**ENN523 Advanced Network Engineering**

**Assignment Part 2**

**Call for Book Chapters**

Group16

**JUI-TENG HUANG**

N10596623

**YI-CHEN CHEN**

N11564628

**ALI MONAVVARI**

N11760311

# Overview

Since many software and applications support virtualization, numerous new network security approaches have emerged. Micro-segmentation is one such useful solution for enhancing network security on virtualized platforms, such as virtual machines and the cloud. Unlike traditional segmentation, micro-segmentation provides a more flexible and scalable environment for users to protect their data.

In this report, we will provide a clearly explanation of micro-segmentation, detailing its implementation, benefits, and challenges across various domains, including 5G networks, cloud security, and virtual machines. Additionally, we will explore the integration of micro-segmentation within the Zero Trust Security model, a framework that focuses on continuous verification, least privilege access, and the segregation of network traffic to enhance defense mechanisms against both internal and external threats.

# Table of Content

[Overview 1](#_Toc681259214)

[Table of Content 2](#_Toc472122611)

[1. Background 3](#_Toc730761964)

[2. Evaluation 4](#_Toc855907220)

[2.1 Segmentation 5](#_Toc2015304153)

[2.2 How micro-segmentation implemented in Cisco 5](#_Toc304461870)

[2.3 All Types of Micro-segmentation 5](#_Toc1937767980)

[2.4 Advantage and Disadvantage of Micro-Segmentation 6](#_Toc2125531860)

[3. Zero-trust Security model 8](#_Toc1317760221)

[3.1 Core Principles of Zero Trust 8](#_Toc1660169815)

[3.2 Implementation of the ZTA Components 9](#_Toc1838966370)

[3.3 Benefits of Zero Trust Model 9](#_Toc2088103951)

[3.4 Challenges and Considerations 9](#_Toc1743216016)

[4. Micro-segmentation in different areas 11](#_Toc29332832)

[4.1 Micro-segmentation 5G Network 11](#_Toc113182699)

[4.2 Micro-segmentation in cloud security 13](#_Toc1847939342)

[4.2.1 ZTA & Micro-segmentation 14](#_Toc1026493609)

[4.2.2 Challenges to implementing cloud security: 14](#_Toc1584029868)

[4.2.3 Best Practices to implement Micro-segmentation in Cloud 15](#_Toc2147312017)

[4.2.4 Network Level Control in Cloud Security Model 15](#_Toc1598603466)

[4.2.5 Cloud vs. Traditional Security Architecture 15](#_Toc690041744)

[4.3 Micro-segmentation in Virtual Machine 16](#_Toc2139347720)

[Chapter Summary 18](#_Toc648259122)

[Reference 19](#_Toc256692767)

[Figure References 20](#_Toc428958045)

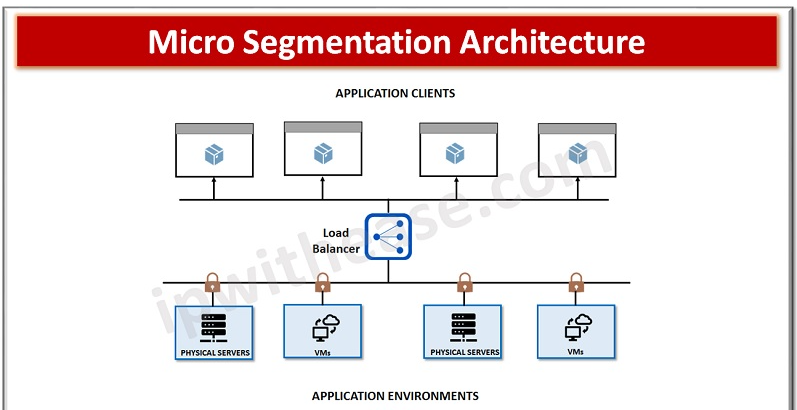
[Acronyms 20](#_Toc1833390234)

# 1. Background

Micro-segmentation is a network security technique that divides a network into smaller, distinct security segments, each tailored to individual workloads or applications. In other words, it is a technique in network security that allows security architects to establish per-machine network security zone boundaries in data centres and cloud deployments, to segregate and independently secure workloads. Micro-segmentation employs firewall policies to restrict east-west traffic between workloads, based on a zero-trust security approach, to minimize attack surfaces, prevent the spread of threats, contain breaches, and enhance regulatory compliance. Each micro-segments is isolated from others and will not automatically compromise the others, which is designed to contain breaches and prevent lateral movement of threats across the network. Each microsegment establishes its own security policy. These policies not only define the behaviours of each microsegment but also access controls and traffic rules tailored to the specific needs of each segment by using network virtualization technology. In this case, these policies enforce the use of network security tools without needing to download them. For this reason, micro-segmentation heavily relies on policy management and enforcement capabilities to ensure a secure network environment because automated systems often assist in managing and dynamically adjusting these policies based on network conditions and security threats. Additionally, micro-segmentation allows users to monitor each microsegment individually, which enhances the efficiency in detecting errors, and easier to pinpoint issues, and respond promptly.

Micro-segmentation technology began with the rise of virtualization technology, early 2000s. VMware, a company that focuses on this area, started to develop this technology. However, unlike micro-segmentation's focus on security today, it initially focused only on enhancing efficiency. Until Late 2000s and early 2010s, As cloud computing started to gain momentum, the need for improved network security within virtualized environments became clear. This period marked the conceptual beginnings of micro-segmentation, where isolation within virtual environments was recognized as a potential method to enhance security. In 2013, VMware NSX was released which introduced advanced network virtualization capabilities, including fine-grained security policies that could be applied to individual workloads.

This was a significant shift that helped organizations improve security within their data centres and cloud environments. Until now, the adoption of micro-segmentation has accelerated with the increasing move towards hybrid and multi-cloud environments. The growing awareness of cybersecurity threats and the adoption of zero-trust security models have further driven the need for technologies like micro-segmentation. The technology has become integral to strategies that require granular control over network traffic and stringent isolation between workloads. In terms of VMware, another company also developing its micro-segmentation technology is Cisco, which developed ACI to provide an application-centric infrastructure that simplifies operations and enhances security by automating policy enforcement and network provisioning across entire data centers, extending micro-segmentation capabilities to support dynamic and scalable environments.



**Figure 1 - micro-segmentation Architecture**

# 2. Evaluation

## 2.1 Segmentation

Micro-segmentation is a cutting-edge technology that enhances network security, evolving from traditional segmentation practices. Unlike micro-segmentation, which divides network services into their own secure zones, traditional segmentation, like VLANs, focuses on broader network divisions. A notable example of traditional segmentation is the implementation of Cisco Virtual LANs (VLANs) within Layer 2 of the access switch as voice VLANs. At Layer 3 of the access switch, network engineers can implement Access Control Lists (ACLs) on VLAN interfaces to prevent attacks [1].

