



WebSpy Sentinel 3.1
Planning and Installation Guide



Table of Contents

Introduction.....	1
<i>Getting Help.....</i>	<i>1</i>
Before you start... ..	1
<i>Hardware Requirements.....</i>	<i>2</i>
<i>Software Requirements.....</i>	<i>2</i>
<i>Network Structure Questions</i>	<i>3</i>
<i>Sentinel Usage Questions</i>	<i>3</i>
User Name Resolution	4
<i>Windows NT® 4.....</i>	<i>4</i>
<i>Windows® 2000 and Windows® XP.....</i>	<i>6</i>
Deploying Sentinel	8
<i>Determining your Optimum Installation Point.....</i>	<i>9</i>
<i>Connecting Sentinel to the Optimum Installation Point</i>	<i>10</i>
Definitions	11
Network Diagrams	13
<i>Case Study One.....</i>	<i>13</i>
<i>Case Study Two.....</i>	<i>14</i>
<i>Case Study Three.....</i>	<i>15</i>
<i>Case Study Four</i>	<i>16</i>
<i>Case Study Five.....</i>	<i>17</i>
<i>Case Study Six</i>	<i>18</i>

© WebSpy Ltd. 2001 - 2002

All Rights Reserved. No part of this document may be photocopied, reproduced, stored in a retrieval system, or transmitted, in any form or by any means whether, electronic, mechanical, or otherwise without the prior written permission of WebSpy Ltd.

No warranty of accuracy is given concerning the contents of the information contained in this publication. To the extent permitted by law no liability (including liability to any person by reason of negligence) will be accepted by WebSpy Ltd, its subsidiaries or employees for any direct or indirect loss or damage caused by omissions from or inaccuracies in this document.

WebSpy Ltd. reserves the right to change details in this publication without notice.

Windows is a trademark and Microsoft, MS-DOS, and Windows NT are registered trademarks of Microsoft Corporation. Other product and company names herein may be the trademarks of their respective owners.

This product includes software developed by the Politecnico di Torino, and its contributors.

Copyright (c) 1999, 2000, Politecnico di Torino. All rights reserved.



Introduction

WebSpy Sentinel is a program that enables you to record all web, mail newsgroup, telnet and FTP traffic on your network without the need for proxy server software. The logged data is stored in a log file format that can subsequently be imported into *WebSpy Analyzer* and examined to identify Internet usage patterns of your employees or departments. See *Analyzer's Help* for details on how to import and examine your log files.

WebSpy Sentinel captures all traffic passing through the network on which it is installed but only keeps (or logs) the protocols that you choose. You can log just the basic information about the Internet traffic you are seeing (i.e. source, destination, URL etc.) or you can capture all of the content of that traffic. See *Sentinel's Getting Started Guide* for more information.

WebSpy Sentinel is made up of two parts: Sentinel Service, and Sentinel Management. Sentinel Service is the driver, which connects to your Network Card, and the service, which logs the data. The driver and the service are always installed together, so that the driver can 'see' all Internet traffic. Sentinel Management is used to configure the Sentinel Service running on multiple computers on the same network. You can install Sentinel Management on any computer on your network with access to all of the computers running Sentinel Service. This guide will help you to determine where to install. Therefore it is essential that the point of installation for the Service is planned and implemented correctly.

Please see on page 11 for an explanation of terms used in this guide.

Getting Help

For more information on installing, configuring and using *Sentinel*, please see *Sentinel's Users' Guide*. If you require help within the product itself, press F1 to open *Sentinel's* help at the most appropriate topic.

Support is available by contacting WebSpy Support at support@webspy.com. If you contact Support, please provide full details about your network structure and software, including the types and manufacturers of your hardware and the software installed on your Sentinel Servers.

Before you start...

This guide is intended to help you decide how many installations of *Sentinel* you will require, where to put them, and what computers to install *Sentinel* on.



Hardware Requirements

A computer that has Sentinel installed on it is referred to as a Sentinel Server. This Sentinel Server must have the following hardware:

Item	Minimum	Recommended
CPU	P200 MX	PIII 450
RAM	64 MB	128 MB
Disk Space	6 MB for program, plus storage space for data	6 MB for program, plus at least 200 MB for data
Network Device	Ethernet network card	Ethernet network card

Hint: To calculate the storage space required, check with your ISP to see how much data you download each month, for example, and use this to determine how much storage space you will need. If this information is not available, just provide a reasonable amount of space, e.g. 200 MB, and monitor the amount used each day to judge the storage requirements. Remember, you can configure each Sentinel Server to store data locally or on your network.

Software Requirements

Your Sentinel Server must have either Windows NT® 4 SP5, Windows® 2000, Windows® XP, Windows® 98 SE or Windows® ME installed. Optimally, your Sentinel Server will have Windows NT®, Windows® 2000 or Windows® XP installed.

Additional applications may be run on the same machine that *Sentinel* is installed onto. However, if you use an application similar to *Sentinel*, you must install it on a different computer.

Windows® 98, Windows® 98 SE, Windows® ME

- Because these operating systems are not as efficient at managing memory as Windows NT®, Windows® 2000 and Windows® XP, the performance of *WebSpy Sentinel* will not be optimal.
- Sentinel Service will run as an application – not a service – on these operating systems. To start the Sentinel Service application, find the location of the file Sentinel.exe. To stop the application, you will have to press Ctrl+Alt+Delete to open the Close Program dialog and close *Sentinel* from there.
- Username resolution is not available, since these operating systems do not provide the required information.



