Red Education

(EDU-330) Firewall Troubleshooting Expert

PALO ALTO NETWORKS
Certification Training Explained

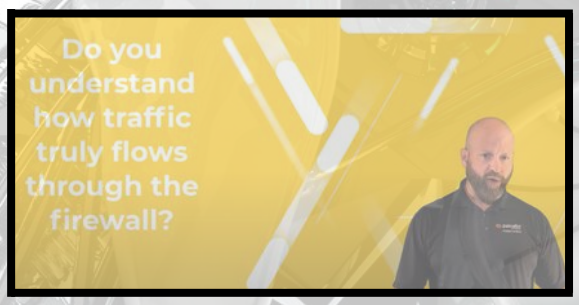
Firewall troubleshooting can be a daunting task without the proper training. Cybersecurity incidents are on the rise, and trying to keep up with continual technological advancements, such as cloud-delivered security services supporting cloud assets, makes the management of firewalls a challenge without certification training.

Thankfully, Red Education offers an authorised certification training programme. This three-day instructor led course helps you obtain the skills you need to troubleshoot Palo Alto Networks next-generation firewalls successfully. This course will provide participants with ample opportunities for hands-on troubleshooting related to the configuration and operation of Palo Alto Networks systems. Upon successful completion and at the end of this class, you will have in-depth knowledge of troubleshooting whilst providing visibility and control over applications, users, content and certification to fast-track knowledge and career progression.

Who should attend

Participants of EDU-330: Firewall Troubleshooting should already have experience configuring and managing Palo Alto Networks firewalls. The course is ideal for security engineers, network engineers, and support staff who have completed the EDU-210 – Firewall Essentials: Configuration and Management method or have equivalent experience. If you use Panorama, earlier attendance of the EDU-220 Panorama: Managing Firewalls at Scale is beneficial but not required.

This 3-day, instructor led training course will consist of a combination of lectures and labs. The classes will cover critical concepts, while the virtual labs will provide participants with opportunities to put those concepts into practice in real-world scenarios. By the end of this course, participants should feel confident in their ability to troubleshoot issues like a pro!



What are some common issues you might encounter when deploying or troubleshooting a firewall in a network?

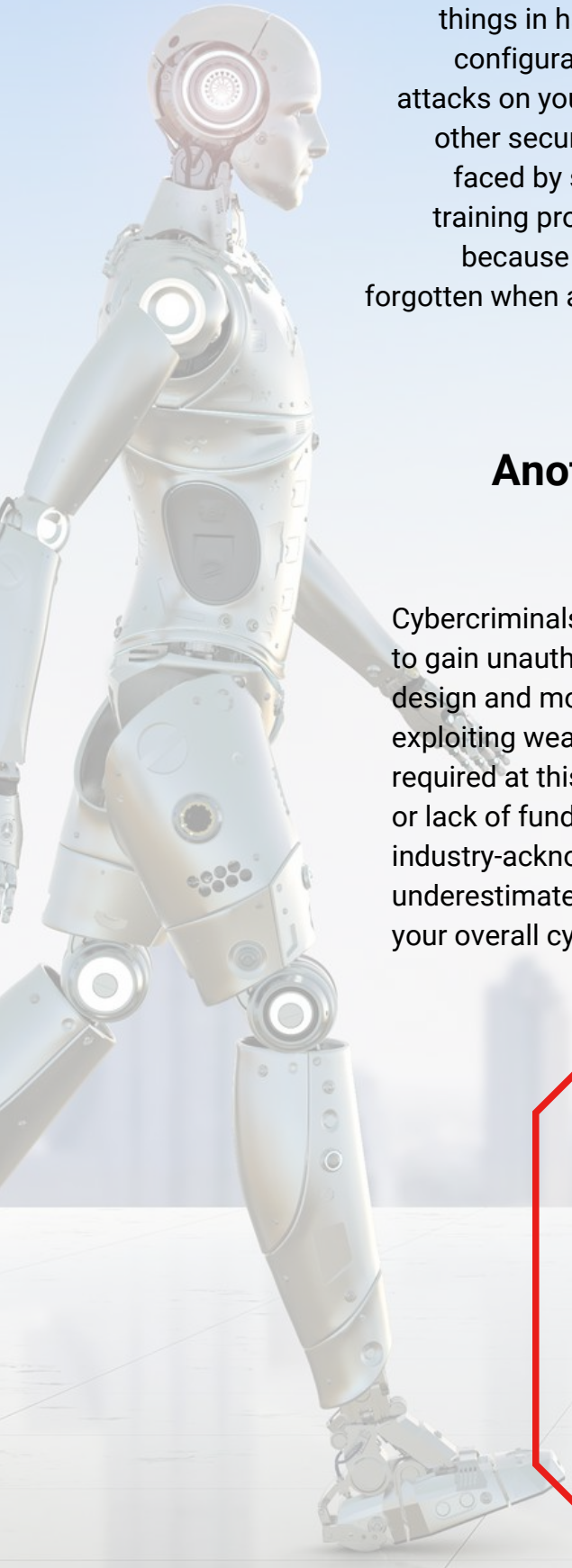
Connectivity issues, Policy or NAT-related issues, GlobalProtect™ and WildFire™ incompatibilities, High CPU or memory usage problems, and many others. Poor configuration of firewalls and other security controls may lead to gaps in protection against attacks; how can these occur?

