CHAPTER 6

Using Cisco Centri Firewall to Protect Your Network

Introduction

To use Cisco Centri Firewall, you must determine what assets you want to protect, who you are protecting those assets from, who can access them, how they can be accessed, and who can change the rules about accessing them. In addition, you need to determine what information you want to know about your network's activity and what to do and who to notify if someone attacks your assets. The basic install and configuration process involves seven tasks:

1. Define your administrative accounts.
2. Set up your network objects.
3. Define your network services.
4. Define your user authentication policies.
5. Define your security policies.
6. Apply your security policies.
7. Set up reporting and monitoring.

This chapter provides an overview of these seven tasks and provides information to help you plan the deployment of your Cisco Centri Firewall, as well as worksheets for collecting and organizing the information about your network that you will need to know when configuring Cisco Centri Firewall. Detailed procedures for performing these tasks are provided in the HTML Reference documentation that is installed with the security system.

Define Administrative Accounts

You must define at least one administrative account for Cisco Centri Firewall to allow privileged users to administer the security system. In addition, you must specify which Windows NT user account should be used to install Cisco Centri Firewall. This user account must have administrative privileges because the Cisco Centri Firewall must be able to run its services with administrative or system-level privileges.

During the install process, you can choose to rename the Administrator account provided by Windows NT and use this account to install the product. The advantage of not using an existing account name, such as Administrator, is that these account names are common to all multi-user operating systems, and therefore, they are more vulnerable to password attacks—perpetrators already know the account name. Therefore, all they have to guess is the password. By renaming the provided account, you take the common knowledge away from perpetrators who do not know what firewall software you are using.

Note You should not present information about what operating system or firewall software you are using to any users. For example, in the Welcome and Deny messages associated with the different network services, you should only include the information that the user needs to understand and take appropriate actions, such as “Welcome to Cisco Systems, Inc.” or “You do not have permission to access this service.”

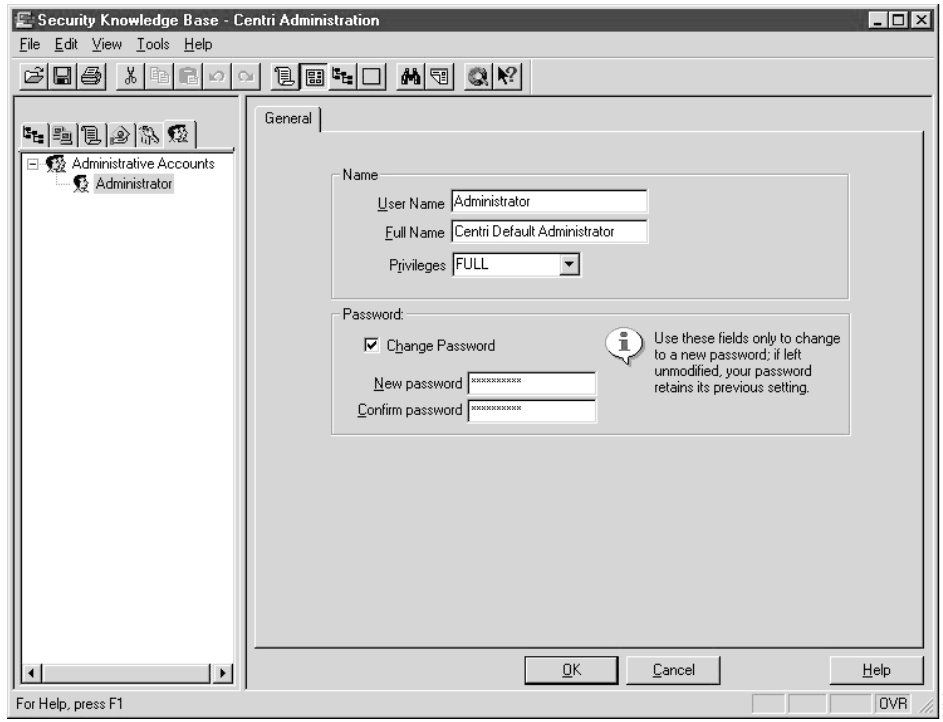
The less information that you openly provide about your network, the better off you are. Many networks have been compromised by widely advertised bugs in operating systems and applications. When an attacker sees that you are running a particular version of a particular operating system or firewall software that is known to contain bugs, the more likely that attacker is to penetrate your network successfully.

