

Security: Letting Them In

Sean Costello

Sean has been working for over 20 years to provide Mac and IT support to business users across North America, most recently with his team at IronGate Server Management in Ottawa.

With a strong interest in being able to deliver service securely without always having to get in the car or hop on a plane, Sean has been quite motivated to ensure that each client network has a secure perimeter in place, with the ability to keep the bad guys out but let the good guys in.

It seems that not everyone knows how to go about this... and so Sean is on a mission.



Providing managed access to business resources:

- Why place limits on existing users?
- Do different users have different access?
- How do you manage data integrity?
- How do you allow yourself (admin) to get in from outside when there are issues?

Identifying access and authorization to resources:

- How do I integrate access with authorization?
- How do I monitor and manage access?
- What do you do when you find an anomaly in access?
 - Be careful how you come off: you may not want to be perceived as “big brother.”

Consider an evenhanded approach:

- Continued monitoring.
- Shutting off access.
- Researching if data was breached.
- Report as required within your organization and by law.
 - Personal credit information and personal health information have specific legal reporting requirements.
 - Do you know the industry? If not, find out!

How to make it easy for the end user to use:

- Consider different ways that people will access.
- Use case analysis.
 - What are the end users actually trying to do?
 - What roadblocks have we placed before them?

With the gap, how can we increase the ease of use for these users?

- Always increase ease of use if it doesn't reduce security.
- If it does reduce security, consider the balance with the client/organization.
- Ensure any legal compliance is still met through the changes in risk.

Business Case Analysis

- Who?
- Why?
- What methods?

Who has access to the data?

- Owners
- Management
- Employees
- Contractors and consultants
- External parties
- Admins
- etc...

Why?

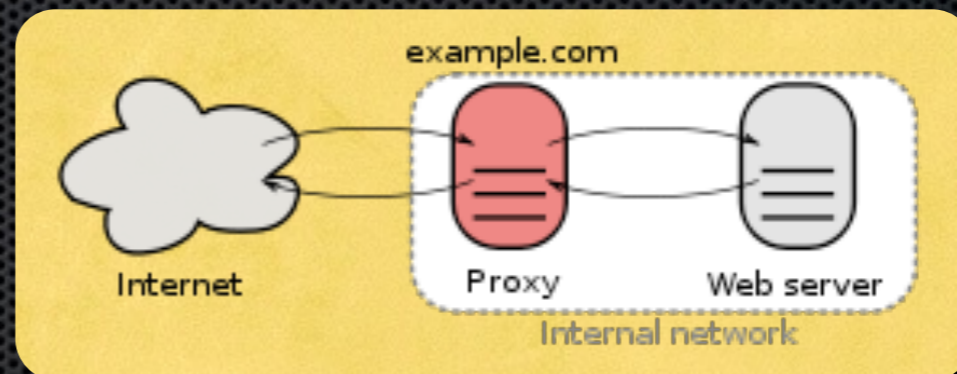
- Who should (based on the actual business) have this access?
- Can we remove parties from this list and conduct business?

What methodologies?

- Methodologies can manage the process in rapidly changing environment.
- Document what access you've implemented.
- How do we identify and manage new roles and/or staff?
- How do we review existing access in our environment?
- How often do you review existing access?

Overcome Through Technology!

- Utilize Reverse Proxies
 - e.g., for specific access rather than general network access.



- Software VPN (OS X!) For Availability
- Data Redundancy For Safety
(The backup session!)

Terms and things you need to know:

- Authentication vs. Authorization.
- Software VPN vs. Hardware VPN.
 - Native vs. IPSec vs. Proprietary.
 - SSL - pros and cons.
- OS X Server capabilities and limitations.
 - Software VPN.
 - Web services.
 - Certificate services.
 - Authentication services (Kerberos, etc.).

SAML, Kerberos, PKI, and/or Federation for Access & Authorization

- Every business is different.
- PKI and Kerberos are free and built into OS X.
- SAML is available from many third party resources.
- Federation is an excellent tool in coordination with a windows environment.

Questions?



Sean Costello

Sean@BackgroundBackup.ca

[@SeanInMotion](#)