Insider threats bypassing traditional security controls

One of the biggest dangers to organisations is the insider threat. This threat comes from within the organisation and can include malicious employees, contractors, or partners. These individuals have access to the organisation's systems and data and can use that access to steal or damage information. They may also be able to use their access key to gain an advantage in competing with the organisation or for personal financial gain. Traditional security controls, such as firewalls, are ineffective at preventing these attacks. Insider threats can easily bypass these security controls using their knowledge of the network and its systems. They may also be able to use their access to sensitive data to evade detection. Organisations need to take additional steps to protect themselves from insider threats. These steps include implementing robust authentication procedures, monitoring employee activity, and encrypting data. Organisations should also have a plan for responding to a breach if one occurs.

A simple lack of knowledge

You need sufficient Palo Alto Networks certified administrators and security professionals to manage this solution. A lack of skilled professionals can lead to an overworked and stressed team deciding things in haste. Without appropriate security controls in place, a poor configuration can lead to gaps in protection against various types of attacks on your network, such as malware infections, data breaches, and other security incidents. This is one of the most easily rectified issues faced by security professionals merely by applying for a certification training programme however is one of the most overlooked strategies because of the perception of cost and time. However, this is quickly forgotten when a costly breach occurs, running into hundreds of thousands if not millions of dollars in punitive damages and fines .



Another cause is the attackers themselves

Cybercriminals attempt to manipulate firewall configurations maliciously to gain unauthorised access or cause disruption. So attention to detail, design and monitoring is an essential tactic to keep cybercriminals from exploiting weaknesses in the configuration set-up. The expertise required at this level cannot be ignored, irrespective of headcount costs or lack of funding to hire and train security operations specialists; having industry-acknowledged certifications within the team cannot be underestimated or dismissed as they are crucial deterrents to support your overall cyber strategy.

