UNIT-5

Security

Syllabus :

Data Security: data control, encrypt everything, regulatory and standards compliance; Network Security: firewall rules, network intrusion detection; Host Security: system hardening, antivirus protection, host intrusion detection, data segmentation, credential management; Compromise response.

Introduction

Data Security

- Physical security defines how you control physical access to the servers that support your infrastructure.
- The cloud still has physical security constraints, there are actual servers running somewhere.
- 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.

6.1 Data Control

The big difference between traditional data centers and the cloud is the location of your data on someone else's servers, inability to see or touch the servers on which their data is hosted

The following events could create trouble for your infrastructure:

- The cloud provider declares bankruptcy and its servers are seized.
- A third party (competitor) gaining access to all servers owned by the cloud provider.
- Failure of your cloud provider in the maintenance of physical access controls—results in the compromise of your systems.

The solution is encrypt everything and keep off-site backups

- 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 to make sure any current and historical data can be recovered.

When the cloud provider goes down

- The cloud provider goes down because of many reasons due to bankruptcy, deciding to take the business in another direction, or a widespread and extended outage. Whatever is going on, you risk losing access.
- Set up your backups and recover from this. So take regular “off-site” backups and choose second cloud provider through which you can launch a replacement infrastructure.

When your cloud provider fails to adequately protect their network

- When select a cloud provider, must understand how they treat physical, network, and host security.

- The most secure cloud provider is one in which you never know where the physical server behind your virtual instance is running.

- 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.

- 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.

- If you follow everything recommend below your data confidentiality will be strongly protected against even complete incompetence on the part of your cloud provider.

6.2 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

- Encrypt network traffic for the most part.

- A nice feature of the Amazon cloud is that virtual servers cannot sniff the traffic of other virtual server.

- You should therefore encrypt all network traffic, not just web traffic.

Encrypt your backups

- When 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.

- Encryption eats up CPU.

- As a result, recommend is 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.

- Not only does the use of a backup server avoid taxing your application server and database server CPUs, it also enables you to have a single higher security.

Encrypt your file systems

- Each virtual server you manage will mount ephemeral storage devices (such as the /mnt partition on Unix EC2 instances) or block storage devices.

- Snapshots for block storage devices, The most secure approach to both scenarios is to mount ephemeral and block storage devices using an encrypted filesystem.

- The challenge with encrypted filesystems on servers lies in how you manage the decryption password.

- A given server needs your decryption password before it can mount any given encrypted filesystem.

- The most common approach to this problem is to store the password on an unencrypted root filesystem.

