
# PAVING THE PATH TO THE ELIMINATION OF THE TRADITIONAL DMZ

A RSACCESS WHITE PAPER

SAFE-T

Smart Security Made Simple.

## 1. The Traditional Role of DMZ

A demilitarized zone or DMZ, is used to refer to any kind of screened sub-network placed between an internal network (i.e., a corporate network) and the Internet. The screening of the subnets is generally achieved by implementing a dual firewall architecture, which typically includes security elements such as bastion hosts, choke routers, reverse proxies, and commercial firewalls. The purpose of the firewalls in such an architecture is to provide controlled access to/from the DMZ from both the Internet as well as the corporate or trusted network.
A DMZ architecture creates three distinct areas (as can be seen in figure 1 below) to which access is controlled by the rules set by the firewalls.

- **The public (Internet) area** - provides no protection to systems located in it. This area is defined as being accessible to the general public. The Internet area is typically used for public Web services or any type of public application services that a company may want to provide to the Internet community (e.g. company web site).
  From a security perspective, all systems and data located in the Internet area are assumed to be insecure and potentially compromised. Any information placed on systems in the Internet area must not be sensitive, critical, confidential or proprietary in nature.
- **The middle area, "DMZ"** - used to house systems that can provide data and application services to clients of the company via the Internet. Such application services are usually comprised of web front-ends to internal systems, such as SharePoint, web mail services, ERP and CRM systems. In some case, companies deploy complete applications including all tiers within the DMZ. This is usually done to improve performance for external users, as well as prevent external users from accessing the internal area (network).
- **The "Internal" area** - represents the corporate or trusted network. All systems and hosts in this area are considered to be fully protected and secured according to company security policies and standards.

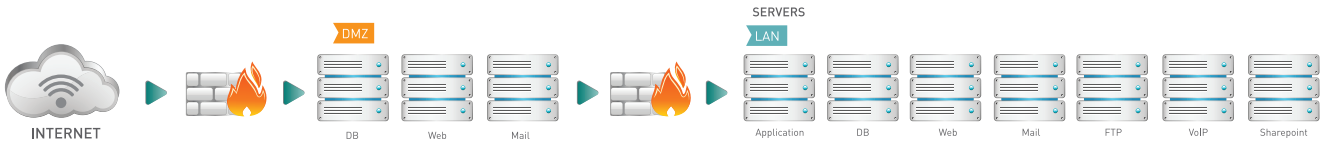


Figure 1 - Typical DMZ Architecture

The three areas are controlled by the external and internal firewalls, which protect and restrict access to/from the DMZ. The primary role of the external firewall is to allow controlled access by providing packet filtering rules as well as additional authentication to systems located in the DMZ. The primary role of the internal firewall is to allow only those systems and services that reside in the DMZ to pass into company network.

## 2. The Challenges of today's DMZ deployments

When deploying a DMZ architecture, CIOs, CSOs, and network administrators face three main challenges:

### 2.1 Ensuring the Security of Application and Data Located in the DMZ

As discussed above, in order to share information with external users, companies extend their application to the DMZ area to create an extranet-facing access point. While this provides direct access for external users, this architecture essentially places servers and databases in the DMZ, which store sensitive information and place them at risk of being hacked or compromised.

In addition, the communication between the servers inside the DMZ is not always secure. This means that if one application is compromised in the DMZ, other applications become exposed to increased risk.

### 2.2 Preventing Hacking into the Internal Network from the DMZ

One of the fundamental security vulnerabilities in most DMZ implementations is that the DMZ's network ports remain open to the Internet. As a result, they expose the entire internal network to external attacks. Hackers relentlessly scan networks for open ports to exploit in order to gain access to the internal network from which they can steal data.