THREATS

EMOTET
DENIAL OF SERVICE
MAN IN THE MIDDLE
PHISHING
SQL INJECTION
PASSWORD ATTACKS
INTERNET OF THINGS

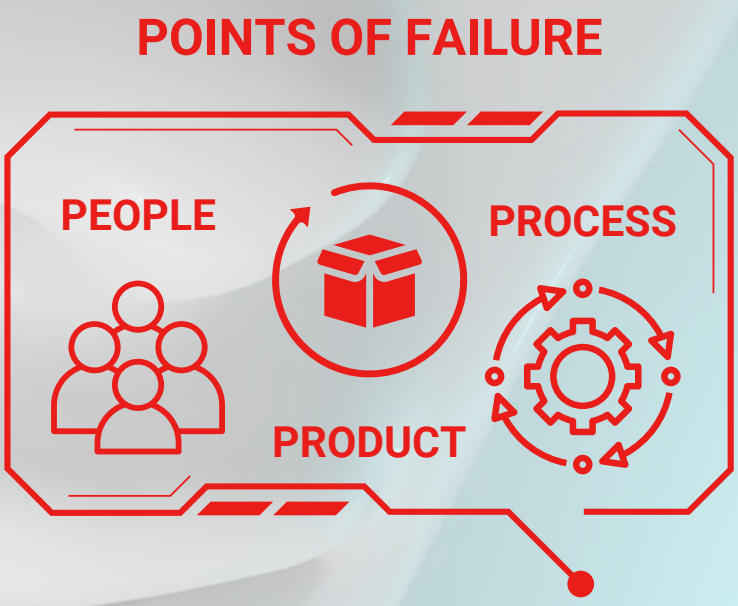
Red Education

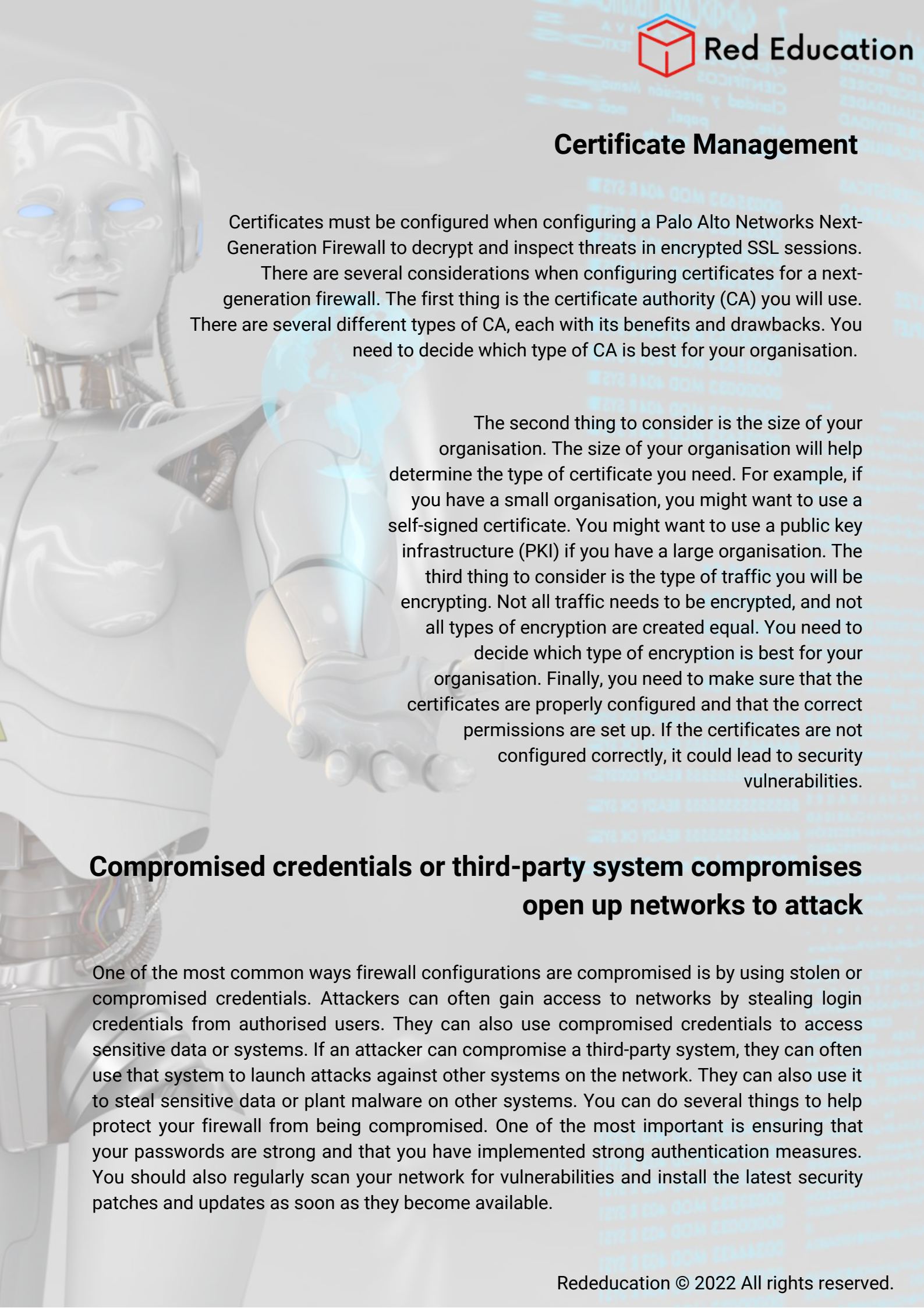
Lax compliance within organisational security policies

Another key consideration to prevent your firewall from being misconfigured is robust policy control procedures. This means having policies that are well-defined, comprehensive, and continually updated. Security professionals and security analysts need to be sure that they are not only following these policies but also enforcing them. Having a policy is a good start, but it's not enough. You must ensure that everyone responsible for managing your firewall knows these policies and how to follow them. More importantly, it's vitally essential that changes need to be recorded and obsolete policies removed when new procedures take place. Leaving legacy policies and data points behind is a future recipe for disaster. Overall, the best way to prevent misconfigurations is to implement a professional approach to robust change management processes, including testing and review steps before any changes are made.

