Network Fundamentals for Cloud

BITS Pilani
Pilani Campus

Nishit Narang
WILPD-CSIS

innovate achieve lead

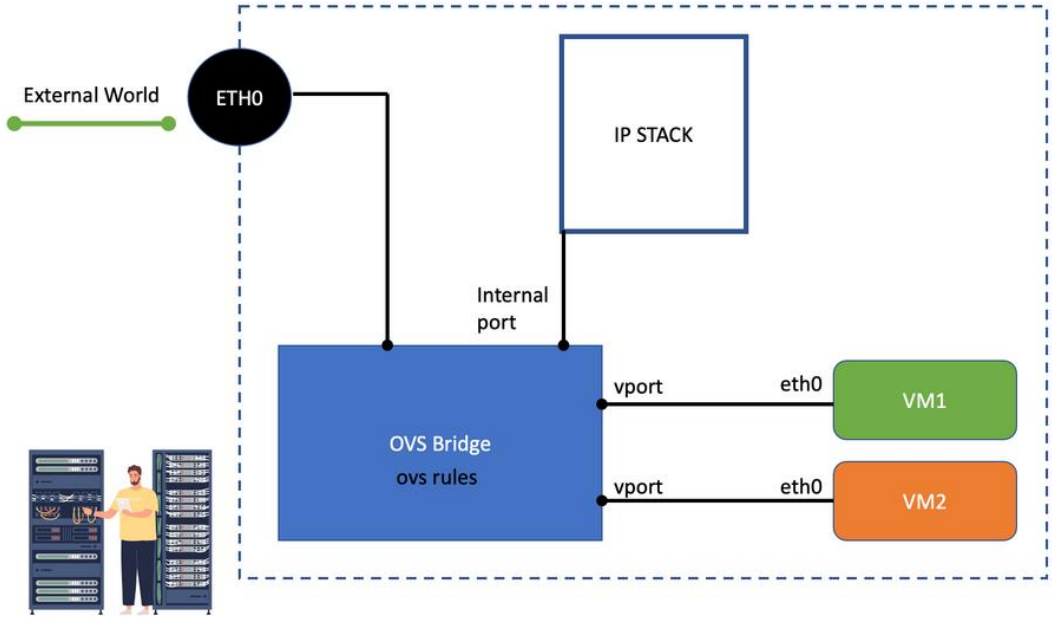
BITS Pilani
Pilani Campus

CC ZG503: Network Fundamentals for Cloud

Lecture No. 14 : Container Networking & Cloud Network Security

RECAP: OVS

- OVS (Open vSwitch) is a fundamental component of modern and open data center SDNs, where it aggregates all the virtual machines at the server hypervisor layer.
- It represents the ingress point for all the traffic exiting VMs, and can be used to forward traffic between multiple virtual network functions in the form of service chains.



Source: OVS Bridge and Open vSwitch (OVS) Basics (network-insight.net) and Data centre networking: what is OVS? | Canonical

Container Networking

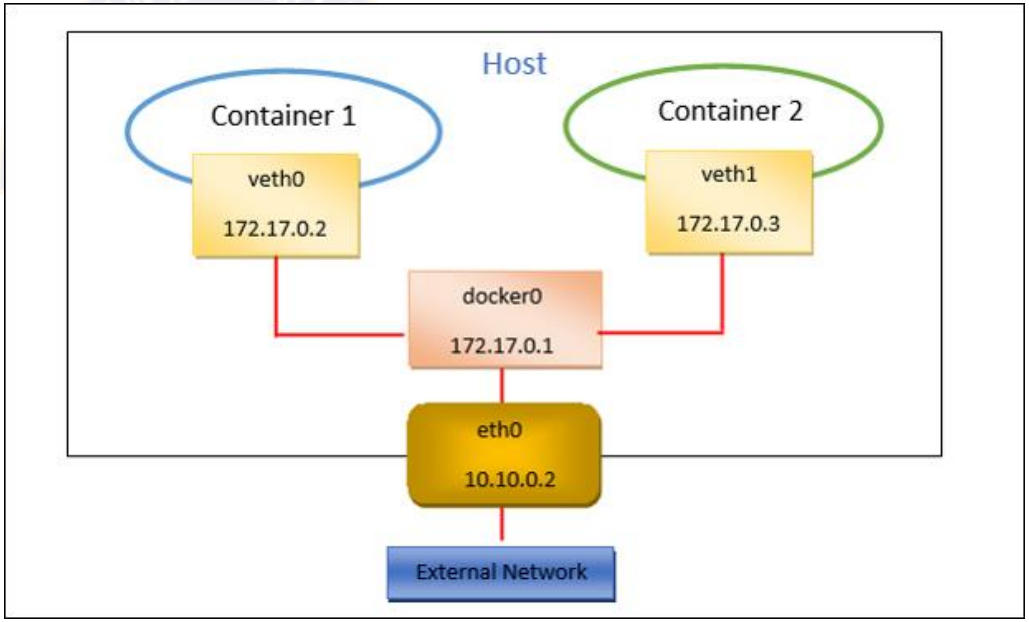
Container networking has four operating modes:

