This chapter covers the following topics:

- Components of SAFE Small Network Design
- Corporate Internet Module
- Campus Module
- Branch Versus Headend/Standalone Considerations for Small Networks

CHAPTER 13

Designing Small SAFE Networks

The principle goal of Cisco SAFE blueprints is to provide to interested parties best-practice information on how to design and implement secure networks. SAFE serves as a guide to network architects who are examining the security requirements of their networks. SAFE blueprints combat security threats by using a modular method that allows for the creation of a scalable, corporate-wide security solution.

This is the first of three chapters that cover the specific design requirements of the "SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks" (SAFE SMR) design model. The focus of this chapter is the specific security design requirements of the small network.

"Do I Know This Already?" Quiz

The purpose of the "Do I Know This Already?" quiz is to help you decide if you really need to read the entire chapter. If you already intend to read the entire chapter, you do not necessarily need to answer these questions now.

The nine-question quiz, derived from the major sections in the "Foundation Topics" portion of the chapter, helps you determine how to spend your limited study time.

Table 13-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 13-1 *"Do I Know This Already?" Foundation Topics Section-to-Question Mapping*

Foundation Topics Section	Questions Covered in This Section
Components of SAFE Small Network Design	1
Corporate Internet Module in Small Networks	2–6
Campus Module in Small Networks	7–9

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark this question wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. The SAFE small network design consists of which of the following modules?
   a. ISP module
   b. Campus module
   c. Remote User module
   d. Corporate Internet module
   e. E-Commerce module

2. Which of the following are components of the Corporate Internet module?
   a. Firewall
   b. Management server
   c. Corporate users
   d. Layer 3 switch
   e. DNS server

3. VPN connectivity is terminated in the Corporate Internet module.
   a. True
   b. False

4. What is the most likely point of attack in the Corporate Internet module?
   a. Firewall
   b. Switch
   c. Router
   d. Public services
   e. ISP router

5. It is common to avoid using private VLANs on the public services segment of the Corporate Internet module.

a. True

b. False

6. What provides network-level protection, stateful filtering of traffic, and VPN termination within the Corporate Internet module?

a. VPN concentrator

b. Cisco IOS Firewall

c. Layer 2 switch

d. PIX Firewall

e. Public server

7. The Campus module of the small network design contains which of the following?

a. Filtering

b. Layer 2 functionality

c. Corporate users

d. Public servers

e. Intranet servers

8. In the small network design, user authentication is implemented within the Campus module.

a. True

b. False

9. Because no Layer 3 services are used within the Campus module, the small network design places an emphasis on what?

a. Routing

b. Host security

c. Filtering

d. Connectivity

e. Application security

The answers to the “Do I Know This Already?” quiz are found in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Q&A Sections.” The suggested choices for your next step are as follows:

- **7 or less overall score**—Read the entire chapter. This includes the “Foundation Topics” and “Foundation Summary” sections, and the “Q&A” section.
- **8 or more overall score**—If you want more review on these topics, skip to the “Foundation Summary” section and then go to the “Q&A” section. Otherwise, move to the next chapter.

Foundation Topics

The design philosophy behind the SAFE blueprint was first introduced in Chapter 2, “SAFE Design Fundamentals.” This chapter builds on the objectives of that design philosophy by combining them with the desired network functionality required for a small network.

The small network is like most networks connected to the Internet. Internal users require access to external resources, whereas external users might need access to internal resources. Consequently, this can leave the network open to various types of threats both from internal users and from users on the publicly addressable hosts. When designing any security solution, you must always be aware of the potential for these types of threats.

The small network can be designed in two ways: as a headend or standalone configuration or as a branch configuration. The design recommendations for each of these two configuration types are similar, but some functionality found in the branch configuration might be superfluous because it is provided for in the headend configuration of the network.

For the discussion purposes of this chapter, in addition to presenting the headend or standalone configuration, any specific design changes in relation to a branch configuration are also given.

