

Palo Alto Networks Panorama: NGFW Management (Ersatz für EDU-220)

Diese Schulung ist ein spezieller Kurs für Panorama zur zentralen Verwaltung von Firewalls in großem Maßstab. Es werden nicht nur die Merkmale und Funktionen von Panorama vermittelt, sondern auch Anleitungen für das Design eines distributed Firewall-Netzwerks gegeben, das von einem zentralen Standort aus verwaltet wird.

Kursinhalt

- Lernen Sie, wie Sie den Panorama FireWall Management Server entwerfen, konfigurieren und verwalten
- Sammeln Sie Erfahrungen mit der zentralen Verwaltung von Richtlinien mithilfe von Gerätegruppen
- Lernen Sie, wie Sie die Netzwerk- und Gerätekonfiguration mit Hilfe von Vorlagen und Vorlagenvariablen auf viele FireWalls ausweiten können.
- Erwerben Sie Erfahrungen mit der Administration, der Protokollerfassung sowie der Protokollierung und Berichterstellung
- Sie werden mit den Planungs- und Designüberlegungen für die Panorama-Bereitstellung vertraut.

Zielgruppe

- Security Architects
- Security Administrators
- Security Operations Specialists
- Security Analysts
- Security Engineers

Kunden, die Palo Alto Networks Next-Generation Firewalls mit Panorama verwalten, sollten diesen Kurs besuchen.

Voraussetzungen

Der Kurs Firewall Configuration and Management (EDU-210) oder gleichwertige praktische Erfahrung im Umgang mit der Palo Alto Networks Next-Generation FireWall ist eine empfohlene Voraussetzung für die Teilnahme an dieser Palo Alto Panorama-Schulung. Die Teilnehmer sollten außerdem mit grundlegenden Sicherheitskonzepten vertraut sein. Vertrautheit mit Netzwerkkonzepten, einschließlich Routing, Switching und IP-Adressierung, wird empfohlen.

Kursziel

- Lernen Sie, wie Sie den Panorama FireWall Management Server entwerfen, konfigurieren und verwalten
- Erfahrungen mit der zentralen Verwaltung von Richtlinien mithilfe von Gerätegruppen sammeln
- Lernen Sie, wie Sie die Netzwerk- und Gerätekonfiguration mit Hilfe von Vorlagen und Vorlagenvariablen auf viele FireWalls ausweiten können.
- Erfahrungen mit der Administration, der Protokollerfassung sowie der Protokollierung und Berichterstellung sammeln
- Sie werden mit den Planungs- und Designüberlegungen für die Panorama-Bereitstellung vertraut.

Schulungsempfehlungen für die Zertifizierung zum Next-Generation Firewall Engineer:

- Firewall: Configuration and Management (EDU-210)
- Palo Alto Networks Panorama: NGFW Management (ersetzt den EDU-220)
- Firewall: Troubleshooting (EDU-330) (optional, aber von Vorteil)

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.de/go/PNGF

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training		Preise zzgl. MwSt.	
Termine in Deutschland	2 Tage	€ 1.795,-	
Online Training	2 Tage	€ 1.795,-	
Termin/Kursort	Kursprache Deutsch 		
12.06.-13.06.25	 Online	24.11.-25.11.25	 Frankfurt
18.09.-19.09.25	 Frankfurt	24.11.-25.11.25	 Online
18.09.-19.09.25	 Online		

Stand 20.05.2025

Inhaltsverzeichnis

Palo Alto Networks Panorama: NGFW Management – (Ersatz für EDU-220)

Adding Firewalls to Panorama

- Adding New Firewalls to Panorama
- Add a FireWall
- Automated Commit recovery
- Automatically Add multiple FireWalls via CSV import
- Tagging
- Organizing Summary Information
- Secure Communication Settings
- Manage device licenses
- Master key
- Upgrade firewalls from Panorama

- Deploy Content ID Updates to firewalls from Panorama

- Lab
- Set location for firewalls
- Copy serial firewall numbers
- Configure firewalls to communicate with Panorama
- Add firewalls to Panorama
- Modify Summary Window columns
- Assign firewall Tags
- Verify firewall licenses
- Schedule Dynamic Updates for firewalls

Initial Configuration

- Panorama solution overview
- Deployment options
- Panorama platforms
- Register and License Panorama
- GUI overview
- Panorama License and Software update
- Plugin Architecture
- Services and Interface Configuration
- Panorama Commits
- Configuration Management

- Config Operations
- Manage Backup incl. export device state from FireWall
- Config export

- Lab
- Lab Overview
- Connect to the lab environment
- Log in to the Panorama appliance and both firewalls
- Document configuration and license information
- Configure Panorama Management Interface
- Configure Panorama Settings
- Schedule automatic config exports
- Schedule Content Updates
- Save and export Panorama configuration
- Commit changes

Templates

- Templates overview
- Configuring templates
- Device configuration via template
- Local overwrite

- Template Variables
- Overview
- Configuration
- Real-life use cases and best practices

- Lab
- Create templates
- Create template stacks
- Create template variables
- Push the template stack to managed devices

Device Groups

- Device groups overview
- Configuring Device Groups
- Setup Device-group hierarchy
- Group and push to HA Peers
- Objects
- Create an object – shared/disable override
- Override
- Move
- Device Group and template mapping
- Policies
- Rules Hierarchy
- Rulebase structuring
- Configure rules
- Move Rules
- Rulebase preview
- Unused Rules
- Policy rule targets
- Rule changes archive
- Audit Comments
- Tag-Based Rule Groups
- Real-life use cases and best practices

- Lab
- Create device groups
- Configure device group settings

Log Forwarding and Collection

- Design Considerations for Deployment
- Log storage and retention
- Determine the Log Rate
- Storage calculation
- Log retention
- Planning Considerations
- Panorama log event forwarding

- Lab
- Configure log forwarding on the firewalls
- Configure log settings on the firewalls
- Confirm log forwarding

Using Panorama Logs

- Customizing Log Tables
- Using Filters in Log Tables
- Exporting Filtered Data

- Lab
- Customize Log Tables in Panorama
- Create and Apply Filters in Log Tables
- Export Filtered Data

Administrative Accounts

- Authenticating Panorama administrators
- Panorama authentication methods
- Admin Role
- Creating Administrative Accounts
- Custom Panorama Admin incl. Admin Role
- Device Group and Template Admin incl. Access Domain and Admin Role
- Password Profile and Password Complexity
- External Authentication
- Authentication Profile
- LDAP Server Profile
- Concurrent Administration
- Config Lock

- Lab
- Create LDAP and RADIUS Server Profiles
- Configure Authentication Profiles for LDAP and RADIUS
- Configure admin roles
- Configure admin accounts
- Create access domains
- Demonstrate the use of commit locks

Aggregated Monitoring and Reporting

- Data Sources Used by Panorama
- Operational Information Available in Panorama
- Reporting Capabilities in Panorama

- Lab
- Examine Panorama ACC data
- Run reports on Panorama
- Explore App Scope
- Identify and respond to threats

Troubleshooting

- Health and Summary Information of Managed Firewalls
- Troubleshooting Communication Issues with Panorama
- Troubleshooting Commit Errors
- Test policy functionality

- Lab
- Troubleshoot connectivity issues with a firewall
- Troubleshoot various commit errors
- Troubleshoot loss of internet connectivity

Add on: Transition a Firewall to Panorama Management

This is an additional module which is not part of the official course. The instructor will demo the import of an existing FireWall's local configuration into Panorama and explain various caveats.