- **No network:** is used when a container has no desire to communicate with the outside world and so has no network connectivity of any sort
- **Host network:** the container shares the network namespace with the host OS. In other words, the container sees everything that the host sees with no isolation.
  - Normally, run in a privileged mode, where the container can modify the host operating system's network state such as routing table, MAC table, interface state, and so on.
  - FRR, the open source routing suite, when running as a container on a server, runs in privileged mode, allowing routing to be provided as a containerized service on a server.
  - The main disadvantage of this mode is that containers share the network state, thereby making it difficult to have two containers using the same TCP/UDP port number to communicate with the outside world
- **Single-host network:** is the default network provided by Docker. In this mode, containers running on the same host can communicate with one another in addition to communicating with the outside world
- **Multi-host network:** allows containers running on different servers to communicate with one another.

Source: Dinesh G. Dutt. Cloud Native Data Center Networking: Architecture, Protocols and Tools, O'Reilly 2020

Network drivers

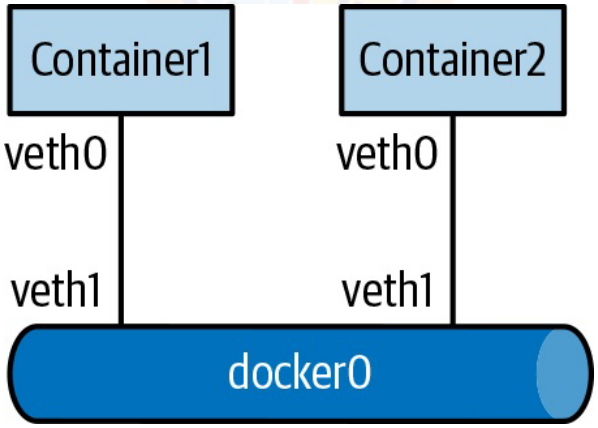
- Docker’s networking subsystem is pluggable, using drivers.
- Several drivers exist by default, and provide core networking functionality:
  - Bridge
  - Host
  - Overlay
  - Ipvlan
  - Macvlan
  - none



Single-Host Container Networking

Two common ways in which containers running on the same host can communicate with one another and with the outside world:

- **BRIDGE:** When a Docker service is first instantiated, it creates a docker0 device, which is a Linux bridge.
- Whenever new containers are created via the docker run command without specifying a network option, Docker creates a veth pair of interfaces, assigns one of them to the container's netns, and attaches the other to the docker0 bridge.
- Additional containers created in a similar fashion have the same behavior.
- Thus, multiple containers created on the host can communicate with one another because one end of the veth interfaces in each of these containers is connected to the docker0 bridge

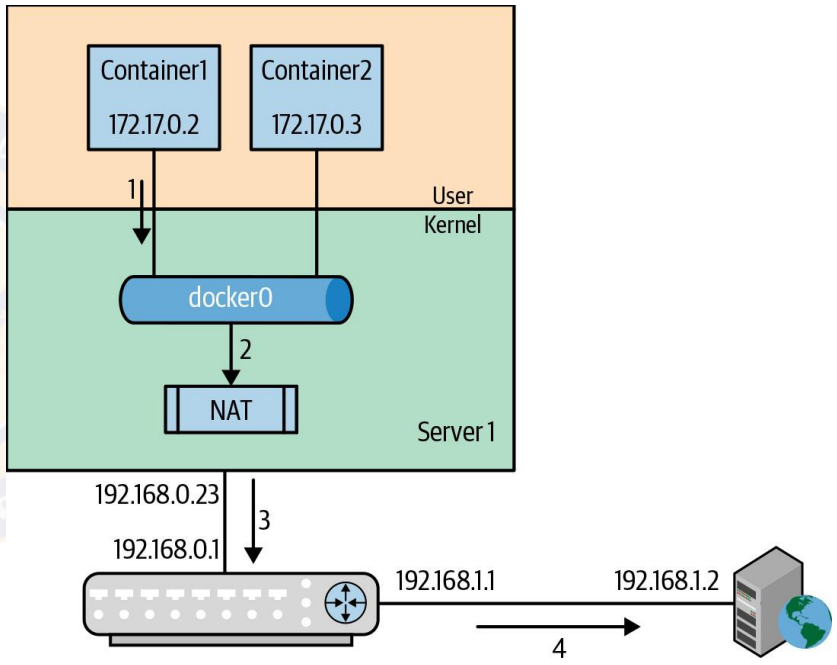


Source: Dinesh G. Dutt. Cloud Native Data Center Networking: Architecture, Protocols and Tools, O'Reilly 2020

Single-Host Container Networking

Two common ways in which containers running on the same host can communicate with one another and with the outside world:

- **BRIDGE:** Docker uses a default subnet of 172.17.0.0/16 to the docker0 bridge
- It assigns the address 172.17.0.1 to the bridge itself.
- As a container is spun up that has a network interface associated with the docker0 bridge, Docker automatically assigns an unused IP address from the docker0 subnet, 172.17.0.0/16, to the container.
- Docker also adds a default route in the container's namespace that specifies the next hop as the docker0's IP address, 172.17.0.1.
- Docker by default also configures any packet from the bridge destined to the outside world to undergo NAT so that multiple containers can share a single host IP address to communicate with entities other than the host.



