UNIT-IV

PART-A

Security

Syllabus

- Data Security
- Network Security
- Host Security

Data Security

- Data Control
- Encrypt Everything
- Regulatory and Standards Compliance

- The first question I hear from most executives is, “Should I be concerned about losing control over where my data is stored?”

Data Security

- **Physical security** defines how you control physical access to the servers that support your infrastructure.
- The cloud still has physical security **constraints**.
- When selecting a **cloud provider**, you should understand their **physical security protocols** and the **things** you need to do on your end to secure your systems against **physical vulnerabilities.**

DATA CONTROL

- The big chasm between traditional data centers and the cloud is the location of your data on **someone else's servers.**
- **Companies** who have outsourced their data centers to a managed services **provider** may have crossed part of that chasm; what cloud services add is the **inability** to **see** or **touch** the servers on which their data is hosted.


SECURITY
Security Assessment
Two-factor
Anti-virus
FIM
Log Review
WAF
DDOS
Vulnerability Scanning
IDS/IPS
Firewall
Dedicated Firewall
PROFESSIONAL SERVICES
DATA PROTECTION
CLOUD

DATA CONTROL

- The main practical problem is that factors that have nothing to do with your business can **compromise** your operations and your data.
- For **example**, any of the following **events** could **create trouble** for your infrastructure:
  - The cloud provider declares **bankruptcy** and its servers are seized or it ceases operations.
  - A third party with no relationship to you (or, worse, a competitor) sues your cloud provider and obtains a blanket **subpoena** granting access to all servers owned by the cloud provider.
  - Failure of your cloud provider to properly secure portions of its infrastructure—especially in the maintenance of physical access controls—results in the compromise of your systems.

THE LAWYER GLOSSARY

Legal Terms Simplified

SUBPOENA

NOUN, VERB [SUH-PEE-NUH]

LATIN MEANING 'UNDER PENALTY' AN ORDER REQUIRING A PERSON TO TESTIFY BEFORE THE COURTS IN A CASE, OR DEMANDING THE SUBMISSION OF EVIDENCE IN THE FORM OR DOCUMENTS, MEDIA OR RELEVANT MATERIALS.

DATA CONTROL

- **The solution is to do two things:**
  - **Encrypt** sensitive data in your database and in memory. Decrypt it only in memory for the duration of the need for the data. Encrypt your backups and encrypt all network communications.
  - Choose a second provider and use **automated**, regular **backups** (for which many open source and commercial solutions exist) to make sure any current and historical data can be **recovered** even if your cloud provider were to **disappear** from the face of the earth.

DATA CONTROL

- How these **measures** deal with each **scenario**,
  - When the cloud provider goes down
  - When a subpoena compels your cloud provider to turn over your data
  - When your cloud provider fails to adequately protect their network

When the cloud provider goes down

- This scenario has a number of variants:
  - Bankruptcy
  - Deciding to take the business in another direction
  - A widespread and extended outage

When a subpoena compels your cloud provider to turn over your data

- If the subpoena is directed at you, obviously you have to turn over the data to the courts, regardless of what precautions you take, but these legal requirements apply whether your data is in the cloud or on your own internal IT infrastructure.
- What we're dealing with here is a subpoena aimed at your cloud provider that results from court action that has nothing to do with you.
- Encrypting your data will protect you against this scenario. The subpoena will compel your cloud provider to turn over your data and any access it might have to that data, but your cloud provider won't have your access or decryption keys. To get at the data, the court will have to come to you and subpoena you.
- As a result, you will end up with the same level of control you have in your private data center.

When your cloud provider fails to adequately protect their network

- When you select a cloud provider, you absolutely must understand how they treat physical, network, and host security.
- Though it may sound counterintuitive, the most secure cloud provider is one in which you never know where the physical server behind your virtual instance is running.
- Chances are that if you cannot figure it out, a determined hacker who is specifically targeting your organization is going to have a much harder time breaching the physical environment in which your data is hosted.

Note

- **Amazon** does not even disclose where their data centers are located; they simply claim that each data center is housed in a nondescript building with a military-grade perimeter.
- Even if you know that my database server is in the **us-east-1a availability zone,** you don't know where the data center(s) behind that availability zone is located, or even which of the three East Coast availability zones us-east-1a represents.
- Amazon publishes its security standards and processes at *http://aws.amazon.com*. Whatever cloud provider you use, you should understand their security standards and practices, and expect them to exceed anything you require.

Encrypt Everything

- Encrypt your network traffic
- Encrypt your backups
- Encrypt your filesystems

Encrypt Everything

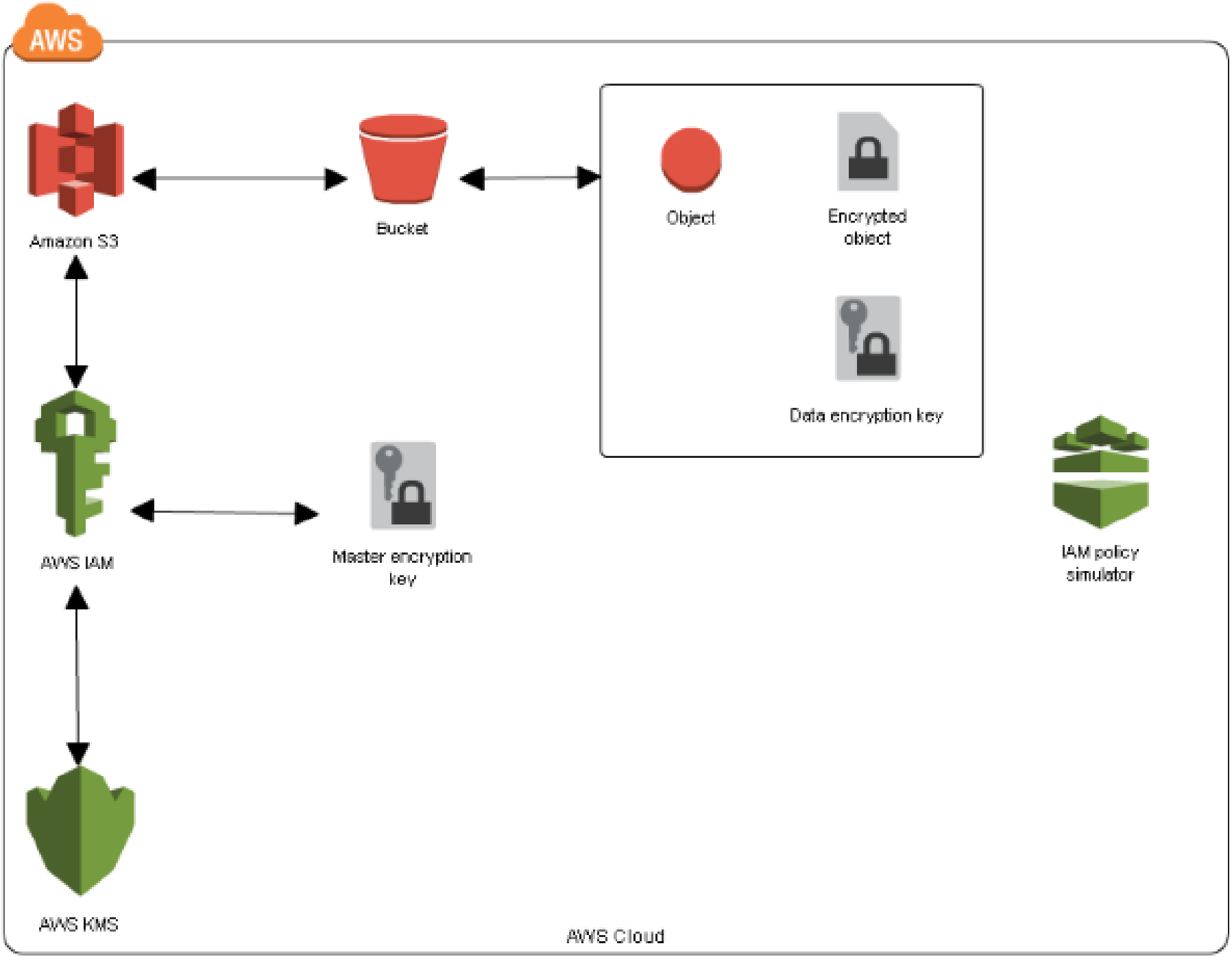
- In the cloud, your data is **stored** somewhere; you just don't know exactly where. However, you know some **basic parameters**:
  - Your data lies within a virtual machine guest operating system, and you **control** the mechanisms for access to that data.
  - Network traffic **exchanging** data between instances is not visible to other virtual hosts.
  - For most cloud **storage** services, access to data is private by default. Many, including Amazon S3, nevertheless allow you to make that data public.

