INTERNET SECURITY SYSTEMS®

INTERNET|SECURITY|SYSTEMS®
proventia®
intrusion prevention appliance

G100/G200/G1000 G1200 Quick Start Guide

Internet Security Systems, Inc.
6303 Barfield Road
Atlanta, Georgia 30328-4233
United States
(404) 236-2600
http://www.iss.net

© Internet Security Systems, Inc. 2003-2005. All rights reserved worldwide. Customers may make reasonable numbers of copies of this publication for internal use only. This publication may not otherwise be copied or reproduced, in whole or in part, by any other person or entity without the express prior written consent of Internet Security Systems, Inc.

Patent pending.

© Intel Corporation, 2002.

Internet Security Systems, System Scanner, Wireless Scanner, SiteProtector, Proventia, ADDME, AlertCon, ActiveAlert, FireCell, FlexCheck, Secure Steps, SecurePartner, SecureU, and X-Press Update are trademarks and service marks, and the Internet Security Systems logo, X-Force, SAFEsuite, Internet Scanner, Database Scanner, Online Scanner, and RealSecure registered trademarks, of Internet Security Systems, Inc. Network ICE, the Network ICE logo, and ICEpac are trademarks, BlackICE a licensed trademark, and ICEcap a registered trademark, of Network ICE Corporation, a wholly owned subsidiary of Internet Security Systems, Inc. SilentRunner is a registered trademark of Raytheon Company. Acrobat and Adobe are registered trademarks of Adobe Systems Incorporated. Certicom is a trademark and Security Builder is a registered trademark of Certicom Corp. Check Point, FireWall-1, OPSEC, Provider-1, and VPN-1 are registered trademarks of Check Point Software Technologies Ltd. or its affiliates. Cisco and Cisco IOS are registered trademarks of Cisco Systems, Inc. HP-UX and OpenView are registered trademarks of Hewlett-Packard Company. IBM and AIX are registered trademarks of IBM Corporation. InstallShield is a registered trademark and service mark of InstallShield Software Corporation in the United States and/or other countries. Intel and Pentium are registered trademarks of Intel. Lucent is a trademark of Lucent Technologies, Inc. ActiveX, Microsoft, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation. Net8, Oracle, Oracle8, SQL*Loader, and SQL*Plus are trademarks or registered trademarks of Oracle Corporation. Seagate Crystal Reports, Seagate Info, Seagate, Seagate Software, and the Seagate logo are trademarks or registered trademarks of Seagate Software Holdings, Inc. and/or Seagate Technology, Inc. Secure Shell and SSH are trademarks or registered trademarks of SSH Communications Security. iplanet, Sun, Sun Microsystems, the Sun Logo, Netra, SHIELD, Solaris, SPARC, and UltraSPARC are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the United States and other countries. Adaptive Server, SQL, SQL Server, and Sybase are trademarks of Sybase, Inc., its affiliates and licensers. Tivoli is a registered trademark of Tivoli Systems Inc. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd. All other trademarks are the property of their respective owners and are used here in an editorial context without intent of infringement. Specifications are subject to change without notice.

Disclaimer: The information contained in this document may change without notice, and may have been altered or changed if you have received it from a source other than ISS or the X-Force. Use of this information constitutes acceptance for use in an "AS IS" condition, without warranties of any kind, and any use of this information is at the user's own risk. ISS and the X-Force disclaim all warranties, either expressed or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall ISS or the X-Force be liable for any damages whatsoever, including direct, indirect, incidental, consequential or special damages, arising from the use or dissemination hereof, even if ISS or the X-Force has been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages, so the foregoing limitation may not apply.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Internet Security Systems, Inc. The views and opinions of authors expressed herein do not necessarily state or reflect those of Internet Security Systems, Inc., and shall not be used for advertising or product endorsement purposes.

Links and addresses to Internet resources are inspected thoroughly prior to release, but the ever-changing nature of the Internet prevents Internet Security Systems from guaranteeing the content or existence of the resource. When possible, the reference contains alternate sites or keywords that could be used to acquire the information by other methods. If you find a broken or inappropriate link, please send an email with the topic name, link, and its behavior to support@iss.net.

March 3, 2005

DOC-QSG-PROVIPAG-005-A

Contents

Preface

Overview

Introduction

This guide describes the procedures for connecting, starting, and configuring the Proventia G100/G200/G1000 or G1200 Intrusion Prevention Appliances. These appliances are inline intrusion prevention systems (IPS) that automatically block malicious attacks while preserving network bandwidth and availability.

Audience

This guide is intended for users of Proventia G100/G200/G1000 or G1200 model Intrusion Prevention Appliances.

In this guide

The *Proventia G100/G200/G1000/G1200 Quick Start Guide* includes information about the following topics:

- installing the appliance hardware
- configuring the appliance software
- reinstalling the appliance software

About the Proventia G Intrusion Prevention Appliances

Introduction

Proventia G Intrusion Prevention appliances offer the following intrusion prevention technologies:

- three modes of operation
- firewall rules
- dynamic blocking response
- drop response
- agent settings for processing traffic

Proventia G Intrusion Prevention appliances

Use the Proventia G Intrusion Prevention appliances to do the following:

- configure packet captures
- configure firewall rules
- configure operation modes
- configure appliance settings
- review event details for dynamic blocking and drop responses

Note: The Proventia G Appliance Setup Utility is your local configuration interface. Use this tool to configure your appliance configuration settings. Use the SiteProtector management console to manage the Proventia G100, G200, G1000, and G1200 appliances.

How to Use Proventia G Appliances Documentation

Using this guide

Use this guide to install and configure Proventia G Intrusion Prevention Appliances.

Related publications

For the latest available appliance documentation, refer to the online Help found in the SiteProtector management console and the Readme files associated with each appliance release.

For information about how to use the appliance, see the following:

- *Proventia G Series Appliances User Guide*

  This document is available on the ISS Web site at the following location:

  http://www.iss.net/support/documentation/

Conventions Used in this Guide

Introduction

This topic explains the typographic conventions used in this guide to make information in procedures and commands easier to recognize.