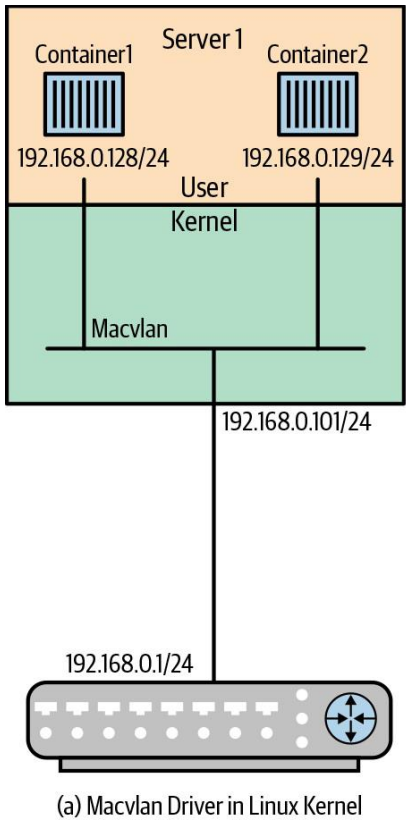
External communication via docker0

Source: Dinesh G. Dutt. Cloud Native Data Center Networking: Architecture, Protocols and Tools, O'Reilly 2020

Single-Host Container Networking

Two common ways in which containers running on the same host can communicate with one another and with the outside world:

- **MACVLAN:** As an alternative to using a bridge for single-host container communication, you can use a Macvlan, an L2 virtual network interface associated with a physical interface.
- The kernel driver assigns each Macvlan interface a unique MAC address.
- The kernel delivers an incoming packet to the Macvlan interface whose MAC address matches the packet's destination MAC address, and thereby to the correct container.
- The containers associated with the Macvlan network need to be assigned IP addresses in a subnet associated with the upstream interface

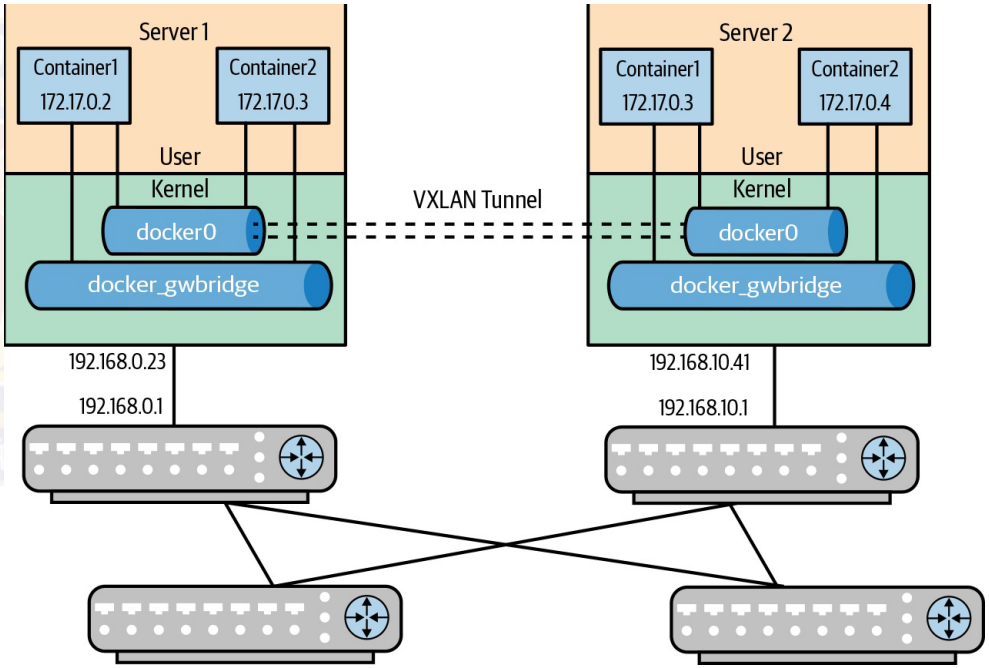


(a) Macvlan Driver in Linux Kernel

Source: Dinesh G. Dutt. Cloud Native Data Center Networking: Architecture, Protocols and Tools, O'Reilly 2020

