-Gateway VPN functions

Symantec Client VPN software may be licensed for an appliance. The Symantec Client VPN software version must be listed as supported in the *Symantec Gateway Security 300 Series Release Notes*. The Client-to-Gateway VPN add-on is licensed by the maximum number of concurrent VPN sessions allowed. The appliance comes with a license for one Client-to-Gateway VPN session. You can purchase additional licenses for concurrent VPN sessions. For example, you may have 15 users who need VPN access as part of their normal work habits, but at any time, only 10 users are ever connected by way of the VPN.

In this situation, you only need a license for 10 concurrent VPN sessions. You must obtain additional licenses as necessary to allow the maximum number of concurrent sessions you require. You are licensed to load the client software on as many nodes as you like, but these clients are licensed for use only with the accompanying Symantec Gateway Security appliance.

Additive session licenses

Additive session licenses are available for Client-to-Gateway VPN functions. Client-to-Gateway VPN session licenses are independent of base function licenses and the maximum number of concurrent sessions may be limited by hardware performance, your network implementation or traffic characteristics.

SYMANTEC GATEWAY SECURITY APPLIANCE LICENSE AND WARRANTY AGREEMENT

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE INCLUDED WITH THE APPLIANCE YOU HAVE PURCHASED TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") AND TO PROVIDE WARRANTIES ON THE APPLIANCE ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AND WARRANTY AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AND WARRANTY AGREEMENT CAREFULLY BEFORE USING THE APPLIANCE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, REQUESTING A LICENSE KEY OR USING THE SOFTWARE AND THE APPLIANCE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE" OR "NO" BUTTON IF APPLICABLE AND DO NOT USE THE SOFTWARE AND THE APPLIANCE.

1. Software License:

The software (the "Software") which accompanies the appliance You have purchased (the "Appliance") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") which accompanies, precedes, or follows this license, and as may be further defined in the user documentation accompanying the Appliance and/or the Software, Your rights and obligations with respect to the use of this Software are as follows:

You may:

- A. _____ use the Software solely as part of the Appliance.
- B. _____ make copies of the printed documentation which accompanies the Appliance as necessary to support Your authorized use of the Appliance; and
- C. _____ after written notice to Symantec and in connection with a transfer of the Appliance, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software, Symantec consents to the transfer and the transferee agrees in writing to the terms and conditions of this agreement.

You may not:

- A. _____ sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;
- B. _____ use, if You received the Software distributed on an Appliance containing multiple Symantec products, any Symantec software on the Appliance for which You have not received a permission in a License Module; or
- C. _____ use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Symantec software products utilize content that is updated from time to time (e.g., antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; some firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.); collectively, these are referred to as "Content Updates"). You may obtain Content Updates for each Software functionality which You have purchased and activated for use with the Appliance for any period for which You have (i) purchased a subscription for Content Updates for such Software functionality; (ii) entered into a support agreement that includes Content Updates for such Software functionality; or (iii) otherwise separately acquired the right to obtain Content Updates for such Software functionality. This license does not otherwise permit You to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the Software will perform on the Appliance in substantial compliance with the written documentation accompanying the Appliance for a period of thirty (30) days from the date of original purchase of the Appliance. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, repair or replace any defective Software returned to Symantec within the warranty period or refund the money You paid for the Appliance.

Symantec warrants that the hardware component of the Appliance (the "Hardware") shall be free from defects in material and workmanship under normal use and service and substantially conform to the written documentation accompanying the Appliance for a period of three hundred sixty-five (365) days from the date of original purchase of the Appliance. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, repair or replace any defective Hardware returned to Symantec within the warranty period or refund the money You paid for the Appliance.

The warranties contained in this agreement will not apply to any Software or Hardware which:

- A. _____ has been altered, supplemented, upgraded or modified in any way; or
- B. _____ has been repaired except by Symantec or its designee.

Additionally, the warranties contained in this agreement do not apply to repair or replacement caused or necessitated by: (i) events occurring after risk of loss passes to You such as loss or damage during shipment; (ii) acts of God including without limitation natural acts such as fire, flood, wind earthquake, lightning or similar disaster; (iii) improper use, environment, installation or electrical supply, improper maintenance, or any other misuse, abuse or mishandling; (iv) governmental actions or inactions; (v) strikes or work stoppages; (vi) Your failure to follow applicable use or operations instructions or manuals; (vii) Your failure to implement, or to allow Symantec or its designee to implement, any corrections or modifications to the Appliance made available to You by Symantec; or (viii) such other events outside Symantec's reasonable control.