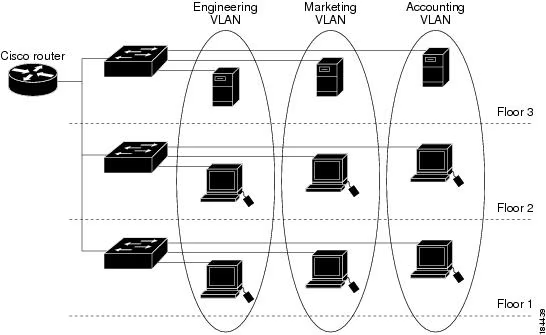


Figure 2 – VLANs Example

Figure 2 illustrates how VLANs divide a network into multiple segments, typically based on departmental or functional needs, thus segregating network traffic across the same physical infrastructure but maintaining distinct broadcast domains. This segmentation enhances security and performance by limiting the broadcast scope and reducing the potential attack surface.

However, while VLANs offer considerable advantages in segmenting traffic, they do not provide the granularity required to control east-west traffic—traffic that travels within the data center or between servers on the same network segment. This limitation is where micro-segmentation plays a crucial role. Micro-segmentation extends the concept of segmentation by not only isolating network traffic but also applying security policies at a much finer granularity. Each workload or application instance can have its own unique security policy, effectively containing potential breaches to a single point and significantly limiting an attacker's ability to move laterally within the network.

## 2.2 How micro-segmentation implemented in Cisco

As mentioned above, micro-segmentation offers some security benefits that traditional segmentation does not provide. One of the main benefits is that micro-segmentation uses policies to control each segment, eliminating the need for separate networks with VLANs, which increases flexibility and security. In Cisco devices, two modern architectures that utilize micro-segmentation technology and policy enforcement are Cisco Software-Defined Access (SDA) and Cisco TrustSec.

Cisco SDA, a component of the Cisco Digital Network Architecture (DNA), offers software-defined networking solutions tailored for campus environments [1]. The micro-segmentation in Cisco SDA has been implemented in Cisco Jabber (a voice chat tool). The security policy in Jabber ensures that users can move anywhere physically while still being protected by network security. Additionally, Jabber implements segmentation for managing network traffic, allowing Jabber's traffic to be isolated from other network traffic.

## 2.3 All Types of Micro-segmentation

**Application Segmentation:**

This method protects important applications, whether they are running on physical servers, virtual machines (VMs), or containers. It limits internal (east-west) communication within a network to meet security standards like PCI DSS, SOX, or HIPAA. For instance, only necessary parts of the network can interact with sensitive applications, reducing the risk of unauthorized access.

**Environmental Segmentation:**

This approach separates different environments such as development, testing, and production. By doing so, it prevents these environments from communicating with each other, which is generally unnecessary and can be a security risk if exploited by attackers. Traditional security methods cannot achieve this because these environments are often spread across various data centers, both on-premises and in the cloud.

**Tier-Level Segmentation:**

When an application has multiple parts, like a web server, an application server, and a database, it is useful to isolate each part from the others. This way, if an attacker compromises one part, they cannot easily move to another part. For example, even if the web server is attacked, the database remains protected.

**Process-Based Segmentation:**

This is a very detailed form of segmentation that focuses on individual processes or services. For example, a specific software service can be restricted to communicate only on certain network paths, using specific protocols and ports. This ensures that only authorized communications happen, enhancing security.

**User Segmentation:**

This type of segmentation uses groups in systems like Microsoft Active Directory. Instead of segmenting the network itself, it controls access based on user groups within a VLAN. This means that different users in the same network can have different access rights depending on their group membership. For example, an HR employee and an IT specialist might be on the same network but have access to different systems.

## 2.4 Advantage and Disadvantage of Micro-Segmentation

**Advantage**

While micro-segmentation is an emerging technology that has just developed in recent years, it is said that micro-segmentation could help improve the environment of information technology.

The weakness of security is the key feature that may have made a made a big advance in development. A typical case allows for granular and specific security policies to enhance the effectiveness and consistency of network protection measures [2]. Granular east-west policy control is a scalable method to set up a safe perimeter zone around every workload that works the same way for all workload types and environments. This could improve and expand the visibility and control of network or zone-based firewalls [3].

Similarly, SDN automates security management, which makes it easier for businesses to set up and follow their network security rules [4]. Software-defined networking (SDN) keeps the network's control plane and data plane separate. Because of this separation, network managers can use software to control security policies and the flow of data in one place. One easy way to divide a network into smaller, more manageable parts is to use SDN. We can refer to these smaller parts as virtual networks. There are different security policies for each virtual network, and you can keep them all separate [5].

This is an example of SDN format:

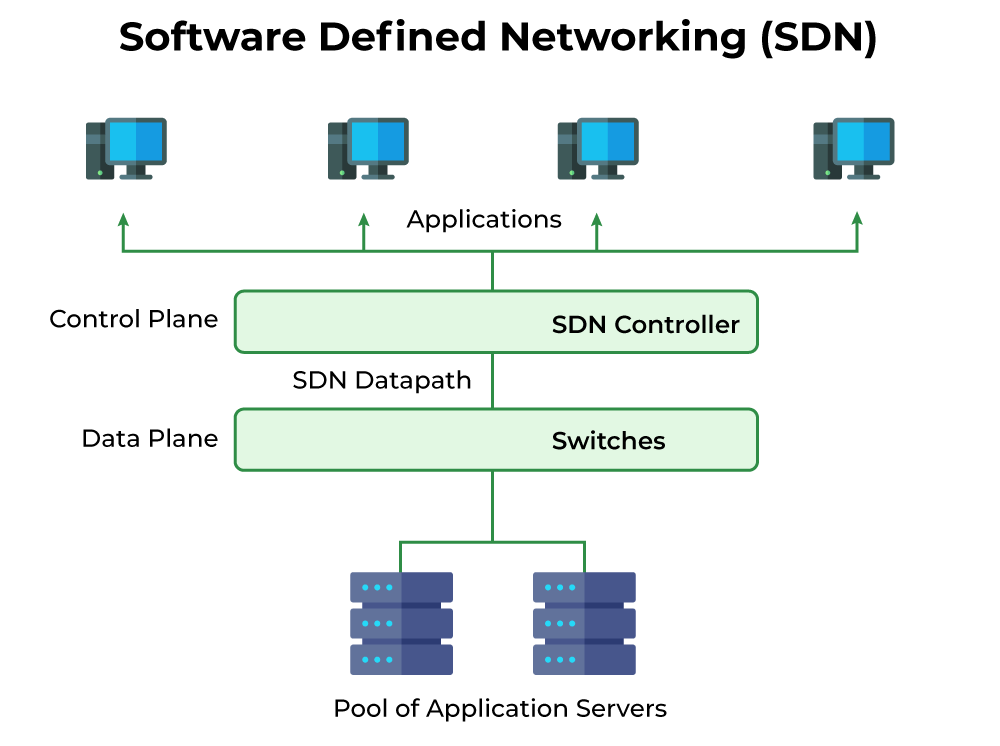


Figure 3: An SDN example [6]

