Reference Architecture: Enterprise Security For The Cloud

A Rackspace Whitepaper

RACKSPACE® HOSTING | 1 FANATICAL PLACE | SAN ANTONIO, TX 78218 U.S.A

rackspace®
the open cloud company

Table of Contents

rackspace®
the open cloud company

1. Introduction

As we have stated before[1], maintaining a secure environment for applications and infrastructure is a common concern of companies of all sizes. When building an application and its cloud infrastructure, how should one incorporate security considerations into the design, particularly when there are numerous kinds of attacks, all with varying levels of sophistication?

There is rarely a single answer to all design questions because each application is unique and requires a custom solution that targets its specific requirements. However, some security aspects are common in many applications. The rest of this document will focus on those common aspects and on the specific security products and services that are available at Rackspace.

2. Network and application threat protection

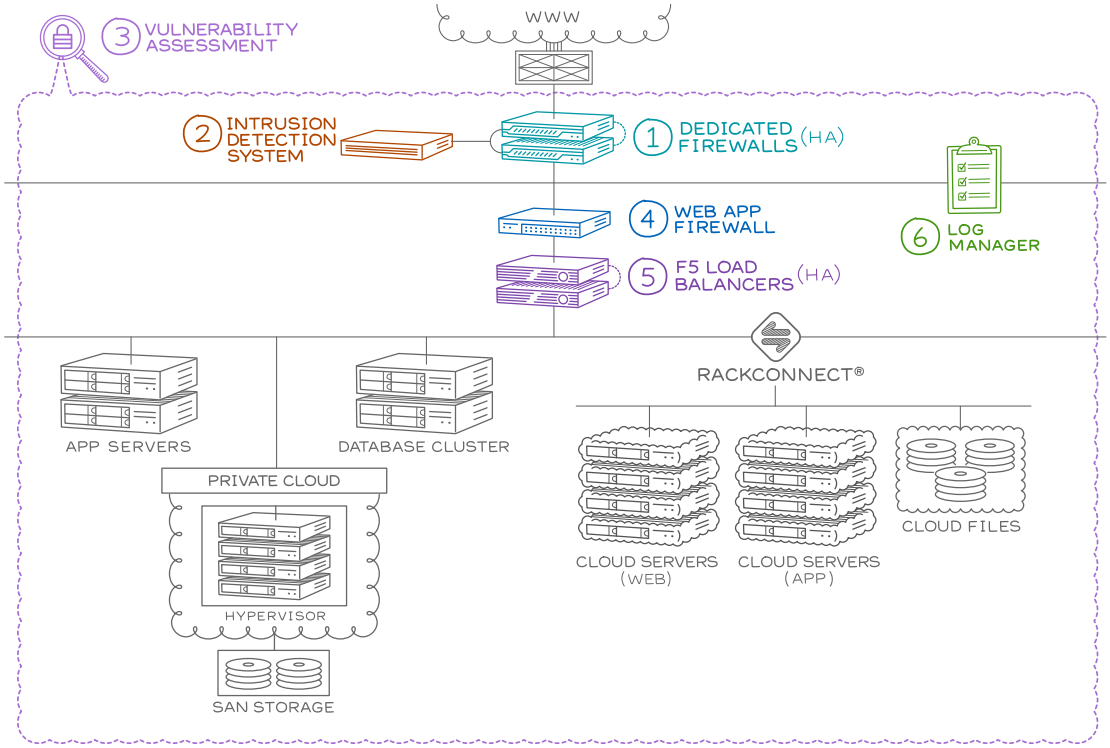
When looking at the top types of incidents that Rackspace identified in a recent month, we found the following:

- 31% of all incidents involved SQL injection exploit attempts
- 21% involved SSH brute force attacks
- 18% involved MySQL Login brute force attempts
- 9% involved XML-RPC exploit attempts
- 5% involved vulnerability scans

Having clarity on the types of attacks that a given architecture might encounter is an important consideration in a design. The reference architecture below reflects that. More importantly, the data also provides insight into the attacks that your own application may face.

3. Reference architecture

The picture below is a conceptual architecture diagram we will use to guide this discussion. In the diagram, we highlight six common components of a secure architecture for a generic cloud solution. Together, all of these components provide security to the rest of the application. In this reference architecture we highlight aspects of a dedicated infrastructure, private cloud and the Rackspace Cloud. The architecture includes application servers, database clusters, a private cloud, and elements from our public cloud, including Cloud Servers™ and Cloud Files™ object storage. RackConnect® provides the connectivity necessary to create the hybrid network, connecting the elements on the public Rackspace cloud with the rest of the dedicated infrastructure.



We will now discuss each of the highlighted security components in the solution.

1. DEDICATED FIREWALL

A firewall is an application's first line of defense of a given application. It serves as an anchor for all other security technologies involved, from load balancers, to web application firewalls and intrusion detection services. Having a dedicated firewall between the public internet and the rest of your infrastructure allows you to control traffic between trusted and untrusted networks.

2. INTRUSION DETECTION SYSTEM

Attackers use many different mechanisms to compromise systems and data. It is important to have controls in place to detect when these attacks are happening to enable a quick response and minimize the possibility of data loss or compromised systems.

According to the Verizon Data Breach Investigation report[2], third parties discovered 92% of all incidents in the study, and 85% of breaches took weeks to discover. In general, attacks are happening without the knowledge of the system owners. An Intrusion Detection System, or IDS, may help give you visibility into these vulnerabilities.