Upon discovery of any failure of the Hardware, or component thereof, to conform to the applicable warranty during the applicable warranty period, You are required to contact us within ten (10) days after such failure and seek a return material authorization ("RMA") number. Symantec will promptly issue the requested RMA as long as we determine that You meet the conditions for warranty service. The allegedly defective Appliance, or component thereof, shall be returned to Symantec, securely and properly packaged, freight and insurance prepaid, with the RMA number prominently displayed on the exterior of the shipment packaging and with the Appliance. Symantec will have no obligation to accept any Appliance which is returned without an RMA number.

Upon completion of repair or if Symantec decides, in accordance with the warranty, to replace a defective Appliance, Symantec will return such repaired or replacement Appliance to You, freight and insurance prepaid. In the event that Symantec, in its sole discretion, determines that it is unable to replace or repair the Hardware, Symantec will refund to You the F.O.B. price paid by You for the defective Appliance. Defective Appliances returned to Symantec will become the property of Symantec.

Syantec does not warrant that the Appliance will meet Your requirements or that operation of the Appliance will be uninterrupted or that the Appliance will be error-free.

In order to exercise any of the warranty rights contained in this Agreement, You must have available an original sales receipt or bill of sale demonstrating proof of purchase with Your warranty claim.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE APPLIANCE. The disclaimers and limitations set forth above will apply regardless of whether You accept the Software or the Appliance.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

6. Export Regulation:

Certain Symantec products are subject to export controls by the U.S. Department of Commerce (DOC), under the Export Administration Regulations (EAR) (see www.bxa.doc.gov). Violation of U.S. law is strictly prohibited. Licensee agrees to comply with the requirements of the EAR and all applicable international, national, state, regional and local laws, and regulations, including any applicable import and use restrictions. Symantec products are currently prohibited for export or re-export to Cuba, North Korea, Iran, Iraq, Libya, Syria and Sudan or to any country subject to applicable trade sanctions. Licensee agrees not to export, or re-export, directly or indirectly, any product to any country outlined in the EAR, nor to any person or entity on the DOC Denied Persons, Entities and Unverified Lists, the U.S. Department of State's Debarred List, or on the U.S. Department of Treasury's lists of Specially Designated Nationals, Specially Designated Narcotics Traffickers, or Specially Designated Terrorists. Furthermore, Licensee agrees not to export, or re-export, Symantec products to any military entity not approved under the EAR, or to any other entity for any military purpose, nor will it sell any Symantec product for use in connection with chemical, biological, or nuclear weapons or missiles capable of delivering such weapons.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Appliance and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement may only be modified by a License Module or by a written document which has been signed by both You and Symantec. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software and shall return the Appliance to Symantec. The disclaimers of warranties and damages and limitations on liability shall survive termination. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, USA, or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

Specifications and safety

This chapter includes the following topics:

- [Product specifications](#)
- [Safeguard instructions](#)
- [Product certifications](#)

This appendix lists the product specifications and safety certifications.

Product specifications

Each respective Symantec Gateway Security 300 Series model offers increased performance and these different specifications are listed in [Table C-1](#).

Table C-1 Product specifications

Parameter	Model 320	Model 360 and 360R
Length	33.0 cm (12.99 inches)	33.0 cm (12.99 inches)
Width	25.6 cm (10.07 inches)	25.6 cm (10.07 inches)
Height	7.0 cm (2.75 inches)	7.0 cm (2.75 inches)
Weight	1.228 kg (2.707 lb)	1.259 kg (2.776 lb)
Network interfaces	5 10/100 Ethernet ports (1 WAN and 4 LAN) 1 RS-232 serial port	10 10/100 Ethernet ports (2 WAN and 8 LAN) 1 RS-232 serial port
User interface	Security Gateway Management Interface (SGMI)	Security Gateway Management Interface (SGMI)
Processor	140 MHz	170 MHz
RAM	64MB	64MB

Table C-1 Product specifications (Continued)

