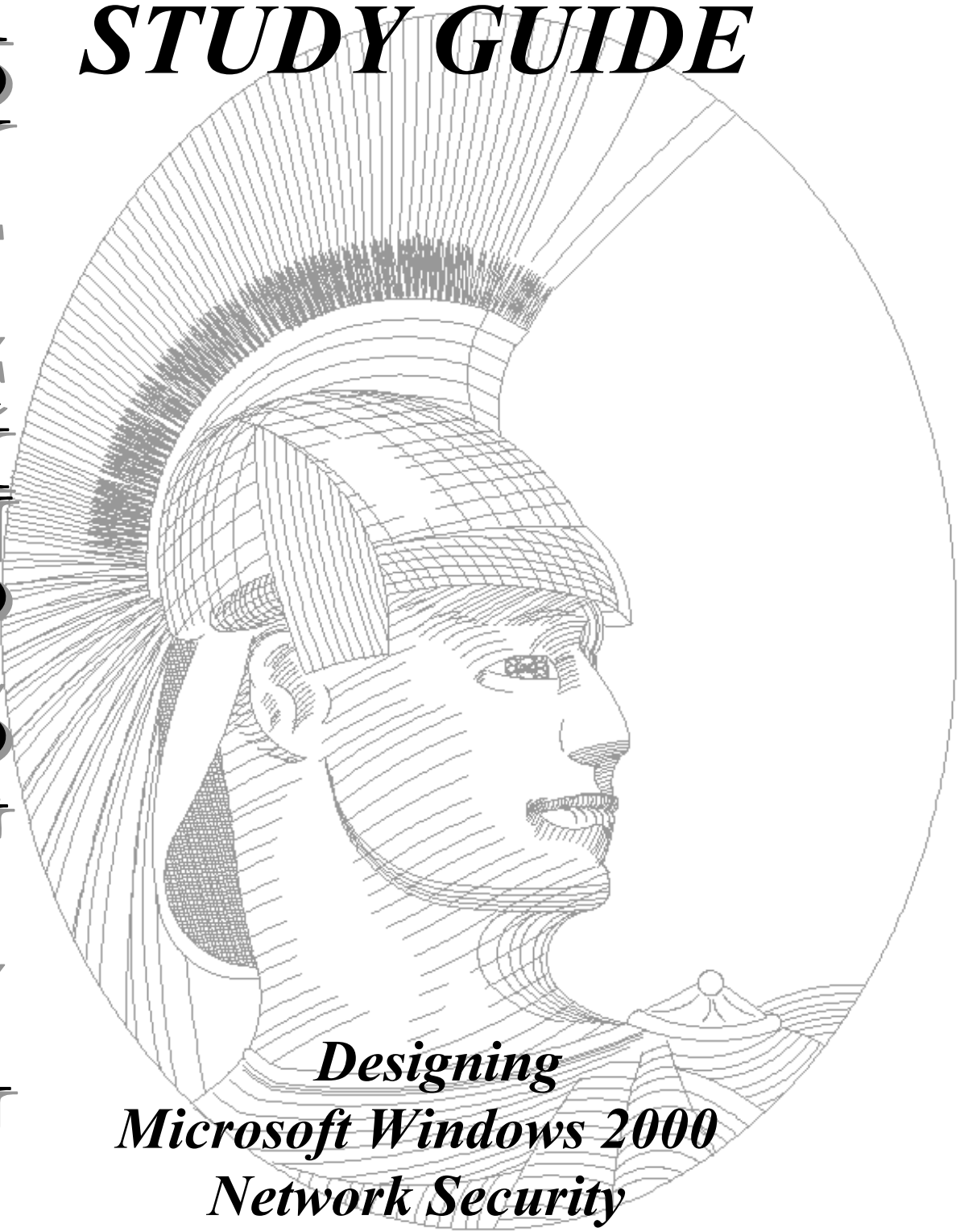


ASU
S
H
G
O
H
O
Z
O
H
I
S
D
S
A

MCSE *STUDY GUIDE*



Designing
Microsoft Windows 2000
Network Security
Exam 70-220

Edition 2

Congratulations!!

You have purchased a *Troy Technologies USA* Study Guide.

This study guide is a selection of questions and answers similar to the ones you will find on the official Designing Microsoft Windows 2000 Network Security MCSE exam. Study and memorize the following concepts, questions and answers for approximately 10 to 12 hours and you will be prepared to take the exams. We guarantee it!

Remember, average study time is 10 to 12 hours and then you are ready!!!

GOOD LUCK!

Guarantee

If you use this study guide correctly and still fail the exam, send your official score notice and mailing address to:

Troy Technologies USA
8200 Pat Booker Rd. #368
San Antonio, TX 78233

We will gladly refund the cost of this study guide. However, you will not need this guarantee if you follow the above instructions.