Multi-Host Container Networking

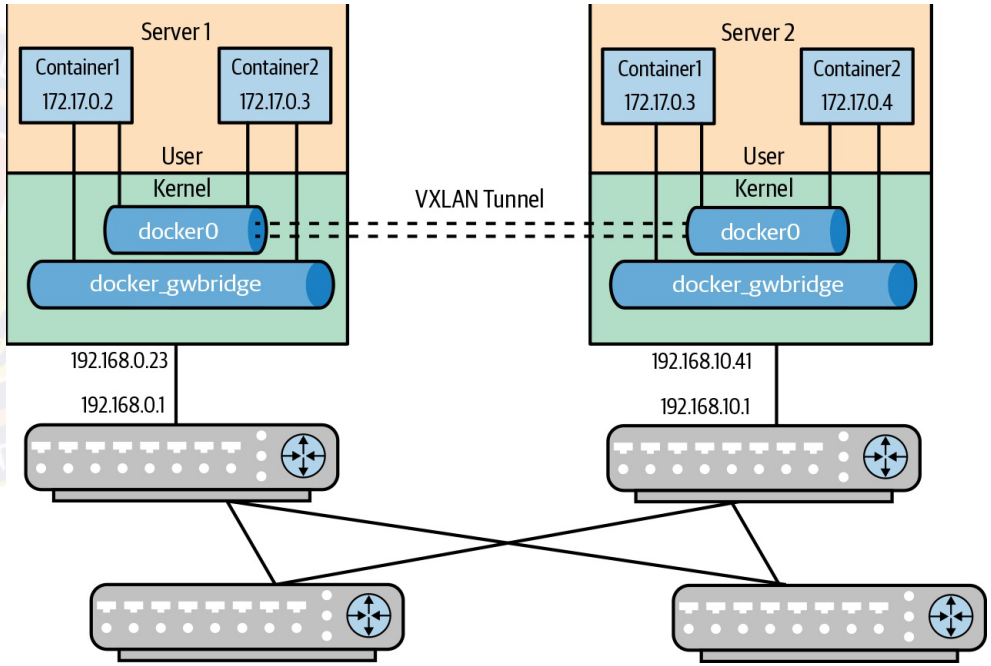
- **OVERLAY NETWORK:** Docker defines a network type called overlay for a multi-host connectivity.
- Although the documentation doesn't make it explicit, the overlay network used is VXLAN
  - This is an L2 network. In other words, the containers spread across the hosts are in the same subnet
  - Coordinating IP address assignments for the same subnet across hosts is no longer as simple as the local Docker daemon allocating the address on container spinup.
  - Therefore, Docker requires the Swarm functionality when creating an overlay network.
  - Swarm is the Docker control plane that handles IP Address Management (IPAM) across multiple hosts, provides service abstraction, and so on



Source: Dinesh G. Dutt. Cloud Native Data Center Networking: Architecture, Protocols and Tools, O'Reilly 2020

Multi-Host Container Networking

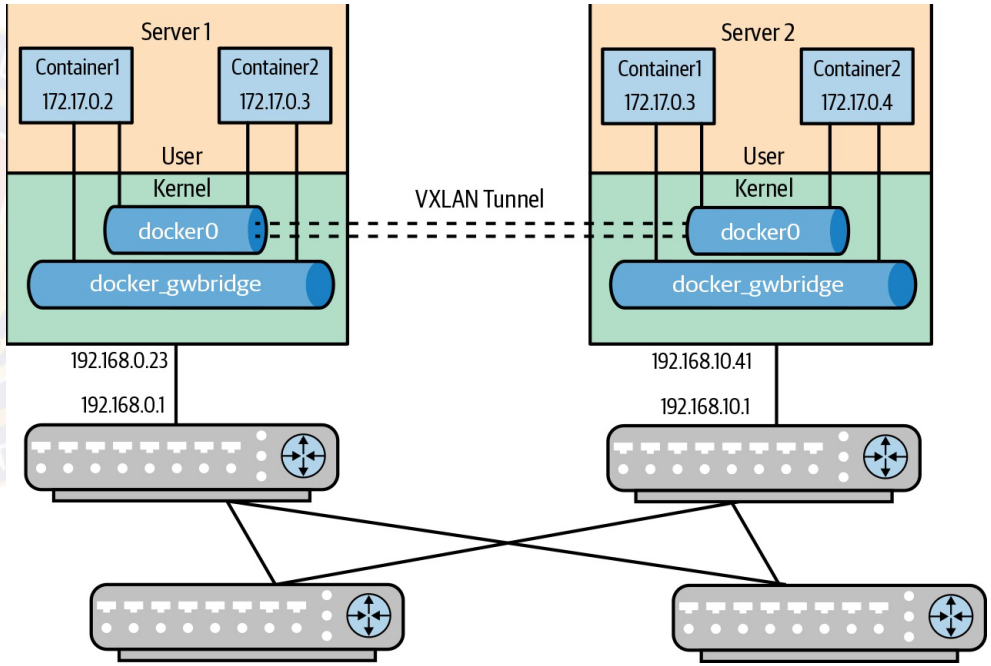
- **OVERLAY NETWORK:** The containers in the two different servers all belong to the same subnet, 172.17.0.0/24.
- Server 1 has a VTEP IP address of 192.168.0.23, whereas Server 2's VTEP IP is 192.168.10.41.
- The routers will have exchanged routing information so that all the routers know how to reach the 192.168.0.0/24 and 192.168.10.0/24 subnets.
- So a VXLAN-encapsulated packet from Server 1 to Server 2 would be routable across the network shown
- From the container's perspective, a veth interface hooked up to a Linux bridge works just as in a single-host bridge network. However, under the covers, the overlay network also creates a VXLAN tunnel between the nodes in the network.
- Every node that is joined in Swarm (or Flannel or Weave) has a VXLAN tunnel created and attached to the bridge to allow packets to tunnel through the underlay network.



