Securing Sensitive Data by Isolation

Introduction

Information security must be a process of continuous improvement. During an examination of UCR's security posture, Computing & Communications (C&C) felt our current model of placing key systems together in layers of private firewalled networks could be improved upon. C&C's new design isolates systems from each other to ensure that a compromise of a low level system does not provide a means to access a sensitive system sharing the same private management or data network. Essentially, C&C has created walled gardens for each type of application.

The catalyst for this design was UCR's new Banner Student Information System (SIS) and Enterprise Systems Bus (ESB). Both the SIS and ESB required additional protection from other systems as well as from external access.

To date C&C has isolated six application environments and plans to add more in the future. The environments are defined as follows:

Application Environment	Description
Banner	The Banner system includes 128 application and database servers running on physical hardware and virtual machines.
Enterprise Service Bus	The ESB consists of 15 virtual machines.
Own Cloud	Own Cloud is UCR's private researcher cloud for storing large research data sets potentially including sensitive or protected information. Data is accessed via two private application servers that manage a replicated, distributed file system.
Infrastructure Services	This network contains the privately accessible DNS, LDAP, Kerberos, Active Directory services that are accessed by the other isolated networks through the Firewall/Router.
Security Compliant Services	Systems in this network do not rise to the level of their own dedicated isolated network. Joining this network requires a robust set of security protocols including OS security monitoring, vulnerability scans, restricted services and access.
Minimum Security Compliant Services	This network contains systems that are unable to meet the robust security protocols of the previous network. It is intended that these systems be the "exception to the rule". It serves to isolate these "exceptions" from the rest of the systems that have higher level security requirements and features. These systems must meet campus minimum security standards of patching, firewalls, and restriction of unnecessary services.

Goals

- Provide a high level of security for sensitive data
- Utilize high-performance technology for isolation to minimize impact to services
- Enforce least access necessary
- Minimize configuration and security maintenance

Technology and Implementation

Previous technology

It has been C&C's practice, for many years, to use private networks for system administration, database access and file server access. This provided layers of security for UCR's application and database servers. However, all servers shared the same management network and the application servers often were connected to the campus or public network for things like web traffic.

New design

The team architected a new design beginning with UCR's Banner implementation isolating application and database servers in their own dedicated network environment with no direct access from any other public or private network. All traffic to/from systems not within the isolated environment must pass through a mediation appliance listed below.

Mediation Appliance	Description
Load Balancer (F5 Big-IP)	Public network access to servers is accomplished through a Load Balancer that also acts as an application firewall. Since isolated servers do not have public addresses the Load Balancer proxies the user requests (e.g. web traffic) to the private address space of the server. Only approved traffic is allowed through the Load Balancer.
Router/Firewall (Cisco ASR 1002-X)	A router with stateful zone-based firewall services controls all access in and out of the isolated private network. This ensures that only approved and necessary communication is permitted between other private and public networks. Examples of external communication are Authentication, Configuration Management, System Reporting, DNS, LDAP, Active Directory and external servers.
VPN (Cisco ASA)	A dedicated VPN is used for management, developer and DBA access to the environments. The VPN grants access to specific systems and ports via access policies based on the username logged into the VPN. Multifactor Authentication further enhances security on the VPN.

Cross Functional Collaboration

The cross functional team that came together included Network Engineers, Systems Engineers, Security and Architecture Experts, and Database Administrators. The team worked together to ensure that the final implementation was reliable, secure and performant.

Configuration of System

Figure 1 shows how the various pieces of this solution are connected. Note the three mediation appliances. Also please note that all communication between environments is controlled by the Firewall. Thus if Banner needs to communicate with the Enterprise Service Bus it goes through the Firewall or alternately to a service on the Load Balancer. The ESB environment is shown in more detail in Figure 2 below.