Windows NT®, Windows® 2000, Windows® XP

- Sentinel Service will run as a Service and can be stopped or started manually, or set to run at startup, just like any other service.
- Because these operating systems are better at managing memory and CPU resources, *WebSpy Sentinel* will perform most effectively.
- Username resolution is available, but will require configuration.

Network Structure Questions

You will need to know what hardware and software you have on your network to decide where to install *WebSpy Sentinel*. If you don't have this information, consult your network administrator.

Alternatively you can forward your questions to WebSpy support at support@webspy.com. Please remember to collate as much information on your network as possible including the Internet connection, operating systems, server applications and network hardware before sending in your query.

Sentinel Usage Questions

Is Sentinel going to be used to capture full content?

For most effective content capture, ensure that the Sentinel Server has additional RAM and CPU – like most applications, *Sentinel* works best with a faster CPU and more RAM. The CPU usage and RAM requirements will be dependent on the amount of traffic and whether you choose to capture content or not. Capture of HTTP is not recommended, unless for a specific purpose as this will greatly affect computer performance. Please see the *WebSpy Sentinel* Integration Guide, which explains the effects of capturing content.

Is Sentinel going to resolve usernames?

Sentinel must be installed on a computer using Windows NT®, Windows® 2000 or Windows® XP, on a network using a Windows NT®, Windows® 2000 or Windows® XP server if you wish to resolve user names. Please see User Name Resolution on page 4 for more information.

Which protocols are to be captured?

You can choose which protocols you want to capture. As different protocols are affected by other applications on the network, you may need to install *Sentinel* in more than one position i.e. one server to capture Web and one to capture SMTP. A good example of this situation is if you use Microsoft® Exchange server. Microsoft Outlook communicates with Exchange server using a proprietary protocol that *Sentinel* cannot capture. For further information please see Determining your Optimum Installation Point on page 9.

Hint: If you want to see your internal e-mail usage, and you use Microsoft® Exchange Server, you can import your Exchange tracking logs into *WebSpy Analyzer*.

If I have to install Sentinel in more than one location, how do I administer the software?



After installing the software on one or more computers, you can use Sentinel Management to configure and monitor each Sentinel Server. You can install Sentinel Management on any convenient computer that has access to the Sentinel Servers.

User Name Resolution

To find out the actual user name for each person on your network accessing the Internet, you must install *WebSpy Sentinel* on a computer using Windows NT®, Windows® 2000 or Windows® XP that has access to a Windows NT®, Windows® 2000 or Windows® XP Primary or Backup Domain Controller.

To use a domain controller to get the information *Sentinel* needs, you must set Sentinel Service up so that it has permission to audit the security logs. See the section below for the instructions appropriate to your operating system.

For Sentinel to be able to resolve usernames, there are five things you will need to do:

- Create a new user account belonging to the Domain Admins group for Sentinel Service to run as
- Ensure that the security logs are created with the appropriate information about users logging on and off
- Give the Sentinel user permission to audit security logs
- Make sure the Sentinel user has permission to log on as a service
- Make Sentinel Service run using the Sentinel user account you created

Note: These actions must be performed by a domain administrator.

Windows NT® 4

You will need to perform these tasks on your primary domain controller.

To create a new user account for Sentinel:

- 1 Go to **Start | Programs | Administrative Tools (Common) | User Manager for Domains**. The User Manager dialog is opened for you.
- 2 Select **User | New User** from the main menu of the User Manager dialog to open the New User dialog
- 3 In the New User dialog:
 - Type an appropriate name for the Sentinel user into the Username edit box
 - Enter a password for the Sentinel user
 - Confirm that password, and
 - Select any other password options in accordance with your organization's password policy
- 4 Click on the **Groups** button at the bottom of the New User dialog to open the Group Memberships dialog
- 5 In the Group Memberships dialog
 - Select the Domain Admins group from the right-hand list



- Click on the **<-Add** button to add the Sentinel User to the Domain Admins group
 - Click **OK** to close the Group Memberships dialog
- 6 In the New User dialog click on the Add button to create the user account. Click Close to return to the User Manager dialog. The new Sentinel user you just created will be in the list of users at the top of the dialog.

To create domain security logs with the appropriate information for Sentinel:

- 1 In the User Manager dialog, select **Policies | Audit...** from the main menu to open the Audit Policy dialog
- 2 Select the 'Audit These Events' radio button to enable the checkboxes in the dialog
- 3 Check the Logon and Logoff 'Success' and 'Failure' checkboxes
- 4 Click **OK** to return to the User Manager dialog

To give the Sentinel user permission to audit domain security logs:

- 1 In the User Manager dialog, select **Policies | User Rights** to open the User Rights Policy dialog
- 2 Check the 'Show Advanced User Rights' checkbox at the bottom of the dialog
- 3 Select 'Generate security audits' from the Right drop down list
- 4 Click on the **Add** button to open the Add Users and Groups dialog
- 5 In the Add Users and Groups dialog:
 - Click on the **Show Users** button
 - Select the Sentinel user in the Names List
 - Click on the **Add** button. The Sentinel user will appear in the Add Names list
 - Click **OK** to add the Sentinel user to the list of users with permission to audit domain security logs and close the dialog.
- 6 Click **OK** to close the User Rights Policy dialog and return to the User Manager dialog