Source: Dinesh G. Dutt. Cloud Native Data Center Networking: Architecture, Protocols and Tools, O'Reilly 2020

Multi-Host Container Networking

- **OVERLAY NETWORK:** When overlay networking is used, Docker sets up two interfaces inside a container.
- One is for the communication between containers in the same subnet using the overlay.
- The other communicates with the outside world.
- This new interface is also a veth, but it's connected to a different bridge called docker_gwbridge. It also gets its own IP subnet.
- The routing table inside a container is set up to use the appropriate interface for each form of communication.
- Packets going through docker_gwbridge undergo NAT by default, just as in the case of docker0 bridge



Source: Dinesh G. Dutt. Cloud Native Data Center Networking: Architecture, Protocols and Tools, O'Reilly 2020

innovate achieve lead

BITS Pilani

Pilani Campus

Network Security Overview

Securing Network Perimeter and Network Services

Defence In Depth

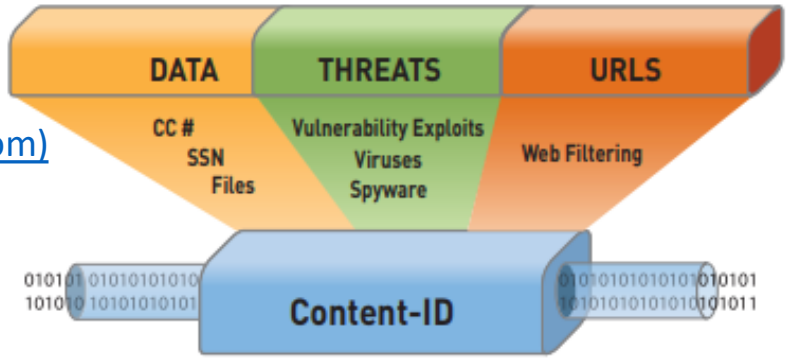
- When developing an enterprise security strategy, a layered approach is the best method to ensure detection and mitigation of attacks at each tier of the network infrastructure
  - *"Defence in depth is a **military strategy** that seeks to delay rather than prevent the advance of an attacker, buying time and causing additional casualties by yielding space. Rather than defeating an attacker with a single, strong defensive line, defence in depth relies on the tendency of an attack to lose momentum over time or as it covers a larger area."* Source: Wikipedia
- Although the enterprise network perimeter is changing, the basic network security mechanisms still have their purpose
  - the same types of security mechanisms need to persist, however, where they are implemented may change slightly depending upon the network architecture
- In general, we will not focus much on where the network perimeter is, but on what needs to be protected

Next Generation Firewalls

- Standard firewalls simply check for the policy allowing the source IP, destination IP, and TCP/UDP port, without a further deep packet analysis
- Next Generation Firewalls (NGFW) perform more deep packet analysis to mitigate malicious traffic masquerading as legitimate
  - Example: DNS traffic inspected by a standard firewall may look legitimate, but in reality, the DNS packets may be padded with data that is being ex-filtrated from the network
- An NGFW can inspect traffic for data, threats, and web traffic

Content_ID_tech.pdf (paloaltonetworks.com)

Palo Alto
etworks - ContentI



IDS/IPS

- Intrusion detection and prevention technology has remained a mainstay at the network perimeter
  - While several firewall technologies are integrating intrusion prevention into their offerings, there has not been a complete shift to this implementation
- Intrusion detection is a method for detecting an attack but taking no action
  - this has been abandoned at the network perimeter when a breach is undesirable
  - it seems to still have a significant implementation in the internal network server segments to passively observe the behaviors of internal network users
  - has all the detection logic of intrusion prevention but without the ability to actively mitigate a threat
- Intrusion prevention is similar to intrusion detection, but has the capability to disrupt and mitigate malicious traffic by blocking and other methods
  - Many IPS devices have purposefully built denial of service mitigation technology
  - can be deployed at the network perimeter
  - should also be considered for implementation in the internal network to protect the most critical assets within the organization
- As the attacks have become advanced, there is debate on the overall advantage of the IDS/IPS
  - However, a defense in-depth strategy is best implemented by including IDS/IPS as an essential network protection mechanism

IDS/IPS: Detection Methods

- IDS/IPS devices use a combination of three methods to detect and mitigate attacks
  - behavior, anomaly, and signature
  - initial IDS/IPS systems were specialized in one method or another
  - Today, it is rare to find a detection method without the others
  - Also because attacks are not always as simple as protocol misuse or a known Trojan signature

