

Chapter

1

Getting Started with FireSIGHT



COPYRIGHTED MATERIAL



Let's begin our journey into the world of FireSIGHT by building a solid foundation in defining key, industry-wide, and Cisco-specific terms that we'll be using throughout this book.

We'll also introduce a variety of FireSIGHT appliance models and talk about licensing and network design.

We'll move on to tour the web-based user interface and describe Cisco FireSIGHT policy-based management; then we'll wrap the chapter up by guiding you through the new appliance initial setup process.

Industry Terminology

Let's get started by covering some important industry-wide terms that mean the same thing to Cisco as they do to the rest of the world. You're probably familiar with some of these, but they're vital for a well-built knowledge base, so make sure you thoroughly understand them all!

Firewall Traditional firewalls work at the network/transport layer by allowing or blocking traffic based on criteria such as an IP address and/or port. Much more than a router with an access list, a firewall offers us lots of more advanced features—for example, the capacity to ensure that only packets associated with a stateful connection are allowed to pass through.

Intrusion Prevention System or Intrusion Protection System (IPS) An IPS is a device inserted between other network components in an inline configuration. This placement forces packets to pass through the IPS, enabling it to block any traffic deemed malicious. But what equips an IPS to make that kind of judgment call? Well, an IPS is capable of *deep packet inspection*, meaning it inspects the data portion of the packets, not just packet headers. Also, most IPS systems use *rules* or *signatures*—which look for specific conditions in packets—to identify known malicious behavior. When traffic matching the signature arrives, the IPS can generate an alert, drop the offending packet(s), or both.

Intrusion Detection System (IDS) An IDS is similar to the IPS we just talked about, but instead of being deployed inline, it's connected passively via a *network tap* or a switch's span port. The traffic that the IDS examines is actually a copy of the packets, which traverse the network. Even though the detection capabilities of an IDS are identical to those of an IPS, an IDS can't actively block traffic it considers suspect—it can only alert us to it.

Next-Generation IPS (NGIPS) An NGIPS device provides all the traditional IPS features but packs additional powers like the ability to allow/block traffic based on specific application or user information. This expanded level of control provides more flexibility in restraining

specific applications, regardless of their IP address or port. An NGIPS also gives you control over exactly who can or cannot access applications like your favorite social media site.

Next-Generation Firewall (NGFW) This device offers all the usual features that a classic firewall does, but it adds the application/user control features of an NGIPS into the mix, arming you with a firewall and NGIPS in one package!

Practically speaking, the line between an NGIPS and an NGFW is pretty fine. The main difference is the particular network layer where the two devices run. NGIPS typically operates as a “bump in the wire,” meaning packets that enter on one interface of an inline interface pair always exit the other interface. The device doesn’t have IP addresses assigned to the detection interfaces and it doesn’t build a *CAM table* of MAC addresses either. It simply inspects packets on their way through.

Alternatively, the NGFW performs the role of a traditional firewall and adds NGIPS features. Interfaces have IP addresses assigned and the device performs Layer 3 routing of traffic.

Cisco Terminology

At this writing, Cisco is in the midst of a branding transition. Following the acquisition of Sourcefire in late 2013, Cisco retained the Sourcefire name across much of its NGIPS/NGFW product line. It was basically business as usual, with the models and product names remaining unchanged as the integration between the two companies progressed. But beginning in late 2014, the names of the various components started changing, effectively removing the Sourcefire moniker. However, given that familiar terms tend to linger, it is likely that legacy names will continue to be used for some time. The more years someone has spent using the Sourcefire IPS legacy names, the greater the odds these experienced individuals will continue to do so—if only colloquially. This means you should definitely be fluent in both the legacy and new terms to work effectively with everyone in the brave new world of Cisco FireSIGHT.

So, let’s take some time now to discuss these changes and equip you with a keen ability to clearly navigate the sea of terms you must be familiar with.