Sophisticated malware, including zero-day exploits

Zero-day exploits are a particularly nasty type of malware that takes advantage of security vulnerabilities that have not yet been patched. They can be tough to detect and often go undetected for a long time. One way to help protect your network from zero-day exploits is to ensure that your firewall is configured correctly and up-to-date. You should also provide the latest security patches and updates installed on your devices. You should also have a comprehensive security plan that includes regular updates and patches and robust backup and disaster recovery procedures. If you are concerned about zero-day exploits, or any other type of malware, it is always a good idea to consult a qualified security professional. They can help you put the necessary safeguards in, to protect your network from attack.





Red Education

Certificate Management

Certificates must be configured when configuring a Palo Alto Networks Next-Generation Firewall to decrypt and inspect threats in encrypted SSL sessions. There are several considerations when configuring certificates for a next-generation firewall. The first thing is the certificate authority (CA) you will use. There are several different types of CA, each with its benefits and drawbacks. You need to decide which type of CA is best for your organisation.

The second thing to consider is the size of your organisation. The size of your organisation will help determine the type of certificate you need. For example, if you have a small organisation, you might want to use a self-signed certificate. You might want to use a public key infrastructure (PKI) if you have a large organisation. The third thing to consider is the type of traffic you will be encrypting. Not all traffic needs to be encrypted, and not all types of encryption are created equal. You need to decide which type of encryption is best for your organisation. Finally, you need to make sure that the certificates are properly configured and that the correct permissions are set up. If the certificates are not configured correctly, it could lead to security vulnerabilities.

Compromised credentials or third-party system compromises open up networks to attack

One of the most common ways firewall configurations are compromised is by using stolen or compromised credentials. Attackers can often gain access to networks by stealing login credentials from authorised users. They can also use compromised credentials to access sensitive data or systems. If an attacker can compromise a third-party system, they can often use that system to launch attacks against other systems on the network. They can also use it to steal sensitive data or plant malware on other systems. You can do several things to help protect your firewall from being compromised. One of the most important is ensuring that your passwords are strong and that you have implemented strong authentication measures. You should also regularly scan your network for vulnerabilities and install the latest security patches and updates as soon as they become available.

Deficiencies in toolsets

Another mistake is a lack of proper tools. Any good tradesperson knows they must have the right tools to complete the job; if you lack these, you must demand products that streamline systems, increase automation and reduce manual workloads. On-premises toolsets explicitly designed for an organisation's needs increase productivity and reduce mistakes, leading to a more efficient team.

Third party vulnerabilities

Are another common cause of firewall misconfiguration. When an organization fails to vet third-party systems properly, it can often lead to malicious actors gaining access to the network. This can allow them to steal sensitive data or plant malware on the network. To help prevent these types of problems, it is essential to have a well-defined incident response plan in place. The plan should include robust testing and review procedures, up-to-date toolsets, and training programs.

Why attend Certification Training?

When it comes to efficiency in operations, education is crucial. Sometimes it's hard to get through the training and certification process. Yet, there are numerous upsides to this. Learning the fundamentals of security as you go or in small, independent chunks is no longer adequate. Because real life sometimes gets in the way of formal education, you need thorough Instructor led training to firmly establish desirable work habits. **If you knew the pilot wasn't licenced to fly, would you still get on the plane?** Competent administrators, operators, and security engineers all share the thirst for knowledge. This is a really intricate procedure. It's a recipe for catastrophe to invest millions in a cybersecurity platform and then let poorly trained staff handle the management of sophisticated systems. Maintaining employment is much easier if you have the proper certifications.

I’m interested in telling me more

There is no universally applicable substitute for actual work experience and training. What benefits one person may not benefit another. Therefore, classes taught by an expert can be beneficial. They provide students with the chance to study in a practical setting while also receiving help and support from a knowledgeable instructor. The (EDU-330) Troubleshooting course is one example. Everything from the suggested use of tools and troubleshooting processes is covered in depth over this comprehensive three-day training programme. Whether you're just starting or want to take your profession to the next level, this course is ideal for you if you want to learn or improve your abilities to FastTrack problem-solving techniques.

In a nutshell, this is a worthwhile investment that may yield results both immediately and down the road. Therefore, register directly to improve your competence in this field. It's a decision you won't come to regret.

