



PALO ALTO



About Course

Palo Alto Networks offers an enterprise cybersecurity platform which provides network security, cloud security, endpoint protection, and various cloud-delivered security services.

Most firewalls report flow rates without security protections enabled, and they even default their configuration to disabling all security features. Palo Alto Networks utilizes single-pass architecture, allowing us to inspect and protect traffic at high rates.

PALO ALTO

CURRICULUM

① How To Set Up Lab Environment

Setting Up EVE-NG Community PART 1

Setting Up EVE-NG Community PART 2

EVE-NG Installation with Linux

How to assigned a static IP to EVE-NG

How to add Palo Alto to EVE-NG

How to Add a Cisco Router

Connect To Palo Alto Firewall GUI with EVE-NG

Add a cisco Switch to EVE

Palo Alto Networks with AWS

② Basic Palo Alto

Traffic Processing Sequence

How the commit works

Creating Dynamic Admin Account

Creating Custom Role-Based Account

Non-Local Administrator Accounts

③ Security Operating Platform And Architecture

Cortex

Securing the Enterprise Primary Next Generation Features

4

Interfaces

Intro

Security Zones

Security Policy

Tap Mode

Virtual Wire Lab simple

Virtual Wire Lab Advanced

L2 Lab Simple

L2 Lab Advanced with no Sub Interfaces

L2 Deployment With Sub interfaces

L2 Deployment With Sub interfaces and Router on a Stick

L3 Lab Simple

L3 Lab Advanced

Layer 3 Subinterfaces with Firewall on a Stick

Tap, Virtual Wire, L2, and L3

Interface Management Profile

Virtual Routers

Virtual Routers with multiple VRs Lab

Routing Protocols

OSPF

OSPF Between PAN, Cisco Router and Juniper Firewall

Capture traffic on the management interface

Interfaces

5 Security Policies

Intro

Controlling the traffic

Palo Alto is Stateful

Security Rule Types

Creating a Security Policy

Edit the Policies Tab

Schedule a Policy

Creating Objects

Tags

NAT Types

Source NAT

Source NAT LAB

Destination NAT

Creating Network Diagram

Diagram

Time-Based QoS Configuration

6 App-ID

Intro

What is App-ID

How does App-Id Works

Application Shift

Application Shift Lab

Implicit Applications

Content-ID

Intro

Content ID

Vulnerability Protection Default

Cloning A Vulnerability Protection

Creating A Vulnerability Protection

Vulnerability Protection Exceptions

Antivirus Profile Intro + Default

Clone and add exceptions to Antivirus Profile

Anti-Spyware Profile Intro + Default

Clone and add exception for a new Anti-Spyware

Anti-Spyware DNS Signatures and Sinkhole

Anti-Spyware Sinkhole, DNS Signature and Exceptions

File Blocking Profile

Creating File Blocking Profile

Blocking Multi-Level Encoding

Data Filtering Profiles

Data Filtering Profiles Demo

Security Profile Group Demo

Telemetry

Dos Protection

DoS Protection Part Deux

DoS Protection Policies

URL Filtering

URL Filtering profile

Safe Search

Block Website with Custom URL Category

URL Filtering Profile With Continue, Blocked, and Override

8 Decryption

Intro

SSL/TLS Overview

Firewall Decryption Types

PKI, CA, Root CA

Looking at a real Certificate

CA Certificate Choices

Generate Certificate Lab

Forward Proxy Decryption

Configuring a Forward Trusted Certificate

Configuring Forward Untrusted Certificate

Configure SSL Forward Proxy Policy

Configure SSL Forward Proxy Profile

SSL Inbound Inspection

SSL Inbound Inspection Lab

Decryption

9 WildFire

Intro

WildFire Intro

WildFire Email Protection

WildFire License

WF-500

Configuring WildFire Settings

WildFire Analysis Profile

Creating a WildFire Profile

WildFire

10

User-ID

Intro

Intro to User-ID

User Mapping Methods

Syslog Monitoring

DC Monitoring and Session Monitoring

Steps to configure User-ID

Active Directory and PC Enrollment

Configuring PAN-OS Integrated User-ID Agent

Windows Based Agent Configuration Steps

BONUS - Authenticating User with Domain Controller

User-ID

11

GlobalProtect

GlobalProtect Intro

GlobalProtect Connection Sequence

Prima Access

Clientless VPN

Custom Reports
PDF Summary Report
SaaS Application Usage Report
Report Group
Emailing Reports
Syslog
Add a Syslog Server Profile
SNMP
Monitoring and Reporting

14 High Availability

Intro
High availability Overview
Active/Passive
Active/Active
HA Prerequisites
Components and Operations
HA Backup Links
Designating a Firewall
Detecting Failure
HA Active/Passive Configuration
Configuring Link Groups
Configuring Link Groups Lab
Path Monitoring
Path Monitoring Lab
HA

15

Panorama

Initial Configuration

Set Panorama Management Interface


Device Groups and Template



 www.softcrayons.com

 info@softcrayons.com

 (+91) 854 501 2345

 693, Sector 14-A, Vasundhara,
Ghaziabad (U.P.), 201012

   @softcrayons