Built-in user accounts, such as Administrator and Guest, are common avenues for attack. You should rename or disable any such accounts on your firewall server.

During the installation process, you will be prompted to define your default administrative account for Cisco Centri Firewall. Once you install the product, you must consider additional accounts for administrators who need to administer the firewall from remote workstations (see Figure 6-1). To set up administrative accounts for Centri Firewall, you

must determine who can administer your firewall server and from what computers on your network they can administer it. This process defines the remote administration privileges and user accounts.

Figure 6-1 Administrative Accounts for Cisco Centri Firewall



Note In Cisco Centri Firewall, you can define additional administrative accounts, as well as select which remote computers can be used to access that account. The remote computers must have the Remote Administrative Interface installed.

Set up Your Network

Once you have installed Cisco Centri Firewall, you need to set up your network by identifying the network objects that you want to protect, and possibly, those network objects that exist on untrusted networks that you want to allow your users to access while adhering to specific security policies.

Within Cisco Centri Firewall, trusted network objects are placed under the Network tree. Two types of trusted networks exist: physical networks and logical networks.

Physical networks represent the topological layout of your network, such as sites, routers, Windows NT domain controllers that contain Group and User account databases to which you want to assign security policies, and any computers that are on the perimeter network. By associating a physical network with a trusted or untrusted site, you can delineate proper routing rules for your network.

Logical networks organize network objects into logical groups that are meaningful to the administrator. Logical network definitions are used to apply security policies to network objects in a way that makes sense to you. You can use them to mimic your organizational structure or other schemes that you use when considering your network, such as domains.

As with trusted network objects, untrusted network objects can also exist within physical or logical networks. These network objects are defined under *The Internet* icon within the Network tree. By itself, *The Internet* icon represents all unknown networks and network objects. If you define untrusted network objects below *The Internet*, you are identifying those networks that you know something about. By defining such untrusted networks, you can apply security policies to those network objects that handle special communication cases, such as preventing communications from those networks to your trusted networks or only allowing through specific network services.

Define Physical Relationships of Your Network

The physical relationships that you must define during the install process instruct the Cisco Centri Firewall about the proper flow of network traffic across the firewall server. The relationships include whether to hide or expose the internal site addresses (basic rules for network address translation) and what internal network servers you want to share with external network users. The physical relationships also define many physical characteristics of your network, such as:

- which subnetworks exist on your network;

- the network addresses of the routers on your DMZ and internal networks;
- which of your installed network adapter cards are trusted and which are not;
- what sites are applied to which network adapter cards; and
- the routing rules that define secondary paths in the event of network device failures or overload.

By defining the physical relationships of your network, you can do more than define routing rules—you can define Windows NT domain controllers that allow you to apply security policies to the Group and User accounts within the user account databases on those domain controllers.

The Windows NT domain model is a logical model, but first Cisco Centri Firewall must be a member of one of the trusted domains on your network, and the trust relationship of your domains must ensure that the Cisco Centri Firewall can access the user account databases stored on them. By following the Windows NT domain model, you can take advantage of on-the-fly authentication for all network services by using the Windows NT authentication model.

The Windows NT authentication model provides several benefits:

- allows administrators to apply security policies to users rather than IP addresses, which eases the administration of environments that use DHCP to dynamically assign IP addresses to network objects;
- users can access all network services provided by the firewall server transparently; and
- security policies applied to users follow them from computer to computer as long as the computer is a client of the Windows NT domain controller.

Note Using the Windows NT authentication may require that you configure your internal routers to allow the Windows NT authentication traffic through the router so that the firewall server can perform lookups.

Defining the physical relationships involves three basic tasks:

- configuring the Centri Server;

- configuring the Centri Firewall; and
- defining the physical network objects, including routers, Windows NT domain controllers, and computers on the perimeter networks.

The next section discusses how you can use logical relationships to simplify the administration of your network.