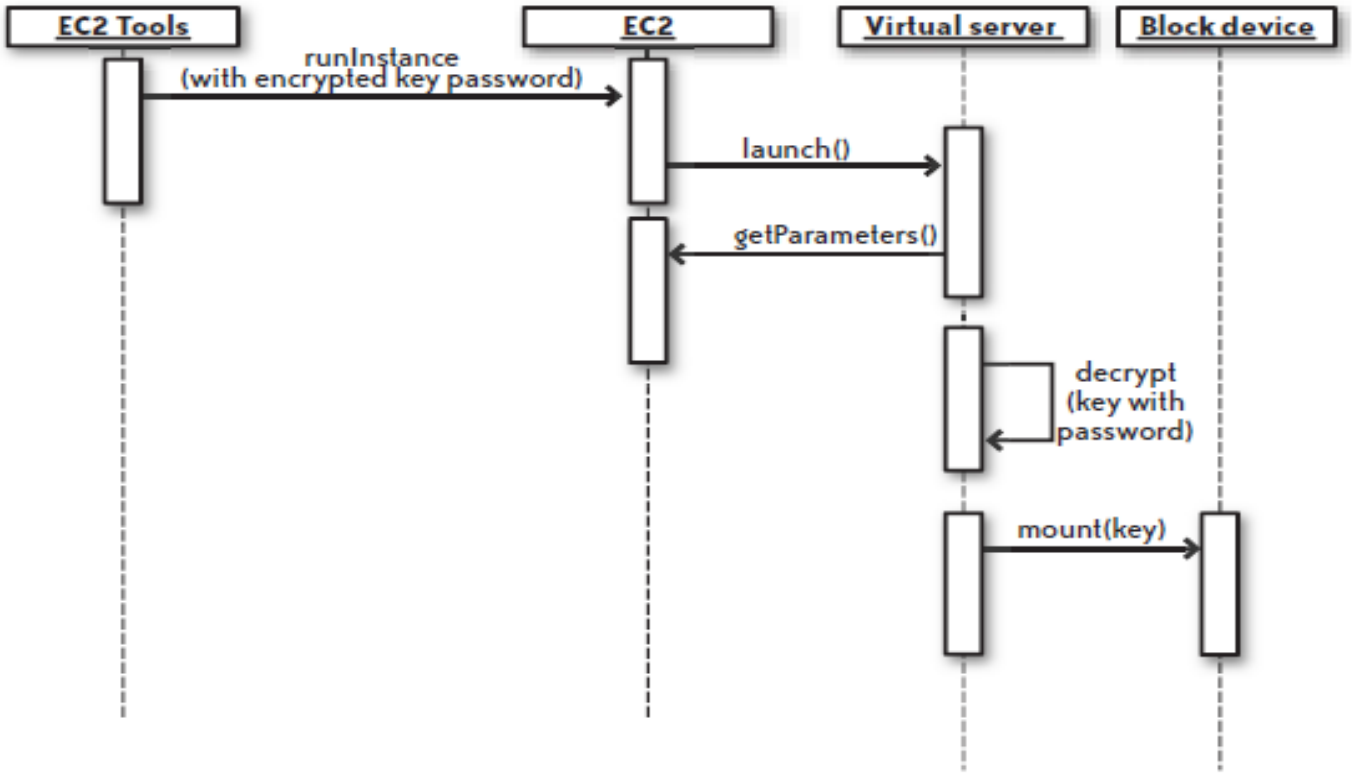
- Because the objective of filesystem encryption is to protect against physical access to the disk image, the storage of the password on a separate, virtual instance.

- In the cloud, you don't have to store the decryption password in the cloud. Instead, you can provide the decryption password to your new virtual instance when you start it up.

- The server can then grab the encryption key out of the server's startup parameters and subsequently mount any ephemeral or block devices using an encrypted filesystem.

You can add an extra layer of security into the mix by encrypting the password and storing the key for decrypting the password in the machine image.

Figure illustrates the process of starting up a virtual server that mounts an encrypted filesystem using an encrypted password.