In procedures

The typographic conventions used in procedures are shown in the following table:

Convention	What it Indicates	Examples
Bold	An element on the graphical user interface.	Type the computer's address in the **IP Address** box. Select the **Print** check box. Click **OK**.
SMALL CAPS	A key on the keyboard.	Press ENTER. Press the PLUS SIGN (+).
`Constant width`	A file name, folder name, path name, or other information that you must type exactly as shown.	Save the `User.txt` file in the `Addresses` folder. Type `IUSR_SMA` in the **Username** box.
`Constant width italic`	A file name, folder name, path name, or other information that you must supply.	Type `Version` *`number`* in the **Identification information** box.
→	A sequence of commands from the taskbar or menu bar.	From the taskbar, select **Start→Run**. On the **File** menu, select **Utilities→Compare Documents.**

Table 1: *Typographic conventions for procedures*

Command conventions

The typographic conventions used for command lines are shown in the following table:

Convention	What it Indicates	Examples
Constant width bold	Information to type in exactly as shown.	**md ISS**
Italic	Information that varies according to your circumstances.	**md** *your_folder_name*
[ ]	Optional information.	**dir** [*drive:*][*path*] [*filename*] [**/P**][**/W**] [**/D**]
|	Two mutually exclusive choices.	**verify** [**ON**|**OFF**]
{ }	A set of choices from which you must choose one.	**%** **chmod** {**u g o a**}=[**r**][**w**][**x**] *file*

Table 2: *Typographic conventions for commands*

Chapter 1

Connecting the Appliance

Overview

Introduction

This chapter contains procedures for connecting Proventia G Intrusion Prevention appliances.

In this chapter

This chapter contains the following topics:

Installing the Appliance

Introduction

There are two options for installing Proventia G appliances in a rack mount or cabinet system. Instruction sheets are located in your appliance packaging.

- sliding rail for 2U appliances
- mid-mount rack for 1U and 2U appliances

Box contents

The Proventia G appliance packaging includes the following:

- AC or DC power cable(s)
- sliding rail kit (option 1)
- mid-mount rack kit (option 2)
- appliance recovery CD
- RJ-45 to DB9 serial cable
- strain relief
- warranty statement
- bezel cover with keys
- mouse/keyboard Y-cable
- crossover connector and patch cable (copper only)

Proventia G Appliances Front and Back Panels

Introduction

This topic identifies the parts of a Proventia G100, G200, G1000, and G1200 appliance. The front and back panel figures have descriptions for each item.

Front panel diagram

The Proventia G100, G200, G1000, G1200 front panel is shown in Figure 1:

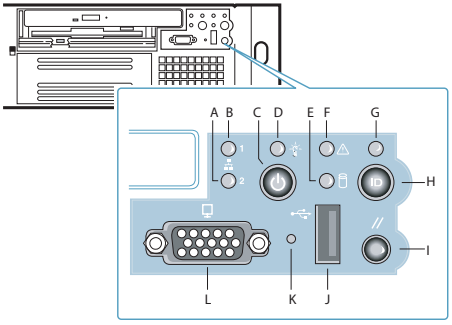

Figure 1: *G100/G200/G1000/G1200 appliance front panel*

Front panel legend

The front panel of a Proventia G100, G200, G1000, G1200 appliance includes the following:

- A (2) - Management Interface LED
- B (1) - RSKill Interface LED
- C - Power Button
- D - Power LED
- E - Hard Drive Activity LED
- F - Fault LED
- G - System ID LED
- H - System ID Button
- I - Reset Button
- J - USB (unused)
- K - Unused
- L - Video

Caution: You must operate this unit with the top cover installed to ensure proper cooling.

Note: A Fault LED light generally does not indicate a problem with the appliance itself. The light can appear if the power supply is not plugged in.

Back panel diagram (G100/G200)

The Proventia G100 /G200 (1U) back panel is shown in Figure 2:

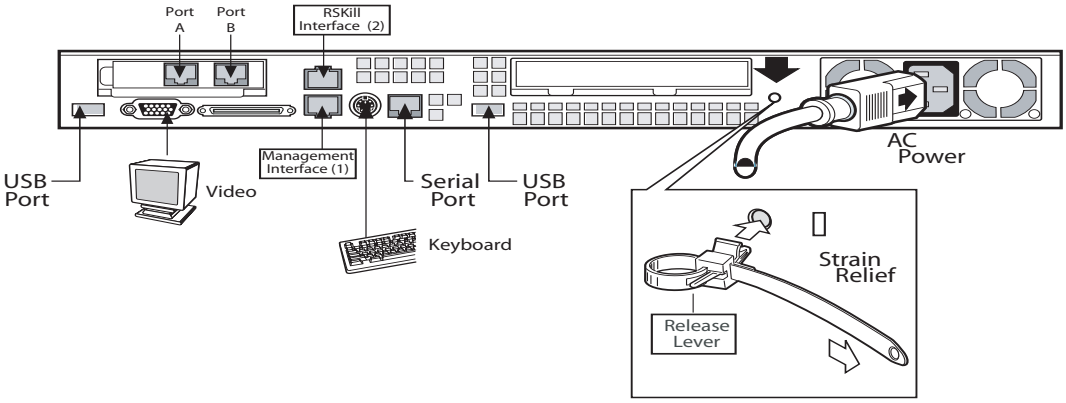

Figure 2: *G100/G200 appliance back panel*

Back panel diagram (G1000/G1200)

The network card is on the right side of the Proventia G1000 appliance. The Proventia G1200 appliance has eight ports. The Proventia G1200 offers AC or a DC power option. The Proventia G1000/G1200 (2U) back panel is shown in Figure 3:

Note: The AC power option is shown in Figure 3. The DC power information is shown in Figure 4 on page 7.