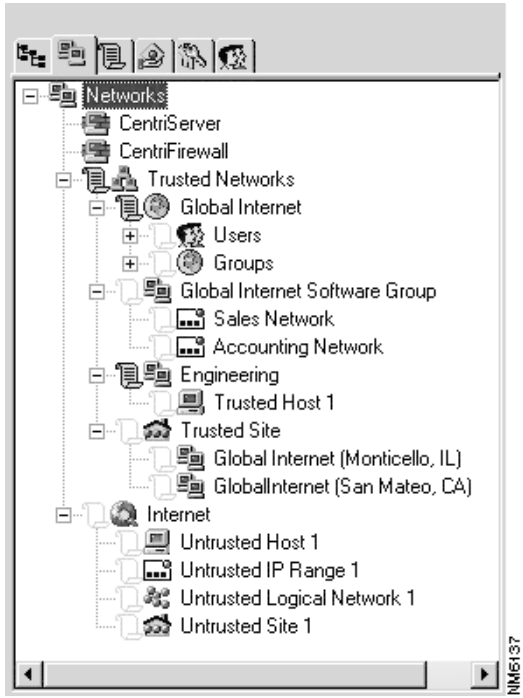
Define Logical Relationships of Your Network

The logical relationships of your network allow you to administer it more efficiently, without worrying about the physical layout of your network. By defining logical network objects, you can group network objects that reside behind routers, as well as apply specific security polices to users and hosts that do not run Windows NT client operating systems (Windows NT Workstation, Windows 95, and Windows for Workgroups 3.x).

With physical network objects, you are more concerned about communicating with the first line of network objects, such as routers, to ensure that the firewall server directs traffic correctly. With logical network objects, your focus is on how you want to view and administer the network objects for the purpose of simplifying security policy deployment (see Figure 6-2). You can provide as much or as little detail about your network as needed to administer it in the manner that your security policy dictates.

For example, if you had a homogenous UNIX environment connected to your firewall server (either trusted or untrusted), you could mimic the domain model in which you commonly administer the UNIX workstations. You could represent this domain model as entire domains using subnetwork and IP address ranges, or you could represent the domains populated with every workstation within that domain. These two examples would allow you to apply security policies on a domain-only, a domain-workstation combination, or a workstation-only basis.

Figure 6-2 Network Objects



Note You can apply security polices to network objects that are trusted or untrusted and logical or physical, as well as Windows NT Domains and Group and User accounts.

In addition, you could define user authentication requirements for each of these network objects to comply with corporate policy. If you are more comfortable with usernames, you can identify specific computers or networks using the names of your users or departments within your organization instead of using hostnames and domain names.

Logical networks provide the advantage of being easier to learn, making it easier to share the responsibility of administering the firewall server. In addition, they provide a simple way to define rules for a specific user or computer and can be easily updated to reflect

organizational changes. Configurations based on subnetworks and IP address ranges also can enforce security policies on a per instance basis for new network objects that fall within the defined ranges. As you add new network objects that fall within a range, any security policies that are already applied to that range automatically apply to the new objects as well.

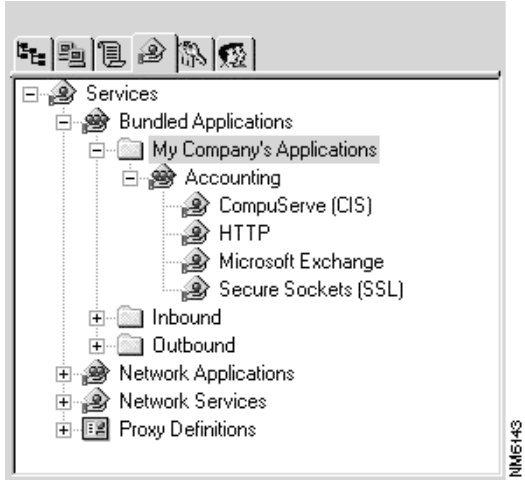
Once you determine the organizational model by which you want to administer your network, you must define the logical network objects and groups that reflect that model to the level of detail that you require.

Define Your Network Services

How you go about defining your network services depends on your site requirements. You can simply modify the network services and network applications in Bundled Applications to correspond with what you want to allow your network users to access, or you can define your own Bundled Applications, Network Applications, and Network Services.