Malicious code, which continuously evolves and becomes ever more sophisticated, can be embedded in legitimate communications in order to exploit network design, implementation and configuration weaknesses and circumvent monitoring and filtering mechanisms. Even if all security mechanisms are kept current and validated vigilantly, the reactive nature of identification of threats and creation of counter-measures creates windows of opportunity for external threats to defeat the network.

These considerations must be taken into account when designing DMZ systems and determining the viability and potential liability of client data that reside there.

### 2.3 Operational & Capital Costs

In addition to security vulnerabilities, the DMZ network configuration also imposes a costly operations burden on the enterprise. To use the DMZ network to protect against external threats, data and services in the internal network must be duplicated in the DMZ. This duplication requires additional hardware and software licenses, as well as perpetual replication processes to ensure that data is synchronized between the internal network and the DMZ. This additional hosting and synchronization requires a complex layer of data and network operations which can be complicated and costly to manage.

## 3. Safe-T RSAccess

Safe-T's patent-pending approach for securing the network from the outside removes the need to open any ports within the internal firewall, providing unmatched protection for enterprise data networks from the Internet and other public networks.

***"Our friends from Safe-T have launched their new RSAccess. After we have tested and learned about the product we absolutely believe it will revolutionize the way we see DMZ and other big security concepts!"***

### 3.1 Deployment

Safe-T's RSAccess Secure Front-End solution is a two tier deployment:

1. **External RSAccess Node –** installed in the DMZ segment
2. **Internal RSAccess Node –** installed on a LAN segment

#### 3.1.1 External RSAccess Node

The role of the external RSAccess node is to act as a front-end to all services published within the DMZ, operating without the need to open any ports within the external firewall, it ensures only legitimate session data can pass through into the LAN.
The external RSAccess node can be deployed in two main locations within the DMZ, either before the web/application front-ends, essentially replacing them completely. Or after the web/application front-ends providing an additional layer of defense within the DMZ and preventing any attacks from being generated from within the front-end servers.

Regardless of the location in which the external RSAccess node is located (before or after the web/application front-ends), its main capability of ensuring secure connectivity into the internal network, allows to move any user directory (e.g. Active Directory) and database services from the DMZ into the internal LAN.

#### 3.1.2 Internal RSAccess Node

The role of the internal RSAccess node is to pull the session data into the LAN from the external RSAccess node, scan it using various security techniques including anti-virus and application firewall, and then pass it to the destination application server.

When Safe-T's RSAccess Secure Front-End solution is deployed in the network, the architecture looks as depicted in Figure 2 below

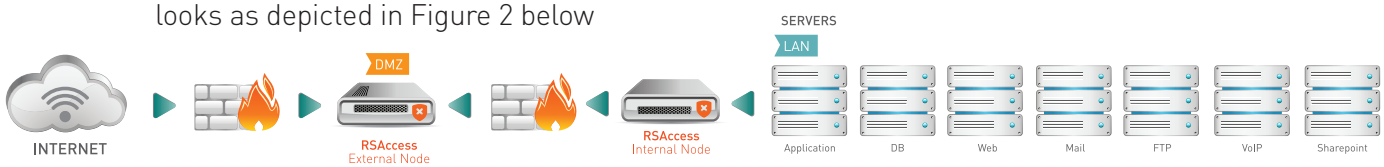


Figure 2 - Safe-T RSAccess Secure Front-End Solution Architecture

### 3.2 How it works?

1. Initial state full session is initiated from the RSAccess Internal Node to the RSAccess External Node on TCP 808.
2. The RSAccess Internal Node checks every few milliseconds for new sessions that arrive to the RSAccess External Node from external clients.
3. Incoming request from the Internet reaches the RSAccess External Node. The RSAccess

External Node strips the key attributes (Port number, Protocol, IP, URL, etc.), verifies the request (Port, White/Black lists, etc), and holds the request in a queue.