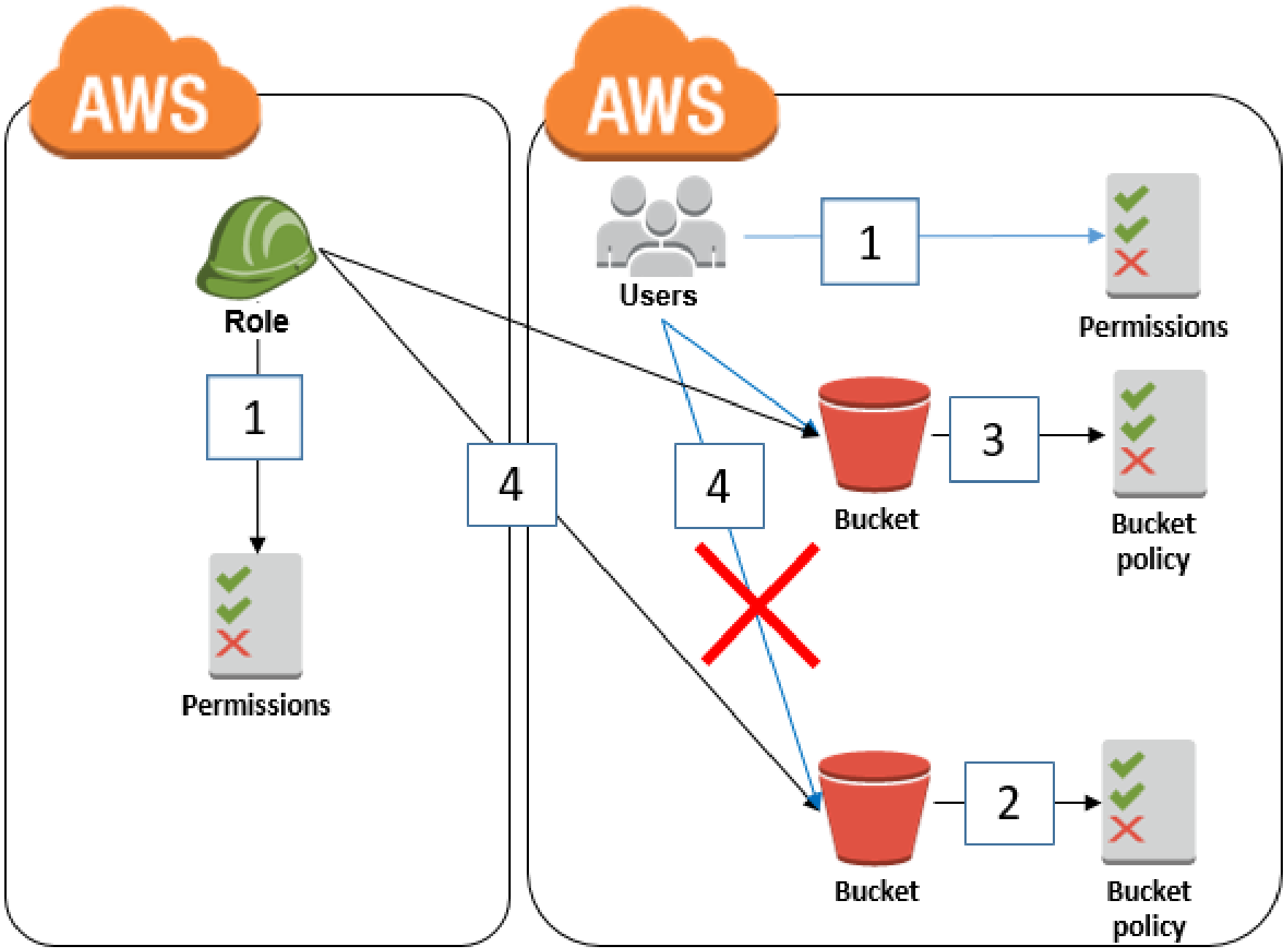
Encrypt your network traffic

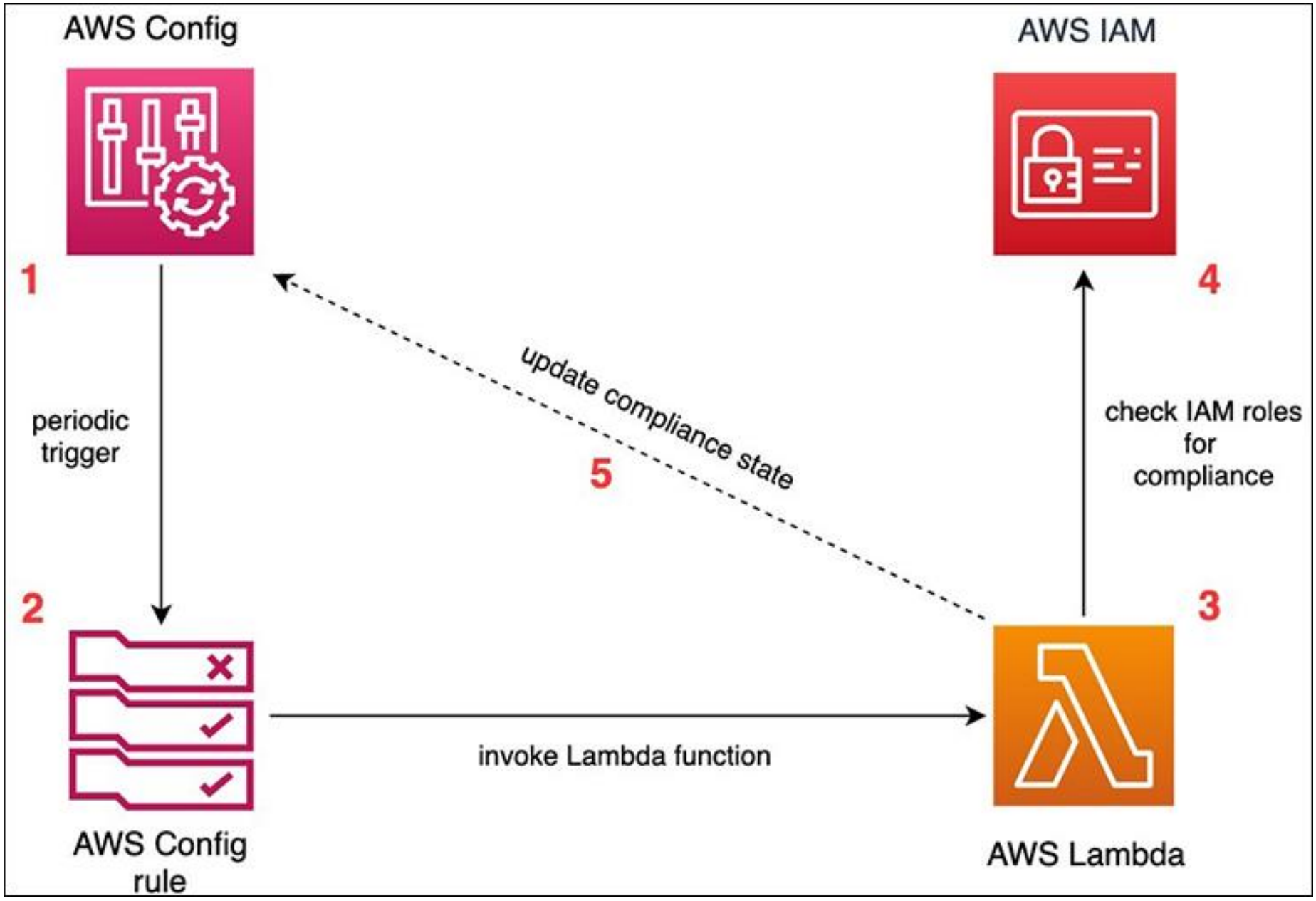
- No matter how lax your current security practices, you probably have network traffic encrypted—at least for the most part.
- A nice feature of the Amazon cloud is that virtual servers cannot sniff the traffic of other virtual servers.

