- Cybersecurity Academy Resource Page
- Palo Alto Networks Learning Center LMS

The Learning Center is our corporate LMS which is open to anyone wanting to learn more about Palo Alto Networks products. It is a separate LMS so you will need to enroll as a guest first before you can access this LMS. To create your account access the Learning Center using this URL: https://www.paloaltonetworks.com/service/education

  - Register for an assortment of self directed training courses.
  - Browse through the catalog of Palo Alto Networks learning opportunities.
  - Manage your Palo Alto Networks learning transcript and print your certificates
- Cyber Security Survival Guide
- Interesting Web Links

In this folder you will find some links to interesting postings on the Web that may help you better prepare for your CCDC competitions. This is fantastic tutorial with pcaps and all that it takes a deep dive into the Dridex RAT with emphasis on using PKI to encrypt the malware. To achieve the next level of protection for your team's network, it's really important to use decryption on your PANW firewall appliance so your firewall can decrypt and then block malware.

https://unit42.paloaltonetworks.com/wireshark-tutorial-dridex-infection-traffic/

- Mitre ATT&CK Framework

I just discovered this Mitre site while reading about the solar storm attack and I think it is an outstanding resource to help you prepare for your CCDC competitions. It is the attack life cycle on steroids. It lists all the current attack methods or TTPs (Tactics, Techniques and Procedures) and more importantly provides recommended mitigations. No matter what you do defensively, you have to assume the red team is in your network and after the very sophisticated solar storm attack, you have to assume the bad guys are in your network in the real world too despite all your intrusion prevention efforts. After all the best NGFW only has milliseconds to make a decision to let traffic in our not to let traffic in. You still need your PANW firewall to block known attacks but there may be some new custom red team attacks that slip through. Probably not too many because it does take some effort to design a new attack.

The Mitre ATT&CK framework provides you with indicators that you can use to search your network logs and hopefully find and mitigate attacks. If you can't stop the delivery of malware into your network, you can still disrupt an attack by blocking C2 connections coming from the inside of your network to the outside. Your PANW firewall, properly configured, will help you disrupt attacks but you also need end point protection to block communications to C2 external servers. If you can block ET from phoning home, you are doing well.

- Preparing for The Collegiate Cyber Defense Competition

National CyberWatch Center's guide for new teams and recommendations for experienced players.

- Blue Team Cheat Sheets

This is a great pdf document resource to print out and use during your CCDC competitions or to prepare for your CCDC competitions.

- Zero Trust

Zero Trust architecture, rooted in the principle of “never trust, always verify,” is designed to address lateral threat movement within the network by leveraging micro-segmentation and granular perimeters enforcement, based on user, data and location. Lateral movement defines different techniques that attackers use to move through a network in search of valuable assets and data.

The Zero Trust model is different than traditional perimeter-based network security model. In the traditional model, some devices and users are trusted more than other devices and users. For example, using the traditional model, internal computer devices and users are more trusted than external computer devices. The zero trust model assumes that any computer device and user can be compromised so for cybersecurity administrators, all devices and users, whether external or internal should all have the same level of trust which is "0". As a result, you need to inspect all traffic entering and exiting each of your network devices.

Zero Trust is the perfect architecture for CCDC competitions and your Palo Alto Networks firewall appliance, properly configured, can help you achieve a Zero Trust architecture.

- Unit 42 Threat Intelligence Center

Unit 42 is the global threat intelligence team at Palo Alto Networks®. We believe threat intelligence should be free, shared and available to all for the common good. We deliver high-quality, in-depth research on adversaries, malware families and attack campaigns. Our analysts uncover and document adversary behaviors, and then share playbooks that give insight into the various tools, techniques and procedures threat actors execute to compromise organizations.

We share our findings freely so defenders everywhere can access world-class threat intelligence. Unit 42 is a recognized authority on cyberthreats, frequently sought out by enterprises and government agencies around the world.

Unit 42 is headed by Rick Howard, Palo Alto Networks CSO, and Ryan Olson, Palo Alto Networks VP of Threat Intelligence.