The Rackspace Threat Management offering addresses two key portions of Requirement 11 of PCI-DSS ("Regularly test security systems and processes") through Intrusion Detection Systems and Vulnerability Assessments, which is discussed below.

3. VULNERABILITY ASSESSMENT

Vulnerability Assessment, or VA, is a fundamental security requirement that helps identify exploitable weaknesses in your systems. Periodic scans (which can be performed at different intervals, such as weekly, monthly or quarterly) are required to ensure the timely identification of vulnerabilities that can be introduced as a result of configuration changes or flawed designs.

VA is a preventive control that helps proactively identify an application's or infrastructure's weaknesses before they are exploited. For example, a vulnerability scan could help identify that a given system supports a legacy version of the SSH protocol that is susceptible to brute force attempts, one of the most common forms of attacks. Taking actions to repair a given vulnerability is necessary to prevent future exploits, particularly because attackers use scanning systems to find weaknesses to exploit.

Again, our Threat Management offering at Rackspace includes Vulnerability Assessments to help you address key portions of Requirement 11 of PCI-DSS ("Regularly test security systems and processes"). Rackspace also offers Vulnerability Assessments as a standalone offering.

4. WEB APPLICATION FIREWALL

A Web Application Firewall (WAF) filters and blocks non-essential traffic to the application layer and can protect poorly coded applications from exploits. A very common protection provided by WAFs is to proactively block SQL Injection attempts, another very common form of attack, or to detect and block XML-RPC Exploit Attempts. In general, a network firewall alone cannot block these kinds of attacks.

According to the Verizon Data Breach investigation report referenced above, applications represent the third most used attack vector, just behind remote attacks and use of backdoor channels. However, web applications are associated with over a third of the total data loss. As a gateway to all systems behind a firewall, web applications are a logical target for access to sensitive data, and one that web application firewalls can help protect.

5. LOAD BALANCERS

Load Balancers are traditionally discussed when application availability is a concern, but their security benefits are rarely discussed.

Among many other features, Load Balancers allow for termination of SSL traffic, and can help provide other security benefits, including centralized certificate management, central restriction of weak SSL ciphers (as opposed to doing this on each individual server), and HTTP and HTTPS session persistence.

More commonly known, a load balancer allows for a given server to be taken out of the running environment for patching, and it normalizes TCP traffic which can also help protect against insertion and evasion network attacks, which attackers use to counteract or evade an IDS or a firewall.

6. LOG MANAGEMENT

Log management is a critical defense-in-depth tool because it helps protect, detect and respond to security incidents. From a protection perspective, a log management solution helps identify unauthorized access attempts (such as SSH and MySQL brute force attempts), particularly when coupled with daily Log Reviews before sensitive data is compromised. It can also help detect unauthorized changes and misuse of privileges. Finally, it helps respond to attacks and shorten recovery times by providing insightful log data to support a breach investigation.

4. Conclusion

As we said above, every application has specific security needs. The reference architecture we have discussed here provides an overview of the most common security elements in a cloud solution at Rackspace. Consider these solutions in your design. Rackspace specialists are known for their Fanatical Support®, and can help you in your journey to a more secure cloud implementation.

5. Notes

1. Please refer to **the whitepaper "Security is a Partnership"** available at Rackspace.com
2. Verizon's Data Breach Investigations Report, available at **http://www.verizon.com/enterprise/databreach**

DISCLAIMER

This Whitepaper is for informational purposes only and is provided "AS IS." The information set forth in this document is intended as a guide and not as a step-by-step process, and does not represent an assessment of any specific compliance with laws or regulations or constitute advice. We strongly recommend that you engage additional expertise in order to further evaluate applicable requirements for your specific environment.

RACKSPACE MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED, AS TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS DOCUMENT AND RESERVES THE RIGHT TO MAKE CHANGES TO SPECIFICATIONS AND PRODUCT/SERVICES DESCRIPTION AT ANY TIME WITHOUT NOTICE. RACKSPACE RESERVES THE RIGHT TO DISCONTINUE OR MAKE CHANGES TO ITS SERVICES

OFFERINGS AT ANY TIME WITHOUT NOTICE. USERS MUST TAKE FULL RESPONSIBILITY FOR APPLICATION OF ANY SERVICES AND/OR PROCESSES MENTIONED HEREIN. EXCEPT AS SET FORTH IN RACKSPACE GENERAL TERMS AND CONDITIONS, CLOUD TERMS OF SERVICE AND/OR OTHER AGREEMENT YOU SIGN WITH RACKSPACE, RACKSPACE ASSUMES NO LIABILITY WHATSOEVER, AND DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO ITS SERVICES INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT.

Except as expressly provided in any written license agreement from Rackspace, the furnishing of this document does not give you any license to patents, trademarks, copyrights, or other intellectual property. Rackspace, Rackspace logo, Fanatical Support, RackConnect, and/or other Rackspace marks mentioned in this document are either registered service marks or service marks of Rackspace US, Inc. in the United States and/or other countries. OpenStack® and OpenStack logo are either registered trademarks or trademarks of OpenStack™, LLC in the United States and/or other countries.

All other product names and trademarks used in this document are for identification purposes only to refer to either the entities claiming the marks and names or their products, and are property of their respective owners. We do not intend our use or display of other companies' tradenames, trademarks, or service marks to imply a relationship with, or endorsement or sponsorship of us by, these other companies.