Encrypt your backups

- When you bundle your data for backups, you should be encrypting it using some kind of strong cryptography, such as **PGP**.
- You can then safely store it in a moderately secure cloud storage environment like **Amazon S3**, or even in a completely insecure environment.
- Encryption **eats** up CPU. As a result, it is recommend first copying your files in **plain text** over to a temporary backup server whose job it is to perform encryption, and then **uploading** the backups into your cloud storage system.


AWS
Amazon S3
Bucket
Object
Encrypted object
Data encryption key
AWS IAM
Master encryption key
IAM policy simulator
AWS KMS
AWS Cloud


AWS
AWS
Role
1
Permissions
4
Users
1
Permissions
4
Bucket
3
Bucket policy
Bucket
2
Bucket policy


AWS Config
AWS IAM
1
4
periodic trigger
update compliance state
5
check IAM roles for compliance
2
3
invoke Lambda function
AWS Config rule
AWS Lambda

```
{
  "type": "AssumedRole",
  "principalId": "AROAJI4AVVEXAMPLE:ROLE-SESSION-NAME",
  "arn": "arn:aws:sts::ACCOUNTNUMBER:assumed-role/ROLE-NAME/ROLE-SESSION-NAME",
  "accountId": "ACCOUNTNUMBER",
  "accessKeyId": "ASIAEXAMPLEKEY",
  "sessionContext": {
    "attributes": {
      "mfaAuthenticated": "false",
      "creationDate": "XXXX-XX-XXTXX:XX:XXZ"
    },
    "sessionIssuer": {
      "type": "Role",
      "principalId": "AROAJI4AVV3EXAMPLEID",
      "arn": "arn:aws:iam::ACCOUNTNUMBER:role/ROLE-NAME",
      "accountId": "ACCOUNTNUBMER",
      "userName": "ROLE-SESSION-NAME"
    }
  }
}
```

Encrypt your filesystems

- Each virtual server you manage will mount ephemeral storage devices (such as the /mnt partition on Unix EC2 instances) or block storage devices.
- The failure to encrypt ephemeral devices poses only a very moderate risk in an EC2 environment because the EC2 Xen system zeros out that storage when your instance terminates.
- Snapshots for block storage devices, however, sit in Amazon S3 unencrypted unless you take special action to encrypt them.

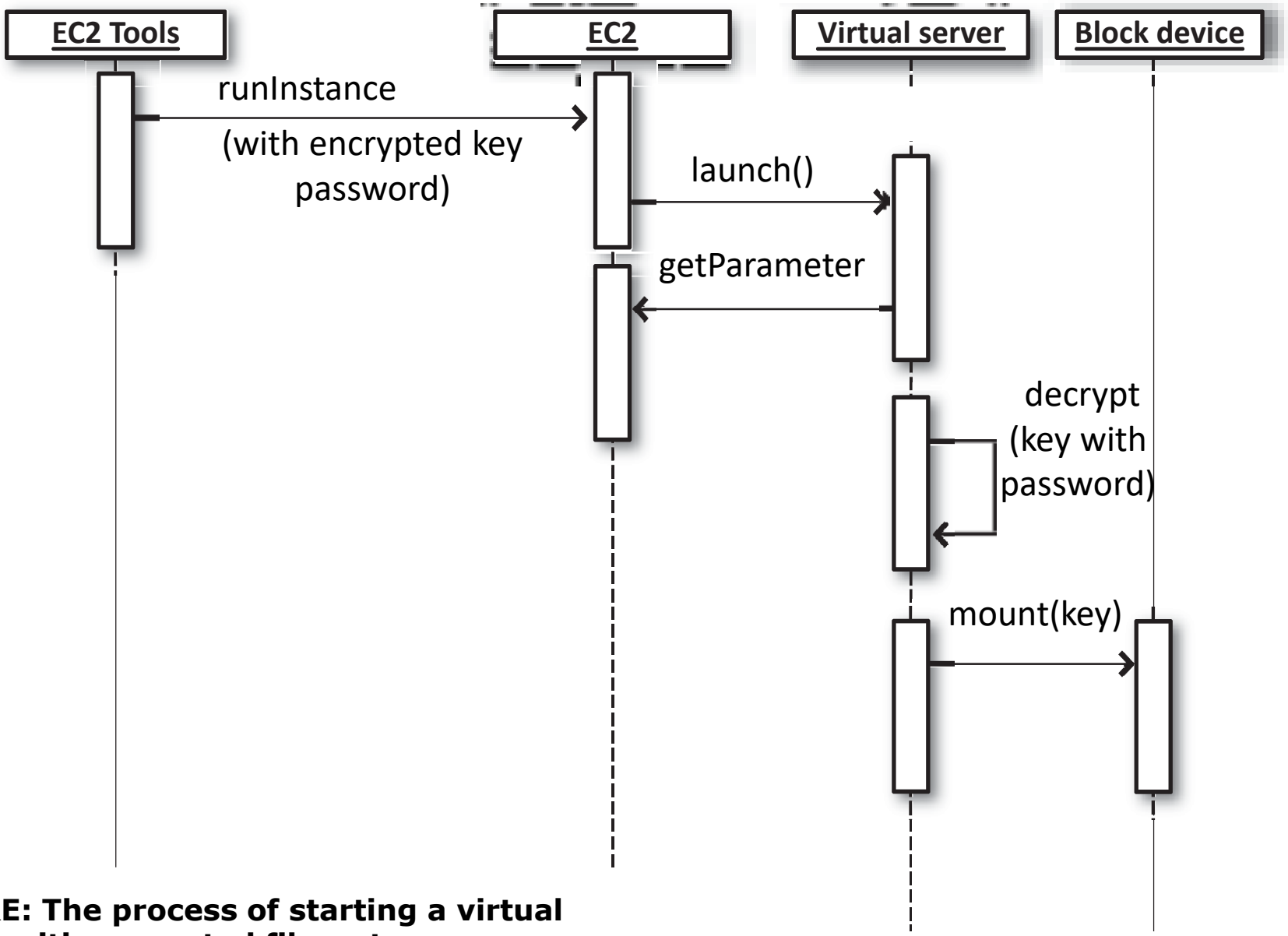


FIGURE: The process of starting a virtual server with encrypted filesystems

Regulatory and Standards Compliance

- Most problems with regulatory and standards compliance lie not with the cloud, but in the fact that the regulations and standards written for Internet applications predate the acceptance of virtualization technologies.
- In other words, chances are you can meet the spirit of any particular specification, but you may not be able to meet the letter of the specification.

Regulatory and Standards Compliance

- **Directive 95/46/EC -** EC Directive on Data Protection. A 1995 directive for European Union nations relating to the protection of private data and where it can be shared.
- **HIPAA -** Health Insurance Portability and Accountability Act. A comprehensive law relating to a number of health care issues. Of particular concern to technologists are the privacy and security regulations around the handling of health care data.
- **PCI or PCI DSS -** Payment Card Industry Data Security Standard. A standard that defines the information security processes and procedures to which an organization must adhere when handling credit card transactions.
- **SOX -** Sarbanes-Oxley Act. Establishes legal requirements around the reporting of publicly held companies to their shareholders.

Regulatory and Standards Compliance

- From a security perspective, you'll encounter three kinds of issues in standards and regulations:
  - **"How" issues** - These result from a standard such as PCI or regulations such as HIPAA or SOX, which govern how an application of a specific type should operate in order to protect certain concerns specific to its problem domain. For example, HIPAA defines how you should handle personally identifying health care data.
  - **"Where" issues** - These result from a directive such as Directive 95/46/EC that governs where you can store certain information. One key impact of this particular directive is that the private data on EU citizens may not be stored in the United States (or any other country that does not treat private data in the same way as the EU).
  - **"What" issues** - These result from standards prescribing very specific components to your infrastructure. For example, PCI prescribes the use of antivirus software on all servers processing credit card data.

