Cloud Firewalls and Security

Cloud-Foundations-Infrastructure Fundamentals

[Pick the date]

[Type the company name]

Chhaya Nikam

# Cloud firewalls and security

Ref: <https://www.techtarget.com/searchnetworking/definition/east-west-traffic>

 The terms **North-South** and **East-West** refer to traffic flowing across private and public networks. These are the concepts of data traffic on a private network flowing horizontally (east and west) and data traffic flowing vertically (north and south) between a private network and public networks.

The two traffic patterns of North-South and East-West apply in all data centers, whether in the cloud, physical data center, or hybrid environment.

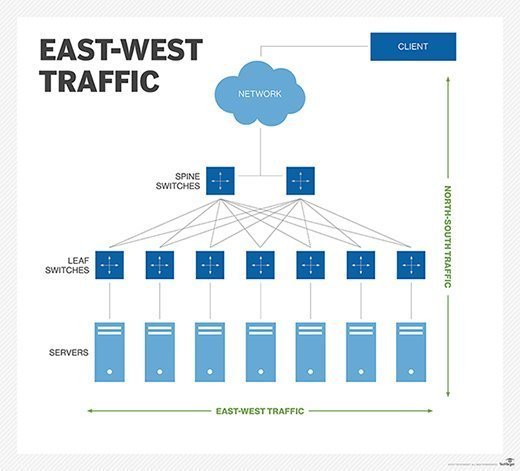
Organizations used to 'trust and verify' traffic flowing East-West because the private network was considered secure. North-South traffic was considered untrustworthy.

# east-west traffic

East-west traffic, in a networking context, is the transfer of data packets from [server](https://www.techtarget.com/whatis/definition/server) to server within a [data center.](https://www.techtarget.com/searchdatacenter/definition/data-center) The term east-west for this type of traffic comes from [network diagram](https://www.techtarget.com/searchnetworking/feature/Discover-8-network-diagramming-tools-aimed-at-architects) drawings that usually depict local area network ([LAN](https://www.techtarget.com/searchnetworking/definition/local-area-network-LAN)) traffic horizontally. In contrast, north-south traffic describes [client-to-server](https://www.techtarget.com/searchnetworking/definition/client-server) traffic that moves between the data center and a location outside of the data center network. North-south traffic is typically depicted vertically to illustrate traffic that flows above or below the data center.

In the past few years, the volume of east-west traffic has grown as a result of [virtualization](https://searchservervirtualization.techtarget.com/definition/virtualization) and data center trends such as [converged infrastructure](https://searchconvergedinfrastructure.techtarget.com/definition/converged-infrastructure). Today, network [controllers](https://www.techtarget.com/whatis/definition/controller), virtual machines ([VMs](https://searchservervirtualization.techtarget.com/definition/virtual-machine)) and other devices perform various functions and services that previously ran on physical hardware. As these components relay data to each other, they increase traffic on the network, which in turn, can cause [latency](https://www.techtarget.com/whatis/definition/latency) issues that negatively impact network performance. For example, if hosts on one access switch need to quickly communicate with systems on another access switch, uplinks among the access layer and aggregation layer become congested.

To compensate, many organizations have migrated from traditional three-layer data center architectures to various forms of [leaf-spine](https://www.techtarget.com/searchdatacenter/definition/Leaf-spine) architectures. The simplicity of a leaf-spine approach is well-suited to handling higher volumes of east-west traffic; leaf switches consolidate traffic from users and then connect to the spine, which comprises the network core of servers and storage systems.



East-west traffic

### Securing east-west traffic

Visibility into east-west traffic is critical for organizations to determine the best security practices for their networks and data centers. While many organizations tend to focus on securing external traffic that enters their networks, it is increasingly important for organizations to monitor internal traffic patterns for [malware](https://www.techtarget.com/searchsecurity/definition/malware) that has infiltrated the network and [insider threats](https://www.techtarget.com/searchsecurity/definition/insider-threat).

Microsegmentation can significantly reduce the surface available for malicious activity and lessen the impact of an attack on east-west traffic. If the data center is segmented into logical units, data center administrators can tailor unique security policies and rules for each logical unit. This tighly-coupled approach eliminates the tedious, error-prone manual configuration processes that often lead to security flaws after a migration.

https://learn.microsoft.com/en-us/azure/architecture/framework/security/design-network-flow

# Traffic flow security in Azure

Protect data anywhere it goes including cloud services, mobile devices, workstations, or collaboration platforms. In addition to using access control and encryption mechanisms, apply strong network controls that detect, monitor, and contain attacks.

