KEMP | LOAD BALANCERS

Securing Internet Facing Applications

Technical White Paper

Ten years ago protecting the corporate network meant deploying traditional firewalls and intrusion detection solutions at the perimeter of the "trusted network" in order to protect internal applications and data from the dangers of the "untrusted network" or Internet. Even then, these strategies were not very effective at protecting networks from rogue or careless internal users. In the 21st century, however, just about every organization has published applications to the Internet for remote access. These applications are used by remote road warriors, contractors, partners, telecommuters, weekend workers, and customers bearing any number of mobile devices. The result: Perimeter security has long since become obsolete as a complete security solution.

As organizations permit customers, partners, contractors and others to access internal applications, they open up their network to malware, data breaches and a variety of other security hazards. The recent parade of damaging, widely publicized breaches of supposedly secure retailers, banks, government agencies and even defense contractors demonstrates the dangers every organization faces. That's why today, securing the network can only be accomplished with a multilayered, defense-in depth strategy that secures not just the network gateway, but endpoints, servers, network devices, applications and data. Here are security components every organization should consider deploying to protect its application access:

Gateway Security

While it's no longer a complete solution, any network security strategy starts at the network edge with the perimeter firewall. It's important to understand, however, that traditional firewalls focus on the network layer, rarely providing protection from application level attacks that traverse commonly open and accessed firewall ports. That means they provide little to no defense against common email and Web based malware, denial of service attacks or more current Web application attacks such as cross site scripting or SQL injection.

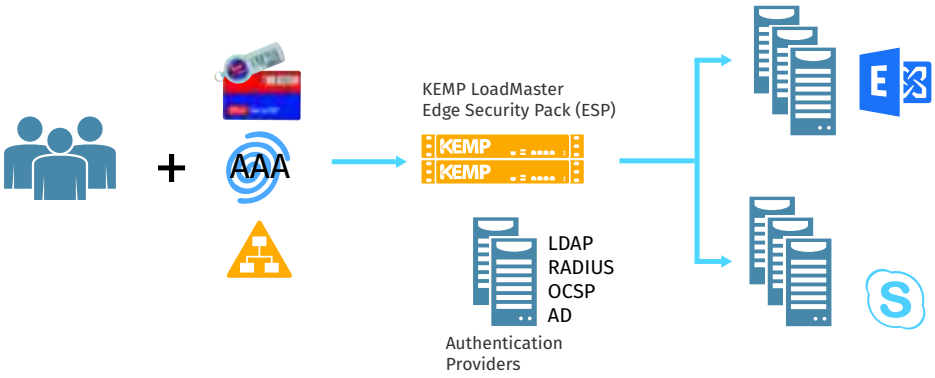
Nevertheless, certain measures should be taken to ensure firewalls are used to their maximum potential. Many organizations fall victim to a condition known as *configuration drift*, in which IT members open up ports or make small, supposedly temporary firewall configuration changes to accommodate any number of users and applications—changes that open their network to attacks and often end up permanent. To protect their networks, organizations should seek out firewalls that

include checks for protecting against policy drift, whether in the form of alerts or the capability to check existing configurations against known good configurations, manually or automatically.

Network demilitarized zones (DMZs) are an effective second layer of perimeter defense, providing a separate, less trusted perimeter network between the supposedly trusted and untrusted networks for Internet facing application components such as externally facing Web, email and DNS servers. Traditionally IT configures firewall protection at both ends of the DMZ--between the external Internet and the DMZ, and the DMZ and the internal network--so that externally facing Web servers have restricted access to internal application and/or database servers and any users attempting to breach the internal network through externally facing applications must get through two levels of perimeter firewall protection.

Identity Management

With so many different types of users accessing internal applications through multiple devices, identity has become the new perimeter. Identity Management tools have become essential to permit access to applications and data only to authorized persons.



Today, any organization publishing applications to local and remote users must ensure it can positively identify and authenticate each and every user and user device attempting to access a published application. Then it must ensure that the user has the assigned rights to access whatever application and data he or she is seeking.

There was a time when user names and passwords were a viable means of identifying a person or device but users have been notoriously careless about creating strong passwords and changing them at appropriate intervals and hackers now have a variety of tools to hack even strong passwords. According to research from Verizon, 76 percent of network hacks take advantage of poor credentials and 48 percent of data breaches are the cause of stolen passwords.

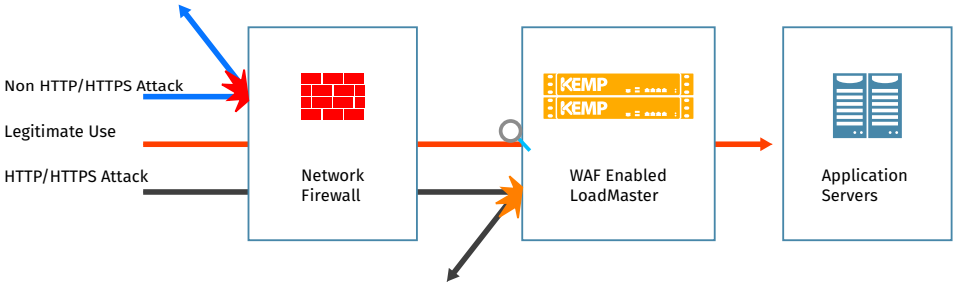
That's why any security strategy must include the enforcement of frequent password resets and strong passwords with complex combinations of letters, numbers and symbols, with no two accounts sharing the same password. In response to the increasing sophistication of password hacks, however, many organizations have moved to *multi-factor* or *two-factor* authentication.