Network Security

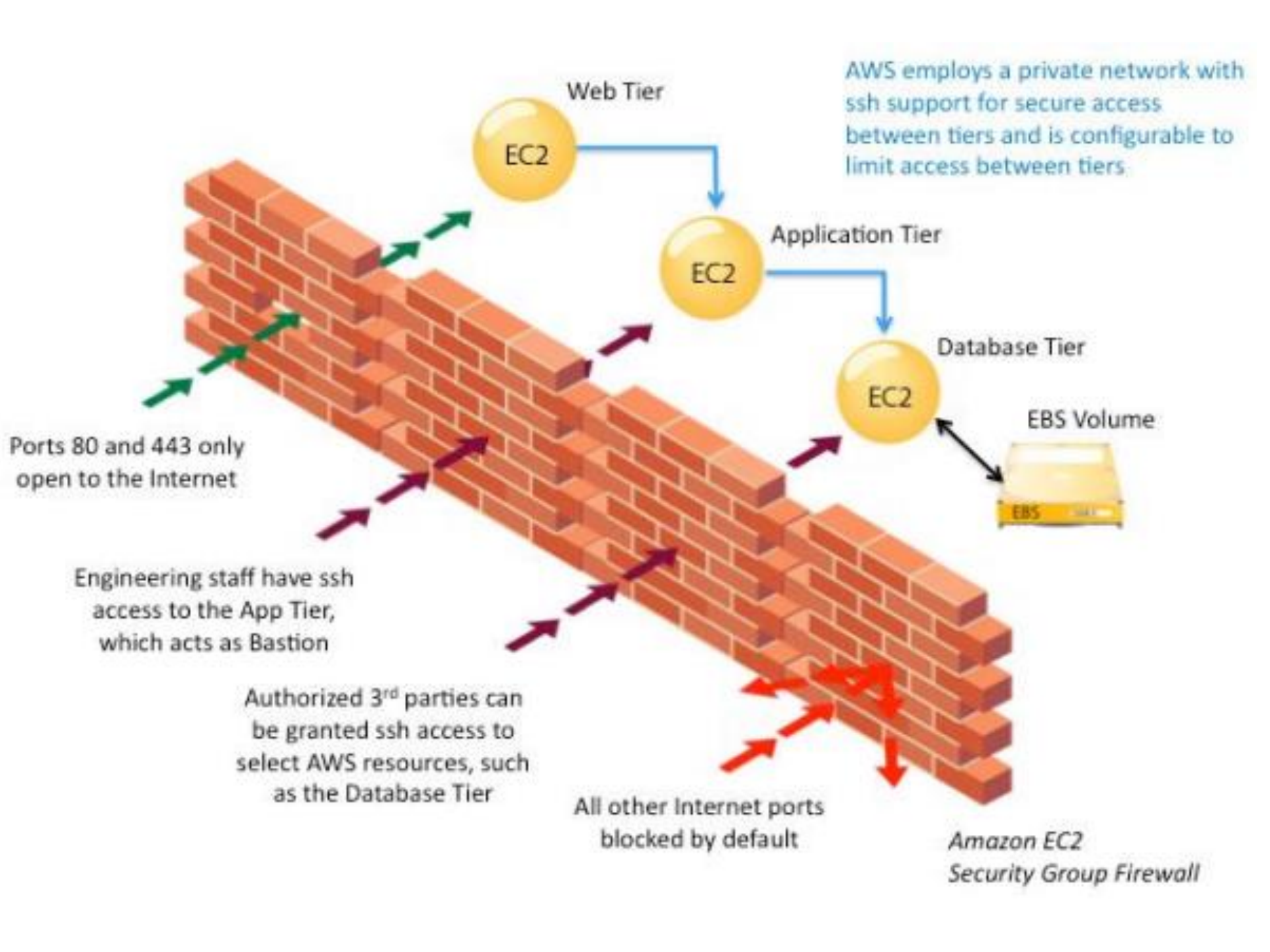
- Firewall Rules
- Network Intrusion Detection
  - The purpose of a network intrusion detection system
  - Implementing network intrusion detection in the cloud

Network Security

- Amazon's cloud has no perimeter. Instead, EC2 provides security groups that define firewall-like traffic rules governing what traffic can reach virtual servers in that group.

Network Security

- Security groups as if they were virtual network segments protected by a firewall, they most definitely are not virtual network segments, due to the following:
  - Two servers in two different Amazon EC2 availability zones can operate in the same security group
  - A server may belong to more than one security group
  - Servers in the same security group may not be able to talk to each other at all
  - Servers in the same network segment may not share any IP characteristics—they may even be in different class address spaces
  - No server in EC2 can see the network traffic bound for other servers. If you try placing your virtual Linux server in promiscuous mode, the only network traffic you will see is traffic originating from or destined for your server


AWS employs a private network with ssh support for secure access between tiers and is configurable to limit access between tiers
Web Tier
EC2
Application Tier
EC2
Database Tier
EC2
EBS Volume
EBS
Ports 80 and 443 only open to the Internet
Engineering staff have ssh access to the App Tier, which acts as Bastion
Authorized 3rd parties can be granted ssh access to select AWS resources, such as the Database Tier
All other Internet ports blocked by default
Amazon EC2 Security Group Firewall

Firewall Rules

- Typically, a firewall protects the perimeter of one or more network segments. Below Figure illustrates how a firewall protects the perimeter.

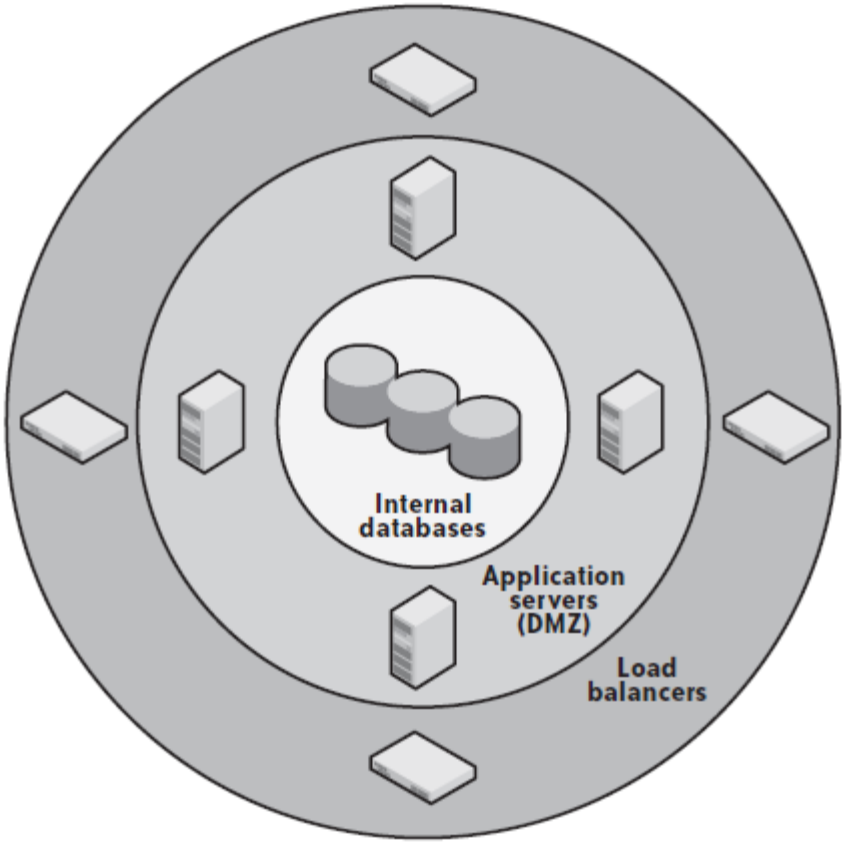


Fig: Firewalls are the primary tool in perimeter security

Firewall Rules

- A main firewall protects the outermost perimeter, allowing in only HTTP, HTTPS, and (sometimes) FTP traffic.
- Within that network segment are border systems, such as load balancers, that route traffic into a DMZ protected by another firewall.
- Finally, within the DMZ are application servers that make database and other requests across a third firewall into protected systems on a highly sensitive internal network.

Firewall Rules

- Below Figure provides a visual look at how the concept of a firewall rule in the Amazon cloud is different from that in a traditional data center.