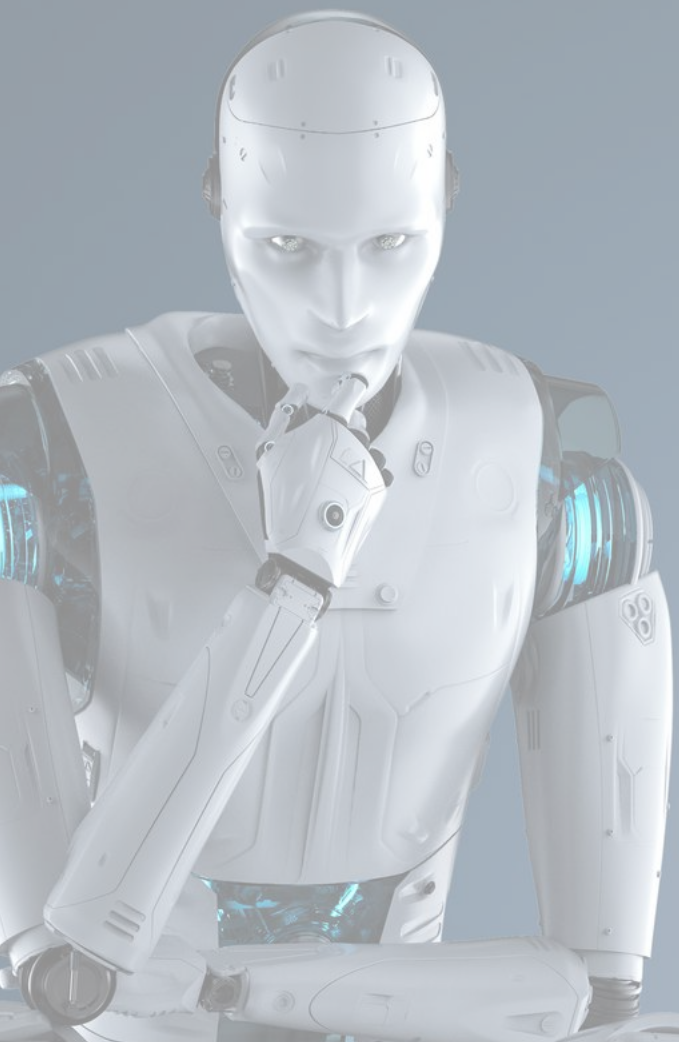
What are the objectives of attending Palo Alto Networks training?

- To enhance the participant's understanding of how to troubleshoot the full line of Palo Alto Networks next-generation firewalls.
- To provide hands-on troubleshooting as recommended by Palo Alto Networks best practice recommendations relating to network security, the configuration and operation of the Palo Alto Networks firewall.
- To help participants develop an in-depth knowledge of how to troubleshoot visibility and control over applications, users, and content.
- Prevent unknown threats

The skills you will learn by attending the Palo Alto Networks EDU-330: Firewall Troubleshooting three-day instructor-led training course:

- Use Firewall tools, including the WebUI and CLI, to investigate networking issues
- Follow proven troubleshooting methodologies that are specific to individual features
- Understand the Flow-Logic used by the Next-Generation Firewall
- Learn how to configure and enable Packet Capture and advanced Packet-Level Diagnostic Features
- Identify necessary System Daemons and their logs to resolve various real-life scenarios
- Solve numerous advanced, scenario-based challenges
- Troubleshoot common issues related to firewall deployment
- Troubleshoot connectivity problems
- Troubleshoot policy and NAT-related issues
- Troubleshoot User-ID
- Troubleshoot Site-to-Site VPN problems
- Troubleshoot GlobalProtect™ related issues
- Identify performance problems
- How to use the Customer Support Portal

Red Education



Why train with us

Education is the key to success. But what does it mean to be "educated?" Does it simply suggest going to school and getting good grades? Or is there more to it than that? We at Red Education believe education is more than memorising facts and regurgitating information. It's about developing the skills and knowledge so that security engineers can succeed in whatever field they choose; it's all about providing quality, affordable education accessible to everyone and changing behaviour.

In the last nine consecutive years, Red Education has won ATC of the Year, Instructor of the Year, and the prestigious Australian Business Award for Training Innovation. These awards prove our company delivers the quality of training demanded by the industry.

Our customer satisfaction scores are also industry-leading, with an average score of 4.8 out of 5 across all courses. We are very proud of these accomplishments and our commitment to excellence in everything we do. They consistently rate us as having the best instructors in the region, and they rave about our overall customer experience.

Now that you know all about the benefits of EDU330, it's time to sign up for the course! By enrolling now, you'll be able to take advantage of all the great benefits this course offers.

CUSTOMER SATISFACTION IS GUARANTEED!

Digital Certification Badge

So if you're looking to take your troubleshooting skills to the next level, look no further than the Palo Alto Networks Firewall Troubleshooting Training course! Don't wait.
Contact us NOW.