Building a Cloud

Table of Contents

Notices

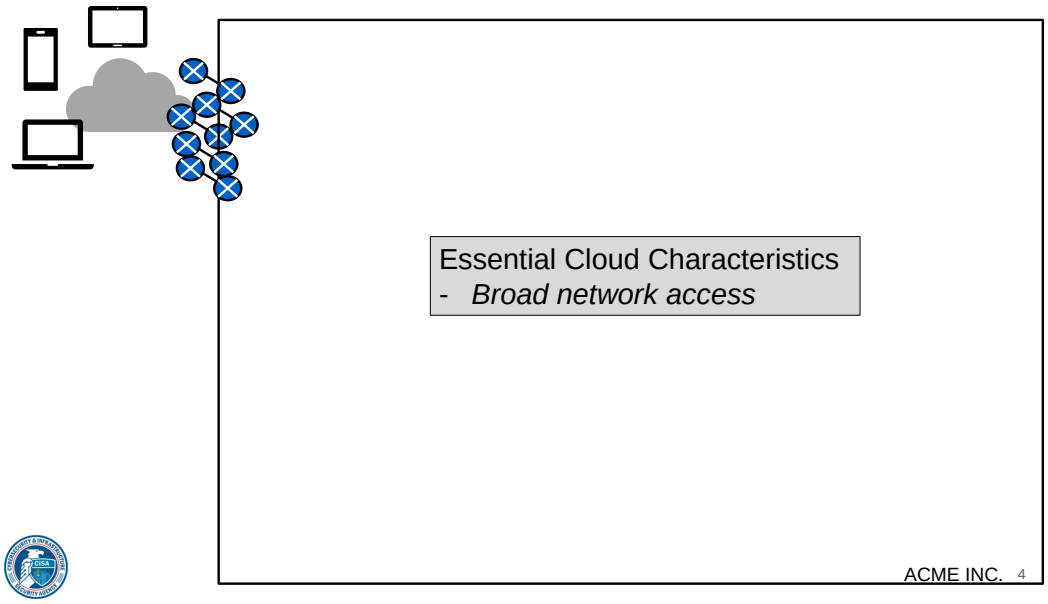
119

**001 Instructor: Do you want to build a cloud?

Building a Cloud

**002 Let's look at an example

Essential Cloud Characteristics Broad network access



**004 company and how they would traditionally set up some basic services.

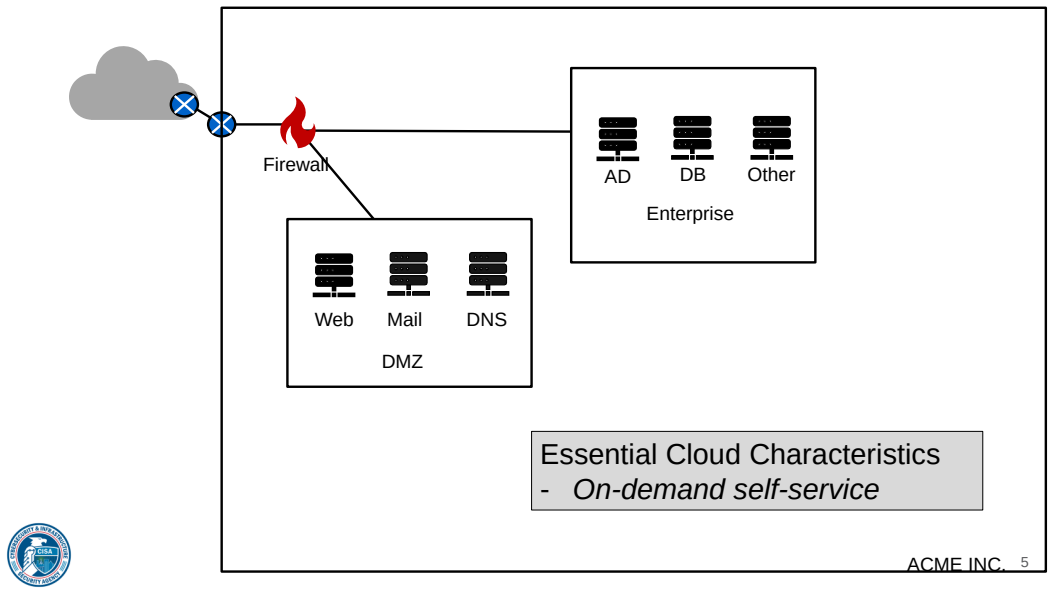
First of all, you will need to get connected to your internet service provider's network. Typically this includes a network router in your facility, which is referred to as CPE, or customer-provided equipment, or customer premise equipment. Your organization will most likely be required to configure, monitor, and manage this device.