Isolating devices reduces the possibility of a hacked device spreading to other devices or networks. Implementation options include VLANs, subnets, and micro-segmentation in SDN contexts. Each segment, or micro-segment, has a group of devices that can only communicate within the segment unless security regulations explicitly allow it, whose benefits include limiting potential breaches to a smaller sector and facilitating risk management and mitigation.

At the same time, controlling data flow may ensure authorised data transfers, which reduces the risk of malicious transmission or leakage when established firewall and routeing rules to control data flow within the network. In SDN topologies, these rules are managed centrally by the SDN controller, which dynamically adjusts them depending on real-time network traffic and threat analysis, preventing malware transmission, restricting potentially compromised data transfer, and ensuring compliance with privacy rules.

**Disadvantage**

Despite it looks like micro-segmentation offers a lot of benefits, however, some drawbacks seem come to light.

“The more micro-segment you implement, the more difficult it becomes to operate and maintain [7].”

Nonetheless, it has been predicted that increasing the likelihood of implementing systems in inappropriate areas is a future trend. So, what possible issues that “over implementation” may bring to the IT world [7]?

* Bottlenecks in the network
* Increased complexity in operation, prone to mistakes from the operations teams
* Lack of understanding from the engineering teams leading to de-segmentation
* Uncertainty in the implementation leading to maturity regression
* Lack of trust in the overall model leading to doubt in the team’s mind

1. **Bottlenecks in the network**

Micro-segmentation divides the network into smaller parts, each with its own series of security policies. This makes things safer by making it harder for attackers to move laterally, but it can also cause problems if it is not put in place carefully. Over-segmentation can lead to too much traffic between segments, which can slow down data transmission and block up network paths.

1. **Increased complexity in operation, prone to mistakes from the operations teams**

It gets harder to manage segments as the number of them grows. It can be hard for operational teams to keep track of all the rules that apply to each segment, which can lead to mistakes or missed security holes. Meanwhile, keeping up with managing a network that is very divided is another challenge, as you need to know every detail and understand how each component works.

1. **Lack of understanding from the engineering teams leading to de-segmentation**

Complex micro-segmentation schemes require in-depth knowledge and expertise from engineering teams responsible for their implementation. If employees on the team are unfamiliar with the fundamental concepts or the logic behind certain segmentation choices, they might try to make the network architecture simpler by removing or omitting segmentation completely. This breaking down of segments hurts the security that micro-segmentation was provided, leaving the network vulnerable to attacks.

1. **Uncertainty in the implementation leading to maturity regression**

Overuse of micro-segmentation can make it unclear whether or not certain segmentation strategies are needed or effective. It might be difficult for teams to figure out how segmentation affects security and operational performance. This uncertainty can cause teams to abandon on segmentation efforts and go back to less detailed or unexpected security measures, which makes the network less secure in the future.

1. **Lack of trust in the overall model leading to doubt in the team’s mind**

When there is too much segmentation without a clear reason or actual advantages, team members can lose belief in the micro-segmentation plan. If the segmentation strategy appears illogical or overly complex without carrying commensurate security enhancements, it can produce scepticism and doubt within the team, finally, lacking confidence may further undermine collaboration and cooperation, hindering efforts to maintain and optimize the segmented network effectively.

# 3. Zero-trust Security model

The Zero Trust Security model is a contemporary cybersecurity framework that rejects the notion of inherent trust within a network, regardless of whether access is initiated from within or outside the network perimeter. The model operates on the principle that threats can exist both inside and outside the network, thus mandating strict verification processes for all access requests. Zero Trust model includes its principles, components, benefits, and challenges, along with examples to illustrate its application [8].

## 3.1 Core Principles of Zero Trust

The Zero trust model architecture is built based on some principles which are listed as follows:

**Continuous Verification:**

Every access request is subject to continuous verification based on all available data points, such as user identity, device health, location, and anomalies in behaviour. For instance, an employee logging in from a new location or device might be required to undergo additional verification steps.

**Multi-Factor Authentication (MFA):**

MFA is a common example, where users must provide multiple forms of verification, such as a password and a temporary code sent to their phone. End users have limited access to review and add their authentication method by adding or removing their personal devices into the security portal after first registration.

For instance, Microsoft Azure users can download and use Microsoft Authentication App on their mobile and prove their identity to Microsoft Azure and depended services.

Least Privilege Access:

**Role-Based Access Control (RBAC):**

Users are granted the minimum level of access necessary for their role. For example, a finance employee might have access to financial records but not to HR documents. When number of users in departments grows RBAC provide flexible way to adjust the access to each department of security policy and privilege usage has changed for whole organization.

**Just-In-Time (JIT) Access:**

Access is granted for a limited time to perform specific tasks, reducing the window of opportunity for misuse.

**Micro-Segmentation:**

The network is divided into smaller, isolated segments, each with its own security controls. For instance, an organization might segment its network into different zones for HR, finance, and IT, ensuring that a breach in one zone does not compromise the others.

**Encryption and Monitoring:**

Data is encrypted both in transit and at rest, and continuous monitoring is implemented to detect and respond to suspicious activities.

## 3.2 Implementation of the ZTA Components

Identity and Access Management (IAM):

Centralized IAM Systems: Solutions like Microsoft Azure AD or Entra ID provide centralized control over user identities and access permissions, facilitating secure and streamlined access management.

Network Segmentation and Micro-Segmentation:

Software-Defined Networking (SDN): Technologies like VMware NSX allow for granular network segmentation, enabling policies that isolate traffic between different segments.

Endpoint Security:

Endpoint Detection and Response (EDR): Tools such as CrowdStrike Falcon or Microsoft Defender ATP continuously monitor endpoints for threats, providing real-time detection and response capabilities.

Data Protection:

Data Loss Prevention (DLP): Systems like Symantec DLP monitor data usage and movement, preventing unauthorized access and exfiltration of sensitive information.