FirePOWER and FireSIGHT

In early 2012, Sourcefire introduced version 5 of the *Sourcefire System*. Along with this new version came several new brands, an important one being FirePOWER, which was used to represent the advanced network interface hardware in the latest detection devices. The *Netronome Flow Processor (NFP)* included far more advanced technology than a typical network interface card. And technically, this is still the case—the power behind the detection speed of the system is still FirePOWER. But today this term has changed a bit and is used in conjunction with the Cisco Adaptive Security Appliance (ASA) software. So when you see *FirePOWER*, it’s typically used to describe FirePOWER services on ASA. Furthermore, the term can refer to software services or the FirePOWER blade installed on the ASA 5585-X, which can be a little confusing.

FireSIGHT is another term introduced with version 5. Historically, meaning pre-Cisco, the term *FireSIGHT* referred to the passive detection capabilities of the Sourcefire System. In version 4.x, these capabilities were called Realtime Network Awareness (RNA) and Realtime User Awareness (RUA). When version 5 hit the scene, these two names were rebranded and combined into FireSIGHT. Prior to the Cisco acquisition, FireSIGHT never referred to the entire system. It was all about network and user awareness. These days the term *FireSIGHT* has been expanded to encompass the entire NGIPS/NGFW system—the term *FireSIGHT System* now refers to the new Cisco NGIPS.



While Cisco has expanded the sub-brand FireSIGHT to mean the entire system, this change has not filtered down to the current SSFIPS exam. When you see the term *FireSIGHT* in an exam question, it refers to only the system's network and user awareness capabilities.

A Passive IPS?

Cisco is unlikely to ever refer to the FireSIGHT System as an IDS. The term *IPS* is used almost exclusively throughout the documentation. The FireSIGHT IPS can still be deployed in a passive manner when connected to a passive tap or switch span port, but it's called an IPS.

Out with the Old...

As Cisco's integration of Sourcefire progresses, many of the previous product names are being updated. This is why it's vital to know both the older and newer terms for the various components. Table 1.1 depicts some key terminology changes, including transitional terms.

TABLE 1.1 Old and new terminology

Old	New
Sourcefire	Cisco
Sourcefire Defense Center	FireSIGHT Management Center (FMC or FSMC)
Sensor	Device
Defense Center (DC)	FireSIGHT Management Center
Sourcefire 3D System	FireSIGHT System
Sourcefire Managed Device	Managed Device

The right way to refer to the various components in Table 1.1 lies in the details. For the most part, Sourcefire avoided inner capitalization of words in its brand names. The company name itself depicts this; it's not SourceFire, but rather Sourcefire. Something else you will notice is the capitalization on other terms such as FireSIGHT or FirePOWER; the all uppercase second term is the correct way to write these brands.

How to Look Like a Noob

Spell *Sourcefire* with a capital *F*.

Spell *FireSIGHT* as *FireSight* or *Firesight*.

Appliance Models

Before we dive into talking about the many appliance models available, let's clarify a couple of related definitions.

- *Appliance* is the broad term used for any of the physical or virtual machines that make up the FireSIGHT System. This includes the Defense Center as well as the detection appliances.
- A *device* is a detection appliance. These contain the actual detection interfaces and inspect network traffic. While the Defense Center is an appliance, it is not a device. Some types of policies, such as Access Control, Intrusion Prevention, and Network Discovery, are applied only to devices.

The FireSIGHT IPS is available in a wide range of hardware and virtual appliance models, with the main difference being their bandwidth capacity. IPS throughput ratings range from 50Mbps for the lowly FS7010 up to a whopping 60Gbps for an FS8390 *stack*! It's also important to note that the Defense Center, which provides central management, event storage, correlation, and aggregation, is available in several hardware models and even as a virtual appliance.

As is typical when you're faced with picking out networking equipment, appliance selection is narrowed down by the size of your budget and the amount of bandwidth you need. The good news is that the FireSIGHT System is a really great value in terms of cost per megabit protected. Still, quality rarely comes cheap, and all that protection isn't inexpensive. Fortunately, the wide range of appliance choices helps out tremendously by offering enough options to ensure that you pay only for what you really need.

An important fact you need to remember is that the bandwidth numbers published for each appliance are guidelines based on IPS protection. Adding features such as URL filtering or file malware analysis will reduce this number, but Cisco sales engineers are equipped with sizing guidelines to help you choose the right appliance model based on the features you want.