## East-west and north-south traffic

When analyzing the network flow of a workload, distinguish between east-west traffic from north-south traffic. Most cloud architectures use a combination of both types.

**Is the traffic between subnets, Azure components and tiers of the workload managed and secured?**

* **North-south traffic**

North-south refers to the traffic that flows in and out of a datacenter. For example, traffic from an application to a backend service. This type of traffic is a typical target for attack vectors because it flows over the public internet. Proper network controls must be in place so that the queries to and from a data center are secure.

Consider a typical flow in an Azure Kubernetes Service (AKS) cluster. The cluster receives incoming (ingress) traffic from HTTP requests. The cluster can also send outgoing (egress) traffic to send queries to other services, such as pulling a container image.

Your design can use Web Application Firewall on Application Gateway to secure ingress traffic, and Azure Firewall to secure outgoing (egress) traffic.

* **East-west traffic**
* East-West traffic refers to network traffic flowing across a private network.
* Modern cloud infrastructure can produce larger volumes of East-West traffic than traditional infrastructure. All [VMs](https://www.snapt.net/glossary/what-is-a-virtual-machine-vm), [containers](https://www.snapt.net/glossary/what-are-docker-containers), network devices, and network controllers inside a private network generate communication traffic. This is all East-West traffic.

East-west traffic refers to traffic between or within data centers. For this type of traffic, several resources of the network infrastructure communicate with each other. Those resources can be virtual networks, subnets within those virtual networks, and so on. Security of east-west traffic can get overlooked even though it makes up a large portion of the workload traffic. It's assumed that the infrastructure firewalls are sufficient to block attacks. Make sure there are proper controls between network resources.

Extending the example of the AKS cluster to this concept, east-west traffic is the traffic within the cluster. For example, communication between pods, such as the ingress controller and the workload. If your workload is composed of multiple applications, the communication between those applications would fall into this category.

By using Kubernetes network policies, you can restrict which pods can communicate, starting from a Zero-Trust policy and then opening specific communication paths as needed.

## Examples of north-south traffic

* A public browser client sends a southbound request for resources on a web application server. In this scenario, the northbound traffic would be the [server response to the client](https://www.snapt.net/glossary/what-is-the-client-server-model).
* A [(REST) API](https://www.snapt.net/glossary/what-is-an-application-programming-interface-api) can be implemented as the interface to external entities. This northbound API can allow components like network controllers to communicate with higher-level network components.

North-South traffic typically contains communications such as database queries, commands, or other data submissions being sent and received. The public and private nature of these communications make them untrusted therefore the security of the private network relies on firewalls and network monitoring at the perimeter.

## Examples of East-west traffic

* Routers exchanging [routing table information](https://www.snapt.net/glossary/how-does-routing-work).
* Switches exchanging spanning-tree information.
* Microservice and API communications.
* A LAN client communicating with a server.

**Southbound vs. Northbound SDN** **Software-defined Networking (SDN)**

**: What are the differences?**

# Ref: https://tucu.ca/what-is-perimeter-network-security/

# Perimeter security

In the IT realm, perimeter security involves safeguarding a company’s network limits from hackers, intruders, and other unwanted individuals. It includes surveillance detection, analyzing patterns, recognizing threats, and dealing with them effectively.

Every private network has a perimeter around it. It’s the secure boundary between networks, for instance, your company’s private intranet and the ‘public’ internet.

Your [network support company](https://tucu.ca/network-support/),  **[Managed Service Provider](https://tucu.ca/managed-it-services-toronto/)** (MSP) or at times the internal IT department, deploys systems that keep your network secure from outside threats from the public web. These threats include hacking attempts, malware, ransomware, and others trying to infiltrate the network.

There are a few components of a network perimeter including:

* firewalls
* border routers
* Intrusion Detection Systems (IDS)
* Intrusion Prevention Systems (IPS)
* Unified Threat Management (UTM) systems

### Border Routers

Routers direct traffic into and out of networks – border routers are the last on the company’s private network before traffic goes on to public networks on the internet.

