

Comparing the NGX Certified Professional 1.0 and 1.1 exams:

Exam	156-215	156-215.1
Pre-requisites	None	None
Training Document	Check Point Security Administration NGX I version 1.0 using document # DOC-VPN-01-S-NGX, revision # RSNGX001	Check Point Security Administration NGX I version 1.1 - document # DOC-VPN-01-S-NGX-1.1, revision # RSNGX001.1
Objectives	<ul style="list-style-type: none"> • Show how VPN-1 NGX components and Check Point's Secure Virtual Network Architecture protect critical information assets. • Create rules and modify a Security Policy's properties. • Use private IP-address allocation and unregistered internal addressing schemes, to overcome IP addressing limitations. • Use monitoring tools to track, monitor, and account for all connections logged by Check Point components. • Protect organizations from known network attacks and entire categories of emerging or unknown attacks, using SmartDefense. • Distribute content security to Security Gateways, screen URLs and block suspicious Web data, and provide auditing capabilities and detailed reports. • Verify the identity of users logging in to VPN-1 NGX, using VPN-1 NGX authentication schemes. • Implement LDAP and integrate it with VPN-1 NGX SmartCenter Server. • Configure VPN's, using IKE encryption and Check Point's simplified VPN setup. • Back up critical files and directories, for availability and timely recovery of Security Gateways and SmartCenter Servers. 	<ul style="list-style-type: none"> • Create rules and modify a Security Policy's properties. • Use private IP-address allocation and unregistered internal addressing schemes, to overcome IP addressing limitations. • Use monitoring tools to track, monitor, and account for all connections logged by Check Point components. • Protect organizations from known network attacks and entire categories of emerging or unknown attacks, using SmartDefense. • Verify the identity of users logging in to VPN-1 NGX, using VPN-1 NGX authentication schemes. • Implement LDAP and integrate it with VPN-1 NGX SmartCenter Server. • Back up critical files and directories, for availability and timely recovery of Security Gateways and SmartCenter Servers. • Show how VPN-1 NGX components and Check Point's Secure Virtual Network Architecture protect critical information assets. • Use advanced NGX features to minimize the information-security management burden, when working with objects and rules • Compare and contrast common encryption methods
Number of questions	67	70
Length	90 min	90 min
Exam type	Conventional Multiple-choice	Conventional Multiple-choice

Exam	156-315	156-315.1
Pre-requisites	156-215	156-215.1
Training Document	Check Point Security Administration NGX II version 1.0 using document # DOC-VPN-02-S-NGX, revision # RSNGX002	Check Point Security Administration NGX II version 1.1 - document # DOC-VPN-02-S-NGX-1.1, revision # RSNGX002.1
Objectives	<ul style="list-style-type: none"> • Use NGX tools to install NGX on Windows Server 2003 and SecurePlatform. • Use NGX tools to upgrade to NGX, from VPN-1/FireWall-1 NG or VPN-1 NG with Application Intelligence. • Use advanced NGX features to minimize the information-security management burden, when working with objects and rules • Use the fw monitor, fw ctl pstat, and cpinfo commands to debug and troubleshoot NGX issues • Given a variety of Check Point QoS configurations, determine how to allocate bandwidth • Configure NGX to allow VoIP traffic to pass through a corporate Security Gateway • Identify different modes in ClusterXL configuration, and configure ClusterXL VPN • Configure a Policy Server and SecureClient Rule Base, a route-based VPN, and dynamic VPN routing 	<ul style="list-style-type: none"> • Distribute content security to Security Gateways, screen URLs and block suspicious Web data, and provide auditing capabilities and detailed reports. • Configure VPN's, using IKE encryption and Check Point's simplified VPN setup. • Use NGX tools to install NGX on Windows Server 2003 and SecurePlatform. • Use NGX tools to upgrade to NGX, from VPN-1/FireWall-1 NG or VPN-1 NG with Application Intelligence. • Use the fw monitor, fw ctl pstat, and cpinfo commands to debug and troubleshoot NGX issues • Given a variety of Check Point QoS configurations, determine how to allocate bandwidth • Configure NGX to allow VoIP traffic to pass through a corporate Security Gateway • Configure a Policy Server and SecureClient Rule Base, a route-based VPN, and dynamic VPN routing • Identify different modes in ClusterXL configuration, and configure ClusterXL VPN
Number of questions	57	70
Length	90 min	90 min
Exam type	Conventional Multiple-choice	Conventional Multiple-choice
Exam	156-915	156-915.1
Pre-requisites	CCSE NG	CCSE NG
Training Document	Check Point Accelerated CCSE Student Handbook NGX" version 1 using document # DOC-VPN-ACCEL-CCSE-S-NGX, revision # RSNGX001	Check Point Accelerated CCSE Student Handbook NGX" version 1.1 using document # DOC-VPN-ACCEL-CCSE-S-NGX-1.1, revision # RSNGX001.1
Objectives	<ul style="list-style-type: none"> • Create rules and modify a Security Policy's properties. 	<ul style="list-style-type: none"> • Use NGX tools to upgrade to NGX, from VPN-1/FireWall-1 NG or

	<ul style="list-style-type: none"> • Use private IP-address allocation and unregistered internal addressing schemes, to overcome IP addressing limitations. • Use monitoring tools to track, monitor, and account for all connections logged by Check Point components. • Distribute content security to Security Gateways, screen URLs and block suspicious Web data, and provide auditing capabilities and detailed reports. • Implement LDAP and integrate it with VPN-1 NGX SmartCenter Server • Configure VPN's, using IKE encryption and Check Point's simplified VPN setup. • Back up critical files and directories, for availability and timely recovery of Security Gateways and SmartCenter Servers. • Use NGX tools to install NGX on Windows Server 2003 and SecurePlatform. Use NGX tools to upgrade to NGX, from VPN-1/FireWall-1 NG or VPN-1 NG with Application Intelligence • Use advanced NGX features to minimize the information-security management burden, when working with objects and rules • Use the fw monitor, fw ctl pstat, and cpinfo commands to debug and troubleshoot NGX issues • Given a variety of Check Point QoS configurations, determine how to allocate bandwidth • Configure NGX to allow VoIP traffic to pass through a corporate Security Gateway • Identify different modes in ClusterXL configuration, and configure ClusterXL VPN • Configure a Policy Server and SecureClient Rule Base, a route-based VPN, and dynamic VPN routing 	<p>VPN-1 NG with Application Intelligence</p> <ul style="list-style-type: none"> • Use NGX tools to install NGX on Windows Server 2003 and SecurePlatform • Work with Security Policy rules and NGX objects, using NGX object-cloning and Database Revision Control features • Use VPN-1 SecuRemote/SecureClient to configure remote access • Use monitoring tools to track, monitor, and account for all connections logged by Check Point components • Implement LDAP, and integrate it with NGX SmartCenter Server • Given a variety of Check Point QoS configurations, determine how to allocate bandwidth • Identify features and limitations of Check Point High Availability solutions
Number of questions	70	80

Length	90 min	90 min
Exam type	Conventional Multiple-choice	Conventional Multiple-choice