With the ubiquity of high-speed internet, broad network access is pretty much assured whether you are using a traditional on-premise solution or whether leveraging a cloud service provider. However, with a CSP, you do not need to manage this last hop into your environment and you get the added

benefit of redundancy and availability already built into their platform.

One of the essential characteristics of cloud computing is broad network access. This goes beyond just ubiquitous broadband internet, to mean that these cloud-based resources must be reachable by a variety of devices such as computers, tablets, and mobile devices over a network. Typically this network is the internet.

Essential Cloud Characteristics On-demand self-service

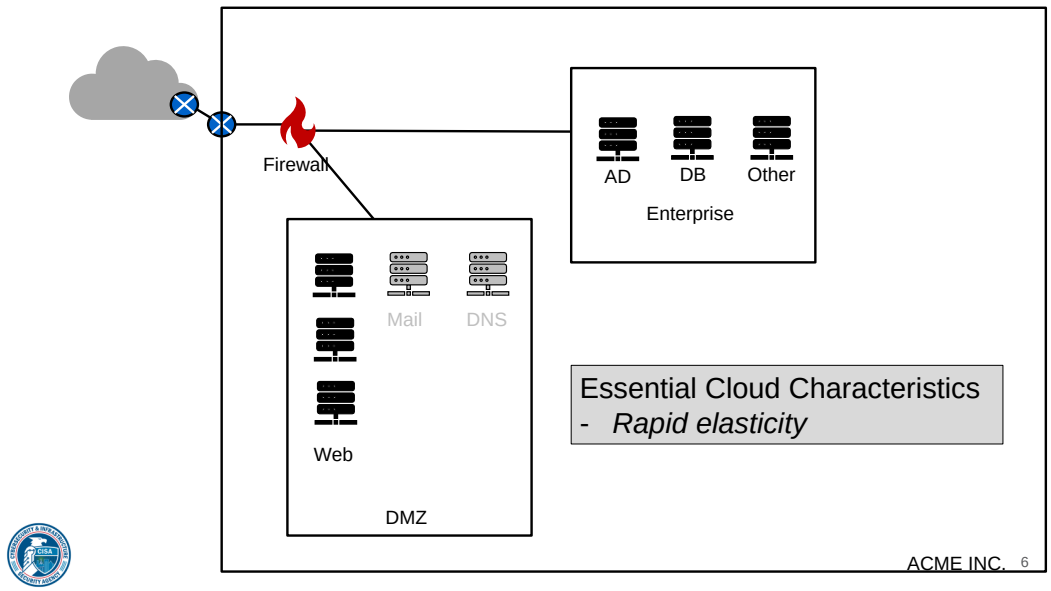


**005 For our example, let's show a simplified connection. As we continue building our network, we will need a firewall from which we can configure access control lists, activity monitoring, logging, and other controls. Next we build out our demilitarized zone or DMZ, which may include typical internet-facing web, mail, and DNS services.

Add on a separate network segment for some enterprise services like Active Directory, databases, and perhaps some other applications to support finance, marketing, etcetera.