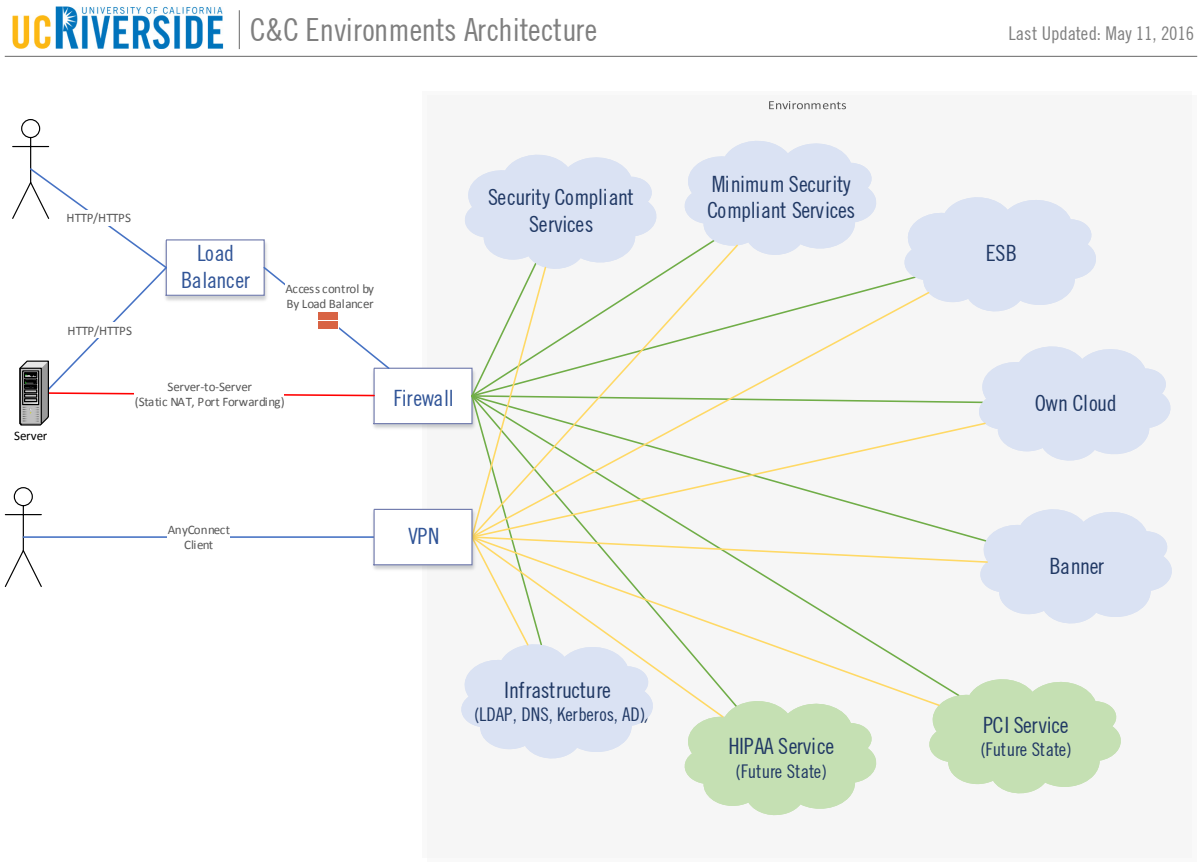

Figure 1: Overall Environments layout

Conclusion

This approach is innovative because of the degree of isolation of each environment. By creating individual walled gardens with highly restricted access controls the security of each environment is enhanced dramatically. C&C believes this approach can serve as a model for other organizations desiring to similarly protect their sensitive systems and we would be happy to collaborate with other locations to share details of our design.

Since C&C began the implementation, the number of isolated environments has grown from two to six. C&C has significantly reduced UCR's risk by moving systems that had interfaces in the campus or

publically routed network to private networks only. These systems have only the necessary services exposed through mitigating firewalls, load balancers and VPNs that restrict access using the least-privilege standard.

Except for a few systems requiring configuration changes to access resources via the new secured access model, there has been minimal impact caused by this improvement to our security posture. Portions of Banner are in production and C&C will complete the full rollout this Fall. Given the number of systems using this new model in production already, this new architecture has been a great success for UCR.