To ensure the Sentinel user logs on as a service:

- 1 In the User Manager dialog, select **Policies | User Rights** from the main menu to open the User Rights Policy dialog
- 2 Check the 'Show Advanced User Rights' checkbox at the bottom of the dialog
- 3 Select 'Log on as a service' from the Right drop down list
- 4 Click on the **Add** button to open the Add Users and Groups dialog
- 5 In the Add Users and Groups dialog:
 - Click on the **Show Users** button
 - Select the Sentinel user in the Names List
 - Click on the **Add** button. The Sentinel user will appear in the Add Names list



- Click **OK** to add the Sentinel user to the list of users that log on as a service
- 6 Click **OK** to close the User Rights Policy dialog and return to the User Manager dialog

To set Sentinel Service to run as the Sentinel user:

- 1 Go to Start | Settings | Control Panel | Services to open the Services dialog
- 2 Select Sentinel from the Service list
- 3 Click on the **Stop** button and wait until your computer says the service has been successfully stopped
- 4 Double click on Sentinel in the Service list to open the Service dialog
- 5 Select the 'This Account' radio button in the Log on as section of the dialog
- 6 Click on the ... button to the right of the Account Name edit box to open the Add User dialog, then:
 - Select the Sentinel user from the Names list
 - Click on the **Add** button, then click **OK** to return to the Service dialog
- 7 Enter the password you chose for the Sentinel user
- 8 Click **OK** to return to the Services dialog
- 9 Click on the **Start** button to restart Sentinel Service
- 10 Click **Close** to close the Services dialog

Windows® 2000 and Windows® XP

You will need to perform these tasks on your primary domain controller.

To create a new user account for Sentinel:

- 1 Go to Start | Settings | Control Panel | Administrative Tools | Active Directory Users and Computers to open the Active Directory Users and Computers dialog
- 2 In the Tree section, expand your domain and click on the Users folder
- 3 Click on the **New User** button on the toolbar to open the New Object – User dialog
- 4 In the New Object – User dialog:
 - Type an appropriate name for the Sentinel user into the Full name and User logon name edit boxes, and click **Next**
 - Enter a password for the Sentinel user, confirm that password, and select any other password options in accordance with your organization's password policy, and click **Next**
 - Check the summary for the Sentinel user is correct, and click **Finish** to close the New Object – User dialog. The new user will be added to the User list on the right hand side of the Active Directory Users and Computers dialog.
- 5 Make sure the Sentinel user is selected, and then click on the **Add user to group** button on the toolbar of the Active Directory Users and Computers dialog to open the Select Group dialog



- 6 In the Select Group dialog:
 - Select the Domain Admins group from the list
 - Click **OK** to close the Select Group dialog

To create domain security logs with the appropriate information for Sentinel:

- 1 Go to Start | Settings | Control Panel | Administrative Tools | Domain Controller Security Policy to open the Domain Controller Security Policy dialog
- 2 In the Tree section, expand the 'Security Settings' item. You may have a short wait.
- 3 Expand the 'Local Policies' item, and select the 'Audit Policy item'
- 4 Double click the 'Audit account logon events' item in the right-hand list to open the Security Policy Setting dialog
- 5 Check all the checkboxes in the dialog
- 6 Click **OK** to return to the Domain Controller Security Policy dialog. The Computer Setting information for the 'Audit account logon events' item will change to Success, Failure.
- 7 Double click the 'Audit logon events' item in the right-hand list to open the Security Policy Setting dialog
- 8 Check all the checkboxes in the dialog
- 9 Click **OK** to return to the Domain Controller Security Policy dialog. The Computer Setting information for the 'Audit account logon events' and 'Audit logon events' items should be Success, Failure.

To give the Sentinel user permission to audit security logs:

- 1 In the Domain Controller Security Policy dialog, expand the 'Security Settings' item in the Tree section. You may have a short wait.
- 2 Expand the 'Local Policies' item, and select the 'User Rights' Assignment item
- 3 Double click the 'Generate security audits' item in the right-hand list to open the Security Policy Setting dialog
- 4 In the Security Policy Setting dialog, ensure the checkbox is checked and then click on the **Add** button to open the Add user or group dialog
- 5 In the Add user or group dialog:
 - Click on the **Browse** button to open the Select Users or Groups dialog
 - Select the Sentinel user from the Names list
 - Click on the **Add** button. The Sentinel user will appear in the Add Names list
 - Click **OK** to close the Select Users or Groups dialog
 - Click **OK** to close the Add user or group dialog
- 6 Click **OK** to close the Security Policy Setting dialog and return to the Domain Controller Security Policy dialog

To ensure the Sentinel user logs on as a service:

- 1 In the Domain Controller Security Policy dialog, expand the 'Security Settings' item in the Tree section. You may have a short wait.
- 2 Expand the 'Local Policies' item, and select the 'User Rights Assignment' item
- 3 Double click the 'Log on as a service' item in the right-hand list to open the Security Policy Setting dialog
- 4 In the Security Policy Setting dialog, ensure the checkbox is checked and then click on the **Add** button to open the Add user or group dialog
- 5 In the Add user or group dialog:
 - Click on the **Browse** button to open the Select Users or Groups dialog
 - Select the Sentinel user from the Names list
 - Click on the **Add** button. The Sentinel user will appear in the Add Names list
 - Click **OK** to close the Select Users or Groups dialog
 - Click **OK** to close the Add user or group dialog
- 6 Click **OK** to close the Security Policy Setting dialog and return to the Domain Controller Security Policy dialog

