H3C GB0-510

H3C Constructing Small- and Medium-Sized Enterprise Security Networks Certification Questions & Answers

Exam Summary – Syllabus – Questions

GB0-510

H3C Certified Network Engineer for Security (H3CNE-Security)

50 Questions Exam – 600/1000 Cut Score – Duration of 60 minutes

Table of Contents:

Know Your GB0-510 Certification Well:

The GB0-510 is best suitable for candidates who want to gain knowledge in the H3C Security. Before you start your GB0-510 preparation you may struggle to get all the crucial Constructing Small- and Medium-Sized Enterprise Security Networks materials like GB0-510 syllabus, sample questions, study guide.

But don't worry the GB0-510 PDF is here to help you prepare in a stress-free manner.

The PDF is a combination of all **your queries like**-
- What is in the GB0-510 syllabus?
- How many questions are there in the GB0-510 exam?
- Which Practice test would help me to pass the GB0-510 exam at the first attempt?

Passing the GB0-510 exam makes you H3C Certified Network Engineer for Security (H3CNE-Security). Having the Constructing Small- and Medium-Sized Enterprise Security Networks certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

H3C GB0-510 Constructing Small- and Medium-Sized Enterprise Security Networks Certification Details:

Exam Name	H3C Constructing Small- and Medium-Sized Enterprise Security Networks
Exam Code	GB0-510
Exam Price	$165 USD
Duration	60 minutes
Number of Questions	50
Passing Score	600/1000
Recommended Training	**Constructing Small- and Medium-Sized Enterprise Security Networks**
Exam Registration	**PROMETRIC**

Sample Questions	H3C GB0-510 Sample Questions
Practice Exam	H3C Certified Network Engineer for Security (H3CNE-Security) Practice Test

GB0-510 Syllabus:

Section	Weight
Overview of network security	- Fundamental of TCP/IP protocol: OSI model, layered structure of TCP/IP model, TCP three-way handshake, transmission layer protocol, etc. - TCP/IP protocol security: IPv4 potential hazard, common security risks of TCP/IP protocol stack, route interception, MAC spoofing, IP spoofing attack, Smurf attack, IP scanning attack, port scanning attack, TCP Denial of Service (DoS), WEB attack, etc. - Network threats: Active attacks, passive attacks, etc.
Basic firewall technology	- Firewall development and technical evolution: firewall introduction, categorizing, and technical evolution, etc. - Basic firewall functions: routing & switching, NAT, reasons for attack prevention, forms and principles of attacks, device configuration for attack protection, principle and operation patterns of dual hot-standby, log review, etc. - Firewall performance metrics: throughput, latency, new connections, concurrent connections, etc. - Firewall networking approaches: principle of two-layer mode, principle of three-layer mode, firewall management, firewall management configuration, file management, upgrade, license management, basic firewall configuration process, etc.
Firewall user management	- AAA technology principle: AAA introduction, AAA certification approach, RADIUS certification, RADIUS message format, RADIUS attributes, RADIUS configuration, HWTACACS certification, HWTACACS configuration, LDAP certification, LDAP configuration, etc. - Firewall user sorting: users for device management, and users for network access - Firewall user management and application: domain-based user management, ISP domain-based AAA realization, local user configuration, local user group configuration, local certification and permission allocation of users for management, RADIUS certification and permission allocation of users for access, certification and permission allocation of users for network operation

Section	Weight
Firewall security policy	- Packet filtering technology: definition of packet filtering, ACL categorizing, matching sequence of ACL rules, packet filtering configuration task, basic ACL configuration, advanced ACL configuration, layer 2 ACL configuration, ACL packet filtering on interfaces, etc. - Security domain: definition of security domain, relation of security domain and interface, precautions for security domain configuration, security domain configuration task, display of security domain, etc. - Firewall forwarding principle: flow and session, creation of session, session entry and long connection, session management configuration, message forwarding process, etc. - Firewall security policy: definition of firewall security policy, development of security policy, advantages and rules of security policy, filter conditions and matching sequence of rules, security policy process, security policy configuration tasks, configuration address object group, security policy configuration, etc.
Network address conversion technology	- NAT overview: NAT technical background, public and private addresses, NAT technology principle, NAT terminology, NAT categories, advantages and disadvantages of NAT technology, etc. - Dynamic NAT: principle and realization of dynamic NAT (NO-PAT mode), dynamic NAT (NO-PAT mode) configuration, principle and realization of dynamic NAT (PAT mode), dynamic NAT (PAT mode) configuration, principle and realization of dynamic NAT (Easy IP mode), dynamic NAT (Easy IP mode) configuration, etc. - Internal server: principle of internal server, realization of internal server, internal server configuration, etc. - Static NAT: principle of static NAT, realization of static NAT, static NAT configuration, etc. - NAT ALG function: principle of NAT ALG, realization of NAT ALG.
Principle and configuration of VPN	- VPN overview: it includes key conceptual terms of VPN, VPN classification, key VPN technology overview, etc. - GRE VPN: GRE packaging format, GRE VPN operation principle, method of GRE passing through NAT, GRE VPN configuration under command line, GRE VPN configuration under WEB, etc. - L2TP VPN: concepts and terms of L2TP, L2TP topology, L2TP protocol packaging, L2TP protocol operation and multiple instances, L2TP configuration under command line,