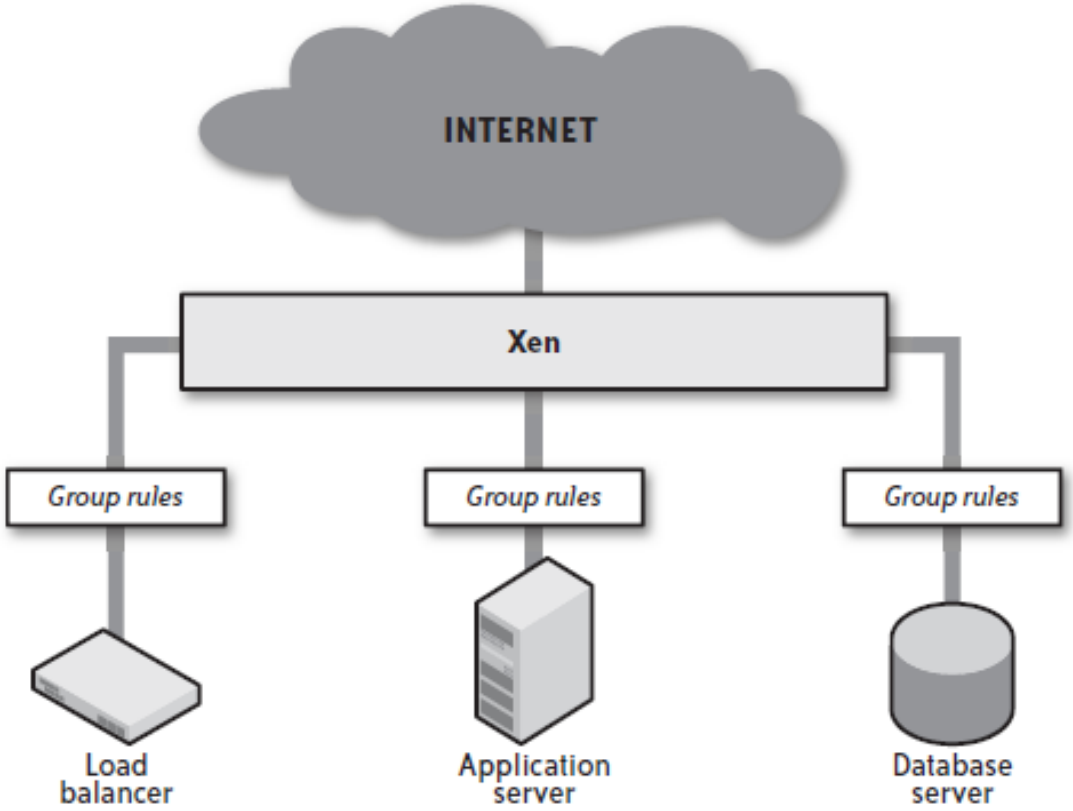


Fig: There are no network segments or perimeters in the cloud

Firewall Rules

- Each virtual server occupies the same level in the network, with its traffic managed through a security group definition. There are no network segments, and there is no perimeter.
- Membership in the same group does not provide any privileged access to other servers in that security group, unless you define rules that provide privileged access.
- Finally, an individual server can be a member of multiple security groups. The rules for a given server are simply the union of the rules assigned to all groups of which the server is a member.

Firewall Rules

- You can set up security groups to help you mimic traditional perimeter security. For example, you can create the following:
  - A border security group that listens to all traffic on ports 80 and 443.
  - A DMZ security group that listens to traffic from the border group on ports 80 and 443.
  - An internal security group that listens to traffic on port 3306 from the DMZ security group.

Firewall Rules

- The two advantages of this security architecture are the following:
  - Because you control your firewall rules remotely, an intruder does not have a single target to attack, as he does with a physical firewall
  - You don’t have the opportunity to accidentally destroy your network rules and thus permanently remove everyone’s access to a given network segment

Firewall Rules

- A few best practices for your network security include:
  - Run only one network service (plus necessary administrative services) on each virtual server.
  - Do not open up direct access to your most sensitive data.
  - Open only the ports absolutely necessary to support a server's service and nothing more.
  - Limit access to your services to clients who need to access them.
  - Even if you are not doing load balancing, use a reverse proxy.
  - Use the dynamic nature of the cloud to automate your security embarrassments.

Network Intrusion Detection

- Perimeter security often involves network intrusion detection systems (NIDS), such as Snort, which monitor local traffic for anything that looks irregular. Examples of irregular traffic include:
  - Port scans
  - Denial-of-service attacks
  - Known vulnerability exploit attempts
- A network-based intrusion detection system (**NIDS**) is used to monitor and analyze network traffic to protect a system from network-based threats. A **NIDS** reads all inbound packets and searches for any suspicious patterns.
- You perform network intrusion detection either by routing all traffic through a system that analyzes it or by doing passive monitoring from one box on local traffic on your network. In the Amazon cloud, only the former is possible; the latter is meaningless since an EC2 instance can see only its own traffic.

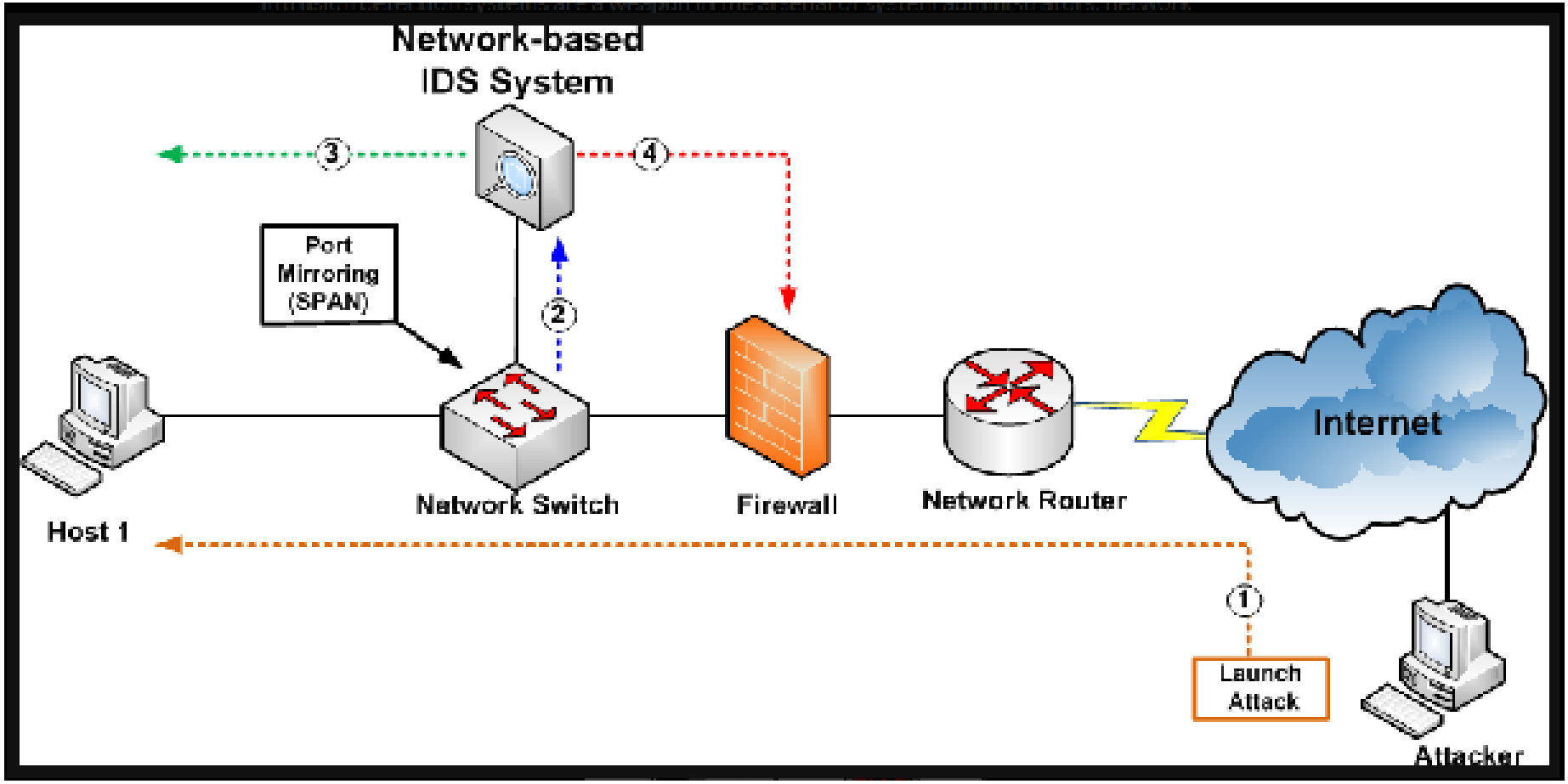


Figure: Architecture of Network based IDS

The purpose of a network intrusion detection system

- Network intrusion detection exists to alert you of attacks before they happen and, in some cases, foil attacks as they happen. Because of the way the Amazon cloud is set up, however, many of the things you look for in a NIDS are meaningless.
- For example, a NIDS typically alerts you to port scans as evidence of a precursor to a potential future attack.

