TRAINING HANDBOOK

INCREASE REVENUE AND CUSTOMER VALUE WITH EXCLUSIVE NETWORKS PROFESSIONAL & SUPPORT SERVICES

Exclusive Networks
Alresford House, Mill Lane, Alton, Hampshire, GU34 2QJ
Tel: +44 (0)845 521 7217 or +44 (0)1420 548248
Email: Training@exclusive-networks.com

TRAINING HANDBOOK

INTRODUCTION

Exclusive Networks offers the highest standard of technical education on products and solutions in its portfolio. All courses are delivered by vendor accredited trainers with real world experience and practical insight, providing attendees with tangible capability as well as study book theory. Courses are designed to equip engineers with the skills needed to understand, configure, support, troubleshoot and manage products in their care. Knowledge transfer through the training programme helps both business partners and their customers become more effective in supporting/managing solutions. Exclusive Networks' high levels of accreditation and training credentials speak for themselves, through authorised training endorsements from the vendors in Exclusive Networks' product portfolio.

Exclusive Networks UK operates authorised training centres for:

FORESCOUT. FORTINET. Infoblox NEXT LEVEL NETWORKING

NUTANIX. paloalto NETWORKS THALES

Accredited training can be provided in accordance with the vendor courseware either from Exclusive Networks' training suites, at the customer's premises or a suitable location for all parties. Alternatively, bespoke training courses using selected material from the vendor courseware can be provided where necessary. Both accredited training and bespoke training include instructorled training and hands-on labs. Knowledge transfer sessions are also available which provide instruction and demonstration of customer selected topics.*

All of Exclusive Networks' trainers adopt a 'hands-on' approach, which means they teach course content with real-world practical experience, rather than simply facilitate how to achieve accreditation.

*Knowledge transfer sessions do not include courseware or hands-on labs.

COURSE NAME: Forescout Certified Administrator (FSCA)

DURATION: 4 Days **PRODUCT VERSION:** Forescout Administrator Training and Certification

DESCRIPTION

At Forescout Technologies, we believe customer training is a critical component of a successful solution. Our instructors are highly skilled teachers and technologists who bring a wealth of practical experience to the classroom. As members of our Professional Services team, they are experts at training as well as designing and implementing Forescout platform deployments.

HIGHLIGHTS

Learn from Certified Professionals: FSCA training is taught by Forescout Certified instructors who have years of real-world network security experience.

Hands-On: Learn our best practices by configuring, deploying and maintaining the Forescout platform.

Lab-Focused: Train in a real network environment. Install, configure and troubleshoot the platform in your personal lab simulation.

Flexible and Convenient: Come to us, or we'll come to you. On-site training provides a private learning experience for your team to discuss your unique needs. Our instructors will travel to your preferred location, allowing you to stay at home and save while still achieving strong results.

Pathway to Certification: This course is the first step on the training path to Forescout FSCA Certification. Students learn the theory and fundamentals of Forescout platform administration and should leave the course prepared to attain FSCA certification.

The Pathway to Success: Our instructor-led Forescout Certified Administrator (FSCA) training covers the practical skills of configuring and maintaining the Forescout platform. Classes can be delivered on site, at your facility, or in one of several Training Partner classrooms across the globe.

Standardised: Our FSCA course is based on a pre-defined set of key concepts. Hands on exercises give students a chance to experiment with the tools and practice the concepts covered during classroom sessions.

Flexible: We offer a variety of training options (Forescout-hosted, partner-hosted, at your facility or virtual training). These options help us deliver a training solution that meets your budget, schedule and organisational needs.

CERTIFICATION

Forescout Certified Administrator training is a four-day course featuring instruction as well as hands-on labs in a simulated IT environment. Students learn how to establish security policies using all of our available tools. Students will classify and control assets in a network environment and observe how the Forescout platform monitors and protects an enterprise network. The FSCA course curriculum is listed on the right.

COURSE OUTLINE

Day 1

- Introduction
- Terms and Architecture
- Forescout Platform Installation
- Console Overview

Day 2

- Platform Configuration
- Platform Deployment
- Policy Overview
- Classification

Day 3

- Clarification
- Compliance
- Control
- Forescout Platform Host Management

Day 4

- Forescout Platform Administration
- Inventory, Assets, Reporting Dashboard
- Troubleshooting

+ Course details are subject to change

COURSE NAME: FortiGate Security

DURATION: 3 Days **PRODUCT VERSION:** FortiGate 6.2

DESCRIPTION

The FortiGate Security course combines instructor-led training and interactive labs to build a working knowledge of basic configuration and administration of FortiGate appliances' most commonly used features. Administrative fundamentals such as the Fortinet Security Fabric, firewall policies, NAT, user authentication, logging, certificates, SSL inspection, SSL and dial-up VPNs, and FortiGate's security profiles will provide a solid understanding of how to integrate and maintain basic network security using FortiGate appliances.