Continuous Monitoring and Analytics:

Security Information and Event Management (SIEM): Platforms like Splunk or IBM QRadar aggregate and analyze logs from across the network to detect anomalies and potential security incidents.

Application Security:

Web Application Firewalls (WAF): Solutions such as AWS WAF protect web applications from common exploits and vulnerabilities.

## 3.3 Benefits of Zero Trust Model

Enhanced Security Posture:

By removing implicit trust, Zero Trust minimizes the risk of insider threats and lateral movement by attackers within the network. For example, if an attacker compromises a user’s credentials, they still face significant barriers accessing critical systems and data.

With micro-segmentation and least privilege principles, Zero Trust confines potential breaches to isolated segments, reducing the overall impact. For instance, if malware infects a user’s device, it is restricted to the segment that the device is allowed to access. Zero Trust helps organizations meet regulatory requirements by enforcing strict access controls and data protection measures. Compliance frameworks like GDPR, HIPAA, and PCI-DSS mandate such controls to protect sensitive data. Also, continuous monitoring and detailed logging provide comprehensive insights into user activities and network traffic, aiding in proactive threat management. For example, detailed audit logs can help quickly trace the source and impact of a security incident.

## 3.4 Challenges and Considerations

Implementing Zero Trust can be resource-intensive, requiring significant investment in new technologies and continuous management. Organizations must assess their current infrastructure and plan for phased implementation.

Transitioning to Zero Trust involves a significant cultural shift within the organization. Employees and IT staff must adapt to new security protocols and practices, which may initially be met with resistance.

Integrating Zero Trust with legacy systems can be challenging. Older systems may lack the necessary support for modern authentication methods or network segmentation techniques, necessitating upgrades or replacements.

Google's BeyondCorp:

Google implemented its own Zero Trust framework called BeyondCorp, which allows employees to work securely from any location without relying on a traditional VPN. Access is granted based on device health and user identity, with continuous monitoring to detect anomalies.

Microsoft Zero Trust Deployment:

Microsoft uses its Zero Trust architecture to protect its cloud services. This involves MFA, conditional access policies, and continuous risk assessment to ensure secure access to Microsoft 365 services.

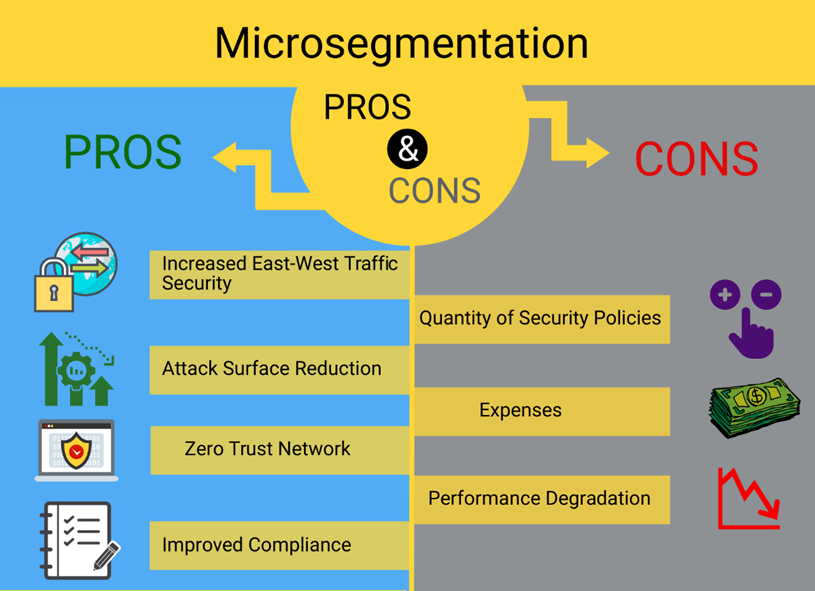


Figure 4 – Micro-segmentation pros and cons

**Micro-Segmentation Security Architecture Design**

Micro-segmentation is a cornerstone of the Zero Trust Security model, providing fine-grained control over network traffic within and between application workloads. This approach involves creating isolated segments within the network, each governed by its own set of security policies. Below is a detailed design of a micro-segmentation security architecture.

**Design Principles**

1. **Granular Control**:
   * Implement security policies at the individual workload or application level. This involves defining rules that control which services can communicate with each other, based on factors such as application type, user identity, and device health.
2. **Dynamic Policy Enforcement**:
   * Use dynamic, context-aware policies that adapt to changes in the network environment. For instance, policies can adjust based on real-time threat intelligence and behavioral analytics.
3. **Automation and Orchestration**:
   * Automate the deployment and management of security policies using orchestration tools. This ensures consistency and reduces the likelihood of human error.

**Key Components**

1. **Policy Definition and Management**:
   * Centralized platforms for defining, managing, and enforcing security policies across all segments. Examples include VMware NSX and Cisco Tetration, which provide comprehensive tools for policy creation and management.
2. **Segmentation Gateway**:
   * Gateways that enforce policies and monitor traffic between segments. These can be implemented using virtual firewalls or dedicated segmentation appliances.
3. **Micro-Segmentation Agents**:
   * Lightweight agents installed on endpoints and workloads that enforce security policies and report on compliance. These agents communicate with the central policy management platform to ensure consistent policy enforcement.
4. **Visibility and Analytics Tools**:
   * Tools that provide detailed visibility into network traffic and application interactions. This includes SIEM platforms like Splunk, which aggregate and analyze log data to identify potential threats and policy violations.

**Implementation Steps**

1. **Asset Inventory and Classification**:
   * Conduct a thorough inventory of all network assets, including devices, applications, and data flows. Classify assets based on their criticality and sensitivity.
2. **Baseline Security Policies**:
   * Define baseline security policies for each class of assets. These policies should include rules for access control, data protection, and incident response.
3. **Network Segmentation**:
   * Segment the network into smaller, isolated zones. Each zone should be governed by its own set of security policies. For example, create separate segments for HR, finance, and IT departments.
4. **Micro-Segmentation Implementation**:
   * Deploy micro-segmentation agents on all endpoints and workloads. Configure segmentation gateways to enforce policies and monitor traffic between segments.
5. **Continuous Monitoring and Adjustment**:
   * Continuously monitor network traffic and application interactions. Use analytics tools to identify potential threats and policy violations. Adjust security policies as needed to address emerging threats and vulnerabilities.

