This Cram Sheet contains the distilled, key facts about the ISA Server 2000 exam. Review this information immediately before entering the test room, paying special attention to those areas in which you feel you need the most review. Remember, you can transfer any of these facts that you've crammed into your short-term memory onto a blank piece of paper before beginning the exam.

Installing ISA Server

1. Minimum requirements for hardware:
   * 300MHz Pentium II, 256MB RAM
   * 20MB available drive space
   * 100MB+.5MB/user of NTFS formatted space if caching Web content.
2. Minimum requirements for software:
   * Windows 2000 Server, Advanced Server, or Datacenter Server
   * Windows 2000 Service Pack 1 (Service Pack 2 or later recommended)
3. Installation modes and their features:
   * Base feature set - Web publishing, realtime alerts and monitoring, report generation
   * Cache - Web caching
   * Firewall - Server publishing, VPN Server and passthru, packet filtering, application filtering
   * Integrated - All features included
4. Steps to perform before installation:
   * Confirm proper installation of Windows 2000, current Service Pack.
   * Confirm proper quantity of RAM, and pagefile size and location.
   * Confirm that DNS is fully 100 percent functional.
   * Confirm full Internet connectivity from the ISA Server.
5. Installation of an array:
   * Enterprise Initialization Tool (MSISAENT.EXE)
   * Schema Extensions requires Schema Admin permissions
6. Steps for migration from Proxy Server 2:
   * Stop all existing Proxy services.
   * Upgrade server to Windows 2000.
   * Install ISA Server.
7. What is migrated from Proxy Server 2 (if the server will be part of an Enterprise array, only the settings that do not conflict with the Enterprise policy will be migrated):
   * Cache settings
   * Proxy rules
8. What isn't migrated from Proxy Server 2:
   * Cache content
   * SOCKS rules
9. What's changed from Proxy Server 2:
   * No IPX/SPX support
   * Proxy listener port changed from 80 (normal HTTP) to 8080

Caching

10. Forward caching—ISA Server caches information for clients on the internal network.
11. The three types of forward caching configurations are standalone, distributed, and hierarchical.
12. Reverse caching—ISA Server caches information for external clients.
13. The Time to Live (TTL) determines how long objects in the cache remain valid.
14. Objects in the cache expire if:
    * TTL assigned by the server of origin expires.
    * TTL manually configured for cached objects expires.
    * TTL configured for scheduled content download expires.
15. Active caching—ISA Server caches the most popular objects accessed by clients.

Rules

16. Protocol rules grant or deny clients access to Internet protocols.
17. Site and content rules define the Internet content to which clients behind an ISA Server have access.
18. For users to access the Internet, a protocol rule and a site and content rule must be configured to permit access.
19. Packet filtering allows ISA Server to inspect IP packets before allowing them into the internal network. Packet filtering includes:
    * Dynamic filtering - Allows IP packets to pass through as needed
    * Static filtering - Explicitly allows or denies specific packets to pass to the internal network
20. Routing rules determine how client requests are routed.
21. The default routing rule routes all requests to the Internet if they are not in the cache.
22. Client requests can be routed to the Internet, to an upstream server or array, or redirected to another server.

Arrays

23. Array members must be in the same domain and the same site.
24. Arrays require Active Directory; therefore, a Windows 2000 domain is required.
25. Proxy Server 2 and ISA Server arrays can coexist.
26. The two types of array configurations are distributed and hierarchical.
27. In an array, CARP is enabled for outgoing requests and disabled for incoming requests.

Configuring and Troubleshooting ISA Server Services

28. The three primary configurations for an ISA Server installation are bastion host, three-homed, and back-to-back.
29. Make certain that the LAT is properly configured.
    * For bastion host and three-homed servers, only the local network addresses should be part of the LAT.
    * For back-to-back servers, the one physically plugged into the local network should include only those addresses. The external server should include the LAN and DMZ addresses in its LAT.
30. To allow internal machines to make PPTP calls out (IPSec does not work with SecureNAT routing): Allow PPTP through ISA Firewall (part of Access Policy).
31. To allow remote users to call your ISA Server via VPN (supports IPSec and PPTP):
    * Allow VPN connections (right-click

on Network Configuration)
   * This automatically configures RRAS and creates packet filters. It also configures RRAS to try for the most secure connection possible.

32. To link two ISA Server-equipped LANs together via VPN, use the VPN Wizard at each end (the second with a file generated from first):

Configuring, Managing, and Troubleshooting Policies and Rules

33. The Enterprise policy may be the only policy. It may be further tightened by array policies, or it may be left unused, allowing array policies only.
34. Always create policy elements before creating the policy itself.
35. Web publishing:
   * Requires an inbound Web request listener on port 80.
   * Requires a destination set pointing to the Web server (not to the external clients).
   * Requires host headers.
   * Requires a publishing rule to redirect traffic with the host header to the published Web server.
36. Dealing with SSL Traffic:
   * Install a certificate on the ISA Server.
   * Enable SSL listeners on port 443; redirect traffic to the internal Web server.
37. Web publishing rules are processed from top to bottom. The default rule (drop incoming packets) should remain at the bottom of the list; otherwise, rules after it will not be processed.
38. Web publishing rules work with ISA Server in cache or integrated mode.
39. Server publishing rule order is unimportant.
40. Protocol rule order is unimportant.
41. Server publishing rules work with ISA Server in firewall or integrated mode.
42. SecureNAT clients may be restricted by IP address, but not by user or group.

H.323 Gatekeeper

43. Gatekeeper is an extra service included with ISA Server.
44. The H.323 Gatekeeper maintains a database of registered H.323 clients, and maps their alias names to IP addresses.
45. The H.323 Gatekeeper service is needed:
   * To accept incoming calls to clients by using their alias names.
   * To connect dissimilar networks and provide translation services.
46. If clients will be using H.323 applications only on the internal network, install the Gatekeeper service and configure a DNS service location resource record.
47. If H.323 applications will be used over the Internet, install the Gatekeeper service, configure a DNS resource record, enable the H.323 protocol filter, and configure an allow protocol rule for the H.323 protocol.

Deploying, Configuring, and Troubleshooting the Client Computer

48. Client types:
   * SecureNAT - Any protocols are allowed if defined.
   * Firewall - Any protocols are allowed if defined.
   * Web Proxy - HTTP 1.1 browser or newer only.
49. Installation:
   * Automated from existing DHCP server
   * Automated from DNS server
   * Automated via Group Policy
50. MSPLAT.TXT copied to Firewall clients periodically from the ISA Server for client awareness of the LAT.

Monitoring, Managing, and Analyzing ISA Server Use

51. Set up “Load Factors” for array
   * Logging (optimize logging speed)
   * Logging to file
   * Logging to Database with Open Database Connectivity (ODBC)
   * Enable Intrusion Detection
   * Logs unavailable for approximately 24 hours unless “immediate” is chosen