



## TRANSFORM A REVERSE-PROXY INTO A SECURE ENTRY SERVER

**Reverse Proxies are one of the most accepted methods to protect your web server from Internet attacks. Unfortunately, not all of them offer the protection customers require and demand. This fact sheet provides you with information about advantages and disadvantages of the different models, from the simple, transparent reverse proxy to the Secure Entry Server.**

The classic architecture to operate web servers in the Internet (see figure 1) is straining its limits due to the ever increasing attacks. Even the smallest security gaps in web server or operating system are abused to intrude and maliciously gain access to the systems.

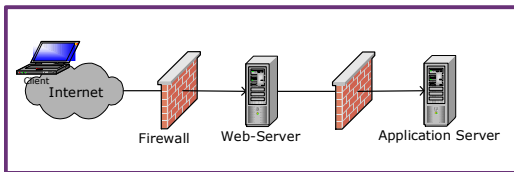


Figure 1: Classic firewall architecture.

The consequences are steeply increased operational cost to keep web server and operating system abreast of current threats by analysing the issues, assessing the risks, and – if necessary – applying the patches. Cost pressure and the need for efficiency boosts demand simplification and centralised solutions. Reverse proxies can provide the answer. By channeling all the traffic through one front-end system, you can greatly reduce the workload as you only have to focus on this one system which protects the others!

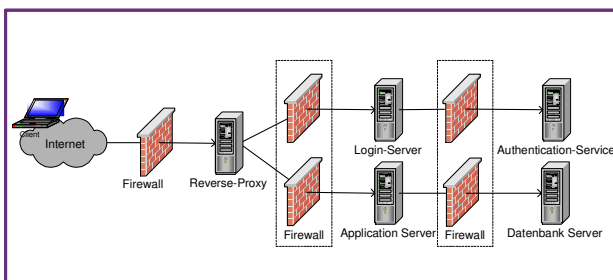


Figure 2: Reverse Proxy architecture.

### WHAT IS A REVERSE-PROXY?

A Reverse Proxy (RP) has much in common with a normal proxy with the main difference being the direction of operation. While the latter is installed at the client-side and hides the Internet, the Reverse Proxy is at the server-side and hides your application servers. It is the only server

visible on the Internet, receives all HTTP-traffic destined for your application servers, and forwards the requests in its own name, as web client. The resulting separation of the TCP connections between browser and server is a Reverse Proxy's main feature (see Figure 2).

### ARE THERE DIFFERENT TYPES OF REVERSE-PROXIES?

Due to its central placement, the Reverse Proxy is ideally positioned to (like a firewall) analyse all incoming requests. Possible actions range from simple forwarding to corrective steps or even request elimination. Reverse Proxies come in the following flavours:

#### Transparent Reverse-Proxy (trp)

A trp is not visible to the application. Its only function consists of receiving HTTP requests and forwarding them unfiltered on to the application server.

#### Reverse Proxy with HTTP request filtering (RPf)

This kind of Reverse Proxy analyses incoming requests before they get forwarded. Depending on its configuration, some of them may be corrected or even eliminated.

#### Reverse Proxy with Authorisation (RPa)

As an additional protection layer, an RPa enforces authentication before client requests can be sent to the application server. Some products even provide coarse-grained authorisation and only allow application access to entitled users.

#### Secure Entry Server (SES)

The Secure Entry Server by United Security Providers is not only a Reverse Proxy with authorization, it also features all known security mechanisms available on the market.

### FIREWALLS.

All borders between Internet, demilitarized zone (DMZ), or application zones are controlled by firewalls. Applying technologies such as packet filtering or stateful inspection, they are responsible to protect your site on the network layer.



### FUNCTIONALITY.

- Filtering of IP packets based on addressing information and protocol flags (origin address, destination address, protocol type, port number, sequence numbers, etc.).
- Prevent unauthorized access by making use of the above filtering technologies. Rules define which system can be accessed how?
- Hide internal network structure.

### REVERSE PROXY INFRASTRUCTURE.

In the DMZ, between Internet and application zones the Reverse Proxy provides the next level of protection. It understands the relevant application layer protocols and denies direct connections to the application server. Thus it is able to provide the means to control user authentication independently from the application and integrate various authorisation systems. One central Reverse Proxy can concurrently provide its protective functionality to all of the companies Internet application servers.

### FUNCTIONALITY.

- Separation of the direct communication paths between users and applications.
- Defense against multiple types of attacks, irrespective of their origin (Internet, intranet or extranet).
- Support different application classes with differing protection needs (public access, member systems, e-business applications).
- Enforce and verify user authentication.
- Provide bastion host, easily maintained and kept at current patchlevel
- Filter requests on application data fields
- Distribute requests to the corresponding application server, including load-balancing and automatic fail-over.
- Data encryption and integrity
- Interface for auditing and intrusion detection systems.

The Reverse Proxy infrastructure usually consists of the Reverse Proxy system itself, located in the DMZ, and the authentication server. The latter supports many standard and high-security mechanisms to securely identify users: passwords, certificates, SecurID, etc. External and proprietary authentication systems, such as RSA ACE Server, can

be integrated as user repositories, it supports Active Directory, LDAP, X.500, and others.

### SECURITY LEVELS.

The following table provides an overview of the security levels that can be achieved by the different Reverse Proxy models:

attack	FW	tRP	RPa	RPf	SES
DoS (Syn-flooding)	Best protection	Medium protection	Unprotected	Unprotected	Unprotected
Protokoll	Best protection	Medium protection	Not anonym	Medium protection	Not anonym
Injection (SQL, XSS)	Unprotected	Unprotected	Unprotected	Best protection	Best protection
Session Hijacking (Cookie Stealing)	Unprotected	Unprotected	Unprotected	Unprotected	Best protection
Malicious Code	Unprotected	Unprotected	Not anonym	Medium protection	Best protection
Unknown Attacks	Unprotected	Unprotected	Not anonym	Unprotected	Best protection

Table 1: security levels.

Legend: **best protection** medium protection unprotected

### DO YOU WANT TO KNOW MORE ABOUT REVERSE – PROXIES?

Reverse Proxies are infrastructure components providing application services. They can never work alone, independently of other systems. Seamless integration is the key to a successful implementation of a Reverse Proxy project. With more than eight years of experience and the know-how from many customer installations- with a major focus on Secure Entry Servers – our experts put invaluable in-depth knowledge at your disposal. They combine integration and security know-how, enabling them to cover the most important aspect of Reverse Proxies. Our focus is the integration of existing security solutions with newly deployed technologies. We support our customers in all project phases, from initial analysis to operational questions, from product selection to integration and implementation of an efficiently functioning system.

United Security Providers. Protecting what matters