To define new services so, simply select the network services and applications that you want to allow on your network and organized them into meaningful Bundled Applications (see Figure 6-3). Using Bundled Applications, you can organize network services and applications into a higher level object that you can reference in your security policies as a single entity.

Figure 6-3 Bundled Applications



If the network services and network applications provided with the Cisco Centri Firewall do not fit your needs, you can also use the New Service Wizard to define new network services that you can also include in your custom Bundled Applications. To access this wizard, select the Network Services branch within the Services tree. On the shortcut menu (accessed using the right-mouse button), click the **Service Wizard** option from the New option (see Figure 6-4).

The network services wizard walks you through the process of defining a new network service based on the kernel proxies that compose the dynamic stack that will be used to evaluate sessions for that network service.

Figure 6-4 Network Service Wizard Menu Option

The last step required to set up your network services is to define the rules for HTTP filtering. Like other value-added services, such as ActiveX and Java filtering, you can specify the enforcement of these filtering rules on a per instance basis within security policies. Centri Firewall provides the ability to control which Internet sites are accessible to the users on your private network, as well as prevent access to specific types of files. To specify rules for the HTTP filtering service, select the Centri Server node under the Networks tree.

Define Your User Authentication Policies

You can configure the FTP, Telnet, and HTTP network services to authorize specific external users to access your network. However, this open-ended access poses a threat to your network's security because malicious external users often attempt to penetrate a company's firewall by copying an authorized external user's transactions and then masquerading as that user. You can prevent this kind of attack by requiring authorized external users to prove that they are who they say they are before granting them access to your network. Cisco Centri Firewall's user authentication policies provide a means of enforcing this proof concept.

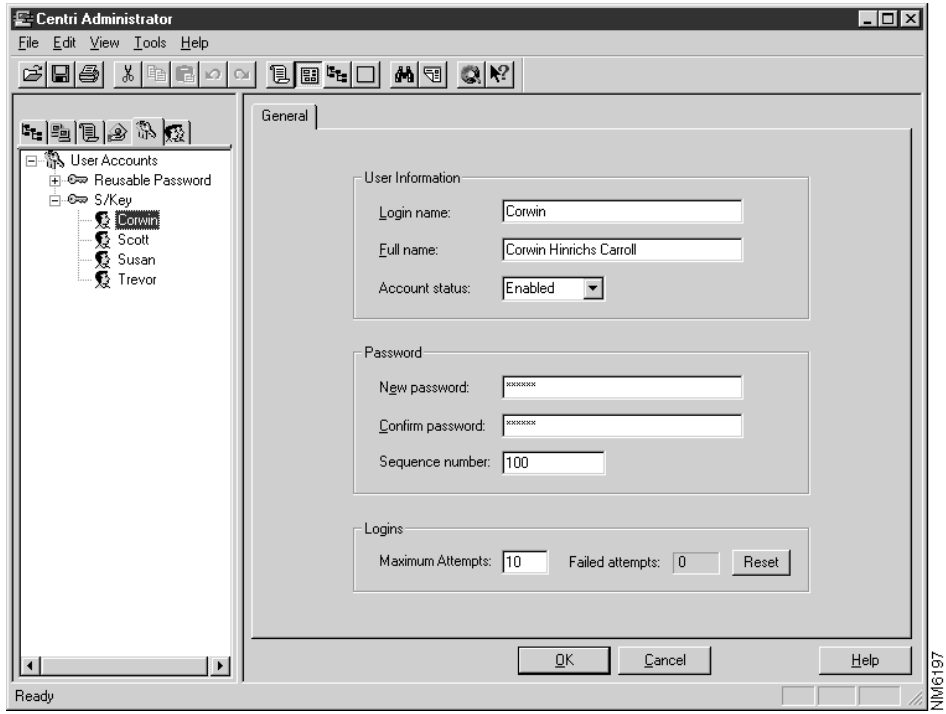
To define your user authentication policies, you must first determine whether you are going to require user authentication and if so, you must select the form of user authentication that you want to use: S/Key or reusable passwords. Once you have determined the need and authentication method, you must gather the information required by your users to authenticate themselves. Table 6-1 identifies the information that you will need to gather depending on which authentication method you choose.