To set Sentinel Service to run as the Sentinel user:

- 1 Go to Start | Settings | Control Panel | Administrative Tools | Services to open the Services dialog
- 2 Select Sentinel from the list on the right of the dialog
- 3 Click on the **Stop** button on the toolbar
- 4 Double click on Sentinel to open the Sentinel Properties dialog
- 5 Select the Log on tab
- 6 Select the 'This account' radio button and click on the **Browse** button to open the Select User dialog
- 7 In the Select User dialog:
 - Select the name of the user in the list
 - Click **OK** to return to the Sentinel Properties dialog
- 8 Type the password for the Sentinel user in the appropriate edit boxes and click **OK** to close the Sentinel Properties dialog
- 9 Click on the **Start** button on the toolbar of the Services dialog to restart Sentinel Service.

Deploying Sentinel

When you choose to install *WebSpy Sentinel*, there are a few preliminary steps you will need to go through to ensure *Sentinel* will work most effectively. These steps are:

- Determine your optimum installation point or points, where all the Internet traffic on your network passes in a form that *Sentinel* can use
- Decide the most efficient way for you to tap into the installation point(s)



- Remove any existing *WebSpy Sentinel* components from the computer that will be running *WebSpy Sentinel 3.1*

Once you have completed these steps, you can install *WebSpy Sentinel*.

Usually, you will only need one, or perhaps two, computers running Sentinel Service to capture all the Internet traffic on your network. You can install Sentinel Management on any computer with access to the computer(s) running Sentinel Service.

Please note that *Sentinel* cannot be installed on a multiprocessor machine. The current version of the network driver used by *Sentinel* is incompatible with multiprocessor architectures. This issue will be addressed in a future release of *Sentinel*.

Determining your Optimum Installation Point

The optimum installation point for Sentinel Service will depend on your network topology (i.e. how it is structured and connected). It may be possible that no one point is optimal; in these cases you will need two or more copies of Sentinel Service, depending on the network. You can install Sentinel Management on any computer with access to the computer(s) running Sentinel Service.

Please refer to Table 1 below to determine your optimum installation point.

Table 1 - Optimum Installation Point

I have...	The optimum installation position for Sentinel is...
A proxy server	On the same side of the proxy server as your users to capture web traffic
Multiple proxy servers	On the same side of each proxy server as your users to capture web traffic
A firewall	On the same side of the firewall as your users
A router connecting my network to the Internet	On the same side of the router as your users
Multiple Subnets	Between all the subnets' routers and your Internet gateway or router OR One computer running <i>Sentinel</i> on the same side of each subnet's router as that subnet's users
Network Address Translation software	Between the software and your users
A Microsoft® Exchange Server	Between the server and your Internet gateway to capture external email traffic. To log internal email traffic, enable your Microsoft® Exchange tracking logs.
Multiple Microsoft® Exchange Servers	On the same side of each server as your Internet gateway to capture external email traffic



Multiple Domains	One computer running <i>Sentinel</i> in each domain. Follow the points above to work out the optimum installation point for each domain.
A computer with two network cards acting as my Internet gateway	On the Internet gateway itself if the gateway is a computer running Microsoft® Windows

Connecting Sentinel to the Optimum Installation Point

Once you have determined where to install *WebSpy Sentinel*, you will have to determine how to connect the computer running *Sentinel* to that point. See Table 2 below for instructions. The different installation points are graphically displayed in the Diagrams section of the document.

Table 2 - Connecting Sentinel to the Optimum Installation Point

My Optimum Installation Point is...	Install Sentinel Service...
A hub	On any computer connected to that hub that has all of the internet traffic passing through it
A managed switch	On a computer attached to the switch's monitoring port
An unmanaged switch	On a computer connected to a hub connecting the unmanaged switch and the Internet gateway OR On a computer connected to the monitoring port of a managed switch connecting the unmanaged switch and the Internet gateway OR On the Internet gateway itself if the gateway is a computer running Microsoft® Windows OR On each computer connected to the switch
A network cable	By replacing the single cable with two cables and a device (hub, managed switch or computer with two network cards) between them. You can then install <i>Sentinel</i> in a position appropriate for the connecting device (see above).

Definitions

Domain Controller

A domain controller is the computer that logs users on to domain accounts in a Windows NT® Server domain. The primary domain controller keeps track of any changes to the domain accounts, and will log users on to domain accounts. By default, *Sentinel* uses the primary domain controller to resolve user names. A backup domain controller is kept up to date with changes by the primary domain controller, and can be used to provide the information *Sentinel* needs, if the primary domain controller is not available.

Firewall

A system of hardware and/or software designed to prevent unauthorized [access](#) to or from a private network. All items entering or leaving your network have to pass through the firewall, which examines each item and blocks those that do not meet its specified [security](#) criteria. Firewalls are a form of Gateway.

Gateway (Internet)

A gateway is a combination of hardware and software that links two different types of networks. Internet gateways connect an organization's LAN to the Internet. It is therefore important that *Sentinel* is installed on the inside of a Gateway.

Hub

A hub is a common connection point for devices in a network. Hubs are commonly used to connect segments of a LAN. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets. Therefore, if Internet traffic is going through a hub and *Sentinel* is installed onto the hub, *Sentinel* will see the traffic.

