Cisco Security

Assessment Fact Sheet

Overview	The Cisco Security test measures the candidate's knowledge of network and computer security in a Cisco system. It should cover all aspects of the everyday function for this. Security issues should include those that affect software, hardware, and networking. Designed for experienced IT professionals who have responsibilities surrounding network security and are running a Cisco environment. This test includes the following topics: Appliances, Firewalls, IPS/IDS Management, Secure Network Management, Secure Routing, Security Information, Security Protocols, Security Technologies, VPN Management.

Job Level	Professional
Job Family/Title	Information Technology

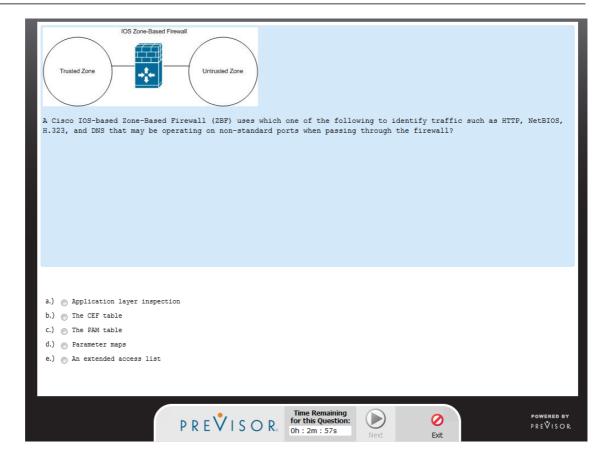| Details		
Average Testing Time (minutes)	27 minutes
Allowed Time (minutes)	90 minutes
Maximum Number of Questions	30 questions
Number of Sittings	One
Designed for Unproctored Environment	Yes
Question Format	Adaptive, Multiple Choice, Skills
Product Category	Brainbench IT

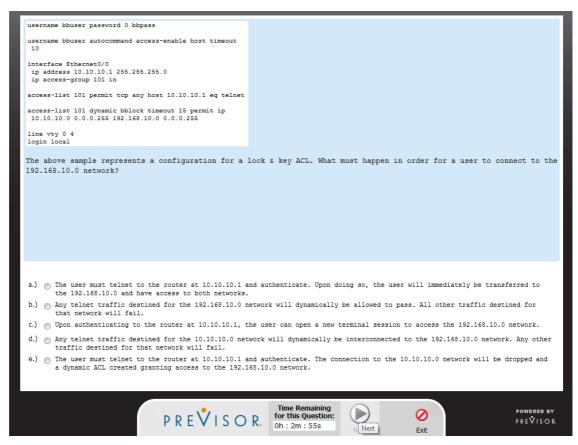**Knowledge, Skills, Abilities and Competencies Measured**

Measures knowledge of the following areas:

- Appliances
- Firewalls
- IPS/IDS Management
- Secure Network Management
- Secure Routing
- Security Information
- Security Protocols
- Security Technologies
- VPN Management

Example Questions

A Cisco IOS-based Zone-Based Firewall (ZBF) uses which one of the following to identify traffic such as HTTP, NetBIOS, H.323, and DNS that may be operating on non-standard ports when passing through the firewall?

a.) ○ Application layer inspection

b.) ○ The CEF table

c.) ○ The PAM table

d.) ○ Parameter maps

e.) ○ An extended access list

Time Remaining for this Question: 0h : 2m : 57s

```
username bbuser password 0 bbpass

username bbuser autocommand access-enable host timeout
 10

interface Ethernet0/0
 ip address 10.10.10.1 255.255.255.0
 ip access-group 101 in

access-list 101 permit tcp any host 10.10.10.1 eq telnet

access-list 101 dynamic bblock timeout 15 permit ip
 10.10.10.0 0.0.0.255 192.168.10.0 0.0.0.255

line vty 0 4
login local
```

The above sample represents a configuration for a lock & key ACL. What must happen in order for a user to connect to the 192.168.10.0 network?

a.) ○ The user must telnet to the router at 10.10.10.1 and authenticate. Upon doing so, the user will immediately be transferred to the 192.168.10.0 and have access to both networks.

b.) ○ Any telnet traffic destined for the 192.168.10.0 network will dynamically be allowed to pass. All other traffic destined for that network will fail.

c.) ○ Upon authenticating to the router at 10.10.10.1, the user can open a new terminal session to access the 192.168.10.0 network.

d.) ○ Any telnet traffic destined for the 10.10.10.0 network will dynamically be interconnected to the 192.168.10.0 network. Any other traffic destined for that network will fail.

e.) ○ The user must telnet to the router at 10.10.10.1 and authenticate. The connection to the 10.10.10.0 network will be dropped and a dynamic ACL created granting access to the 192.168.10.0 network.

Time Remaining for this Question: 0h : 2m : 55s

Example Reports

POWERED BY
PREVISOR

Score Report

Session: 85504797306737

Job ID: 1208	Job Title: Test - Cisco Security - Adaptive
Library Name:	
Started: 11/30/10 4:02 PM	Completed: 11/30/10 4:04 PM
Candidate: **Jean Korn**	Candidate Reference:
Email:	Phone:
Hiring Team: Default Hiring Team (previsor)	
City:	State/Province:

Test: Cisco Security

This report is confidential and its contents are intended to assist in the prediction of an applicant's work behavior. If you would like more information about this interpretive report or other products that PreVisor offers, please contact your account representative.

Score: 2.65
Proficiency Level: Proficient (2.51 - 3.50)
The candidate has mastered the basic concepts of Cisco Security, including:

- Security Protocols
- Security Information
- Secure Network Management

The candidate demonstrates a clear understanding of intermediate Cisco Security concepts, such as:

- Firewalls
- IPS/IDS Management
- Security Technologies