Hewlett Packard Enterprise

Configuring and Deploying HPE VPN Firewalls H3K71S

Learn to manage HPE VPN Firewalls in this 4-day hands-on instructor-led training.

HPE course number	H3K71S
Course length	4 days
Delivery mode	ILT
View schedule, local pricing, and register	**View now**
View related courses	**View now**

Why HPE Education Services?

- IDC MarketScape leader 4 years running for IT education and training*
- Recognized by IDC for leading with global coverage, unmatched technical expertise, and targeted education consulting services*
- Key partnerships with industry leaders OpenStack®, VMware®, Linux®, Microsoft®, ITIL, PMI, CSA, and (ISC)[2]
- Complete continuum of training delivery options—self-paced eLearning, custom education consulting, traditional classroom, video on-demand instruction, live virtual instructor-led with hands-on lab, dedicated onsite training
- Simplified purchase option with HPE Training Credits

Audience

Network administrators, network architects, security consultants, and security systems engineer

Course objectives

Upon successful completion of this course, you should be able to:

- Describe firewall features of the HPE VPN Firewall family and its various deployment modes
- Describe network security components and concepts
- Describe security zones and their relationship to Ethernet ports and network interfaces
- Describe security zones and their relationship to Ethernet ports and network interfaces
- Establish client and site-to-site VPNs
- Configure firewall rules
- Implement virtual firewalls
- Use Intelligent Resilient Framework (IRF) and Virtual Router Redundancy Protocol (VRRP) in a high availability configuration
- Interpret logs and statistics
- Resolve common issue

*Realize Technology Value with Training, IDC Infographic 2037, Sponsored by HPE, January 2016

Detailed course outline

Module 1: Introduction	• Welcome to Configuring and Deploying HPE VPN Firewalls • Course Overview • Course Agenda—Day 1 • Course Agenda—Day 2	• Course Agenda—Day 3 • Course Agenda—Day 4 • Prerequisite knowledge • Introductions
Module 2: Product Overview	• Objectives • Main product features • Virtual private network (VPN) • Secure management • Layer 3 routing capabilities • Additional security features • Firewall application at the enterprise egress • Firewall and VPN application for SMB • Firewall and VPN application for SOHO users • Firewall and VPN backup application for branch offices • HPE VPN firewall products • HPE VPN firewall appliances • HPE VPN FW appliances—Hardware and performance • HPE U200 Unified Threat Management (UTM) Appliance Series	• HPE U200 UTMs—Hardware and performance • HPE VPN firewall modules • HPE VPN FW modules: Performance • HPE 5820 VPN Firewall Module (JD255A) • 5820 module: Front panel • HPE 12500 VPN Firewall Module (JC635A) • HPE 10500/7500 Advanced VPN Firewall Module (JD249A) • HPE 9500 VPN Firewall Module (JD245A) • 12500/9500/7500 modules—Front panel • 12500/9500/7500 modules—Front panel • 12500/9500/7500 modules—LEDs • Network security overview—Parallel processing • Network security overview—Control Panel • Summary
Module 3: Security Features	• Objectives • Network security • Recommended firewall features • Isolation and access control: Example using DMZ • Interzone policies • ASPF process • Advantages of ASPF • Stateful packet inspection • TCP state inspection 2-9 • Dynamic channel inspection • Application-level gateway (ALG) • Virtual firewall (VFW) • Traffic delivery to a VFW • VFW in MPLS VPN network • Network address translation (NAT) • NAT modes • NAT—DNS mapping	• NAT—FTP: Active mode, server located on Internet • Virtual private network (VPN) • GRE over IPsec VPN • IPsec and NAT (tunnel mode) • Attack prevention • Embedded anti-attack features • Enabling packet inspection • Web filtering • Enabling policy and configuring thresholds • High availability • ID authentication • Security management • Licensed UTM Services • Real-time anti-virus defense • Spam filtering • URL filtering • Summary
Module 4: Device Management Options	• Objectives • Management options • Command line interface (CLI) • Main CLI views • CLI access options • Debugging options • Preparing the VPN FW for login	• Open Application Platform (OAP) module • Redirecting to the VPN FW module from host device • Resetting the OS of the VPN FW module • Web-based Network Management: Firewall • Management paths for FW module • Web-based Network Management: UTM • Summary
Module 5: File System Management	• Objectives • Files used by the firewall device • Configuration file types • Configuration file contents • Using the CLI to manage configuration files • Using the Web to save the configuration • Using the Web to back up the configuration	• Using the CLI to manage software • Using the Web to manage software • Adjusting the Web Idle Timeout • Using the BootWare menu to upgrade software • Summary • Lab Activity 4: Lab topology • Lab Activity 4 Debrief