4. Once a new session is opened to the RSAccess External Node over the designated service port (e.g. TCP 80 for HTTP traffic), the RSAccess Internal Node opens a session to the destination server over the designated port. A callback session is then opened from RSAccess Internal Node to the RSAccess External Node over the callback port.
5. The RSAccess Internal Node then pulls the TCP session data from the RSAccess External Node, verifies the data using a built in application firewall, and forwards it to designated server.
6. The reply from the designated server returns to the RSAccess Internal Node and pushed to the RSAccess External Node over the callback port.
7. The RSAccess External Node then forwards the reply to the source client.

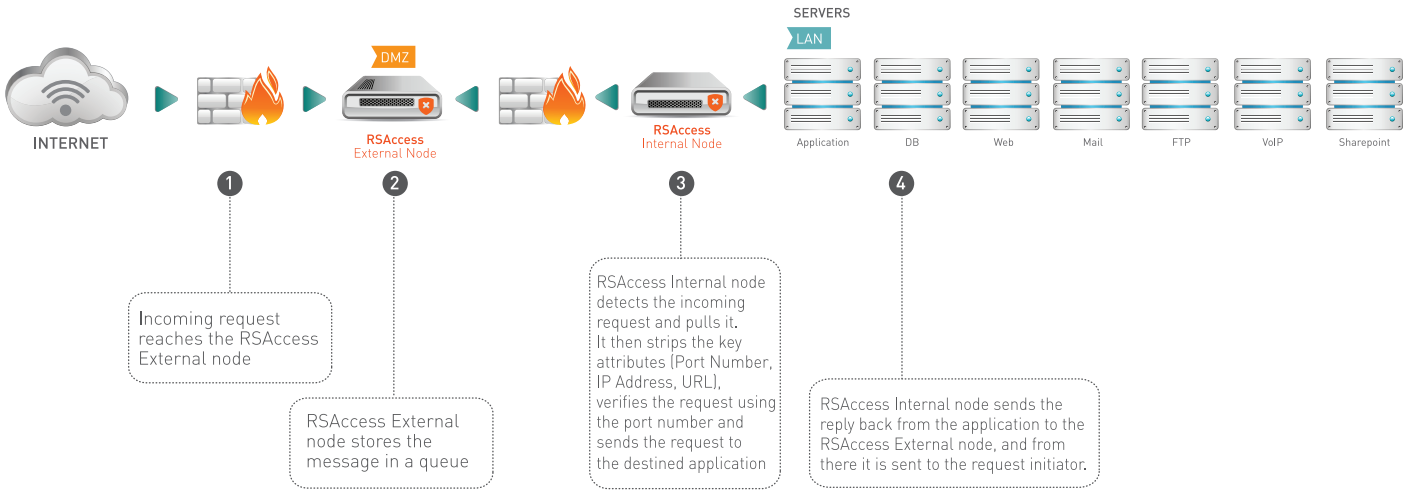


Figure 3 - Safe-T RSAccess Workflow

### 3.3 RSAccess Security Features

RSAccess provides the following layers of security protection:

- **Block Layer 3 and Layer 4 level attacks –** the main benefit of Safe-T's unique technology, which allows passing session data into the internal network without opening any inbound ports on the internal firewall, is that it allows the complete blocking of any network or Layer 4 based attacks such as port scanning, ICMP scanning, TCP bases attacks, etc.
- **Block Application level attacks –** In case a hacker attempts to generate an application level attack such as application exploits, malware, etc, to traverse the pair of RSAccess nodes, the attack will be blocked by RSAccess's built-in application firewall. RSAccess built-in application firewall inspects and controls incoming traffic on the application layer to detect and mitigate attacks of viruses, Trojans, and malware both on clear channels and encrypted channels such as HTTPS.

- **Prevent hacking attempts into RSAccess –** The external RSAccess node does not run any application in order to handle incoming sessions, but rather it utilizes Safe-T's unique listener technology. This means that it is not possible to hack into and take control of the external RSAccess itself to initiate attacks.