TARGET AUDIENCE

The FortiGate Security course is intended for anyone who is responsible for the day-to-day management of the security of a FortiGate appliance. This includes network managers, administrators, installers, sales engineers, systems engineers, professional services engineers (presales and post sales) and technical support professionals.

Anyone planning on taking the FortiGate Infrastructure course is strongly recommended to complete the FortiGate Security course first.

PRE-REQUISITE(S)

- TCP/IP network experience
- Basic understanding of firewall concepts

CERTIFICATION

The FortiGate Security course combined with the FortiGate Infrastructure course is highly recommended to prepare for the NSE 4 exam to achieve Network Security Expert status.

COURSE OUTLINE

Day 1

- Introduction to FortiGate and the Security Fabric
- Firewall Policies
- Network Access Translation
- Firewall Authentication

Day 2

- Logging and Monitoring
- Certificate Operations
- Web Filtering
- Application Control

Day 3

- Antivirus
- Intrusion Prevention and Denial of Service
- SSL-VPN
- Dial-up IPSec VPN
- Data Leak Prevention

+ Course details are subject to change

COURSE NAME: FortiGate Infrastructure

DURATION: 2 Days **PRODUCT VERSION:** FortiGate 6.2

DESCRIPTION

The FortiGate Infrastructure course combines instructor-led training and interactive labs to build a working knowledge of advanced FortiGate networking and security features. This course follows the FortiGate Infrastructure course.

Topics that are covered include features commonly used in complex or larger enterprise/MSSP networks, such as routing, SDWAN, virtual domains, layer 2 switching, site-to-site IPSec VPN, Fortinet Single Sign On, high availability, explicit proxy, and diagnostics.

TARGET AUDIENCE

The FortiGate Infrastructure course is intended for networking and security professionals who are involved in the design, implementation and administration of a network infrastructure using FortiGate appliances. This includes network managers, administrators, installers, sales engineers, systems engineers, professional services engineers (presales and post sales) and technical support professionals.

Anyone planning on taking the FortiGate Infrastructure course is strongly recommended to complete the FortiGate Security course before this course.

PRE-REQUISITE(S)

- Familiarity with all topics presented in the prerequisite FortiGate Security course
- Knowledge of OSI layers
- Good knowledge of firewalling concepts in an IPv4 network

CERTIFICATION

The FortiGate Infrastructure course combined with the FortiGate Security is highly recommended to prepare for the NSE 4 exam to achieve Network Security Expert status.

COURSE OUTLINE

Day 1

- Routing
- Software Defined WAN
- Virtual Domains
- Layer 2 Switching
- Site-to-Site IPSec VPN

Day 2

- Fortinet Single Sign-On
- High Availability
- Web Proxy
- Diagnostics

+ Course details are subject to change

COURSE NAME: FortiAnalyzer

DURATION: 1 Day **PRODUCT VERSION:** FortiAnalyzer 6.0

DESCRIPTION

TThe FortiAnalyzer course combines instructor-led training and interactive labs to build a solid understanding of how to integrate FortiAnalyzer into your network awareness infrastructure. It will provide working knowledge of setting up a FortiAnalyzer, registering supported devices and securing communications between the FortiAnalyzer and devices, managing logs and archiving, and configuring both predefined and customised reports.

Topics that are covered include key features and concepts of FortiAnalyzer, ADOMs, RAID, disk quotas, backing up and restoring log data, content archiving, SQL queries and datasets, designing datasets, charts and custom reports, and generating reports by schedule or on-demand.

TARGET AUDIENCE

The FortiAnalyzer course is intended for networking and security professionals who are involved in the day-to-day management of a FortiAnalyzer appliance and FortiGate security information. This includes network managers, and administrators, however installers, sales engineers, systems engineers, professional services engineers (presales and post sales) and technical support professionals can also benefit from this course.

PRE-REQUISITE(S)

- Familiarity with all topics presented in the FortiGate Security and FortiGate Infrastructure courses
- Knowledge of the SQL 'select' syntax is beneficial

CERTIFICATION

The FortiAnalyzer course combined with the FortiManager course are the recommended training to prepare for the NSE 5 certification exam to achieve Network Security Expert status.

COURSE OUTLINE

Day 1

- Introduction and initial configuration
- Administration and Management
- Device Registration and Communication
- Logging
- Reporting

+ Course details are subject to change

COURSE NAME: FortiManager

DURATION: 2 Days **PRODUCT VERSION:** FortiManager 6.0

DESCRIPTION

The FortiManager course combines instructor-led training and interactive labs to build a solid understanding of the fundamentals of using FortiManager for centralised network administration of many FortiGate devices.

