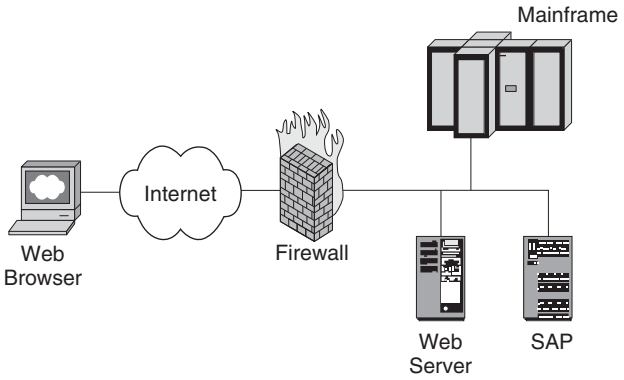
13.4 Demilitarized Zone

Any organization conducting e-commerce or publishing information over Web technologies must make their service easily accessible to their users. However, any form of Web site or e-commerce system is a potential target for attack, especially those on the Internet. A Demilitarized Zone (DMZ) separates the business functionality and information from the Web servers that deliver it, and places the Web servers in a secure area. This reduces the 'surface area' of the system that is open to attack.

Example

A commercial Internet system holds customer profiling information, dealer order information and commercially-sensitive sales information, any of which could be stolen or corrupted by an attacker. This information must be shared with the organization's corporate systems, making them liable to attack as well.

You could use a firewall to control access to your systems from the outside world as shown below.



Firewall protection against outside attacks

The firewall would be configured to allow only inbound traffic to access the Web server. However, this places a large onus on the system administrators to configure the firewall correctly, and on the firewall software to operate correctly. If the firewall fails, an attacker could potentially have direct access to other business resources such as the SAP system or mainframe shown in the diagram. The configuration

of the firewall is further complicated by the fact that for any highly-available Web-based system, multiple servers must be exposed to support either load balancing or failover. If the Web-based system is also high-functionality, additional protocols must be allowed through the firewall. All of this makes a configuration error more likely.

Context

An APPLICATION SERVER ARCHITECTURE [Dys04] has been adopted to deliver an Internet technology application. The business logic and dynamic Web content generation of the application resides on application servers, while all static content is provided by Web servers that also act as a PROTECTION REVERSE PROXY (457) for the dynamic Web content. The application holds information on users and provides important functionality for users, but the application is exposed to an environment that contains potential attackers.

Problem

Internet technology systems, particularly those facing the public Internet, are regularly subject to attacks against their functionality, resources and information. How do we protect our systems from direct attacks?

Solving this problem requires you to resolve the following forces:

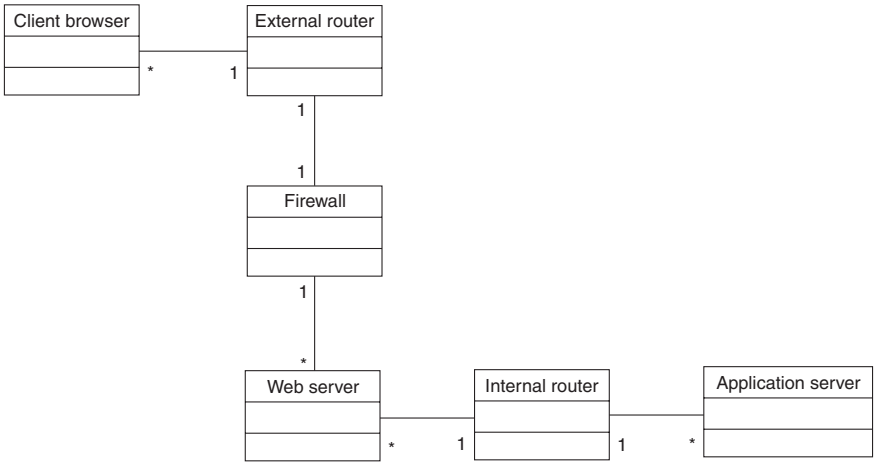
- The cost of an extensive security solution will be high, but the cost of an intrusion may also be high in terms of system damage, theft and loss of customer confidence. If the potential rewards from the attack are high in terms of financial gain or publicity, the risk of such an attack will be higher. The scope, and hence cost, of any countermeasure must be commensurate with the level of perceived threat and the potential cost of the intrusion.
- To prevent attack, we must make intrusion into any part of the system as difficult as possible, especially an organization's internal business systems. However, increasing the level of security will generally make the system more difficult to use, which conflicts with the goal of making the system open and easy for legitimate users.