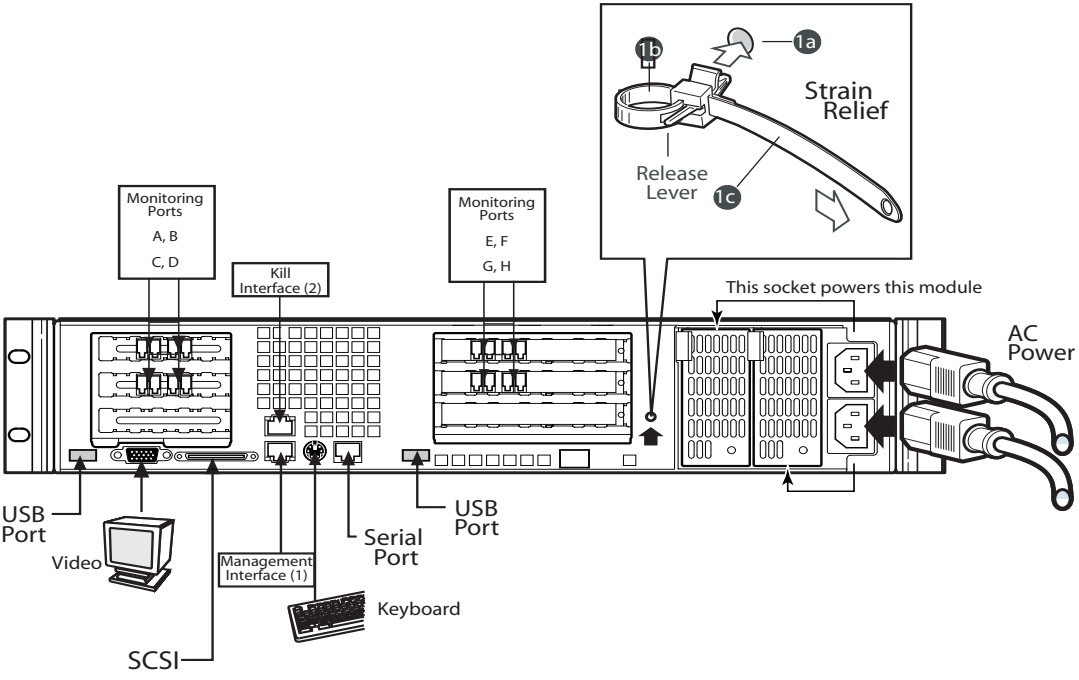

Figure 3: *G1000/G1200 appliance back panel*

Connecting the Cables and Starting the Appliance

Introduction

This topic provides instructions for connecting cables and starting a Proventia G Intrusion Prevention appliance.

Important: ISS recommends that the SiteProtector or remote access computer(s) that communicate with the appliance (this occurs through the management port, port 1) are all on the same logical side of the network as the management port. If network traffic is unable to traverse the appliance's NIC and the SiteProtector and remote access computer(s) are not on the same logical side as the management port, they will not be able to communicate with the appliance.

Installing the appliance

You can use a VT100-compatible terminal emulation program, such as Hyperterminal, to install the appliance. You can also connect the appliance to a keyboard and monitor.

Connecting the AC power cord

The Proventia G100/G200 (1U) appliances come with one AC power connector. The Proventia G1000/G1200 (2U) appliances come with dual standard AC power connectors and a DC power option (G1200 only). To connect the AC power cord(s):

1. Press the strain relief into the platform hole until it snaps into place.
2. Place the power cord into the loop. Leave some slack in the power cord between the strain relief and the power supply.
3. Pull the tab to secure the power cord in the loop.
4. Insert the female end the power cord into the back of the appliance as shown in Figure 2 and Figure 3.
5. Insert the male end of the power cord into a standard AC power supply.

DC power supply

The DC power supply used with the Proventia G1200 appliance uses a -48 to -60 VDC input switching power subsystem, which provides up to 470 Watts with -48 to -60 VDC input and with current and remote sense regulation. The power subsystem consists of one or two 470-Watt power supply modules. A system with two modules forms a redundant, hot-swappable (1+1) power subsystem.

Note: The DC power supply is only available for the Proventia G1200 appliance.

Back panel diagram (G1200)

The Proventia G1200 appliance has eight ports. DC power option is only offered on the Proventia G1200 appliance. The Proventia G1200 (2U) back panel is shown in Figure 4:

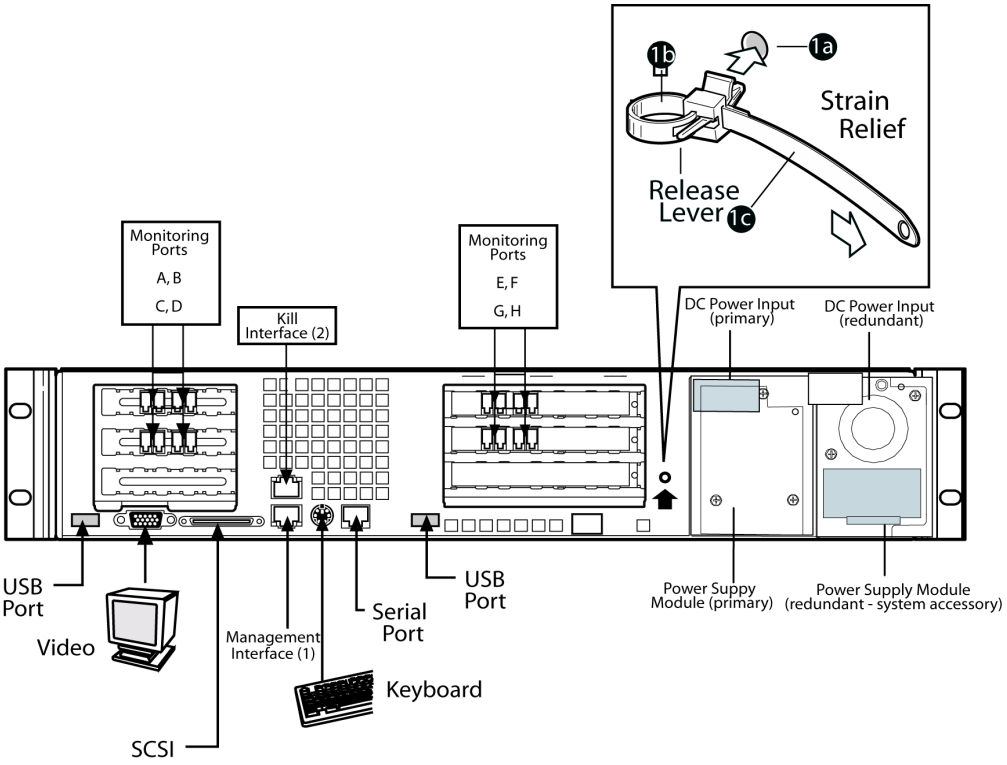

Figure 4: *G1200 appliance back panel with DC power option*

DC power supply features

The DC power supply includes the following features:

- 470-Watt output capability in full DC input voltage range
- power good indication LEDs
- predictive failure warning
- iInternal cooling fans with multi-speed capability