Topics that are covered include deployment strategies using single or multiple ADOMs, workspaces and workflow mode, provisioning templates and scripts, policy packages, dynamic objects, centralised IPSec VPN management, revision history, shared objects, and using the FortiManager as a local FortiGuard Distribution server for managed firewalls.

TARGET AUDIENCE

The FortiManager course is intended for networking and security professionals who are responsible for day-to-day management of many FortiGate devices via the FortiManager platform. This includes network managers, and administrators, however installers, sales engineers, systems engineers, professional services engineers (presales and post sales) and technical support professionals can also benefit from this course.

PRE-REQUISITE(S)

- Familiarity with all topics presented in the FortiGate Security and FortiGate Infrastructure courses
- Knowledge of firewalling concepts in an IPv4 network
- Basic understanding of network management system

CERTIFICATION

The FortiManager course combined with the FortiAnalyzer course are the recommended training to prepare for the NSE 5 exam to achieve Network Security Expert status.

COURSE OUTLINE

Day 1

- Introduction and Initial Configuration
- Administration and Management
- Device Registration
- Device Level Configuration and Installation

Day 2

- Policy and Objects
- Manager Panes
- Diagnostics and Troubleshooting
- Advanced Configuration

+ Course details are subject to change

COURSE NAME: Enterprise Firewall

DURATION: 3 Days **PRODUCT VERSION:** FortiGate 6.0

DESCRIPTION

The Enterprise Firewall course combines instructor-led training and interactive labs to build a working knowledge of how to isolate and fix the most common issues in networks with FortiGate.

Topics that are covered include resolving FortiGate misconfigurations, monitoring traffic passing through FortiGate, optimising FortiGate memory usage, FortiGate diagnostic tools, troubleshooting FortiGate issues, scaling out FortiGate deployments, configuring BGP, OSPF, and Autodiscovery VPN (ADVPN).

TARGET AUDIENCE

The Enterprise Firewall course is intended for networking and security professionals who are involved in the administration and support of a security infrastructure using FortiGate appliances. This includes network managers, administrators, installers, sales engineers, systems engineers, professional services engineers (presales and post sales) and technical support professionals.

Anyone planning to taking Enterprise Firewall course is strongly recommended to complete the Fortigate Security, Fortigate Infrastructure and FortiManager courses before this course

PRE-REQUISITE(S)

- Advanced knowlege of all topics presented in the Fortigate Security andInfrastructure courses
- Knowledge of network protocols
- Knowledge of network security concepts

CERTIFICATION

The Enterprise Firewall course is the recommended training to prepare for the NSE 7 certification exam to achieve Network Security Expert status.

COURSE OUTLINE

Day 1

- Enterprise Firewall Solution Overview
- FortiOS Architecture
- System Troubleshooting
- Traffic and Session Monitoring
- Routing

Day 2

- FortiGuard
- Central Management
- OSPF
- Web Filtering

Day 3

- Intrusion Prevention System
- BGP
- IPSec
- Autodiscovery VPN (ADVPN)

+ Course details are subject to change

COURSE NAME: Core DDI Configuration & Administration (CDCA)

DURATION: 5 Days **PRODUCT VERSION:** NIOS 8.1

DESCRIPTION

The Core DDI Configuration & Administration Course (CDCA) combines instructor-led training and interactive labs to build a working in-depth knowledge of how to configure and manage Infoblox network appliances running Infoblox NIOS operating system.

Network fundamentals such as forward and reverse mapping DNS zones, DNS views; DHCP networks, custom options, ranges and fixed addresses; and visually manage the IP space using IPAM; performing Grid management, including system and protocol level monitoring, remote authentication, and NIOS upgrades all provide a solid understanding of how integrate and maintain Infoblox's Core DDI product. Implementation of advanced NIOS features are also covered including dynamic DNS with TSIG and GSSTSIG, DNSSEC zone signing and validation, DNS Anycast, and DHCP failover.

TARGET AUDIENCE

The CDCA course is intended for anyone responsible for the implementation, administration, operations, maintenance, support, and day-to-day management of an Infoblox Core DDI product. This includes system administrators, network administrators, installers, sales engineers, systems engineers, professional services engineers (presales and post sales), and technical support professionals.

Anyone planning on taking the Core DDI Advanced Troubleshooting course (CDAT) are required to complete this course before attending the CDAT course.

PRE-REQUISITE(S)

Attendees should have either of the following:

- A working knowledge of DNS and DHCP
- Completed the Core DDI Fundamentals e-learning course

CERTIFICATION

The CDAC course includes an exam voucher for the Core DDI Configuration & Administration (CDCA) exam for the Core DDI Configuration & Administration (CDCA) accreditation. The CDCA accreditation certifies essential knowledge of network service protocols and configuration of Infoblox Core DDI product. The CDCA exam can be taken during the course.