Module 6: Security Zones and Interfaces

- Objectives
- Security zones
- Security zone types
- Default security zones
- Security zone preference
- Security zone configuration
- Firewall interface
- Modifying interfaces
- Interface settings
- Creating a new interface
- Add a subinterface
- Virtual 10 Gigabit Ethernet interface (CLI view)
- Add an interface to a security zone: Choose zone
- Add an interface to a security zone: Choose interface
- DHCP server
- Create a dynamic IP address pool
- Static routing
- Summary
- Lab Activity 5: Lab topology
- Lab Activity Preview: Security zones and interfaces
- Lab Activity 5 Debrief

Module 7: Firewall Configuration

- Objectives
- Resources and resource groups
- Resource-oriented management
- Four address resource categories
- Create an IP address subnet resource
- Define starting address and wildcard mask
- Wildcard mask
- Service resources and groups
- Create a service group (1 of 3)
- Create a service group (2 of 3)
- Create a service group (3 of 3)
- Time Range resource
- Create a Time Range resource
- Access control list (ACL)
- ACL classification
- ACL match order
- Create an advanced ACL
- Define an ACL rule (1 of 2)
- Define an ACL rule (2 of 2)
- Interzone policies
- Create an interzone policy
- Choose source and destination zones
- Specify source and destination addresses
- Specify services or service groups
- Specify multiple services or service groups
- Exporting a firewall's resources
- Importing resources to another firewall
- Network address translation (NAT)
- NAT types
- Create a dynamic NAT (Easy IP) policy (1 of 2)
- Create a dynamic NAT (Easy IP) policy (2 of 2)
- Internal server
- Summary
- Lab Activity 6: Lab Topology
- Lab Activity Preview: Firewall configuration
- Lab Activity 6 Debrief

Module 8: Virtual Private Networks (VPN)

- Objectives
- VPN principles
- Virtual private network (VPN)
- Multiple VPN access methods
- IKE
- IKE operation
- IKE modes
- Functions of IKE in IPsec
- IKE overview
- IPsec overview (1 of 2)
- IPsec overview (2 of 2)
- IPsec concepts (1 of 3)
- IPsec concepts (2 of 3)
- IPsec concepts (3 of 3)
- IPsec encapsulation modes
- IPsec authentication algorithms
- IPsec encryption algorithms
- IPsec policy configuration
- IPsec configuration and monitoring tasks
- Site-to-site IPsec VPN configuration example
- FW1—London: ACLs (1 of 2)
- FW1—London: ACLs (2 of 2)
- FW2—Halifax: IKE and IPsec configuration
- FW2—Halifax: Apply policy
- Verify configuration
- View the IPsec security association (SA)
- View IPsec statistics
- CLI verification
- IPsec and NAT (1 of 2)
- IPsec and NAT (2 of 2)
- Lab activity 7-1: Lab topology
- Lab activity Preview: Site-to-site VPN
- Lab Activity 7-1 Debrief
- Virtual private dial-up network (VPDN)
- Typical L2TP application
- L2TP concepts (1 of 2)
- L2TP concepts (2 of 2)
- L2TP tunnel modes and tunnel establishment process
- L2TP configuration and monitoring tasks
- L2TP configuration example
- L2TP configuration: Adding an L2TP group
- L2TP configuration: Adding an ISP domain
- L2TP configuration: Adding a local user
- L2TP configuration: IMC iNode VPN client