Components of SAFE Small Network Design

The following two modules and their associated devices, shown in Figure 13-1, make up the small network design:

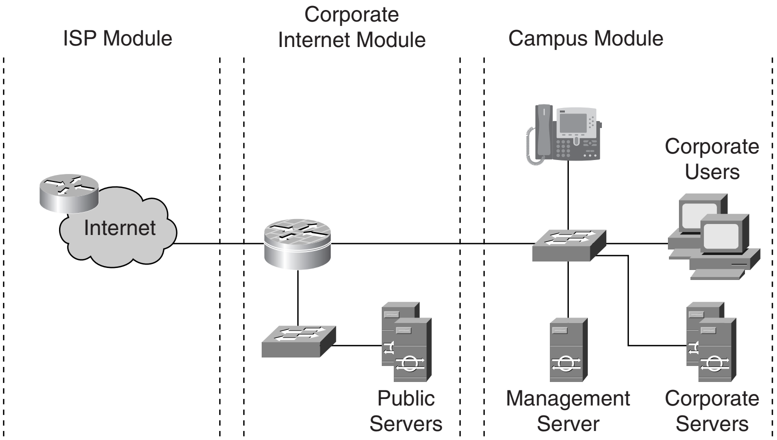
- Corporate Internet module
- Campus module

NOTE Figure 13-1 also shows an ISP module, for clarity, but it is not considered a part of the small network design model.

The Corporate Internet module provides connectivity to the Internet and terminates any VPN connectivity. Traffic for public services such as mail, web, file transfer, and name lookups are also terminated at the Corporate Internet module.

The Campus module incorporates the internal Layer 2 switching, including corporate users, corporate intranet servers, and management servers.

Figure 13-1 *Small Network Model*



Corporate Internet Module in Small Networks

The Corporate Internet module provides internal users connectivity to Internet services and provides Internet users access to information on the corporate public servers. This module also provides remote access for remote locations and telecommuters through the use of VPN connectivity.

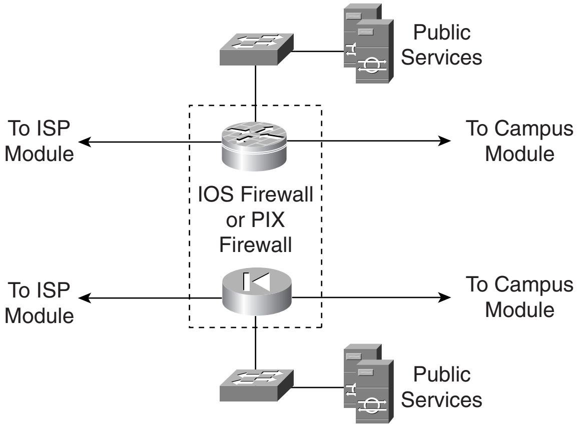
Several key devices make up the Corporate Internet module. These devices are described in Table 13-2.

Table 13-2 *Corporate Internet Module Devices*

Device	Description
Mail server	Acts as a relay between the Internet and the intranet mail servers and scans for mail-based attacks
DNS server	Serves as the authoritative external DNS server and relays internal requests to the Internet
Web/file server	Provides public information about the organization
Firewall or Cisco IOS Firewall router	Provides network-level protection of resources, stateful filtering of traffic, and VPN termination for remote sites and users
Layer 2 switch	Ensures that data from managed devices can only cross directly to the Cisco IOS Firewall and provides private VLAN support

As shown in Figure 13-2, either a Cisco IOS Firewall router or a PIX Firewall is used within the Corporate Internet module. The particular choice of hardware platform depends on the specific network requirements and any associated design criteria. Design considerations are discussed in subsequent sections of this chapter.

Figure 13-2 *Small Network Corporate Internet Module*



Mitigating Threats in the Corporate Internet Module

The most likely point of attack within the Corporate Internet module is on the public services segment. Positioned on this segment are the publicly addressed servers. Table 13-3 shows the anticipated threats and mitigation actions expected on this segment.

Table 13-3 *Corporate Internet Module Threats and Threat Mitigation*

Threat	Threat Mitigation
Application layer attacks	Mitigated through HIDSs on the public servers
DoS	Limited through the use of CAR* at ISP edge and TCP setup controls at firewall
IP spoofing	Mitigated through RFC 2827 and RFC 1918 filtering at ISP edge and local firewall
Network reconnaissance	Mitigated through HIDS detecting reconnaissance and by the use of protocol filtering to limit visibility
Packet sniffers	Mitigated through use of a switched infrastructure and HIDS to limit exposure
Password attacks	Mitigated by limiting the services available to brute force; operating system and IDS can detect the threat

