Securing e-Commerce Web Sites.

Introduction

Securing web sites, and web servers in particular, has been the focus of many security articles and conferences over the past few years. Obviously, a web site's security level is heavily influenced by the security means, which are used by, and on, the web server. It seems obvious that the key to a secure web site is the level of security achieved from security of the web server. One might have "stumbled" over a web site's database security issues if he or she was interested in DBA chores. Database security is also a well-known subject in web site security, but it is mostly documented as a standalone issue.

Building a web site is a task that involves more then one OS and more then one kind of software. Therefore, the security of the web site is achieved from the synergy of all the factors and not from the web server alone.

When I set out to write this paper, little did I know that public information regarding the "fortification" of complex web sites will be hard to come by. Only few sites publicize the internal workings of their systems, and fewer the security make-up and configuration. All this said, the question I will be trying to answer in this paper is, "How do I put all these ingredients together in order to build a secure e-Commerce web site?"

Assumptions

When building a web site we must survey the risks facing the web site from all different aspects. Not all web sites face the same "threats"; many web sites are just another collection of HTML pages in the vast cyberspace of the Internet. But, web sites conducting business, containing information (considered valuable for a malicious hacker) or holding a political view, are at higher risk then others. E-commerce web sites often hold valuable information (credit card numbers or other private, personal data) and conduct business, and are thus placed at a high-risk position.

Having recognized a web site is in the high-risk zone, we must consider the different types of security hazards:

- Denial of Service (including distributed).
- Defacement (the replacement of content on a web site, indicating it has been hacked).
- Data Theft.
- Fraud (data manipulation or actual theft).

While any of these attacks might cause revenue lose, the method of defense against each is different. Since there is no global security solution that can provide the full defensive spectrum an e-commerce web site requires, it has become extremely difficult to choose the right line of defense.

Security is a product that comes with a price tag. At first, this might be very obvious since products such as firewall and anti-virus have known pricing. However, the costs of on-going security, software-security updates, new web-site technologies etc, cannot be calculated during initial installation planning. Eventually the web site owner will have to decide what level of security will be provided, while considering the current risks and costs involved.

Known Web Configuration

There is no single way to install a web site that will hold all the security answers. The different ways to install and configure the different web and network components varies greatly as web sites become more complex.
A few known configurations that address the security issues are:

Configuration 1 – Basic Disjointed

A straightforward configuration, which includes the web server as a multi-homed server with one interface connected to the world and a second interface dedicated for database communications. All communications to and from the web site are maintained by the firewall while internal communications are not monitored or filtered.

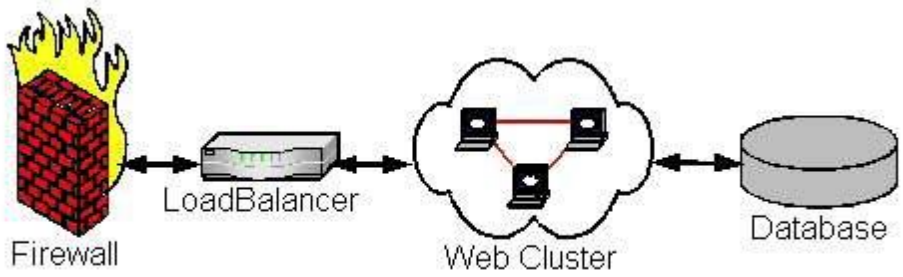


Figure 1 – Basic Disjointed

Pros:

1. Simplicity and streamlining of communications.
2. Easy troubleshooting on all levels.

3. Scalability (when no n-tier[4] architecture is needed).
4. Low cost implementation and minimum hardware.

Cons:

1. Management of the DB server requires an out-of-band[5] communication method or web server routing.
2. Web content is distributed manually or via local scripts and applications.

Security considerations:

1. This basic configuration provides network level security (via the firewall) and DB protection (via disjointed networks).
2. The load balancer (if external hardware is used) can be used as the second level network-filtering device for extra security.
3. The use of two network cards provides low-level protection against poorly configured firewall devices (for example, fire-walking will not reveal the DB server).

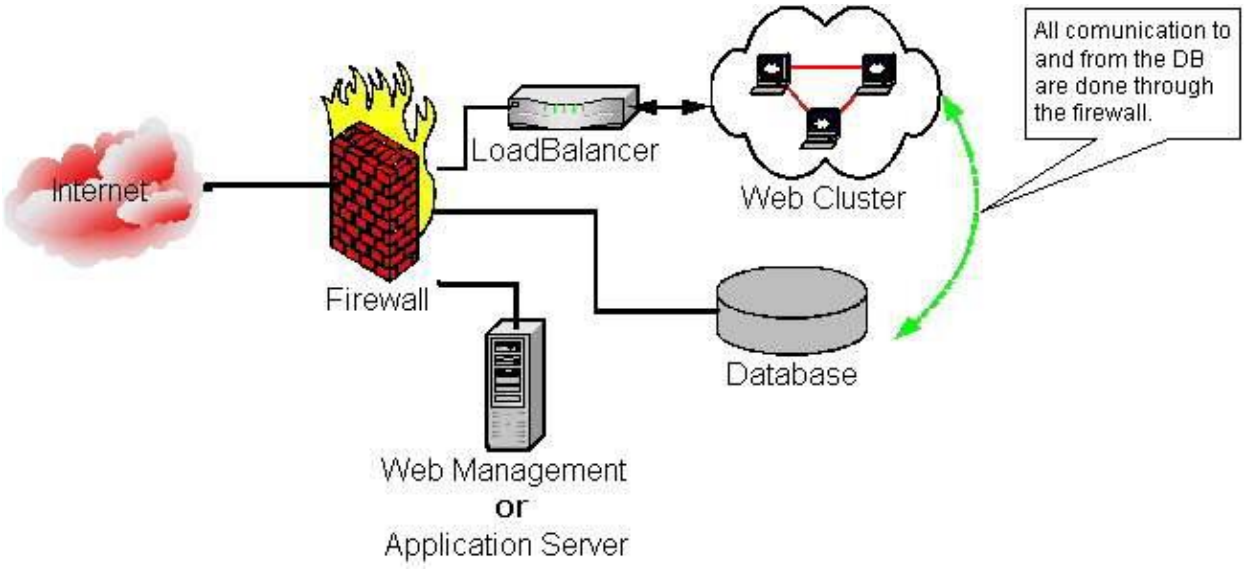
Configuration 2 – Filtered Disjointed (figure 2)