- remote sense of 3.3-Volt, 5-Volt, and 12-Volt DC outputs
- "DC_OK" circuitry for brown-out protection and recovery
- built-in load sharing capability
- built-in overloading protection capability
- onboard field replaceable unit (FRU) information
- I^2C interface for server management functions
- integral handle for insertion/extraction

Interface requirements for DC power

Table 3 identifies the interface requirements for DC power:

Interface	Description
DC Input	The DC power source may produce hazardous voltage levels exceeding -60 VDC and high energy levels above 240VA that may cause electric shock or burns. All DC input connections should be made only by a qualified service person to prevent injury. All wiring terminals connected to the DC input terminal block must be fully insulated with no exposed bare metal.
DC Output Connectors	The power subsystem DC power and control signals are connected to the server system by means of a wire harnesses when the power supply modules are inserted into the power subsystem enclosure. The safety ground pin of the power supply module is the first pin to connect and the last to disconnect when the module is being inserted or removed from the power subsystem housing. In addition to the 5-V Standby, -12 V, +3.3 V, +5 V and +12 VDC outputs, the following signals and output pins are included: • +3.3 VDC remote sense • +5 VDC remote sense • +12 VDC remote sense • Remote sense return • Power Subsystem On (DC PWR enable) • Power Good

Table 3: *Interface requirements for DC power*

DC power supply module LED indicators

There is a single bi-color LED to indicate power supply status that is visible on the back of the system. Table 4 shows the conditions confirmed by the LED indicators.:

Power Supply Condition	Power Supply LED
No DC power to all PSUs	OFF
No DC power to this PSU only	AMBER
DC present/Only Standby Outputs On	BLINK GREEN
Power supply DC outputs ON and OK	GREEN
Current limit	AMBER
Power supply failure (OTP, OCP, OVP, UV)	AMBER

Table 4: *DC power supply LED status conditions*

Note: S Failure, PS Presence, PS Predictive Fail, +12 V Mon, +5 V Mon, and the 5 V Standby rails failure are being monitored via an I2C interface chip.

DC input voltage specification

The power supply will operate within all specified limits over the input voltage range outlined in the Table 5. The power supply will power-off if the DC input is less than -34 VDC.

Parameter	Minimum Tolerance	Nominal Rating	Maximum Tolerance	Maximum Input Current
Voltage	-38VDC	-48 to -60VDC	-75VDC	17.0 Amps

Table 5: *DC input voltage range*

DC output current specifications

The combined output power of all outputs will not exceed 450 W. The power supply meets both static and dynamic voltage regulation requirements for the minimum dynamic loading conditions. The power supply meets only the static load voltage regulation requirements for the minimu1. Combined 3.3V/5V shall not exceed 0A.

Each output has a maximum and minimum current rating, as shown in Table 6.

Voltage	Current Rating
+3.3 VDC Output	20 Amp Max[1]
+5 VDC Output	26 Amp Max[1]
+12 V1DC Output	16 Amp Max[2]
+12 V2DC Output	12.0 Amp Max[2]
+12 V3DC Output	12.0 Amp Max[2]
-12 VDC Output	0.5 Amp Max
+5 VDC Standby	2.0 Amp Max
Output balancing	Total combined output power of all output shall not exceed 450 W.
DC Line Voltage	-48VDC to –60VDC
DC Input Current	17.0 Amp maximum

Table 6: *DC output voltage range*

Note: 1. Combined 3.3V/5V shall not exceed 150W. 2. Maximum continuous load on the combined 12V output shall not exceed 25A. Peak load on the combined 12V output shall not exceed 30A for greater than 10 seconds.

Connecting the appliance to a computer or laptop

To connect the appliance to a computer or laptop:

1. Plug one end of the serial cable into the serial port on the back of the appliance as shown in Figure 2 on page 4 and Figure 3 on page 5.
2. Plug the other end of the serial cable into the serial port on your computer or laptop.
3. Use a VT100-compatible terminal emulation program, such as Hyperterminal, to create a connection to the appliance with the following settings:

Note: If you are not using the Hyperterminal program, then your settings in Table 7 may be different. For more information, refer to the documentation for your program.

Setting	Value
Bits per second	9600
Data bits	8
Parity	None
Stop bits	1
Flow control	None
Communications Port	Typically COM1, but this depends on the computer you are using

Table 7: *Hyperterminal settings*

Setting up terminal emulation

To set up the terminal emulation:

1. In the Hyperterminal application, go to **File→ Properties→ Settings**.
2. Select **Emulation = VT100**.
3. Click **OK**.

Connecting the network cable

To connect the network cable:

1. Connect the management interface on the back panel to the network you will use to manage it.
2. Connect the network cables to correspond with the operation mode (inline or passive) you plan to use for the appliance.

   Note: If you configure the appliance to operate in inline protection or inline simulation modes, see "Inline Deployment Scenarios" on page 14.
3. If you are using passive mode, then use the kill interface to connect the appliance to the network and send the RSKill response for events, and use detection port A to connect to one hub, SPAN port, or tap.

   Note: The appliance still aggregates full-duplex traffic with a full-duplex tap set up to use both ports A and B. The cable and coupler will not be used. The appliance can monitor a total of one segment despite the existence of two ports (A and B).

Connecting the External Bypass Unit

Introduction

This topic explains how to connect the external bypass unit to a Proventia G fiber or copper-fiber appliance. The external bypass unit monitors the appliance and ensures that network traffic continues to pass if the appliance fails or loses power.

Included items

The bypass unit box contains the following items:

Single Bypass Unit	Dual Bypass Unit
One USB cable	Two USB cables
Two fiber cables	Four fiber cables
Bezel cover with keys	Bezel cover with keys
Proventia G100/G200/G1000/G1200 Quick Start Guide	Proventia G100/G200/G1000/G1200 Quick Start Guide

Additional network cables required

You must have two additional network cables to connect a bypass unit to a network switch/router. This shipment does not include these cables.

Connecting the cables

To connect the bypass unit to the appliance:

1. Connect the fiber cables from the network ports on the bypass unit to network switch/routers.

   Important: Verify that traffic flows before you proceed with Step 2.

2. Connect the fiber cables (included with shipment) from the appliance ports on the bypass unit to the corresponding ports on the back of the appliance.
3. Connect the USB cable from the USB port on the bypass unit to the USB port on the back of the appliance.