### Firewalls

A firewall is a device with a filtering mechanism, containing a predefined set of rules to allow and restrict traffic from the public to enter the private network and vice versa. It’s an additional safety mechanism to protect a company’s network from unwanted packets of information that may be hiding threats.

### Intrusion Detection Systems – IDS

Intrusion detection systems monitor the traffic and information ‘packets’ being transferred between public and private networks.

It tallies all information against a known list of cyber-attack signatures, and your Managed Service Provider (MSP) takes necessary action to stop harmful information from entering your company’s private network.

They can compare network activity with the prebuilt threat database that can detect different security violations, port scanners, and malware.

The IDS is basically an alarm system that alerts the company about suspicious activity. It’s built from a single device or can use strategically placed sensors on different points of a network.

### Intrusion Prevention Systems – IPS

Intrusion prevention systems are control systems that can accept or reject data packets based on a preset list of rules that are updated regularly by your managed service provider or automatically.

In comparison to a traditional IDS system that notifies administrators and your MSPs about threats, Intrusion prevention systems can have an automated defense mechanism to stop the information from entering the network without human intervention.

### Unified Threat Management (UTM) Systems

Unified Threat Management (UTM) systems protect the network by combining features of IDS and IPS systems.

A single security device provides many security functions from one point in the private network. Thanks to the antivirus, firewall, anti-spyware, anti-spam, virtual private network (VPN) and other functions, the information entering a company’s network stays protected.

A UTM system protects against viruses, hacking attempts, malware, malicious attachments, and more thanks to deep packet inspection.

**Deep packet inspection (DPI)** does a complete evaluation, inside and out, of the data being transmitted over the network and performs checks for compliance violations such as spam, Trojans, viruses, or other defined criteria. If it notices these violations, it blocks the information from being received or transmitted.

## Defining & Defending The Network Perimeter

Your managed service provider (MSP) or IT department has to know the complete layout of your network perimeter and understand it to provide the best possible security.

Continuous scanning and assessment of this perimeter can help you identify when company resources and data are misused by individuals or are under threat by hackers.

However, it has become dynamic due to the possibilities of working remotely and using your own devices (BYOD), but that doesn’t negate the fact that entry and exit points for a private network such as that of a business must be protected.

### Monitor Passively

Passive monitoring tools can be useful in discovering devices that are connected to the network to see how much access and discretion they’ve been granted. These tools scan the network for weaknesses and vulnerabilities, locating the different devices connected to the network.

These devices may be remote servers, routers, desktops, security devices, application routers as well as firewalls. The monitoring tool can analyze the configuration, operating system, installed apps, and patch levels of these devices to find vulnerabilities that allow hackers unauthorized access.

The passive tools need to be activated or scheduled manually by your MSP or IT department to perform vulnerability checks.

### Monitor Actively

Active monitoring tools allow for continuous surveillance of your network, scanning it for irregular traffic patterns, unknown IP structures, communications, and transmission of data. These tools can help your MSP map out architecture for your business’s private network and help set guidelines for communication between devices on the network. This helps your employees stay compliant with company guidelines.

These tools monitor your most critical business assets and apps, taking action against illegal access, employee misuse of resources, malicious content, and other security fallouts. They audit your security in real-time, creating logs and reports to meet security compliance policy requirements.

### Network Zoning

The concept of zoning takes all the areas of a network into account and divides them into controlled, uncontrolled, restricted, and secure zones.

The main advantage of zoning comes from restricting a potential security breach to individual zones where it occurred, preventing it from entering other zones.  
Network boundaries help separate networking zones with different security policies. These boundaries create restrictions on the kind of traffic that’s permitted in different zones. For instance, HTTP traffic may be restricted on specific ports or restricting HTTPs traffic coming from other ports from the public networks (internet and other uncontrolled networks).

Firewalls can be used to allow and restrict traffic – the firewall sends back the information packet or traffic where it came from, by readdressing - the traffic being sent back looks like it came from an address connected to the firewall. In this way, the identity of the trusted network stays hidden from the other untrusted networks connected to the internet.

**Key Takeaway**

Perimeter security is a philosophy that involves setting up functional devices, tools, and techniques around the boundary of a network to secure its data and resources. It is one facet of the greater security field and plays a vital role in active system protection.

