SearchSecurity.com
Security School

Life at the edge: Securing the network perimeter

By Michael Cobb

The Internet is an unbounded network environment. It has no central administrative control and no unified security policy. Despite best efforts, no amount of hardening can guarantee that a system connected to an unbounded network is invulnerable to attack. A Web server is publicly available on the Internet, so a network infrastructure must play a role in protecting the Web site and other IT assets. Airtight security is not possible, so don't get caught in the trap of trying to achieve it. You must aim to establish a balance of adequate security with cost effectiveness and common sense. Security is about ensuring that systems can deliver essential services and maintain essential properties such as integrity, confidentiality and performance despite the presence of intrusions; in other words, reliability in the face of adversity.

To be able to deliver essential services, a "reliable" system must demonstrate four key properties:

1. Resistance to attacks
2. Recognition of attacks and the extent of any damage
3. Recovery of full and essential services after attack
4. Adjustment to reduce effectiveness of future attacks

I cover properties 2-4 in Web Security School webcasts 2 and 3. (SearchSecurity.com/WebSecuritySchool) Here, we'll take a look at strategies for resisting attacks.

An overview of Web security architectures

When planning Web-based services you must fully understand what needs to be protected. Thus, the process to ensure survivability is an organizational one, rather than purely an IT one. Once your organization has defined its minimum levels of acceptable service and security for each service, the task of planning the Web security architecture can begin. Never use a totally "flat" network design, one where all devices connect directly to each other, as you must avoid hackers gaining access to your Web server and finding that your entire network is wide open.

The network layout should ensure that the failure of one level of protection does not result in a succession of compromises. Practice defense-in-depth and utilize multiple security devices including firewalls, border routers with packet filtering and intrusion-detection systems (IDSes). Further protect Web service resources with a segmented network topology, which reduces the scope of any compromise and buys time to respond to it. This is achieved by dividing the system into trust domains bounded by trust boundaries, with resources placed in the appropriate domain. This outermost barrier in your Web site defense is a secure network perimeter or demilitarized zone (DMZ).

Divide and conquer – DMZs

A network DMZ separates and isolates a trusted network from an untrusted network by creating screened subnets. By dividing the system into segments and creating DMZs where only intermediate levels of trust exist, the system has a much greater resistance to successive compromise, thereby protecting the key resources even if other components fail. DMZs work because network traffic cannot travel between two network subnets without being routed.

Your Web servers, FTP servers, mail servers and external DNS servers should be placed in this DMZ, or "perimeter network," along with additional network defenses, such as an IDS. By putting these public services in the DMZ, you put them on a different subnet to your internal network. Your internal network is where your back-end systems such as database servers should be located. Any machine placed in the DMZ is still at risk, but if an intruder compromises the DMZ, he does not automatically have access to the internal network.

Each access point into the DMZ blocks and filters network traffic to only allow activity to or from certain network addresses, over certain ports, to pass through. Great care should be taken so that interactions with the DMZ do not expose the internal network. The barriers between each segment are controlled and screened by firewalls and routers, and protected by access control lists, strong authentication and encryption. For the ultimate in DMZ security, place each service on its own DMZ segment, configuring firewall policies to meet the needs of each server.

Network layouts

There are two DMZ network layouts we'll look at. The first, called a triple-homed perimeter network, is suitable for low-budget Web sites that do not connect to a critical internal network. The second is a back-to-back perimeter network, which is required for e-commerce and other mission-critical Web sites.

Triple-homed perimeter network

This topology uses a single firewall to separate the Internet, the perimeter network and the corporate intranet. It is also known as a single-screened subnet because the DMZ is bounded by only a single firewall with three network cards: one connected to the Internet, one to the DMZ and one to the corporate intranet (see figure 1 below). The disadvantage of this network layout is that there is a single point of failure. When ports are opened through a perimeter guarded by a single firewall, the perimeter security is unavoidably weakened. If an intruder compromises the firewall in this topology, he has access to both the server in the DMZ and the corporate intranet.