LAN

A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may serve as few as two or three users (for example, in a home network) or many thousands of users (for example, in a large corporation).

Mail

For *WebSpy Sentinel's* purposes, this is Internet traffic received via SMTP (Simple Mail Transfer Protocol), not POP3 or IMAP. SMTP is a TCP/IP protocol used in sending and receiving e-mail. POP3 or IMAP are protocols that let the user save messages in a server mailbox and download them periodically from the server. Users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving messages that have been stored for them at their local server.

Newsgroups

A newsgroup is a discussion about a particular subject consisting of e-mails or notes written to a central Internet site and redistributed through Usenet, a worldwide network of news discussion groups. The protocol used is Network News Transfer Protocol (NNTP).

Packet

A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file (e-mail message, HTML file, GIF file, URL request, and so forth) is sent from one place to

another on the Internet, the file is divided into "chunks" or packets of a suitable size for efficient routing. Each of these packets is separately numbered and includes the Internet address of the destination.

Protocol

A protocol is a special set of rules or conventions for communication between two computers, both of which must recognize and observe the protocol. Different types of Internet traffic use different protocols. Protocols are often described in an industry or international standard.

Switch/Managed Switch

A switch is a network device that selects a path or circuit for sending a unit of data to its next destination.

Telnet

Telnet enables you to access another computer across the Internet, assuming they have given you permission. Such a computer is known as a 'host' computer. With Telnet, you log on as a regular user with whatever privileges you may have been granted to the specific application on that computer.

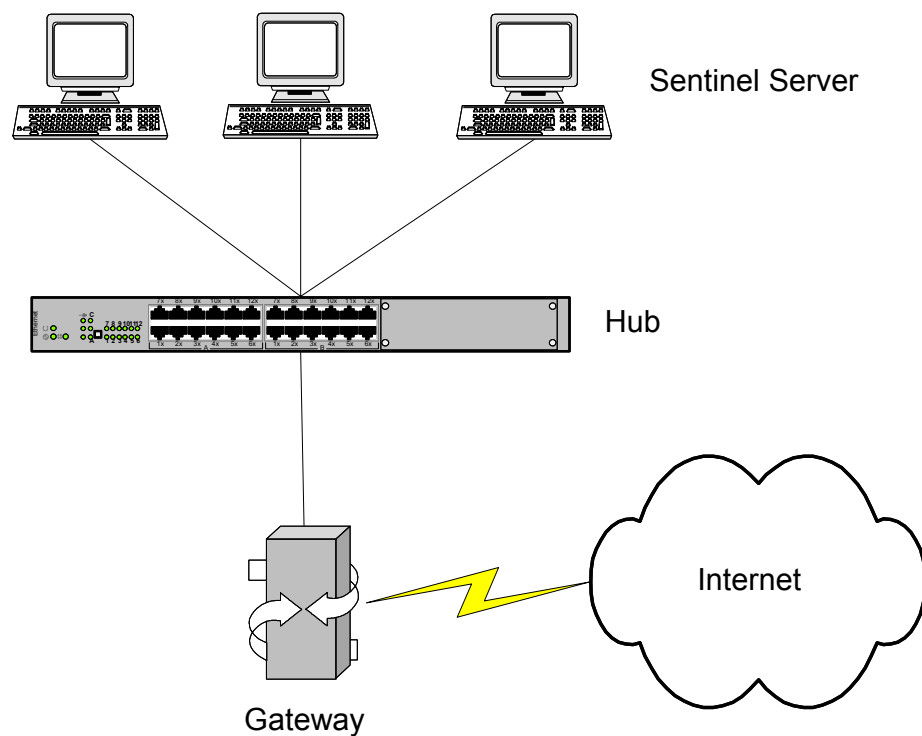
Web

For *WebSpy Sentinel's* purposes, this is any Internet traffic received via HTTP (Hypertext Transfer Protocol). HTTP is the set of rules for exchanging files (text, graphics, sound, video, and other multimedia files) on the World Wide Web (WWW).