So essentially, perimeter security experts take a perimeter-based approach to secure your systems and ward off any threats before they enter the network. They follow best practices like threat recognition, pattern analysis, and surveillance detection to set up high-quality and highly efficient processes to ensure internal security.

# Network Security

## What Is Network Security?

**Network security is defined as the process of creating a strategic defensive approach that secures a company’s data and its resources across its network. It protects the organization against any form of a**[**potential threat**](https://www.spiceworks.com/security/vulnerability-management/articles/what-is-cyber-threat/)**or unauthorized access. Irrespective of the organization’s size, industry, or infrastructure, network security solutions protect it against the ever-evolving threat of cyberattacks.**

**Network Security** refers to the measures taken by any enterprise or organization to secure its computer network and data using both hardware and software systems. This aims at securing the confidentiality and accessibility of the data and network. Every company or organization that handles a large amount of data, has a degree of solutions against many **cyber threats**.

The most basic example of Network Security is password protection which the user of the network oneself chooses. In recent times, Network Security has become the central topic of cyber security with many organizations inviting applications from people who have skills in this area. The network security solutions protect various **vulnerabilities of the computer systems** such as: 

**1.** Users

**2.** Locations

**3.** Data

**4.** Devices

**5.** Applications

**Network Security: Working**   
The basic principle of network security is protecting huge stored data and networks in layers that ensure the bedding of rules and regulations that have to be acknowledged before performing any activity on the data. 

These levels are:

**1.** Physical

**2.** Technical

**3.** Administrative

1. **Physical Network Security:**   
   This is the most basic level that includes protecting the data and network through unauthorized personnel from acquiring control over the confidentiality of the network. These include external peripherals and routers that might be used for cable connections. The same can be achieved by using devices like biometric systems.
2. **Technical Network Security:**   
   It primarily focuses on protecting the data stored in the network or data involved in transitions through the network. This type serves two purposes. One is protected from unauthorized users, and the other is protection from malicious activities.
3. **Administrative Network Security:**   
   This level of network security protects user behavior like how the permission has been granted and how the authorization process takes place. This also ensures the level of sophistication the network might need for protecting it through all the attacks. This level also suggests necessary amendments that have to be done to the infrastructure.

**Types of Network Security:**   
The few types of network securities are discussed below :

1. [**Access Control**](https://www.geeksforgeeks.org/access-control-in-computer-network/)**:**   
   Not every person should have a complete allowance for the accessibility to the network or its data. One way to examine this is by going through each personnel’s details. This is done through Network Access Control which ensures that only a handful of authorized personnel must be able to work with the allowed amount of resources.
2. [**Antivirus**](https://www.geeksforgeeks.org/how-an-antivirus-works/)**and Anti-malware Software:**   
   This type of network security ensures that any malicious software does not enter the network and jeopardize the security of the data. The malicious software like [Viruses, Trojans, and Worms](https://www.geeksforgeeks.org/malware-and-its-types/) is handled by the same. This ensures that not only the entry of the malware is protected but also that the system is well equipped to fight once it has entered.
3. **Cloud Security:**   
   Now a day, a lot many organizations are joining hands with cloud technology where a large amount of important data is stored over the internet. This is very vulnerable to the malpractices that few unauthorized dealers might pertain. This data must be protected and it should be ensured that this protection is not jeopardized by anything. Many businesses embrace SaaS applications for providing some of their employees the allowance of accessing the data stored over the cloud. This type of security ensures creating gaps in the visibility of the data.

### Type of network security vulnerabilities

Before examining different kinds of security attacks and how network security helps avoid them, understanding where the network’s vulnerability lies is key. Any vulnerability gives hackers the ability to access infrastructure, install malware, and even steal and modify data, if not destroy or erase it. These [vulnerabilities](https://www.spiceworks.com/security/vulnerability-management/articles/what-is-a-security-vulnerability/) include:

* **Missing data encryption:**Sometimes, a software does not encrypt or secure sensitive data before transmitting or saving it.
* **Operating system command injection:**Through an operating system command injection**,** a hacker can execute a random OS, corrupting the server running an application and compromising its functioning completely.
* **SQL injection:**A hacker uses an SQL injection to intercept queries that an application makes to its server.
* **Missing authentication:**Sometimes, a software does not conduct any [authentication of user identity](https://www.spiceworks.com/it-security/identity-access-management/articles/what-is-multi-factor-authentication/)or the resources being utilized.
* **Unrestricted upload of dangerous file types:**Another common type of network security vulnerability is the unrestricted upload of dangerous file types where a software permits a hacker to upload dangerous files and run them on the software’s environment.
* **Other vulnerabilities** include weak passwords, buffer overflow, missing authorization, cross-site scripting and forgery, download of codes without integrity checks, use of broken algorithms, URL redirection to untrusted sites, path traversal, and bugs.