Hardware vs. Virtual Devices

Now, as we mentioned, FireSIGHT devices come in a number of hardware models as well as a 64-bit virtual appliance. Virtual appliances are supported on VMware ESXi and VMware vCloud Director environments. An important limitation you need to keep in mind is that the virtual appliance can only perform as an NGIPS and not as an NGFW. This limitation exists because capabilities such as VPN, stacking, clustering, and switched and routed interfaces require the specialized silicon found only in hardware devices. Also, unlike hardware devices, the virtual devices do not have a web-based user interface and are accessible only via Secure Shell (SSH).

Device Models

Table 1.2 gives an idea of the various models and their throughputs.

TABLE 1.2 Device models and throughputs

Model	IPS Throughput
Virtual	150–200Mbps per core
7010	50Mbps
7020	100Mbps
7030	250Mbps
7110	500Mbps
7115*	750Mbps
7120	1Gbps
7125*	1.25Gbps
8120	2Gbps
8130	4Gbps
8140	6Gbps
8250	10Gbps
8260**	20Gbps

Model	IPS Throughput
8270**	30Gbps
8290**	40Gbps
8350	15Gbps
8360**	30Gbps
8370**	45Gbps
8390**	60Gbps

*The 7115 and 7125 use SFP interfaces and do not support bypass; these are designed for switch/firewall deployments where bypass is not desired.

**These models are stacked devices.

Defense Center Models

Although the Defense Center is the heart of the FireSIGHT System, it doesn't perform detection itself. Think of it like this: if you consider the devices to be the worker bees in the system, the Defense Center is the queen. Almost all the device configuration is performed from here, and all of the alerting and event logging from the devices is sent to it as well. This means while performing normal day-to-day operations, you only need to log in to the Defense Center's web-based UI.

Also good to know is that if the Defense Center fails for some reason or communication to a device is severed, the devices will continue to perform according to the last instructions they were given. So if they're inline, they will continue to drop traffic based on the last policies applied. However, any alerts generated will be queued on the device until connectivity is restored. Only at that point will the devices forward all queued events, which will then be processed on the revived Defense Center.

You're probably thinking, "How long will the devices queue events if the Defense Center goes down?" Well, it depends. If connectivity is lost, the device will begin to write alerts to its local storage and continue to do so until the local disk is full. How long this takes is determined by the policies applied and the volume of traffic inspected. In the real world, this is typically several weeks or more. So, barring a zombie apocalypse, you should have plenty of time to restore or replace the Defense Center before you lose any events. In the event of said zombie apocalypse, fixing the Defense Center is the least of your worries.

Deciding which Defense Center model to purchase depends on how many devices you'll be managing and what kind of event volume you expect. Taking these factors into consideration, Table 1.3 shows how the different models compare.

TABLE 1.3 Comparing Defense Center models

Model	Max Devices	Hosts/ Users	IPS Event Storage
DC750	10	2,000	30 million
DC1500	35	50,000	50 million
DC3500	150	300,000	150 million
Virtual DC	25	50,000	10 million

Note that new models are also added from time to time, such as the new FS2000 and FS4000 appliances, which begin to leverage the Cisco Unified Computing System (UCS) platform.

FireSIGHT Licensing

The FireSIGHT system has a number of detection and analysis features, and each of the physical device models is capable of performing any or all of them. To enable a specific feature, you must install the appropriate license on the Defense Center; the license can then be assigned to the devices.

And just forget about thinking you can get away with opting for the low-end devices if you want to perform multiple functions such as NGIPS, anti-malware, URL filtering and virtual private network (VPN) functions. While this is theoretically possible, if you actually try this, you're going to end up with some serious performance issues!

Here are descriptions of the different license types available:

FireSIGHT This license is included with the Defense Center and sets the upper limit on the number of IP hosts and users that can be collected. The license count is fixed depending on the DC model and cannot be upgraded.

Protect This is your basic, entry-level license for a device that you have earmarked to become an NGIPS. It enables intrusion detection/prevention, file control, and Security Intelligence filtering.