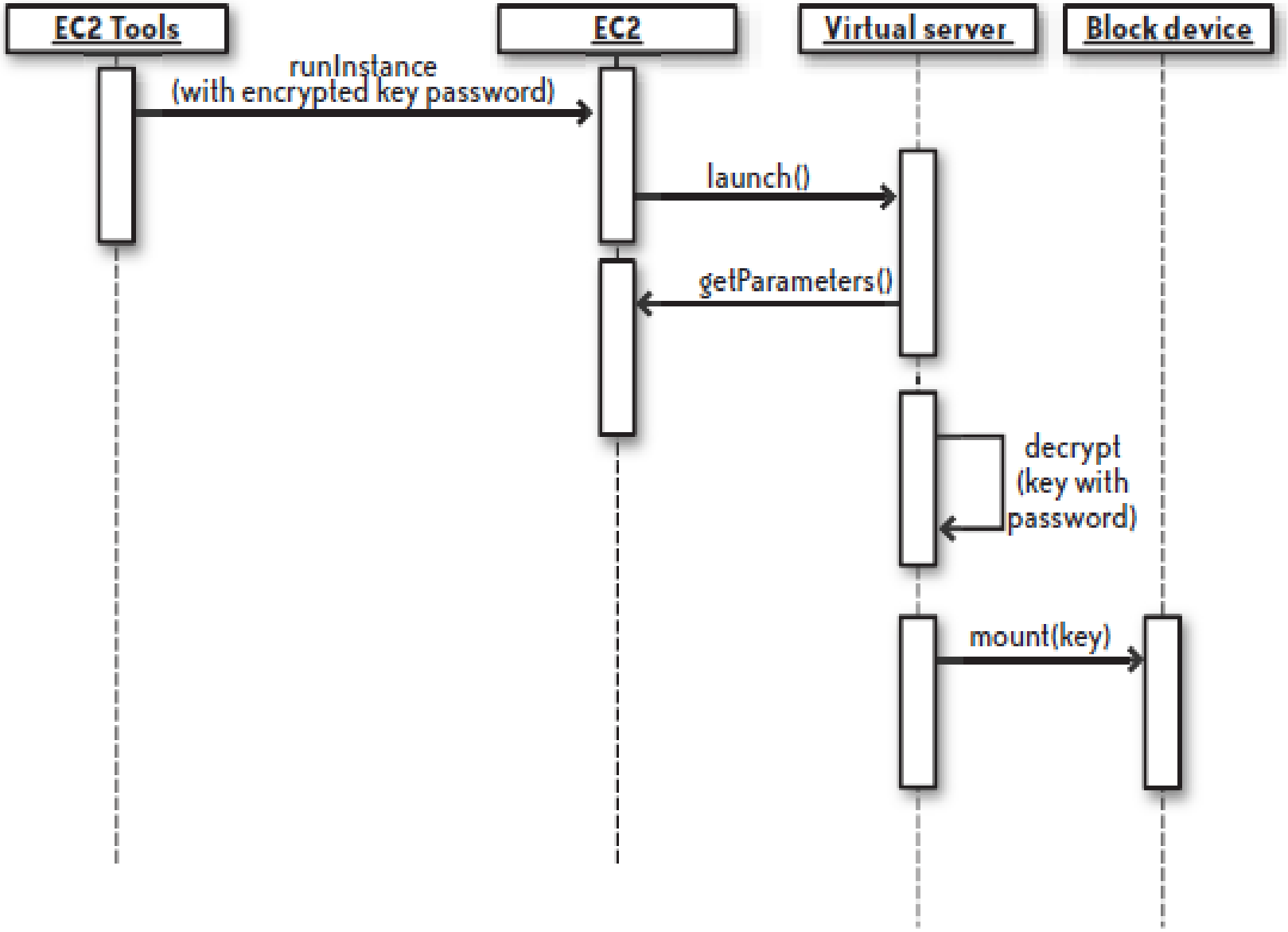


Fig : The process of starting a virtual server with encrypted filesystems

6.3 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(earlier) the acceptance of virtualization technologies

Some regulations

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.

From a security perspective, you'll encounter three kinds of issues in standards and regulations:

1) "**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.

2) "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).

3) “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.

6.4 Network Security

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

- 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.

- No server in EC2 can see the network traffic bound for other servers

6.4.1 Firewall Rules

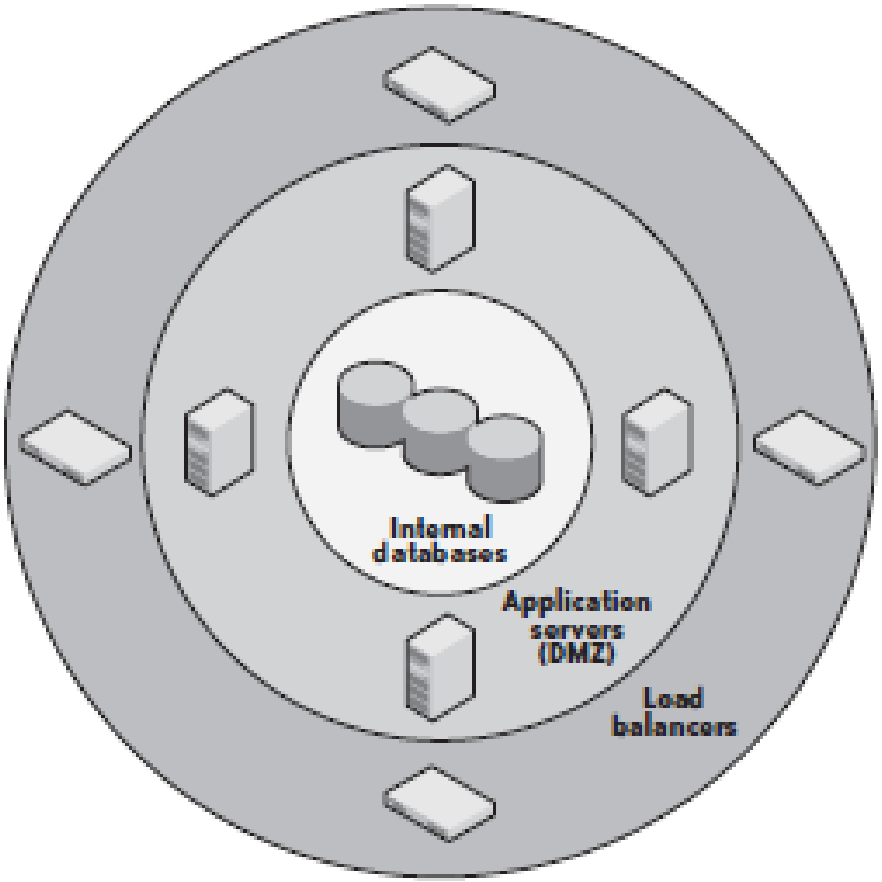
A firewall protects the perimeter of one or more network segments.