What is a network security Group

. A network security group contains [security rules](https://learn.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#security-rules) that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

# What is ASG? Application Security Group (ASG)

## An application security group is a logical collection of virtual machines (NICs). You join virtual machines to the application security group, and then use the application security group as a source or destination in NSG rules

Normally when you deploy a network security group (NSG) it is either assigned to a NIC or a subnet (preferred). If you deploy that NSG to a subnet then the rules apply to all of the NICs, or virtual machines, in that subnet. This is OK when you’re deploying a new system where you can easily place virtual machines into subnets, and treat each subnet as its own security zone. But in the real world, things aren’t always that clean, and you might need something that allows a more dynamic or flexible means of assigning rules to some machines in a subnet.

ASGs are used within a NSG to apply a network security rule to a specific workload or group of VMs — defined by ASG worked as being the “network object” & explicit IP addresses are added to this object. This provides the capability to group VMs into associated groups or workloads, simplifying the NSG rule definition process. Another great use of this is for scalability, creating the virtual machine and assigning the newly created virtual machine to its ASG will provide it with all the NSG rules in place for that specific ASG — zero distribution to your service!

## What does endpoint mean in Azure/cloud?

An endpoint **provides mapping from one port to another port for a specific virtual machine**. This allows many different virtual machines to be accessed through the single cloud service virtual IP address by using unique external ports for each service and each virtual machine.

## What is service endpoint and private endpoint in Azure/cloud?

**A Service Endpoint remains a publicly routable IP address.** **A Private Endpoint is a private IP in the address space of the virtual network where the private endpoint is configured**.

## What is load balancing in cloud computing

Cloud load balancing is defined as the method of splitting workloads and computing properties in a cloud computing. It enables enterprise to manage workload demands or application demands by distributing resources among numerous computers, networks or servers. Cloud load balancing includes holding the circulation of workload traffic and demands that exist over the Internet.

As the traffic on the internet growing rapidly, which is about 100% annually of the present traffic. Hence, the workload on the server growing so fast which leads to the overloading of servers mainly for popular web server. There are two elementary solutions to overcome the problem of overloading on the servers-

* First is a single-server solution in which the server is upgraded to a higher performance server. However, the new server may also be overloaded soon, demanding another upgrade. Moreover, the upgrading process is arduous and expensive.
* Second is a multiple-server solution in which a scalable service system on a cluster of servers is built. That’s why it is more cost effective as well as more scalable to build a server cluster system for network services.

Load balancing is beneficial with almost any type of service, like HTTP, SMTP, DNS, FTP, and POP/IMAP. It also rises reliability through redundancy. The balancing service is provided by a dedicated hardware device or program. Cloud-based servers farms can attain more precise scalability and availability using server load balancing.

**Load balancing solutions can be categorized into two types –**

1. **Software-based load balancers:**Software-based load balancers run on standard hardware (desktop, PCs) and standard operating systems.
2. **Hardware-based load balancer:**Hardware-based load balancers are dedicated boxes which include Application Specific Integrated Circuits (ASICs) adapted for a particular use. ASICs allows high speed promoting of network traffic and are frequently used for transport-level load balancing because hardware-based load balancing is faster in comparison to software solution.

## What is Application Gateway

## Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to Application Gateway

Application gateways provide high-level secure network system communication. For example, when a client requests access to server resources such as files, Web pages and databases, the client first connects with the proxy server, which then establishes a connection with the main server.

The application gateway resides on the client and server firewall. The proxy server hides Internet Protocol (IP) addresses and other secure information on the client’s behalf. A computer’s internal system may communicate with an external computer using firewall protection. The application gateway and external computer function without client information or knowledge of the proxy server IP address.