Configuration diagram

Figure 5 illustrates the bypass unit to appliance configuration:

Note: Internet Security Systems recommends that the connection ports on the internal bypass unit and the appliance face the back of the rack for easy connectivity.

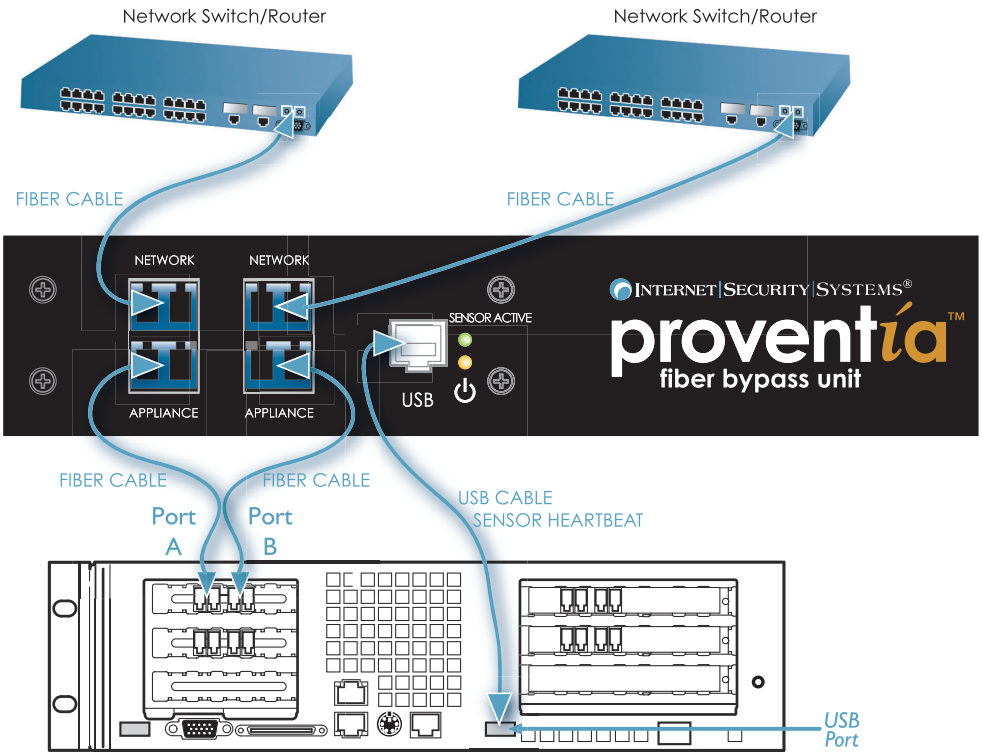

Figure 5: *Bypass unit to appliance configuration*

Inline Deployment Scenarios

Introduction

The Proventia G100, G200, G1000, and G1200 appliances have built-in copper bypass hardware, which ensures that traffic continues to pass if the appliance fails or loses power.

Note: The Proventia G1000F and G1200F do not have built-in bypass hardware. You can purchase an external fiber bypass unit that provides bypass functionality (contact Internet Security Systems for availability). See "Connecting the External Bypass Unit" on page 12.

Cabling guidelines

Place a CAT5 crossover cable between a Proventia G appliance and a server or workstation. ISS recommends using a CAT5 crossover cable between a Proventia G appliance and a router. A straight cable is sufficient between a Proventia G appliance and a switch or hub.

Caution: Make sure you verify that traffic is flowing **before** powering on the appliance. If cabling is incorrectly installed, the bypass will not function.

Note: Where a crossover is needed, you may use your own CAT5 crossover cable or the provided one-foot cable and crossover coupler that ships with the appliance. When the appliance is not running, its monitoring interfaces function as a crossover. The following scenarios work independently of the monitoring port (A or B) you use.

Switch/Hub1 to Switch/Hub2

When you deploy the appliance between two switches or hubs, establish straight-through connections using CAT 5 cable from Switch1/Hub1 to the appliance and from the appliance to Switch2/Hub2, as shown inFigure 6:

Figure 6: *Inline deployment scenario, switch/hub to switch/hub*

Workstation/ Server to Router

When you deploy the appliance between a workstation/server and a router, establish a CAT5 crossover connection from the workstation/ server to the appliance. Establish a crossover CAT 5 connection from the appliance to the router as shown in Figure 7:

Figure 7: *Inline deployment scenario, workstation server to router*

Workstation/ Server to Switch/ Hub

When you deploy the appliance between a workstation/server and a switch/hub, establish a CAT5 crossover connection from the workstation/server to the appliance. Establish a straight cable connection from the appliance to the switch/hub as shown in Figure 8:

Figure 8: *Inline deployment scenario, workstation server to switch/hub*

Router to Switch/ Hub

When you deploy the appliance between a router and a switch/hub, establish a CAT5 crossover connection from the router to the appliance. Establish a straight cable connection from the appliance to the switch/ hub as shown in Figure 9:

Figure 9: *Inline deployment scenario, router to switch/hub*

Router to Router

When you deploy the appliance between two routers, establish a CAT5 crossover connections from Router 1 to the appliance and from the appliance to Router 2, as shown in Figure 10:

Figure 10: *Inline deployment scenario, router to router server*

Chapter 2

Configuring the Appliance

Overview

Introduction

This chapter describes how to configure Proventia G100/G200/G1000/G1200 appliances.

In this chapter

This chapter contains the following topics:

What You Need to Know Before You Start

Introduction

This topic provides a checklist of the information that you need prior to configuring Proventia G Intrusion Prevention Appliances.

Required information checklist

Use the following checklist to obtain the information you need to configure your Proventia G appliance.

✓	Setting	Description
❑	Appliance hostname	The unique computer name for your appliance **Format:** *appliance.example.com.*
	Your setting:	
❑	Appliance domain name	The domain suffix for the network (DNS search path)
	Your setting:	
❑	Appliance domain name server	This is the IP address of the server you are using to perform domain name lookups.
	Your setting:	
❑	Management Interface IP Address	This is the IP address of the management network adapter.
	Your setting:	
❑	Management interface subnet mask	This is the subnet mask value for the network that will connect to your management interface.
	Your setting:	
❑	Management interface default gateway (IP address)	This is the IP address for the management gateway.
	Your setting:	

Table 8: *Checklist and worksheet for configuration information*

✓	Setting	Description
❑	Operation mode	This is the operation mode to use for the appliance. The operation mode you plan to use should correspond to the way you connected the network cables.
	Your setting:	

Table 8: *Checklist and worksheet for configuration information (Continued)*

Logging On and Configuring the Appliance

Introduction

This topic describes how to log on to and configure a Proventia G Intrusion Prevention Appliance.