COURSE OUTLINE

Day 1

- The Infoblox Grid
- Setting up the Grid
- Grid Manager
- Managing Grid Members
- High Availability

Day 2

- DHCP Service
- DHCP Networks
- DHCP Objects
- Extensible Attributes
- User Accounts
- Scheduled Tasks

Day 3

- DNS Service
- DNS Zones
- DNS Resource Records
- IPAM
- CSV Export and Import

Day 4

- Remote Authentication
- DNS Anycast
- DNSSEC
- NIOS Upgrades
- DNS and Network Views)

Day 5

- Advanced DHCP Options
- DHCP Failover
- Dynamic DNS
- TSIG and GSS TSIG
- Reporting and Analytics

+ Course details are subject to change

COURSE NAME: Core DDI Advanced Troubleshooting (CDAT)

DURATION: 2 Days **PRODUCT VERSION:** NIOS 8.1

DESCRIPTION

The Core DDI Configuration & Administration Course (CDCA) combines instructor-led training and interactive labs to build a working in-depth knowledge of how to configure and manage Infoblox network appliances running Infoblox NIOS operating system.

Network fundamentals such as forward and reverse mapping DNS zones, DNS views; DHCP networks, custom options, ranges and fixed addresses; and visually manage the IP space using IPAM; performing Grid management, including system and protocol level monitoring, remote authentication, and NIOS upgrades all provide a solid understanding of how integrate and maintain Infoblox's Core DDI product. Implementation of advanced NIOS features are also covered including dynamic DNS with TSIG and GSSTSIG, DNSSEC zone signing and validation, DNS Anycast, and DHCP failover.

TARGET AUDIENCE

The CDCA course is intended for anyone responsible for the implementation, administration, operations, maintenance, support, and day-to-day management of an Infoblox Core DDI product. This includes system administrators, network administrators, installers, sales engineers, systems engineers, professional services engineers (presales and post sales), and technical support professionals.

Anyone planning on taking the Core DDI Advanced Troubleshooting course (CDAT) are required to complete this course before attending the CDAT course.

PRE-REQUISITE(S)

- Six months experience supporting Infoblox Core DDI products
- Attendance of Core DDI Configuration & Administration course
- Core DDI Configuration & Administration accreditation status

CERTIFICATION

The CDAT course includes an exam voucher for the Core DDI Advanced Troubleshooting exam to gain the Core DDI Advanced Troubleshooting accreditation. The CDAT accreditation certifies the ability to diagnose and resolve support issues for Infoblox solutions. The CDAT exam can be taken during the course.

COURSE OUTLINE

Day 1

- Infoblox Support
- Troubleshooting
- NIOS Expert Topics
- Grid and Grid Members
- DNS

Day 2

- Dynamic DNS
- DHCP
- Service Failure-Recovery

+ Course details are subject to change

COURSE NAME: NetMRI Configuration and Administration (NMCA)

DURATION: 2 Days **PRODUCT VERSION:** 7.2

DESCRIPTION

The NetMRI Configuration and Administration (NMCA) course combines instructor-led training and interactive labs to build a working knowledge of how to configure, use and manage Infoblox network appliances running NetMRI. The course provides an understanding of the automated collection of network device configuration information, how to use the collected information for configuration and change management, network policy management and automated compliance checks and reports, as well as general configuration and reporting features available in NetMRI.

TARGET AUDIENCE

The NMCA course is intended for anyone who is responsible for the day to day management of an Infoblox Network Automation appliance. This includes network administrators, network engineers and operations staff without experience using Infoblox NetMRI.

PRE-REQUISITE(S)

- A working knowledge of TCP/IP protocols, including SNMP and IP networking.
- A conceptual understanding of fault, configuration, change, and performance management.

CERTIFICATION

The NMCA course includes the option to take the NetMRI Configuration and Administration (NMCA) accreditation exam. The NMCA accreditation exam can be taken during the course.

COURSE OUTLINE

Day 1

- Overview and Installation
- Networking Discovery and Groups
- Virtual Routing and Forwarding
- User Interfaces
- Settings
- Network Explorer

Day 2

- Switch Port Manager
- Network Analysis and Issues
- Configuration Management
- Rules and Policies
- Jobs and Remediation
- Dashboard and Reporting

+ Course details are subject to change

COURSE NAME: BloxOne Threat Defense (B1D)

Infoblox
NEXT LEVEL NETWORKING

DURATION: 3 or 5 Days **PRODUCT VERSION:** NIOS 8.4

DESCRIPTION

The Secure DNS Configuration & Administration (SDCA) course combines instructor-led training and interactive labs to build working knowledge of how to implement, configure, and manage an Infoblox Secure DNS product including the prerequisite knowledge of Infoblox Core DDI products. The course builds a basic knowledge of managing the DNS protocol including forward and reverse mapping DNS zones, and DNS views, before moving onto advanced DNS security related features including Dynamic DNS with TSIG and GSS-TSIG, DNSSEC zone signing and validation, and DNS Anycast. The course builds a baseline working knowledge of how to configure and Infoblox on premise Secure DNS product, including DNS Firewall with ActiveTrust, TIDE and Dossier, Threat Insight and Advanced DNS Protection.