- What is a Zero Trust Architecture
- Palo Alto Networks | TechDocs Home

The Palo Alto Networks Technical Documentation portal provides access to all of the platform documentation and software documentation you will need to successfully deploy and use the Palo Alto Networks Security Operating Platform.

- Automation Tools to Help You Configure Your Firewall Appliance

In the URL links below, you will find info about our Expedition virtual machine OVA that you can download and use and our iron-skillet github repository of best practice firewall configs.

Expedition will help automatically generate security policies based on real log traffic and also has a best practice assessment tool to check your firewall's configuration for compliance with our best practice recommended firewall appliance configurations.

Iron-skillet is a repo where you can download best practice firewall appliance configurations and install them on your appliance either via GUI or command line.

- One Fully licensed VM-50 Firewall Appliance for Every Competing Team

Please contact your regional CCDC director to obtain your VM-50 virtual firewall appliance license and VM-50 ova. Every CCDC competing team will receive one fully licensed VM-50 virtual firewall appliance to use for practicing. The Web-UI for the management interface and the configuration commands for the VM-50 firewall appliance are identical to the PA-3050 hardware firewall appliance Web-UI and configuration commands. The feature set of the VM-50 firewall appliance is also nearly identical to the PA-3050 hardware firewall appliance. The bottom line is, if you can configure a VM-50 firewall appliance, you will be able to configure a PA-3050.

As a reminder, Palo Alto Networks has a great Cybersecurity Academy program for colleges and universities. The Cybersecurity Academy provides curriculum, structured labs and licenses for lab firewall appliances at no cost. If your college or university is a Palo Alto Network Cybersecurity Academy, then you can obtain your VM-50 firewall appliance licenses directly through the Cybersecurity Academy program, so you will not need to obtain your VM-50 firewall appliance license from your regional CCDC director.

- Expedition Migration Tool

With Expedition, we have gone one step further, not only because we want to continue helping to facilitate the transition of a security policy (This video explains how to configure and optimize your security policies on the PAN-OS) from others vendors to PAN-OS, but we want to ensure the outcome is the best as possible. This is why we added a Machine Learning module that can help you generate new security policies based on real log traffic and the introduction of the Best Practices Assessment Tool to check the configuration complies with the Best Practices recommended by our security experts.

- Iron-skillet Best Practice Firewall Appliance Configs

Iron-Skillet is a set of day one configuration templates to help enable alignment with security best practices. See the Quick Start section below to get started using the template configurations.

- MineMeld Threat Intelligence Sharing

MineMeld is an open source Palo Alto Networks appliance that allows you to aggregate threat intelligence across public, private and commercial intelligence sources, including government and commercial organizations. It may be useful during a CCDC competition if you have time during the competition to set it up. It consolidates threat feeds and provides a single dynamic IP and or url block list feed to your firewall. The drawback of course is that red team activity usually makes block lists ineffective but MineMeld is pretty cool and might be worth exploring if for nothing else other than for your own personal learning journey.

- Palo Alto Networks Cybersecurity Academy Program

Palo Alto Networks has a great Cybersecurity Academy Program that is available to all colleges and universities at no cost. We provide all our academies with as many fully licensed VM-50 virtual firewall appliances academies require to teach our our curriculum. Please click this link to find out more information.

- NetDevGroup (NDG) Firewall Essentials Labs
  - Lab 01: Initial Configuration
  - Lab 02: Interface Configuration
  - Lab 03: Security and NAT Policies
  - Lab 04: App-ID
  - Lab 05-A: Content-ID
  - Lab 05-B: Content-ID
  - Lab 06: URL Filtering
  - Lab 07: Decryption
  - Lab 08: WildFire
  - Lab 09: User-ID
  - Lab 10: GlobalProtect
  - Lab 11: Site-to-Site VPN
  - Lab 12: Monitoring and Reporting
  - Lab 13: Active/Passive High Availability

Module 1 - CCDC FW Appliance Security Architecture Planning

- CCDC Firewall Essentials Quick Start Deployment and Configuration Guide

Read this first and print it for your CCDC competition. Covers the basics to quickly deploy and configure your PA 3050 to protect your network. You can also use the steps to deploy and configure virtual firewall appliances.