This material is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this material, or any portion thereof, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

© Copyright 2000 Troy Technologies USA. All Rights Reserved.
<http://www.troytec.com>

Table of Contents

Analyzing Technical Requirements	1
EVALUATING THE EXISTING AND PLANNED TECHNICAL ENVIRONMENT	1
Analyzing Company Size and User and Resource Distribution	1
Assessing Available Connectivity and Bandwidth	2
Performance Requirements	2
Analyzing Data and System Access Patterns.....	2
Analyzing Network Roles and Responsibilities.....	2
Analyzing Security Considerations	3
ANALYZING THE IMPACT OF SECURITY DESIGN	3
Assessing Existing Systems and Applications.....	3
Identifying Upgrades and Rollouts	3
Analyze Technical Support Structure	3
Analyze Existing and Planned Network and Systems Management.....	3
Analyzing Security Requirements.....	4
DESIGNING A SECURITY BASELINE	4
DOMAIN CONTROLLERS BASELINE	4
OPERATIONS MASTERS	4
APPLICATION SERVERS	4
FILE AND PRINT SERVERS.....	5
RAS SERVERS	5
DESKTOP COMPUTERS.....	5
KIOSKS	6
IDENTIFYING REQUIRED LEVELS OF SECURITY.....	6
PRINTER.....	6
INTERNET ACCESS	6
DIAL-IN ACCESS.....	6
Designing a Windows 2000 Security Solution	7
DESIGNING AND AUDIT POLICY.....	7
DESIGNING A DELEGATION OF AUTHORITY STRATEGY	7
DESIGNING THE PLACEMENT AND INHERITANCE OF SECURITY POLICIES.....	7
DESIGNING AN ENCRYPTING FILE SYSTEM STRATEGY	7
DESIGNING AND AUTHENTICATION STRATEGY	8
AUTHENTION METHODS.....	8
DESIGNING A SECURITY GROUP STRATEGY	9
DESIGNING A PUBLIC KEY INFRASTRUCTURE	10
CERTIFICATE AUTHORITY HIERARCHIES.....	10
CERTIFICATE SERVER ROLES	11
INTEGRATE WITH THIRD-PARTY CAs	11
MAPPING CERTIFICATES	11
DESIGN WINDOWS 2000 NETWORK SERVICES SECURITY	12
DNS SECURITY	12
RIS SECURITY	14

SNMP	14
TERMINAL SERVICES	15
Providing Secure Access Between Networks	16
NAT AND INTERNET CONNECTION SHARING	16
ROUTING AND REMOTE ACCESS SERVICES	16
INTERNET AUTHENTICATION SERVICES	17
RADIUS Protocol	17
VIRTUAL PRIVATE NETWORKING	17
VPN Connections	18
Tunneling Protocols	18
SECURE ACCESS TO PUBLIC NETWORKS	18
SECURE ACCESS TO PRIVATE NETWORK RESOURCES	19
SECURE ACCESS BETWEEN PRIVATE NETWORKS	19
Security and the LAN	19
Securing WAN Access	20
DESIGN WINDOWS 2000 SECURITY FOR REMOTE ACCESS USERS	20
Designing Security for Communication Channels	20
SMB SIGNING	20
IPSEC	21
IPSec Encryption Scheme Design	22
Designing IPSec Management	22
Designing Negotiation Policies and Encryption Schemes	22
Design security policies.	23
Design IP filters	23
Predefined Policies	25

Designing Windows 2000 Network Security Concepts

Analyzing Technical Requirements

You must assess how directory services will impact the technical aspects of the network infrastructure. These aspects include performance and stability. You should evaluate the company's existing and planned technical environment. You should attempt to predict the impact of the Active Directory design on the existing and planned technical environment. The following factors are critical:

- Available connectivity between the geographic locations of sites
- Available network bandwidth and latency
- Company size
- Existing and planned network and systems management
- Existing methods for accessing data and systems
- Network roles and responsibilities
- Performance requirements
- Technical support structure
- User and resource distribution

EVALUATING THE EXISTING AND PLANNED TECHNICAL ENVIRONMENT

Areas you will want to consider in assessing the existing technical environment and developing a plan for the transition to Windows 2000 include:

- Proactive training of users before the rollout of the new operating system.
- Training of all technical personnel on the new operating system and how to use the directory services.
- Written documentation to aid in assisting users with common problems, and documenting reported problems.

Analyzing Company Size and User and Resource Distribution

The geographic scope plays an important part of designing your Directory Services. You must take into account the size and geographic location of all parts of the company. Analysis should also include the size and distribution of users, both internal and external. Resource allocation for peripherals and server access must be determined. Connectivity issues across geographic locations and within sites must also be documented. Identify if users are connecting for authentication only or for the entire session as with a Terminal Server.