Network Diagrams

Case Study One

Hub Installation

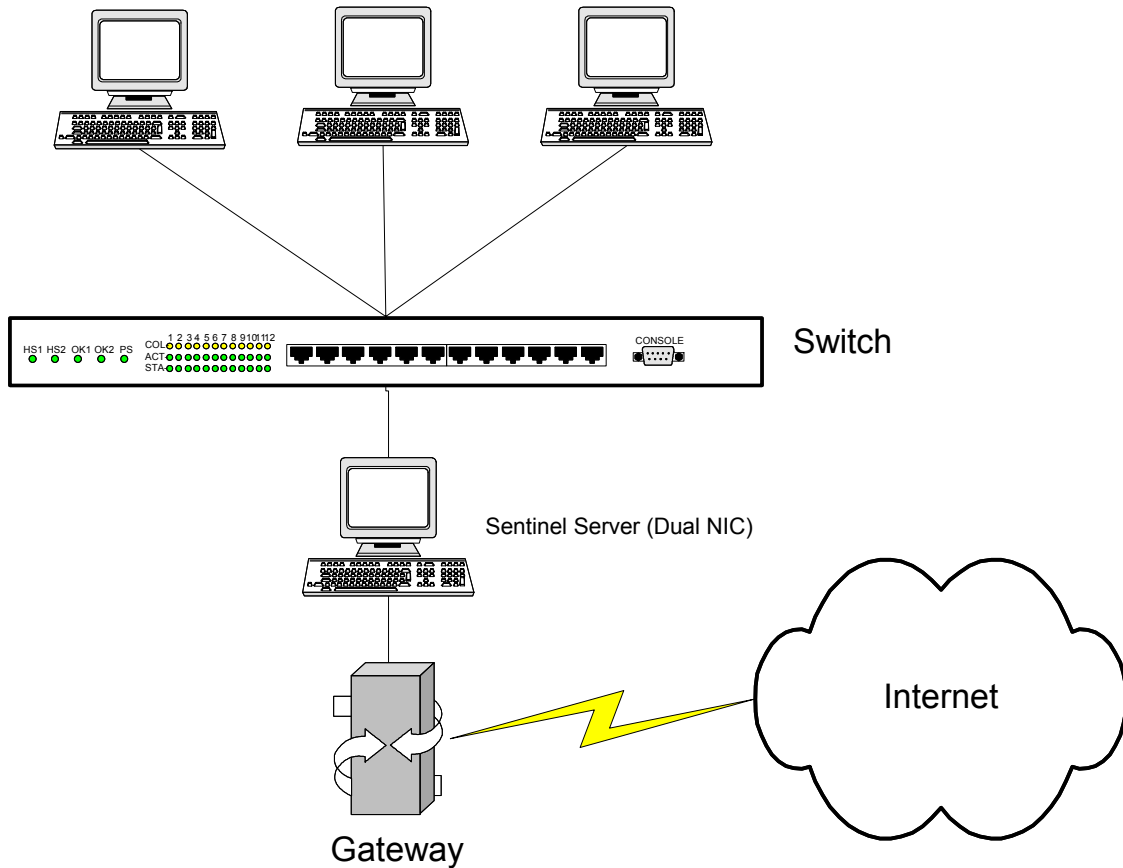


Sentinel can be installed on any computer connected to a hub, whether a workstation or a gateway or firewall.

If *Sentinel* is installed on the gateway or firewall, please make sure that it is monitoring the internal network card and not the external network card.

Case Study Two

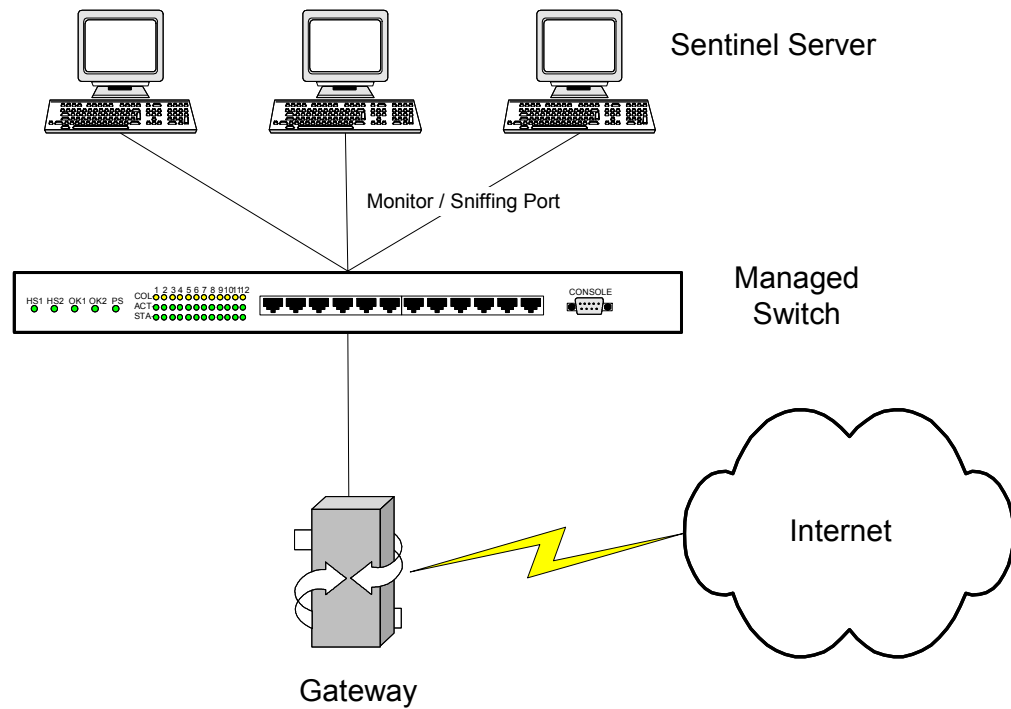
Unmanaged Switch



None of these computers can listen to the others' traffic because of the switch, and since it is an unmanaged switch, no monitoring port is available. Therefore, *WebSpy Sentinel* must be installed on either the existing gateway or on an additional computer with dual network cards. Alternatively, see Case Study Six on page 18 for another way of managing this situation.