## 4. The Difference between RSAccess and a Reverse Proxy

A reverse-proxy is a "backwards" proxy-cache server; it's a proxy server that, rather than allowing internal users to access the Internet, it lets Internet users indirectly access certain internal servers.

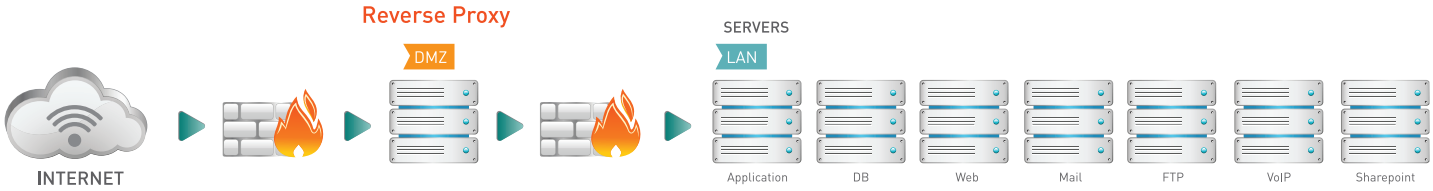


Figure 4 - DMZ Architecture using a Reverse Proxy

The reverse-proxy server is used as an intermediary by Internet users who want to access an internal website, by sending its requests indirectly.
With a reverse-proxy, the web server is protected from direct outside attacks, which increases the internal network's strength. What's more, a reverse-proxy's cache function can lower the workload of the server it is assigned to. For this reason, is sometimes called a server accelerator.

However, for a reverse proxy to operate, the IT administrator must allow certain protocols to pass through the internal firewall and connect to specific hosts in the internal network (e.g. TCP 80/443 for web or Microsoft SharePoint applications). With this configuration, the reverse proxy can access the internal network directly.

Too often, administrators seeking to troubleshoot a problem create a rule allowing full access between a DMZ system and a back-end server on the internal network (or the entire internal network).
As can be seen above, the user of a reverse proxy creates various security and application challenges –

- Once ports are open in the internal firewall, the DMZ is effectively merged with the internal network
- If an external attacker compromises the reverse proxy server, the attacker may also be able to get access into the company's internal servers, applications, and internal network.
- A large number of translations must be done between the reverse proxy and the firewall adding latency to user application requests.

However, as described above, RSAccess does not open any ports in the internal firewall, ensuring that the DMZ and LAN are totally separated environments.
In addition, since the external RSAccess node does not run any application but rather acts as a listener, it cannot be hacked and thus used to launch attacks into the internal network.

The main differences between RSAccess and a reverse proxy can be summarized in the following table:

| Solution | Protection vs. L3-4 Attacks | Protection vs. Application attacks | Resistance to hacking attempts |
|---|---|---|---|
| Safe-T RSAccess | ✓ | ✓ | ✓ |
| Reverse Proxy | ✗ | ✗ requires deploying an application firewall | ✗ |

## 5. RSAccess Use cases

### 5.1 Securing the DMZ Front-End

As discussed above, companies use the DMZ in order to share information with external users, this can be insurance statements in case of an insurance company, or health care information in the case of HMOs. While this provides the end user with streamlined access to the data, it poses great security and operational concerns.

By deploying RSAccess in the DMZ, IT managers can now provide a vastly improved enterprise network security, reducing the DMZ's hardware and software footprint, and eliminating the time- and effort-consuming requirement of data synchronization, thus simplifying network management and business operations.

#### 5.1.1 SharePoint Example

When using SharePoint, if the company wants to share information between users who are within the corporate domain and external users, it is required to extend the SharePoint Web application to create an extranet-facing access point.

Extending an existing SharePoint Web application provides a separate Internet Information Services (IIS) Web site in the DMZ zone. This Web site exposes the same content to all users, even if they are within different security domains. RSAccess allows reducing the number of hardware servers, software licenses, and their associated fees by eliminating application redundancies associated with maintaining data synchronization between the DMZ and the internal network.