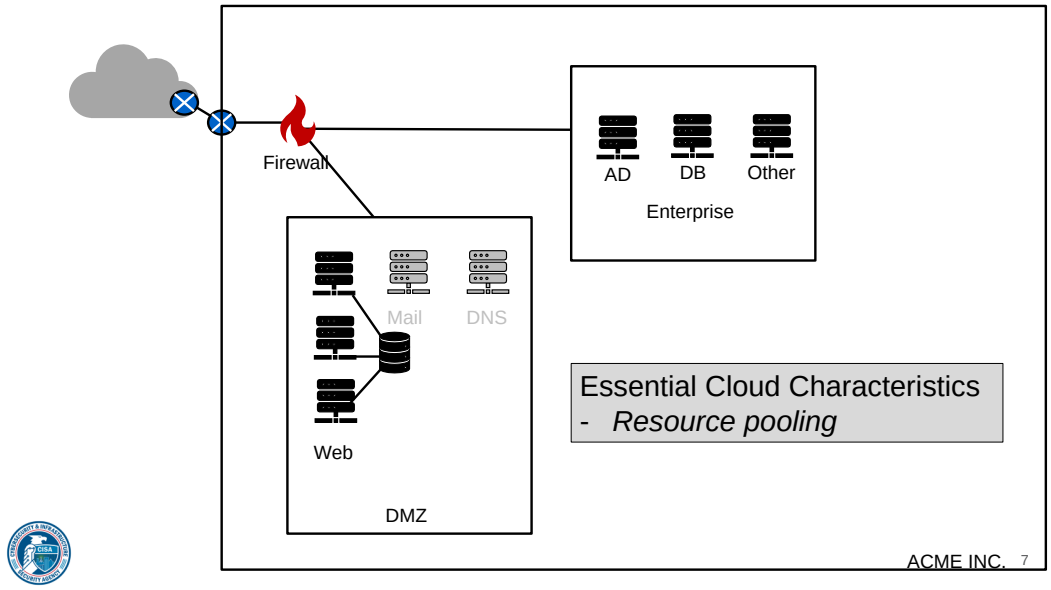
The ability to initiate all of these builds easily, on-demand, and, in some cases, in a completely automated fashion aligns with another key tenet of cloud computing, that of on-demand self-service.

Essential Cloud Characteristics Rapid elasticity



**006 But what happens when we need to scale up our infrastructure to meet higher demands? In our example here, we need to add more web servers to fulfill this need. The ability to add these additional services quickly, easily and automatically is another characteristic of cloud computing.

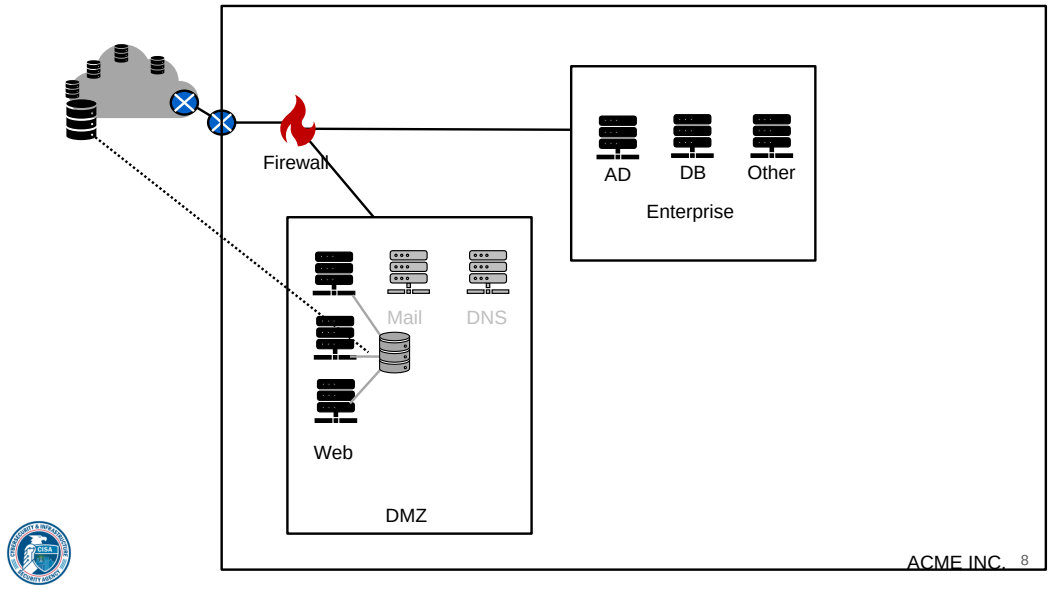
Essential Cloud Characteristics Resource pooling



**007 This pool of web application servers presents a new challenge, the first of which is content synchronization. We need to create shared storage for these files and perhaps for log collection. The cloud service providers make creation of this type of service pretty easy but managing data replication, application access, and user access to these shared drives needs to be well planned and executed.

The ability to share an underlying pool of compute, storage, and network resources to facilitate this expansion is yet another one of the key aspects of cloud computing.

ACME INC.

