ZTCA Latest Real Test - Pdf Demo ZTCA Download

Zero Trust Container Architecture (ZTCA): A Framework for Applying Zero Trust Principals to Docker Containers

Darragh Leahy and Christina Thorpe
Technological University Dublin, Blanchardstown, Dublin, Ireland
ZeroTCA@gmail.com
christina.thorpe@tudublin.ie

Abstract: Containerisation is quickly becoming an accepted industry standard for development environments and Gartner, in a recent market forecast, estimated that by 2022 more than 75% of organisations will be using containers in production deployments. With this explosion in growth comes an added focus on security and best practices for using containers. The use of containers, in particular Docker containers, has altered some of the more traditional deployment paradigms by giving control of deployments to the development teams. This has massively benefited the DevOps release cycle, but at the expense of many mature security and review processes that are integrated into traditional deployments. Like all systems, containers need frameworks to guide best practices for deployments and to ensure mistakes are not made that increase the risk level or attack surface of an application or service using containers, or the containers themselves. Indeed, according to a recent presentation during DevSecCon24 by Justin Cormack, Security Lead at Docker Inc., Cormack believes most security issues related to Docker are due to misconfiguration rather than direct exploit. While work has been previously conducted with regards to container security and separately applying Zero Trust Networking Architecture to containers, in this work we will investigate the security state of a default deployment of the Docker container engine on Linux and analyse how the principals of Zero Trust Architecture can be extended beyond the domain of networking, distilled into a "Zero Trust Containers Architecture" and applied to secure Docker deployments. In order to determine this, research was conducted into the current state of Docker security and Zero Trust Architecture. Practical and theoretical attacks were reviewed against a default Docker deployment to identify common themes and areas of issue. Results were used to advise a generalised trust-based framework which was then used to analyse a Docker deployment and validate mitigation of a selection of the identified attacks, proving out the concept of the proposed "Zero Trust Container Architecture" framework.

Keywords: Zero-Trust Architecture, Containerisation, Virtualisation, Security, DevSecOps

1. Introduction

Regardless of the forecast advances made by Docker Inc. in securing the product, the current security state of Docker is still a concern. Many security issues do exist currently, this is driven by a combination of technical factors such as vulnerabilities in the Docker Engine and Linux OS, misconfigurations of the Docker system or limitations of its design, however equally important are the concepts of 'system espoused' versus the 'system in use' problem. That is, the difference between what the product developer aims to achieve and consequently what they design for, as opposed to how the system is actually used in the real world. Work in (Martin 2018) demonstrated that a fundamental difference exists in what Docker considers the recommended use case versus what is actually being done in the real world. These differences, combined with the technical issues, as well as the rapid adoption of Docker have combined to create a potential storm of security concern. Zero Trust Networking Architecture (ZTA/ZTNA) is a design paradigm for networks which identified the need to move the defensive perimeter down from the edge of the network. In a traditional edge firewall and Intrusion Prevention/Intrusion Detection system, the edge of the network was considered the point of security, with anything inside broadly trusted. ZTA advised to redefine this boundary away from the perimeter and down to the user and resource in use. ZTA re-frames the question of network security into one of trust, that is, the inherent insecurity of assumed trust that exists once inside the network perimeter. ZTA advises to assume no explicit trust within a system, that internal users accessing internal services without explicit authentication and authorisation cannot be trusted any more than external actors. ZTA's ethos can be summed up with the line 'never trust, always verify'. ZTA offers opportunities to be re-purposed for use in securing Docker containers and thereby mitigating some of the known configuration issues as well as minimise the surface area of exploits and vulnerabilities.

This research will review and identify the issues with a default deployment of Docker through a combination of practical experimentation to answer the core research question: ***Using a novel generalised trust-based framework, based on the proven principals of ZTA, can a Docker deployment be secured?*** Some ancillary questions have also been defined: (1) What issues currently affect a default deployment of Docker? (2) What

Our company conducts our ZTCA real questions as high quality rather than unprincipled company which just cuts and pastes content into their materials and sells them to exam candidates. We have always been the vanguard of this field over ten years. It means we hold the position of supremacy of ZTCA practice materials by high quality and high accuracy. Besides, all exam candidates who choose our ZTCA real questions gain unforeseen success in this exam, and continue buying our ZTCA practice materials when they have other exam materials' needs. It is our running tenet to offer the most considerate help and services for exam candidates just like you. By virtue of our ZTCA Study Tool, many customers get comfortable experiences of whole package of services and of course passing the ZTCA exam successfully. Just hold the supposition that you may fail the exam even by the help of our ZTCA study tool, we can give full refund back or switch other versions for you to relieve you of any kind of losses. What is more, we offer supplementary content like updates for one year after your purchase.