Control The Control license enables NGFW features like user and application control as well as switched and routed interfaces. This license is also required for clustering or stacking supported devices.

Note that under the new Cisco sales model, the Protect and Control licenses are typically included with any device sale.

URL Filtering URL Filtering enables allowing/blocking websites based on their URL, category, or reputation. Information such as category and business relevance is updated on the Defense Center via a cloud connection.

Advanced Malware Protection Advanced Malware Protection (AMP) provides cloud-based malware lookup and sandbox analysis, including file trajectory and tracking across the network.

VPN The VPN license enables site-to-site VPN capabilities between devices, and it can be used to create a secure tunnel to a remote office location without having to install separate VPN hardware.

Subscription vs. Perpetual Licenses

Each license type is available in a subscription version and a perpetual version. Subscription licenses are valid for a given period of time, and you can buy single or multiple-year licenses. The valid license period is coded into the license key. Once installed, the license key will enable the appropriate feature between the start and expiration dates. Currently, the Malware and URL Filtering licenses fall into this category.

A perpetual license has no begin or end date, and predictably, once installed, this license will enable the appropriate feature indefinitely.

License Dependencies

While licensing is somewhat of an à la carte affair, the license types are not completely independent. Some require installation of a previous license before they can be utilized on a device. Table 1.4 shows the prerequisites for each type.

TABLE 1.4 Prerequisites by license type

License Type	Requires
Protect	N/A
Control	Protect
URL Filtering	Protect
Malware	Protect
VPN	Protect, Control

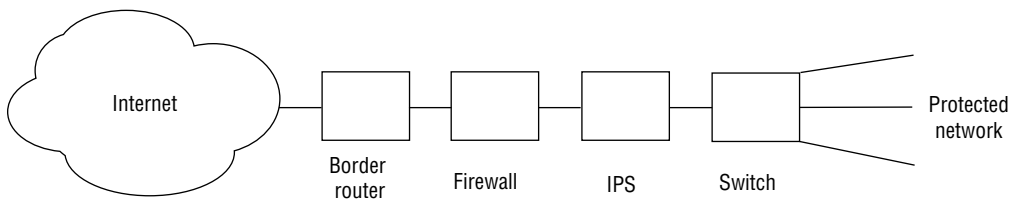
Network Design

Let's take a high-level look at just how you can deploy FireSIGHT within your network. Here we'll talk about and illustrate some simplified network designs to clearly demonstrate ways you can utilize these devices.

Inline IPS

The first design we’re going to cover is probably the most common. The device is installed near the perimeter of the network using an inline interface set. This means packets pass in one interface, are processed by the various policies, and then exit through a second interface. In this type of design, the device acts as the “bump in the wire” we mentioned earlier, which means the other network devices aren’t actually aware of its presence. And remember, the detection interfaces have no IP addresses; the device does not build a Content Addressable Memory (CAM) table to map host MAC addresses to ports. You would expect this if the device operates at Layer 2 like a switch. However, the bump in the wire is more like a Layer 1 (physical) connection between the two inline interfaces. Inline IPS devices are often deployed just inside the Internet firewall or at other strategic choke points in the network. Figure 1.1 illustrates the placement of such a device.

FIGURE 1.1 Inline IPS



Inside or Outside the Firewall?

By definition, an IPS is not a firewall—it doesn’t perform stateful inspection and typically doesn’t allow/block traffic based on the port or IP address. It basically exists to inspect traffic and look for evil, so we still need an actual firewall. This is because firewalls handle the critical functions of filtering the network ports and protocols that are allowed into or out of your network. All you have to do to see just how vital firewalls are is simply execute a packet capture outside your firewall. Doing that will reveal some pretty scary stuff! Capture traffic immediately inside the firewall and you should see a much more sanitized stream.

Because of this, the best location for a perimeter IPS is *inside* the firewall. Placing your IPS outside the firewall will just result in a legion of intrusion events. Even so, most of these events won’t be actionable. Many of the external attacks you see will be blocked by the firewall. This is why it’s much more efficient to let your strategically placed firewall do its job and then let the IPS inspect the leftovers of what’s been allowed through.