Solution

Provide a region of the system that is separated from both the external users and the internal data and functionality—commonly known as a demilitarized zone (DMZ). This region will contain the servers, such as Web servers, that expose the functionality of the Web-based application. Restrict access to this region from the outside by limiting network traffic flow to certain physical servers. Use the same techniques to restrict access from servers in the DMZ to the internal systems.

Structure

A DMZ requires the following elements:



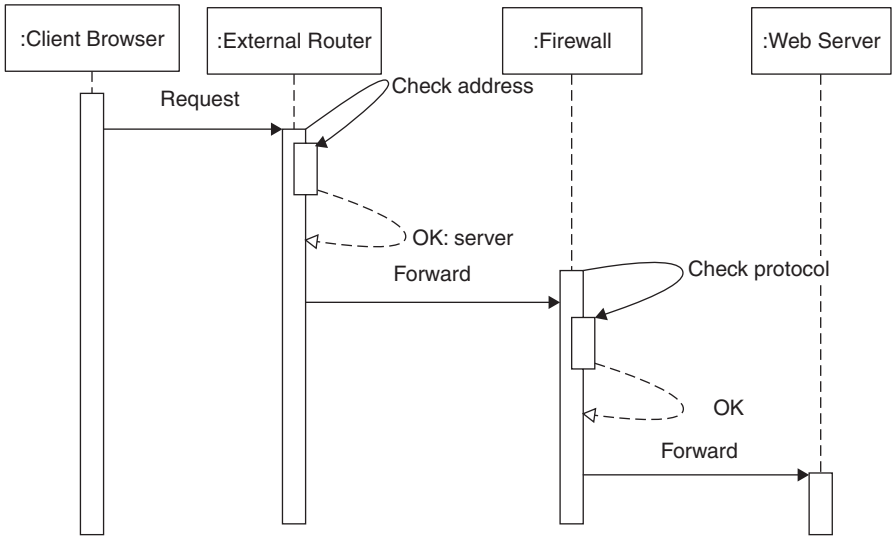
DEMILITARIZED ZONE (DMZ) structure

- External router, a filtering router whose principal responsibility is to ensure that all inbound traffic is directed to the firewall. Its secondary responsibility may be to keep out random traffic generated by attackers.
- Firewall, responsible for receiving inbound requests from the external router and subjecting them to more sophisticated analysis, such as stateful inspection. If a request is judged to be legitimate, it will be forwarded to an appropriate Web server.
- Web servers, providing access to the application's functionality and information. There may be multiple Web servers that are accessed through a load balancer. A Web server will receive a request from the firewall and service that request. A request for a static resource, such as a fixed page of HTML or an image, may be delivered from a cache held on a local disk. A request for a dynamic resource will be proxied through to an application server that is shielded from the outside world in the style of a PROTECTION REVERSE PROXY (457). No application functionality, such as servlets or ASP.NET pages, will run on the Web servers, as this makes them open to direct attack. Although described here as 'Web' servers, these servers may support access through other protocols such as FTP.
- Internal router, a filtering router whose principal responsibility is to ensure that it only passes legitimate traffic from the Web servers through to the internal network.

- Application servers, a platform on which the application's code runs, typically in the form of Web components such as servlets and business components such as EJBs.

Dynamics

The first scenario shows a successful client request for some business functionality. The client browser request is filtered by the external router to ensure that it is destined for a valid server. The request is forwarded to the firewall to undergo more rigorous checking. If the firewall is happy with the protocol use, the request goes onwards to the server requested by the client.