The purpose of a network intrusion detection system

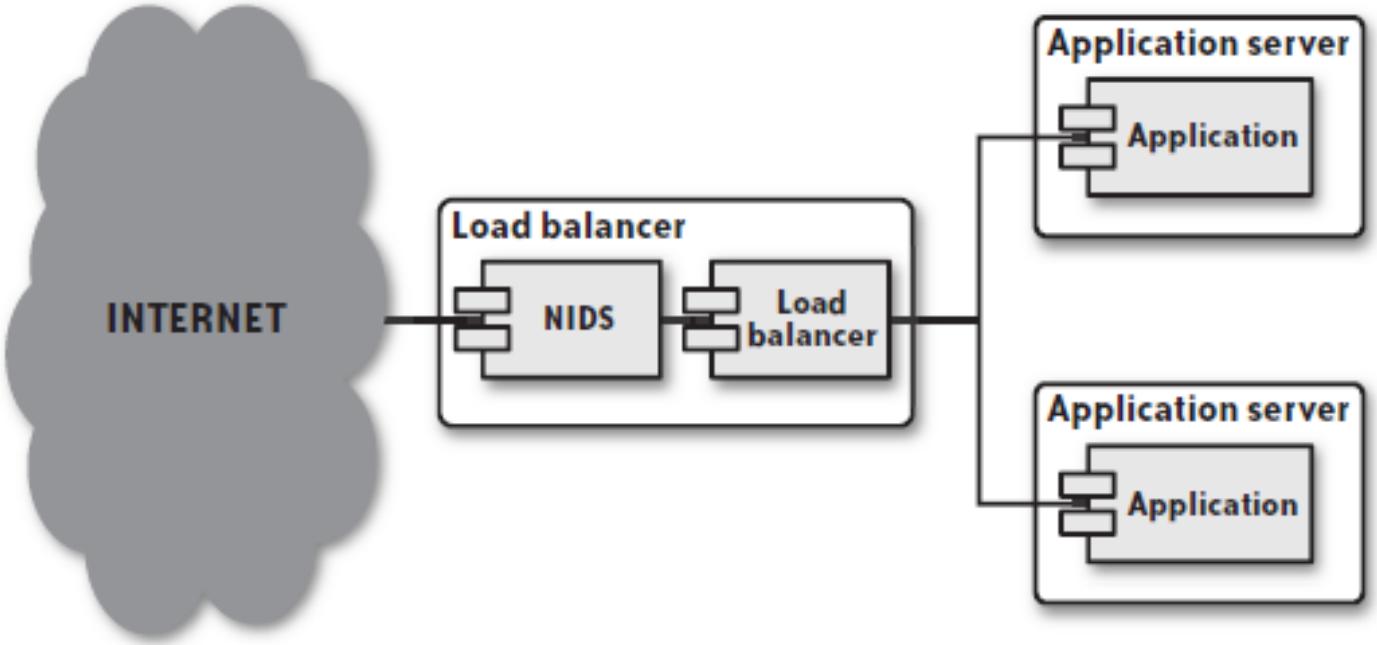
- In the Amazon cloud, however, you are not likely to notice a port scan because your NIDS will be aware only of requests coming in on the ports allowed by your security group rules. All other traffic will be invisible to the NIDS and thus are not likely to be perceived as a port scan.
- As with port scans, Amazon network intrusion systems are actively looking for denial-of-service attacks and would likely identify any such attempts long before your own intrusion detection software.

Implementing network intrusion detection in the cloud

- You cannot simply implement a network intrusion detection system in the Amazon cloud that passively listens to local network traffic.
- Instead, you must run the NIDS on your load balancer or on each server in your infrastructure.
- There are advantages and disadvantages to each approach.

Implementing network intrusion detection in the cloud

- The simplest approach is to have a dedicated NIDS server in front of the network as a whole that watches all incoming traffic and acts accordingly.
- Below figure illustrates this architecture.



Implementing network intrusion detection in the cloud

- Because the only software running on the load balancer is the NIDS software and Apache, it maintains a very low attack profile.
- The load balancer approach creates a single point of failure for your network intrusion detection system because, in general, the load balancer is the most exposed component in your infrastructure.
- By finding a way to compromise your load balancer, the intruder not only takes control of the load balancer, but also has the ability to silence detection of further attacks against your cloud environment.

Implementing network intrusion detection in the cloud

- You can alternately implement intrusion detection on a server behind the load balancer that acts as an intermediate point between the load balancer and the rest of the system.
- This design is generally superior to the previously described design, except that it leaves the load balancer exposed (only traffic passed by the load balancer is examined) and reduces the overall availability of the system.

Implementing network intrusion detection in the cloud

- Another approach is to implement network intrusion detection on each server in the network.
- This approach creates a very slight increase in the attack profile of the system as a whole because you end up with common software on all servers.
- A vulnerability in your NIDS would result in a vulnerability on each server in your cloud architecture. On a positive note, you make it much more difficult for an intruder to hide his footprints.

Host Security

- System Hardening
- Antivirus Protection
- Host Intrusion Detection
- Data Segmentation
- Credential Management

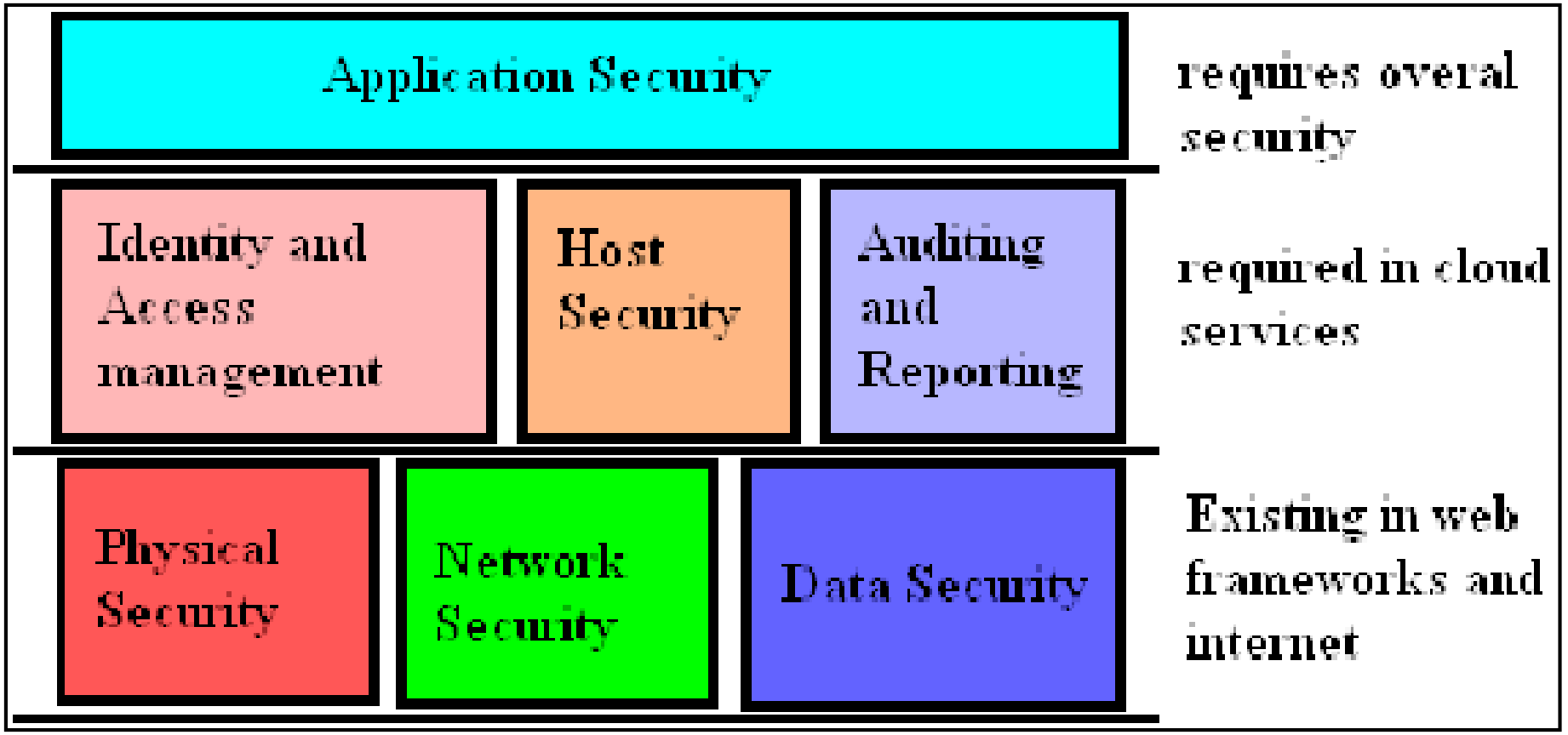


Figure: Security levels in cloud computing

Host Security

- Host security describes how your server is set up for the following **tasks**:
  - Preventing attacks
  - Minimizing the impact of a successful attack on the overall system
  - Responding to attacks when they occur