Another reason for this placement is because firewall inspection is less complex than IPS deep packet inspection, which translates to cost. Your cost per megabit protected should be less for the firewall than for the IPS. So be wise and place this expensive detection on the inside where it really belongs. You’ll be rewarded with less traffic to deal with!

Finally, consider Network Address Translation (NAT) or web proxies. The IPS inspects traffic initiated from inside as well as outside your network. Many of the outbound rules are designed to detect the results of a malware infection, but the problem is correlating the event to a specific host. If your IPS is outside of your NAT firewall or web proxy, you'll only have a single source IP for all events triggered by outbound traffic. If you've got a web proxy, you might be able to cross-reference the IPS event time with the web proxy log to tie it back to a specific internal IP, but that's often a cumbersome process. And if you're dealing with NAT translation, it's likely that you just won't have a way to tie the event back to an original internal IP address at all. So here we are again, left with non-actionable intrusion events.

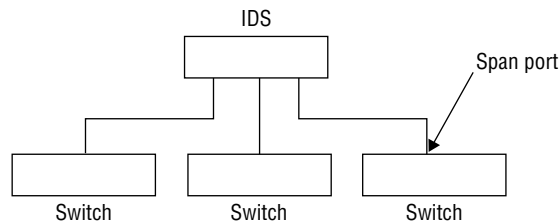
Everything we just talked about still won't be enough to stop some people from placing their IPS outside the firewall. Our goal here is to simply identify the trade-offs in doing so. Just know the pros and cons and that an IPS placed outside the firewall will probably need to be augmented with additional detection inside.

Passive IPS

You already know that the term *passive IPS* is really a misnomer. In reality, it's either passive, as in IDS, or it's inline, as in IPS.

As we've mentioned, in passive mode, the IPS receives a copy of the packets from a switch span port or network tap. Packets that enter the IPS are then inspected, and if they are deemed malicious, an alert is generated. An advantage to this design is that it won't impact the performance of your network, but the disadvantage is that it can only notify of attacks—it can't stop them. Figure 1.2 depicts typical device placement for passive detection.

FIGURE 1.2 Passive IPS



Router, Switch, and Firewall

A Cisco FireSIGHT device can be deployed as a router, a switch, or a firewall. From an intrusion detection perspective, the effect is similar to an inline IPS. Packets pass through a virtual switch or router and are inspected before being allowed to exit. In the real world, deploying the FireSIGHT System as a router/switch/firewall is uncommon because the purpose-driven switches and routers out there have more features and they're faster and

cheaper than using FireSIGHT. FireSIGHT is a specifically designed security device that's just not that great at performing legacy, networking functions. Even so, the SSFIPS exam will present you with some questions about this configuration, so we'll cover it later in the book. All you need to know for now is that network locations where you would deploy a FireSIGHT device in routing or switching mode are identical to where you would deploy traditional switches, routers, or firewalls.

Policies

You will hear a lot about policies regarding the FireSIGHT system—there's a policy for everything! To help you keep your ears from bleeding, just think of policies as “settings saved in the Defense Center database.” These settings control all aspects of system operation and detection on the managed devices. And know that with each new feature added to the system, there's at least one policy to manage that feature associated with it. Here's a list of all the policies available in version 5.3, with a nice little description of each.

Access Control Policy The mother of all policies, the access control (AC) policy is the central traffic cop for packets entering the device, and it works much like a firewall rule set. Traffic is evaluated by the AC rules from top to bottom. When the traffic matches a particular rule, the selected action (block, trust, allow, etc.) is taken and processing stops. All detection features such as IPS, security intelligence, and malware detection are implemented through AC rules.

IPS Policy This policy controls the configuration for IPS detection. If you have ever used or investigated the open source Snort IPS, you will find that most of the settings in the IPS policy correlate directly to an entry in the `snort.conf`. In this policy, you configure the specific Snort rules you want enabled—whether they should block or just alert—as well as myriad advanced options for preprocessors and other Snort options.