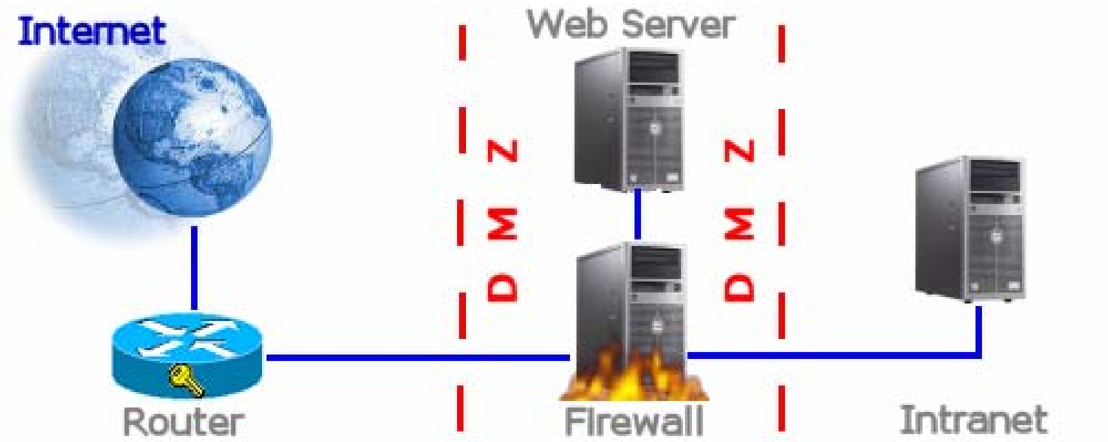

Figure 1: Triple-homed perimeter network. Note that this topology specifies the use of a secured router between the Internet and the DMZ. Ports on this router should be locked down. Examples of ports that you would typically need open to ensure correct Web server functionality would be port 80 for HTTP and port 443 for HTTPS.

Back-to-back perimeter network

The back-to-back perimeter network topology shown in figure 2 is widely regarded as one of the most secure. The perimeter network is separated from the Internet on one side and from the internal network on the other side by using two firewalls. Each firewall has two network adapters. The external firewall has one network adapter connected to the Internet and the other connected to the perimeter network, while the internal firewall has one network adapter connected to the perimeter network and the other connected to the internal network (see figure 2 below). This provides an added layer of protection. If an intruder from the Internet compromises the perimeter network, he does not automatically gain access to resources in the internal network, as there is another barrier between the intruder and the rest of the network.

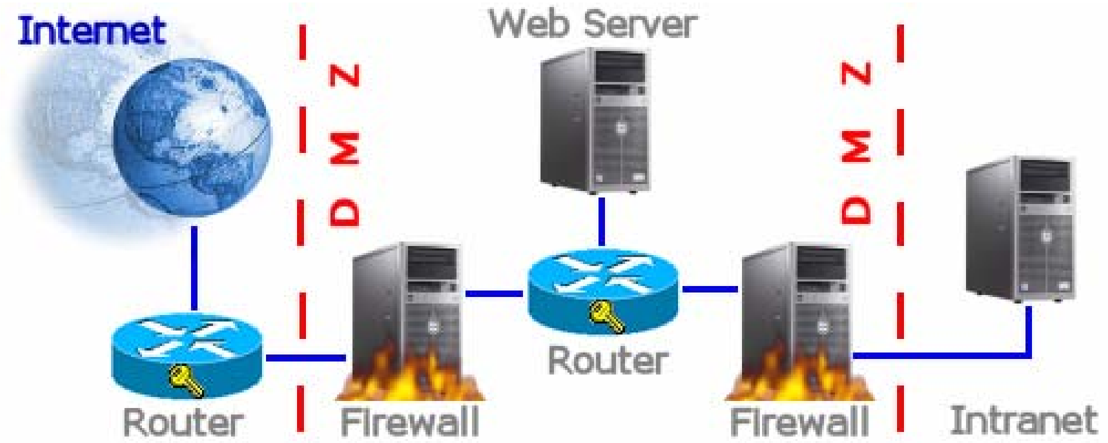

Figure 2: A dual screened subnet or back-to-back perimeter network using two firewalls. Note that there is another secured router separating the network segments that compose the perimeter network. Although locking down this router is not as important as locking down the router connected to the Internet, ensuring that non-essential ports are closed can give additional security.

