CYBERSECURITY ACADEMY

Protecting life in the digital age one student at a time

WASTC 2020 Faculty Development Weeks

Palo Alto Networks Faculty Training: Admin I & II

Dates: Fully Online, June 8-12, 2020
Times: 9:30 – 4:30 (PST) 1 hour Lecture then 1 hour Lab, repeat this schedule until 4:30
More detailed schedule below

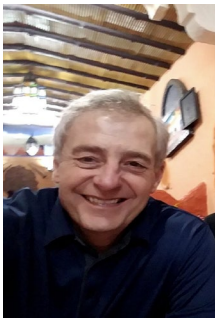
Target Audience: This course is for you if …

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

Workshop Overview:
This faculty training will prepare you to teach the Cybersecurity Infrastructure Configuration (CIC) and Cybersecurity Prevention & Countermeasures (CPC) courses offered through participating in the **Palo Alto Networks Cybersecurity Academy** program. It will provide hands-on experience to do the Next-Generation Firewall (NGFW) course labs. Further it prepares faculty to become **Palo Alto Networks Certified Network Security Administrator (PCNSA)**.

Cybersecurity Infrastructure Configuration (CIC)
This course provides you with a general understanding of how to install, configure, and manage firewalls for defense of enterprise network architecture. You will learn the theory and configuration steps for setting up the security, networking, threat prevention, logging, and reporting features of next generation firewall technologies.

Cybersecurity Prevention & Countermeasures (CPC)
This course provides you with advanced information for how to install, configure, and manage firewalls for defense of enterprise network architecture. You will learn the theory and extended configuration features necessary for setting up traffic handling, advanced content/user identification, quality of service, global protect, monitoring/reporting and high availability of next generation firewall technologies.



Instructor: Jim Boardman is a Palo Alto Networks academy technical engineer and his duties include training faculty, setting up new academies, managing cybersecurity competition support and providing curriculum support. Before joining Palo Alto Networks, Jim worked at Alfred State College, Alfred, NY, where he taught networking, cybersecurity and served as the department chair. While at Alfred State, Jim was a certified Palo Alto Networks academy instructor, certified VMware academy instructor, a certified Cisco academy instructor and a certified Linux Professional Institute academy instructor. Jim was also the coach of Alfred State College's cybersecurity teams that competed at local and national competitions such as the North East Collegiate Cyber Defense Competition, CyberSEED and the Collegiate Penetration Testing Competition.

Jim's current certifications include: Certified Information System Security Professional (CISSP), AWS Certified Solutions Architect Associate and PCNSE7. Before working at Alfred State College, Jim was the senior network solutions architect at the startup company Power Up Networks and was a network solutions architect at Nortel Networks.

Sponsored by:

WASTC 2020

Palo Alto Networks Admin I and Admin II Faculty Training

- Track Title: Palo Alto Networks Faculty Training Admin I and Admin II (Cybersecurity-Infrastructure-Configuration and Cybersecurity Prevention and Countermeasures Course)

- Track Description

  This course provides the student with a general understanding of how to install, configure, and manage firewalls for defense of enterprise network architecture. Students will learn the theory and configuration steps for setting up the security, networking, threat prevention, logging, and reporting features of next generation firewall technologies.

- Learning Objectives of this course
  - Compare and contrast industry leading firewall platforms, architecture, and defense capability related to zero trust security models and public cloud security.
  - Demonstrate and apply configuration of firewall initial access, interfaces, security zones, virtual routing, filtering, licensing, service routes, software updates, and policy-based forwarding.
  - Analyze security policy administrative concepts related to source and destination network address translation.
  - Outline and construct security policies to identify known and unknown application software running on the service network.
  - Differentiate, configure, and deploy filtering technologies such as anti-virus, antispyware, and file blocking, to protect against telemetry induced attack vectors.

- Course Agenda

  Topics:
  Topic 0: Cybersecurity Academy Overview and Course Overview
  Topic 1: Next-Generation Security Platform and Architecture Module
  Topic2: Initial Configuration
  Topic 3: Overview of NIST/NICE Cybersecurity Workforce Framework
  Topic 4: Interface Configuration
  Topic 5: Security and NAT Policies
  Topic 6: App-ID
  Topic 7: Application-ID
  Topic 8: URL Filtering
  Topic 9: Decryption and Certification Management
  Topic 10: End User Identification
  Topic 11: Remote Access Security: Client VPN and Site-to-Site-VPN
  Topic 12: Security Monitoring and Reporting
  Topic 13: Security and Device High Availability

Tentative Daily Schedule

Day 1 Pacific Time Zone

8:30 AM – 9:20 AM: Introductions

10:30 AM – 11:20 AM: Brief Academy Overview and Platforms and Architecture
11:30 AM – 12:00 PM: CIC- Configuration Infrastructure Course (CIC) - Platforms and Architecture (Continued)
12:00 PM – 1:00 PM: Lunch Break
1:00 PM – 1:50 PM: CIC - Initial Configuration
2:00 PM – 3:00 PM: Lab and Quiz Time and break
3:00 PM – 3:50 PM: CIC - Interface Configuration
4:00 PM – 4:30 PM: Lab and Quiz Time

Day 2 Pacific Time Zone

8:30 AM – 9:20 AM: CIC - NAT and Security Policy
9:30 AM – 10:20 AM: Lab and Quiz Time
10:30 AM – 11:20 AM: CIC - App-ID
11:30 AM – 12:00 PM: Lab and Quiz Time
12:00 PM – 1:00 PM: Lunch Break
1:00 PM – 1:20 PM: CIC - Lab and Quiz Time
1:30 PM – 2:20 PM: CIC - Content-ID
2:30 PM – 3:20 PM: CIC - Lab and Quiz Time
3:30 PM – 4:20 PM: CIC - URL Profile

Day 3 Pacific Time Zone

8:30 AM – 9:20 AM: Lab, CIC Review and Quiz Time
9:30 AM – 10:20 PM: Cybersecurity Prevention and Countermeasures – Decryption and Certificate Management
10:30 AM – 11:20 PM: Lab and Quiz Time
11:30 AM – 12:00 PM: CPC - Virus analysis and Mitigation – WildFire
12:00 PM – 1:00 PM: Lunch Break
1:00 PM – 1:20 PM: CPC - Virus analysis and Mitigation – WildFire (Continued)
1:30 PM – 2:20 PM: Lab and Quiz Time
2:30 PM – 3:20 PM: CPC - End User Identification – UserID
3:30 PM – 4:20 PM: Lab and Quiz Time

Day 4 Pacific Time Zone

8:30 AM – 9:20 AM: CPC – Remote Access Security - GlobalProtect
9:30 AM – 10:20 PM: Lab and Quiz Time
10:30 AM – 11:20 PM: CPC – Remote Access Security – Site-to-Site-VPN
11:30 – 1200 PM: Lab and Quiz Time
12:00 PM – 1:00 PM: Lunch Break
1:00 PM – 1:20 PM: Lab and Quiz Time
1:30 PM – 2:20 PM: CPC – Security Monitoring and Reporting
3:00 PM – 3:50 PM: Lab and Quiz Time

Day 5 Pacific Time Zone

9:30 AM – 10:20 – CPC – Security Device High Availability
10:30 AM – 11:20 – Lab and Quiz Time
11:30 AM – 12: 20 – NICE Cybersecurity Work Force Framework, CPC Review

- Any pre-requisites for the track
  A good understanding of networking and cybersecurity concepts and completion of Cybersecurity Academy Orientation course

- All required textbooks are in your Academy Moodle Course