Zscaler ZTCA Exam Syllabus Topics:

Topic	Details
Topic 1	• Control Content & Access: This domain covers how organizations assess risk, prevent compromise, and protect sensitive data when users access applications or services. It emphasizes adaptive controls, security inspection, and data protection practices aligned with Zero Trust principles.
Topic 2	• An Overview of Zero Trust: This section explains the shift from traditional network security models to a Zero Trust architecture. It covers how Zero Trust connections are established and introduces the key principles of verifying identity, controlling content and access, enforcing policy, and securely initiating connections to applications.

Topic 3	- Zero Trust Architecture Deep Dive Introduction: This domain introduces the foundational concepts of Zero Trust Architecture and prepares learners for deeper topics in the course. It provides a high-level understanding of how the Zero Trust framework operates within modern security environments.
Topic 4	- Zero Trust Architecture Deep Dive Summary: This domain provides a recap of the Zero Trust concepts and practices discussed throughout the course. It reinforces the key elements required to successfully design and implement a Zero Trust architecture.
Topic 5	- Enforce Policy: This section explains how security policies are applied and enforced across user connections and application access. It focuses on ensuring that access decisions follow defined policies and that connections to applications remain secure and compliant.

>> ZTCA Latest Real Test <<

Pdf Demo ZTCA Download, Latest ZTCA Dumps Questions

One of the key factors for passing the exam is practice. Candidates must use Zscaler ZTCA practice test material to be able to perform at their best on the real exam. This is why Itcertmaster has developed three formats to assist candidates in their Zscaler ZTCA Preparation. These formats include desktop-based Zscaler ZTCA practice test software, web-based practice test, and a PDF format.

Zscaler Zero Trust Cyber Associate Sample Questions (Q36-Q41):

NEW QUESTION # 36
Enterprises can deliver full security controls inline, without needing to decrypt traffic.

- A. False
- B. True

Answer: A

Explanation:
The correct answer is B. False . In Zero Trust architecture, full inline security depends on the ability to inspect what is actually inside the traffic flow, not just the fact that a connection exists. When traffic is encrypted, security services cannot fully evaluate malware, command-and-control traffic, sensitive data movement, risky application behavior, or policy violations unless the traffic is decrypted and inspected .
Zscaler's TLS/SSL inspection guidance makes this clear by positioning decryption as essential for complete visibility and enforcement across encrypted internet traffic.
Without decryption, an organization may still apply limited controls such as destination reputation, IP-based filtering, category decisions, or metadata-based enforcement. However, that is not the same as full security controls inline . Full Zero Trust protection requires deeper visibility into content and transactions so that threat prevention, Data Loss Prevention (DLP), cloud application controls, sandboxing, and other advanced protections can be applied accurately. Because modern traffic is heavily encrypted, failing to decrypt creates blind spots and weakens policy enforcement. Therefore, the statement is false: enterprises cannot deliver full inline security controls across encrypted traffic without decryption.

NEW QUESTION # 37
What is policy enforcement built to enable?

- A. Granular access from the verified initiator only to the verified application, under the correct risk and content controls.
- B. Forwarding traffic on to a virtual DMZ.
- C. Network access to all available applications.
- D. Blocking access to applications and the network.

Answer: A

Explanation:
The correct answer is C. In Zero Trust architecture, policy enforcement exists to provide precise, least- privileged access. It is not

designed to place a user broadly onto the network, and it is not limited to simply blocking everything. Instead, it enables granular access from the verified initiator to the specific verified application, while also applying the correct policy conditions related to risk, content inspection, and business requirements.
This is one of the central differences between Zero Trust and legacy security models. Traditional VPN and firewall architectures often grant broad network connectivity first and then attempt to restrict behavior afterward. Zero Trust reverses that logic. The user is not trusted because they reached the network. Instead, the user receives access only to the exact application or service that policy permits, and only under the validated conditions for that request.
That is why granular policy enforcement is so important. It reduces attack surface, limits lateral movement, and aligns access with identity, context, and content-aware controls. Therefore, the best answer is granular access from the verified initiator only to the verified application, under the correct risk and content controls.