Parameter	Model 320	Model 360 and 360R
Operating temperature range	32 to 104° F (0 to 40° C)	32 to 104° F (0 to 40° C)
Non-operating temperature range	-4 to 149° F (-20 to 65° C)	-4 to 149° F (-20 to 65° C)
Operating humidity	10-90% humidity, non-condensing at altitudes of 0 to 6500 feet (2000 m)	10-90% humidity, non-condensing at altitudes of 0 to 6500 feet (2000 m)
Non-operating humidity	10-90% humidity, non-condensing at altitudes of 0 to 15000 feet (4750 m)	10-90% humidity, non-condensing at altitudes of 0 to 15000 feet (4750 m)
AC power	<p>North American power supply unit</p> <ul style="list-style-type: none"> ■ Line voltage range: 100 V to 120 V AC ■ Current: 1.1 Amps (at 115 V) ■ Frequency: 59 - 61 Hz, single phase ■ Power: 10 W <p>The multi-national power supply unit includes four removable wall-plug clips to support the following geographies: USA, Europe, UK and Australia.</p> <ul style="list-style-type: none"> ■ Line voltage range: 207 V to 253V AC ■ Current: 55 Amps (at 230 V) ■ Frequency: 49.5 - 50.5 Hz, single phase ■ Power: 10 W 	<p>North American power supply unit</p> <ul style="list-style-type: none"> ■ Line voltage range: 100 V to 120 V AC ■ Current: 1.1 Amps (at 115 V) ■ Frequency: 59 - 61 Hz, single phase ■ Power: 10 W <p>The multi-national power supply unit includes four removable wall-plug clips to support the following geographies: USA, Europe, UK and Australia.</p> <ul style="list-style-type: none"> ■ Line voltage range: 207 V to 253V AC ■ Current: 55 Amps (at 230 V) ■ Frequency: 49.5 - 50.5 Hz, single phase ■ Power: 10 W
Operating shock and vibration	<ul style="list-style-type: none"> ■ Shock: 250 G, < 2 ms ■ Vibration: 0.41 Grms² (3-500 Hz) random input 	<ul style="list-style-type: none"> ■ Shock: 250 G, < 2 ms ■ Vibration: 0.41 Grms² (3-500 Hz) random input
Non-operating shock and vibration	<ul style="list-style-type: none"> ■ Shock: 65 G, 8 ms ■ Vibration: 1.12 Grms² (3-500 Hz) random input 	<ul style="list-style-type: none"> ■ Shock: 65 G, 8 ms ■ Vibration: 1.12 Grms² (3-500 Hz) random input

Safeguard instructions

For your protection, please read all these instructions regarding your appliance.

- **Read instructions**
Read and understand all the safety and operating instructions before operating the appliance.
- **Ventilation**
Vents on the front and rear and the fan opening on the back panel of the Symantec Gateway Security 5400 Series provide ventilation for reliable product operation and to protect it from overheating. These openings must not be blocked or covered. This product should not be placed in an enclosure unless proper ventilation is provided.
- **Power cord**

Caution: The power-supply cord is used as the main disconnect device. Ensure that the socket outlet is located or installed near the equipment and is easily accessible.

Warning: To reduce the risk of electrical shock, do not disassemble this product. Return it to Symantec when service or repair work is required. Opening or removing covers may expose you to dangerous voltage or other risks. Incorrect reassembly can cause electric shock when this product is subsequently used.

Note: Breaking the seal on the left side and bottom of the appliance or opening the appliance in any way voids your warranty.

Warning: To prevent a possible electrical shock when installing the device, ensure that the power cord for the device is unplugged before installing network cables.

Warning: To prevent a possible electrical shock, when adding the device to a system, disconnect all power cords, if possible, from the existing system before connecting the signal cable to that device.

Warning: To prevent a possible electrical shock during an electrical storm, do not connect or disconnect cables.

Warning: To prevent a possible electrical shock from touching two surfaces with different electrical grounds, use one hand, when possible, to connect or disconnect signal cables.

Warning: To avoid a shock hazard, the power cord must be connected to a properly wired and earthed receptacle.

Warning: To avoid a shock hazard, any equipment to which this product will be attached must also be connected to properly wired receptacles.

Warning: Electrical current from power, telephone, and network cables is hazardous.

- Operating the unit in an equipment rack
If you plan to install the Symantec Gateway Security 300 Series in an equipment rack, use these precautions:
 - Ensure the ambient temperature around the appliance (which may be higher than the room temperature) are within the specified limits.
 - Ensure there is sufficient air flow around the unit.
 - Ensure electrical circuits are not overloaded; consider the nameplate ratings of all the connected equipment and ensure you have overcurrent protection.
 - Ensure the equipment is properly grounded, particularly any equipment connected to a power strip.
 - Do not place any objects on top of the appliance.
 - Remove the protective plastic sheet from the top of the appliance.