Mutifactor authentication verifies not only something the user knows, such as a username and password, but something the user either *possesses*--such as a smart card, RSA token, smart phone, or email account—or a physical *attribute* of the user such as a fingerprint, face or iris, using the appropriate scanner. Anyone accessing an online bank account or other secure account today has had the experience of having to check an email or text message sent by the bank with a link or code to input in addition to entering a user name and password. These are perhaps the simplest forms of two-factor authentication and make it considerably more difficult for a hacker to pose as a legitimate user.

Once a user is identified, fine-grained access control must validate each user's rights to a requested service and data. Ideally any remote or mobile authentication and authorization solution should integrate with existing standard directory services such as Active Directory and LDAP, and their group memberships and policies, as well as enterprise authentication solutions as RADIUS, RSA and Microsoft Multifactor Authentication Services.

Web Application Firewalls

Traditional network firewalls are not terribly effective at stopping application level attacks that employ exploits such as cross site scripting, SQL injection, forceful browsing, and cookie poisoning. Unfortunately, today applications are the most targeted exploit for attackers. Any organization seeking PCI-DSS compliance must be able to prove it can deflect these kinds of attacks as well as prevent any sensitive data from ending up in the wrong hands.



Specialized Web Application Firewalls are architected specifically to stop these kinds of attacks and can be updated to block new application level attacks as they are discovered. Web application firewalls can also detect a number of data exfiltration techniques used by hackers attempting to steal sensitive data.

Virtual Private Networks

Any organizations allowing external users to access internal applications and data must ensure that the any sensitive data traversing the Internet to and from these applications cannot be breached, particularly over an insecure connection such as a public WiFi service used in a hotel, airport, or coffee bar.

Typically the best way to protect users of these services is through SSL Virtual Private Network solutions that encrypt all application communications over the wired or wireless connection. Ideally all SSL encrypted connections should terminate as close to the application as possible. While other types of VPN's are available, SSL VPN's have the advantage of integration with most current mobile and PC Web Browsers such as Internet Explorer, Chrome, and Firefox, so they are much easier to deploy and use than other VPN solutions that require the client to use separate VPN software.

Where to Deploy Security Solutions

Identity Management, Web Application Firewalls and SSL VPN termination can be deployed just about anywhere on the network. However, if an organization is publishing internal applications to the Internet, in most cases, the closer to the application these solutions are deployed the better. Deploying them on the servers running applications is one solution, but with a multi-server application deployment the risk is that controls will not be applied in a consistent manner to each server. That is why application delivery controllers, AKA load balancers, are a perfect place to implement security solutions

ADC's provide a highly scalable, high performance, fault tolerant point of access to applications running on multiple servers. Most organizations deploying ADC's have used them as the point of SSL termination as well as it secures all communications, external and internal, right up to the point of application access.

It stands to reason that the ADC is also an ideal place for multifactor authentication and a Web application firewall, as these controls can be applied right at the point of SSL termination, just when the data communication is decrypted, obviating the need to encrypt and decrypt the data in transit several times before reaches the application. Deploying these measures at the ADC rather than each individual server also ensures consistent configurations and policies, combining scalability with security.

The KEMP Solution

For organizations seeking a complete performance and security solution for Internet published applications, Kemp ADC solutions can also be equipped with high performance SSL VPN termination and acceleration, and Kemp's Edge Security Pack (ESP), which provides multifactor authentication and fine-grained authorization. ESP includes Active Directory integration, support for RADIUS authentication and dual factor authentication with RSA SecurID.

Kemp also offers the Web Application Firewall Pack, which brings Web application firewall functions close to the application, addressing damaging application exploits such as SQL injection and cross site scripting. The Web Application Firewall Pack is even capable of processing and securing encrypted Web based traffic flows. By acting as a check on exfiltration of sensitive credit card and other personal information, it helps organizations satisfy PCI-DSS compliance requirements.

Kemp ADC's also provide a second level of traditional network firewall protection, controlling access to public services and the ports and protocols used for that access as well as network whitelisting and blacklisting.

Organizations can no longer rely on traditional perimeter firewall and intrusion detection to protect their Internet published applications. To protect their networks from today's applications hazards, they must apply a raft of security solutions to their end points, servers, applications and data. One of the best ways to protect applications is to apply multiple security measures as close to the application as possible. Application delivery controllers are ideal for such a strategy and Kemp ADC solutions provide a host of tools for ensuring Internet published applications are not only fast, but secure.

With over 26,000 worldwide deployments and offices in America, Europe, Asia and South America, KEMP Technologies is the industry leader in advanced Layer 2 – 7 Application Delivery Controllers (ADC) and application-centric load balancing. Named one of the fastest growing technology companies in North America by Deloitte with a 499.1% growth rate, KEMP is changing the way modern enterprises and service providers are building cloud-enabled application delivery infrastructure. Over the past decade, KEMP has been a consistent leader in innovation with a number of industry firsts, including high performance ADC appliance virtualization, application-centric SDN and NFV integration, innovative pricing and licensing models and true platform ubiquity that can scale to support enterprises of every size and workload requirement.