www.spkaa.com
Ph: 888-310-4540

SPK and Associates
900 E Hamilton Ave, Ste.100
Campbell, CA 95008

Managing Infrastructure for a Corporate Web Service

Andrew McLeod, Systems Integration Architect, SPK and Associates

This document will describe a basic setup of hardware and networks necessary to support running a Web service for corporate use. This is not required for the average household website. Equipment required is:

- Firewall – preferably one with Intrusion Detection Systems (IDS) built into it. I prefer the Juniper SSG line. They are robust but affordable firewalls. Consumer grade may give you a quick start if budget is a concern. However, these don't typically have a DMZ network or as much flexibility of configuration.

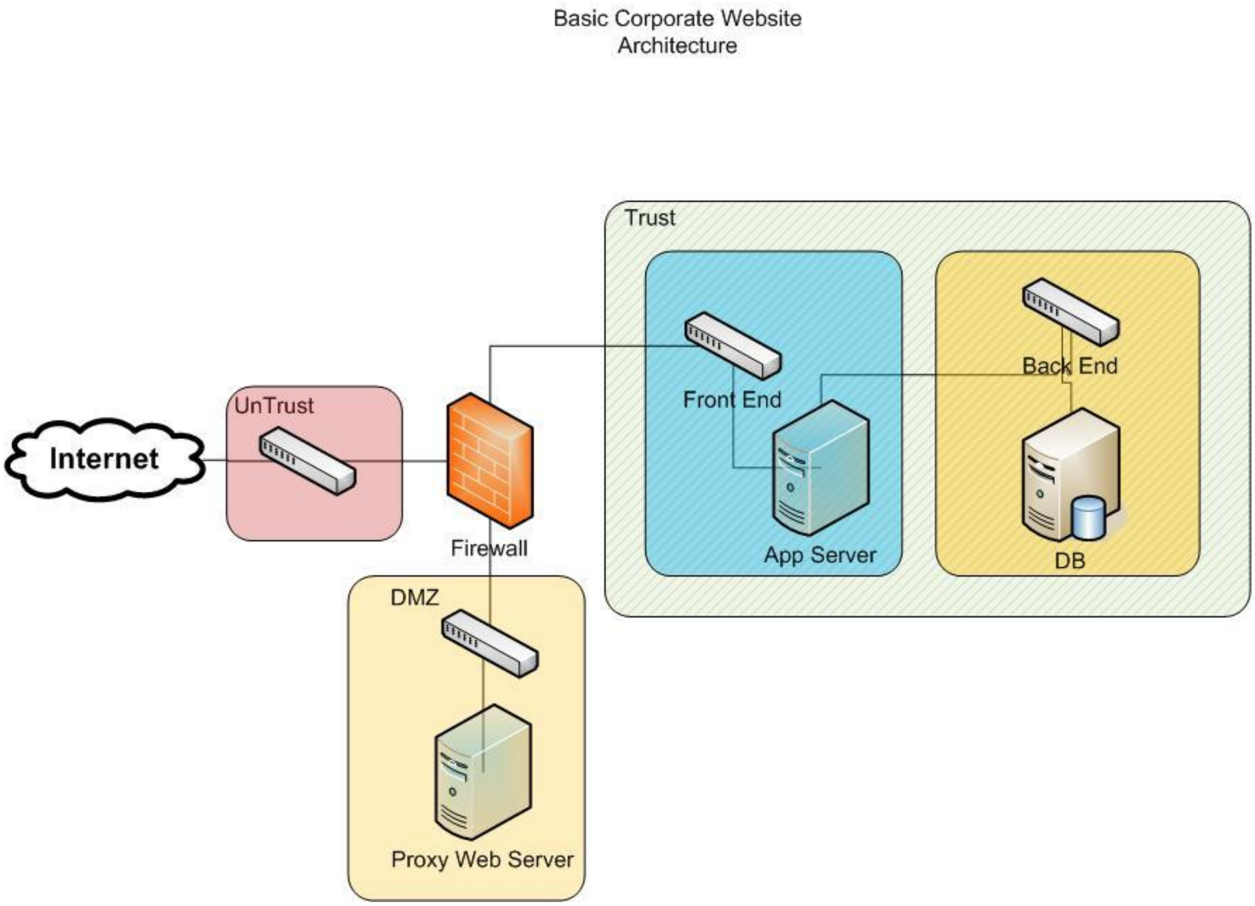
- Switches – dedicated switches for Untrust, and DMZ. Front end and Backend can be combined or two separate switches depending on security demands. Consumer grade switches like Linksys or D-Link are OK for smaller websites. For larger, Cisco, HP, and Juniper are better suited.

- Proxy Web server. This is typically a scaled down web server. I prefer Apache on RHEL to keep it simple and secure. I like cheaper low performance 1U boxes such as the SuperMicro chassis sold by ASA computer.

- Application Web server. This can be simply Apache or IIS …or there are many content management solutions that offer additional features including: Wikis, Oracle Content Management, WebSphere, etc. I prefer HP DL300 series for heavier application servers. They have more processing power and a robust ILO for remote management.

- Database server – I prefer MySQL on a RHEL box. HP DL500 series are used for larger memory footprints and bays for disks.

Below is the typical setup.



There are 3 “zones” that are setup on the basic website: Untrust, DMZ, and Trust. On the Trust side, there may be an additional “Backend” network where secure data travels between application server and DB. Untrust is where there’s no security. Anyone from the internet can connect into anything attached to Untrust on any port. DMZ is the demilitarized zone. Here, limited access is available from the internet based on specific ports. Trust is even more limited to the outside world and is where application data is stored and served through a web server application. The item protecting each zone from each other is the Firewall.

The idea is to limit how someone on the internet can connect into the servers where information is stored. In the above setup, it is impossible to directly connect into the application server or database (DB) server from the internet. This provides some security of the underlying data from attack.

Proxy servers are Web servers that proxy traffic. Their sole use is to ensure only specific ports are open to the application servers. The proxy checks the domain name, sees if it’s one that we have information to serve, and then forwards the request to the application server. If it’s not a domain we serve, the request is dropped or transferred to a login portal that goes no-where.

When installing all this equipment, it’s imperative to update versions to latest levels. Most hardware and software comes in a down-revved version from the factory. Regular patching is the single most effective way to ensure that the site remains secure.

After you have the website setup, it’s important to verify it’s secure. There’s 3rd party applications that do much of the work for you. My two favorites are: Nessus:

http://www.nessus.org/nessus/intro.php and Qualys: http://www.qualys.com/. You point them at the machine and they will try all known security attacks and generate reports to tell you next steps to mitigate any issues.