TARGET AUDIENCE

The SDCA course is intended for anyone who is responsible for the implementation, administration, operation, support, or maintenance of Infoblox Secure DNS products. This includes system administrators, network administrators, installers, sales engineers, systems engineers, professional services engineers (presales and post sales) and technical support professionals..

PRE-REQUISITE(S)

The following is required when attending the course:

- Basic understanding of DNS.
- Previous attendance of the Core DDI Configuration and Administration (CDCA) course allows for the option of attending only days 3-5 due to already having the prerequisite knowledge.

CERTIFICATION

The SDCA course includes an exam voucher for the Secure DNS Configuration & Administration (SDCA) accreditation exam for the Secure DNS Configuration and Administration (SDCA) accreditation. The SDCA exam can be taken during the course.

COURSE OUTLINE

Day 1

- Introduction: The Infoblox Grid
- Setting Up the Grid
- Grid Manager
- Managing Grid Members
- Infoblox HA Availability

Day 2

- DNS Services
- DNS Zones
- DNS Resource Records
- DNS Anycast
- DNSSEC
- DNS and Network Views

Day 3

- Reporting: Dashboards
- Reporting: Searches. Reports & Alerts
- DNS Firewall Overview
- Local RPZ and RPZ Rules
- BloxOne Threat Defense RPZ Feeds
- DNS Firewall Monitoring and Reporting

Day 4

- Infoblox TIDE
- Infoblox Dossier
- Dosser API
- Threat Insight Overview
- Configuring Threat Insight
- Threat Insight Monitoring and Reporting

Day 5

- ADP Overview
- ADP Appliance Configuration
- ADP Rulesets, Rules & Profiles
- ADP Monitoring & Reporting

+ Course details are subject to change

COURSE NAME: Nutanix Enterprise Cloud Platform Administration 5.15

DURATION: 4 Days **PRODUCT VERSION:** AOS 5.15

DESCRIPTION

The Nutanix Enterprise Cloud Platform (ECP) Administration 5.15 course combines instructor-led training and interactive labs to build a working knowledge of all tasks that a Nutanix administrator performs on the job. The course walks through the complete process of setting up, configuring, and then maintaining the environment. Basic concepts of the Enterprise Cloud Platform such as racking a Nutanix block, installing and configuring a cluster, and use of a different interface to manage the cluster will be covered. Management of VMs in Acropolis, monitoring cluster health and performance, protecting data and optimising cluster capacity, and performance in-place hypervisor conversion will also be covered along with the use of Nutanix's Prism interface to monitor and manage multiple activities across clusters, review and analyse resource needs, and assess future resource requirements.

TARGET AUDIENCE

The Nutanix Enterprise Cloud Platform Administration course intended for anyone who is responsible for the day to day management, installation, or support of a Nutanix cluster in a datacentre or anyone seeking baseline preparation for the Nutanix Platform Professional (NPP).This includes managers and technical staff seeking more information before making a purchase decision.

PRE-REQUISITE(S)

- Familiarity with traditional virtualisation storage architectures
- Comfort with Unix/Linus command line interface

CERTIFICATION

The ECP is the recommended training to prepare for the Nutanix Platform Professional (NPP) certification.

COURSE OUTLINE

Day 1

- Introduction to the Nutanix Enterprise Cloud Platform
- Administering the Nutanix Cluster
- Configuring the Nutanix Cluster
- User Interfaces

Day 2

- Health Monitoring and Alerts
- Networking
- VM Management
- Distributed Storage Fabric

Day 3

- AHV Workload Migration
- Services
- Business Continuity
- Data Protection

Day 4

- Prism Central
- Concluding the Installation
- Lifecycle Operations

+ Course details are subject to change

COURSE NAME: Firewall 10.0 Essentials: Configuration and Management (EDU-210)

DURATION: 5 Days **PRODUCT VERSION:** PANOS 10.0

DESCRIPTION

The Firewall 10.0 Essentials: Configuration and Management course combines instructor-led training and interactive hands-on labs to build a working knowledge of how to configure and manage Palo Alto Networks® Next-Generation Firewalls.

The five days of training will help to:

- Configure and manage the essential features of Palo Alto Networks Next-Generation Firewalls.
- Configure and manage Security and NAT policies to enable approved traffic to and from zones.
- Configure and manage Threat Prevention strategies to block traffic from known and unknown IP addresses, domains, and URLs.
- Monitor network traffic using the interactive web interface and firewall reports.