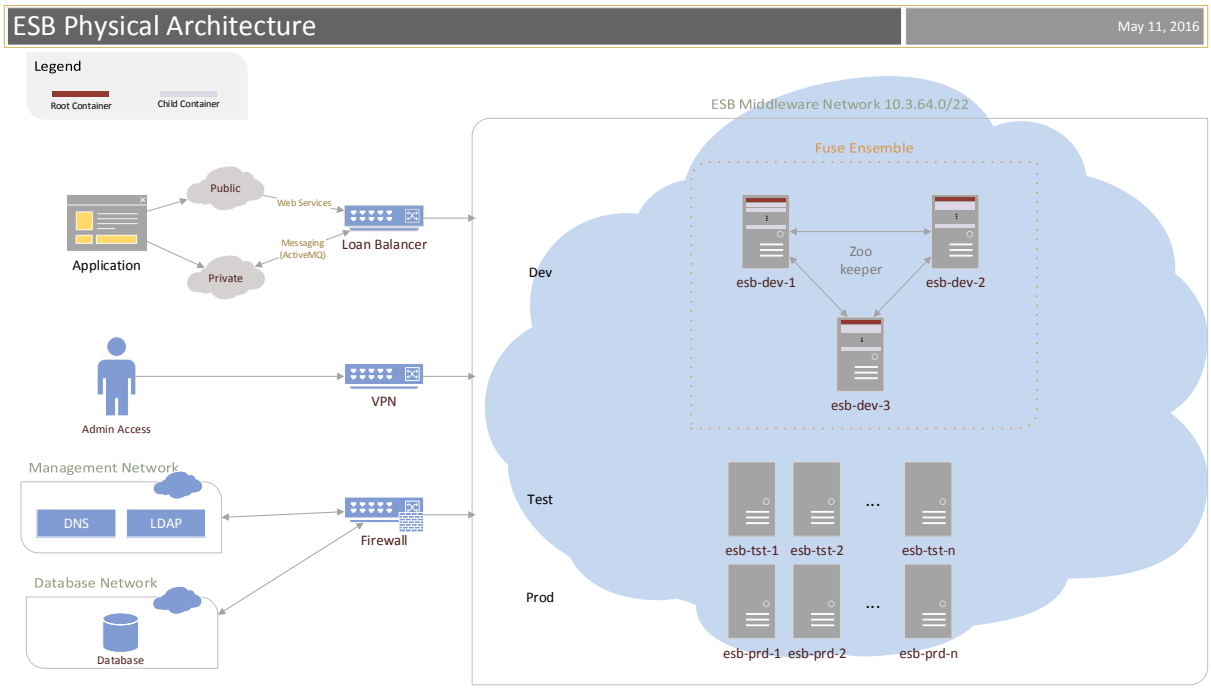

Figure 2: ESB Environment Configuration. Each of the environments are similar.

Testimonials

What an excellent idea it was to create the private network specifically for the Banner Student Information System (SIS). In addition to creating a more secure, well monitored, and restricted environment, the process identified additional UCR developed and other student related systems and processes communicating with Banner SIS that also needed to be locked down. It is a comfort to know that Banner and other student-related transactional systems are together in this single, secure environment. *– Mary Livaudais, Director Academic Information Systems, UC Riverside*

In a world where almost any service can be compromised, isolation is a key component to reducing the risk that one hacked system will not spread to another. This implementation using VPN and private networks goes a long way towards achieving that goal.

– Russ Harvey, Director Computing Infrastructure and Security, UC Riverside

Timeline

February 2014	Project Start
April 2014	Design Completed and Private Banner Environment created
May 2014	Firewall/Router ASR 1002 installed
December 2014	Enterprise Service Bus Environment created
November 2015	Own Cloud Environment created
April 2016	Security Compliant & Minimum Security Compliant Environments created

Project Leaders

Computing & Communications

Michael Kennedy, Enterprise Architect
Stephen Hock, Manager of Infrastructure Engineering
Brett Stetzko, Senior Network Engineer

Team Members

Computing & Communications

Nick Turley, Chief Information Security Officer
Andrew Tristan, Associate Director, Infrastructure and Security
Glen Kanavel, Associate Director, Database Group
Loren Irwin, Infrastructure Engineer
Colleen Jaehnig, Infrastructure Engineer
Daniel Villarreal, Infrastructure Engineer

Submitted By

Bob Grant
Chief Technology Officer
Computing & Communications
University of California, Riverside
bob.grant@ucr.edu
(951) 827-4878