Table 6-1 Required User Authentication Information

Authentication Field	Description
Username	Identifies the account name that your network user will enter in conjunction with a password to authenticate himself to the firewall server.
Full Name	Identifies the user's full name. This information helps you identify exactly who owns a particular user account.
Status	Specifies whether the user account is enabled or disabled. Using this feature, you can define user accounts in advance and only enable them when the user requires access to the firewall server. This level of control reduces the risk of attackers compromising the user account.
Passwords	Identifies the passwords that your network user will enter in conjunction with a user account to authenticate himself to the firewall server.
Sequence Number	This option is used exclusively by the S/Key authentication method. It specifies how many times a user can log into the firewall server before the user account/password list must be updated. This number decrements each time the user logs in, and when it reaches zero, the account is automatically disabled by the firewall server.
Maximum Attempts	Identifies the maximum number of attempts that a user can consecutively fail to log into this account before it is automatically disabled. You must reset disabled accounts manually.

The last step of this task is to define the user accounts within the User Authentication tree of the Cisco Centri Firewall user interface. From within the User Accounts tree, you can define both reusable- and S/Key-based user authentication accounts. Once these accounts are defined, you can require that your network users authenticate themselves to the firewall server before accessing the HTTP, FTP, or Telnet services.User Authentication Methods.

Figure 6-5 User Authentication Methods



Define Your Security Policies

Because many network services and applications perform bi-directional communications (both the client and server can initiate a session), you must define two types of security polices:

- Security policies that restrict and protect outbound communications from your trusted networks behind the firewall server.
- Security policies that restrict and protect inbound traffic from the untrusted and unknown networks that are external to the networks that you administer.

Outbound security policies specify which users and services, such as FTP and e-mail servers, on your trusted networks can communicate with users and services that reside on untrusted and unknown networks. Inbound security policies specify which users and services can communicate with the users and services that reside on your trusted networks.

For example, if you want your users to be able to send and deliver e-mail to users who reside on untrusted and unknown networks, you must specify an inbound security policy that allows SMTP-based messages (or a similar mail service) to reach your internal mail server. In addition, you must specify an outbound security policy that allows your internal mail server to deliver SMTP-based messages out to untrusted and unknown networks.

When defining your security polices, you must determine which network services, applications, and bundles you want to allow your logical network objects to access. You must also specify any run-time session controls that you want applied to specific network services, such as user authentication, ActiveX and Java filtering, and time-of-day access restrictions.

Apply Security Policies to Network Objects

To enable bi-directional communication, you must apply the security polices to the appropriate network objects. To enable inbound communications, you must apply security policies that enable the allowed network services to the Internet branch or any children nodes that you have defined below it. By doing so, you are allowing network objects that are external to your network to communicate with internal network objects on your internal trusted networks.

To allow outbound communications, you simply apply the security policies that you defined for outbound communications to the logical network objects that you defined within the Trusted Networks branch of the Networks tree. Thus, you are allowing your internal network objects to use the specified network services and applications to communicate with external network objects.