Product certifications

These appliances have been certified for the following electrical and safety standards:

EMC:

- FCC Part 15 Class B
- ICES-003 (Canada)
- EN 301.489-1 & -17
- EN55022 (1998), Class B Emissions (Radiated & Conducted)
- EN61000-3-2 (2000), Harmonics
- EN61000-3-3 (1995), Flicker
- EN61000-4-2 (1995), ESD: ± 8 kV AD, ± 4 kV CD
- EN61000-4-3 (2002), RF Immunity: 10 V/m, 80 MHz - 1 GHz
- EN61000-4-4 (1995), EFT/Burst: ± 1 kV Power, $\pm .5$ kV Signal Cables
- EN61000-4-5 (1995), Surge: ± 1 kV (L-L), ± 2 kV (L-G)
- EN61000-4-6 (1996), Conducted RF Immunity: 3V, 150 kHz – 80 MHz
- EN61000-4-11 (1994): $>95\%/0.5T$, $30\%/25T$, $>95\%/250T$

Safety:

- UL 1950
- CSA 22.2 No. 950-95
- EN60950-1 (2002)

LEDs and DIP switches

This chapter includes the following topics:

- [About LEDs](#)
- [DIP switches](#)

About LEDs

The front panel on Symantec Gateway Security 300 Series models 320, 360, and 360R have LED lights that indicate the status of the appliance. Each LED indicates status of a different part of the appliance, such as the LAN and WAN ports. You can also determine the status of the appliance by the combination of the LEDs.

[Figure D-1](#) shows the LEDs on the front panel of models 320, 360, and 360R.

Figure D-1 LED configuration on models 320, 360, and 360R

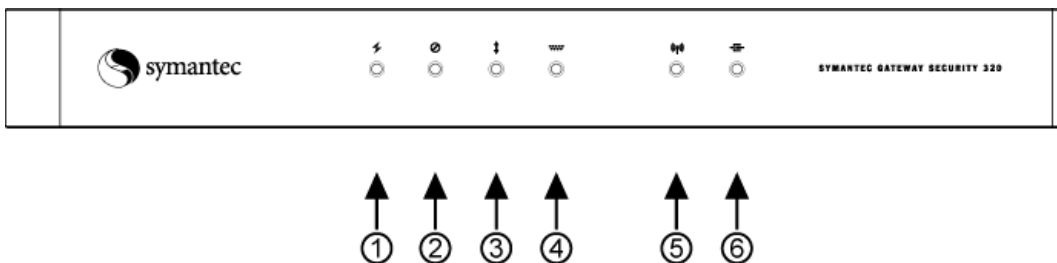








Table D-1 describes each LED.

Table D-1 LEDs

Location	Symbol	Feature	Description
1		Power	Illuminates when the appliance is turned on.
2		Error	Illuminates if there is a problem with the appliance.
3		Transmit	Illuminates or flashes when traffic is being passed over the LAN or WAN ports.
4		Backup	Illuminates or flashes when the serial port is being used or is not functioning correctly.
5		Wireless-ready	Illuminates when the wireless card is inserted and functioning properly.
6		Wireless-active	Illuminates or flashes when the wireless card is transmitting or receiving data.

Interpreting the LEDs

The LEDs on the front panel of the appliance have three states: solid on, flashing, and solid off. The combination of the Error and Transmit LED states indicate the status of the appliance. Table D-2 describes the LEDs state combinations and appliance status that they indicate.

Table D-2 LEDs states and appliance status

Error LED state	Transmit LED state	Appliance status
Solid off	Solid on	Normal operation.
Solid off	Flashing	Transmitting/receiving Data from LAN.

Table D-2 LEDs states and appliance status (Continued)

Error LED state	Transmit LED state	Appliance status
Flashing	Flashing	<ul style="list-style-type: none"> ■ MAC address not assigned. ■ Firmware problem. Appliance is ready for a forced download. ■ Appliance detected an error and cannot recover.
Flashing	Solid on	Configuration mode.
Solid on	Solid on	Hardware problem.
Flashing once	Solid off	RAM error.
Flashing twice	Solid off	Timer error.
Flash three	Solid off	DMA error.
Solid on	Flashing once	LAN error.
Solid on	Flashing twice	WAN error.
Solid on	Flashing three	Serial error.
Solid off	Solid off	No power.
Both flashing alternatively.		<ul style="list-style-type: none"> ■ Download in progress. ■ Appliance is writing to flash.

LiveUpdate LED status

Automatic firmware updates using LiveUpdate have a special set of LED sequences. [Table D-3](#) describes the LED activity before, during, and after a LiveUpdate firmware update.