In this configuration, the addition of the filtering firewall, via the second “DMZ” on the main firewall provides an added level of security[8]. Any hacking on the web servers will provide only minimal access to the database servers. Obviously the web servers can access the database server with an appropriate ODBC connector or similar means. This

configuration could potentially provide a hacker (should he be able to “own” the web server machine) limited direct data access capabilities.

Application business logic for the web site is based on a separate server to allow for easier scalability. This server may also be used for web management. Software such as MS Site Server or MS Application Server provides the content distribution, web statistics etc.

Figure 2 – Filtered Disjointed



Pros:
1. Relatively easy installation and routing configuration.
2. Easy troubleshooting for connectivity and system level events.
3. Minimal hardware.

Cons:
1. Development environment must be similar to the production web site, to allow developers to adjust application connectivity with internal servers to the filtering device used.
2. The use of one firewall as a filtering device might show a degradation in the site’s performance. Should the use of extra firewalls be applied, cost and ease of installation will no longer be an advantage for this configuration.

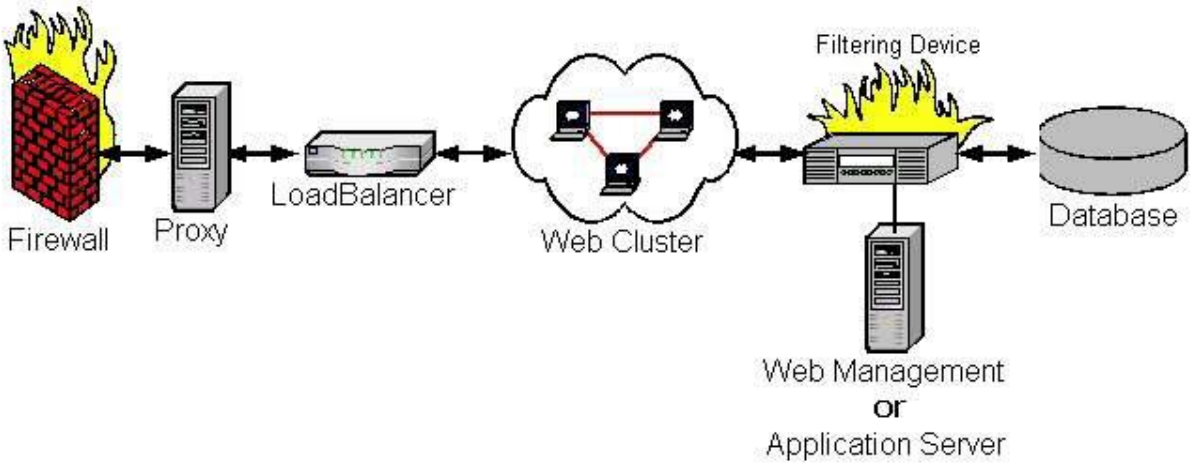
Security considerations:
1. This configuration provides network level security (via the firewall) and DB protection (via disjointed networks). It also provides low-level application protection since core data processing is shifted from the front-end web servers to back office application servers that have no direct communications with the site’s users.
2. If MS SQL is used, TCP 1433 should be used instead of named pipes. This will provide a higher level of filtering.
3. When implementing the web content distribution mechanism it is recommended

not to use windows shares. FTP or MS Site Server replications are preferred.

Configuration 3 – Application Protection (figure 3)
In the effort to protect the web site from application level hacking, we need to use a "higher level" filter. The filter would be used to examine the HTTP protocol, and if possible the HTTP GET, HEAD, POST, and PUT commands and parameters.

This approach apposes the Microsoft e-commerce strategy shown earlier in configuration 1, and in the e-commerce web site security, that all application level security should be driven from the DNA design and proper code writing.

Figure 3 – Application Protection



Pros:
1. High level of assurance that Internet traffic enters the various applications in the correct form and manner.
2. The use of proxy servers could improve performance, if the proxies implement a caching mechanism.

Cons:
1. Extremely hard to troubleshoot and configure.
2. High cost of hardware and initial installation.
3. The use of filter devises at the application level could cause functionality issues. This is due to the fact that the connection terminates at the proxy level and connection stickiness, session information and other client information might be misinterpreted before they reach the web servers.
4. It is imperative that the development of the development of the application is done with full awareness to the system configuration. Not all existing web sites can use this configuration with no application adjustments.

Security considerations:
1. This configuration provides a high level of security, both network and application level.
2. Application filtering might require the use of out-of-band management tools, since not all proxy servers can act as routers for other non-HTTP protocols