# 4. Micro-segmentation in different areas

## 4.1 Micro-segmentation 5G Network

**Introduction**

The mobile network has experienced transformative development in increasingly complex and varied ways. It is hard to believe that only forty years have passed since the advent of wireless cellular technology, progressing from the first generation (1G) to the fifth generation (5G). However, "the more operations placed in the network, the more opportunities there are for an adversary to do significant damage [4]." Alongside these advancements, new security challenges concerning the network environment have emerged. Whether in public or personal use environments, devices are experiencing a revolution in their functionality.

In the past, people used products with single functions; nowadays, these products are gradually being updated to digitally combine multiple functions by integrating into a wireless network. However, if a hack occurs on one device, it could potentially jeopardize other devices connected to the same network. In recently years, some studies have founded that micro-segmentation can contribute to 5G network in aspects of security, efficiency, as well as management, further applied in various fields.

**5G Network Security**

Micro-segmentation brings a lot of important advantages for 5G networks, including aspects of security, efficiency, and management. Despite the fact that segmentation is a quite new technology and that not much research has been done about it, some research has shown its usefulness in security.

First of all, micro-segmentation enables customised security policies that are tailored to each microsegment or workload in order to guarantee network security.

When each segmentation has separate access control policies, it could effectively reduce attackers moving laterally within the network until they reach their final destination, causing serious security threats issues. Give an example based on enterprise scenario, an attack may carry computer virus, be started from an employee’s device, then try to infect virus laterally to the other employees’ devices within the network, even internal servers.

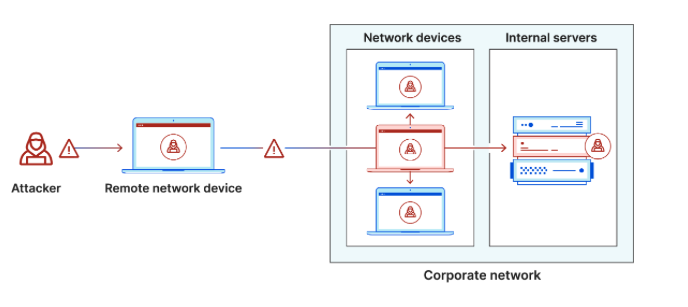


Figure 5: lateral movement

Nowadays, with the emergence of the IoT, more and more devices are being linked within the 5G network and the Internet. Examples include New Radio (NR), NR mmWave Prototype, Network-Wide Management Systems, etc. Therefore, network security is facing new challenges regarding 5G.

A micro-segment in a 5G network refers to a distinct component of the network that is separate from the physical 5G hardware. It is specifically designed for a particular application or user group and supports functions with similar security needs. Micro-segments can be defined as smaller divisions inside a larger entity, with a particular focus on enhancing network security. An end-to-end slice encompasses all the essential 5G functions required for organising a complete service, but a micro-segment may consist of simply a subset of services, sometimes even only one [2].

*End-to-End Slice (E2E):*

*An end-to-end slice in a 5G network is a comprehensive, isolated section of the network that includes all necessary 5G functions, providing a complete service. It includes the full range of network resources from the core network to the end user, ensuring tailored performance and security for specific applications.*

In order to ensure that application isolation is maintained, end-to-end connectivity should be achieved by linking many micro-segments, and each micro-segment can have individualised and detailed access controls, while customised security policies and processes that uphold distinct trust models relevant to each application. In fact, micro-segmentation allows for the formation of smaller and more similar sections inside the network. Finally, enhanced efficiency and precision can be attained in security [2].

To give an instance, the requirements for an end-to-end slice may related to the inclusion of Virtual Network Functions (VNFs) for radio access technology (RAT) and traffic acceleration in the access network. Additionally, packet routeing and mobility management functions are needed from the serving network, while subscriber authentication and accounting functions are required from the home network. Furthermore, functions for Internet connectivity are necessary from the transport network. In the case of a micro-segment, the number of functions may be reduced. The RAT and acceleration functionalities in base stations or mobile edge data centres at various locations may exist in distinct micro-segments. The functions of mobility management, routeing, and authentication, which are designated for different degrees of service quality, can be maintained in separate micro-segments [2].

Micro-segments can be distributed across many components of the 5G infrastructure. Figure 3 illustrates the correlation between the micro-segments and the 5G security architecture, as shown in the 5G-ENSURE reports from 2017 and 2016. The shown domain model represents a progression of the 3GPP's security architecture. It highlights the growing trend of infrastructure sharing by dividing domains into separate horizontal sections for infrastructure (hardware) and tenants (software) [2].

*The 3rd Generation Partnership Project (3GPP)*

*An international partnership that develops and maintains the technical specifications for 2G, 3G, 4G, LTE-Advanced, and 5G mobile networks. The partners include seven telecommunications standard development organisations: ARB, ATIS, CCSA, ETSI, TSG, ITU, and TTA. To guarantee the development of the newest technologies, the 3GPP also collaborates with other service providers like telcos, software vendors, mobile networks, and phone makers [9] [10].*

A diagram of a computer system

Description automatically generated

*Figure 6: Security architecture of 3GPP 5G*

The management domains emphasise the objective of 5G to prioritise more adaptable and cost-effective management. Moreover, the concept of slicing is demonstrated by the distribution of domains among various tenant domains. Micro-segments can be found in all domains, as they are divided into slices. Within user equipment domains, the micro-segments can be observed through the use of device-specific application isolation techniques. Micro-segments are implemented as logical sections of the network in access, serving, transit, residential networks, and potentially in 3rd party and IP service providers networks [2].

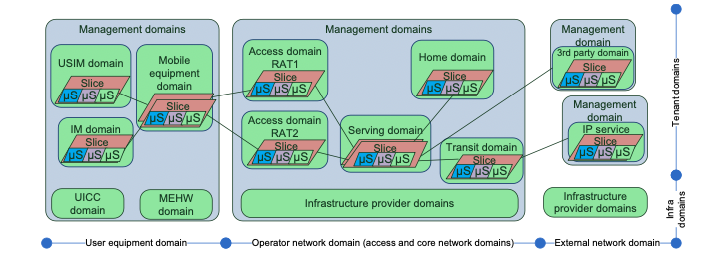
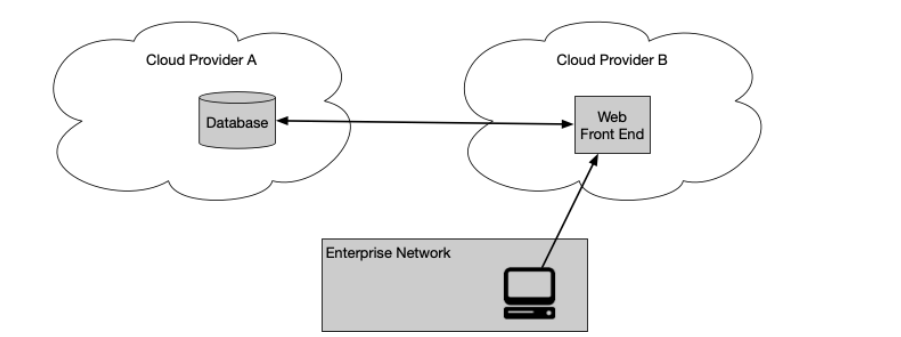


Figure7: Applying micro-segmentation in 5G security network architecture

## 4.2 Micro-segmentation in cloud security

### 4.2.1 ZTA & Micro-segmentation

One of the areas that Micro-segmentation has common usage is deploying ZTA – Zero Trust Architecture – utilizing multiple cloud providers. See figure 8.