IDS/IPS: Behavior Analysis

- Behavioral analysis takes some intelligence from the platform to first gain an understanding of how the network "normally" operates
  - what systems communicate with other systems, how they communicate, and how much
- Any deviation from this baseline becomes an outlier and triggers the IDS/IPS based on this behavioral deviation
  - Example, if a system is compromised, the connection rates exceed what is common for the system
- The primary caveat with this approach is the mistake of baselining malicious traffic within standard network traffic as "normal“
  - This common and almost unavoidable mistake requires the other detection methods to bring real value

IDS/IPS: Anomaly Detection

- Malware writers often attempt to masquerade their application as a legitimate application
  - this method is commonly employed by chat clients, bit torrent, and other P2P applications
  - Such apps are typically not permitted, so developers have written the applications to look harmless
- Anomaly detection at the network perimeter can be extremely effective in analyzing inbound HTTP requests where the protocol is correct, but there has been some manipulation to the packet
- Nonetheless, understanding the RFC specifications for every protocol is a daunting task!!

IDS/IPS: Signature-based Detection

- A consistent method to detect known malicious attacks
- IDS/IPS looks for known patterns in the packets being inspected
- When a signature or pattern match is found, a predetermined action is taken
- Detects the most common, generic attacks
- Ineffective for the more sophisticated attacks
- Another annoyance with this method is the high rate of false positives

With a majority of attacks targeted at the network being Distributed Denial of Service (DDoS) and SQL injection (SQLi), signature-based IPS can be very effective in mitigating these attacks and continue to provide value at the network perimeter

Securing Network Services (NS)

- Enterprises provide and leverage Internet services such as DNS, e-mail, and file transfer
  - The latest malware threats utilize these common services in order to redirect internal hosts to Internet destinations under the control of the malware writers
  - However, with correctly implemented architecture, this scenario would mostly be a mute point, and with additional security mechanisms, a rare occurrence

NS: DNS Service Security

- DNS provides a mapping of an IP address to a fully qualified domain name
- A system can be directed anywhere on the Internet with DNS, so the authenticity of the source of this information is critical
- This is where **DNS Security Extensions** (**DNSSEC**) come into play
  - provide authenticity for DNS resolver data
  - DNS data cannot be forged and attacks like DNS poisoning, where erroneous DNS is injected into DNS and propagated, resulting in pointing hosts to the wrong system on the Internet is mitigated. This is a common method used by malware writers and in phishing attacks
- Another area of security in regards to DNS implementation are DNS zone transfers
  - mechanism used in DNS to provide other DNS servers with what domains the DNS server is responsible for and all the details available for each record in the zone

NS: DNS Resolution

- DNS resolution can make for easy exploitation if there is no control on where the mapping information is obtained
  - This has been the main method used by the Zeus botnet
  - Hosts are pointed to maliciously controlled Internet servers by manipulating DNS information
  - The method also relies on compromised or specifically built DNS servers on the Internet, allowing malware writers to make up their own, unique and sometimes inconspicuous domain names

NS: DNS Zone Transfer

- A DNS zone transfer should be limited to only trusted partners and limited to only zones that need to be transferred
  - An enterprise may have several domain names for various services they provide to business partners and employees that are not "known" by the general public
    - Example, office-specific records, a VPN URL, SIP address for VoIP, etc
  - While the fact remains that if the service is available on the Internet, it can be found, a simple zone transfer reduces the discovery process significantly
- There may be internal and external DNS implementations with records specific to the network areas they service
  - the internal DNS server may have records for all internal hosts and services, while a DNS server in the DMZ may only have records for DMZ services
  - it is critical to keep the records uncontaminated from other zones
  - Specifically, TXT may give too much information that can be used in a malicious manner against the enterprise

NS: DNSSEC

- Most prevalent DNS attack is **DNS poisoning**, where the DNS information on the Internet is poisoned with false information, allowing attackers to direct clients to whatever IP address they desire
- Security extensions have been added to the DNS protocol by the **Internet Engineering Task Force** (**IETF**) **DNS Security** (**DNSSEC**) specification
  - provides security for specific information components of the DNS protocol in an effort to provide authenticity to the DNS information
- The importance of DNSSEC is that it is intended to give the recipient DNS server confidence in the source of the DNS records or resolver data that it receives

NS: Email Service Security

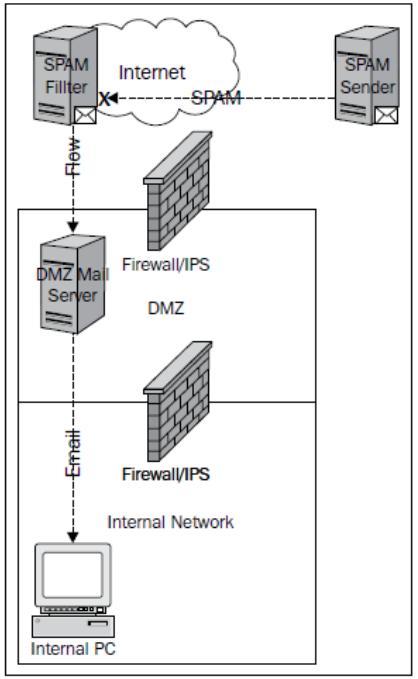
- Email service is a critical business function
- With the increased growth and acceptance of cloud-based services, e-mail is amongst the first to be leveraged
- Some enterprises have already moved their e-mail implementation to the cloud
  - + Enables lower cost and *as-a-service* implementation
  - - enterprises have lower control over email security
- The next few slides will cover common e-mail threats and present methods to secure e-mail services