continues

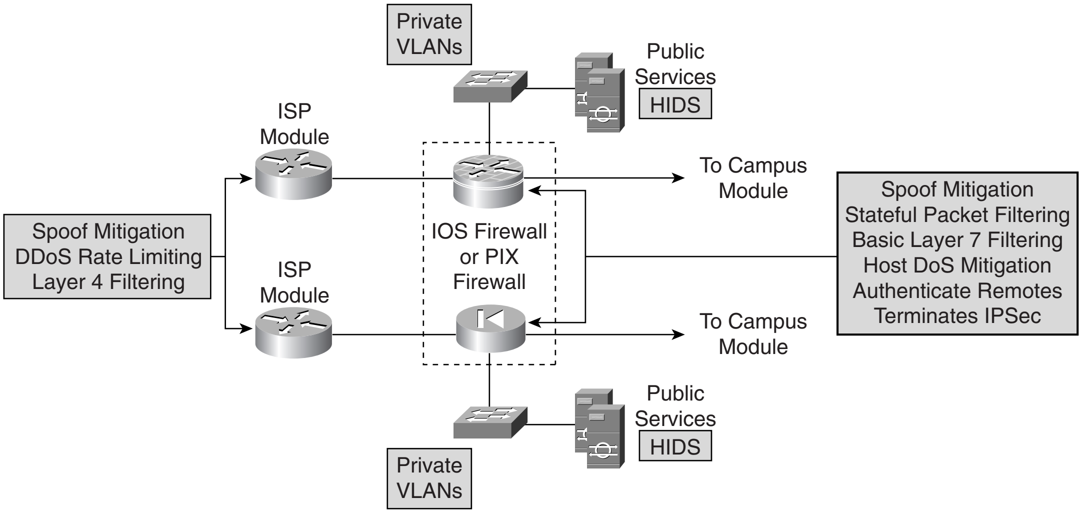
Table 13-3 *Corporate Internet Module Threats and Threat Mitigation (Continued)*

Threat	Threat Mitigation
Port redirection	Mitigated through restrictive filtering and HIDS to limit attack
Trust exploitation	Mitigated through restrictive trust model and private VLANs to limit trust-based attacks
Unauthorized access	Mitigated through filtering at the firewall
Virus and Trojan-horse attacks	Mitigated through virus scanning at the host level

*CAR = committed access rate

Figure 13-3 displays the threat-mitigation roles of each of the devices found within the Corporate Internet module.

Figure 13-3 *Small Network Corporate Internet Module Threat-Mitigation Roles*



Design Guidelines for the Corporate Internet Module

The small network model represents a scaled-down security-centric network design with all the security and VPN functionality that is found within a single device. As described earlier and shown in Figure 13-2, two options are available within this design model:

- Cisco IOS router
- Firewall

The first option uses a Cisco IOS router with firewall and VPN functionality. This option provides the greatest flexibility within the small network design because the router is capable of supporting not only the firewall and VPN functionality but also the advanced features now offered to Cisco IOS routers, such as QoS and multiprotocol support.

The second option available in the small network design is to use a dedicated firewall, but because most firewalls are Ethernet-only devices, deployment issues might arise if a WAN termination is required for the ISP circuit. If WAN connectivity is required, a router must be used in the design. However, using a dedicated firewall does have the advantage of easier configuration of security services, and a dedicated firewall can provide improved performance when performing firewall functions.

Whichever option is finally chosen, stateful firewall inspection is used to examine traffic in all directions, to ensure that only legitimate traffic crosses the firewall.

Filtering and Access Control

Even before any traffic reaches the firewall, it is ideal to implement some form of security filtering on the perimeter traffic flow. Table 13-4 shows the filter parameters that can be applied to perimeter traffic flow.

Table 13-4 *Perimeter Traffic Flow Filtering*

Filter Location	Flow	Filter Description	Mitigation
ISP router	Egress	ISP rate limits nonessential traffic that exceeds a predefined threshold	DDoS
ISP router	Egress	RFC 1918 and RFC 2827 filtering	IP spoofing
Router or firewall	Ingress	RFC 1918 and RFC 2827 filtering	IP spoofing—verifies ISP filtering
Router or firewall	Ingress	VPN- and firewall-specific traffic	Unauthorized access

The stateful firewall also provides connection-state enforcement and detailed filtering for sessions initiated through the firewall. Additionally, the advance features within the software protect against TCP synchronization (TCP SYN) attacks on the publicly facing servers by controlling the limits on half-open sessions that are transiting the firewall.