## What is a Web Application Firewall?

Web Application Firewall protects the web application by filtering, monitoring, and blocking any malicious HTTP/S traffic that might penetrate the web application. In simple words, a Web Application Firewall acts as a shield between a web application and the Internet. This shield protects the web application from different types of attacks.

### Working of Web Application Firewall

* According to the OSI model, WAF is a protocol layer seven defense.
* When a WAF is deployed in front of a web application, a shield is created between the web application and the Internet.
* The advantage of WAF is that it functions independently from the application, but yet it can constantly adapt to the application behavior changes.
* The clients are passed through the WAF before reaching the server in order to protect the server from exposure.
* WAF can be set to various levels of examinations, usually in a range from low to high, which allows the WAF to provide a better level of security.

### Types of Web Application Firewall:

* **Network-based WAFs**are usually hardware-based. They provide latency reduction due to local installation. Network-based WAFs are the most expensive and also require the storage and maintenance of physical equipment.
* **Host-based WAFs** may be completely integrated into an application’s software. They exist as modules for a web server. It is a cheaper solution compared to hardware-based WAFs, which are used for small web applications. The disadvantage of a host-based WAF is the consumption of local server resources because of which the performance may degrade.
* **Cloud-based WAFs** are low-cost and have fewer resources to manage.The cloud-based solution is the perfect choice when a person doesn’t want to restrict themselves with performance capabilities. The service providers can provide with unlimited hardware pool but after a certain point of time, the service fees might increase.

### Importance of Web Application Firewall:

There are several hackers out there who are ready to execute their malicious attacks. The most common attacks such as XSS, SQL Injection, etc. can be prevented with the help of WAF and that will be discussed further. The purpose of WAF is to protect your webpage from such malicious attacks. The WAF constantly monitors for potential attacks, blocking these attacks if they are found to be malicious in any way.

### Policy in Web Application Firewall:

* The set of rules through which a WAF operates is called a policy.
* The purpose of these policies is to protect against the vulnerabilities in the application by filtering out malicious traffic.
* The value of a WAF comes in part depending upon the speed and efficiency with which the policy modification is implemented.

### Types of Attacks a Web Application Firewall Can Prevent:

* [**DDOS Attack**](https://www.geeksforgeeks.org/denial-of-service-ddos-attack/) aims to target a particular web application/ website/ server with fake traffic.
* [**Cross-Site Scripting (XSS) Attacks**](https://www.geeksforgeeks.org/what-is-cross-site-scripting-xss/) are aimed at those users who use vulnerable web applications/ websites in order to gain access to and control their browsers.
* [**SQL Injection Attacks**](https://www.geeksforgeeks.org/sql-injection-2/)**:** A malicious SQL code is injected in the form of requests or queries in the user input box on the web applications that the user is using.
* [**Man-in-the-middle attacks**](https://www.geeksforgeeks.org/how-to-prevent-man-in-the-middle-attack/)take place when the perpetrators position themselves in between the application and the legitimate users in order to extract confidential details.
* [**Zero-day attacks**](https://www.geeksforgeeks.org/zero-day-exploit-cyber-security-attack/) are unexpected attacks that take place. The organization knows about the existence of vulnerabilities in the hardware/ software only when the attack has taken place.

### Blocklist and Allowlist in Web Application Firewalls:

* **Blocklist:**A WAF that is based on a blocklist protects against known attacks. Visualize blocklist WAF as a college security guard who is instructed to deny admittance to the students who don’t bring their ID-Cards.
* **Allowlist:**A WAF based on an allow list only admits traffic that has been pre-approved. This is like the college security guard who only admits people who are on the list.

Both Blocklist and Allowlist have equal advantages and disadvantages because of which many WAFs offer a hybrid security model, which implements both.

### Advantages:

* Low-cost for cloud-based WAF solution.
* Prevent attacks which include SQL injections, cross-site scripting (XSS) attacks, etc.
* It prevents cookie poisoning. Cookie poisoning is the manipulation of cookies in order to keep track of users’ information.
* Prevents data from being compromised.

### Disadvantages:

* If the software has vulnerabilities, then there are chances that some attacks might bypass them.
* Sometimes the complete solution comes at an expensive cost.
* A lot of resources are consumed.
* There is a lack of cloud support because WAFs are majorly deployed as hardware on-premise.