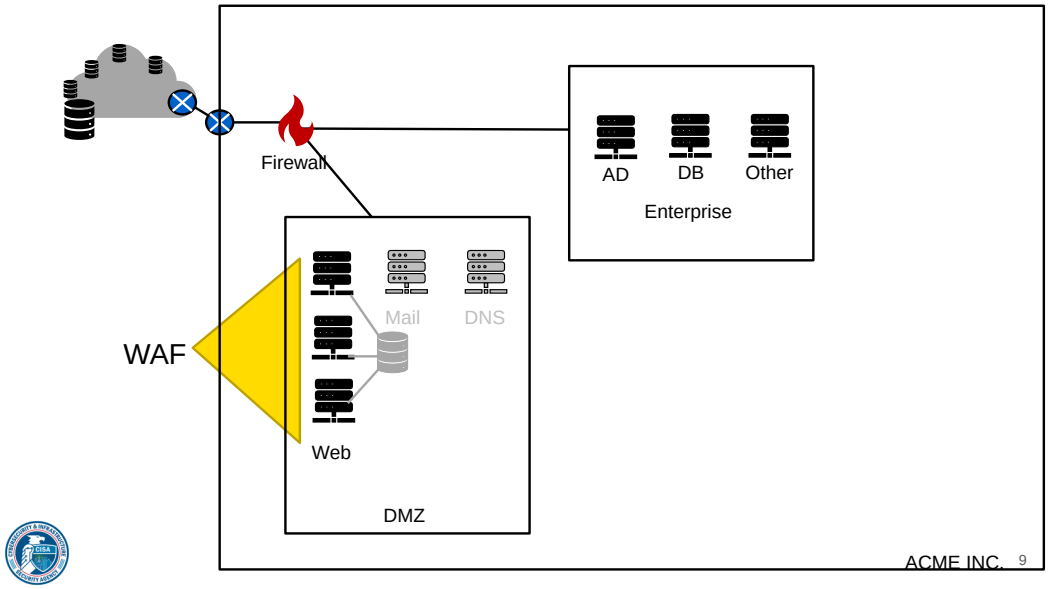


**008 Even with high-speed internet access to the cloud provider's network, you may still want to leverage a content delivery network, or CDN. Akamai and Amazon's CloudFront are two examples of this. These services replicate and distribute your files across the internet to get them as close to the client as possible. This can dramatically improve the performance of web applications by reducing the download time for large images and media files. Note, however, that it is vital for you to work closely with your CDM provider to implement any required security configurations. This could include things like encrypted storage, URL obfuscation, or token- and time-based access.

The bottom line is that you'll want to limit access to only those people that

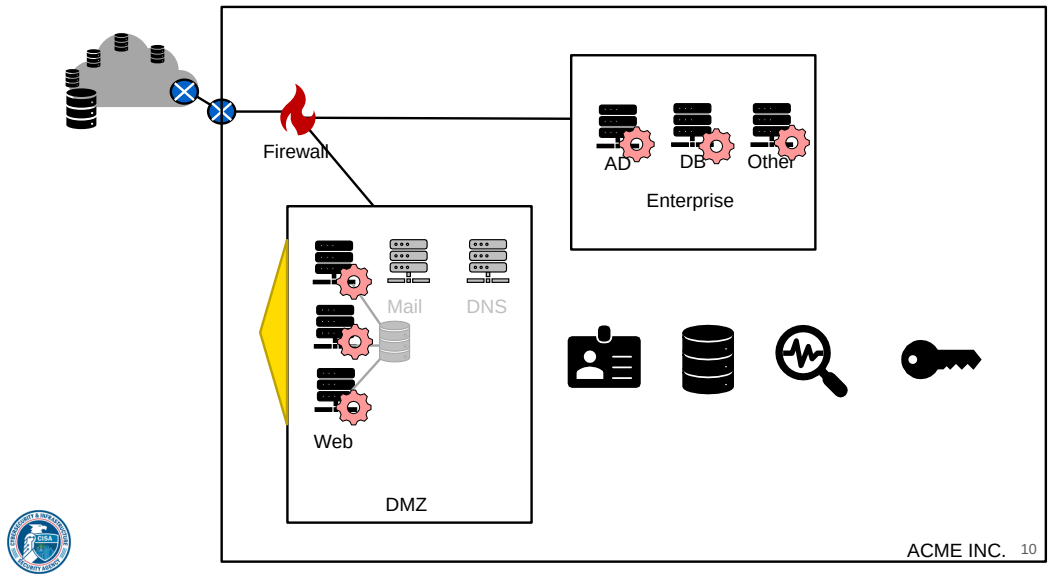
need it and when they need it; and depending on the data being replicated across that network, it may require specific controls. CDNs were some of the first, quote-unquote, "cloud" services.