TARGET AUDIENCE

Successful completion of this five-day, instructor-led course should enhance the student's understanding of how to configure and manage Palo Alto Networks Next-Generation Firewalls. The course includes hands-on experience configuring, managing, and monitoring a firewall in a lab environment. It is targeted at Security Administrators, Security Engineers, Security Operations Specialists, Security Analysts, and Support Staff.

Anyone planning to attend the Firewall 10.0: Improving Security Posture and Hardening PAN-OS Firewalls (EDU-214), Panorama 10.0: Manage Firewalls at Scale (EDU-220), and Firewall 10.0: Troubleshooting (EDU-330), are strongly recommended to complete the Firewall 10.0: Configuration and Management course before attending those courses.

PRE-REQUISITE(S)

The following is required when attending the course:

- Basic familiarity with networking concepts including routing, switching and IP addressing
- Familiarity with basic security concepts
- Experience with other security technologies (IPS, proxy, and content filtering) is a plus.

CERTIFICATION

The Firewall 10.0 Essentials: Configuration and Management course is the recommended training for taking the Palo Alto Networks Certified Network Security Administrator (PCNSA) exam.

Additionally, the Firewall 10.0 Essentials: Configuration and Management course combined with the Firewall 10.0: Improving Security Posture and Hardening PAN-OS Firewalls (EDU-214) and Panorama 10.0: Manage Multiple Firewalls (EDU-220) courses are the recommended training for anyone planning on taking the Palo Alto Networks Certified Network Security Engineer (PCNSE) certification exam, or any of the Palo Alto Networks® Systems Engineer certifications.

COURSE OUTLINE

Day 1

- Palo Alto Networks Portfolio and Architecture
- Connect to the Management Network
- Manage Firewall Configurations
- Manage Administrator Accounts

Day 2

- Connect to Production Networks
- The Cyber Attack Lifestyle
- Block Threats Using Security and NAT Policies
- Block Packet-and Protocol-Based Attacks

Day 3

- Block Threats from Known Bad Sources
- Block Threats by Identifying Applications
- Maintain Application-Based Policies
- Block Threats using Custom Applications

Day 4

- Block Threats by Identifying Users
- Block Threats by Identifying Devices
- Block Unknown Threats
- Block Threats in Encrypted Traffic

Day 5

- Prevent Stolen Credentials
- Block Threats using Security Profiles
- View Threat and Traffic Information
- Next Steps

+ Course details are subject to change

COURSE NAME: Firewall 10.0: Improving Security Posture and Hardening PAN-OS Firewalls (EDU-214)

DURATION: 3 Days **PRODUCT VERSION:** PANOS 10.0

DESCRIPTION

The Firewall 10.0: Improving Security Posture and Hardening PAN-OS Firewalls course is three days of instructor-led training that will help you to:

- Determine the efficacy of your current security policies
- Develop workflows for managing your security posture
- Identify rule usage across security policy sets
- Modify your existing policy set to implement Security Best Practices
- Monitor network traffic using the interactive web interface and firewall reports
- Utilize tools such as the BPA tool to further understand your environment

Successful completion of this course will assist in maintaining and managing and existing Palo Alto Networks Firewall protected environment, improve non-greenfield environments, and ensure configurations match security best practice.

TARGET AUDIENCE

This course is intended for Security Administrators, Security Engineers, Security Operations Specialists, Security Analysts, and Support Staff.

PRE-REQUISITE(S)

The following is required when attending the course:

- Complete the Firewall 10.0 Essentials: Configuration and Management (EDU-210) or equivalent experience
- Basic familiarity with networking concepts including routing, switching, and IP addressing
- Basic familiarity with networking concepts, including routing, switching, and IP addressing.

CERTIFICATION

Firewall 10.0: Improving Security Posture and Hardening PAN-OS Firewalls (EDU-214) course is a recommended training for taking the Palo Alto Networks Certified Network Security Engineer (PCNSE) exam.

Additionally, the Firewall 10.0 Essentials: Configuration and Management (EDU-210) and Panorama 10.0: Manage Multiple Firewalls (EDU-220) courses are the other recommended training courses for anyone planning on taking the Palo Alto Networks Certified Network Security Engineer (PCNSE) certification exam.

COURSE OUTLINE

Day 1

- Introduction
- Security Profile Revision
- Daily Operations and Maintenance
- Establish Initial Baseline Visibility.