 Figure 8: basic cloud

In this method, the enterprise has local network resources but uses two or more cloud service providers to host all services and applications and the data.

For ease of management and performance, cloud provide A should directly connect to data source located on cloud provider B without needing to tunnel back to the local network / on-premises.

This model design is a server-server implementation of the software defined perimeter (SDP) specification.

The zero trust approach to multi-cloud use is to place PEPs (Policy enforcement point) at the access point of each service and their data sources.

The client (via a portal or local installed agent) then accesses the PEPs directly. That way, the enterprise can still manage access to resources even when hosted outside the enterprise. One challenge is that different cloud providers have unique ways of implementing similar functionality. Enterprise architects will need to be aware of the how to implement their enterprise ZTA with each cloud provider.

### 4.2.2 Challenges to implementing cloud security:

While technical issues certainly need addressing, many obstacles to adopting micro-segmentation are organizational and behavioural. It's crucial to dispel misconceptions that hinder or delay these projects.

For instance, mid-size enterprises often fear that micro-segmentation requires a large staff for implementation and administration, making it seem suitable only for large enterprises. They may believe the policy definition process is overly complex, time-consuming, and risky if done incorrectly. Some organizations worry that stringent security controls will disrupt normal business processes. In reality, when implemented correctly, micro-segmentation enhances the productivity and effectiveness of stretched security teams. Visualization tools, automation, and standardized policy recommendations streamline the grouping of applications and policy creation, while a flexible policy engine allows for testing and refining policies to balance security and business needs.

Cloud customers often assume their cloud service providers' native security controls, which may include segmentation tools, are sufficient. However, providers operate on a shared security model, securing the cloud infrastructure while customers must secure their own operating systems, applications, and data. Moreover, a provider's controls are only effective within that specific environment. Enterprises must manage multiple security platforms and make manual adjustments as applications move across different cloud environments. Most native security controls focus on the port level (Layer 4) rather than the process level (Layer 7), where vulnerable applications reside, thus failing to reduce the attack surface adequately [11].

Perhaps the greatest cause of enterprise inertia is the fear that micro-segmentation is an 'all or nothing' proposition. Organizations are intimidated by the perceived need to secure every application in a single, extensive project that could take years and consume significant resources. However, successful enterprises have taken a phased approach, starting with a few priority projects, becoming familiar with the tools and processes, and gradually expanding. Like any new process, successful micro-segmentation requires internal champions and dedicated resources. By adopting a phased approach, organizations will begin seeing immediate value in their key priorities, and the learning curve will flatten as users gain experience.

### 4.2.3 Best Practices to implement Micro-segmentation in Cloud

Success with micro-segmentation requires more than just choosing the right solution; it involves efficient implementation aligned with organizational goals and agreed-upon success measures. Here are some best practices based on extensive experience with successful implementations:

Good Project Planning: Start with a planning workshop involving all stakeholders. Include your solution provider to lead, share experiences, and guide the process.

Define Roles and Responsibilities: Clearly assign ownership for various aspects of the project. Set priorities, goals, and milestones. Create an implementation hierarchy starting with easily defined projects.

Address Pitfalls and Obstacles: Identify potential issues and plan how to overcome them. Establish labelling conventions and policy creation specifics.

Integration: Determine the necessary IT infrastructure integrations to support the implementation and ongoing management of the program.

Thoughtful planning and advance mapping will save time during implementation.

Micro-segmentation effectively secures datacentre assets and supports a zero-trust model in hybrid or multi-cloud environments. Recent technological advances have made it viable for organizations of all sizes. By taking a phased approach with specific short-term goals, it's easier to operationalize. When done right, micro-segmentation optimizes cloud strategies, enhances agility and innovation, and significantly reduces the risk of compromise.

### 4.2.4 Network Level Control in Cloud Security Model

Network-level controls remain important in the cloud era, but their applicability is more restricted compared to an on-premises setup. For SaaS applications, applying network controls can be challenging since the service is provided by the cloud service provider (CSP) from shared instances serving multiple consumers, making it difficult to restrict access to specific customers or tenancies. However, in PaaS or IaaS scenarios, network-level controls become significantly more important.

To reduce the blast radius of any breach, it is a best practice in network security to segment the network. Micro-segmentation can effectively control traffic flows at the network layer. This is made easier with Software-Defined Networking (SDN) overlays that automate policy enforcement. SDN is integrated into cloud platforms, enabling micro-segmentation without additional investment in tools or specialized knowledge. Micro-segmentation allows for very strict controls over network resource access by isolating different service layers into their own network segments and controlling access between these segments. Any traffic passing through segment boundaries is inspected and denied by default unless specifically whitelisted.

Cloud networks, being SDN-based, have management built into the platforms, facilitating micro-segmentation adoption. SDN supports cloud networks, which are virtual and defined by the applications, solutions, or services. Using SDN in the cloud is not optional, but the correct mindset is needed to fully benefit from micro-segmentation. It's crucial not only to control ingress and egress traffic but also east-west traffic (between segments). For this, a default deny policy should be the standard.

### 4.2.5 Cloud vs. Traditional Security Architecture

When comparing traditional security architectures to cloud security architectures, IaaS (Infrastructure as a Service) is the closest match. In IaaS, many traditional security responsibilities are managed by the service provider, limiting customer control over how these aspects are secured. For instance, the integrity of the service is managed by the provider and can come in different tiers for customers to choose from.

Public clouds introduce unique security concerns due to their nature and service delivery methods. Many SaaS (Software as a Service) applications share PaaS (Platform as a Service) or IaaS components through a multitenancy model, where multiple customers share the same environment. In some industries, public cloud use is prohibited because data privacy is crucial, and the risk of data leakage is too high. Although service providers implement controls to protect customer data, there is always a risk of these controls being flawed, as seen in cases of cross-tenant access due to backend service vulnerabilities.