Host Security

- In the cloud, rolling out a patch across the infrastructure takes **three** simple steps:
  - Patch your AMI (Amazon Machine Image) with the new security fixes
  - Test the results
  - Relaunch your virtual servers

Host Security

- Here a tool such as **enStratus** or **RightScale** for managing your infrastructure becomes absolutely critical.
- If you have to **manually** perform these three steps, the cloud can become a **horrible** maintenance **headache**.

System Hardening

- **Server hardening is the process of disabling or removing unnecessary services and eliminating unimportant user accounts.**
- Tools such as **Bastille Linux** can make the process of hardening your machine images much more efficient.
- Once you install Bastille Linux, you execute the interactive scripts that ask you questions about your server.
- It then proceeds to disable services and accounts.

System Hardening


SERVER
HARDENING
FOR SECURITY
AND AVAILABILITY

System Hardening

- Hardened system meets the following **criteria**:
  - **No network services** are running except those necessary to support the server's function
  - **No user accounts** are enabled on the server except those necessary to support the services running on the server or to provide access for users who need it
  - **All configuration files** for common server software are configured to the most secure settings
  - **All necessary services** run under a nonprivileged role user account (e.g., run MySQL as the mysql user, not root)
  - When possible, run services in a restricted filesystem, such as a **Chroot jail**.

System Hardening

- Before bundling your machine image, you should remove all interactive user accounts and passwords stored in configuration files.
- Although the machine image will be stored in an encrypted format, Amazon holds the encryption keys and thus can be compelled to provide a third party with access through a court subpoena.

Antivirus Protection

- Some regulations and standards require the implementation of an antivirus (AV) system on your servers.
- It’s definitely a controversial issue, since an AV system with an exploit is itself an attack vector and, on some operating systems, the percentage of AV exploits to known viruses is relatively high.

Antivirus Protection

- When looking at the AV question, you first should understand what your requirements are.
- If you are required to implement AV, then you should definitely do it.
- Look for **two** critical features in your AV software:
  - How wide is the protection it provides? In other words, **what percentage of known exploits** does it cover?
  - What is the **median delta between** the time when a virus is **released** into the wild and the time your AV product of choice provides **protection** against it?

Host Intrusion Detection

- Whereas a network intrusion detection system (**NIDS**) monitors **network traffic** for suspicious activity, a host intrusion detection system (**HIDS**) such as OSSEC monitors the **state of your server** for anything unusual.
- OSSEC (**Open Source HIDS SECurity**) is a free, open-source host-based intrusion detection system (HIDS). It performs log analysis, Integrity checking, Windows registry monitoring, rootkit detection, time-based alerting and active response.
- An HIDS is in some ways similar to an AV system, except it examines the system for all signs of compromise and notifies you when any core operating system or service file changes.

OSSEC WebUI
Version 0.8

Main | Search | Integrity checking | Stats | About

April 23rd, 2018 08:55:58 AM

Available agents:

+ossec-server (127.0.0.1)
+a1 (172.31.28.131)

Latest modified files:

+/etc/gshadow
+/etc/gshadow-
+/etc/group
+/etc/group-
+/etc/shadow
+/etc/shadow-

Latest events

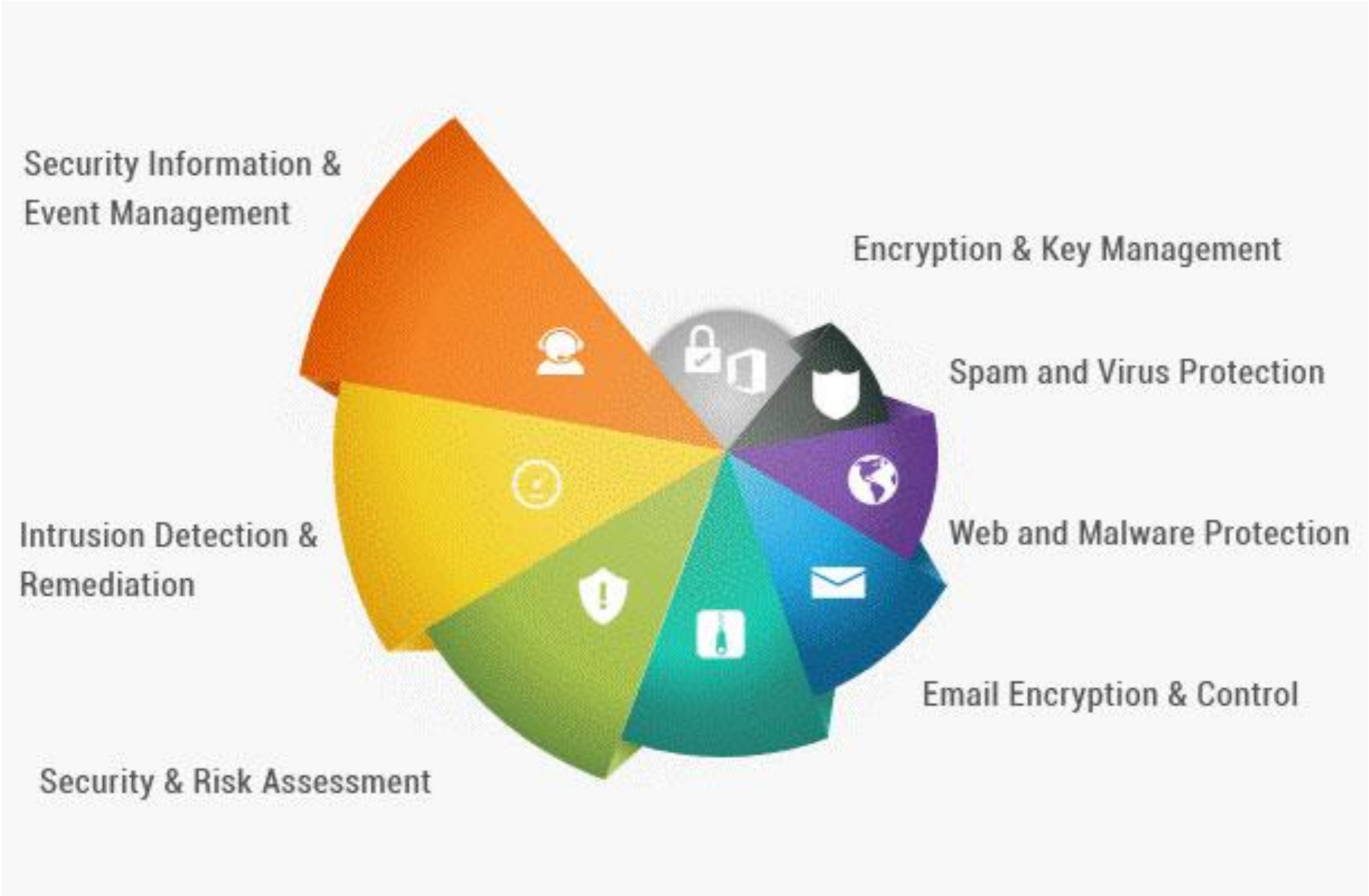
Level: 3 - Login session closed. **2018 Apr 23 08:49:39**
Rule Id: 5502
Location: ip-172-31-17-63->/var/log/secure
Apr 23 08:49:37 ip-172-31-17-63 su: pam_unix(su-l:session): session closed for user root