Day 2

- Analyse and Update Security Rules Passing Traffic
- Inbound Security Rules Best Practices and Analysis
- Outbound Security Rules Best Practices and Analysis

Day 3

- Internal Security Rules Best Practices and Analysis
- Administratively Hardening PAN-OS
- Reducing Policy set and Simplification

+ Course details are subject to change

COURSE NAME: Panorama 10.0: Managing Firewalls at Scale (EDU-220)

DURATION: 2 Days **PRODUCT VERSION:** PANOS 10.0

DESCRIPTION

Panorama 10.0: Managing Firewalls at Scale course combines instructor-led training and interactive labs that should help to:

- Learn how to configure and manage the next-generation Panorama Management server
- Gain Experience configuring templates (including template variables) and device groups
- Gain experience with administration, log collection, and logging and reporting
- Become familiar with planning and design considerations for Panorama deployment

Administrators that complete this course will become familiar with the Panorama management server's role in managing and securing the overall network, including Panorama aggregated reporting can provide a holistic view of a network of Palo Alto Networks next-generation firewalls.

TARGET AUDIENCE

The Panorama 10.0: Manage Firewalls at Scale course is intended for security administrators, security operations specialists, security analysts, security engineers, and security architects.

PRE-REQUISITE(S)

- Completion of Firewall 10.0 Essentials: Configuration and Management (EDU-210) or equivalent experience.
- Familiarity with Palo Alto Networks® next generation firewall management, and basic networking concepts including routing, switching, and IP addressing.

CERTIFICATION

The Panorama 10.0: Manage Firewalls at Scale (EDU-220) course combined with Firewall 10.0 Essentials: Configuration and Management (EDU-210) and Firewall 10.0: Improving Security Posture and Hardening PAN-OS Firewalls (EDU-214) courses are the recommended training for anyone planning on taking the Palo Alto Networks® Certified Network Security Engineer (PCNSE) certification exam.

COURSE OUTLINE

Day 1

- Initial Configuration
- Adding Firewalls
- Templates
- Device Groups

Day 2

- Log Forwarding and Collection
- Using Panorama Logs
- Panorama Administrative Accounts
- Reporting
- Troubleshooting

+ Course details are subject to change

COURSE NAME: Cortex XDR 2: Prevention, Analysis and Response (EDU-260)

DURATION: 3 Days **PRODUCT VERSION:** Cortex XDR 2

DESCRIPTION

This course combines instructor-led topics and hands-on lab activities to cover installation and management activities for the following:

- Activate the Cortex XDR instance, create and install Cortex XDR agent packages
- Create security policies and profiles to protect endpoints against multi-stage, fileless attacks that use combinations of malware and exploits
- Behavioural threat analysis, log stitching, agent-provided enhanced endpoint data and causality analysis

They will also learn how to:

- Investigate and triage attacks using the incident management page of Cortex XDR
- Analyse alerts through Causality and Timeline analysis views
- Use API to insert alerts
- Create BIOC rules and search a lead in raw data sets using Cortex XDR Query Builder

TARGET AUDIENCE

The Cortex XDR 2: Prevention, Analysis & Response (EDU-260) course is intended for Cybersecurity analysts and engineers, and security operations specialists. This can also include security engineers and security administrators.

PRE-REQUISITE(S)

The following is required when attending the course:

- Familiarity with the enterprise security concepts

CERTIFICATION

There is to be a new Micro Credential for XDR Analyst test that will complement this course. Release date to be confirmed by Palo Alto Networks.

COURSE OUTLINE

Day 1

- Cortex XDR Family Overview
- Working with Cortex Apps
- Getting Started with Endpoint Protection
- Malware & Exploit Protection

Day 2

- Exceptions and Response Actions
- Behavioural Threat Analysis
- Cortex XDR Rules
- Incident Management

Day 3

- Alert Analysis Views
- Search and Investigate
- Basic Troubleshooting

+ Course details are subject to change

COURSE NAME: Prisma Access SASE Security: Design and Operation (EDU-318)

DURATION: 2 Days **PRODUCT VERSION:** Prisma Access Secure Access Service Edge (SASE)

DESCRIPTION

The Prisma Access SASE Security: Design and Operation (EDU-318) course describes Prisma Access Secure Access Service Edge (SASE) and how it helps organisations embrace cloud and mobility by providing network and network security services from the cloud.

TARGET AUDIENCE

This course is intended for people in the fields of public cloud security and cybersecurity, or for anyone who wants to learn how to secure remote networks and mobile users.

- Security Engineers
- Security Administrators
- Security Operations Specialists
- Security Analysts
- Network Engineers.

PRE-REQUISITE(S)

The following is required when attending the course:

- Participants should have a basic knowledge of cloud computing and the public cloud.
- Participants also must have experience with networking concepts including routing, switching, and IP addressing.
- Participants must have attended the EDU-210- Firewall Essentials and the EDU-220 – Managing Firewalls at Scale courses

CERTIFICATION

Successful completion of this two-day, instructor-led course will help enhance your understanding of how to better protect your applications, remote networks, and mobile users using a SASE implementation. You will get detailed instruction on configuring, managing, and troubleshooting Prisma Access in a production environment.