The outside firewall protects against external attacks and manages all Internet access to the DMZ. The inside firewall manages DMZ access to the internal network. This firewall should have different rules than the firewall facing the Internet, allowing only inbound application-specific service calls to reach specified systems and preventing unsolicited inbound port 80 Web traffic into the internal network. In other words, the firewall should only pass inbound traffic from a server in the DMZ that needs to communicate with one of the internal systems. For example, if a Web server communicates with a database via SQL, open TCP ports in the firewall to pass the SQL queries and responses, and block everything else. Security is further enhanced when different makes of firewalls are used on each side of the DMZ. A hacker is less likely to be able to use the same exploit to defeat both systems.

When segmenting a network for security purposes, always choose physical segmentation. A virtual LAN (VLAN) is a network segment that is logically defined and controlled by a switch that can assign its ports to two or more VLAN segments rather than have all its ports belong to the same physical segment. Although this reduces the cost of purchasing multiple switches, the segmentation is virtual. It can be removed and the security the switch provides can be easily bypassed.

Resistance to failure

Security has to be understood and implemented at the architecture, protocol and application levels in order to provide successive protection. Only by understanding all these elements will you be able to build and maintain a system that can resist attack. Bear in mind when designing your network architecture that its survivability is as much protocol-based as topology-based. Particular attention has to be given to any traffic that crosses a trust boundary.

Once you build the network perimeter, you must test it to demonstrate that routing, packet filtering, and logging and alert capabilities all perform as expected. An excellent document covering firewall testing is available from the CERT Security Improvement Modules at CERT.org.

Using encryption

An unencrypted link between your Web site and a browser is essentially an open one. This is not a problem -- if nothing on your site is confidential. But, if you wish to make proprietary information available or take online orders, then you need to protect data as it travels between server and browser. Encryption can be used to provide extra layers of defense for such data, as well as protect it as it crosses trust boundaries. Encryption can be used to support user authentication, data stored in files or communications across a network. For example, Windows NTFS file encryption can be used to augment a server's access control for highly sensitive documents. However, when file encryption is used with a Web site, it's generally done to encrypt specific elements of data for application-specific purposes, such as protecting credit card numbers in a customer database. The most common and practical use for encryption on a Web site is to encrypt sensitive information with SSL/TLS as it is being sent to a browser over a network. The SSL and TLS protocols provide very strong encryption.

SSL, digital certificates and public-key infrastructure

SSL encryption is accomplished by a symmetric cipher after one-time session keys are securely exchanged via public-key encryption. The public-key encryption is RSA, and the default symmetric cipher is RC-4. In addition, all data sent over encrypted connections is protected with a mechanism that detects tampering by determining whether the data has been altered in transit. SSL can be combined with digital certificates to authenticate a Web site. A digital certificate is a digital document that vouches for the identity of an individual or a computer system. The set of products and processes required in order to securely issue, maintain and manage digital certificates is called a public-key infrastructure (PKI). One of the components of PKI is a certificate authority (CA), which operates a certificate server and issues certificates. A CA is responsible for verifying the identity and key ownership of an individual or organization before issuing the certificate.

If you operate an e-commerce Web site or allow users to access confidential information via a Web site, you must use a digital certificate and the SSL/TLS protocol to encrypt communications. A browser authenticates a digital certificate installed on a Web site by comparing the certificate's signature to the public key of the CA's root certificate that is installed on the browser. Thus, the browser verifies that the site belongs to the organization it claims to represent. You can purchase a certificate from a commercial CA such as Verisign, or you can choose to act as your own certificate authority using a product such as Microsoft Certificate Server.