Figure illustrates how a firewall protects the perimeter.

--- 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.



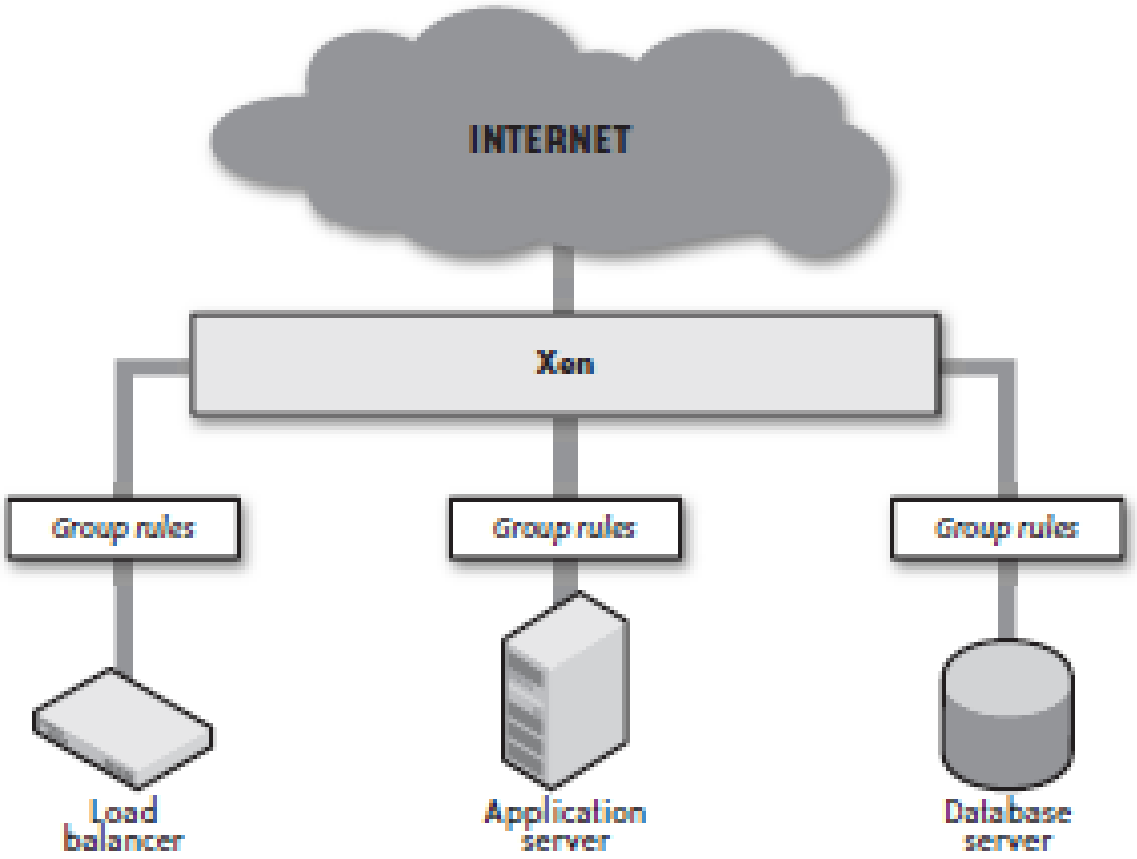
Firewalls are the primary tool in perimeter security

This structure requires you to move through several layers—or perimeters—of network protection in the form of firewalls to gain access to increasingly sensitive data.