- CCDC Threat Environment and Best Practices Part 1
- CCDC Threat Environment and Best Practices Part 2a
- CCDC Threat Environment and Best Practices Part 2b
- Competition Threat Environment

This video highlights recommendations for a successful competition.

- Zero Trust Network Architecture

This video provides an overview of Palo Alto Networks Zero Trust Architecture.

- Cloud Deployment

This video discusses how to accelerate deployment to the cloud.

- Platforms and Architecture Module PDF
  - Platforms and Architecture e-learning
- Palo Alto Networks Firewall Appliance Performance Specs
- Module 1 Quiz

Module 2 - Deploy/Configure FW Appliance for Quick Protection

- Initial Firewall Setup - Private video, unable to access

This video explains how to initially setup and configure the firewall out of the box.

- Network Deployment Options

This video explains the firewall network deployment options available.

- Zone Protection

This video explains how to configure zone protection on the PAN-OS firewall.

- Denial of Service Protection

This video explains how to configure DoS protection on the PAN-OS firewall.

- Command Line Options

This site provides information on how to use the PAN-OS command line.

- Layer 3 Configuration Video Link

This is a fantastic light board video by PANW Sales Engineer Marcelo Lima that shows you how to quickly set up your Layer 3 interfaces on your PANW firewall appliance.

- Deploying VM Series on ESXi using L3 Interfaces with SNAT, DNAT and Sec Policies

This presentation has information about setting up a VM-50/100 on an ESXi hypervisor, creating source NAT (This video explains how to configure Source NAT on the PAN-OS GUI) and Destination NAT policies, security policies, and assigning security profiles to security policies.

- Factory Reset for PANW Firewall

If you have lost your password, you will have to do a factory reset by following the steps in the Web site. If you're using a VM-Series firewall you just access the firewall console from your hypervisor. There is no need for a console cable for VM-series firewalls.

Make sure you give the firewall about 5 minutes after initial boot to start all it's services before trying to log in. You will not be able to log in until all the firewall's services start up which takes about 2-5 mins. If you haven't changed the password it should be the default admin admin. Use the WebUI, it is easier to navigate at first then you can practice using the cli.

Do not try to set up the team's VM-50 firewall without doing the labs in the CCDC 2021 Moodle course first. If you have somehow lost your password then you will need to reboot the firewall and then right at the start of boot up, hit enter and very quickly type "maint" to enter maintenance mode. You don't have a lot of time to type maint so do it quickly. Then in maint mode select factory reset. Hopefully, you have not licensed your appliance yet because if you did you will lose your license when you do a factory reset. Once you have licensed your firewall and downloaded all the dynamic updates, be sure to do a snapshot, in case something goes wrong.

Module 3 - Deploy Firewall Appliance for Advanced Protection

- Security Policy

This video explains how to configure and optimize your security policies on the PAN-OS.

- NAT and Security Policy

This video explains the relationship between NAT and Security Policies on the PAN-OS.

- Source NAT

This video explains how to configure Source NAT on the PAN-OS GUI.

- U-Turn NAT

This video explains how to configure U-Turn NAT on the PAN-OS.

- Custom APP-ID

This video explains how to configure custom APP-ID on the PAN-OS.

- Inbound and Outbound SSL Decryption - Private video, unable to access

This video explains how to configure SSL Decryption on the PAN-OS.

- Wildfire

This video explains how to configure Wildfire on the PAN-OS.

- Site-To-Site VPNs

This video explains how to configure site-to-site VPNs on the PAN-OS.

- Auto-Tagging and DNS Sinkhole

This video explains how to configure auto-tagging and DNS Sinkhole on the PAN-OS.

- GlobalProtect

This video explains how to configure GlobalProtect on the PAN-OS.

- Log Files and Reports

This video explains how to search through log files and reports on the PAN-OS.