Network Discovery Policy Think of this one as a pretty simple set-and-forget policy controlling the scope of host and user discovery for all devices.

File Policy This policy controls the application protocol, direction of transfer, file types, and actions for file and malware detection. With it, you specify that a given type of file transfer traffic will be logged, inspected for malware, or even blocked. For instance, say you want to prevent web servers in your DMZ from uploading Microsoft executable files via HTTP. You can do this and more via the file policy.

NAT Policy Predictably, this policy configures Network Address Translation (NAT). It supports static, dynamic IP or dynamic IP and port rules.

Correlation Policy A policy used in conjunction with correlation rules to alert based on various event criteria. Let's say you want to receive an email when an IPS event is detected on one of your critical servers. You would first create a correlation rule to identify the IPS alert based on criteria such as the destination IP address. You then add the rule to a

correlation policy, which defines the action to take when the rule triggers. In this case, the action would be to send an email to you. Don't worry if this is not clear yet; we address it in much greater detail later in this book.

System Policy This controls a variety of device settings like local firewall, time synchronization, and so on. The system policy is applied to all appliances, meaning to the Defense Center and all devices. Much of the time, a single system policy is used for all the appliances in an organization.

Health Policy This policy sets warning and critical thresholds for various health parameters such as disk space and CPU usage. You can also enable or disable various health checks as your heart desires.

You will find that editing and applying policies is the meat and potatoes of FireSIGHT System management!

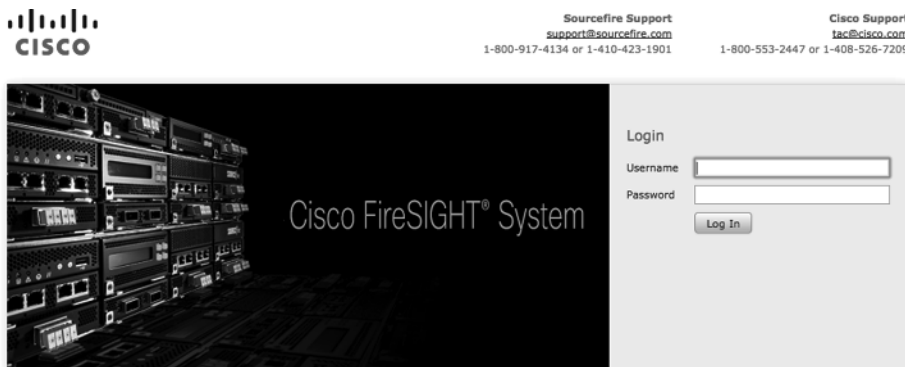
The User Interface

Your primary method to manage the FireSIGHT System is through the web-based user interface on the Defense Center. Something we hear from the mouths of those with extensive experience with other Cisco gear is, “How do I *[insert task here]* using the command line?” Know that with FireSIGHT, there is very little command line management required. Command line access is generally reserved for troubleshooting. Most management tasks can be accomplished only within the web UI.

It's also important to remember that the Defense Center and devices do not listen on port 80. For many secure websites, you can make an initial connection on port 80 and the site will then redirect your browser to connect on port 443. This is not the case with the FireSIGHT web UI, which means when you initially connect, you must type `https://<your appliance IP or hostname>` in your web browser's URL bar.

Upon your initial connection you'll be greeted with a login splash page as shown in Figure 1.3.

FIGURE 1.3 Web UI login screen



The menu system is pretty straightforward, with a top main menu bar and submenus below. Hovering over the top menu will bring up any submenu items. Clicking a submenu item takes you to the appropriate page. Top menu items are separated into left and right groupings. The left-side menu, shown in Figure 1.4, contains mostly items dealing with event analysis and detection configuration.

- Overview – Dashboards and reporting
- Analysis – View/analyze all types of events
- Policies – Configure detection behavior
- Devices – Detection device management
- Objects – Create and manage objects used in policies
- FireAMP – Manage the Defense Center malware detection cloud connection

FIGURE 1.4 Analysis and configuration items



To quickly navigate to the left-most submenu item, you just click the corresponding main menu heading. For example, to get to the Device Management page, simply click Devices in the main menu.