Case Study Three

Managed Switch 'monitoring port'

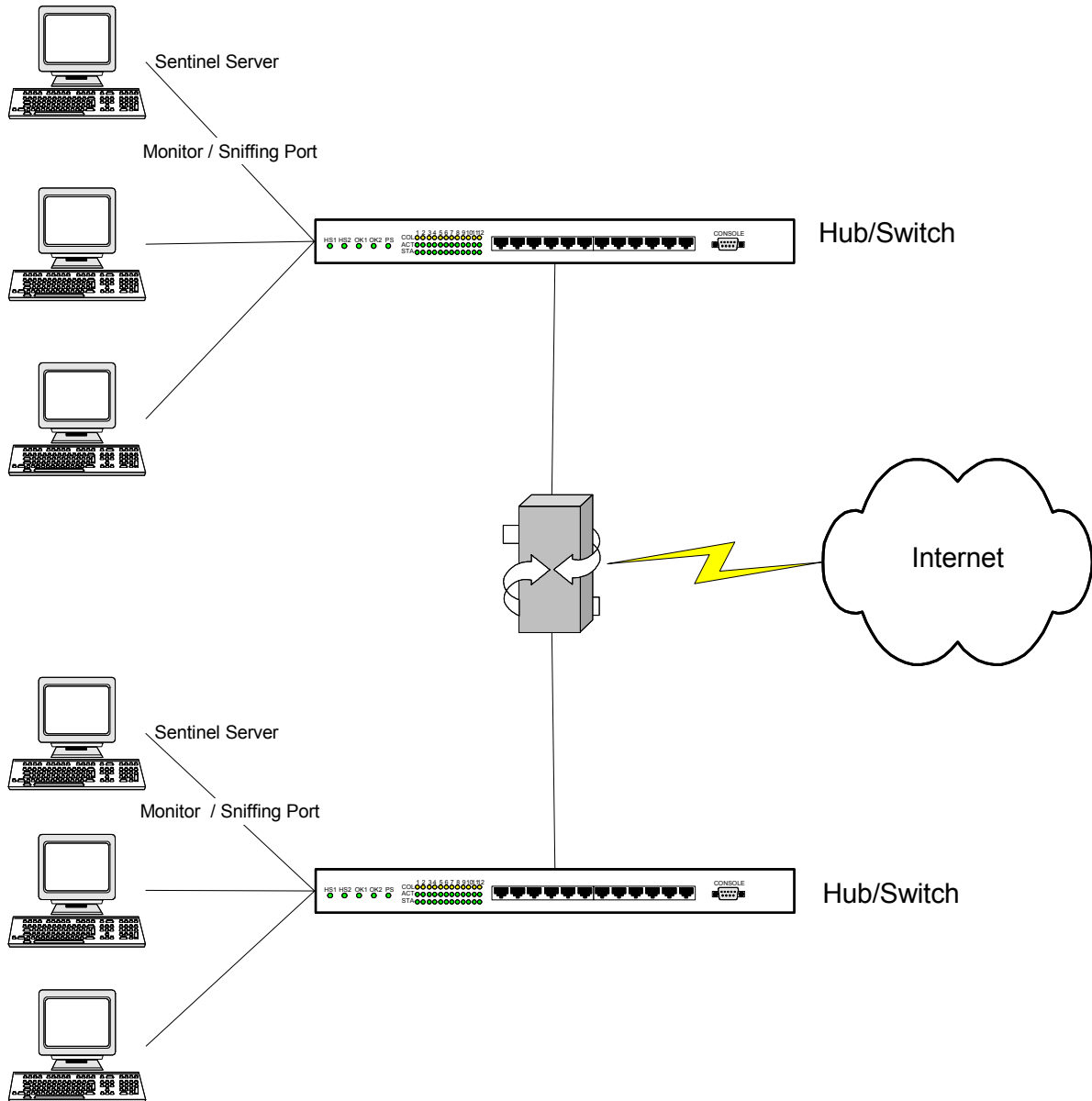


A hub is effectively a broadcaster of information while a switch directs information directly to the port that the information is intended for. Some switches (managed switch) have what is known as a monitoring port. This can 'listen' to all the other ports on the switch if it is enabled.

Alternatively, see Case Study Six on page 18 for another way of managing this situation.