With reference to the public services segment, the filtering of traffic should control not only the flow of traffic destined to specific addresses and ports on the public services segment but also the flow of traffic from the segment. This additional level of filtering prevents an attacker who may have compromised one of the public servers from using that server as a platform to launch further attacks on the network.

For example, if an intruder has managed to circumvent the firewall and HIDS security features on a public-facing DNS server, that server should be permitted only to reply to requests, not to originate requests. This prevents an intruder from using this compromised platform to launch additional attacks.

Finally, the use of private VLANs on the demilitarized zone (DMZ) switch prevents a compromised server from being used to attack other servers on the same segment. The implementation of private VLANs is especially important because this type of vulnerability is not detectable by the firewall.

Intrusion Detection

Every server on the public services segment should be configured with HIDS software, which allows for the monitoring of rogue activity at the operating system level. HIDS can also be configured to monitor certain common server applications. Additionally, all public service applications, such as the web, mail, and DNS services, should be hardened as much as possible so that unnecessary responses cannot be used to assist an intruder in network reconnaissance.

The advanced software features found in Cisco PIX Firewalls and Cisco IOS Firewall routers provide some limited NIDS functionality. They can normally drop many types of attacks without the use of an IDS management station, but obviously dropped events are not reported. However, because these devices are not specifically designed for intrusion detection, it is possible that a degradation in performance of the device might occur. If performance degradation does occur, the drop in performance is normally acceptable when compared to the benefits gained from an increase in attack visibility.

VPN Connectivity

The firewall or Cisco IOS Firewall router provides VPN connectivity for the small network design. Authentication of remote sites and remote users can be accomplished by using preshared keys or the use of an access control server located in the Campus module.

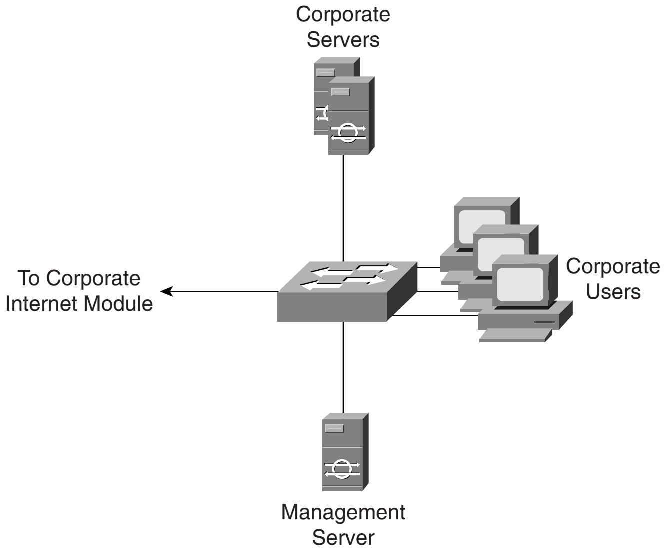
Design Alternatives for the Corporate Internet Module

Usual deviations from these design guidelines normally include the breaking out of the functional components in the network from a single device to individual, specific devices or an increase in network capacity. When these functions are broken out, the design begins to take on the look of the medium-sized network design, which is discussed in Chapter 16, “Implementing Medium-Sized SAFE Networks.” Before you decide that you have to adopt the complete design for a medium-sized network, however, it may be worth considering the placement of a Cisco VPN 3000 Series Concentrator or router on the DMZ to offload processing of VPN traffic. The addition of this device also increases the manageability of VPN connectivity.

Campus Module in Small Networks

The Campus module of the small network design, which is shown in Figure 13-4, provides end-user workstations, corporate intranet servers, management servers, and the associated Layer 2 functionality via a single switch.

Figure 13-4 *Small Network Campus Module*



Four key devices make up the Campus module, which are highlighted in Table 13-5.

Table 13-5 *Campus Module Devices*

Device	Description
Corporate server	Provides services to internal users such as e-mail, file, and printing services
Layer 2 switch	Provides Layer 2 connectivity and also supports private VLANs
Management host	Provides management services, such as authentication, through RADIUS and TACACS+, HIDS, syslog, and other general management services
User workstation	Provides data services to authorized users on the network

Mitigating Threats in the Campus Module

Within the small network Campus module, each device plays a threat-mitigation role, as shown in Figure 13-5. Table 13-6 lists the expected threats and mitigation actions found within this module.