The right side of the main menu (Figure 1.5) contains items focused on the care and feeding of FireSIGHT. This is where you do things like install licenses, download updates, view health status, schedule jobs, and set user preferences.

- Health – Configure and view system health status
- System – Updates, licensing, scheduling, etc.
- Help – Get help
- <username> – Log out, set user preferences

FIGURE 1.5 Operational Items



Initial Appliance Setup

Initial appliance setup includes setting the management IP address and initial connection to the web user interface.

Setting the Management IP

When a new FireSIGHT appliance arrives on the scene, one of the first steps after racking and power is to assign an IP address to the management interface. You can do this several ways:

LCD Panel Each appliance includes an LCD front panel and four buttons, which are used to configure the management IP. Note that using the front panel requires physical access but there's no authentication. If you want, you can disable the IP management feature after the appliance's initial setup. Just follow the onscreen instructions to configure the basic IP settings.

Keyboard/KVM Another method involves logging into the console. First, connect a keyboard and monitor; then, log in using the default credentials of admin/Sourcefire. Your next step is to run the network configuration script as root using the command `sudo configure-network`. This script uses an interview technique to prompt for the necessary IP configuration information.

SSH This final method comes in handy if you want to run the network configuration script but you don't have a keyboard/monitor. Each appliance ships from the factory with a default IP address preassigned to the management interface—this IP address is 192.168.45.45. Sans keyboard/monitor, you can connect a notebook computer with an SSH client right into the management interface network port. After that, configure your notebook with an IP address in the same network and SSH to the appliance. From here, the procedure is the same as it is via the keyboard/KVM method above.



Remember, the default login credentials for all appliances are
 Username: admin
 Password: Sourcefire

Initial Login

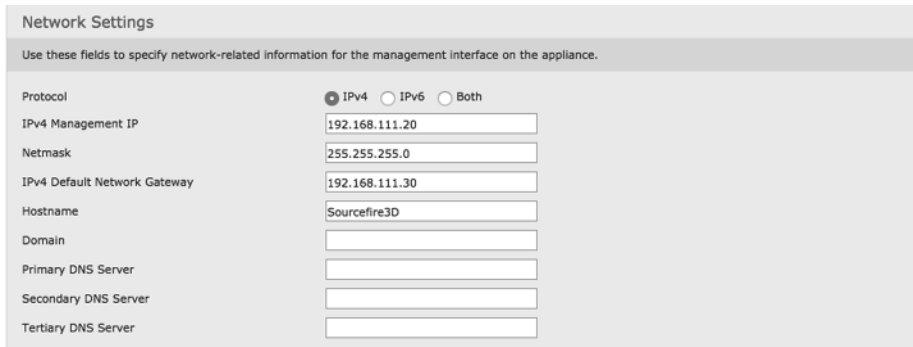
After the management IP address is configured, your next step is to connect to the appliance web UI.

When you first log in, you'll see a one-time configuration web page displayed. The purpose is to gather some initial information and present the end-user license agreement prior to moving on to the standard web UI.

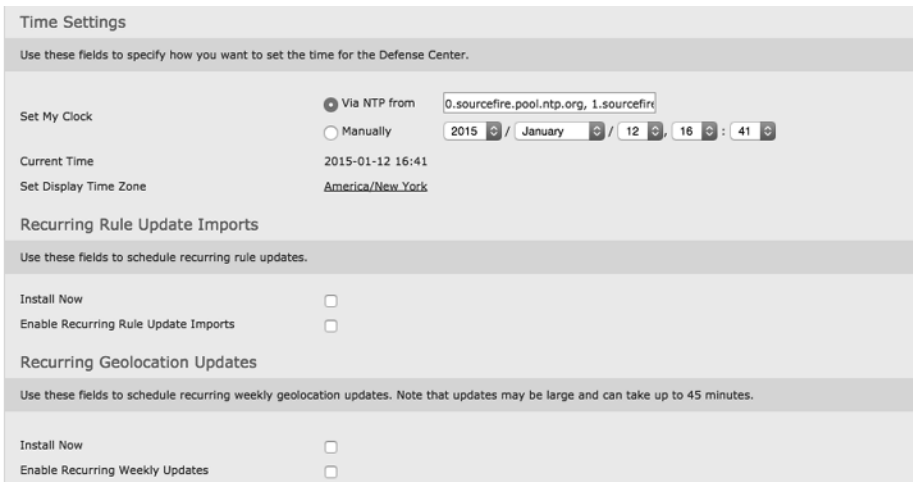
The Defense Center configuration page contains the following sections.