- Application Command Center Part 1

This Part 1 video explains the Application Command Center on the PAN-OS.

- Application Command Center Part 2

This Part 2 video explains the Application Command Center on the PAN-OS.

Module 4 - Infrastructure Device Configuration

- Next Generation Firewall Flow Logic
- Initial Configuration Module PDF
    - Initial Configuration e-learning
- Basic Interface Configuration Module PDF
    - Basic Interface Configuration e-learning
- Initial Configuration Lab
    - Interface Configuration Lab
- Module 4 Quiz

Module 5 - Cybersecurity Policy

- Security and NAT Policy Module PDF
    - Security Policy e-learning
- Security and NAT Policy Lab
- Module 5 Quiz

Module 6 - Application Software Identification

- Application Identification Module PDF
    - Application Identification e-learning
- Application ID Lab
- Module 6 Quiz

Module 7 - Anti-Virus/Anti-Spyware/File Blocking

- Content Identification Module PDF
    - Content Identification e-learning
- Wireshark Tutorial: Examining Trickbot Infections

This is an excellent Unit 42 tutorial about examining the trickbot malware using WireShark. In the article you will find the pcaps with trickbot malware and instructions on how to view the many indicators of compromise (IOC) in the packet captures. I highly recommend all teams complete this tutorial as preparation for CCDC 2020 competitions to acquire a better understanding how malware can hide and penetrate your networks following "the attack life cycle". Use this information to better configure your firewall appliances to disrupt the attack life cycle and prevent the Red team's "acting on an objective".

- Content ID Lab
- Module 7 Quiz

Module 8 - Uniform Resource Locator Filtering

- URL Filtering Module PDF
    - URL Filtering e-learning
- URL Filtering Lab
- Module 8 Quiz

Module 9 - Decryption and Certificate Management

- Decryption Module PDF
    - Decryption e-learning
- Decryption Lab (may need NDG Lab 7)
- Module 9 Quiz

Module 10 - Virus Analysis and Mitigation

- Virus Analysis Module PDF
    - Virus Analysis e-learning
- What is DNS Tunneling

One of the favorite red team attacks is delivering newly crafted or polymorphic malware to endpoints and setting up an on-the-fly new C2 infrastructure during the competition and then use DNS beaconing and DNS Tunneling to exfiltrate data from compromised team networks.

This is a great article that explains how DNS tunneling works. With DNS tunneling, a malware C2 DNS server provides query answers with "tunneled" commands to compromised hosts inside your team's network.

Because the red team's created C2 domains are brand new and haven't been identified as malware domains, it's very hard to provide protection against this type of attack. DNS security on your firewall appliance uses machine learning on Palo Alto Networks threat intelligence cloud to more quickly identify malware domains and block C2 communications.

- DNS Beacon Tunneling C2 Example

This is a great article describing an actual recent attack that involved DNS Tunneling.

- Firewall Appliance DNS Security Protection

DNS security is a relatively new firewall appliance license and protection starting with PanOS 8.1. This feature provides added protection against newly created bad domains. This feature may be very effective against DNS beacon attacks launched by the red team during CCDC competitions. The attached presentation describes how it works.

    - DNS Security Service e-learning
- WildFire Lab (may need NDG Lab 8)
- Module 10 Quiz

Module 11 - End User Identification

- End User-ID
    - End User ID e-learning
- User-ID Lab (may need NDG Lab 9)
- Module 11 Quiz

Module 12 - Remote Access Security

- GlobalProtect Module PDF
    - Global Protect e-learning
- Site-To-Site VPNs Module PDF
    - Site-to-Site VPN e-learning
- GlobalProtect Lab (may need NDG Lab 10)
    - Site-To-Site VPN Lab (may need NDG Lab 11)
- Module 12 Quiz

Module 13 - Security Monitor and Reporting

- Monitor and Report Module PDF
    - Monitor and Reporting e-learning
- Next Generation Security Practices Module PDF
    - NGFW Security Practices e-learning
- Monitor and Report Lab (may need NDG Lab 12)
- Module 13 Quiz