COURSE OUTLINE

Day 1

- Prisma Access Overview
- Planning and Design
- Activate and Configure
- Security Processing Nodes

Day 2

- Panorama Operations for Prisma Access
- Remote Networks
- Mobile Users
- Tune, Monitor, and Troubleshoot
- Manage Multiple Tenants
- Next Steps

****Wrap in: Professional Service Quick Start from Exclusive Networks****

Exclusive Networks will guide you through the design & deployment of Prisma Access in your environment for up to 1000 remote users, to safely enable remote networks & mobile users in the cloud. This quick start service expedites on boarding activities & shortens your time to value while following best practices.

+ Course details are subject to change

COURSE NAME: Firewall 10.0: Troubleshooting (EDU-330)

DURATION: 3 Days **PRODUCT VERSION:** PANOS 10.0

DESCRIPTION

The Firewall 10.0: Troubleshooting course is a three-day course that will help to:

- Investigate networking issues using firewall tools including the CLI
- Follow proven troubleshooting methodologies specific to individual features
- Analyse advanced logs to resolve various real-life scenarios
- Solve advanced, scenario-based challenges

Successful completion will enhance understanding in troubleshooting the full line of Palo Alto Networks Next-Generation Firewalls by performing hands-on troubleshooting related to configuration and operation of a Palo Alto Networks firewall. It will develop an in-depth knowledge of how troubleshoot visibility over applications, users, and content.

TARGET AUDIENCE

The Firewall 10.0: Troubleshooting (EDU-330) course is intended for security engineers, security administrators, security operations specialists, security analysts, network engineers, and support staff.

PRE-REQUISITE(S)

The following is required when attending the course:

- Completion of Firewall 10.0 Essentials: Configuration and Management (EDU-210) course.
- Strong practical knowledge of routing and switching, IP addressing, and network security concepts.
- Experience of at least six months hands on experience with Palo Alto Networks® firewalls.

CERTIFICATION

The Firewall 10.0: Troubleshooting course is very beneficial for anyone planning on taking the Palo Alto Networks® Certified Network Security Engineer (PCNSE) certification exam and would complete the Instructor-led training for Palo Alto Networks Firewalls.

COURSE OUTLINE

Day 1

- Tools and Resources
- CLI Primer
- Flow Logic
- Packet Captures

Day 2

- Packet-Diagnostics Logs
- Host-Inbound Traffic
- Transit Traffic
- System Services

Day 3

- Certificate Management and SSL Decryption
- User-ID
- GlobalProtect TM
- Support Escalation and RMAs
- Next Steps

+ Course details are subject to change

COURSE NAME: The SafeNet Trusted Access (STA) Certification Course

DURATION: 3 Days **PRODUCT VERSION:** SafeNet Authentication Service Cloud

DESCRIPTION

The three-day course now combines both the SAS Cloud Certification course, which provides the knowledge that is necessary for managing SafeNet Authentication Services in a cloud environment and practical understanding of how to deploy SAS cloud services, and the STA Certification course, which provides the knowledge that is necessary for managing Access Control to cloud application and SAML based services with STA.

TARGET AUDIENCE

The SafeNet Trusted Access (STA) Certification Course is recommended for anyone is responsible for ongoing management, installation or support of a SafeNet Authentication Service cloud portal. This includes network managers, information security managers, systems administrators, installers, sales engineers, system engineers, professional services engineers (presales and post sales) and technical support professionals.

PRE-REQUISITE(S)

There are no pre-requisites for attending the course, however some basic knowledge of the following is beneficial:

- Two factor authentication / Multi factor authentication
- RADIUS and / or SAML
- Windows authentication
- A basic understanding of Active Directory, PKI and Kerberos

CERTIFICATION

The SafeNet Trusted Access (STA) Certification Course is the recommended training for STA engineer certification.

Attendance of the course provides automatic enrolment to the certification exam.

COURSE OUTLINE

Day 1

- Solution Technical Overview
- Supported Authenticators
- On-board and Provisioning
- Role Management

Day 2

- User Synchronisation and Management
- Authentication Agents
- SAML Integration
- Self-Service Portal

Day 3

- Alerts and Reporting
- Tokens Policies and Managements
- Pre-Authentication Rules
- Customisation and Branding
- STA Solution Technical Overview
- STA Console
- STA Applications Integration & SSO
- STA Policy Management

+ Course details are subject to change

For more information about Exclusive Networks Professional & Support Services, please email **Training@exclusive-networks.com**

Exclusive Networks
Alresford House, Mill Lane, Alton, Hampshire, GU34 2QJ
Tel: +44 (0)845 521 7217 or +44 (0)1420 548248
Email: Training@exclusive-networks.com