Change Password This is a required field. You must enter a password, changing the appliance default.

Network Settings This section contains the IP information entered via the LCD or `configure-network` script, but it also allows you to add more items like hostnames and DNS servers. (See Figure 1.6.)

FIGURE 1.6 Network configuration


Time Settings This allows you to configure time synchronization from an external Network Time Protocol (NTP) source or manually. As shown in Figure 1.7, if you have multiple NTP servers, they are entered into the data field in a comma-separated format.

FIGURE 1.7 Time and update settings


Recurring Rule Update Imports Permits you to configure updating of IPS rules from Cisco on a recurring basis.

Recurring Geolocation Updates Allows you to configure updating of the IP to geographic location information from Cisco on a recurring basis.

Automated Backups Use this to configure backups of the local policy and configuration database.

License Settings Allows you to add feature license keys.

Device Registration Use this to register managed devices on the Defense Center.

End User License Agreement Here's where you read and accept the Cisco software license agreement. This is a required setting.

While it is possible to configure all of these on the initial screen, most of us configure these settings later via System Policy or Local Configuration settings. The only two you have to worry about are changing the password and accepting the EULA.

Summary

Congratulations are in order! You now have a solid foundation and understand many of the terms that we'll use throughout this book. We covered some industry-wide and Cisco-specific terminology and introduced you to the various FireSIGHT appliance models. We also talked about licensing and network design. We explored the web-based user interface, described Cisco FireSIGHT policy-based management, and explained the new appliance initial setup process—you're ready to delve deeper now and build upon your knowledge!

Hands-on Lab


1. Open your web browser and connect to your Defense Center.
2. Log in to the Defense Center.
3. Check your licenses on your system by going to the top-right menu bar and selecting System > Licenses.



4. Verify that the licenses are valid and that you have all licenses enabled on your Defense Center: URL Filtering, Protection, Control, and Malware.
5. Click Devices on the main menu.
6. Click the edit icon (the pencil icon) to make changes to a device.

Name	License Type	Health Policy	System Policy	Access Control Policy
Ungrouped (1)				
198.18.133.11 198.18.133.11 - Virtual Device 64bit - v5.3.0.1	Protection, Control	Cisco Security BU - Produc	Cisco Security RG - Produc	Cisco Security RG - Produc

7. Click the Device tab and verify that Protection, Control, Malware, and URL filtering are all set to Yes.
8. Verify that the license(s) that are enabled.

License 	
Protection:	Yes
Control:	Yes
Malware:	Yes
URL Filtering:	Yes

Review Questions

You can find the answers in Appendix A.

1. The 32/64-bit device virtual appliance supports which of the following features?
 - A. Switched interfaces
 - B. Passive interfaces
 - C. Routed interfaces
 - D. All of the above
2. The default login for all appliances is username: **admin** and password: _____.
 - A. Sourcefire
 - B. Cisco
 - C. FireSIGHT
 - D. password
3. Which of the following is a valid method for configuring the initial management IP address of an appliance?
 - A. Keyboard/KVM
 - B. SSH
 - C. LCD panel
 - D. All of the above
4. Which of the following licenses is required for a device to operate as a next generation fire-wall (NGFW)?
 - A. Firewall
 - B. Control
 - C. Malware
 - D. URL Filtering
5. Which of the following licenses must be enabled on a device before a Malware license can be enabled?
 - A. Protect
 - B. Control
 - C. VPN
 - D. URL Filtering
6. Which license(s) must be enabled on a device before a VPN license can be enabled?
 - A. Protect
 - B. Control
 - C. Protect and Control
 - D. None of the above