Your server's digital certificate allows users to authenticate your server, but what if you need to authenticate those coming to your site? Internet Information Server (IIS) lets you choose how to handle certificates presented by visitors. You can use client certificates for authentication and prevent users who do not have a valid certificate from accessing the secure content of your site. You can also map client certificates to Windows user accounts on your Web server. If you enable this mapping, then each time a user logs on with a client certificate, your Web server automatically associates that user with the appropriate Windows user account. Using this feature, you can automatically authenticate users who log on with client certificates, without requiring the use of Basic, Messaging Digest or Integrated Windows authentication.

Using IIS secure communications

To configure IIS to handle encrypted sessions you need to:

- Create a public-key pair in IIS to submit to a CA when you request a certificate
- Request a server certificate from the CA
- Install the certificate
- Configure the directories and pages that you want to secure

Request a certificate from a commercial CA via their Web site. Once your certificate is installed, complete the rest of the SSL/TLS configuration. In order to do this properly, think through your site's organization. Most Web sites, even when they use encryption, also have a non-encrypted section, as it's very costly to encrypt every Web page. Most organizations place marketing material, contact information and anything else that they want the public to have easy access to in separate, unencrypted directories. Create a separate directory – or for very sensitive transactions a different site -- for content that is for confidential access, and encrypt only that information.

IIS directory encryption works differently than Windows 2000/2003 directory encryption. In Windows Explorer the information is encrypted on disk. However, it is not practical to use on a high-volume Web site, because encrypting all the site’s data would bog down even the most powerful server. In contrast, SSL/TLS encrypts information as it is being sent over the network to a browser client. To ensure that your site is safe, you should not use less than 128-bit encryption.

How to protect yourself when things go wrong

Survivability depends as much upon the risk management skills of an organization as it does upon the technical expertise of its computer security experts. Any compromise of your Web-based services could have a severe impact on your organization's ability to survive, and the effects will be more important than the causes. Even with a highly protected system you must have contingency and risk-mitigation strategies in place in order to protect the organization in the days after a compromise. Contingency planning requires that your executive management make risk-management decisions and economic tradeoffs, with guidance from relevant departments based on "what-if" analyses of survival scenarios. A review of potential threats and possible countermeasures should be completed, with reference to comparable projects and current best practices. This will help everyone make the right decisions about security as you work towards meeting these challenges. By documenting this work you create a document that performs business, legal and practical functions -- the Standard of Due Care.

Standard of Due Care

The Standard of Due Care (SDC) provides a consistent and agreed upon basis for information security decisions. Survivability and resistance to failure should be designed into your system in the context of this document, as it determines many of the variables in the security approach, reflecting the type of business, the level of threats, the organization's risk tolerance and so on. The organization that has a standard of due care for its system is much better placed to demonstrate the logic behind its security decisions, and thus justify them in the face of criticism or prosecution. It will have a solid defense against any claims that the organization failed to adequately protect the system and the data it handles.

IIS SSL deployment preparation checklist

- Decide upon your trust policy and authentication method for digital certificates.
- Choose a commercial CA or install a self-managed certificate server.
- Create a public-key pair in IIS Internet Services Manager by creating a certificate signing request that will be submitted to a CA when you request a certificate.
- Request a server certificate from your CA by visiting the certificate request URL and filling out the certificate request application.
- Install the certificate on your Web server by following the instructions included in the response you get from the CA.
- Configure the directories and pages that you want to secure by following these steps:
    - Set the Web Site Properties to use port 443 (or another port of your choice) for SSL/TLS.
    - From the Directory Security tab, access the Secure Communications window and configure the settings so that 128-bit SSL is required.
    - Decide whether you want to require client authentication by digital certificates, and make the appropriate selections in the Secure Communications window.