#### 5.1.2 Oracle Example

Large Organizations want to expose their Oracle Application services outside their private LAN. Usually these exposures must exist to promote external communication. They want to separate an external network from directly referencing an internal network. The Infrastructure contains front-end server and DB servers in the DMZ zone. RSAccess Simplifies network configuration and reduces hardware footprint by eliminating data redundancy between the internal network and the DMZ.

### 5.2 Protecting Classified Networks

In order to achieve greater security, large organizations also divide their internal networks into disparate sub-networks. Sub-networks avoid compromising the entire network if hackers gain unauthorized access to one of the internal sub-networks. Even though each sub-network is protected by a firewall, it is nevertheless affected with similar vulnerabilities as the DMZ. If sub-network ports remain open, hackers can gain access from one sub-network to another and eventually compromise the entire network.

As RSAccess allows data to travel only in one direction, it can be used in conjunction with the firewalls, enabling connectivity between sub-networks without exposing one sub-network to another and preventing the leakage of sensitive data or the propagation of attacks between sub-networks.

### 5.3 B2B

B2B Ecommerce (business-to-business) forms, is quickly overtaking the brick and mortar, with the purchase of goods and services increasingly performed over the Internet. Online transactions require the use of sensitive credit card data, which are typically exchanged via email and file transfer systems and can easily be targeted for abuse by hackers. RSAccess protects confidential information with Safe-T's unique, high-security encryption technology automatically without the disruption of work practices.

### 5.4 OEM for Software Houses

Software houses that develop applications requiring access to data within the organization (e.g. a mobile Payroll and attendance application, or a mobile application integrating into ERP/CRM systems), are required today to also develop a front-end server which is located in the DMZ and proxies the traffic between the internal application and the mobile end-point.
In addition to the developing the front-end, it is then also up to the software house to convince the organization's IT to open the required ports within the firewall in order for the front-end to communicate with the internal application.

By deploying RSAccess as part of the application (in the form of an OEM) in the DMZ, software houses are now free to develop only their client side and internal side application, without needing to cope with the hassles derived by developing and deploying a front-end. The organization vastly reduces their application's footprint and development costs while simplifying application adoption and deployment.

## 6. Solution Benefits

Eliminates sensitive data from DMZ, paving the path to elimination of the traditional role of the DMZ.

Improves data security by completely closing the HTTP, HTTPS, SFTP, SSH and other protocol ports in the firewall that are constantly exploited by external hackers.

Simplifies network configuration and reduces hardware footprint by eliminating data redundancy between the internal network and the DMZ.

Streamlines network, data management, and business operations by eliminating the ongoing and time consuming duplication of data and applications.

Reduces the number of software licenses and their associated fees by eliminating application redundancies associated with maintaining data synchronization.

Does not affect performance, with end users completely unaware of the background communications processes.

No need to deploy reverse proxy.

Simplified application development and deployment for independent software houses

## 7. Summary

In conclusion, it is clear that the role and architecture of the traditional DMZ has to be evaluated by all organizations' IT and security teams. The evaluation must verify which data is stored within the DMZ and whether it can be relocated it into the internal network or a sub-subnet of the DMZ.

As we saw, by utilizing RSAccess, organization can now freely relocate data and hardware out of the DMZ, eventually eliminating all components from the DMZ, leaving only the external RSAccess node. This allows organizations to continue to publish the required services to the outside world, while ensuring the highest level of security and reducing costs.

To learn more about how you can start the journey to eliminate all components within your DMZ, please go to - http://www.safe-t.com/landingrsaccess/.

© 2013 Safe-T Data Ltd. All Rights Reserved. Safe-T and all other Safe-T product and service names are registered trademarks of Safe-T Data in the U.S. and other countries. All other trademarks and names are the property of their respective owners.