Level: 3 - Login session closed. **2018 Apr 23 08:49:39**
Rule Id: 5502
Location: ip-172-31-17-63->/var/log/secure
Apr 23 08:49:37 ip-172-31-17-63 sshd[2915]: pam_unix(sshd:session): session closed for user ec2-user

Level: 5 - Attempt to login using a non-existent user **2018 Apr 23 08:49:25**
Rule Id: 5710
Location: ip-172-31-17-63->/var/log/secure
Apr 23 08:49:24 ip-172-31-17-63 sshd[24780]: Invalid user admin from 196.202.94.179 port 42939

Level: 5 - Attempt to login using a non-existent user **2018 Apr 23 08:49:19**
Rule Id: 5710
Location: ip-172-31-17-63->/var/log/secure

Cloud Security Services and Cloud Security possible Solutions



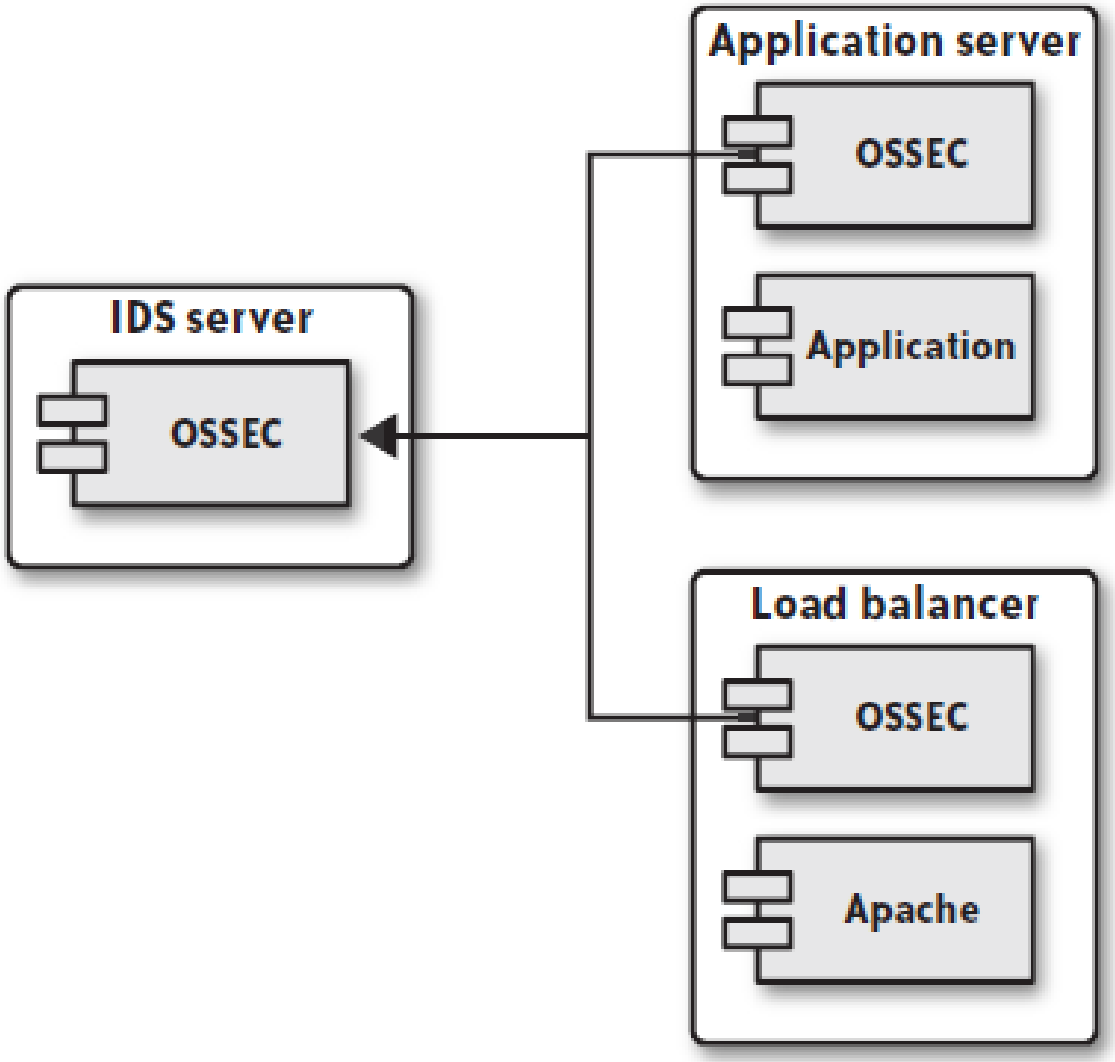
Host Intrusion Detection

- In Linux deployments, we use OSSEC (http://www.ossec.net) for host-based intrusion detection.
- OSSEC has two configuration profiles:
  - Standalone, in which each server scans itself and sends you alerts.
  - Centralized, in which you create a centralized HIDS server to which each of the other servers sends reports.

Host Intrusion Detection

- In the cloud, you should always opt for the centralized configuration.
- It centralizes your rules and analysis so that it is much easier to keep your HIDS infrastructure up to date.
- Furthermore, it enables you to craft a higher security profile for your HIDS processing than the individual services might allow for.
- Below figure illustrates a cloud network using centralized HIDS.

A HIDS infrastructure reporting to a centralized server



Host Intrusion Detection

- As with an AV solution, you must keep your HIDS servers up to date constantly, but you do not need to update your individual servers as often.
- The downside of an HIDS is that it requires CPU power to operate, and thus can eat up resources on your server.
- By going with a centralized deployment model, you can push a lot of that processing onto a specialized intrusion detection server.

Data Segmentation

- In addition to assuming that the services on your servers have security exploits, you should further assume that eventually one of them will be compromised.
- Obviously, you never want any server to be compromised.
- The best infrastructure is tolerant of—in fact, it assumes—the compromise of any individual node.
- This tolerance is not meant to encourage lax security for individual servers, but is meant to minimize the impact of the compromise of specific nodes.

Data Segmentation

- Making this assumption provides you with a system that has the following advantages:
  - Access to your most sensitive data requires a full system breach
  - The compromise of the entire system requires multiple attack vectors with potentially different skill sets
  - The downtime associated with the compromise of an individual node is negligible or nonexistent

Data Segmentation

- The segmentation of data based on differing levels of sensitivity is your first tool in minimizing the impact of a successful attack.
- We examined a form of data segmentation in previous topic when we separated credit card data from customer data.
- In that example, an attacker who accesses your customer database has found some important information, but that attacker still lacks access to the credit card data.
- To be able to access credit card data, decrypt it, and associate it with a specific individual, the attacker must compromise both the e-commerce application server and the credit card processor.

Data Segmentation

- Here again the approach of one server/one service helps out.
- Because each type of server in the chain offers a different attack vector, an attacker will need to exploit multiple attack vectors to compromise the system as a whole.

Credential Management

- Your machine images OSSEC profile should have no user accounts embedded in them.
- In fact, you should never allow password-based shell access to your virtual servers.
- The most secure approach to providing access to virtual servers is the dynamic delivery of public SSH keys to target servers.
- In other words, if someone needs access to a server, you should provide her credentials to the server when it starts up or via an administrative interface instead of embedding that information in the machine image.

Credential Management

- Of course, it is perfectly secure to embed public SSH keys in a machine image, and it makes life a lot easier.
- Unfortunately, it makes it harder to build the general-purpose machine images.
- Specifically, if you embed the public key credentials in a machine image, the user behind those credentials will have access to every machine built on that image.
- To remove her access or add access for another individual, you subsequently have to build a new machine image reflecting the changed dynamics.

Credential Management

- Therefore, you should keep things simple and maintainable by passing in user credentials as part of the process of launching your virtual server.
- At boot time, the virtual server has access to all of the parameters you pass in and can thus set up user accounts for each user you specify.
- It’s simple because it requires no tools other than those that Amazon already provides.
- On the other hand, adding and removing access after the system boots up becomes a manual task.

Credential Management

- Another approach is to use existing cloud infrastructure management tools or build your own that enable you to store user credentials outside the cloud and dynamically add and remove users to your cloud servers at runtime.
- This approach requires an administrative service running on each host and thus represents an extra attack vector against your server.