## Services available for Security in various cloud platforms

## AWS Security, Identity, & Compliance services

|  |  |  |
| --- | --- | --- |
| **Category** | **What is it** | **AWS service** |
| Detection | Track user activity and API usage | AWS CloudTrail |
| Security management for IoT devices | AWS IoT Device Defender |
| Network and application protection | Network security | AWS Network Firewall |
| DDoS protection | AWS Shield |

## Azure Security Tools – A Comprehensive List

* Azure Active Directory.
* Azure AD identity protection.
* Azure AD Privileged Identity Management.
* Network Security.
* Resource management security.
* Encryption for data at rest.
* Configure application security.

## Google Security Services – A Comprehensive List

| PRODUCT |
| --- |
| **[Access Transparency](https://cloud.google.com/access-transparency)** Cloud provider visibility through near real-time logs. |
| **[Assured Workloads](https://cloud.google.com/assured-workloads)** Compliance and security controls for sensitive workloads. |
| **[Binary Authorization](https://cloud.google.com/binary-authorization)** Deploy only trusted containers on Kubernetes Engine. |
| **[Chronicle](https://chronicle.security/products/platform/" \t "_blank)** Extract signals from your security telemetry to find threats instantly. |
| **[Cloud Asset Inventory](https://cloud.google.com/asset-inventory)** View, monitor, and analyze Google Cloud and Anthos assets across projects and services. |
| **[Cloud Data Loss Prevention](https://cloud.google.com/dlp)** Sensitive data inspection, classification, and redaction platform. |
| **[Cloud IDS](https://cloud.google.com/ids)** Cloud-native, managed network threat detection with industry-leading security. |
| **[Cloud Key Management](https://cloud.google.com/security-key-management)** Manage encryption keys on Google Cloud. |
| **[Confidential Computing](https://cloud.google.com/confidential-computing)** Encrypt data in use with Confidential VMs. |
| **[Firewalls](https://cloud.google.com/firewalls)** Global and flexible firewalls to protect your cloud resources. |
| **[Secret Manager](https://cloud.google.com/secret-manager)** Store API keys, passwords, certificates, and other sensitive data. |
| **[Security Command Center](https://cloud.google.com/security-command-center)** Platform for defending against threats to your Google Cloud assets. |
| **[Shielded VMs](https://cloud.google.com/shielded-vm)** Virtual machines hardened with security controls and defenses. |
| **[VPC Service Controls](https://cloud.google.com/vpc-service-controls)** Protect sensitive data in Google Cloud services using security perimeters. |
| **[BeyondCorp Enterprise](https://cloud.google.com/beyondcorp-enterprise)** Scalable zero trust platform with integrated threat and data protection. |
| **[Certificate Authority Service](https://cloud.google.com/certificate-authority-service)** Simplify the deployment and management of private CAs. |
| **[Cloud Identity](https://cloud.google.com/identity)** Unified platform for IT admins to manage user devices and apps. |
| **[Identity and Access Management](https://cloud.google.com/iam)** Permissions management system for Google Cloud resources. |
| **[Identity-Aware Proxy](https://cloud.google.com/iap)** Use identity and context to guard access to your applications and VMs. |
| **[Identity Platform](https://cloud.google.com/identity-platform)** Add Google-grade identity and access management to your apps. |
| **[Managed Service for Microsoft Active Directory](https://cloud.google.com/managed-microsoft-ad)** Hardened service running Microsoft® Active Directory (AD). |
| **[Policy Intelligence](https://cloud.google.com/policy-intelligence)** Smart access control for your Google Cloud resources. |
| **[Resource Manager](https://cloud.google.com/resource-manager)** Hierarchical management for organizing resources on Google Cloud. |
| **[Titan Security Key](https://cloud.google.com/titan-security-key)** Two-factor authentication device for user account protection. |
| **[reCAPTCHA Enterprise](https://cloud.google.com/recaptcha-enterprise)** Help protect your website from fraudulent activity, spam, and abuse. |
| **[Web Risk](https://cloud.google.com/web-risk)** Detect malicious URLs on your website and in client applications |

# Knowledge check ==.>Southbound is the ans

Q. Traffic going from laptop via VPN client to datacenters is an example of southbound traffic