Set up Reporting and Monitoring

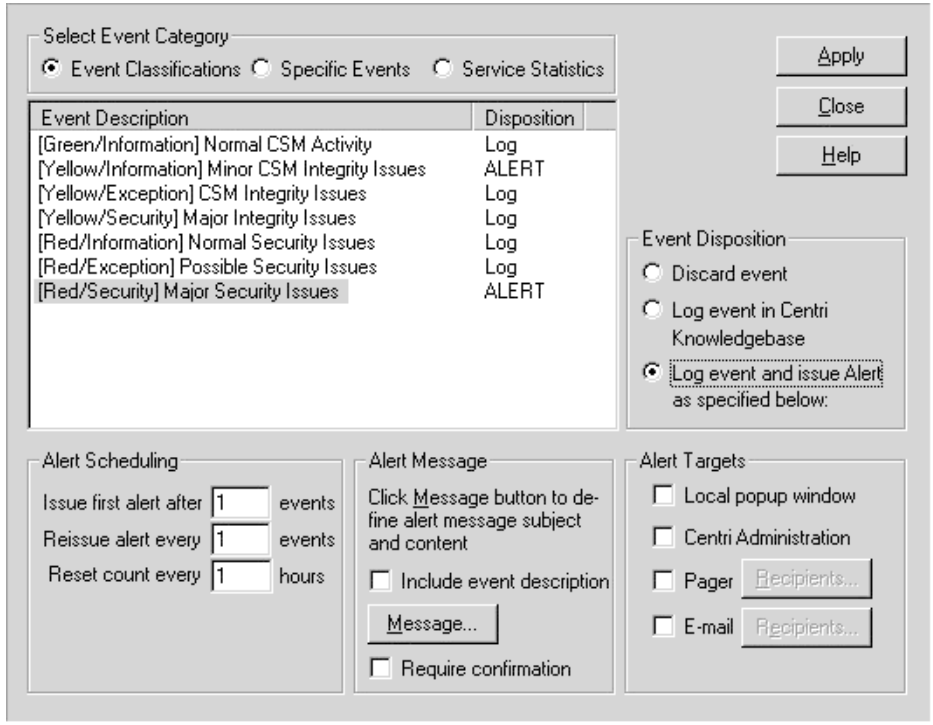
Within Cisco Centri Firewall, reporting and monitoring are closely related because the information that is processed for reports and evaluated by the monitoring system is dependent upon the events that you decide to store in the Security Knowledge Base. Two concepts are central to both of these subsystems: audit events and event filtering.

Audit events generate audit records that explain what is happening within the security system. All components and agents within the security system have assigned audit events, and the audit records that these events generate provide the information that is used to generate reports and administrator notifications.

Event filtering determines whether a specific event will be stored in the audit records of the Security Knowledge Base and whether an administrator will be notified. It provides the ability to filter out audit records that you do not want to permanently store in the Security Knowledge Base. Thus, event filtering is based on what the administrator believes is important to monitor. Some administrators want to study detailed reports describing every audit event that occurred within the security system, while others are more interested in specific information about how the security system is operating.

The first step in setting up your reporting and monitoring is to determine which audit events you want to generate records for and how and when you want to notify someone on your staff if a particular audit event occurs. By doing so, you are defining the monitoring settings.

Figure 6-6 Generating Audit Records



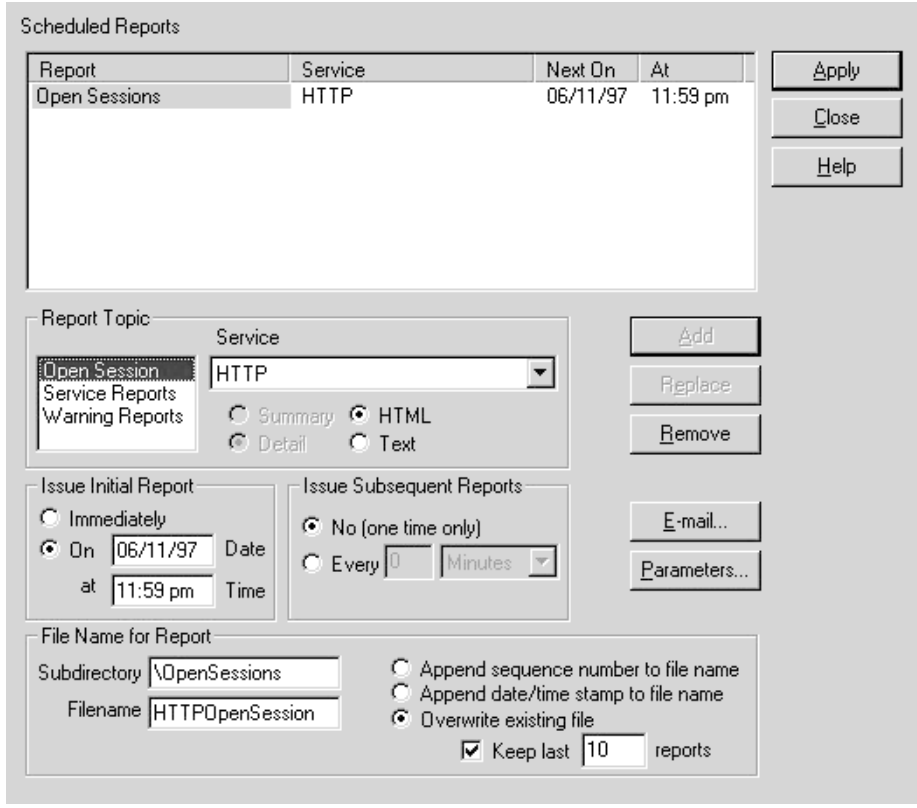
Note Cisco Centri Firewall's ability to provide detailed and interesting reports as well as to notify administrators of suspicious network activity and possible problems in the state of the firewall server is largely a result of what audit events an administrator chooses to have the system evaluate.