Data residency requirements can also be challenging with global cloud service providers. If customer data must remain in a specific region, a disaster in that region could wipe out the data, raising compliance and recovery concerns. Despite these issues, public cloud offerings improve security posture by handling many security concerns, such as physical security, which becomes the provider's responsibility. Customers also benefit from the provider's experience with security incidents faced by other customers, leading to better controls and detections.

Hybrid Cloud is another common scenario where a customer uses public cloud services for some purposes, private cloud services (dedicated to a single customer) for others, and on-premises environments for the most sensitive or business-critical assets or legacy services that can't be easily migrated. A multi-cloud presence, using services from multiple public cloud providers, is also part of the hybrid cloud category. Each provider has its own methods for handling security controls like authentication, auditing, and log management, requiring adjustments in security architecture while maintaining a similar high-level structure to traditional architectures.

The main research question, "How is cloud security architecture different from traditional security architecture?" reveals that the core elements are similar in both. However, their importance and the factors influencing them may differ. Cloud-specific elements like CSPM (Cloud Security Posture Management) and the shared responsibility model are necessary but aren't entirely new concepts. The core elements remain the same, with adjustments needed for balance and importance.

Organizations must modernize their security architecture to match the evolving landscape when adopting cloud services that are easy to onboard and accessible from anywhere. This modernization ensures the organization remains secure in the new environment.

## 4.3 Micro-segmentation in Virtual Machine

Virtual machine is one of example that micro-sagmentation is implemented to enhance the security. As we mentioned in backgorund, VMware is one of company that develop micro-sagmeantation so far and bring this teachnology to our world. NSX is developed From VMware for enhancing the security of virtual machine [12]. With the protection of virtual machine, the application run inside also can be protected. There are few points that NSX is helpful fro virtual machine security as provide below:

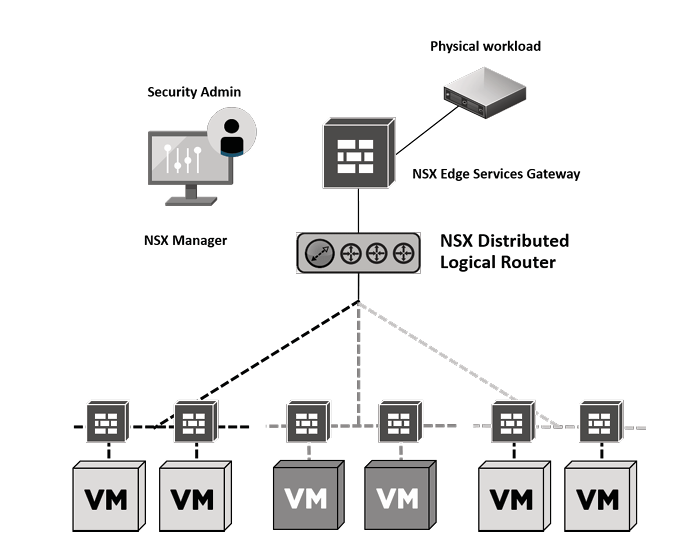


Figure 9 – distribution of firewall

**Distributed Stateful Firewalling**: Micro-segmentation reduces the attack surface by implementing distributed stateful firewalling. Each VM can have specific firewall rules applied, which scales with the infrastructure and provides protection on a per-application basis. this ensures that even as VMs move or change, their security policies remain consistent, reducing the risk of lateral attacks within the data center. Figure 1, showing how each virtul machine have their own firewall.

**Topology Agnostic Segmentation**: NSX allows for application firewall protection regardless of network topology. This means both Layer 2 (L2) and Layer 3 (L3) topologies are supported, with logical network overlays or VLANs.This flexibility ensures that micro-segmentation can be applied broadly across different network configurations without being tied to specific hardware or layouts.

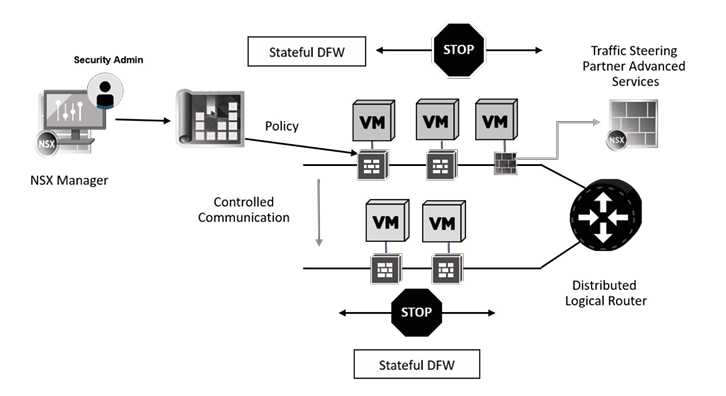


Figure 10 – centralized policy

**Centralized Policy Control**: NSX can use dynamic constructs such as OS types, VM names, or specific logical constructs to group and apply granular policies.This enables highly specific security controls tailored to each application or workload, enhancing protection without relying on broader network constructs like VLANs. Figure 2, NSX manager can directly control policies and set them in different firewalls.

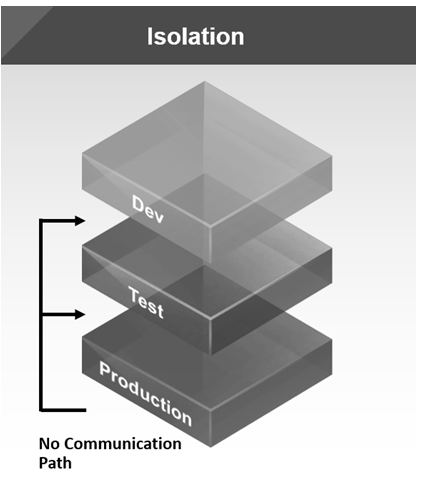
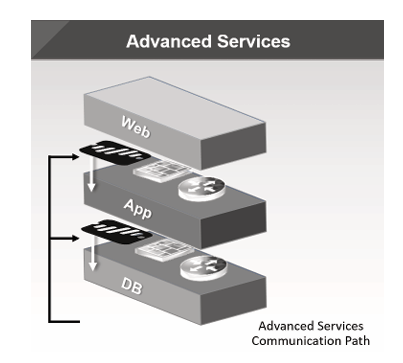
 

Figure 11 – isolation Figure 12 – communication method

**Network-based Isolation:** Logical network overlays enable isolation independent of physical hardware. This supports up to 16 million overlay-based segments per fabric.This high level of isolation prevents threats from spreading within the data center, even across large and complex environments. Figure 3.1 and 3.2 show how network isolation is implemented.