Section	Weight
	L2TP configuration under WEB, etc. - IPSec VPN: concepts and terms of IPSec VPN, IPSec VPN structure, AH protocol, ESP protocol, relation of IKE and IPSec, methods of IPSec VPN passing through NAT, IPSec VPN configuration under command line, IPSec VPN configuration under WEB, IPSec troubleshooting - SSL VPN: evolution of SSL protocol, SSL work model and structure, recording layer in SSL protocol, SSL handshake protocol, functions and realization of SSL VPN, SSL VPN configuration, etc.
DPI technology	- DPI technology background: security threats, definition of DPI, DPI feature library, DPI business, basic DPI operation principles, etc. - DPI technology principle: IPS technology, IPS features, IPS actions, anti-virus technology, features and actions of virus, URL filter, filter rules, rule matching approaches, file filter technology, data filter features, etc. - DPI technology configuration: basic DPI configuration, License application, feature library upgrade, IPS configuration, anti-virus configuration, URL filter configuration, etc.
Application control technology	- Application control technology overview: application recognition challenges - Application filter: precise application recognition, refined application authorization, ACG gateway application recognition and review principle, application review configuration, etc. - Bandwidth management: concept of bandwidth management, global work load control, bandwidth utilization, matching principle of bandwidth management, bandwidth management configuration, etc. - Log report: application work load analysis, log type, log content output, website visit log, application review log, log analysis and management platform, in-depth data exploration, etc. - Users and verification: user identity discovery, anonymous users, local users, verified on WeChat, verification policy, etc.

H3C GB0-510 Sample Questions:

Question: 1

Which of the following are key VPN technologies?

(Select all that apply)

a) GRE
b) FTP
c) L2TP
d) SMTP
e) IPSec
f) HTTP

Answer: a, c, e

Question: 2

The principle and operation patterns of _____ provide fault tolerance by ensuring seamless operation in case of a failure in one firewall device.

a) Load balancing
b) Port forwarding
c) Intrusion Detection System (IDS)
d) Dual hot-standby

Answer: d

Question: 3

Firewall user management can be domain-based, allowing different domains to have their own user databases and authentication rules. This approach is commonly used in _____ environments.

a) Local network
b) Home automation
c) ISP domain-based
d) Social media

Answer: c

Question: 4

In a firewall, what types of users can be configured for device management?

(Select all that apply)

a) Local users
b) Domain-based users
c) ISP domain-based users
d) Network-based users

Answer: a, b, c

Question: 5

What does AAA stand for in the context of network security?

a) Advanced Application Authorization
b) Authentication, Authorization, and Accounting
c) Access Allocation and Accounting
d) Application Access Approval

Answer: b

Question: 6

Which of the following are elements of AAA certification approaches? (Select all that apply)

a) RADIUS certification
b) Firewall performance metrics
c) HWTACACS certification
d) LDAP configuration

Answer: a, c

Question: 7

How are ACLs (Access Control Lists) categorized in packet filtering technology?

a) By source IP address
b) By packet type
c) By matching sequence
d) By source and destination ports

Answer: c

Question: 8

In GRE VPN, what is the purpose of the GRE packaging format?

(Select all that apply)

    a) To encapsulate data packets
    b) To encrypt data
    c) To compress data
    d) To establish tunnels

Answer: a, d

Question: 9

How can user identity discovery be achieved in Application Control Technology?

(Select all that apply)

    a) Anonymous user login
    b) Local user authentication
    c) Verification through WeChat
    d) Facial recognition

Answer: b, c

Question: 10

Firewall throughput is a metric that measures:

    a) The amount of data a firewall can process per unit of time
    b) The time taken to establish a connection
    c) The number of firewall rules in place
    d) The size of the firewall's log files

Answer: a

Study Guide to Crack H3C Constructing Small- and Medium-Sized Enterprise Security Networks GB0-510 Exam:

- Getting details of the GB0-510 syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the GB0-510 exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the H3C provided training for GB0-510 exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the GB0-510 sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on GB0-510 practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for GB0-510 Certification

Make NWExam.com your best friend during your H3C Constructing Small- and Medium-Sized Enterprise Security Networks exam preparation. We provide authentic practice tests for the GB0-510 exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual GB0-510 exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the GB0-510 exam.

Start Online practice of GB0-510 Exam by visiting URL
https://www.nwexam.com/h3c/gb0-510-h3c-constructing-small-and-medium-sized-enterprise-security-networks-h3cne-security