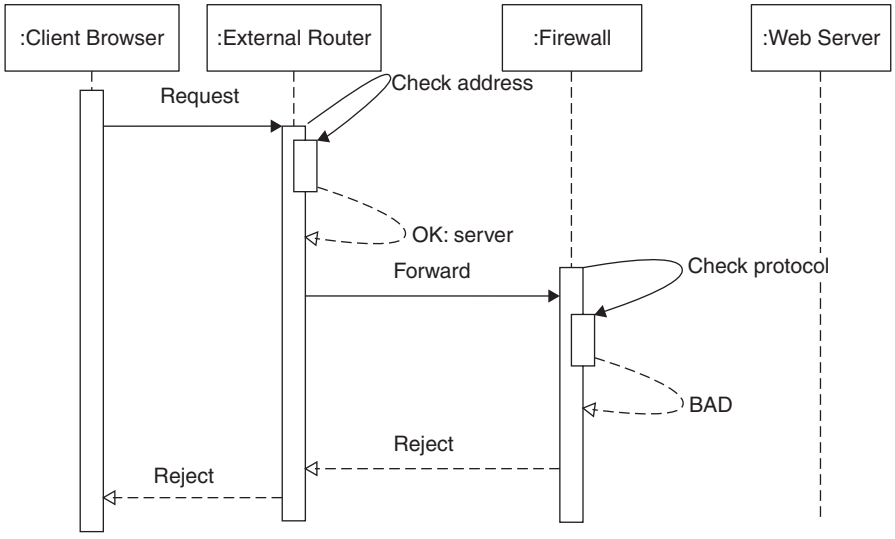


Filtering a client request in a DMZ

The second scenario shows a malicious client call being blocked by the firewall. The client browser request is again filtered by the external router to ensure that it is destined for a valid server. The request is then forwarded to the firewall to undergo more rigorous checking. At this stage, the firewall detects invalid protocol use—maybe some form of protocol-based attack, or an attempt to flood the server. The request is rejected and the suspicious activity is logged. See figure on page 453.

Implementation

Since the request handling and business functionality must be separated by a filter, it is best to use DEDICATED WEB and APPLICATION SERVERS [Dys04] where any



Rejecting a client request in a DMZ

programmatic functionality, whether business or presentation, is deployed on an application server that is physically separate from the Web server. These application servers can be placed on a more protected network than the Web servers. This protected network will have easier (possibly direct) access to the corporate information and services required by the Web-based application.

The external router should be configured to deny any attempted access to any network addresses outside of those known in the DMZ. To increase security, any requests with a destination address that does not match the Web server address (or that of the Web server cluster) may be rejected. The external router may also reject requests based on the port number of the request, for example rejecting any request that is not for port 80. The external router will therefore block direct attacks on the internal router, and possibly the firewall.

The Web servers will be built solely for the purpose of delivering static Web content or proxying requests through to the application servers. These Web servers should be locked down (or 'hardened') by removing unnecessary functionality. Such hardening helps to prevent other, unintended, access to the servers.

The internal router will limit network traffic to connections between the Web servers on the DMZ and specific internal servers, such as the application servers, using a fixed set of protocols. This restriction reduces the risk of attack on other internal systems. The use of an internal router helps to reduce the risk of attack should the external router be breached. Because of this threat, no traffic should be allowed directly from the external router to the internal router.

The whole operation of the routers and the traffic filtering may be controlled from a machine running specific firewall software. This makes it easier to apply consistent rules to the routers and to use statistical analysis to detect potential attacks. The firewall applies more sophisticated traffic filtering rules to detect more complex attacks. Depending on the type of firewall, the network traffic may or may not pass through the firewall itself.

Because the number of servers exposed to the outside world is reduced, it means that fewer parts of the system need a high level of security. In the scenario described, the application servers will not need to be hardened to the same level as the Web servers. To access those servers not directly exposed (and hence less securely configured), any attacker will have to breach several security elements that form part of the DMZ. Hopefully, they will set off various intruder alerts as they do so—if, indeed, they are capable of doing so.

Applying a DMZ to a system is a good way to provide protection for the system. However, you must remember that protecting the platforms on which the system is built is only part of the solution. Since security is a matter of policy as well as technology, all protection mechanisms—such as a DMZ— must be backed up with appropriate procedures and processes to ensure that the level of security remains high—see the patterns in Chapter 6, *Enterprise Security and Risk Management*. If there is a high level of concern about possible attacks on the system, an intrusion detection system (IDS) (see INTRUSION DETECTION REQUIREMENTS (388)) may also be used. An IDS monitors the traffic on the network, or on specific hosts, looking for suspicious activity. If the IDS identifies a pattern of network or host traffic that indicates an attack is underway, it will notify the system administrators. An IDS could be used on the DMZ itself, on the internal network, or both.