NEW QUESTION # 38
A Zero Trust policy enablement and subsequent application connection should always be permanent.

- A. False
- B. True

Answer: A

Explanation:
The correct answer is B. False . Zero Trust architecture is built around least-privileged, context-based access
, not permanent entitlement. Zscaler's ZPA guidance explains that ZTNA provides users secure connectivity to private applications without ever placing them on the network and that access is granted based on granular policies . When a user attempts to access a resource, the user's context is matched against policy, and if the requirements are not met, the application is effectively unreachable. This means access is conditional and specific , not permanently enabled after one successful decision.
Zscaler also emphasizes that users connect directly to apps, not the network , minimizing attack surface and eliminating lateral movement. A permanent connection model would resemble legacy VPN behavior, where a user gains broad, lasting access to a routed network environment. Zero Trust rejects that model. Instead, policy enablement and application connectivity are tied to the active request and the context at the time of access. If posture, location, or policy conditions change, the decision can also change. Therefore, Zero Trust connections should not always be permanent, and the correct answer is False .

NEW QUESTION # 39
Zero Trust access can work over any type of network.

- A. True
- B. False

Answer: A

Explanation:
The correct answer is A. True. Zero Trust architecture is designed so that access decisions are independent of the underlying network as a trust boundary. Zscaler's ZPA guidance states that Zero Trust Network Access (ZTNA) gives users secure connectivity to private applications without ever placing them on the network, and that users can access applications without sharing network context with them.
Zscaler Client Connector guidance also states that it connects user devices to Zscaler cloud-hosted services independent of the user's location, and the ZIA traffic-forwarding architecture explains that the same authentication and policy follow the user wherever they are. This means the access model can work across corporate networks, home broadband, public Wi-Fi, mobile networks, branch environments, and other transport types, because trust is derived from identity, posture, context, and policy, not from being on a particular network.
The network still carries the traffic, but it does not determine trust. That is one of the defining characteristics of Zero Trust. Therefore, the statement is true: Zero Trust access can work over any type of network.

NEW QUESTION # 40
How is risky behavior controlled in a Zero Trust architecture?

- A. Deploying best-in-class security appliances.
- B. Permanent quarantining of devices in a particular VLAN.

- C. Logging violations in a public database.
- D. Re-categorization of an initiator, and their organization, so that subsequent access requests are limited, deceived, or stopped.

Answer: D

Explanation:
The correct answer is B . In Zero Trust architecture, risky behavior is controlled through continuous evaluation and policy-based response , not through static network constructs such as VLAN quarantine or dependence on standalone appliances. Zscaler's Zero Trust guidance emphasizes granular, context-based policies that evaluate the user, device, application, and surrounding conditions before and during access. In the ZPA architecture material, Zscaler states that applications should remain inaccessible unless the user is authorized, and policy should be independent of IP address or location.
The strongest architecture match is option B , because Zscaler documentation describes security outcomes such as inline prevention, deception, and threat isolation for compromised or risky users. That means when behavior becomes suspicious, later access attempts can be restricted, misdirected, or blocked based on updated policy context. This is fundamentally different from a legacy response such as placing a device permanently in a VLAN, which remains network-centric and coarse-grained. Logging alone also does not control risk, and simply deploying security appliances does not deliver Zero Trust by itself. Zero Trust controls risky behavior by dynamically adjusting enforcement based on observed context and threat posture, which best aligns with option B.

NEW QUESTION # 41
......

Our Zscaler Zero Trust Cyber Associate exam question has been widely praised by all of our customers in many countries and our company has become the leader in this field. Our product boost varied functions and they include the self-learning and the self-assessment functions, the timing function and the function to stimulate the exam to make you learn efficiently and easily. There are many advantages of our ZTCA Study Tool. To understand the details of our product you have to read the introduction of our product as follow firstly.