Table D-3 LED states for LiveUpdate status

LiveUpdate status	Power LED state	Error LED state	Transmit LED state
During retrieval of LiveUpdate firmware from Internet (or TFTP) there is no effect on appliance operation. LEDs are in normal operational pattern.	On	On	On (flashing for traffic)
Firmware downloaded and CRC verified. Flash erase begins (about 10 seconds).	On	Off	Off

Table D-3 LED states for LiveUpdate status

LiveUpdate status	Power LED state	Error LED state	Transmit LED state
Writing new image to flash (seconds depend on firmware size).	On	Flashing alternately	Flashing alternately
Write Complete – Briefly for 1 second before reset.	On	On	On
Unit Resets – All LEDs flashed ON and end in Normal Operational pattern.	On	Off	On (flashing for traffic)

DIP switches

DIP switches allow for manual intervention on the appliance to perform tasks like upgrading the firmware, backing up your configuration, and using the serial port for maintenance operations. See *Symantec Gateway Security 300 Series Administrator's Guide* for more information.

For normal operation, set all the DIP switches to off (down).

About troubleshooting

This chapter includes the following topics:

- **Accessing troubleshooting information**

You can find up-to-date troubleshooting information for Symantec Gateway Security 300 Series (and all Symantec products) on the Symantec Web site, www.symantec.com.

Accessing troubleshooting information

Use the following procedure to access troubleshooting information from the Symantec Knowledge Base.

To access Symantec Gateway Security 300 Series troubleshooting information

- 1 Go to www.symantec.com.
- 2 On the top of the home page, click **support**.
- 3 Under Product Support > enterprise, click **Continue**.
- 4 On the Support enterprise page, under Technical Support, click **knowledge base**.
- 5 Under select a knowledge base, scroll down and click **Symantec Gateway Security 300 Series**.
- 6 Click your specific product name and model.
- 7 On the knowledge base page for your appliance model, do any of the following:
 - On the Hot Topics tab, click any of the items in the list to view a detailed list of knowledge base articles on that topic.

- On the Search tab, in the text box, type a string containing your question. Use the drop-down list to determine how the search is performed and click **Search**.
- On the Browse tab, expand a heading to see knowledge base articles related to that topic.

Index

A

- access lists, checklists 40
- administrator password 28
- aDSL 20
- analog 17
- Analog connections 18
- analog, dial-up accounts 22
- appliance
 - back panel 13
 - installation 11
- Asymmetrical Digital Subscriber Line (ASDL) 20

B

- backup dial-up account 22
- broadband
 - accounts 17
 - cable modem 18, 19
- broadband cable connection 19
- broadband connection 18
- buttons
 - power 13
 - restart 13

C

- cable connection 19
- CD-ROMs, replacement 10
- certification 57
- component list 9
- configuring
 - DSL connection 27
 - static IP address connection 27
- connection types 17

D

- defining your organization 34
- DHCP 18, 19
- dial-up accounts 22
- dial-up back-up account 22
- dial-up connection 13, 17

- DIP switches 13, 62
- disconnect idle PPPoE connections 20
- documentation
 - supplied 9
- DSL 17, 18, 20
- DSL connectivity 19
- DSL, configuring 27

E

- electric shock 55

I

- installing, appliance 11
- IP addresses checklist 39
- ISDN connection 17, 18
- ISDN, dial-up accounts 22
- ISP, PPTP connections 21

L

- LAN ports 13
- LEDs
 - flashing 60
 - LiveUpdate 61
- licensing 47
- LiveUpdate 24, 61

M

- manually updating the appliance 13
- modem port 13

N

- network architecture, checklist 44
- network connections (outside or internal) 17
- NICs, checklist 37

P

- password 28
- Point-to-Point Protocol over Ethernet. *See* PPPoE

ports

- LAN 13
- serial 13
- WAN 13

- power button 13
- power cord 13, 15
- power socket 13
- PPPoE

- connectivity 18
- defined 20

PPTP (Point-to-Point Tunneling Protocol) 21

PPTP connection 19

- product certifications 57
- product component list 9
- product specifications 53
- proxies checklist 40

R**rear panel**

- 320 appliance 23
- 360 and 360R appliance 23

regular telephone connection (RJ-11 connector) 22

replacing, CD-ROMs 10

- restart button 13
- RJ-45 cable 17

S**safety 55**

- electric shock 55
- equipment rack 56

secure data transfer 21

security plan checklist 31

serial port 13

Setup Wizard 17, 24

site hardware information, checklist 37

special phone line ISDN 17

specifications 53

specifications and safety 53

static IP 19

static IP address, configuring 27

T

T1 19

T3 17

TCP/IP checklist 38

TCP/IP-based network 21

U

user documentation 9

W

WAN ports 13

- RJ-45 cables 17
- Setup Wizard 17

WAN/ISP multiple IP addresses 20

Web service, checklist 42

worksheets 34

- access lists 42
- allowed TCP/IP services 40
- collect TCP/IP address information 38
- network architecture 45
- notifications 42
- Web service information 42

X

xDSL 20