Because the Reporting Subsystem provides statistical and summary information about the audit events that occurs, how you define your monitoring settings affects the details of the many reports that you can generate about the operation of the security system or a specific network service. Once you have defined the monitoring settings, you can specify which

reports you want to generate on a periodic basis. At any time, you can generate a report on-demand; however, scheduled reports can provide timely information about the security system or a specific network service. For example, you can schedule reports that provide a summary of the network traffic activity once every minute, hour, day, week, month, year, or any number of these periods. You can schedule three basic categories of reports:

- **Statistical/Summary Reports.** Provides summary statistical information about the activity of a specific network service.
- **Detailed Reports.** Provides detailed information about the activity of a specific network service.
- **Warning Reports.** Provides information about the state of the Cisco Centri Firewall.

Figure 6-7 Scheduling Statistical and Summary Reports



Note The Administrative agent allows administrators to stay abreast of the state of the security system and the network usage statistics by allowing them to define the rules for on-demand and scheduled reports.

The last section of this chapter provides worksheets to help you organize and record information you will need as you configure Cisco Centri Firewall.

Worksheets

This section provides worksheets to help you configure Cisco Centri Firewall, as well as to plan and maintain your network security policy. We encourage you to copy these worksheets and to fill them out before you install and begin configuring Cisco Centri Firewall. The following worksheets are provided:

- **Identifying Your Organization's Assets.** This worksheet helps you identify the location of information and its value to your organization. Collecting this information helps you create custom security policies that strictly protect your network's assets.
- **Identifying Your User's Needs.** This worksheet helps you identify what network services your users need. Collecting this information helps you ensure that your users can perform their jobs securely, without loss of productivity due to incorrectly configured network services and security policies. In addition, this worksheet can help you develop Application Bundles by identifying common user needs.
- **Access Summary By Network Object.** This worksheet allows you to organize the information collected on the previous worksheet by network object and to map each network object to a human readable name that you can use in the Cisco Centri Firewall user interface. By completing this worksheet, you have a single reference from which you can define your network security policies to ensure that you provide the requisite security and access for each network object.

Table 6-2 Worksheet 1. Identifying Your Organization's Assets

	Types of Data and Consequences of Data Loss or Theft				
Logical Network Object[1]	**Highly Sensitive**[2]	**Sensitive**[3]	**Mildly Sensitive**[4]	**Internal Use**[5]	**Public Access**[6]

1 List divisions, departments, groups, or other organizational objects. Categorize the type of data deriving from each object and adjust the security policy for that entity/data accordingly.

2 The loss or theft of this type of data would be severely detrimental to the organization. You should protect this data with the strictest security policies.

3 The loss or theft of this type of data would be detrimental to the organization. You should protect this data with fairly strict security policies.

4 The loss or theft of this type of data would not be detrimental but could potentially cause minor harm to the organization. You should protect this data with a reasonable security policy.

5 The loss or theft of this type of data would cause no harm to the organization. You should protect this data with a loose security policy.

6 This type of data is meant for general public access. You do not have to protect this data.

Table 6-3 **Worksheet 2. Identifying Your Users' Needs**

IP Address	User/ Department	Importance (High/Low)	Network Applications	Network Services Required

Table 6-4 Worksheet 3. Access Summary By Network Object

	Network Object			
IP Address	Object Name	Importance (Low/High)	Notes	Type of Access Granted