Logging on and changing the password

To log on to the appliance:

1. Access the Proventia Setup utility (command line interface).
2. At the command login prompt, type **admin** for the user name, and then press ENTER.
3. Type **admin** for the password, and then press ENTER.

   The Proventia G Appliance Setup screen appears.
4. Press ENTER.
5. Read the Software License Agreement, and then type **Y** to accept its terms.
6. Type the old password **admin**, and then a new password.

   Note: You must use a minimum of six characters.
7. Re-type the new password to confirm it, and then press ENTER.

   Note: Record and protect this password. If you lose or forget this password, you must reinstall the appliance.
8. Press ENTER.

   The Network Configuration screen appears.

About configuration settings

The Proventia G appliance includes settings for processing traffic, as follows:

- changing the capture buffer size
- configuring network congestion options
- configuring agent options

Important: Network congestion, unresponsive agent, and agent update options are only used in inline protection modes. These options are not used in passive mode.

Reference: For more information about these settings, see the *Proventia G Series Appliances User Guide*.

Changing the capture buffer size

The default buffer size for capturing packets is 80 MB. In general, the capture buffer size does not need to be changed.

Configuring network congestion options

You can configure how the agent processes traffic when the network is congested. Options are as follows:

Option	Description
Forward Traffic	This option forwards traffic without processing it, or fails open to traffic. When traffic levels return to normal, the agent resumes normal operation.
Drop Traffic	This option blocks some of the traffic without processing it, or fails closed to traffic. When traffic levels return to normal, the agent returns to normal operation.
No Action	This option does not compensate for network congestion. If the agent cannot process the traffic, the appliance may go into bypass mode for a short period on appliance models that have bypass cards (G100/G200/G1000C). The connection to the network may be lost for a short period of time on appliance models that do not have bypass cards (G1000F).

Table 9: *Congestion options*

Configuring the network and host

To configure the network and host:

1. Type the **IP Address**, **Subnet Mask**, and **Gateway** of the appliance's management interface, and then press ENTER.

   The appliance displays the message:

   ```
   Network configured
   ```

2. Press ENTER.

   The Host Configuration screen appears.

3. Type the **Hostname** (required), **Domain Name** (recommended), and **Name Server** (recommended) for the appliance, and then press ENTER.

Note: The appliance uses domain names and DNS information to send Email and SNMP responses. If you do not provide this information now, then you must specify the IP address of the appliance's mail server when you define the Email response on the management console. The appliance must have network access to the mail server.

The appliance displays a progress message while it configures the host settings, and then displays the message:

`Host configuration has been saved.`

4. Press ENTER.

   The Timezone Configuration screen appears.

Configuring the date and time

To configure the date and time at which events occur:

1. Select the continent or ocean in which the appliance is located, and then press ENTER.
2. Select the country in which the appliance is located, and then press ENTER.
3. Select the region in which the appliance is located, and then press ENTER.

   Note: This screen does not appear if the country you selected contains only one time zone.

4. Type **y** to confirm, and then press ENTER.

   The Date/Time Configuration screen appears.

5. Press ENTER to accept the **Date** and **Time** for the appliance, or type a new time and press ENTER.

   Note: Use the format [`HH:MM:SS`] and a 24-hour clock.

   The appliance displays the message `Date and time set`.

6. Press ENTER.

   The Agent Name Configuration screen appears.

Configuring agent options

You can configure how the driver processes traffic if an agent becomes unresponsive or during an agent update. If an agent is not responding, then it is not monitoring and protecting the network. You can configure the agent to pass all traffic (fail open to traffic) or drop all traffic (fail closed to traffic) when it is not responding. Options are as follows:

- maintain link and forward traffic
- maintain link and drop traffic
- do not maintain link

Configuring the agent name

To configure the agent name:

1. Press ENTER to accept the default agent name, or type a specific name and then press ENTER.

   Note: This is the asset name that appears for this appliance in your management interface. ISS recommends that you select a name that corresponds to the appliance's geographic location, business unit, building address, or some other meaningful classification.

   The appliance continues to apply your configuration settings. The status bar displays a message when the configuration ends.

2. Press ENTER.

   The Port Link Configuration screen appears.

Setting duplex and link speed

Proventia G appliance models G100, G200, and G1000 have two ports labeled A and B. The Proventia G1200 appliance has eight ports labeled A through H. You can configure link speed and duplex mode settings appropriate for the appliance you have installed. To improve appliance performance, choose link speed and duplex mode settings to match your environment. If you are not sure which settings are correct for your environment, choose Auto/Auto.

Exception: The default Auto/Auto settings are correct for all environments except for 100 Full Duplex and 10 Full Duplex. You must specifically select the duplex mode and link speed applicable for these environments, as follows:

- 100 Full Duplex–select Full Duplex mode and link speed 100 Mbps
- 10 Full Duplex–select Full Duplex mode and link speed 10 Mbps

Note: For more information, see the *Proventia G Appliances User Guide,* "Changing the Link Speed and Duplex Mode Settings.

Configuring the link speed and duplex mode settings

To configure the link speed and duplex mode settings:

1. Select Port A, and then press the SPACE BAR to select the port link speed and duplex mode.
2. Select Port B, and then press the SPACE BAR to select the port link speed and duplex mode.

   Note: If you are configuring a Proventia G1200 appliance, repeat Steps 1 and 2 to select additional ports.
3. Press ENTER.

   The Mode Configuration screen appears.

Determining the operation mode

Determine the operation mode to use with the appliance. There are three operation modes, as follows:

Operation Mode	Description
Inline Protection	The appliance monitors traffic inline, and blocks attacks that are configured with the drop response, dynamic blocking response, and firewall rules.
Inline Simulation	The appliance monitors traffic inline, but does not block any traffic. Instead, the appliance monitors traffic and provides passive responses.
Passive Monitoring	The appliance monitors traffic from a tap, hub, or span port.