Advantage is that a poorly structured firewall rule on the inner perimeter does not accidentally expose the internal network to the Internet unless the DMZ is already compromised.

In addition, outer layer services tend to be more hardened against Internet vulnerabilities, whereas interior services tend to be less Internet-aware.

The **weakness** of this infrastructure is that a compromise of any individual server inside any given segment provides full access to all servers in that network segment.



There are no network segments or perimeters in the cloud

Above 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.

- 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.

Two other 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.

- Recommend the approach of mimicking traditional perimeter security because it is a well understood approach to managing network traffic and it works.

A few best practices for your network security include:

Run only one network service on each virtual server

Every network service on a system presents an attack vector. When you stick multiple services on a server, you create multiple attack vectors for accessing the data on that server

Do not open up direct access to your most sensitive data

If getting access to your customer database requires compromising a load balancer, an application server, and a database server, an attacker needs to exploit three different attack vectors before he can get to that data.

Open only the ports absolutely necessary to support a server's service and nothing more

Server should be hardened so it is running only the one service you intend to run on it. But sometimes you inadvertently end up with services running that you did not intend.

By blocking access to everything except your intended service, you prevent these kinds of exploits.

Limit access to your services to clients who need to access them

Your load balancers naturally need to open the web ports 80 and 443 to all traffic. Those two protocols and that particular server, however, are the only situations that require open access.

Even if you are not doing load balancing, use a reverse proxy

A reverse proxy is a web server such as Apache that proxies traffic from a client to a server.

6.4.2 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

Exploit attempts are malicious actions by attackers to take advantage of these weaknesses to gain unauthorized access, manipulate data, or cause other types of harm.
Ex: SQL Injection (SQLi)
Exploiting a SQL injection vulnerability on a website to retrieve user passwords.

You perform network intrusion detection either by routing all traffic through a system that analyzes it.

Denial-of-Service attack

A Denial-of-Service (DoS) attack is when someone tries to make a website or online service unavailable by overloading it with too many requests. This flood of requests overwhelms the system, making it slow or completely unresponsive, so real users can't access it. When the attack comes from many devices at once, it's called a Distributed Denial-of-Service (DDoS) attack. The purpose is often to disrupt the service or cause trouble for the business or users.

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.
- 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.
- One place in which an additional network intrusion detection system is useful is its ability to detect malicious payloads coming into your network.
- When the NIDS sees traffic that contains malicious payload, it can either block the traffic or send out an alert that enables you to react.
- Even if the payload is delivered and compromises a server, you should be able to respond quickly and contain the damage.

Implementing network intrusion detection in the cloud

- Run the NIDS on your load balancer or on each server in your infrastructure.

- 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.

- Because the only software running on the load balancer is the NIDS software and Apache, it maintains a very low attack profile.

- Compromising the NIDS server requires a vulnerability in the NIDS software or Apache—assuming the rest of the system is properly hardened and no actual services are listening to any other ports open to the Web as a whole.