Case Study Four

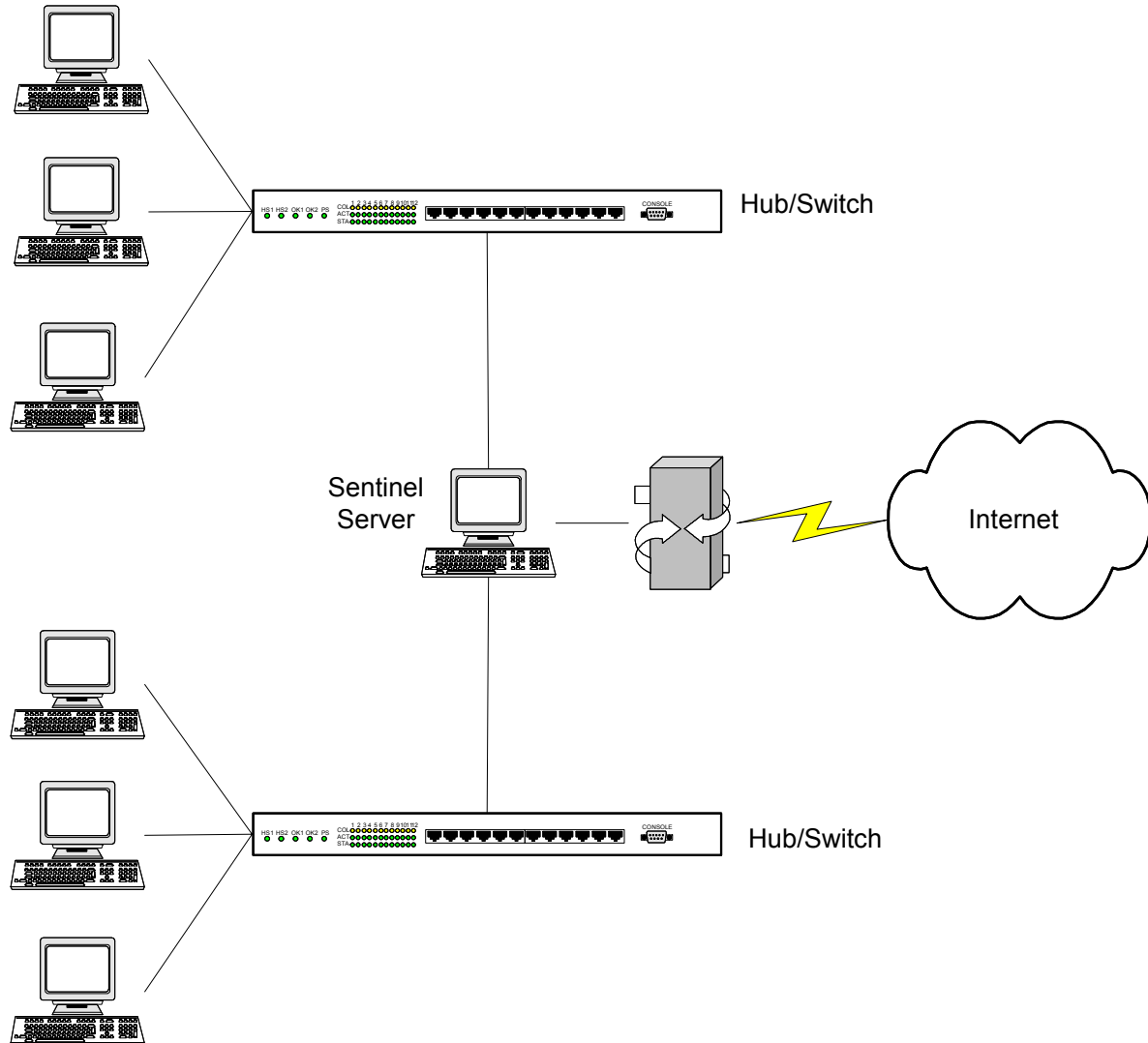
Multiple Subnets



When working with multiple subnets, you can place a Sentinel Server on each subnet to capture that subnet's data. This will also distribute the load between the servers and will provide more efficient data capture.

Case Study Five

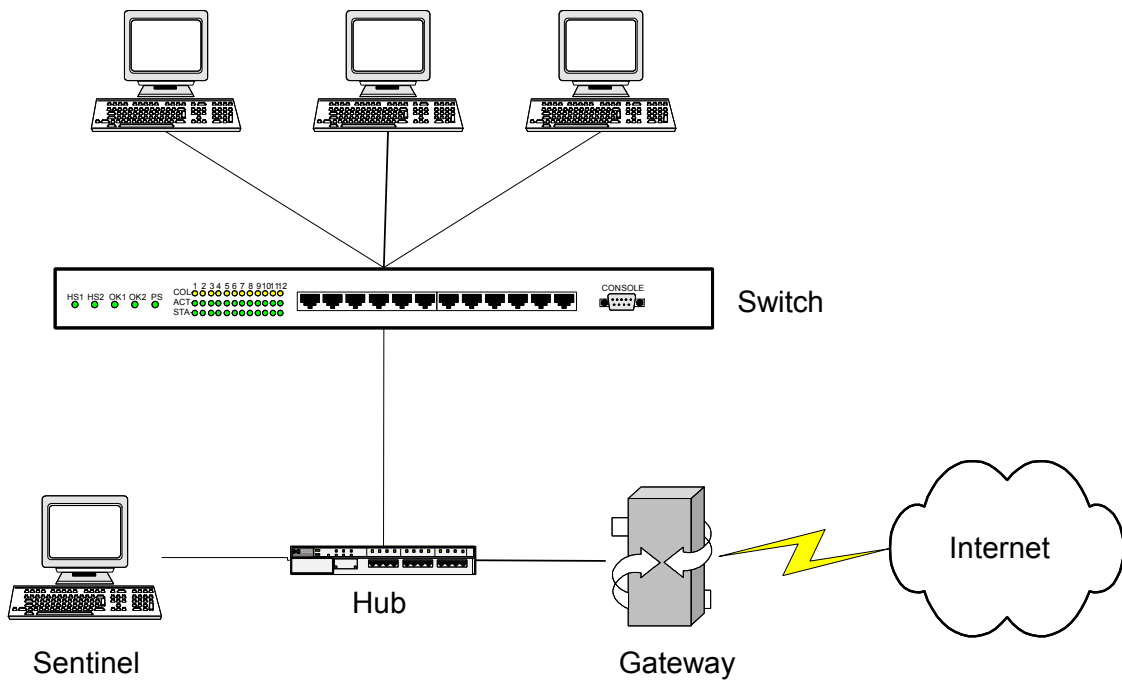
Multiple Subnets – Gateway Solution



When working with multiple subnets you can also place a Sentinel Server in front of the gateway to capture your entire organization's traffic. This is the best solution if you have unmanaged switches, or if you don't want a Sentinel Server on each subnet.

Case Study Six

Hub and Gateway Solution



This solution will prove effective when you can't install *Sentinel* onto your gateway. This may be because you are running Unix, Linux or a hardware device. The installation point will allow all traffic that is entering or exiting your network to be captured by the Sentinel Server.