NS: Spam Filtering

- E-mail is one of the most popular methods to spread malware or lead users to malware hosted on the Internet
  - Most often, this is the single intent of unwanted e-mails in the form of SPAM
  - Receiving SPAM and becoming the source of SPAM while being used as a relay are two sides to the same coin
- Methods to protect the enterprise from SPAM include cloud-based and local SPAM filtering at the network layer and host-based solutions at the client
  - A combination of these methods can prove to be most effective

NS: Spam Filtering @ Cloud

- Works by configuring the DNS **mail record** (**MX**)* to identify the service provider's e-mail servers
  - This configuration forces all e-mails destined to e-mail addresses owned by the enterprise through the SPAM solution filtering systems before forwarding to the final enterprise servers and user mailbox
  - Outbound mail from the enterprise would take the normal path to the destination as configured, to use DNS to find the destination domain email server IP address



Source: Aaron Woody, Enterprise Security: A Data-Centric Approach To Securing The Enterprise

A mail exchanger record (MX record) specifies the mail server responsible for accepting email messages on behalf of a domain name. It is a resource record in the Domain Name System (DNS). It is possible to configure several MX records, typically pointing to an array of mail servers for load balancing and redundancy. Source: Wikipedia

NS: Spam Filtering @ Cloud (2)

- Pros and Cons:
  - + Zero or limited administration of the solution
  - + Reduction in Spam traffic
  - + Reduction in malware and other threats
  - - Significant cost, depending on service fee structure
  - - lack of visibility and control of filters
  - - service failure => no email or unwanted delays
- Enterprise needs to do cost-benefit analysis before taking this option
  - Cost of service
  - Implicit cost (e.g. due to loss of service, or unwanted delays)
  - Benefits (savings due to reduction in spam emails or malware threats)

Network Segmentation

- Even with the most sophisticated security mechanisms, without network segmentation, their value will be greatly undermined
- Internal segmentation is often overlooked, but is extremely important to prevent spread of malware throughout the enterprise
  - advanced threats are introduced through infected consultant systems, unauthorized introduction of personal devices and business-critical applications

Network Segmentation Strategy

- Before any network segmentation can occur, critical data, processes, applications, and systems must be identified
  - helps determine the complexities of moving the assets to a network segment separated by a firewall
- Network segmentation using a firewall is the simplest network-based security control
- Alongside, highly recommended security monitoring tools, such as **Security Information and Event Management** (**SIEM**) and **File Integrity Monitoring** (**FIM**) should be implemented to ensure that in the event of an attack, there is monitoring for early detection and timely incident response
- In some cases, leveraging data loss prevention tools may be ideal to protect against data leakage