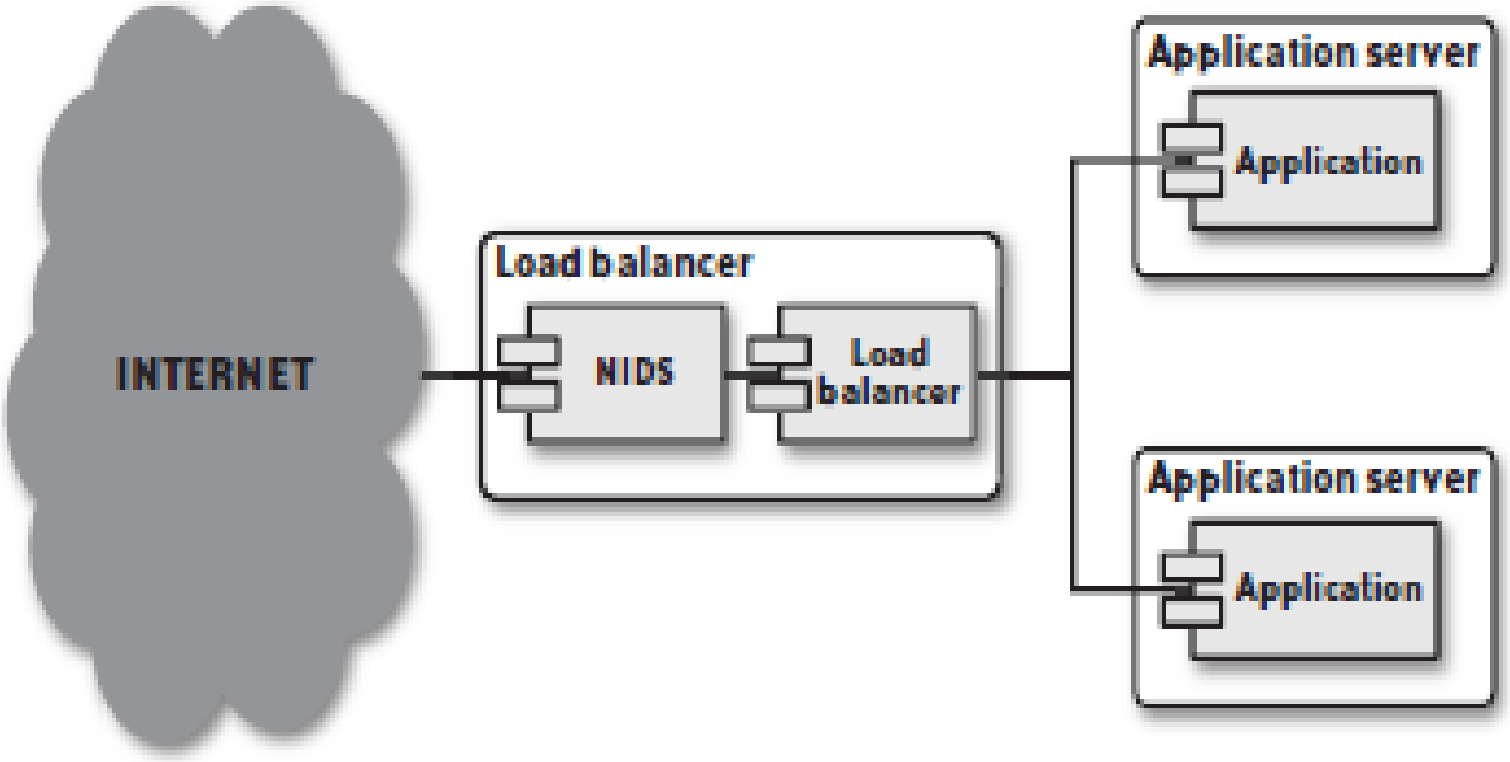


FIGURE : A network intrusion detection system listening on a load balancer

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.

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.

6.5 Host Security

Host security describes how your server is set up for the following tasks:

1. Preventing attacks.
2. Minimizing the impact of a successful attack on the overall system
3. Responding to attacks when they occur.

Each service you run on a host presents a distinct attack vector into the host. The more attack vectors, the more likely an attacker will find one with a security exploit. You must therefore minimize the different kinds of software running on a server.

The tool for preventing attackers from exploiting a vulnerability is the rapid rollout of security patches. In a traditional data center, rolling out security patches across an entire infrastructure is time-consuming and risky.

. In the cloud, rolling out a patch across the infrastructure takes three simple steps:

1. Patch your AMI with the new security fixes.
2. Test the results.
3. Relaunch your virtual servers

Infrastructure management tools such as enStratus or RightScale can automatically roll out the security fixes and minimize human involvement, downtime, and the potential for human-error-induced downtime.

System Hardening

- Prevention begins when you set up your machine image.
- 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.