**Policy-driven Service Insertion and Traffic Steering:** Integration with third-party services allows for advanced security measures like IDS/IPS and anti-virus to be applied at a granular level.This ensures that traffic is inspected and secured as close to the application as possible, providing robust defense against sophisticated attacks.

# Chapter Summary

In this chapter, we have learned how micro-segmentation works and how it has been developed by two major network companies, VMware and Cisco. The explanation of segmentation has also been provided to help us understand how micro-segmentation emerged. By comparing traditional segmentation with micro-segmentation, we can clearly see the benefits and drawbacks of micro-segmentation. To illustrate its practical application, this chapter includes examples from 5G, cloud computing, and VMware NSX, showing how micro-segmentation is used in the industry.

To sum up, micro-segmentation provides numerous benefits in virtualized networks and enhances overall network security. Given our increasing reliance on networks, finding effective methods to reduce the risk of losing important data is crucial. Implementing micro-segmentation ensures that different segments are isolated, preventing one segment from affecting another. With the rise of cloud computing and the Internet of Things, micro-segmentation is poised to become an increasingly significant technology. It is essential that more people become aware of micro-segmentation to better protect their data and devices.

# Reference

[1] Hall, B., & Smith, N. (2020). Practical Cisco Unified Communications Security. Cisco Press.

[2] [Micro-Segmentation 5G] 2018 Mämmelä, O., Suomalainen, J., Ahola, K., Ruuska, P., Majanen, M., & Uitto, M. (2018). Micro-Segmenting 5G. *International Conference on Internet of Things, Big Data and Security*.

*[3] What Is Micro-Segmentation?* (2024, February 8). Cisco. https://www.cisco.com/c/en/us/products/security/what-is-microsegmentation.html

[4] [Towards Micro-Segmentation in 5G Network Security] 2016 Mämmelä, O., Hiltunen, J., Suomalainen, J., Ahola, K., Mannersalo, P., & Vehkaperä, J. (2016). *Towards Micro-Segmentation in 5G Network Security*. Paper presented at European Conference on Networks and Communications, Athens, Greece.

[5] *SDN-based Micro-Segmentation for OT networks*. (n.d.). Allied Telesis. https://www.alliedtelesis.com/au/en/blog/sdn-based-micro-segmentation-ot-networks

[6] GeeksforGeeks. (2023, May 8). *Software defined Networking(SDN)*. GeeksforGeeks. https://www.geeksforgeeks.org/software-defined-networking/

[7] *Micro-segmentation benefits and drawbacks*. (n.d.). https://www.bxc-consulting.com/blog/why-network-microsegmentation-counter-productive

[8] Basta, N., Ikram, M., Kâafar, M. A., & Walker, A. (2022). Towards a Zero-Trust Micro-Segmentation Network Security Strategy: an Evaluation Framework. *NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium*. <https://doi.org/10.1109/noms54207.2022.9789888>

[9] Inseego. (n.d.). *What is 3GPP?*  Inseego. <https://inseego.com/resources/5g-glossary/what-is-3gpp/>

[10] *3GPP 5G security architecture. | Download Scientific Diagram*. (n.d.). ResearchGate. https://www.researchgate.net/figure/3GPP-5G-security-architecture\_fig3\_363386647/actions#reference

[11] Klein, D. (2019). Micro-segmentation: securing complex cloud environments. *Network Security*, *2019*(3), 6–10. <https://doi.org/10.1016/s1353-4858(19)30034-0>

[12] Holmes, W. (2017). *VMware NSX Micro-segmentation - Day 1*. VMware Press. ISBN: 0998610402, ISBN13: 9780998610405.

# Figure References

|  |  |  |
| --- | --- | --- |
| **Figure number** | **Figure name** | **Reference** |
| Figure 1 | micro-segmentation Architecture | (2022, March 25). What is Micro Segmentation?» Network Interview. Network Interview. <https://networkinterview.com/what-is-micro-segmentation/> |
| Figure 2 | VLANs Example | Hall, B., & Smith, N. (2020). Practical Cisco Unified Communications Security. Cisco Press. |
| Figure 3 | An SDN example | GeeksforGeeks. (2023, May 8). *Software defined Networking(SDN)*. GeeksforGeeks.  <https://www.geeksforgeeks.org/software-defined-networking/> |
| Figure 4 | Micro-segmentation pros and cons | Deo, A. (2020, July 14). Microsegmentation - Protect your internal network. 24by7security.com; 247BySecurity, Inc. <https://blog.24by7security.com/microsegmentation-protect-your-internal-network> |
| Figure 5 | lateral movement | What is lateral movement?  <https://www.cloudflare.com/en-au/learning/security/glossary/what-is-lateral-movement/> |
| *Figure 6* | *Security architecture of 3GPP 5G* | *3GPP 5G security architecture. | Download Scientific Diagram. (n.d.). ResearchGate.*  <https://www.researchgate.net/figure/3GPP-5G-securityarchitecture_fig3_363386647/actions#reference> |
| Figure7 | Applying micro-segmentation in 5G security network architecture | Mämmelä, O., Suomalainen, J., Ahola, K., Ruuska, P., Majanen, M., & Uitto, M. (2018). Micro-Segmenting 5G. *International Conference on Internet of Things, Big Data and Security*. |
| Figure 8 | basic cloud |  |
| Figure 9 | distribution of firewall | Holmes, W. (2017). *VMware NSX Micro-segmentation - Day 1*. VMware Press. ISBN: 0998610402, ISBN13: 9780998610405. |
| Figure 10 | centralized policy | Holmes, W. (2017). *VMware NSX Micro-segmentation - Day 1*. VMware Press. ISBN: 0998610402, ISBN13: 9780998610405. |
| Figure 11 | isolation | Holmes, W. (2017). *VMware NSX Micro-segmentation - Day 1*. VMware Press. ISBN: 0998610402, ISBN13: 9780998610405. |
| Figure 12 | communication method | Holmes, W. (2017). *VMware NSX Micro-segmentation - Day 1*. VMware Press. ISBN: 0998610402, ISBN13: 9780998610405. |

# Acronyms

CSPM - Cloud Security Posture Management

Cisco ACI – Cisco Application Centric Infrastructure

Cisco VLANs – Cisco Virtual Local Area Networks

Cisco SDA - Cisco Software-Defined Access

Cisco DNA - Cisco Digital Network Architecture

IaaS – Infrastructure as Service

PaaS – Platform as Service

SaaS – Software as Service

VMware NSX – VMware Network Virtualization and Security Platform

ZTA – Zero Trust Architecture