Assessing Available Connectivity and Bandwidth

You must work closely with the network operations team to assess network connectivity and performance based on reliability, capacity, and latency. Reliability is how dependable the network link is. Capacity is the ability of the connection to transfer data packets. Bandwidth is the theoretical capacity of the network connection. Latency, or delay, is the delay of how long it takes to get data from one point to another.

Performance Requirements

To obtain peak performance, you must assess performance requirements, and create a baseline from which to judge future modifications. You must determine peak utilization, the type of circuits used, application requirements, and resource conflicts. During this analysis, identify any bottlenecks or potential performance hazards.

Analyzing Data and System Access Patterns

In your analysis, you need to determine if all resources are centralized or remotely disbursed. Frequently used resources should be across a highly reliable connection. You must determine if users should go through a firewall, or if they need to use encryption. Authentication can be accomplished through the use of the following:

CHAP	Challenge Handshake Authentication Protocol. Does not use clear-text passwords.
EAP	Extensible Authentication Protocol. The client and the server negotiate the protocol that will be used. Protocols include one-time passwords, username / password combinations, or access tokens.
MS-CHAP	Microsoft Challenge Handshake Authentication Protocol. Requires the client to be using a Microsoft Operating System (Version 2), or other compatible OSs (Version 1).
PAP	Password Authentication Protocol. Uses a plain-text password authentication method and should only be used if clients cannot handle encryption.
SPAP	Shiva Password Authentication Protocol. For backward-compatibility and is not favored for new installations.

Analyzing Network Roles and Responsibilities

Administrative roles are predefined by the operating system with additional responsibilities above the normal user. Administrative type roles include Backup Operator, Server Operator, Print Operator, and Account Operator. Service roles run as services, without user interaction, in the operating system. User roles include the right to logon and use network resources. Other roles include being an application, a group, or owner.

Analyzing Security Considerations

The most effective means of implementing security with Windows 2000 clients is through the use of Group Policies. You must analyze security considerations and provide information about access to data and resources, password policies, security protocols (IPSec), disaster recover, and authentication. You must analyze what are the needs of the organization, and what operating systems does the organization support. In the analysis, ensure that all potential solutions will not conflict with existing third-party tools and applications.

ANALYZING THE IMPACT OF SECURITY DESIGN

Assessing Existing Systems and Applications

To provide high levels of security, Windows 2000 provides the following security features: IPSec, L2TP, Kerberos, an Encrypting Files system (EFS), public key infrastructure, RADIUS, smart card support, and security groups. You need to understand current server applications that may require service packs or patches. You should compile a list of all routers, modems, and remote access servers. This list should include BIOS settings, peripheral device configurations, and driver versions. Determine if current hardware or software is not working due to security reasons. Examine non-Windows NT DNS servers for their implementation of dynamic registration and service (SRV) resource records.

Identifying Upgrades and Rollouts

Identify upgrades and rollouts that are currently in progress. Inquire about and document anything in a planning stage.

Analyze Technical Support Structure

You must determine what kind of support is available, how it's managed, and the level of support staff expertise is.

Analyze Existing and Planned Network and Systems Management

In analyzing the network and systems management, you must document existing policy and guidelines on security. This will help you to determine requirements for appropriate network usage. You must indicate Internet access, all users and their purpose for the Internet access. Document existing policies in place regarding partner access to company networks, whether they are able to access the entire work as recognized users or as anonymous users. Document if encryption and security standards in place or planned, password standards, domain structure, and trust relationships. Identify what security protocols are implemented on the network, (SSL, IPSec or PPTP). Indicate authentication methods for Internet users, dial-up users, and access across WAN links.

Analyzing Security Requirements

DESIGNING A SECURITY BASELINE

DOMAIN CONTROLLERS BASELINE

A domain controller is a Windows 2000 Server that has been configured using the Active Directory Installation Wizard. All Windows 2000 domain controllers store writeable directories. The domain controller manages authentication, user logon processing, directory searches and storage of directory data. You may choose to have several domains to ensure high availability and fault tolerance. The default installation for Windows 2000 Server and Advanced Server is the standalone server model. Servers may be promoted to domain controller status or may be demoted by running the dcpromo wizard.