Hardened system meets the following criteria:

1. No network services are running except those necessary to support the server's function.
2. 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.
3. All configuration files for common server software are configured to the most secure settings.
4. All necessary services run under a nonprivileged role user account (e.g., run MySQL as the mysql user, not root).
5. When possible, run services in a restricted filesystem.

Before bundling your machine image, you should remove all interactive user accounts and passwords stored in configuration files.

Antivirus Protection

Some regulations and standards require the implementation of an antivirus (AV) system on your servers.

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.

When choosing AV first should understand what your requirements are.

If you are required to implement AV, you should definitely do it. Look for two critical features in your AV software:

1. How wide is the protection it provides?

2. 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?

Once you have selected an AV vendor and implemented it on your servers, you absolutely must keep your signatures up to date.

Host Intrusion Detection

A Host Intrusion Detection System (HIDS) such as OSSEC (Open source HIDS) monitors the state of your server or anything unusual.

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 has two configuration profiles:

1. Standalone, in which each server scans itself and sends you alerts.

2. Centralized, in which you create a centralized HIDS server to which each of the other servers sends reports.

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.

Figure illustrates a cloud network using centralized HIDS.

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 requires CPU power to operate, and thus can eat up resources on your server.

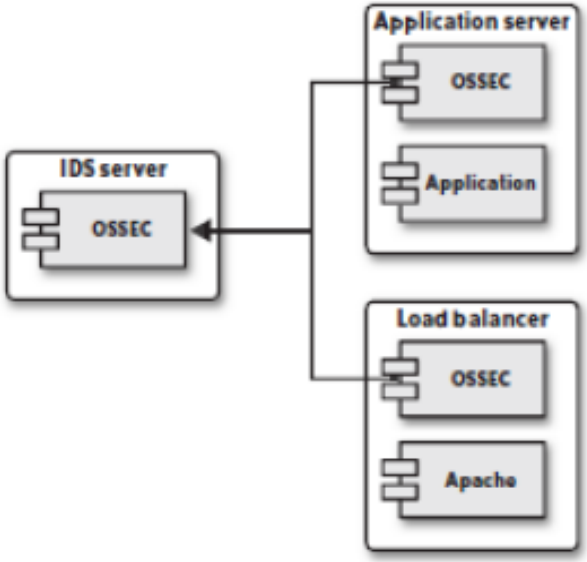


FIGURE : A HIDS infrastructure reporting to a centralized server

By going with a centralized deployment model, however, you can push a lot of that processing onto a specialized intrusion detection server.

Data Segmentation

The best infrastructure, however, 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

Making this assumption provides you with a system that has the following advantages:

1. Access to your most sensitive data requires a full system breach.
2. The compromise of the entire system requires multiple attack vectors with potentially different skill sets.
3. The downtime associated with the compromise of an individual node is negligible or nonexistent.

The segmentation of data based on differing levels of sensitivity is your first tool in minimizing the impact of a successful attack.

Example for data segmentation is 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.

Credential Management

OSSEC profile should have no user accounts, it 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.

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.

It is perfectly secure to embed public SSH keys in a machine image, and it is lot easier to 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.

The simple approach is 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.

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, however, requires an administrative service running on each host and thus represents an extra attack vector against your server.

6.6 Compromise Response

When you detect a compromise on a physical server, the standard operating procedure is a painful, manual process:

1. Remove intruder access to the system, typically by cutting the server off from the rest of the network.

2. Identify the attack vector.

3. Wipe the server clean and start over. This step includes patching the original Vulnerability and rebuilding the system from the most recent uncompromised backup.

4. Launch the server back into service and repeat the process for any server that has the same attack vector.

This process is very labor intensive and can take a long time.

In the cloud, the response is much simpler.

First simply copy the root file system over to one of your block volumes, snapshot your block volumes, shut the server down, and bring up a replacement.

Once the replacement is up, you can bring up a server in a dedicated security group that mounts the compromised volumes.

Because this server has a different root file system and no services running on it, it is not compromised.

You nevertheless have full access to the underlying compromised data, so you can identify the attack vector.

With the attack vector identified, you can apply patches to the machine images.

Once the machine images are patched, simply re launch all your instances.

The end result is a quicker response to a vulnerability with little (if any) downtime.