Figure 13-5 *Small Network Campus Module Threat-Mitigation Roles*

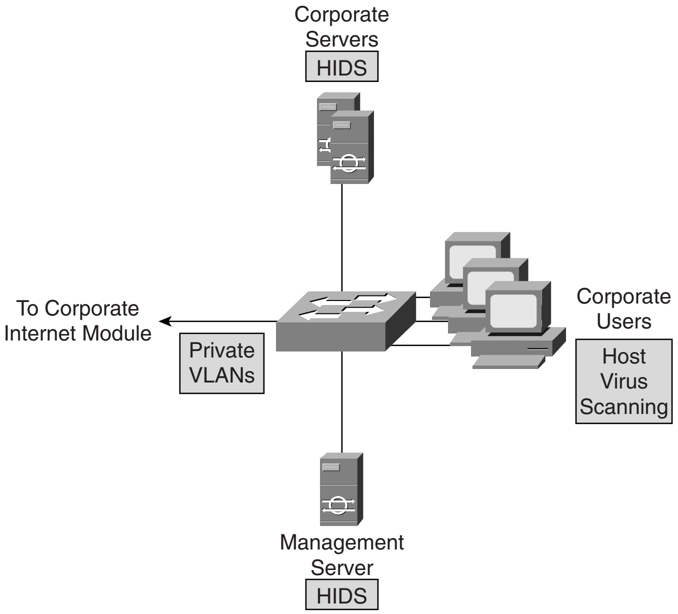


Table 13-6 *Campus Module Threats and Threat Mitigation*

Threat	Threat Mitigation
Application layer attacks	Operating systems, devices, and applications are kept up to date with the latest security fixes and are protected by HIDSs.
Packet sniffers	A switched infrastructure limits the effectiveness of sniffing.
Port redirection	HIDSs prevent port redirection agents from being installed.
Trust exploitation	Private VLANs prevent hosts on the same subnet from communicating unless necessary.
Unauthorized access	HIDSs and application access control are used to mitigate unauthorized access.
Virus and Trojan-horse applications	Host-based virus scanning and host intrusion prevention prevents most viruses and many Trojan horses.

Design Guidelines for the Campus Module

The small network Campus module provides connectivity for the corporate and management servers and also corporate users. Private VLANs can be used within the switch to mitigate trust-exploitation attacks between the devices. For example, corporate users might not require inter-user communications and only need to communicate directly with corporate servers. This functionality can be provided by using private VLANs.

Because the Campus module has no Layer 3 services within its design, there is an increased emphasis on application and host security because of the open nature of the internal network. Consequently, HIDSs have been installed on key devices within the campus, including the corporate servers and management systems.

Design Alternatives for the Campus Module

The placement of a filtering device, such as a firewall or router, to control the flow of management traffic between the management server and the rest of the network provides an increased level of security. Also, if the level of trust within the organization is high, it is possible to consider removing the HIDS from the design but this is not recommended.

Branch Versus Headend/Standalone Considerations for Small Networks

When considering the small network design requirements in a branch role rather than a headend or standalone role, the following should be noted:

- VPN connectivity for remote users is normally not required because it is provided for by the corporate headquarters.
- Management servers and hosts are normally located at the corporate headquarters, requiring management traffic to traverse the site-to-site VPN connection.

Foundation Summary

The "Foundation Summary" section of each chapter lists the most important facts from the chapter. Although this section does not list every fact from the chapter that will be on your CSI exam, a well-prepared CSI candidate should at a minimum know all the details in each "Foundation Summary" section before taking the exam.

The key devices that make up the Corporate Internet module are highlighted in Table 13-7.

Table 13-7 *Corporate Internet Module Devices*

Device	Description
Mail server	Acts as a relay between the Internet and the intranet mail servers and also scans for mail-based attacks
DNS server	Serves as the authoritative external DNS server and relays internal requests to the Internet
Web/file server	Provides public information about the organization
Firewall or Cisco IOS Firewall router	Provides network-level protection of resources, stateful filtering of traffic, and VPN termination for remote sites and users
Layer 2 switch	Ensures that data from managed devices can only cross directly to the Cisco IOS Firewall and provides private VLAN support

Table 13-8 summarizes the Corporate Internet module threats and mitigation techniques.