Table 10: *Operation modes*

Configuring the operation mode

To configure the operation mode:

1. Select an operation mode.
2. Press ENTER.
3. Do one of the following:
   - If you selected passive monitoring, the Mode Change Confirmation screen appears. See "Confirming passive monitoring mode" on page 25.
   - If you selected inline protection or inline simulation, See "Applying settings and logging out" on page 26.

Confirming passive monitoring mode

To confirm passive monitoring mode:

1. Select passive monitoring from the Mode Change Configuration screen.

   The Mode Change Confirmation screen appears

2. You are asked, "Do you want to confirm passive monitoring mode?"
   - If *yes*, type **y**, and then go to Step 2.
   - If *no*, type **n**, and then select a different operation mode, as described in "Configuring the operation mode."

Configuring the RSKILL response

To configure the RSKILL response:

1. When you are in the RSKILL response screen, you are asked the following:

   Do you want to configure the RSKill response?
   - If *yes*, type **y**, and then go to Step 2.
   - If *no*, type **n**, and then Press ENTER.

   Note: When the appliance detects an attack, the RSKill response terminates or resets the connection to the targeted computer.

2. Do you want to use a DHCP server?
   - If *yes*, press the SPACE BAR to select DHCP.
   - If *no*, type the static addresses in the **IP Address**, **Subnet Mask**, and **Gateway**.

   Tip: To move from one field to the next, press TAB.

   Note: The RSKill response occurs in stealth mode. The appliance uses these static network addresses to determine the gateway MAC address. If the appliance cannot determine the MAC address, then you must manually enter the address on the next screen.

3. Press ENTER.

   The appliance attempts to determine and display the gateway MAC address.

4. Did the appliance determine its MAC address?
   - If *yes*, press ENTER.
   - If *no*, type the MAC address.

Note: If you do not know the MAC address, contact your system administrator.

5. Press ENTER.

   The appliance continues to apply your configuration settings, and then displays a message when the configuration is complete.

Applying settings and logging out

To apply settings and log out:

1. Press ENTER.

   The appliance displays a message that it will now log you off. You can log back in at any time to change configuration settings.

2. Press ENTER.

   The login prompt appears.

   Note: You may disconnect the monitor and keyboard or the computer that you just used. You can make all future connections to the appliance using the ISS management interface. Use SSH to access the appliance and maintain configuration settings.

Connecting to the Management Console

Introduction

This topic explains how to connect to the SiteProtector management console.

Managing the appliance from SiteProtector

After you have installed and configured the appliance, you must configure additional appliance settings and edit appliance policies from the SiteProtector management console.

Reference: For instructions on managing the appliance from the management console, see the SiteProtector documentation at http://www.iss.net/support/documentation/. Also see the SiteProtector Help.

Accessing the SiteProtector Help

To access the SiteProtector Help:

1. On the Console menu bar, select **Help→SiteProtector Help**.
2. Open the *Working with Proventia A and Proventia G Appliances and Sensors* section.
3. Look up "Working with Proventia Appliance Policies" and "Working with Asset Properties and Responses."

Licensing

Proventia G appliances require a properly configured license key. If you have not installed the appropriate license key through the management console, you will not be able to manage the appliance.

Purchasing a license: To purchase a license for a Proventia G appliance, contact your local sales representative.

Chapter 3

Reinstalling the Appliance

Overview

Introduction

This chapter describes the processes and procedures for reinstalling the Proventia G100, G200, G1000, or G1200 Intrusion Prevention Appliance. You must reinstall the appliance software to restore the appliance to its original configuration and to remove any customized settings.

What you need

To reinstall a Proventia G appliance, you need:

- a laptop or computer to use as your configuration interface
- a *Proventia G Appliance Recovery CD*

In this chapter

This chapter contains the following topics:

Reinstallation Requirements

Introduction

You can use the *Proventia G Appliance Recovery CD* to reinstall the appliance. The CD reinstalls the original, unconfigured software. To reinstall the software, you must complete the following procedures:

- reinstall the appliance
- log in and change the password
- configure the network and host
- configure the date and time
- configure the agent name
- configure the link speed and duplex mode settings
- configure the operation mode
- confirm passive monitoring mode
- configuring the RSKILL response
- apply settings and log out

Note: After rebooting with the recovery CD, the appliance reverts to the default login name and password.

Prerequisites

Before you reconfigure the appliance, you must have completed the following prerequisites:

- Verify the IP address, subnet mask, and default gateway of the appliance's management interface.
- Verify the hostname (required), domain name (recommended), and DNS name server (recommended) for the appliance.
- Verify that the appliance is operational. If your appliance is not operational, contact ISS Customer Support at support@iss.net.

Reinstalling the Appliance

Reinstalling the appliance

To reinstall the appliance:

1. If there is a bezel cover on the front of the appliance, remove it.
2. Place the *Proventia G Appliance Recovery CD* in the CD-ROM drive.
3. Connect a computer or monitor and keyboard to the appliance.

   Reference: For more information, see "Setting up terminal emulation" on page 11.
4. Reboot the appliance.

   Tip: You can manually turn the power off and on if the appliance is not responding.

   The appliance reboots and reloads the operating system.
5. Type **`reinstall`**, and then press ENTER.

   The appliance displays status messages, ejects the CD, and then reboots.

Logging on and changing the password

To log on and change the password:

1. When the appliance has rebooted, type **`admin`** at the unconfigured login prompt, and then press ENTER.
2. Type **`admin`** at the Password prompt, and then press ENTER.

   The Proventia G Setup screen appears.
3. Press ENTER.

   The Software License Agreement appears.
4. Read the Software License Agreement, and then type **`y`** to accept its terms.

   The Change Password screen appears.
5. Type the old password, **`admin`**, and then type a new password.

   Note: You must use a minimum of six characters.
6. Retype the new password to confirm it, and then press ENTER.

   Note: Record and protect this password. If you lose or forget this password, you must reinstall the appliance.

7. Press ENTER.

   The Network Configuration screen appears.

Configuring the network and host

To configure the network and host:

1. Type the **IP Address**, **Subnet Mask**, and **Gateway** of the appliance's management interface, and then press ENTER.

   The appliance displays the message:

   `Network configured.`

2. Press ENTER.

   The Host Configuration screen appears.

