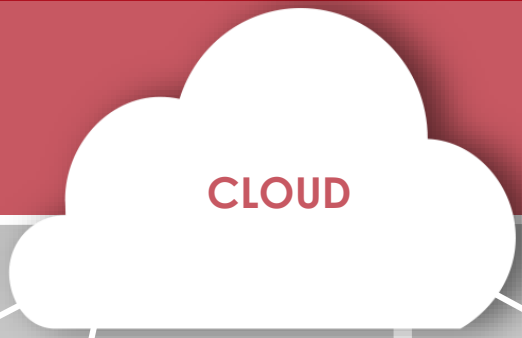
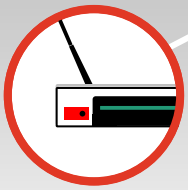
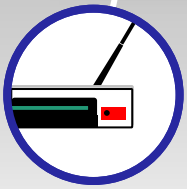
INTERNET SECURITY APPLIANCE

ACE Technology Group





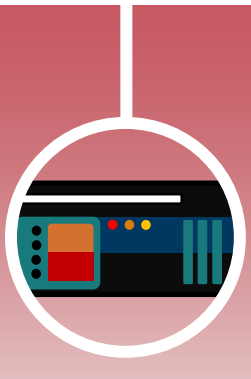
Primary Internet Service Provider



Failover Internet Service Provider (Optional)

ISP Load Balancing— it's beneficial to split the internet traffic over two or more connections in the case that one fails. As a result, the internet uptime and performance is improved which increases the reliability of connectivity.

Virtual Private Network (VPN) - creates a secure connection over the internet by encrypting data to be transmitted privately through a public network.



Internet Security Appliance

A **firewall** is a network security system that actively serves as a physical layer to monitor and block unwanted incoming and outgoing network traffic from external sources, such as the internet. This is typically the first line of defense for a network, which is based on a specific set of security rules.

Cybersecurity appliances often times need enhancements for complex compliancy needs and will utilize **Unified Threat Management**, which is a single installation security feature that allows for multiple security functions working with the firewall.

Features include:

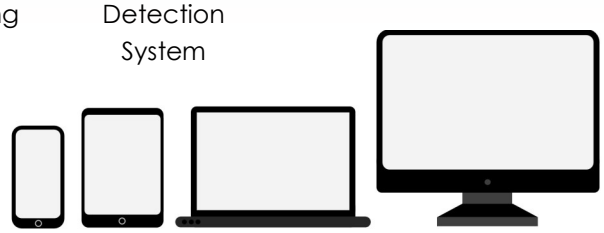
Gateway Anti-Virus & Anti-Spyware

Application Layer Filtering

Intrusion Prevention & Detection System

Content Filtering

Reporting



END POINTS

WHY IS THIS IMPORTANT?

An Internet Security Appliance is important because it acts as an automated defender of an internal network. These devices protect from outside threats, and in most cases, without ever noticing that the network has been attacked. It can also prevent trusted users from downloading an infection, and stopping infections that have infiltrated from spreading through the entire network.

An Internet Security Appliance ultimately frees up time for companies to focus on core business objectives, rather than constantly being on the defense and reacting to threats as they are discovered.