Table 13-8 *Corporate Internet Module Threats and Threat Mitigation*

Threat	Threat Mitigation
Application layer attacks	Mitigated through HIDSs on the public servers
DoS	Limited through use of CAR at ISP edge and TCP setup controls at firewall
IP spoofing	Mitigated through RFC 2827 and RFC 1918 filtering at ISP edge and local firewall
Network reconnaissance	Mitigated through HIDS detecting reconnaissance and by the use of protocol filtering to limit visibility
Packet sniffers	Mitigated through switched infrastructure and HIDS to limit exposure

Table 13-8 *Corporate Internet Module Threats and Threat Mitigation (Continued)*

Threat	Threat Mitigation
Password attacks	Mitigated by limiting the services available to brute force; operating system and IDS can detect the threat
Port redirection	Mitigated through restrictive filtering and HIDSs to limit attack
Trust exploitation	Mitigated through restrictive trust model and private VLANs to limit trust-based attacks
Unauthorized access	Mitigated through filtering at the firewall
Virus and Trojan-horse attacks	Mitigated through virus scanning at the host level

Table 13-9 shows the filter parameters that can be applied to perimeter traffic flow.

Table 13-9 *Perimeter Traffic Flow Filtering*

Filter Location	Flow	Filter Description	Mitigation
ISP router	Egress	ISP rate limits nonessential traffic that exceeds a predefined threshold	DDoS
ISP router	Egress	RFC 1918 and RFC 2827 filtering	IP spoofing
Router or firewall	Ingress	RFC 1918 and RFC 2827 filtering	IP spoofing—verifies ISP filtering
Router or firewall	Ingress	VPN- and firewall-specific traffic	Unauthorized access

The four key devices that make up the Campus module are highlighted in Table 13-10.

Table 13-10 *Campus Module Devices*

Device	Description
Corporate servers	Provides services to internal users such as e-mail, file, and printing services
Layer 2 switch	Provides Layer 2 connectivity and also supports private VLANs
Management host	Provides management services, such as authentication, through RADIUS and TACACS+, HIDS, syslog, and other general management services
User workstation	Provides data services to authorized users on the network

Table 13-11 lists the expected threats and mitigation actions found within the Campus module.

Table 13-11 *Campus Module Threats and Threat Mitigation*

Threat	Threat Mitigation
Application layer attacks	Operating systems, devices, and applications are kept up to date with the latest security fixes and are protected by HIDSs.
Packet sniffers	A switched infrastructure limits the effectiveness of sniffing.
Port redirection	HIDSs prevent port redirection agents from being installed.
Trust exploitation	Private VLANs prevent hosts on the same subnet from communicating unless necessary.
Unauthorized access	HIDSs and application access control are used to mitigate unauthorized access.
Virus and Trojan-horse applications	Host-based virus scanning and host intrusion prevention prevents most viruses and many Trojan horses.

Q&A

As mentioned in the Introduction, "All About the Cisco Certified Security Professional Certification," you have two choices for review questions. The questions that follow next give you a more rigorous challenge than the exam itself by using an open-ended question format. By reviewing now with this more difficult question format, you can exercise your memory better and prove your conceptual and factual knowledge of this chapter. The answers to these questions are found in Appendix A.

For more practice with exam-like question formats, including questions using a router simulator and multiple choice questions, use the exam engine on the CD-ROM.

1. What modules are found within the small network design?
2. Where are private VLANs used in the small network design?
3. What two security devices can be used in the Corporate Internet module to connect to the ISP module?
4. Where would you use intrusion detection in the small network design?
5. VPN functionality is provided by what devices in the small network design?
6. The Corporate Internet module connects to which modules?
7. What are the two configuration types available in the small network design?
8. The Campus module provides functionality to what components?
9. Because no Layer 3 services are available in the Campus module, an increased emphasis is placed on ___________ and ____ security.
10. What is a common design deviation in the Corporate Internet module?
11. The Corporate Internet module provides what services?

Reference

Convery, Sean, and Roland Saville. "SAFE: Extending the Security Blueprint to Small, Midsize, and Remote-User Networks." Cisco Systems, Inc., 2001.