3. Type the **Hostname** (required), **Domain Name** (recommended), and **Name Server** (recommended) for the appliance, and then press ENTER.

   Note: The appliance uses domain names and DNS information to send Email and SNMP responses. If you do not provide this information now, then you must specify the IP address of the appliance's mail server when you define the Email response on the management console. The appliance must have network access to the mail server. For more information, see the management console's user documentation.

   The appliance displays a progress message while it configures the host settings, and then displays the message `Host configuration has been saved` when the configuration is complete.

4. Press ENTER.

   The Timezone Configuration screen appears.

Configuring the date and time

To configure the date and time at which events occur:

1. Select the continent or ocean in which the appliance is located, and then press ENTER.
2. Select the country in which the appliance is located, and then press ENTER.
3. Select the region in which the appliance is located, and then press ENTER.

Note: This screen does not appear if the country you selected contains only one time zone.

4. Type **y** to confirm, and then press ENTER.

   The Date/Time Configuration screen appears.

5. Press ENTER to accept the **Date** and **Time** for the appliance, or type a new time and press ENTER.

   Note: Use the format [`HH:MM:SS`] and a 24-hour clock.

   The appliance displays the message `Date and time set`.

6. Press ENTER.

   The Agent Name Configuration screen appears.

7. Go to "Configuring the agent name," next in this topic.

Configuring the agent name

To configure the agent name:

1. Press ENTER to accept the default agent name, or type a specific name and then press ENTER.

   Note: This is the asset name that appears for this appliance in your management interface. ISS recommends that you select a name that corresponds to the appliance's geographic location, business unit, building address, or some other meaningful classification.

   The appliance continues to apply your configuration settings. The status bar displays a message when the configuration ends.

2. Press ENTER.

   The Port Link Configuration screen appears.

Configuring the link speed and duplex mode settings

Proventia G appliance models G100, G200, and G1000 have two ports labeled A and B. The Proventia G1200 appliance has eight ports labeled A through H. You can configure link speed and duplex mode settings appropriate for the appliance you have installed.

To configure the link speed and duplex mode settings:

1. Select Port A, and then press the SPACE BAR to select the port link speed and duplex mode.
2. Select Port B, and then press the SPACE BAR to select the port link speed and duplex mode.

   Note: If you are configuring a Proventia G1200 appliance, repeat Steps 1 and 2 to select additional ports.
3. Press ENTER.

   The Mode Configuration screen appears.

Configuring the operation mode

To configure the operation mode:

1. Select an operation mode.
2. Press ENTER.
3. Do one of the following:
   - If you selected passive monitoring, the Mode Change Confirmation screen appears. Go to "Confirming passive monitoring mode."
   - If you selected inline protection or inline simulation, see "Applying settings and logging out" on page 36.

Confirming passive monitoring mode

To confirm passive monitoring mode:

1. Do you want to confirm passive monitoring mode?
   - If *yes*, type **y**, and then go to Step 2.
   - If *no*, type **n**, and then select a different operation mode, as described in "Configuring the operation mode."
2. Press ENTER, and then go to "Configuring the RSKILL response" on page 35.

Configuring the RSKILL response

To configure the RSKILL response:

1. Do you want to configure the RSKill response?
   - If *yes*, type **y**, and then go to Step 2.
   - If *no*, type **n**, and then go to Step 1 in "Applying settings and logging out," next in this topic.

   Note: When the appliance detects an attack, the RSKill response terminates or resets the connection to the targeted computer.
2. Do you want to use a DHCP server?
   - If *yes*, press the SPACE BAR to select DHCP.
   - If *no*, type the static addresses in the **IP Address**, **Subnet Mask**, and **Gateway**.

   Tip: To move from one field to the next, press TAB.

   Note: The RSKill response occurs in stealth mode. The appliance uses these static network addresses to determine the gateway MAC address. If the appliance cannot determine the MAC address, then you must manually enter the address on the next screen.
3. Press ENTER.

   The appliance attempts to determine and display the gateway MAC address.
4. Did the appliance determine its MAC address?
   - If *yes*, press ENTER.
   - If *no*, type the MAC address.

   Note: If you do not know the MAC address, contact your system administrator.
5. Press ENTER.

   The appliance continues to apply your configuration settings, and then displays a message when the configuration is complete.

Applying settings and logging out

To apply settings and log out:

1. Press ENTER.

   The appliance displays a message that it will now log you off. You can log back in at any time to change configuration settings.

2. Press ENTER.

   The login prompt appears.

Getting Technical Support

Introduction

ISS provides technical support through its Web site and by email or telephone.

The ISS Web site

The Internet Security Systems (ISS) Resource Center Web site (http://www.iss.net/support/) provides direct access to frequently asked questions (FAQs), white papers, online user documentation, current versions listings, detailed product literature, and the Technical Support Knowledgebase (http://www.iss.net/support/knowledgebase/).

Support levels

ISS offers three levels of support:

- Standard
- Select
- Premium

Each level provides you with 24-7 telephone and electronic support. Select and Premium services provide more features and benefits than the Standard service. Contact Client Services at clientservices@iss.net if you do not know the level of support your organization has selected.

Hours of support

The following table provides hours for Technical Support at the Americas and other locations:

Location	Hours
Americas	24 hours a day
All other locations	Monday through Friday, 9:00 A.M. to 6:00 P.M. during their local time, excluding ISS published holidays **Note:** If your local support office is located outside the Americas, you may call or send an email to the Americas office for help during off-hours.

Table 11: *Hours for technical support*

Contact information

The following table provides electronic support information and telephone numbers for technical support requests:

Regional Office	Electronic Support	Telephone Number
North America	Connect to the MYISS section of our Web site: www.iss.net	**Standard:** (1) (888) 447-4861 (toll free) (1) (404) 236-2700 **Select and Premium:** Refer to your Welcome Kit or call your Primary Designated Contact for this information.
Latin America	support@iss.net	(1) (888) 447-4861 (toll free) (1) (404) 236-2700
Europe, Middle East, and Africa	support@iss.net	(44) (1753) 845105
Asia-Pacific, Australia, and the Philippines	support@iss.net	(1) (888) 447-4861 (toll free) (1) (404) 236-2700
Japan	support@isskk.co.jp	Domestic: (81) (3) 5740-4065

Table 12: *Contact information for technical support*

Index

m

o

p

r

s

t

w