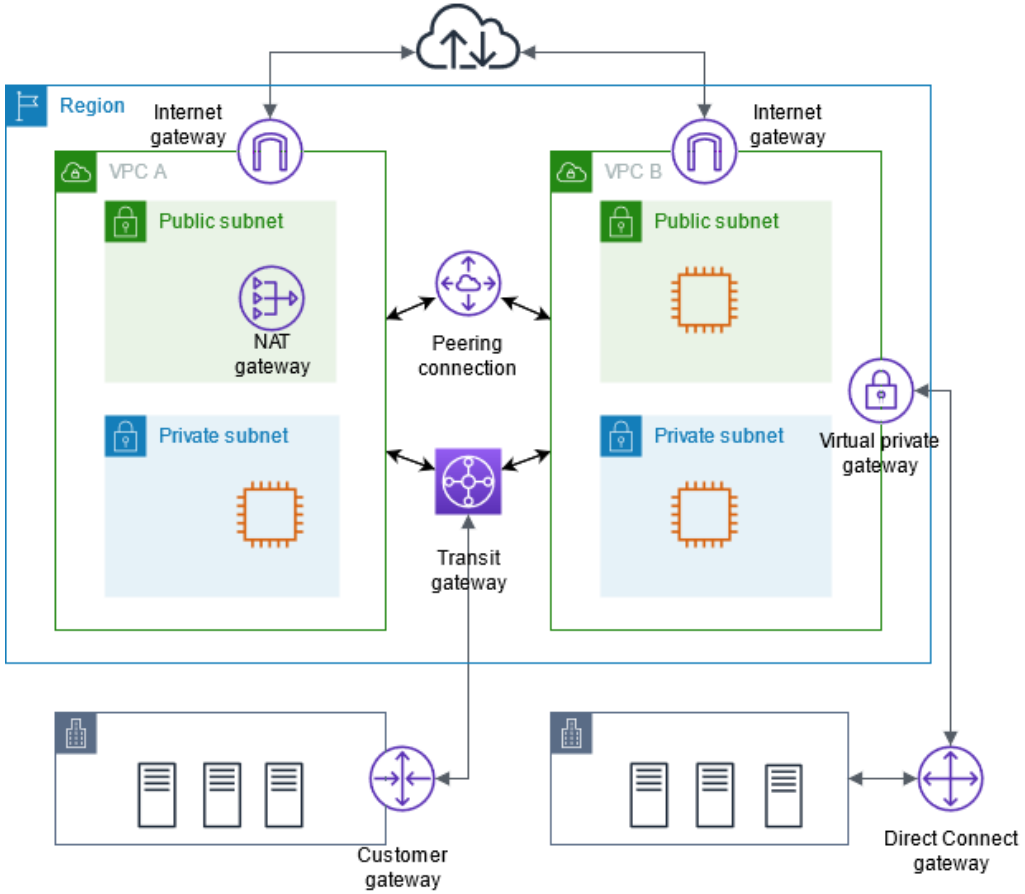
innovate achieve lead

BITS Pilani
Pilani Campus

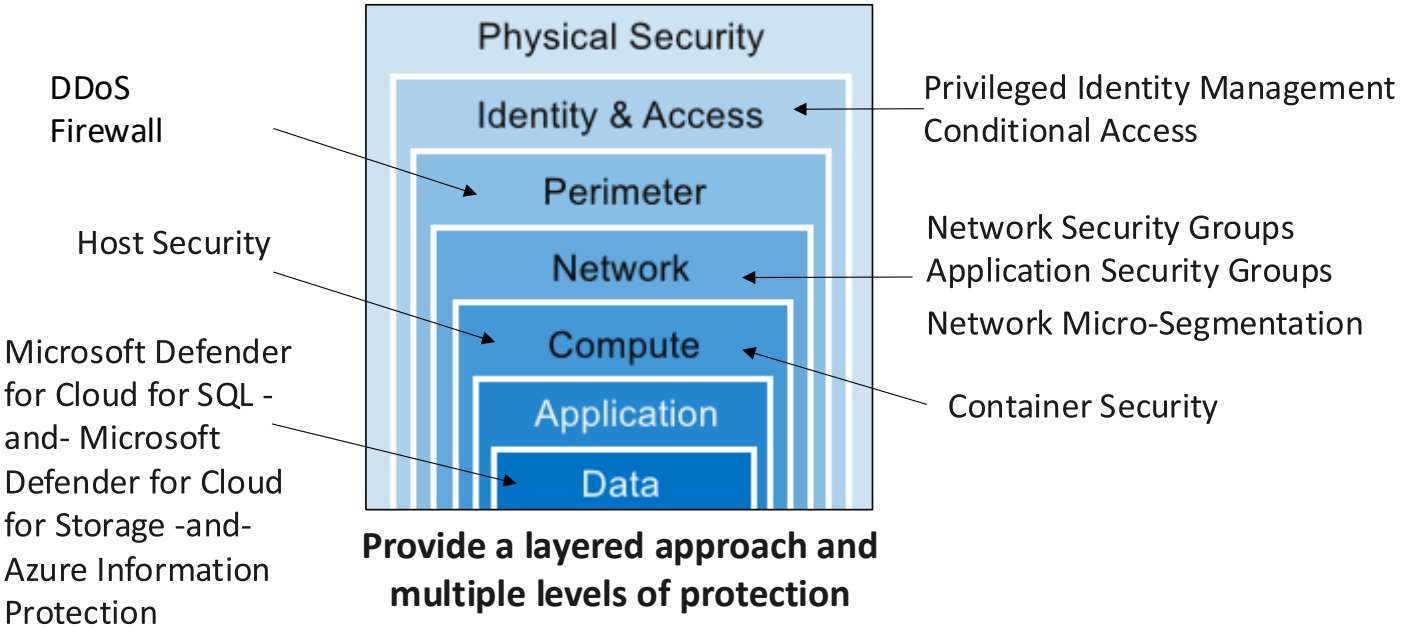
Cloud Network Security

Securing Network Perimeter and Network Services on the Cloud

RECAP: Amazon VPC Networking



Defense in Depth



Cloud Network Security

- Perimeter Security to protect your “virtual network” via combination of:
  - DDoS mitigation solutions
  - Firewall services (Network Firewalls and Web Application Firewalls)
  - VPN services
- Network Security
  - Network segmentation (e.g. hub and spoke vnets, Network Service Groups)
    - Use of security rules to allow or deny network traffic
    - Can be associated to a subnet or a network interface

innovate achieve lead

BITS Pilani

Pilani Campus

Case Study: Platform Security Features in Microsoft Azure

innovate achieve lead

BITS Pilani

Pilani Campus

Extra Reading: Can ZTNA replace your VPN?

ZTNA vs VPN

Thank You!