# The CSI Cram Sheet

This Cram Sheet contains the distilled, key facts about the Cisco SAFE Implementation exam. Review this information last before entering the test room, paying special attention to those areas in which you feel you need the most review. You can transfer any of this information onto the scratch paper or plastic sheet that the exam proctor provides you before you actually begin the exam.

## SECURITY FUNDAMENTALS

1. Need for network security
   - Business and personal data are exposed via the Internet.
   - Hackers constantly create new threats, due to the ubiquity of the Internet, allowing them to share information and tools globally.
   - New threats are also due to the pervasiveness of easy-to-use operating systems and development environments, reducing the knowledge and skill level required to become a hacker.
2. Network attack taxonomy (types of attacks)
   - *Packet sniffers*—Can capture addresses, hostnames, usernames, and passwords. Mitigated by authentication, a switched infrastructure, antisniffer tools, and cryptography.
   - *IP spoofing*—Involves a hacker gaining access by pretending to belong to the network. Mitigated by access control and RFC 2827 filtering.
   - *Denial of service (DoS)*—Consuming so much of a limited resource (bandwidth, buffers, CPU cycles) that others cannot use it. Mitigated by antispoofing measures, rate limiting upstream, and half-open connection limits.
   - *Password attacks*—Involve attempts to learn or crack passwords to gain access. Mitigated by strong passwords (minimum of eight characters and mix of uppercase and lowercase letters, numbers, and special characters), OTP, and encrypting password transmission.
   - *Man-in-the-middle attacks*—Involve a hacker interposing himself between two parties exchanging data. Mitigated by encrypting data exchange.
   - *Application-layer attacks*—Involve a hacker taking advantage of known vulnerabilities in applications. Mitigated by keeping the OS and all applications fully patched and using IDS (primarily HIDS, but also NIDS).
   - *Network reconnaissance*—Involves a hacker learning the network topology and characteristics (naming, addressing, device information). Mitigated by HIDS and NIDS, and protocol filtering.
   - *Trust exploitation*—Involves taking advantage of established operating relationships, in which systems must accept information and inputs from other systems. Mitigated by restrictive trust model, strong access control, and private VLANs.
   - *Port redirection*—Causing traffic that enters a host on one port to be sent to another port, thereby leading it to be acted on by another process. Mitigated by restrictive trust models and HIDS.
   - *Unauthorized access*—Involves obtaining illegitimate access to restricted resources. Mitigated by protocol filtering at the firewall and strong access control.
   - *Virus and trojan horse attacks*—Involve inserting malware into unprotected hosts to exploit them. Mitigated by maintaining currency of OS and applications and antivirus software.
3. Network security policy
   - SAFE Blueprints assume that a policy is already present.
   - A security policy provides management endorsement of security, various usage policies, audit provisions to assess compliance, and incident-response plans.
4. Management protocols and functions
   - SSH and SSL for encrypted device access instead of Telnet, which is cleartext (including passwords).
   - Syslog for device logging and alarm transmittal to servers.
   - TFTP for device image and configuration file transfer.
   - SNMP for device management (rw community) and information (ro community). Use SNMP v3 to have encryption and authentication.
   - NTP for clock synchronization. Use NTP v3 for secure authentication of time data from upstream servers.

## ARCHITECTURAL OVERVIEW

5. Design fundamentals of SAFE SMR Blueprint
   - Security and attack mitigation based on policy
   - Security implementation throughout the infrastructure
   - Cost-effective deployment
   - Secure management and reporting
   - Authentication and authorization of users and administrators to critical network resources
   - Intrusion detection for critical resources and subnets
6. SAFE SMR Blueprint axioms
   - Routers are targets.
   - Switches are targets.
   - Hosts are targets.
   - Networks are targets.
   - Applications are targets.
   - Secure management and reporting.
7. Security wheel: secure, monitor, test, improve; repeat