	• FW1—London: Static route • FW1—London: IKE peer • FW1—London: IKE proposal • FW1—London: IPsec proposal • FW1—London: IPsec policy • FW1—London: Apply policy • FW2—Halifax: Interface and ACLs	• L2TP configuration: Verification • L2TP configuration: Verification from FW • Summary • Lab activity 7–2: Lab topology • Lab Activity Preview: Client-to-site VPN • Lab Activity 7–2 Debrief
Module 9: Virtual Firewalls	• Objectives • Virtual firewall (VFW) • Virtual firewall features • Virtual firewall application scenarios • Virtual firewalls in routing mode • Virtual firewalls in routing mode with shared zones • Virtual firewalls in transparent mode • Virtual firewall key features • Configuring a virtual device. • Creating a virtual device • Adding an interface to a virtual device • Adding VLANs to a virtual device • Selecting a virtual device • Virtual device configuration example • Virtual device configuration—Network diagram • Config example—Create virtual devices (1 of 2) • Config example—Create virtual devices (2 of 2) • Config example—Create virtual interfaces • Config example—Add interfaces to virtual devices • Config example—Add VLANs to virtual devices • Config example—Create security zones	• Config example—Provide access to the FTP server • Config example—Static NAT, Customer_1 • Config example—Dynamic NAT, Customer_1 • Config example—Check connectivity, Customer_2 • Shared security zones • Isolated security zones of virtual firewalls • Routing mode deployment in a multitenant environment (1 of 3) • Routing mode deployment in a multitenant environment (2 of 3) • Routing mode deployment in a multitenant environment (3 of 3) • Transparent mode deployment • Transparent mode configuration (1 of 4) • Transparent mode configuration (2 of 4) • Transparent mode configuration (3 of 4) • Transparent mode configuration (4 of 4) • Summary • Lab Activity 8: Lab topology • Lab Activity Preview: Virtual firewalls • Lab Activity 8 Debrief
Module 10: IRF Stacking, VRRP, and High Availability	• Objectives • IRF advantages • IRF specifications • IRF topology • Increase port density and expand system processing capability • How IRF simplifies networks (1 of 2) • How IRF simplifies networks (2 of 2) • IRF master election • IRF member ID • Configuration files • Configuration steps (1 of 2) • Configuration steps (2 of 2) • Virtual Router Redundancy Protocol (VRRP) • VRRP master and backups • VRRP group • VRRP load balancing • VRRP priority and mode • VRRP tracking • VRRP configuration through the CLI (1 of 2) • VRRP configuration through the CLI (2 of 2) • VRRP configuration example through Web GUI (1 of 7) • VRRP configuration example through Web GUI (2 of 7)	• VRRP configuration example through Web GUI (3 of 7) • VRRP configuration example through Web GUI (4 of 7) • VRRP configuration example through Web GUI (5 of 7) • VRRP configuration example through Web GUI (6 of 7) • VRRP configuration example through Web GUI (7 of 7) • VRRP • Configure VRRP • Configure stateful failover • Select backup interface(s) • Repeat configuration on the backup VPN FW • High availability and stateful failover configuration (1 of 3) • High availability and stateful failover configuration (2 of 3) • High availability and stateful failover configuration (3 of 3) • IRF stacking with 7500 chassis (1 of 5) • IRF stacking with 7500 chassis (2 of 5) • IRF stacking with 7500 chassis (3 of 5) • IRF stacking with 7500 chassis (4 of 5) • IRF stacking with 7500 chassis (5 of 5) • Summary • Lab Activity Preview: High availability and IRF stacking • Lab Activity 9 Debrief

Module 11: Log Management and Reports	• Objectives • Log management • Syslog • User logging • Flow logging (1 of 2) • Flow logging (2 of 2) • Flow logging configuration items • Flow logging statistics • Session logging	• Log management—Session logging policy • Session logging thresholds • Log report • System log report • Interzone policy log report • User log report • Viewing logs on the VPN FW • Summary
Module 12: Troubleshooting	• Objectives • Troubleshooting the system.xml file • Troubleshooting subinterfaces • Troubleshoot IRF (1 of 2) • Troubleshoot IRF (2 of 2)	• Troubleshoot VRRP • Troubleshoot high availability • Summary • Training from HPE

Learn more at
hpe.com/ww/learnnetworking

Follow us:

c04586704, October 2016, Rev. 1

Hewlett Packard Enterprise