ACME INC.



**009 Another consideration is a web application firewall, or WAF. Traditionally this would be a plugin for a web server like Apache or Internet Information Server. A WAF lets you monitor HTTP and HTTPS requests and can prevent certain types of attacks from occurring. Cloud providers have partnered with traditional security vendors to offer integrated solutions, but many include WAFs within their base offerings.

ACME INC.



**010 In our traditional environment, we have several other considerations, the first of which is identity and authentication management, or IM. There are often separate enterprise, local operating system, and application accounts to manage. A good cybersecurity architecture also includes a central log collection, aggregation, and analysis mechanism, commonly referred to as Security Information and Event Management, or SIEM.

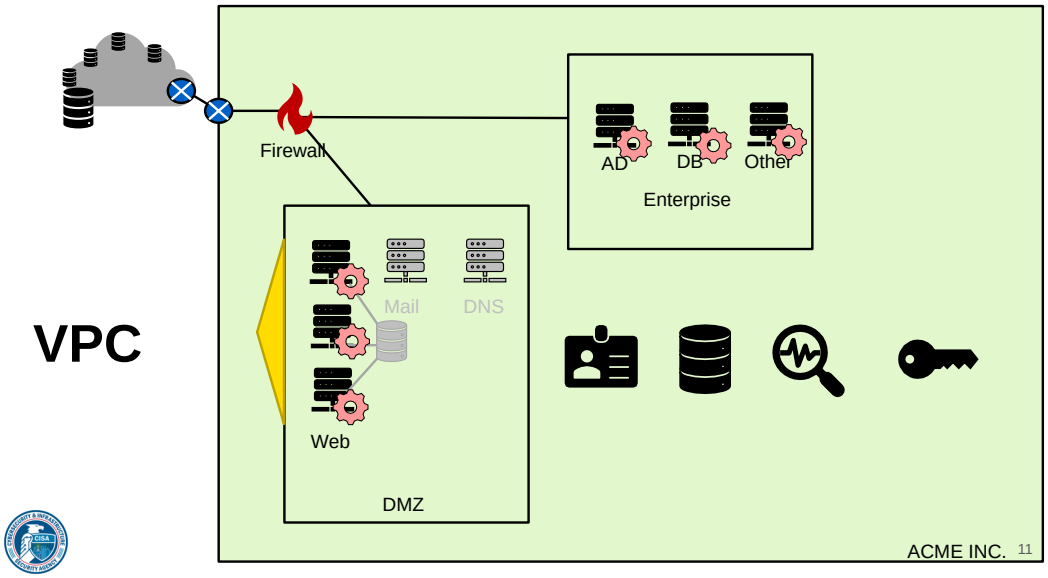
Enterprise architecture must also be monitored for compliance and threats, and these should provide reliable alerts on which actions can be taken.

One of the most challenging things to manage is enterprise encryption, not just certificates for web-based applications, but encryption of data

at rest, on disks, and databases. Not only can cloud service providers help with encryption and key management, but there are numerous inherent capabilities for logging, monitoring, access management, and alerting.

Furthermore, various agents can be deployed to virtual machines and services within a cloud that can perform more advanced functions, including vulnerability assessments and patch management. Deployment methods and capabilities may vary between each provider, but in general the cloud can indeed provide all of the capabilities of traditional on-premise enterprises.

VPC



**011 When you put all this together you end up with your own virtual private cloud, or VPC. Note that cloud service providers may

define VPC slightly different from one another-- in particular, what services can be included within their VPC, how many networks, number of VPN connections into the VPC, and other characteristics.

A virtual private cloud exists within a public cloud, such as Azure, Amazon AWS, or Google Cloud Platform. Keep in mind that deployment methods and capabilities will vary slightly between each provider, but in general the cloud can provide almost all of the capabilities of a traditional IT architecture.