Example Resolved

The commercial organization implements a typical DMZ configuration. The system only allows HTTP and FTP traffic into the organization, and even then such traffic is only allowed to the Web servers. The external router drops any traffic that tries to reach the internal router, firewall, or the external router itself. This rogue traffic is also logged at the firewall and notified to the system administrators to assist in the detection of potential intruders.

The internal router allows inbound traffic only from the Web servers, and even then it limits it to specific protocols (IIOP), specific hosts and specific port ranges. This means that any hacker who achieves a beachhead within the DMZ must either attack the internal router directly (and risk setting off alarms from the router) or they must be literate in IIOP to the degree that they could use it to gain access to one of the servers on the other side of the internal router.

The firewall acts as a clearing house for security alerts and as a management console for the DMZ. The organization chose Firewall-1 software based on its track record and traditional association with Sun, on whose hardware it is deployed. The Firewall software gets alerts from the two routers and provides a unified view of security on the DMZ. The firewall software also controls the configuration of the two routers, to avoid inconsistencies creeping in between the three main parts of the firewall system.

Variants

Multi-homed firewall. The number of machines involved in implementing the DMZ will vary according to the level of protection required (based on anticipated risk) and the amount of money available. In the simplest case, the DMZ may be partitioned using a single firewall machine. This machine will have three network cards: one connected to the Internet, one connected to the internal network and one connected to a dedicated LAN containing only the Web servers and any other 'public facing' parts of the system. The firewall software running on the machine will manage the traffic between the three networks to maintain three separate security zones. The benefits of such an 'multi-homed host' implementation include reduced cost and ease of maintenance. However, this system creates a single point of failure, both in terms of security and availability. It also means that any attacker is only one system away from gaining access to the sensitive internal systems.

Firewall as filter. A multi-homed firewall host may be used in place of the external or internal router. This means that all traffic must pass through the firewall (and its filtering rules) to reach the internal network or the DMZ itself.

Stealth firewall. Rather than relaying traffic, the firewall may simply be attached to the demilitarized network and act in 'stealth' mode, simply monitoring traffic for potential intrusion. This can make the firewall itself more difficult for an intruder to detect.

Known Uses

DMZs are extremely common for almost all Internet sites and advice on the creation of DMZ configurations is offered by almost all major network hardware and software vendors, such as:

- Sun `http://www.sun.com/executives/iforce/solutions/SecuritySolnII-Final3.pdf`
- Microsoft `http://www.microsoft.com/windows2000/techinfo/reskit/en-us/default.asp?url=/windows2000/techinfo/reskit/en-us/deploy/dgcf_inc_icku.asp`
- Cisco (variously described as part of their SAFE Blueprint)

Consequences

The following benefits may be expected from applying this pattern:

- Security is improved, because fewer systems are exposed to attack and multiple firewall artefacts must be breached to compromise security.
- The level and depth of protection can be varied to match the anticipated risk and the cost limitations.
- The additional security is transparent to the users of the system functionality and to the developers of such functionality.
- Fewer hosts must be hardened to withstand attack than if they were all exposed to the outside world.

The following potential liabilities may arise from applying this pattern:

- Availability may be impacted, because the firewall becomes a single point of failure. The standard procedure is therefore for a firewall to 'fail closed'—that is, in the event of failure, it will deny all connections to the protected systems.
- Manageability is impacted, because the very restrictions that limit access to internal data may make it difficult to access the application from an internal monitor.
- Cost is increased, because extra elements must be procured to build the DMZ. These include not only the filtering routers, firewall software and firewall host, but also the extra network equipment, such as switches and cabling, used on the DMZ itself.
- Performance is impacted due to the overhead of network traffic filtering. Performance is also impacted as it becomes necessary physically to separate the Web servers from the application servers. If this has not already been done to improve another non-functional characteristic, it must be done to implement a DMZ, and so will add multiple extra network hops for each user transaction.