OPERATIONS MASTERS

Limiting the role of a domain controller may improve performance. The five operations master roles can be assigned to one or more domain controllers. The roles are schema master, domain naming master, relative ID master, primary domain controller (PDC) emulator, and infrastructure master. There can be only one schema master and one domain naming master in the forest at one time. The schema master controls updates and modifications to the schema. To change the forest schema, you must have access to this domain controller and be a member of the Schema Admins group. The domain naming master is in charge of additions and deletions of domains in the forest and of sites. The domain naming master should be located on a system that also contains the Global Catalog. Three roles are domain-wide. There can be only one PDC emulator, one infrastructure master, and one relative ID master in a domain at one time. The relative ID master allocates relative ID sequences to each domain controller. Each new user, group, or computer in a domain gets a unique security ID composed of a unique domain security ID and a relative ID. The relative ID master operations master is required to move objects within domains using the movetree.exe command. The infrastructure master updates the group-to-user references when group members are changed. The infrastructure master compares its data to the Global Catalog data and requests changes. It then replicates this information to other domain controllers in the domain. The PDC emulator acts as a Windows NT PDC if non-Windows 2000 clients are in the domain, or if Windows NT BDCs are present. It can process password changes and replicate updates to the BDCs. The infrastructure master and the Global Catalog host should not be the same domain controller.

APPLICATION SERVERS

The security baseline settings for application servers will depend on the server applications that are running. If the application meets the specification for the Windows 2000 logo, then all users should be members of the Users group. By default, Windows 2000 assigns some non-administration rights and access. This includes making the Authenticated Users group a

member of the Power Users group for servers. You can remove this setting to further secure servers on which only logo applications are run. If the applications running on the system do not meet the logo requirements, you may have to make all users Power Users to allow them to run the applications. Another way to do this is to use the compatws template.

FILE AND PRINT SERVERS

Baseline settings for file and print servers should be based on usage considerations of the files stored and the printers that it controls. One method of ensuring a measure of security is to set the Unsigned Driver Installation Behavior option to Do Not Allow Installation. Print servers should enable the security option Prevent Users from Installing Printer Drivers.

RAS SERVERS

Remote access permissions and settings include:

Access by the user	Determined by remote access permission for each user account.
Access by policy (native-mode domain)	Set to Control Access through Remote Access Policy to explicit allow, explicit deny, and implicit deny.
Access by policy in (mixed-mode domain)	Control Access Through Remote Access Policy option is not available on the user account. Access is based on matching a user account to the conditions of a policy.

As part of the baseline, you should specify the authentication service used (Windows, RADIUS, EAP) and the resolution of other security issues (use of reversible encrypted password, smart card remote access, certificate-based EAP).

DESKTOP COMPUTERS

Desktop computers are used based on the abilities and duties of their users. Appropriate policies, and templates should be designed based on the role the desktops play. You should set a security baseline for all desktop computers, whether they are laptops, Windows NT-compatible laptops, or secure desktops located in confidential or sensitive areas of the company. Use standard templates and adapt them to the appropriate security policy. Use the hisecws.inf template to develop a special template for laptop computers. The compatws.inf template can be used to assure compatibility with applications that do not meet the Windows 2000 standards. This template is consistent with most legacy applications.

KIOSKS

Kiosks are generally located in public areas, and security is a major concern. Kiosks can include any system used in an open area to look up items, give directions, or provide information. Security can be enhanced by removing keyboards and allow only touch screens, mouse devices, or other pointing devices; and removing external access from modems or the networks. In most cases, a logon will not be required, and data is not stored locally.

IDENTIFYING REQUIRED LEVELS OF SECURITY

PRINTER

Printer permissions are set on the Security tab of the Printer property pages. Printer permissions control who can print, manage a printer, or manage documents. You must identify the role each printer takes, and determine whether you want to restrict printing access to certain printers. These printers include printers that print sensitive or confidential material, or printers that are costly to operate. The Users group is given Print Permission by default. This allows users to connect and print to a printer, pause, resume, restart, and cancel their own documents. You should create a group or choose a user to manage the printer. The Manage Documents permission allows Control Job Settings for All Documents and Pause, Restart, and Delete All Documents. Manage Printer allows a user to Share a Printer, Change Printer Properties, Delete Printers, and Change Printer Permissions. Administrators, Server Operators, and Print Operators groups are given this permission by default.

INTERNET ACCESS

Internet access security can be specified by identifying where access occurs and who has what access permissions. You must identify whether computers have dial-up access via modems, if a proxy server, firewall, or routers are utilized on the network. When using a proxy server, you can control access using Windows 2000 users and groups. Firewalls can be used to both block external access to the network, and server to guard access to the Internet. You should identify the specific type of Internet resource (ftp server, telnet), and identify usage intent. Determine if external users access your network from the Internet, and what servers they should have access to.

DIAL-IN ACCESS

To control dial-in access, you need to restrict the right to even connect to the network. For an Windows NT network, after connecting, resource access can be restricted by setting the ability to access resources on just the RAS server, or throughout the network. In a Windows 2000 network where the RAS server is a Windows 2000 Server, you can restrict access through the Routing and Remote Access console. Access is controlled based on dial-in properties of user accounts and policies which are created and maintained through the Remote Access Policies section. Granular access to resources is controlled by native systems, such as