## CISCO SECURITY PORTFOLIO

8. *IOS routers*—Provide RFC 2827 and RFC 1918 filtering, protocol filtering, and VPN termination, as well as stateful firewall and intercept features.
9. *PIX firewalls*—Provide stateful firewall and VPN termination; 515 and higher support VPN accelerator card from PIX OS v5.3(1) with DES or 3DES license.
10. *Cisco NIDS*—Provides intrusion monitoring across a network segment; usually set to alarm.
11. *Cisco HIDS*—Provides host-level intrusion monitoring; usually set to alarm, drop, and (possibly) reset.
12. *VPN concentrator*—Terminates many VPN tunnels at the headend; often used when more than 20 tunnels must be terminated. Can support a maximum of 100–10,000 simultaneous users. Provides AES and DH Group 7 in addition to DES/3DES and DH Groups 1, 2, 5.
13. *VPN clients*—Hardware client often used for small branches that provides tunnel termination and local DHCP and NAT. Software client used for single-host tunnel termination, with split tunneling not recommended. Receive policy and configuration for both pushed from headend.
14. *Identity*—CiscoSecure ACS for AAA; runs on Windows 2000 server and Solaris (Solaris support ends in 2003).
15. *Security management*—CiscoWorks VPN/Security Management Solution (VMS); Web-based tools for VPN configuration, monitoring, troubleshooting, and firewall and IDS management; also, CiscoSecure Policy Manager (CSPM) firewall-management functions have been moved to VMS.

## SAFE SMALL NETWORK DESIGN

16. *Corporate Internet module*—Contains an ingress router or firewall, switch, and DMZ servers with HIDS. Design alternative is to add a VPN concentrator.
17. *Campus module*—Contains switch, users, corporate servers with HIDS, and management server with HIDS. Design alternative is to add a filtering firewall in front of the management server.

## SAFE MEDIUM NETWORK DESIGN

18. *Corporate Internet module*—Contains ingress router, switches, NAS, firewall, DMZ servers with HIDS, NIDS on DMZ and campus approach paths, and egress router. Design alternatives are to add a stateful firewall at ingress, place a NIDS in front of the existing firewall, eliminate the egress firewall (at egress to the campus), and add content inspection/URL filtering capability.
19. *WAN module*—Contains ingress router for frame relay/ATM leased circuits; passes traffic directly into the campus. Alternatives are to add a firewall or use encryption.
20. *Campus module*—Contains Layer 3 switch with NIDS, Layer 2 switches, users, corporate servers with HIDS, and management server with HIDS. Design alternatives are to eliminate Layer 2 switches (Layer 3 switch supports all traffic), eliminate Layer 3 switch and add a router for iltering and segmentation, and replace the NIDS appliance with a blade on the Layer 3 switch to handle more throughput.

## SAFE REMOTE-USER DESIGN (FOUR OPTIONS)

21. *Software access option*—Contains software VPN client; requires personal firewall on the host. Split tunneling is not recommended. Often used for personnel who travel.
22. *Remote site firewall option*—Contains a broadband access device, a stateful firewall, and a distribution device (hub or switch). Split tunneling possible and can be used for a small branch or home office/teleworker.

23. *Hardware VPN client option*—Contains a broadband access device, a hardware VPN client, and a distribution device (hub or switch). Split tunneling is possible and can be used for a small branch or home office/teleworker.
24. *Remote site broadband router option*—Contains a broadband access device, a router with a firewall and VPN termination, and a distribution device (hub or switch). Split tunneling is possible and can be used for a small branch or home office/teleworker. If the router is integrated with the broadband access device, management might be retained by the ISP.

## BRANCH VERSUS HEADEND OR STANDALONE CONSIDERATIONS

25. Branch networks generally do not need public-facing servers or VPN termination. Therefore, they usually do not need a Corporate Internet module except for local Internet access. They also do not have management servers in the Campus module because this comes from their headends.
26. Headend or standalone networks do need public-facing servers and VPN termination, along with management servers.

## SIMULATION

27. Expect a simulation on the exam. Be able to securely connect a router or a PIX or a VPN concentrator to another device from this list. VPNs require IKE configuration and IPSec configuration.
28. IKE configuration. Set the isakmp policy with any changes from defaults (preshared key, DH group, hash, or encryption). Set the peer.
29. IPSec configuration. Set the transform set with encryption and hash. Add the ACL to define encrypted traffic. Apply to the correct interface. Save.